

FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Unlicensed Open Source Non-public 5G Networking: Design, Implementation and Evaluation

Filipe Lemos Peixoto



Master in Electrical and Computer Engineering

Supervisor: Ana Cristina Costa Aguiar

Second Supervisor: Adriano Almeida Goes

July 23, 2024

Resumo

A evolução do 5G introduziu a tecnologia nova rádio não licenciada (NR-U) como uma abordagem inovadora para aumentar a capacidade das redes móveis além do espectro tradicional licenciado. No contexto dos Sistemas de Transporte Inteligente Cooperativo (C-ITS), que exigem comunicação robusta e confiável para a operação segura de veículos, a NR-U apresenta uma possível solução para comunicações veiculares de alta densidade quando o espectro licenciado é insuficiente ou indisponível. Devido à natureza compartilhada do espectro não licenciado, torna-se imperativo abordar a necessidade de mecanismos eficientes de coexistência. Estes mecanismos enfrentam desafios intensificados devido aos requisitos rigorosos do C-ITS que necessitam de uma troca de dados precisa e confiável para evitar consequências graves, pois falhas de comunicação podem resultar em riscos críticos para a segurança.

Este estudo pretende avaliar o impacto do mecanismo Listen-Before-Talk (LBT) numa rede 5G privada Autônoma (SA NPN), que opera no espectro não licenciado. O LBT é amplamente utilizado pela sua eficácia em prevenir interferências entre múltiplos dispositivos que coexistem e operam no mesmo canal. Apesar da sua robustez conceitual, as implementações práticas deste mecanismo em redes 5G NR-U continua por explorar, especialmente em cenários de baixa latência e elevado desempenho exigidos pelo C-ITS. A adaptabilidade do LBT em ambientes com elevada intensidade de tráfego representa um desafio crítico, pretendendo esta dissertação avaliar a sua eficácia e aplicação prática.

Para solucionar os problemas mencionados, este trabalho propõe uma implementação do LBT adaptada aos requisitos de uma rede 5G SA NPN. Este estudo analisa a eficiência do LBT como mecanismo de coexistência, avaliando a performance da rede 5G numa banda não licenciada. A análise tem como objetivo verificar se a rede 5G pode manter os padrões de qualidade em diferentes condições e identificar potenciais efeitos de degradação no desempenho da rede. Esta investigação fornece perspectivas práticas e metodologias validadas para melhorar as operações no NR-U, essencial para aplicações C-ITS.

Abstract

The evolution of 5G has introduced the New Radio Unlicensed (NR-U) technology as an innovative approach to enhance mobile network capacity beyond the traditional licensed spectrum. In Cooperative Intelligent Transport Systems (C-ITS), which demands robust and reliable communication for safe vehicular operation, NR-U presents a possible solution for high-density vehicular communications when the licensed spectrum is insufficient or unavailable. Due to the shared nature of the unlicensed spectrum, addressing the need for efficient coexistence mechanisms in NR-U becomes critical. These mechanisms face intensified challenges with C-ITS's stringent requirements for precise and reliable data exchange to avoid severe consequences, as communication failures can result in critical safety hazards.

This research will evaluate the impact of the Listen-Before-Talk (LBT) mechanism in a 5G Standalone Non-Public Network (SA NPN) operating in the unlicensed spectrum. LBT is well-known for its effectiveness in preventing interference among multiple devices coexisting and operating on the same channel. Despite its conceptual robustness, practical implementations for 5G NR-U remain underexplored, especially in low-latency, high-performance scenarios required by C-ITS. The adaptability of LBT in high-demand environments presents a critical challenge, necessitating this investigation into its practical application and effectiveness.

To address these challenges, this work proposes an LBT implementation tailored to 5G's unique requirements. The study will analyze the efficiency of spectrum coexistence under LBT and assess how operation in the unlicensed spectrum influences 5G network performance. It will evaluate the network's ability to sustain 5G quality standards while adhering to strict channel access rules. This research intends to provide practical insights and validated methodologies for optimizing NR-U operations essential for C-ITS applications.

Sustainable Development Goals (ODS) of United Nations

The Sustainable Development Goals (SDGs) established by the United Nations outline a global blueprint for achieving a better and more sustainable future for all. These 17 goals address many global challenges, including poverty, inequality, climate change, peace, and justice. Engineering is key in advancing these goals by developing innovative solutions that drive sustainable progress. This research is integrated within the Route 25 – Agenda for Autonomous, Intelligent, Interoperable, and Inclusive Mobility initiative, which aims to leverage advanced technologies to address market needs in the connected mobility sector. Route 25’s main objective is to enable these companies to transfer more and better quality data to and from the cloud while fostering local interactions among devices and users. This extensive initiative aims to support more energy-efficient mobility systems and infrastructures, contributing to a more sustainable and equitable future. This study, focusing on developing and implementing a network operating system in the unlicensed band for vehicular communication, directly supports SDGs, as detailed in Table 1.

Table 1: Contribution of the study to the Sustainable Development Goals (SDGs)

SDG Goal	Specific Targets	Contribution	Performance Indicators and Metrics
9	9.1 Develop quality, reliable, sustainable, and resilient infrastructure	Cost Efficiency: Utilizing the unlicensed band reduces the need for expensive spectrum licenses, making communication systems more accessible.	Cost savings from license fees, number of new technologies deployed, increase in access points.
11	11.2 Provide access to safe, affordable, accessible, and sustainable transport systems for all	Scalability and Flexibility: The unlicensed band offers scalability and flexibility, rapidly deploying technologies that improve traffic flow and reduce emissions.	Deployment speed, traffic flow improvement, and emission reduction rates.
13	13.2 Integrate climate change measures into national policies, strategies, and planning	Enhanced Data Exchange: Improved communication between vehicles and infrastructure optimizes routes, reduces idle times, and lowers emissions.	Improvement in route optimization and reduction in CO2 emissions per vehicle.

Acknowledgements

First and foremost, I thank my parents, my sister, and my grandparents for all their love, wisdom, and support; without you, I could not have reached this point in my journey. Although I may not say it often, I value you immensely.

I thank my girlfriend and colleague Raquel for all the love and support over the last years. Thank you for making this journey so much better!

I sincerely thank my mentor and professor, Ana Cristina Costa Aguiar, for all the wisdom, time, and support you shared. Your guidance was crucial to the most challenging project of my life. Without your expertise and encouragement, this work would never have been completed. Thank you for being such an instrumental figure in my academic journey.

I want to thank my co-mentor, Dr. Adriano Almeida Goes from Capgemini Engineering, for his support and assistance during my research. Adriano's vast experience was crucial in helping me navigate the complexities of my project.

I also extend my heartfelt thanks to all my friends and family. I am genuinely grateful for everything and value each of you immensely.

Finally, I acknowledge Instituto de Telecomunicações (IT) (UIDB/50008/2020) for hosting this research work under the scope of Project Route 25 (02/C05-i01.01/2022.PC645463824-00000063), funded by I.P. - Agência para a Competitividade e Inovação (IAPMEI).

Filipe Lemos Peixoto

*“Do the best you can until you know better.
Then when you know better, do better”*

Maya Angelou

Contents

1	Introduction	1
1.1	Context	1
1.2	Motivation	2
1.3	Goals and Problem Definition	3
1.4	Document Structure	3
2	Background and State of the Art	5
2.1	Introduction to 5G Network Architecture	5
2.1.1	Mobile Cellular Networks	5
2.1.2	Radio Access Network (RAN)	6
2.1.3	5G Mobile Core (5GC)	8
2.2	5G New Radio (NR)	9
2.2.1	5G NR Resource Grid	10
2.2.2	Frame Structure	15
2.2.3	Duplexing Schemes in 5G NR	15
2.2.4	Physical Channels in 5G NR	17
2.3	The Unlicensed Band	25
2.3.1	5G New Radio Unlicensed (NR-U)	26
2.3.2	Frequency and channel allocation of the 5.9 GHz band	28
2.3.3	Listen Before Talk (LBT) Mechanism	29
2.4	State of the art	31
3	LBT for Standalone 5G NR-U: Challenges and Approach	35
3.1	Network Testbed Setup	35
3.2	Problem Formulation and Approach	38
3.2.1	Design and Configuration of the Unlicensed Band	38
3.2.2	5G NR-U - LBT Design and Configuration	39
4	System Design and Implementation	43
4.1	Setting up the NPN for Band 47	43
4.1.1	Modifications for Band 47 Support	43
4.1.2	Design of the Communication Channel	45
4.2	Implementing the Listen Before Talk (LBT) mechanism	52
4.2.1	Understanding RF Frontend Dynamics and Timing Advances in OAI	52
4.2.2	Data Extraction and Code Integration	53
4.2.3	Identifying Slot Types and Executing the Sensing Phase	54
4.2.4	Computing Channel Energy	55
4.2.5	Channel Occupancy Determination	56

4.2.6	Transmission Cancellation in Occupied Channels	57
5	Experiments, Results, and Discussion	59
5.1	Updating the Testbed for LBT Validation and Performance Evaluation	59
5.2	Evaluating 5G Channel Energy and Interference without LBT	62
5.2.1	Baseline Channel Energy Measurement	63
5.2.2	Impact of Interference on Channel Performance	67
5.3	LBT Validation and Network Performance Evaluation	70
5.3.1	Validating LBT	71
5.3.2	Network Performance Evaluation	72
6	Final Remarks	81
6.1	Conclusion	81
6.2	Future Work	81
	References	83
A	Code Listings	86
A.1	Band Configuration Code	86
A.2	Distributed Unit Configuration File for Unlicensed Band	87
A.3	Listen Before Talk Function	88
A.4	Network measurements and experiments	89
A.4.1	Channel Energy Computation by Slot Type Function	89
A.4.2	Channel Energy Computation by Slot Type with Interference Function . .	90
A.4.3	Channel Energy Analysis and Visualization by Slot Type Code	92
A.4.4	5.85GHz Channel Increasing Interference Generator Code	95
A.4.5	One-Way Average Delay Code	95
A.4.6	5.85GHz Channel Interference Generator Code	96
A.4.7	Average Block Error Rate x Frame Plot	96

List of Figures

2.1	Mobile cellular networks consist of a Radio Access Network (RAN) and a Mobile Core. Adapted from [32].	6
2.2	Standalone 5G Service-Based Architecture (SBA). Source: [33].	8
2.3	Bandwidth parts in 5G NR, showing different symbol durations and subcarrier spacings to meet diverse service demands. Source: [25].	11
2.4	5G NR resource blocks and resource elements. Source: [25].	12
2.5	Relationship between PRBs and CRBs in a BWP.	13
2.6	Resource grid signaling details. Source: [25].	14
2.7	Frame structure of 5G NR, in Time Division Duplex (TDD). Source: [16].	16
2.8	TDD configuration for 5G NR showcasing a 5ms periodicity and numerology $\mu = 1$ (SCS = 30 kHz), corresponding to 10 slots, each lasting 0.5 ms, collectively representing half of a standard 10 ms frame.	17
2.9	Mapping between logical, transport, and physical channels. Source: [16].	17
2.10	Time-frequency structure of Synchronization Signal and PBCH block (SSB). Source: 3GPP TS 38.300.	18
2.11	System information acquisition. Source: 3GPP TS 38.331 - 5.2 System information.	20
2.12	Four-step random-access procedure in 5G NR, illustrating the interaction between the UE and the network via PRACH. Source: [16].	22
2.13	Calculation of Resource Indication Value (RIV). Source: [25].	23
2.14	General block diagram of 5G NR PDSCH and PUSCH. Source: [22].	24
2.15	Portugal frequency spectrum. Source: [35]	25
2.16	Representation of carrier aggregation and dual connectivity.	26
2.17	Comparison of New Radio Unlicensed (NR-U) deployment modes: Dual Connectivity and Carrier Aggregation (left) and Standalone 5G NR-U (right).	27
2.18	Frequency and channel allocation of the 5.9 GHz band reserved for V2X services. Source: [20].	28
2.19	Illustration of the Listen Before Talk process with random backoff. Source: [21].	29
3.1	5G Standalone Non-Public Network Architecture.	36
3.2	Detailed view of the 5G Testbed Radio Access Network (RAN) Components.	36
3.3	CCA timing in the mixed slot during guard time with a 2.5ms TDD periodicity.	40
3.4	CCA timing in every slot with a 2.5ms TDD periodicity.	40
4.1	Channel Bandwidth Configurations for Band 78 by OAI.	45
4.2	The measured frequency bandwidth of the MIMO B210 USRP board for different UHD G values. Source: [39].	50
4.3	Configuration of the channel, located in bands 46 and 47, with a 38.16 MHz bandwidth and 106 RBs, showing Point A and SSB positioning.	51

4.4	Interaction between the gNB and UE with timing advance and slot structure. . . .	52
4.5	Impact of UE Timing Advance on TDD Slot Configuration in OAI.	53
4.6	Overview of Time Division Duplex (TDD) configurations at a 30kHz Subcarrier Spacing (SCS), illustrating the arrangement and timing of DL, UL, and empty phases for different periodicities.	54
5.1	Wireless configuration testbed.	60
5.2	Wireless configuration testbed with proper distance to avoid interference.	60
5.3	TCPdump logs from wlan0 on the SBC in monitor mode, confirming predicted energy values from the 5G NPN.	62
5.4	Channel energy distribution during idle mode with predominantly signaling (control-plane) activity, captured at the UE antenna.	63
5.5	Channel energy distribution during active mode with a throughput of 5 Mbits/s generated using <i>iperf</i> for data-plane traffic in the downlink, captured at the UE antenna.	64
5.6	Channel energy distribution during active mode with a throughput of 20 Mbits/s generated using <i>iperf</i> for data-plane traffic in the downlink, captured at the UE antenna.	64
5.7	Channel energy distribution during active mode with a throughput of 40 Mbits/s generated using <i>iperf</i> for data-plane traffic in the downlink, captured at the UE antenna.	65
5.8	Average energy per slot with only control-plane activity, captured at the UE antenna.	65
5.9	Average energy per slot at 40 Mbits/s in the downlink, captured at the UE antenna.	66
5.10	Average energy per slot with only control-plane activity, captured at the base station (gNB) RX antenna.	66
5.11	Average energy per slot with 8 Mbits/s uplink traffic, captured at the base station (gNB) RX antenna.	67
5.12	Channel energy distribution with episodic interference, showing peaks generated at 1 Hz, captured at the UE antenna.	68
5.13	Channel energy distribution with episodic interference, showing peaks generated at 2 Hz, captured at the UE antenna.	69
5.14	Channel energy distribution with 10-second data transmission streams at 5 Mbits/s, captured at the UE antenna.	69
5.15	Channel energy distribution with 10-second data transmission streams at 20 Mbits/s, captured at the UE antenna.	70
5.16	Channel energy distribution with episodic interference, showing peaks generated each second, captured at the UE antenna with the LBT mechanism enabled. . . .	71
5.17	Channel energy distribution with episodic interference, showing peaks generated each second, captured at the gNB antenna with the LBT mechanism enabled. . .	72
5.18	Uplink Latency with an exponential increase in the interference frequency of 3 ms bursts. Network operating in 5 ms TDD Configuration with LBT Mechanism. . .	74
5.19	Downlink Latency with an exponential increase in the interference frequency of 3 ms bursts. Network operating in 5 ms TDD Configuration with LBT Mechanism. . .	75
5.20	Uplink Latency with an exponential increase in the interference frequency of 3 ms bursts. Network operating in 5 ms TDD Configuration without the LBT Mechanism. . .	75
5.21	Average BLER with an exponential increase in the interference frequency of 3 ms bursts. Network operating in 2 ms TDD Configuration with LBT Mechanism. . .	79
5.22	Average BLER with an exponential increase in the interference frequency of 3 ms bursts. Network operating in 2 ms TDD Configuration without LBT Mechanism. . .	79

List of Tables

1	Contribution of the study to the Sustainable Development Goals (SDGs)	iii
2.1	ARFCN values for different frequency ranges. Source: TS 38.104 Table 5.4.2.1-1	15
2.2	Parameters for each numerology, adapted from 3GPP TS 38.211, Table 4.3.2-1. .	15
2.3	GSCN parameters for the global frequency raster. Source: TS 38.104 Table 5.4.3.1-1.	19
2.4	European Commission implementing decision on unlicensed spectrum.	28
2.5	Supported UE Channel Bandwidths for NR Band 47 (Sidelink). Source: 3GPP TS 38.101-1, Table 5.3.5-1.	29
2.6	Comparison of channel access parameter names and values for ETSI EN 301 893, 3GPP Rel-16, and IEEE 802.11 specifications. Priorities are listed from highest to lowest. AC — Access category. Source: [24].	31
3.1	Overview of the OpenAirInterface (OAI) RAN repository sections.	37
4.1	Resource Blocks (RBs) and spectrum utilization rates for different Subcarrier Spacing (SCS) and channel bandwidths in 5G NR.	46
4.2	Channel bandwidth values for the USRP B210 without three-quarter sampling. .	47
4.3	Channel bandwidth values for the USRP B210 with three-quarter sampling enabled.	47
4.4	RIV Calculations for different SCS and Channel Bandwidths	49
4.5	Final design values for band 47 with different numerologies and channel bandwidths	50
5.1	Antenna and Device Gain Specifications	61
5.2	Interference thresholds for UE and gNB based on interference levels.	67
5.3	Baseline Uplink and Downlink latency for different TDD configurations with the LBT implemented, without interference.	73
5.4	Uplink and Downlink latency under different TDD configurations and interference Levels, with the LBT implemented.	73
5.5	Baseline Uplink and Downlink throughput for different TDD configurations without interference and LBT implementation.	76
5.6	Uplink and Downlink throughput under different TDD configurations and interference Levels, with the LBT implemented.	77
5.7	PDSCH and PUSCH Block Error Rate (BLER) under different TDD configurations and interference levels.	78

List of Abbreviations

5GC	5G Core
5G NR	5G New Radio
5QI	5G Quality of Service Identifier
ADC	Analog-to-Digital Conversion
AF	Application Function
AMF	Access and Mobility Management Function
API	Application Programming Interface
AUSF	Authentication Server Function
BLER	Block Error Rate
BSF	Binding Support Function
BWP	Bandwidth Part
CAM	Connected and Automated Mobility
CCA	Clear Channel Assessment
CoMP	Coordinated Multi-Point
CP	Cyclic Prefix
CQI	Channel Quality Indicator
CRB	Common Resource Block
CSP	Communication Service Provider
CU	Central Unit
CW	Contention Window
DCI	Downlink Control Information
DL	Downlink
DFT	Discrete Fourier Transform
DU	Distributed Unit
eMBB	enhanced Mobile Broadband
FDD	Frequency Division Duplex
FEC	Forward Error Correction
FEUP	Faculdade de Engenharia da Universidade do Porto
FFT	Fast Fourier Transform
GSCN	Global Synchronization Channel Number
gNB	Next Generation Node B
gNB-CU	gNB Central Unit
gNB-DU	gNB Distributed Unit
HARQ	Hybrid Automatic Repeat Request
IFFT	Inverse Fast Fourier Transform
IoT	Internet of Things
IT	Instituto de Telecomunicações
LAA	License Assisted Access
LBT	Listen Before Talk

LTE	Long Term Evolution
LTE-U	Long Term Evolution Unlicensed
MAC	Media Access Control
MCOT	Maximum Channel Occupancy Time
MIB	Master Information Block
mMTC	massive Machine Type Communication
MCS	Modulation and Coding Scheme
mPCIe	Mini Peripheral Component Interconnect Express
NPN	Non-Public Networks
NRF	NF Repository Function
NR-U	New Radio Unlicensed
NSSAAF	Network Slice and Service Authorization and Accounting Function
NSSF	Network Slice Selection Function
NEF	Network Exposure Function
OAI	OpenAirInterface
OAI-RAN	OpenAirInterface Radio Access Network
OFDM	Orthogonal Frequency-Division Multiplexing
OpenAI	Open Air Interface
PDCCH	Physical Downlink Control Channel
PDCP	Packet Data Convergence Protocol
PDSCH	Physical Downlink Shared Channel
PCF	Policy and Charging Function
PHY	Physical Layer
PBCH	Physical Broadcast Channel
PRACH	Physical Random Access Channel
PRB	Physical Resource Block
PUCCH	Physical Uplink Control Channel
PUSCH	Physical Uplink Shared Channel
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RAN	Radio Access Network
RAT	Radio Access Technology
RB	Resource Block
RE	Resource Element
RF	Radio Frequency
RLC	Radio Link Control
RRC	Radio Resource Control
RTS/CTS	Request-to-Send/Clear-to-Send
RU	Radio Unit
SBA	Service-Based Architecture
SCP	Service Communication Proxy
SCS	Subcarrier Spacing
SDN	Software-Defined Networking
SDR	Software Defined Radio
SIB	System Information Block
SIFS	Short Inter-Frame Space
SLA	Service Level Agreements
SMF	Session Management Function

SNPN	Standalone Non-Public Network
SSB	Synchronization Signal Block
TDD	Time Division Duplex
UDM	Unified Data Management
UDR	Unified Data Repository
UL	Uplink
UP	User Plane
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communications
USRP	Universal Software Radio Peripheral
UHD	USRP Hardware Driver
UE	User Equipment
V2X	Vehicle-to-Everything
VRB	Virtual Resource Block
vRAN	Virtualized RAN

Chapter 1

Introduction

1.1 Context

The advent of 5G marks significant advancements in mobile communication and introduces the potential for new and innovative applications. A key feature of 5G is its support for Non-Public Networks (NPNs), which are private 5G environments established under specific Service Level Agreements (SLAs) without a public service mandate. These private networks are becoming increasingly important in various sectors, primarily industrial manufacturing, where reliable, high-speed data transfer is necessary for modern production processes. As industries adopt these private networks, NPNs are emerging as a strategic investment that could reshape traditional business models and enhance operational efficiencies [34].

In addition to industrial applications, 5G is transforming the transportation sector through Connected and Automated Mobility (CAM). The European Commission established twelve "digital cross-border corridors" to test 5G for CAM, supporting multiple projects integrating vehicles, road safety, digital rail operations, and high-value services for users like mobile offices or information [14].

Another significant evolution in 5G technology is its venture into unlicensed spectrum bands, heralded by the new Radio Access Technology (RAT) known as New Radio Unlicensed (NR-U), introduced in TR 21.916 3GPP release 16 [2]. This progression is not the first instance of cellular technologies tapping into an unlicensed spectrum. The 4G network had already initiated this journey with Licensed Assisted Access (LAA), a 3GPP-standardized version of LTE-U (Long Term Evolution Unlicensed).

Integrating unlicensed spectrum into 5G brings this concept to a new set of innovative technologies that seek to expand the network capacity and enhance flexibility, particularly beneficial in areas with high user density. However, this approach carries the main challenges from the previous LAA technology, such as the development of efficient spectrum-sharing mechanisms to avoid potential interference, and also a primary concern if it is possible to support low-latency communications in the unlicensed spectrum [19].

This research work is framed within the scope of the **Route 25 - Agenda for Autonomous, Intelligent, Interoperable and Inclusive Mobility** project, led by Capgemini Engineering and supported by IT (Instituto de Telecomunicações). This extensive project encompasses a broad spectrum of initiatives, including a segment dedicated to deploying autonomous vehicle communications using unlicensed bands for primary communication. This study focuses on implementing 5G NR-U within an NPN to support the operation in the unlicensed spectrum. It details the primary challenges and limitations encountered during this adaptation. The study then evaluates the network's effectiveness in the unlicensed spectrum and evaluates its performance.

1.2 Motivation

Researching the utilization of the unlicensed band in 5G networks centers around the advantage of alleviating frequency bandwidth limitations. Frequency bandwidth limitation refers to the finite capacity of the radio waves available for data transmission, which can lead to congestion and slower data speeds, posing challenges for efficient communication. By operating with NR-U, additional capacity is provided, alleviating these bandwidth constraints [11]. According to recent studies, [36, 12], this configuration allows for significant reductions in latency and increases in reliability, essential for applications requiring real-time communication, such as autonomous vehicles and industrial automation. Leveraging multi-channel access and implementing efficient Medium Access Control (MAC) mechanisms such as request-to-send/clear-to-send (RTS/CTS) can minimize periods without access to the unlicensed band.

Moreover, multiple studies [38, 37, 15] discuss the feasibility of achieving Ultra-Reliable and Low-Latency Communications (URLLC) solely in the unlicensed spectrum, indicating that there is no guaranteed immediate availability for users with packet transmission demands. This mode of operation, known as standalone NR-U, presents significant benefits, especially within non-public networks (NPN). Standalone NR-U, in conjunction with the characteristics of NPN, provides greater control and customization of network resources, offering more flexibility and eliminating dependency on public network infrastructures, which come with heavy regulation and often expensive licensed frequencies [11]. This independence is particularly beneficial for industries that require customized network solutions tailored to their specific operational needs and for applications like connected mobility, where cities or highways can deploy assisted services without relying on communication service provider (CSP) company infrastructure and pricing models, potentially lowering operational costs.

Additionally, a significant motivation for this study is the apparent gap in the community and literature regarding practical implementations of the necessary techniques to support 5G in the unlicensed spectrum. While the 3GPP details various mechanisms and adaptations that permit this mode of operation, it remains uncertain whether these can effectively support low-latency communications or even maintain the standard quality of a 5G network under specific scenarios, particularly in standalone mode.

1.3 Goals and Problem Definition

This research project addresses key challenges and issues associated with deploying NR-U in 5G non-public networks. The main goal is establishing a Listen Before Talk (LBT) mechanism for interference avoidance while operating within the unlicensed spectrum. This implementation ensures regulatory adherence and a fair coexistence with multiple nodes operating in the same band, reducing the potential collisions and maximizing the efficiency of the spectrum usage.

In Route 25, the LBT has raised concerns about the ability to support the stringent low-latency requirements essential in autonomous vehicles. As LBT requires a periodic channel assessment, leading to constant transmission delays, it can restrict its suitability for URLLC applications, especially in heavy interference or densely populated networks. Given these challenges, the primary objective of this study is to analyze LBT and validate its feasibility in environments demanding low-latency communication.

Firstly, our work ventures beyond theoretical analysis to practically implement LBT within 5G NR-U. We detail the integration process and operational challenges, including synchronization issues and channel access rules, which are often overlooked in existing literature. Subsequently, we conduct experiments to evaluate the effectiveness of LBT in managing interference in unlicensed spectra. These experiments aim to provide empirical evidence on the performance of LBT under typical operational conditions, which is scarce in current studies.

Additionally, our research seeks to answer whether LBT is a sufficient mechanism for 5G NR-U, particularly considering the demands of URLLC. Through our approach, we aim to identify and analyze LBT's practical limitations, contributing new insights into its applicability and performance in 5G networks. This implementation must accommodate diverse user demands and a variety of technologies, including Wi-Fi, for bandwidth efficiency and fair communication across environments.

1.4 Document Structure

Beyond the introduction, this dissertation is composed of five additional chapters. Chapter 2 provides a comprehensive background of the 5G architecture and 5G New Radio Unlicensed (5G NR-U). It also presents a state-of-the-art presentation highlighting key concepts and recent advancements, particularly in the field of 5G NR-U.

Chapter 3 delves deeper into the technical issues and the strategic approach undertaken for this research. Building on the foundational concepts from Chapter 2, this chapter outlines with more technical detail the problem formulation and methodical approach toward implementing the LBT mechanism in a standalone 5G network. It discusses the primary tasks in transitioning the network to operate on an unlicensed band and explores the theoretical challenges associated with planning and implementing LBT. Additionally, this chapter provides a detailed description of the network testbed designed to host this implementation and future validation experiments.

In Chapter 4, the focus is on the practical design of the unlicensed band and the integration of the LBT mechanism. This chapter details the specific computational strategies, code implementations, and operational adjustments necessitated by unforeseen limitations. It explains the technical setup for configuring the OpenAirInterface Radio Access Network (OAI-RAN) to support the unlicensed band. It explores the immediate operational challenges in integrating LBT for effective spectrum coexistence, providing a bridge from theoretical groundwork exposed in Chapter 3 to actual system operation.

Chapter 5 focuses on testing and evaluating the network performance with the implementations described in the previous chapters. This chapter outlines the experimental setup designed to validate the LBT mechanism and assess network performance under various conditions. A primary focus is the adaptation of the testbed to include new equipment to generate interference. Following the modification, experiments are conducted to validate the LBT mechanism and analyze the network performance under different levels of interference scenarios. The results will evaluate the network's spectrum-sharing capacity and resilience to disruptions caused by increased interference in the unlicensed band, collecting valuable insights into the network's operational capabilities.

Finally, Chapter 6 concludes the dissertation, summarizing the essential findings and insights from the research, reflecting on the challenges encountered, the methodologies applied, and directions for future study.

Chapter 2

Background and State of the Art

This chapter presents a detailed exploration of the fifth generation of mobile networks (5G), starting with a comprehensive review of its overarching network architecture and fundamental principles. Subsequently, it delves into 5G New Radio (NR) specifics, particularly emphasizing the physical layer (PHY). The discussion then shifts to the New Radio Unlicensed (NR-U) mode of operation, outlining the key technologies and channel access rules that facilitate its implementation in private networks. The latter part of the chapter focuses on current state-of-the-art developments in this field, examining the latest innovations and methodologies shaping the deployment and efficiency of 5G NR-U.

2.1 Introduction to 5G Network Architecture

The 5G network architecture, encompassing the broader Mobile Access Network, is comprised of three primary components: User Equipment (UE), Next-Generation Node Bs (gNodeBs), which function as the base stations, and the mobile core, known as the 5G Core (5GC). Together, these components form the backbone of the 5G system. 5G introduces a significant evolution in the Radio Access Technology, known as 5G NR [32]. The subsequent sections will offer a comprehensive overview of each component, elucidating their functions and how they collectively contribute to the advanced capabilities of 5G networks.

2.1.1 Mobile Cellular Networks

To fully comprehend the architecture of 5G networks, it is essential first to understand the concept of mobile cellular networks. These networks are the backbone of modern telecommunications, enabling wireless connectivity for mobile devices over long distances. They consist of numerous interconnected cells, each served by one or multiple base stations, covering specific geographic areas with overlapping coverage for seamless connectivity [32]. The architecture of a mobile cellular network can be primarily understood through two key components, according to [32]:

- **Radio Access Network (RAN):** The RAN, which encompasses the UE and base stations, manages the radio resources (i.e., spectrum) and ensures efficient, high-quality service delivery, meeting each user's Quality of Service (QoS) requirements. UEs include various devices like smartphones, tablets, vehicles, and Internet of Things (IoT) devices, with some being stationary, such as industrial sensors or routers. The base stations in the RAN form a distributed network that facilitates communication between UEs (User Equipments) and the Mobile Core.
- **Mobile Core:** The Mobile Core is the backbone of the network, handling device authentication, providing internet connectivity for data and voice, tracking user mobility for continuous service, and monitoring subscriber usage for billing.

Figure 2.1 depicts the overall architecture of a mobile access network. The illustration highlights the RAN, featuring the gNodeB – a base station used in 5G networks – and UEs. Also included in the figure is the 5G mobile core (5GC). The subsequent sections will offer a comprehensive overview of each component, elucidating their functions and how they collectively contribute to the advanced capabilities of 5G networks.

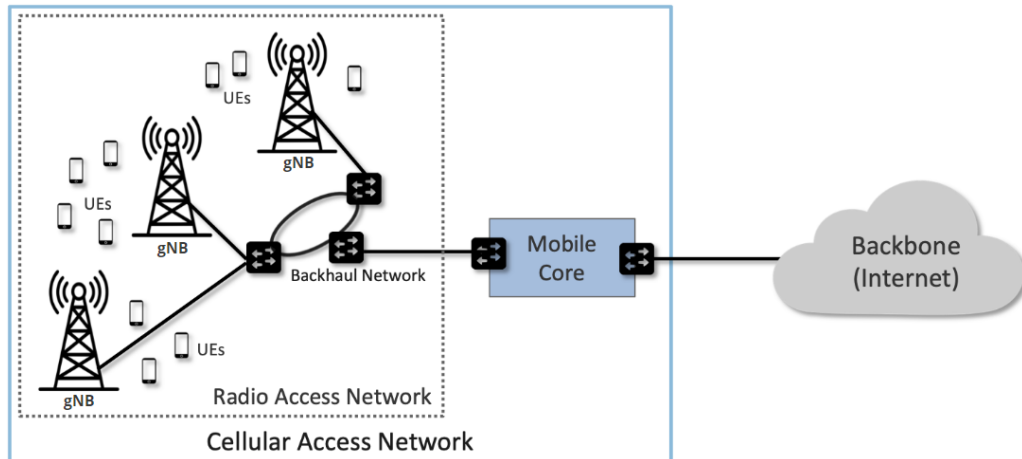


Figure 2.1: Mobile cellular networks consist of a Radio Access Network (RAN) and a Mobile Core. Adapted from [32].

2.1.2 Radio Access Network (RAN)

The 5G Radio Access Network (RAN) is an integral part of the network that manages and distributes the radio spectrum between UEs and base stations.

The base stations are responsible for communication with UEs through electromagnetic radio waves. They are equipped with a multi-layer protocol stack, handling both the digital-to-analog conversion process and the actual transmission and reception of the analog radio waves. The primary function of the RAN in this context is to efficiently manage the radio spectrum, which can be shared among thousands of UEs and numerous base stations across a geographic region.

Regarding specific functions, each base station within the RAN establishes and maintains wireless channels for UEs, manages control plane connectivity between the UEs and the Mobile Core, and establishes tunnels for user plane traffic to the Mobile Core. These base stations are also responsible for forwarding control and user plane packets between the Mobile Core and the UEs, maintaining continuous connectivity and service quality.

The architecture of this component is traditionally centered around base stations, which are the hubs for radio communication with UEs. The gNBs and UEs encompass a series of processing stages as part of their operational pipeline, delineating a symmetrical structure critical that includes several key stages [32]:

- **Radio Resource Control (RRC):** Responsible for configuring the policy-related aspects of the pipeline, operating within the RAN's control plane but not processing user plane packets.
- **Packet Data Convergence Protocol (PDCP):** Handles tasks like compressing and decompressing IP headers, encryption and decryption, ensuring data integrity, and managing packet duplication and reordering.
- **Radio Link Control (RLC):** Focuses on segmenting and reassembling data and ensuring reliable transmission using error correction methods like automatic repeat request (ARQ).
- **Media Access Control (MAC):** Manages buffering, multiplexing, and scheduling decisions regarding data segment transmission. It also enables forwarding decisions to alternative carrier frequencies.
- **Physical Layer (PHY):** Concerned with coding and modulation, including forward error correction (FEC).

Moreover, the virtualization concept, particularly significant in the context of 5G, also modifies the RAN architecture. Virtualized RAN (vRAN) shifts RAN from a traditionally hardware-based system to a more adaptable, software-centric model. In vRAN, network functions are executed on software platforms that can be installed on standard commercial hardware. In line with NFV and SDN principles, this strategy improves scalability and flexibility, potentially lowering costs by reducing the need for specialized hardware.

Simultaneously, RAN is undergoing an architectural evolution characterized by the split RAN process [32]. This includes the concept of splitting the gNB into a gNB-Central Unit (gNB-CU) and one or more gNB-Distributed Unit(s) (gNB-DU), interconnected by the F1 interface [6]. 3GPP defines two main New Generation RAN split architectures in addition to the traditional "monolithic" one, although 3GPP has been extended to agree for multiple split points [5]. The architecture is composed of three main components:

- **Central Units (CUs):** Host the RRC and PDCP layers, managing high-level control plane functions.

- **Distributed Units (DUs):** Handle the RLC and MAC layers for data processing closer to the user.
- **Radio Units (RUs):** Perform D/A conversion and manage the radio frequency (RF) front-end, directly interfacing with the physical transmission medium.

2.1.3 5G Mobile Core (5GC)

The 5GC is responsible for establishing IP connectivity with the RAN. It authenticates UES, tracks their movement across base stations, ensures adherence to QoS requirements, and manages usage for billing purposes.

Separating the Control Plane (CP) and User Plane (UP) has been foundational in telecommunications architectures since the early days of digital and mobile networks. However, 5G networks introduce a novel implementation by physically separating these planes, aligning closely with SDN principles [32]. In this structure, the UP is dedicated to managing the transmission of user data across devices and network services, which encompasses data processing, forwarding, and routing. Conversely, the CP primarily orchestrates network operations, including initiating connections, authenticating user equipment, and managing network-wide optimization and control functions. This logical and physical delineation enhances network flexibility and efficiency, marking a significant advancement in network design.

In line with this evolution, 5GC adopts the 3GPP Service-Based Architecture [1]. Fundamentally, SBA breaks down a system into independent, smaller components known as services. These services are designed to be reused, combined, integrated, and scaled in various ways to create comprehensive network functions or applications. The primary benefit of this architecture is its ability to adapt to changing demands and technologies, enabling organizations to deploy and manage network services more efficiently and with greater agility. Figure 2.2 illustrates the SBA for a 5G network, detailing the user and control plane elements and their interactions. This architecture also showcases the relationship between the RAN and the 5GC components.

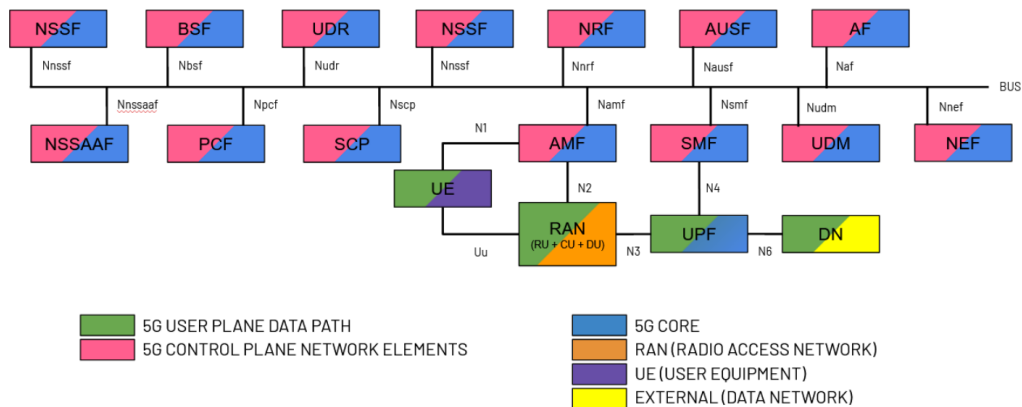


Figure 2.2: Standalone 5G Service-Based Architecture (SBA). Source: [33].

Figure 2.2 SBA components are explained as follows, according to TS 23.501 [1]:

- **NRF (NF Repository Function):** Maintains a repository of available Network Functions in the network.
- **SCP (Service Communication Proxy):** Facilitates communication between services in the SBA and underlying network functions.
- **AMF (Access and Mobility Management Function):** Manages network access and device mobility across different network slices.
- **SMF (Session Management Function):** Handles session setup, modification, and termination between user equipment and the network.
- **UPF (User Plane Function):** Manages the traffic of user data within the network.
- **AUSF (Authentication Server Function):** Performs user equipment authentication and authorization, providing security information to network functions.
- **UDM (Unified Data Management):** Stores user-centric data such as subscription details and device information.
- **UDR (Unified Data Repository):** Holds network-centric data like network slice specifications and policy details.
- **PCF (Policy and Charging Function):** Implements policies and charging rules for network services.
- **NSSF (Network Slice Selection Function):** Determines the suitable network slice for user equipment based on operator policies and user preferences.
- **BSF (Binding Support Function):** Supports binding for authentication of user equipment.
- **NSSAAF (Network Slice and Service Authorization and Accounting Function):** Offers authorization and accounting for network slices and services.
- **AF (Application Function):** Provides network services to applications and manages application-to-network traffic flows.
- **NEF (Network Exposure Function):** Offers a standardized interface for external systems to access network functions and services.

2.2 5G New Radio (NR)

As the successor to 4G's Long Term Evolution (LTE), 5G New Radio (NR) is a new radio access technology (RAT), standardized by 3GPP in release 15, that characterizes the unified and more capable 5G wireless air interface [32] [6]. This section delves into detailed aspects of the physical layer (PHY) because the work conducted in this dissertation requires a thorough understanding of PHY to facilitate its configuration within the testbed environment.

2.2.1 5G NR Resource Grid

The 5G NR resource grid forms the structural backbone of the entire 5G NR architecture, intricately designed to optimize data throughput and network reliability. It is the fundamental framework for structuring all channel and signal mapping, crucial for effectively deploying and operating 5G networks across the PHY and medium access control (MAC) layers.

2.2.1.1 Foundations of OFDM and Subcarriers in 5G NR

To understand the operational capabilities of 5G New Radio (NR), it is crucial to delve into the principles of Orthogonal Frequency Division Multiplexing (OFDM) and the function of subcarriers. OFDM is not a new concept introduced with 5G. It has been a fundamental part of previous wireless standards, including LTE. Its enhanced implementation of OFDM sets 5G apart, which has been adapted to meet more diverse requirements.

OFDM is a digital multi-carrier modulation method where the available spectral bandwidth is divided into multiple narrowband channels called subcarriers. These subcarriers are orthogonal to each other, meaning the peak power spectral density of each sub-carrier aligns with the null points of all other sub-carriers, minimizing the interference between them. This orthogonality allows for dense subcarrier packing, significantly enhancing spectral efficiency, but demands precise timing and frequency synchronization to prevent inter-carrier interference and ensure data integrity across the 5G network.

Each subcarrier in 5G NR independently carries modulated signal-bearing data. Data modulation can vary based on channel conditions and throughput requirements, utilizing various schemes such as QPSK, 16-QAM, or 64-QAM. This modulation is initially performed in the time domain for each symbol sequentially. However, to enable parallel transmission of these time-domain modulated symbols across tightly aligned subcarriers, OFDM employs the Inverse Fast Fourier Transform (IFFT). The IFFT is a mathematical tool that allows these serially modulated symbols to be efficiently transmitted in parallel by distributing them across different frequencies in the frequency domain. This distribution effectively aligns each modulated symbol to a unique subcarrier.

Once transmitted, the OFDM signal transforms back into the time domain using the Fast Fourier Transform (FFT), facilitating the independent demodulation of each subcarrier's data in the frequency domain. This process underscores the concept that while we use mathematical operations to handle signals in distinct domains for practical purposes, these signals coexist across both domains.

5G NR utilizes OFDM for downlink and uplink transmissions, enabling flexible and dynamic resource allocation. A key enhancement in 5G is the introduction of scalable OFDM numerology, which enables subcarrier spacing variations to adapt transmissions to diverse use cases. The subcarrier spacing is $\Delta f = 2^\mu \times 15 \text{ kHz}$, where μ is the numerology index. Figure 2.3 illustrates the division of bandwidth into different parts with varied symbol durations and subcarrier spacings, demonstrating how 5G can be tailored to meet specific service demands, from enhanced Mobile Broadband (eMBB) to Ultra-Reliable Low-Latency Communications (URLLC).

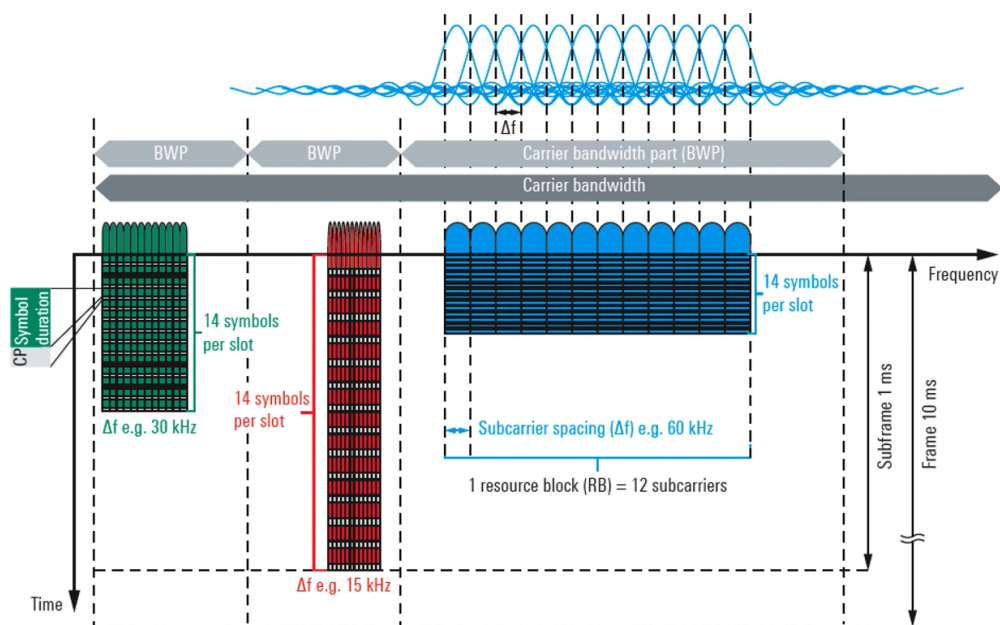


Figure 2.3: Bandwidth parts in 5G NR, showing different symbol durations and subcarrier spacings to meet diverse service demands. Source: [25].

2.2.1.2 Resource Grid Structure (Resource Blocks and Elements)

Building on the foundational understanding of OFDM and its role in optimizing spectrum efficiency in 5G NR, it is equally important to explore how these principles are operationalized as resource elements and blocks.

To provide a comprehensive two-dimensional resource definition that includes both time and frequency domains, the term "resource grid" is used. The resource grid allows for dynamic adaptations, supporting NR's ability to meet diverse operational demands efficiently. Figure 2.4 illustrates the 5G NR resource blocks (RB) and resource elements (RE) structure, highlighting the layered organization within the resource grid that enables such dynamic resource management.

As defined by 3GPP TS 38.211, an RB consists of 12 consecutive subcarriers within the frequency domain. This marks a significant departure from the Evolved Universal Terrestrial Radio Access Network (EUTRAN), used in LTE, where an RB encompasses both frequency and time domain elements—precisely, 12 subcarriers in the frequency domain along with 6 or 7 OFDM symbols in the time domain, depending on the cyclic prefix length. The RB is defined solely as a frequency domain entity in NR. The time domain definition of an RB can vary, with the minimum unit being one OFDM symbol. However, the duration can differ based on the Slot Format and Link-level Information Value (SLIV). This flexibility is exemplified by mini-slots that allocate resources to individual OFDM symbols, a feature crucial for applications demanding URLLC. On the other hand, a RE is the smallest unit of the resource grid in 5G NR, encompassing a single subcarrier in the frequency domain for the duration of one OFDM symbol in the time domain.

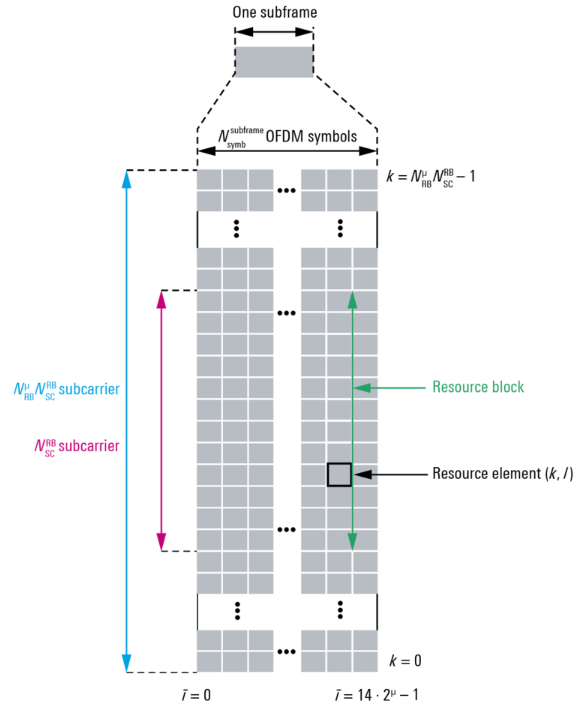


Figure 2.4: 5G NR resource blocks and resource elements. Source: [25].

Additionally, due to the increased flexibility and the introduction of Orthogonal frequency-division multiple access (OFDMA), 3GPP TS 38.211 introduces specific types of blocks:

- **Common Resource Block (CRB):** CRBs serve as a fundamental indexing system within the frequency domain of 5G NR. They number the resource blocks starting from a predetermined reference point, designated as Point A, applicable for a specific numerology or SCS. The primary function of CRBs is to aid in the orientation of frequency allocations within the resource grid. While CRBs do not directly participate in the spectrum allocation process, they are crucial for identifying and referencing frequency positions in a grid that can vary in configuration due to different numerologies.
- **Physical Resource Block (PRB):** In direct association with CRBs, PRBs are used to allocate frequency resources within specific bandwidth parts. They are indexed parallel to CRBs but focus on the spectrum allocation to UE within a Bandwidth Part (BWP).
- **Virtual Resource Block (VRB):** VRBs enable mapping virtual resource block configurations onto physical blocks within the resource grid. This mapping can be implemented in two forms: frequency-contiguous-localized, where virtual blocks correspond to contiguous physical blocks, or distributed, where virtual blocks are mapped across non-contiguous physical blocks. The flexibility offered by VRBs is critical to optimizing resource allocation, particularly in environments with varied and dynamic network demands.

Figure 2.5 illustrates the relationship between PRBs and CRBs within a carrier bandwidth with three BWPs.

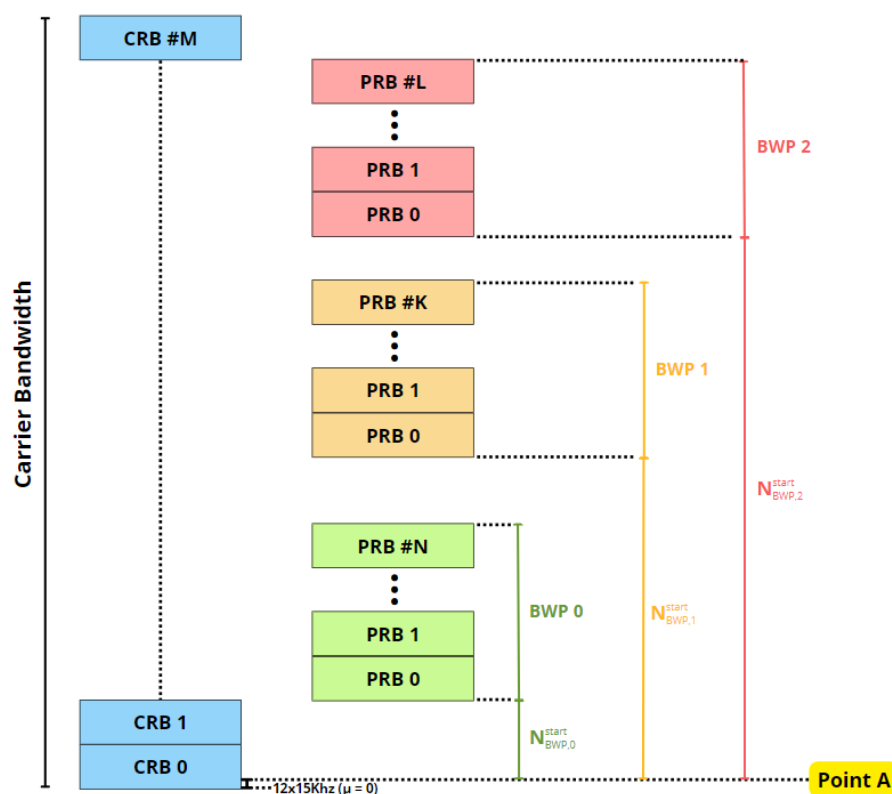


Figure 2.5: Relationship between PRBs and CRBs in a BWP.

In conclusion, each numerology and carrier in 5G NR is associated with a resource grid defined by the number of resource blocks and OFDMA symbols per subframe initiated from a CRB. The definition of a resource grid is adjustable, configured by parameters such as the reference point A and offset to the Secondary Synchronization Signal Block (SSB), which are communicated via the Master Information Block (MIB) and System Information Block (SIB), detailed in Section 2.2.4.1. These parameters are specified within the SCS-Specific Carrier Information Element (IE) and communicated through system broadcast messages or dedicated signaling.

2.2.1.3 The Concept of Point A

In the architectural framework of 5G NR, Point A represents a reference within the frequency domain, allowing the configuration and alignment of resource grids across various subcarrier spacings. Defined in the 3GPP standards, Point A is the center of subcarrier 0 of the common resource block 0 (CRB0) for all subcarrier configurations or resource grids, making it a universal reference point throughout the network's frequency spectrum.

Unlike previous cellular technologies such as LTE, where frequency references might align with the bandwidth edges, Point A in 5G NR does not necessarily coincide with the lower frequency edge of the channel bandwidth. This departure from a bandwidth-centric perspective allows for a more flexible and dynamic approach to spectrum management. It's noteworthy that

Point A can theoretically exist outside the actual carrier bandwidth, a flexibility that enhances the adaptability of NR systems to diverse operational requirements [25].

Moreover, *OffsetToCarrier* specifies the frequency offset from Point A to the beginning of the resource grid for a particular carrier. This offset determines where the carrier's usable frequency range starts relative to Point A. *CarrierBandwidth*, on the other hand, is the total number of CRBs that make up the carrier's bandwidth in the resource grid. This offset and the span of each grid, referred to as *carrierBandwidth*, are quantified in numbers of Common Resource Blocks (CRBs), as stipulated by the higher layer parameter *SCS-Specific Carrier*. This parameterization ensures that every resource grid has a set number of CRBs, with the subcarrier spacing defining the absolute bandwidth of a single CRB, which comprises 12 subcarriers.

Additionally, *OffsetToPointA* is the frequency offset between Point A and the start of the Synchronization Signal Block (SSB), detailed in Section 2.2.4.1. The parameter K_{ssb} defines the subcarrier offset from subcarrier 0 in N_{CRB}^{SSB} to subcarrier 0 of the SS/PBCH block, facilitating the alignment of the SSB within the resource grid's frequency plan. To illustrate the relationship between these elements, Figure 2.6 provides a visual representation of resource grid signaling details.

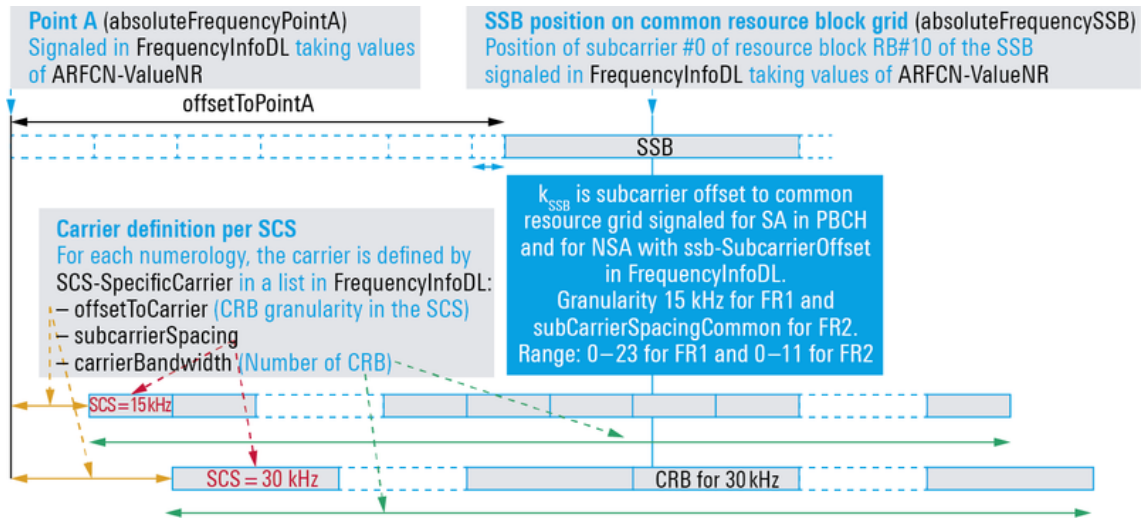


Figure 2.6: Resource grid signaling details. Source: [25].

All the absolute frequency reference parameters are defined in Absolute radio-frequency channel number (ARFCN), which is defined through a specific formula from the 3GPP TS 38.104 specification:

$$\text{Frequency (MHz)} = \Delta F_{\text{Global}} \times (N_{\text{ARFCN}} - N_{\text{REF-Offs}}) + F_{\text{REF-Offs}}$$

This formula, introduced in Release 17, ensures precise calculations necessary for network planning and compliance with communication standards. Table 2.1 provides the ARFCN values based on different frequency ranges specified in 3GPP TS 38.104 Table 5.4.2.1-1.

Table 2.1: ARFCN values for different frequency ranges. Source: TS 38.104 Table 5.4.2.1-1

Frequency Range (MHz)	ΔF_{Global} (kHz)	$F_{\text{REF-Offs}}$ (MHz)	Range of N_{REF} (NR-ARFCN)
0 – 3000	5	0	0 – 599999
3000 – 24250	15	3000	600000 – 2016666
24250 – 100000	60	24250.08	2016667 – 3279165

2.2.2 Frame Structure

Moving from the 5G NR resource grid's detailed components, which delineate the allocation of frequency and time at a micro-level, the frame structure arranges these allocations into a cohesive, timed sequence that dictates how data is processed and transmitted over the network.

In 5G NR, the frame structure is defined to offer a high degree of flexibility in how data is transmitted over the air interface. It consists of frames, sub-frames, and slots, which are dynamically adjustable based on the chosen numerology:

- **Slot:** The primary scheduling unit whose duration depends on the numerology, specifically the subcarrier spacing. Typically, a slot comprises 14 OFDM symbols under normal cyclic prefix conditions. The duration of a slot decreases as the subcarrier spacing increases.
- **Sub-frame:** A sub-frame standard duration is 1 ms. However, the number of slots per sub-frame varies according to the numerology. For instance, with a 15 kHz subcarrier spacing, a sub-frame includes one slot, while a 30 kHz spacing consists of two slots, and so on.
- **Frame:** A frame in 5G NR lasts 10 ms and comprises ten sub-frames, irrespective of the subcarrier spacing. The number of slots in a frame varies based on the numerology, influencing how many slots fit into each sub-frame.

The parameters for each numerology, including the number of symbols per slot and the number of slots per frame and subframe, are detailed in Table 2.2.

Table 2.2: Parameters for each numerology, adapted from 3GPP TS 38.211, Table 4.3.2-1.

μ	$N_{\text{slot}}^{\text{symb}}$	$N_{\text{frame},\mu}^{\text{slot}}$	$N_{\text{subframe},\mu}^{\text{slot}}$	ms per slot	ms per subframe	ms per frame
0	14	10	1	1	1	10
1	14	20	2	0.5	1	10
2	14	40	4	0.25	1	10
3	14	80	8	0.125	1	10
4	14	160	16	0.0625	1	10

2.2.3 Duplexing Schemes in 5G NR

Duplexing defines how uplink (UL) and downlink (DL) communications are structured in cellular networks. In 5G NR, a range of duplexing schemes are introduced, according to [25]:

- **Frequency Division Duplex (FDD) in 5G NR:** This scheme involves using paired spectrum bands for UL and DL. It allows for the dynamic allocation of resources, which can be managed independently for both directions, which is ideal for scenarios requiring balanced traffic and stable connectivity. However, this method requires a guard band to mitigate interference and demands duplex filters at the receiver.
- **Static Time Division Duplex (TDD):** Maintains a fixed UL/DL slot configuration over time, facilitating predictable behavior across cells but limiting flexibility. It is beneficial for environments where the traffic pattern is stable and predictable.
- **Semi-static TDD:** Introduces more flexibility by allowing adjustments to the slot configuration at the frame level, which can be adapted based on network conditions. This scheme uses higher layer configuration parameters to enable cell-specific or user-specific UL/DL allocations, enhancing performance while maintaining control over inter-cell interference.
- **Dynamic TDD:** The most flexible duplexing scheme, enabling slot-level adjustments to UL/DL configurations. This approach suits environments with rapidly changing traffic patterns, such as small cells or isolated indoor settings. Dynamic TDD minimizes the impact of inter-cell interference and supports a highly adaptable network response.

An example of the frame structure in a TDD configuration is represented in Figure 2.7, with a configuration for multiple numerologies, as previously detailed in Table 2.2.

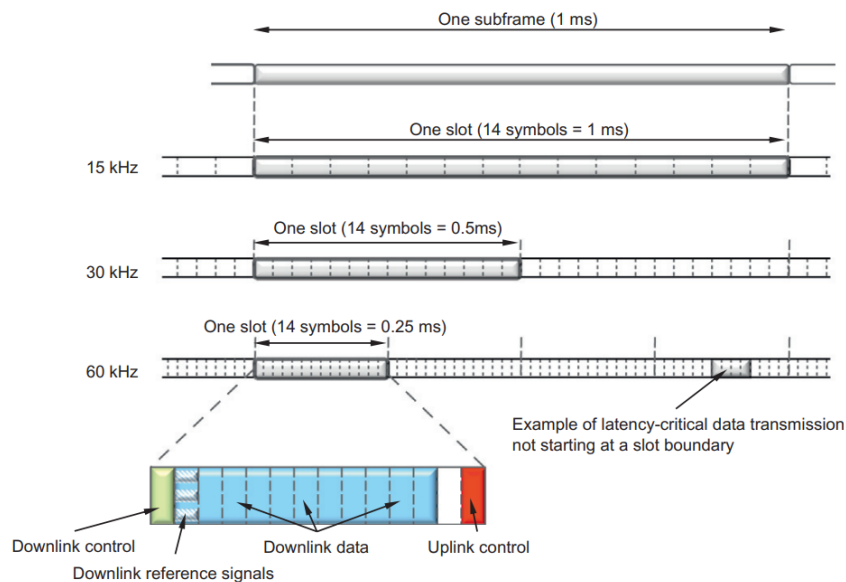


Figure 2.7: Frame structure of 5G NR, in Time Division Duplex (TDD). Source: [16].

When operating in TDD mode, precisely defining the transmission and reception periods is essential. Unlike LTE, where uplink and downlink configurations were predetermined, 5G NR offers more flexibility through the *TDD-UL-DL-ConfigurationCommon* setting, allowing custom definitions of uplink and downlink patterns. This setting specifies the periodicity and number of

uplink and downlink slots and symbols, which can be tailored to the needs of the network, enhancing the efficiency of transmissions. Parameters such as transmission periodicity and the number of uplink and downlink slots are configurable, providing significant adaptability in managing the timing of transmissions based on real-time network conditions.

Figure 2.8 showcases a configuration with a transmission periodicity of 5ms, representing ten slots (half of a frame), illustrating dedicated UL, DL slots, and mixed slots. This repeated pattern is particularly effective for balancing the dynamic demands of uplink and downlink transmissions. The specific number of uplink and downlink slots in a given TDD configuration can change and adapt to different design needs.

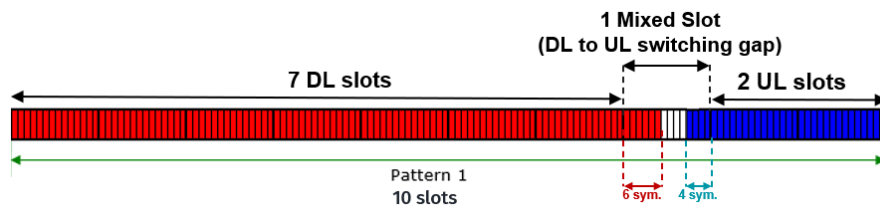


Figure 2.8: TDD configuration for 5G NR showcasing a 5ms periodicity and numerology $\mu = 1$ (SCS = 30 kHz), corresponding to 10 slots, each lasting 0.5 ms, collectively representing half of a standard 10 ms frame.

2.2.4 Physical Channels in 5G NR

In the architecture of 5G NR, channels are classified into three distinct types: Logical, Transport, and Physical. Each channel type fulfills a specific role, contributing to a well-organized and efficient network structure. Figure 2.9 illustrates the channels, clearly representing how they interact within the 5G network architecture.

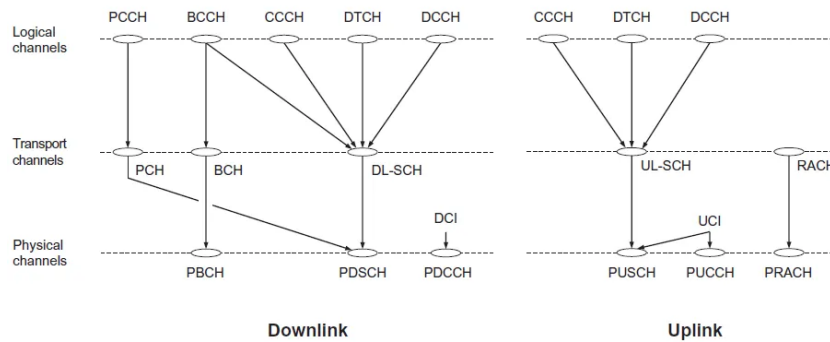


Figure 2.9: Mapping between logical, transport, and physical channels. Source: [16].

Logical channels are divided into two main groups: control channels, which handle the transmission of control plane data, and traffic channels, which transfer user plane data. Transport channels take on multiplexing this logical data for transmission by the physical layer, effectively

managing how data is packaged and delivered across the radio interface. Finally, physical channels are the layers closest to the data transmission over the radio interface. These channels directly convey the data through RF signals across the radio interface, facilitating the final step in data communication [16].

The physical channels are structured and divided according to different functions for both downlink and uplink. In the downlink direction, from the gNB to the UE, the physical channels utilized are the Physical Downlink Shared Channel (PDSCH), Physical Broadcast Channel (PBCH), and Physical Downlink Control Channel (PDCCH). For the uplink direction, from the UE to the gNB, the defined channels are the Physical Uplink Shared Channel (PUSCH), Physical Uplink Control Channel (PUCCH), and Physical Random Access Channel (PRACH).

2.2.4.1 Synchronization signal and Physical Broadcast Channel (PBCH)

In 5G NR, as described in 3GPP TS 38.300, the Synchronization Signal and PBCH block (SSB) consist of primary and secondary synchronization signals (PSS, SSS), each occupying one symbol and 127 subcarriers. PBCH spans 3 OFDM symbols and 240 subcarriers, or 20 RB, but one symbol leaves an unused part in the middle for SSS, as shown in Figure 2.10. This block is designed for the initial cell search, the procedure by which a UE acquires time and frequency synchronization with a cell and detects its Cell ID.

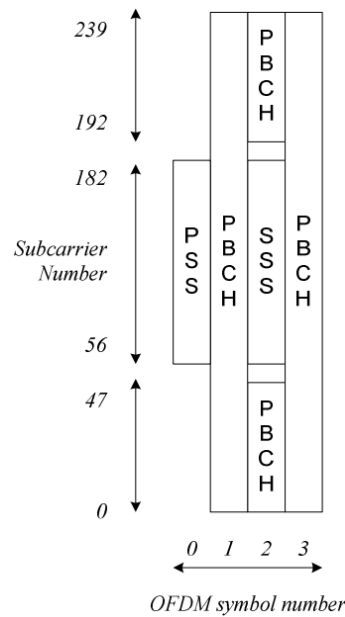


Figure 2.10: Time-frequency structure of Synchronization Signal and PBCH block (SSB). Source: 3GPP TS 38.300.

Unlike LTE, 5G NR utilizes the Global Synchronization Channel Number (GSCN). The GSCN provides a specific set of values where the absolute frequency of SSB can be located within a given band. The formula for converting GSCN to the absolute SSB frequency is defined in 3GPP TS 38.104: $\text{SSB Frequency (MHz)} = \text{Base Frequency (MHz)} + (\text{GSCN} - \text{Base GSCN}) \times$

Frequency Increment (MHz). For a detailed representation, Table 2.3 provides the GSCN values based on different frequency ranges as specified in 3GPP TS 38.104.

Table 2.3: GSCN parameters for the global frequency raster. Source: TS 38.104 Table 5.4.3.1-1.

Frequency Range (MHz)	SS block frequency position SSREF (MHz)	GSCN	Range of GSCN
0 – 3000	$N \times 1200 \text{ kHz} + M \times 50 \text{ kHz}$, $N = 1 : 2499$, $M \in \{1, 3, 5\}$	$3N + (M - 3)/2$	2 – 7498
3000 – 24250	$3000 \text{ MHz} + N \times 1.44 \text{ MHz}$, $N = 0 : 14756$	$7499 + N$	7499 – 22255

Moreover, to detect the SSB, the UE performs the initial cell search, starting to detect the Primary Synchronization Signal (PSS). The detection of PSS serves multiple critical functions, according to 3GPP TS 36.211 [31]:

- **Symbol Synchronization:** This is the process by which the UE aligns its internal timing to match the timing of symbols transmitted by the base station. In practical terms, the UE determines when each transmitted symbol starts and ends. This allows for error-free data reception, demodulating the incoming signal correctly.
- **Frequency Offset Estimation:** It allows the UE to measure and correct any difference in frequency between its oscillator and that of the base station. This is important because even a slight difference in frequency can cause the incoming symbols to blur over time, leading to errors in interpretation.
- **Zadoff-Chu Sequence:** The PSS utilizes the Zadoff-Chu sequence, renowned for its auto-correlation properties. This means that the sequence correlates perfectly with itself at zero offsets and not with its shifted versions, which helps distinguish the start of the PSS even in conditions where multiple paths (reflections) of the signal exist.
- **Cell ID Determination:** By decoding the PSS, the UE identifies a portion of the Cell ID, specifically $N_{(2)}$ ID. Knowledge of the Cell ID is essential for the UE to ensure it communicates with the correct cell, especially in areas with multiple base stations.

Once the PSS is successfully detected, the UE detects the SSS, which is mandatory for two reasons. First, it assists in completing the physical Cell ID determination by providing the $N_{(1)}$ ID, which, when combined with $N_{(2)}$ ID obtained from the PSS, forms the complete Cell ID, defined by the equation: $N_{\text{CELL ID}} = 3N_{(1)\text{ID}} + N_{(2)\text{ID}}$. Secondly, detecting the SSS allows the UE to obtain frame timing information, which allows for proper data decoding and system frame number synchronization.

After detecting the synchronization signals and the Cell ID, the UE can decode the PBCH. The PBCH is responsible for broadcasting the system information, composed of the Master Information Block (MIB) and a given number of SIBs (System Information Block). Unlike LTE,

where all the SIBs are broadcast periodically, 5G NR introduced the SIB by request, which allows transmission only when there is a request from the UE, as detailed in Figure 2.11.

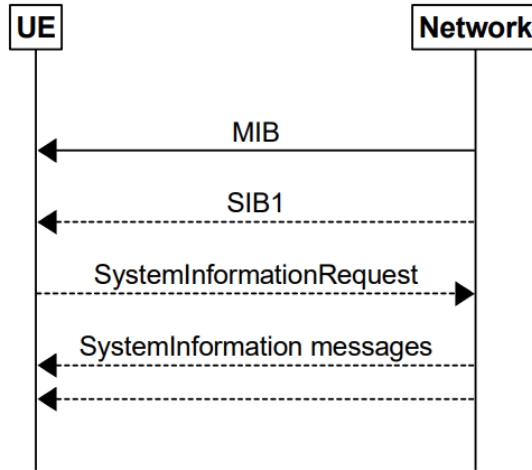


Figure 2.11: System information acquisition. Source: 3GPP TS 38.331 - 5.2 System information.

This MIB is broadcast every 80 ms, as defined in TS 38.212. The first transmission of the MIB is scheduled in subframes as defined in TS 38.213, and repetitions are scheduled according to the period of SSB, which the network can configure. This signal includes the following parameters that are needed to acquire SIB1 from the cell:

- **systemFrameNumber**: Represents the System Frame Number (SFN), a counter that identifies each frame in the system.
- **subCarrierSpacingCommon**: Indicates the Subcarrier spacing for SIB1, Messages 2 and 4 of the initial access, and other SI messages.
- **ssb-SubcarrierOffset**: Indicates the frequency domain offset between SSB and the overall resource block grid in several subcarriers.
- **dmrs-TypeA-Position**: Indicates Position of the first Demodulation Reference Signal (DMRS).
- **pdccch-ConfigSIB1**: Represents the configuration for the Physical Downlink Control Channel (PDCCH) for SIB1 transmission.
- **cellBarred**: Indicates whether the cell is accessible to devices: barred if the cell access is prohibited.
- **intraFreqReselection**: Controls the allowance for reselection to another frequency within the same band. If it is set to not allowed, the UE shall not re-select a cell on the same frequency as the barred cell;
- **spare**: A single bit reserved for future use or padding.

The SIB1 is transmitted on the DL-SCH (Downlink Shared Channel) with a periodicity of 160 ms, as specified in TS 38.213. The default transmission repetition periodicity of SIB1 is 20 ms, but the actual transmission repetition periodicity can be configured. This block includes information regarding the availability and scheduling of other SIBs, indicating whether one or more SIBs are only provided on-demand and, in that case, the configuration the UE needs to perform the SI request.

2.2.4.2 Physical Random Access Channel (PRACH)

The Physical Random Access Channel (PRACH) is an integral part of the 5G New Radio (NR) access network, facilitating the initial connection of UE to the network after successfully detecting a cell and synchronizing with the PBCH, as detailed in Section 2.2.4.1. The initial communication establishment with the network begins when the UE decodes the system information broadcast within the SSB.

PRACH allows the UE to send a preamble, signaling its readiness to communicate and initiate the access procedure. This preamble transmission is the first step in which the UE requests a network connection. It uses a contention-based protocol to manage access attempts by multiple UEs simultaneously. Following the successful reception of the preamble, the network allocates necessary resources to the UE for further communication, which includes providing the details required for establishing a complete connection.

In addition to initiating access, PRACH manages potential signal collisions when multiple preambles are transmitted simultaneously. The network administers these collisions and issues feedback, including timing advance adjustments. This feedback is essential for synchronizing the UEs' transmissions with the network's timing, which is crucial for the integrity and efficiency of subsequent communications.

The random-access process in PRACH is a structured four-step procedure (Figure 2.12), as detailed in [16], designed to handle the access requests from multiple UEs efficiently:

1. **Preamble Transmission (Step 1):** The UE transmits a randomly selected preamble via PRACH. This preamble serves as an initial signal to the network, indicating the UE's presence and its access request.
2. **Random Access Response (RAR) (Step 2):** Upon receiving the preamble, the network sends back a Random Access Response. This response includes a timing advance command to adjust the UE's transmission timing, aligning it more closely with the network's timing structure.
3. **Message 3 Transmission (Step 3):** Following the RAR, the UE sends a connection request message, which includes its identity and other relevant information required by the network to proceed with the connection establishment.

4. **Contention Resolution (Step 4):** The network finalizes the access procedure by sending a contention resolution message. This message confirms the successful establishment of the connection and assigns resources for ongoing communication.

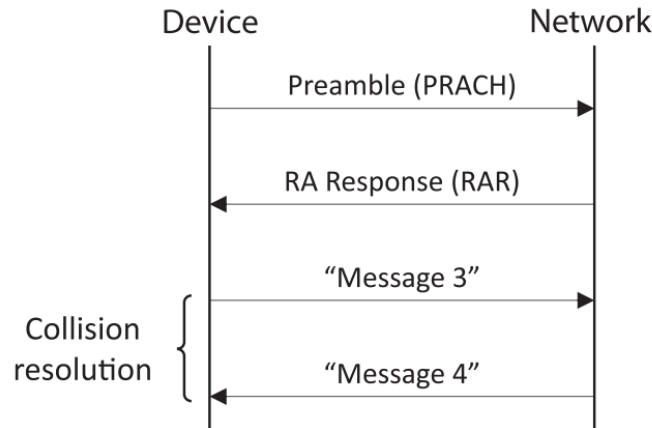


Figure 2.12: Four-step random-access procedure in 5G NR, illustrating the interaction between the UE and the network via PRACH. Source: [16].

These steps ensure that even in simultaneous access attempts resulting in preamble collisions, the network can efficiently process each request, minimizing access delays and optimizing resource allocation. The successful completion of this procedure results in the UE transitioning to a connected state, enabling it to engage in active communication with the network.

2.2.4.3 Control Channels (PDCCH, PUCCH)

In 5G NR, control channels, specifically the Physical Downlink Control Channel (PDCCH) and the Physical Uplink Control Channel (PUCCH), manage the coordination of communication between the base station and UE. These channels convey control information that governs the allocation of network resources and ensures efficient communication.

The PDCCH, designed in 3GPP Release 15 [4], manages the communication schedules between the base station and the User Equipment (UE). It transmits essential control information, primarily Downlink Control Information (DCI), which encompasses several critical functions. According to [13, 30], DCI allocates physical resources for downlink data (PDSCH) and uplink data (PUSCH), adjusting the uplink power for power control to reduce interference, specifying the modulation and coding schemes, managing the Hybrid Automatic Repeat Request (HARQ) processes for reliability, and communicating timing advance corrections to maintain synchronization between the base station and the UE.

Another aspect of DCI is the Resource Indication Value (RIV), which specifies the allocation of resource blocks for downlink and uplink transmissions in 5G networks. As outlined in TS 38.214, the RIV encodes the starting position and the number of resource blocks within a

Bandwidth Part (BWP). This encoding is significant because the scheduling can allocate different numbers of RBs based on transmission needs, ensuring that the RIV precisely indicates the specific segment being scheduled. The RIV calculation considers the total number of RBs in the BWP and the particular needs, including where the RBs start and how many are used. This value is then included in signaling messages, enabling the receiving device to decode it to determine its RB assignment. Figure 2.13 illustrates the RIV concept and how it is computed.

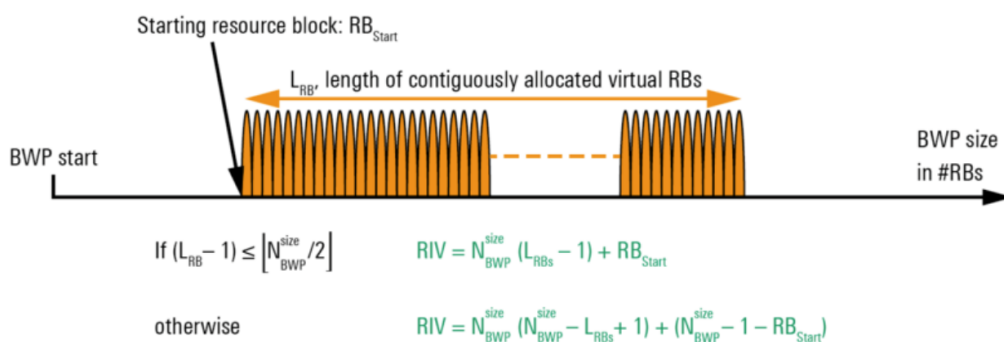


Figure 2.13: Calculation of Resource Indication Value (RIV). Source: [25].

Moreover, the PDCCH operates under a blind decoding mechanism [13]. This means the UE must attempt to decode multiple PDCCH candidates without prior knowledge of which contains relevant DCI, thus requiring efficient processing capabilities to manage potential decoding permutations efficiently.

Following the same logic, the Physical Uplink Control Channel (PUCCH) is a counterpart to PDCCH, focusing primarily on the uplink aspects of control information management. The PUCCH is responsible for transmitting Uplink Control Information (UCI) from the UE to the base station. UCI includes Hybrid Automated Repeat Request-Acknowledgment (HARQ-ACK) for downlink data responses, Scheduling Requests (SR) for uplink resource allocation, and Channel State Information (CSI), which updates the base station on the UE's radio conditions using indicators like Channel Quality Indicator (CQI), Pre-coding Matrix Indicator (PMI), Rank Indicator (RI), layer Indicator (LI) and beam-related information [26]. Unlike LTE, where PUCCH transmission is confined to specific portions of the system bandwidth, NR offers enhanced flexibility in PUCCH configuration to better serve a wide range of applications, particularly those demanding low latency, such as in URLLC scenarios. The NR PUCCH can be configured for short or long durations, depending on the application requirements:

- **Short duration PUCCH:** Typically spans 1 or 2 symbols within a slot and enables rapid feedback by multiplexing with DL and UL data channels in a Time Division Multiplexing (TDM) manner.
- **Long duration PUCCH:** Extends 4 to 14 symbols per slot to ensure robust transmission, accommodating more extensive feedback and control information. It may be multiplexed with the USCH in a Frequency Division Multiplexing (FDM) setup.

2.2.4.4 Data-carrying Channels (PDSCH, PUSCH)

The Physical Downlink Shared Channel (PDSCH) is the primary channel for transmitting user-specific data, system information, paging, and other higher-layer information to all connected devices within a covered area. It also transmits broadcast information not carried on the Physical Broadcast Channel (PBCH), such as System Information Blocks (SIBs). The PDSCH utilizes an Adaptive Modulation and Coding (AMC) scheme, adapting to link conditions such as the signal-to-noise ratio, with allowable modulation schemes including QPSK, 16-QAM, 64-QAM, and 256-QAM. The choice of modulation and coding scheme for each user is determined by the Modulation and Coding Scheme (MCS) specified in the Downlink Control Information (DCI) [9].

In contrast, the Physical Uplink Shared Channel (PUSCH) manages the bulk of uplink data traffic from the user equipment to the base station, including optionally carrying UCI. The PUSCH supports two waveforms: Cyclic Prefix Orthogonal Frequency Division Multiplexing (CP-OFDM) for MIMO configurations and Discrete Fourier Transform Spread OFDM (DFT-s-OFDM) for single-layer transmissions featuring intra-slot frequency hopping. DFT-s-OFDM, known for its lower Peak-to-Average Power Ratio (PAPR) compared to OFDMA, is extensively utilized in the uplink to enhance communication efficiency [22].

Additionally, PUSCH and PDSCH employ Low-Density Parity-Check (LDPC) coding for data channels and Reed-Muller block codes combined with Cyclic Redundancy Check (CRC) for control channels. The general process involves adding CRC to the payload for error detection, followed by selecting an LDPC graph based on the payload size—choosing one graph for smaller payloads and another for larger ones. This payload, referred to as a transport block, is then segmented into code blocks, LDPC-encoded, and subjected to rate matching to synchronize all code blocks. These harmonized code blocks are linked to form a codeword, with up to two codewords transmitted simultaneously on the PDSCH. Codewords are scrambled, modulated based on the adopted modulation scheme, and then mapped to Resource Blocks (RBs) for transmission across the antenna ports as an OFDM signal. The process is detailed in Figure 2.14.

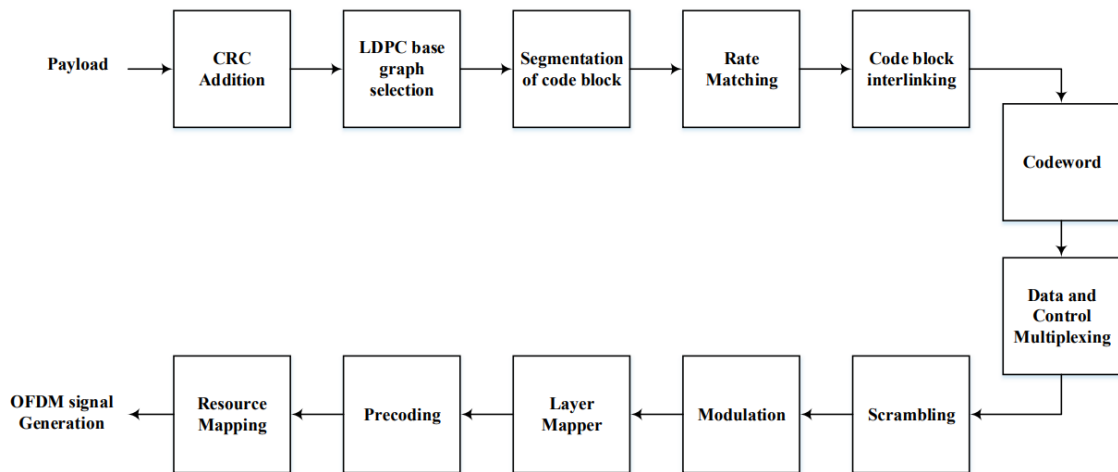


Figure 2.14: General block diagram of 5G NR PDSCH and PUSCH. Source: [22].

The PDSCH and PUSCH facilitate the transmission of various upper-layer channels like PCCH, BCCH, and DTCH. A significant difference is that PDSCH does not transmit DCI, while PUSCH can carry UCI. They mirror each other's functions in uplink and downlink data handling.

2.3 The Unlicensed Band

Spectrum allocation in mobile networks is bifurcated into two primary categories: licensed and unlicensed bands. Licensed bands are specific parts of the radio spectrum that are allocated by regulatory bodies, such as the **Autoridade Nacional de Comunicações (ANACOM)** in Portugal, to individual network operators. These operators purchase the rights to operate within these bands, often through auctions. The key advantage of licensed spectrum is the exclusivity it provides. Since the operator owns the rights to a particular frequency band, there is controlled usage, leading to less interference and more predictable network performance. This makes licensed spectrum ideal for ensuring Quality of Service (QoS) for critical communication and commercial cellular networks. However, this exclusivity comes at a significant cost, as operators must invest substantial amounts to acquire and maintain these rights. Additionally, a public service mandate requires that operators meet specific coverage and service standards, which can be a downside regarding operational flexibility and financial burden. The allocation of these licensed bands in Portugal is visually represented in Figure 2.15.

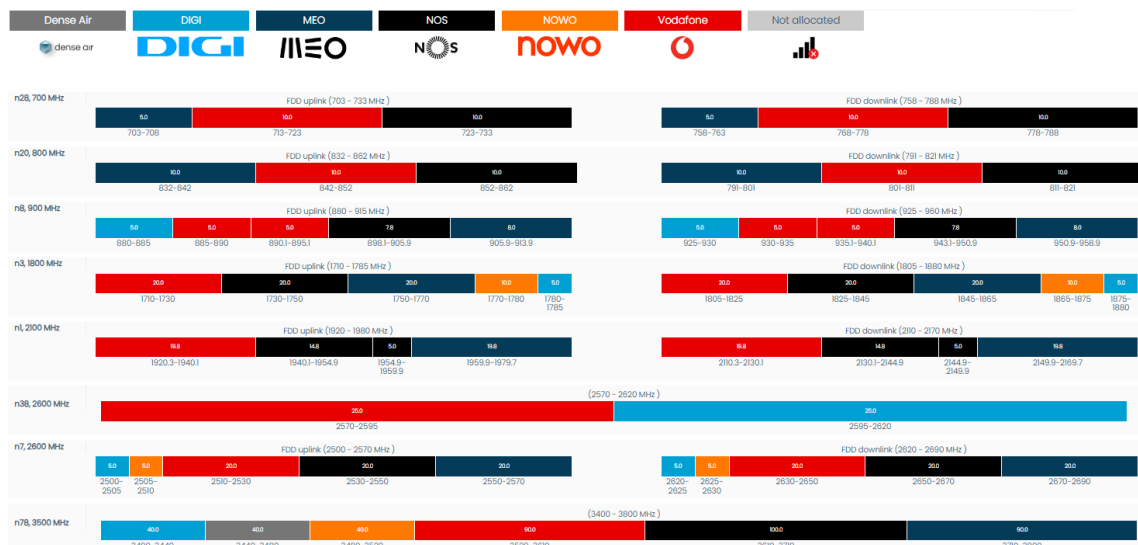


Figure 2.15: Portugal frequency spectrum. Source: [35]

In contrast, unlicensed bands are segments of the radio spectrum that anyone can use without purchasing licensing rights, provided they adhere to the governing bodies' power and operational regulations. The most notable advantage of the unlicensed spectrum is its accessibility and flexibility, allowing for a wide range of applications and innovations. However, this also means that the unlicensed bands are more prone to interference and congestion, as multiple devices and technologies can operate on the same frequencies.

2.3.1 5G New Radio Unlicensed (NR-U)

New Radio Unlicensed (NR-U), introduced in TS 21.916 3GPP release 16 [2], is an evolution of the 4G LTE License Assisted Access (LAA) standards. To comprehend the deployment possibilities of NR-U, it is necessary to understand the underlying concepts of carrier aggregation and dual connectivity. These techniques, previously utilized in LTE, are depicted in Figure 2.16 and detailed as follows:

- **Carrier Aggregation (CA):** This technique allows a mobile device to combine multiple frequency bands into a single logical channel. Specifically, CA enables simultaneous data transmission across several component carriers. Each carrier is treated as a separate entity for processing but managed collectively at the MAC layer. This aggregation can occur intraband, where carriers are contiguous or non-contiguous within the same frequency band, or interband, where carriers are across different frequency bands.
- **Dual Connectivity (DC):** Dual connectivity involves a mobile device maintaining simultaneous connections to two different network nodes. This setup allows for managing two separate data streams that can be used to enhance throughput, reliability, and coverage. In DC, coordination between a master base station and a secondary base station is involved. The separation occurs at the Packet Data Convergence Protocol (PDCP) layer.

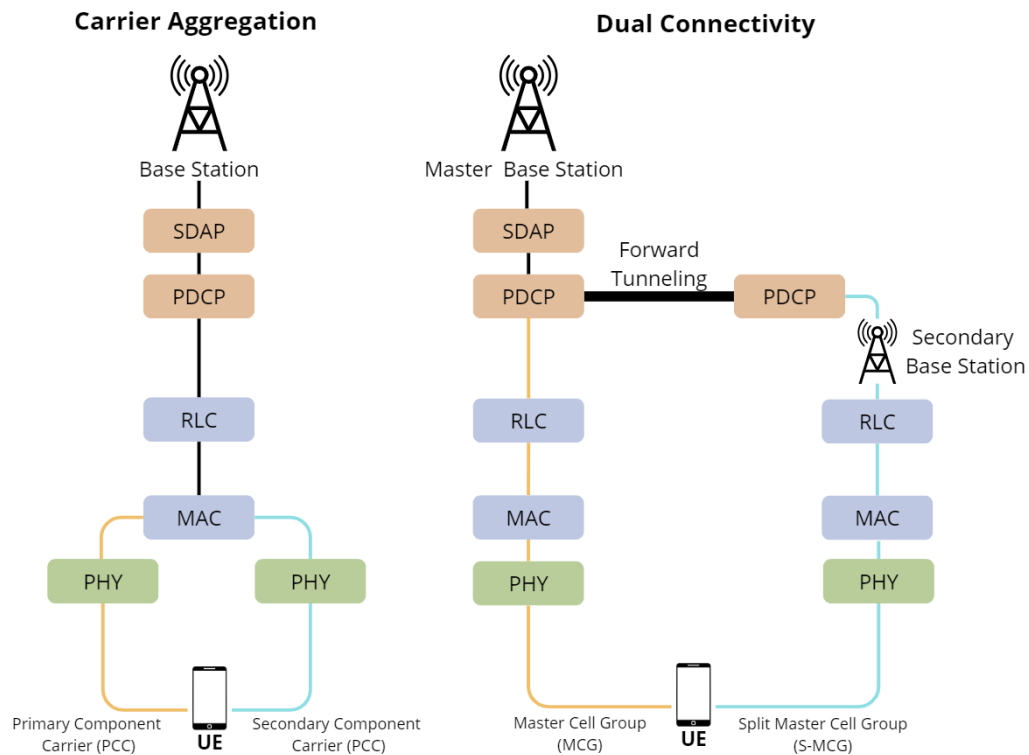


Figure 2.16: Representation of carrier aggregation and dual connectivity.

The NR-U supports the following scenarios, according to [27, 8]:

- **Scenario A:** Carrier aggregation in NR between a licensed band (Pcell) and NR-U (Scell). The NR-U Scell may have both DL and UL or just DL. The NR Pcell is connected to 5GC.
- **Scenario B:** Dual connectivity between LTE in a licensed band (Pcell) and NR-U (PSCell).
- **Scenario C:** Standalone-NR-U connected to 5GC, targeting standalone deployments such as non-public networks.
- **Scenario D:** Standalone cell in an unlicensed band connected to 5GC and UL in a licensed band.
- **Scenario E:** Dual connectivity between NR in a licensed band and NR-U, with the Pcell connected to 5G-CN.

Figure 2.17 represents the deployment modes for Scenarios A, B, and C. It contrasts the dual connectivity and carrier aggregation configurations, which operate independently from the licensed band, which are recognized as anchored NR-U configurations (on the left), against the standalone 5G NR-U configuration (on the right).

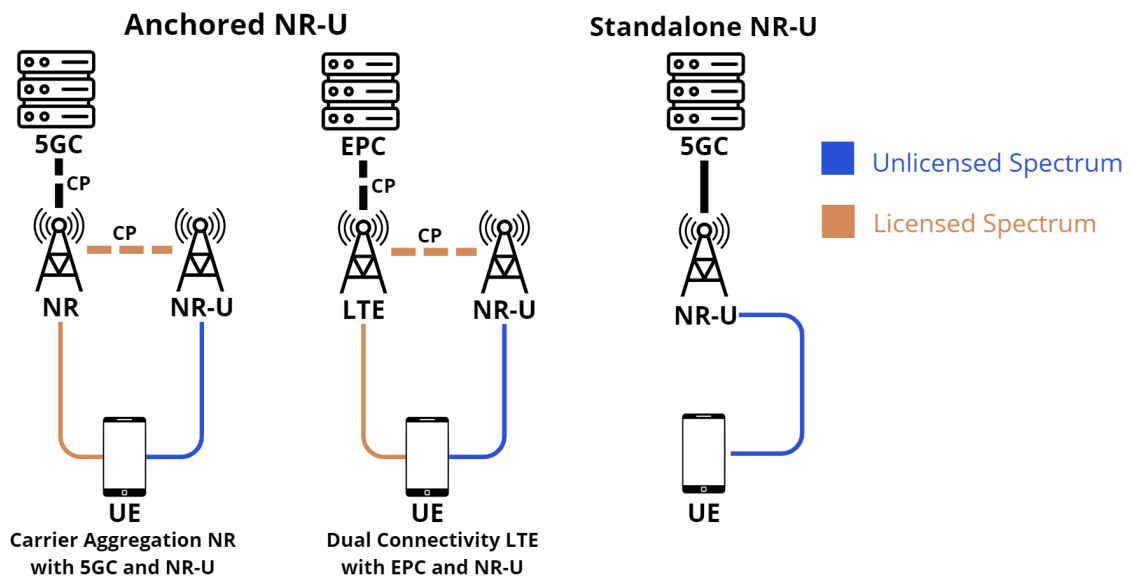


Figure 2.17: Comparison of New Radio Unlicensed (NR-U) deployment modes: Dual Connectivity and Carrier Aggregation (left) and Standalone 5G NR-U (right).

In Europe, NR-U can operate in the frequency range of 5.150 GHz to 5.925 GHz as described in Table 2.4, detailed by Unlicensed National Information Infrastructure (U-NII) bands, by the European Commission [18]. Additionally, the frequency range from 5.945 GHz to 6.425 GHz is currently under discussion.

These bands are shared between 5G and Wi-Fi, so a contention-based Listen Before Talk (LBT) mechanism (referred to asynchronous spectrum sharing) must be employed. This method exemplifies cross-technology spectrum sharing, where each device—a 5G node or a Wi-Fi router—must

Table 2.4: European Commission implementing decision on unlicensed spectrum.

Frequency Range [MHz]	Band	EU legislation
5 150 to 5 250	U-NII-1	2022/179/EU
5 250 to 5 350	U-NII-2a	2022/179/EU
5 470 to 5 725	U-NII-2c	2022/179/EU
5 855 to 5 875	U-NII-4	ECC/REC/(08)01, 2019/1345/EU
5 875 to 5 915	U-NII-4	2020/1426/EU
5 915 to 5 925	U-NII-4	2020/1426/EU

verify the spectrum to ascertain its current use. If the spectrum is occupied, the device delays its transmission until the channel is clear, reducing the likelihood of signal interference.

Although NR-U uses the exact physical (PHY) layer specifications of NR, meaning it has access to multi-numerology and mini-slots, the medium access control (MAC) layer, on the other hand, is aligned with Wi-Fi [2], where an algorithm decides when in time a node is allowed to transmit based on the current channel status and the MAC schedules transmission to minimize the interference in the system to increase the packet reception probability.

2.3.2 Frequency and channel allocation of the 5.9 GHz band

The 5.9GHz band is primarily utilized by the Cooperative Intelligent Transport Systems (C-ITS). Specifically, the European spectrum regulations allocate the 5855-5925 MHz range for ITS applications. This allocation includes the 5855-5875 MHz and 5875-5935 MHz, designated for various C-ITS services to enhance road safety and traffic efficiency. These bands support the IEEE 802.11p/ITS-G5 standard and Cellular V2X (C-V2X) communications, ensuring technology neutrality and interoperability among vehicle communication systems. This spectrum allocation is regulated to avoid interference and ensure the efficient use of the frequencies across Europe by organizations such as 5GAA and C-ITS Deployment Group. Figure 2.18 details the ETSI allocation for ITS-G5.

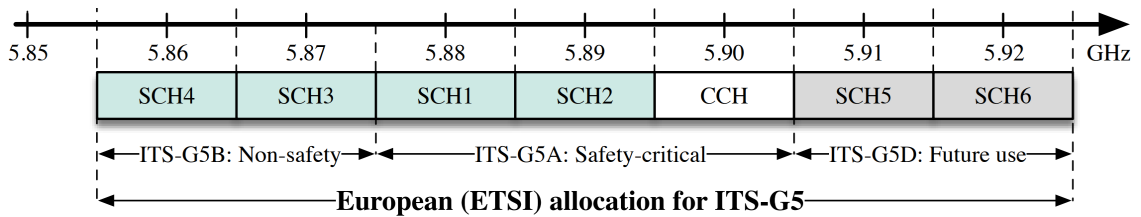


Figure 2.18: Frequency and channel allocation of the 5.9 GHz band reserved for V2X services. Source: [20].

Based on the position paper by the 5GAA [10], the optimal channel bandwidth for Band 47 (5.9 GHz) in Europe varies according to application requirements. For basic safety-related applications using LTE-V2X, a 10 MHz channel bandwidth in the 5905-5915 MHz range is recommended. Meanwhile, for advanced safety-related applications, the deployment of NR-V2X (New Radio V2X) encourages exploring channel bandwidths of 20 MHz or wider within the 5855-5895

MHz and 5875-5895 MHz ranges, specifically prioritizing advanced driving applications. The 3GPP TS 38.101-1 Release 16 document addresses channel bandwidth configuration for the n47 band but in the sidelink. The 3GPP standards indicate approval for 10 MHz, 20 MHz, 30 MHz, and 40 MHz channel bandwidths for various NR bands and Subcarrier Spacing (SCS) configurations, as detailed in Table 2.5.

Table 2.5: Supported UE Channel Bandwidths for NR Band 47 (Sidelink). Source: 3GPP TS 38.101-1, Table 5.3.5-1.

NR band / SCS / UE Channel bandwidth												
NR Band	SCS kHz	5 MHz	10 MHz	15 MHz	20 MHz	25 MHz	30 MHz	40 MHz	50 MHz	60 MHz	70 MHz	80 MHz
n47	15		Yes ¹⁰		Yes ¹⁰		Yes ¹⁰	Yes ¹⁰				
	30		Yes ¹⁰		Yes ¹⁰		Yes ¹⁰	Yes ¹⁰				
	60		Yes ¹⁰		Yes ¹⁰		Yes ¹⁰	Yes ¹⁰				

2.3.3 Listen Before Talk (LBT) Mechanism

Listen Before Talk (LBT), also called Listen Before Transmit or carrier sense multiple access (CSMA), is a technique used in radiocommunications whereby a radio transmitter first senses its radio environment before it starts a transmission. The LBT operation is structured into two primary phases depending on channel conditions. This process is illustrated in Figure 2.19.

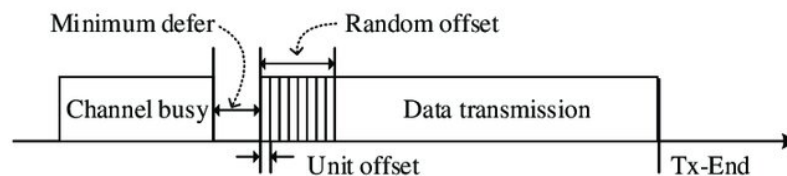


Figure 2.19: Illustration of the Listen Before Talk process with random backoff. Source: [21].

The sensing phase involves the device listening to the channel for a predetermined period to detect the presence of signals from other users. It measures the energy level on the channel and compares it with a predefined threshold to determine if the channel is busy. If the channel is free, the device enters a backoff step, waiting for a random period before attempting to transmit. This randomization is crucial as it helps prevent multiple devices from starting their transmissions simultaneously, reducing the risk of collision and interference. Suppose the channel is busy after several attempts, depending on the protocol specifics and settings. In that case, the device might delay its transmission attempt or cancel it altogether, possibly notifying the upper layers of the network stack about its transmission failure. After a successful sensing phase, the device transmits data over the channel for a maximum period delineated by the Channel Occupancy Time (COT), regardless of the traffic load.

2.3.3.1 LBT in 4G LTE and 5G NR

In NR-U, four distinct LBT categories are defined, each setting specific guidelines for channel access, according to 3GPP TR 21.916 version 16.0.1 [7]. As explained in [19], these categories dictate how a device should behave during transmission:

- **Category 1 LBT:** This mode allows for immediate data transmission after a very brief interval of 16 microseconds, bypassing the Clear Channel Assessment (CCA) process. Category 1 is analogous to the ALOHA protocol.
- **Category 2 LBT:** In this category, devices conduct a fixed-duration CCA, usually around 25 microseconds, to check channel availability. After the CCA, if the channel is clear, the device transmits immediately. This method is similar to 1-persistent Carrier-sense multiple access (CSMA).
- **Category 3 LBT:** The LBT process includes a CCA and a random backoff mechanism if the channel is busy. The duration for CCA is randomly selected from a predefined range known as the contention window (CW). This randomness in backoff timing helps to prevent simultaneous transmission attempts by multiple devices, thereby reducing the risk of signal collision. This category resembles CSMA with static random backoff.
- **Category 4 LBT:** Similar to Category 3, this category also involves a random backoff mechanism and CCA. However, the size of the CW from which the CCA duration is selected can vary depending on the channel conditions. This variability allows the device to adapt its channel access strategy more dynamically to the fluctuating nature of wireless environments. Category 4 is similar to CSMA with dynamic random backoff, akin to the functionality observed in Wi-Fi technologies.

It is essential to emphasize that the foundational principles of LBT closely resemble those of MAC mechanisms such as ALOHA and CSMA. This similarity allows us to leverage Kleinrock's research [23] to anticipate network behavior under similar traffic assumptions, a subject thoroughly explored in Wi-Fi. By understanding these foundational parallels, we can better assess the potential impacts and efficiencies of LBT in real-world scenarios.

2.3.3.2 Channel Access Rules in the 5 GHz Band

In addition to the LBT categories detailed in Section 2.3.3.1, technologies operating in Europe's 5 GHz unlicensed band must adhere to the ETSI EN 301 893 standard [17], which defines the LBT mechanism for Frame Based Equipment (FBE) and Load Based Equipment (LBE) [17].

The LBT mechanism mandates that devices ensure the channel remains idle for 16 μ s—the Short Inter-Frame Space (SIFS)—before initiating any transmission [24]. If a signal surpasses the energy detection threshold, set between -75 and -85 dBm/MHz, the device must delay its transmission and engage in a Clear Channel Assessment (CCA). This threshold range varies depending

on the equipment used, the duplexing scheme, and the environmental conditions, influencing the sensitivity of the channel sensing mechanism.

During CCA, the device observes the channel over multiple slots, each at least $9 \mu\text{s}$ long. If the channel is sensed as busy during any of these slots, the LBT process is restarted. Conversely, if all slots are clear, the device enters a backoff phase, randomly selecting a delay period within a contention window (CW) before it can transmit. The duration of this transmission is then capped by the Maximum Channel Occupancy Time (MCOT), ensuring that no single device monopolizes the channel for too long [24].

This structured access enhances interoperability and enables effective spectrum sharing among various technologies governed by IEEE 802.11, 3GPP standards, and ETSI. Table 2.6 outlines the channel access parameters for the different specifications.

Table 2.6: Comparison of channel access parameter names and values for ETSI EN 301 893, 3GPP Rel-16, and IEEE 802.11 specifications. Priorities are listed from highest to lowest. AC — Access category. Source: [24].

Specification	Priority	Name of inter-frame space number parameter p	Value of inter-frame space number p for DL (UL)	$CW_{\min}$	$CW_{\max}$ for DL (UL)	Name of maximum channel occupancy parameter $\sigma_{\max}$	Value of maximum channel occupancy $\sigma_{\max}$ for DL (UL) [ms]
ETSI	4	p_0	1 (2)	3	7	MCOT	2
	3		1 (2)	7	15		4
	2		3	15	63 (1023)		6 ^{a,b}
	1		7	15	1023		6 ^{a,b}
3GPP	1	m	1 (2)	3	7	MCOT	2
	2		1 (2)	7	15		3 (4)
	3		3	15	63 (1023)		8 (6) ^{a,c}
	4		7	15	1023		8 (6) ^{a,c}
802.11	AC_VO	AIFSN	1 (2)	3	7	$TXOP_{limit}$	2.08 ^d
	AC_VI		1 (2)	7	15		4.096 ^d
	AC_BE		3	15	63 (1023)		2.528 ^d
	AC_BK		7	15	1023		2.528 ^d

^a For UL transmissions, MCOT can be extended up to 8 ms if one or more pauses with a minimum duration of 100 μs are inserted.

^b Additionally, MCOT can be increased up to 10 ms if CW is doubled before and after each DL transmission exceeding 6 ms.

^c Additionally, MCOT can be extended up to 10 ms for UL and DL transmissions without any other technology.

^d IEEE 802.11 also defines the maximum time of data transmission at the physical layer ($PPDU_{MaxTime}$) equal (for all priorities) to 5.484 ms, which may be reached with frame aggregation.

These values illustrate the regulatory requirements that ensure fair access and efficient spectrum use, providing a foundation for robust and reliable communications across the 5 GHz band.

2.4 State of the art

This section provides an in-depth analysis of the current advancements and research in the field of 5G telecommunications, focusing on the role of URLLC in private 5G networks, challenges and evaluations of 5G New Radio Unlicensed (NR-U), the intricacies of 5G Non-Public Networks (NPNs), and the implementation and impact of coexistence mechanisms to support the operation in the unlicensed band, like Listen Before Talk (LBT) in 5G NR-U. The content brings together significant contributions and studies that have shaped our understanding and development of 5G technologies, highlighting the advancements and challenges faced in this rapidly evolving field.

In the context of this study, a central focus is on correctly understanding the 5G network, its current integration into modern telecommunications, and specifically its pivotal role in URLLC. In this regard, two main significant contributions have greatly assisted the community. The 'URLLC for 5G and Beyond: Physical, MAC and Network Solutions 2020 IEEE WCNC Tutorial' [28] by the University of Sydney's Centre of IoT and Telecommunications, presented at IEEE Globecom 2019, comprehensively explores URLLC in the 5G context. It delves deep into the transition from human-to-human (H2H) to machine-to-machine (M2M) communications, highlighting the necessity of URLLC in sectors like industrial automation and intelligent transportation systems. The project delves into various topics, including the technical requirements of 5G networks, the inherent challenges in achieving ultra-low latency and ultra-high reliability, and the dynamic nature of industrial network demands. It thoroughly discusses how to realize URLLC across various network layers—physical, MAC, and network—and examines the integration of advanced technologies such as mobile-edge computing and deep learning in network management.

Complementing this is 'Private 5G: A Systems Approach' [32], co-authored by Larry Peterson, a renowned professor at Princeton University, Oguz Sunay, a 5G innovator and Chief Architect at Intel, and Bruce Davie, a distinguished computer scientist with extensive experience in networking, which provides crucial insights into the overall architecture and functionality of 5G networks. This resource is invaluable for understanding 5G from a systems perspective, particularly highlighting the trends of softwarization and virtualization in telecommunications. It emphasizes how 5G represents a fundamental rearchitecting of the access network, leveraging key technology trends and setting a path for more significant innovation. The book addresses the ambitious requirements for Massive IoT, Mission-Critical Control, URLLC, and Enhanced Mobile Broadband (eMBB), all under 5G capabilities.

Together, these projects form a comprehensive reference for this study, offering a rich source of information for understanding, implementing, and evaluating URLLC communications and the broader 5G network functionalities.

Regarding 5G NR-U, an essential article for the community is "5G New Radio Unlicensed: Challenges and Evaluation," authored by researchers from the University of Arizona [19]. It examines the implementation of 5G NR-U technology, showcasing its advantages over Wi-Fi (802.11ac) in terms of throughput and latency. Moreover, it highlights the differences in buffer occupancies and spectrum utilization between NR-U and Wi-Fi. It emphasizes the challenges in achieving harmonious coexistence due to differences in waveform design, multi-channel operation, and scheduling approaches. While NR-U shows significant improvements over LTE-LAA, particularly in spectrum efficiency and coexistence strategies, the paper voices concerns about its capability to support URLLC applications in unlicensed bands effectively. It also points out the substantial impact of the loss of critical Wi-Fi control messages due to NR-U transmissions, suggesting improved coexistence mechanisms are necessary. This study effectively showcases the enhanced performance of 5G NR-U over Wi-Fi in terms of throughput and latency while highlighting significant challenges. Additionally, the paper underscores the need for more robust coexistence mechanisms, as evidenced by the notable impact of NR-U transmissions on the loss of critical

Wi-Fi control messages.

In the paper "Downlink Channel Access Performance of NR-U: Impact of Numerology and Mini-Slots on Coexistence with Wi-Fi in the 5 GHz Band" by Katarzyna Kosek-Szott and colleagues [24] the authors delve into the intricacies of NR-U's integration into unlicensed 5 GHz bands, mainly focusing on its coexistence with Wi-Fi. They introduce a novel downlink channel access simulation model for NR-U that accounts for the non-uniform transmission attempts arising from synchronization features unique to NR-U. The study contrasts NR-U with the LTE License Assisted Access (LAA), employing simulation and experimental approaches to validate the model. Through extensive FPGA-based experiments with Wi-Fi, LAA, and NR-U prototypes, the research illustrates that NR-U's flexible numerology and use of mini-slots could lead to more efficient spectrum use without compromising the fairness in channel access, compared to the rigid slot-based scheduling of LAA.

Furthermore, the paper confirms the potential of NR-U to enhance downlink channel access and highlights significant concerns regarding the overall fairness and efficiency in coexistence scenarios. It shows that replacing LAA with NR-U could avoid bandwidth wastage due to LAA's reservation signals and potentially preserve fair access among scheduled and random-access systems. However, achieving truly fair coexistence in unlicensed bands remains challenging, necessitating further innovation in coexistence mechanisms. This work underscores the need for continued research to refine these emerging technologies and their interplay with existing wireless systems by comprehensively analyzing downlink channel access performance.

The studies "Future Is Unlicensed: Private 5G Unlicensed Network for Connecting Industries of Future" [11] and "CR-LBT: Listen Before Talk with Collision Resolution for 5G NR-U Networks" [29] provided essential aspects regarding the deployment of Listen Before Talk (LBT). The first article discusses the impact of LBT on the performance of NR-U, particularly in terms of latency and channel access delay. The need for multiple LBT procedures for a single uplink transmission causes these delays. The authors propose potential solutions, such as redesigning the uplink LBT procedure and implementing shared maximum channel occupancy time (MCOT), to optimize the use of the unlicensed spectrum. The CR-LBT article focuses on enhancing throughput in cellular networks by leveraging unlicensed frequency bands. A modified Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol ensures fair channel sharing between NR-U and Wi-Fi, including a binary exponential backoff mechanism similar to Wi-Fi systems. However, the cellular base station in NR-U can only initiate data transmissions at periodic intervals, leading to potential performance bottlenecks.

These studies collectively advance the understanding of 5G NR-U deployment. They emphasize the need for innovative LBT and strategies to manage the unique challenges posed by shared spectrum use, ensuring efficient and harmonious operation alongside existing wireless technologies.

Our research focuses on differentiators from existing studies. First, our work ventures beyond theoretical analysis to practically implement LBT within 5G NR-U. We detail the integration process and operational challenges, such as synchronization issues, channel access rules, and the

design of the unlicensed band and the communication parameters, which deviates from typical literature in the community. Second, we conduct experiments to evaluate the effectiveness of LBT in managing interference. These experiments aim to provide empirical evidence on the performance of LBT under typical operational conditions, which is scarce in current studies. In addition, our research seeks to answer whether LBT is a sufficient mechanism for 5G NR-U, particularly considering the added delays of this mechanism. Our approach aims to identify and analyze LBT's practical limitations, contributing new insights into its applicability and performance in 5G networks.

Chapter 3

LBT for Standalone 5G NR-U: Challenges and Approach

This chapter presents our research methodology, beginning with a detailed analysis of the network testbed setup. Analyzing the setup first is important because one of the primary objectives is to adapt the network context by transitioning the Radio Access Technology (RAT) from NR to NR-U. Additionally, the unlicensed band's design and the Listen Before Talk implementation are intricately linked with the Radio Access Network (RAN) deployment.

Following the network presentation, we delve into the complexities of designing the unlicensed band channel and the practicalities of embedding LBT within the 5G NR framework, adhering to Time Division Duplex (TDD) configurations and signal processing characteristics in 5G.

3.1 Network Testbed Setup

The project's setup is a 5G standalone Non-Public network (NPN) hosted in the Instituto de Telecomunicações (IT) lab and Faculdade de Engenharia da Universidade do Porto (FEUP). The implementation is detailed in previous work by our group [33]. Due to the purpose of the study, we will focus on the Radio Access Network (RAN), and the 5G core, hosted in a server's room in FEUP, will not be detailed in this context.

The RAN follows the "high-level CU/DU split" (option 2), described in TS 38.806 [3]. This setup, excluding the UE, divides the RAN into two distinct components: the Distributed Unit (DU), which encompasses the Radio Unit (RU), and the Central Unit (CU). The DU and RU operate on the same computer, while the CU operates on a dedicated computer. The RU utilizes a Universal Software Radio Peripheral (USRP) B210 as the Software Defined Radio (SDR), which utilizes the USRP Hardware Driver (UHD) API to connect the DU and the RF front end.

Figure 3.1 illustrates the network testbed setup, representing the interaction between the components. Figure 3.2 represents photographs of the RAN testbed components.

The device specifications of each component are represented as follows:

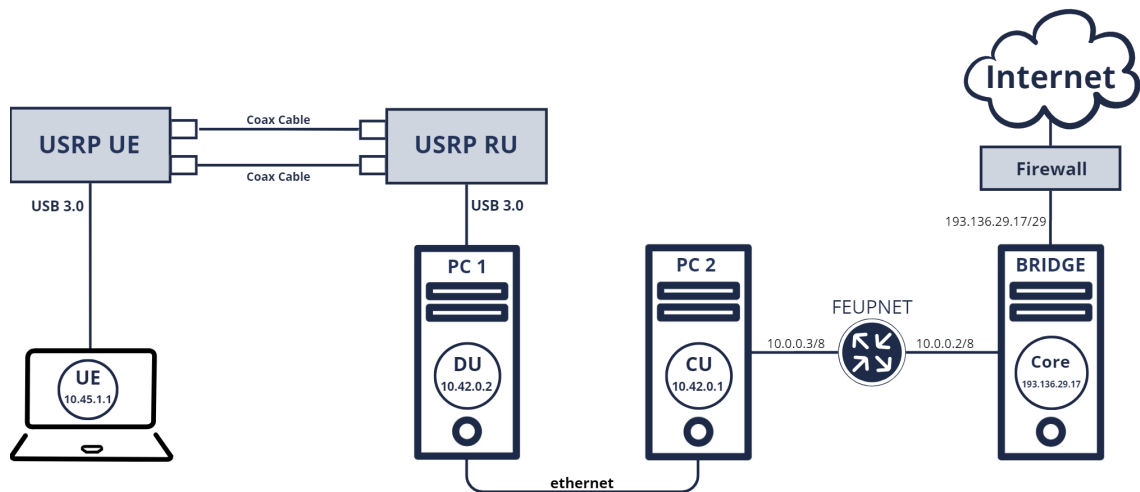


Figure 3.1: 5G Standalone Non-Public Network Architecture.



Figure 3.2: Detailed view of the 5G Testbed Radio Access Network (RAN) Components.

- **User Equipment (UE):** Laptop with Intel Core i9-14900HX processor with a 36 MB cache size and 32 GB of RAM;
- **Central Unit (CU) and Distributed Unit (DU):** Computer with 1x Intel Core i9 13900K 24-Core (2.2GHz-5.8GHz) processor, also with a 36 MB cache size and 32 GB of RAM and an additional 2 GB of swap space.
- **5G Core (5GC):** Dell PowerEdge R710 server machine with Intel Xeon E5520 processor, which has a cache size of 8 MB. The system features 48 GB of RAM and an additional 8 GB of swap space.
- **Communication Channel between USRPs:** Two SMA(male)-to-SMA(female) coaxial cables with a length of 0.5 meters. The Rx of one USRP is connected to the Tx of the other and vice-versa. It also contains attenuators of 60 dB.

- **USRP B210:** SDR platform, 70 MHz – 6 GHz RF coverage, up to 56 MHz bandwidth, full-duplex with 2x2 MIMO, SuperSpeed USB 3.0, supports UHD, Spartan 6 XC6SLX150 FPGA, AD9361 RFIC.

The RAN has been implemented using the open-source project OpenAirInterface (OAI). OAI was chosen because it has a wide community and documentation support but also provides compatibility with 3GPP Release 15 and the desired CU/DU split. The RAN architecture of OAI software is composed of several parts, as represented in Table 3.1:

Table 3.1: Overview of the OpenAirInterface (OAI) RAN repository sections.

Section	Description
ci-scripts	Meta-scripts and configuration files for the OSA CI process.
cmake_targets	Utilities for building and compiling on different platforms.
common	Common utilities for the OpenAirInterface (OAI) project.
doc	Documentation for the OAI RAN repository.
docker	Dockerfiles for building on Ubuntu and RHEL.
executables	Source files for top-level executables such as gNB and eNB.
maketags	Script to generate emacs tags.
nfapi	Code for the MAC-PHY interface.
openair1	Implementation of 3GPP LTE Rel-10/12 PHY layer and 3GPP NR Rel-15 layer.
openair2	Implementation of 3GPP LTE Rel-10 RLC/MAC/PDCP/RRC/X2AP and LTE Rel-14 M2AP, as well as 3GPP NR Rel-15 RLC/MAC/PDCP/RRC/X2AP.
openair3	Implementation of 3GPP LTE Rel-10 for S1AP and NAS GTPV1-U for both eNB and UE.
openshift	Helm charts for OpenShift deployment options of OAI.
radio	Drivers for various radios including USRP, AW2S, RFsim, etc.
targets	Configuration files of historical relevance, subject to potential deletion in the future.

This study's attention was primarily directed towards the `openair1` and `openair2` directories. These sections contain the implementations of the PHY layer and the MAC/RLC layers, respectively. The LBT mechanism must be integrated within these layers. `openair1` addresses the physical aspects of signal processing and radio transmissions. In contrast, `openair2` deals with the data link protocols that manage data transfer across the physical layer to ensure robust and efficient communication.

Another critical aspect of the OAI software architecture is encapsulated within the `executables` directory. This section of the codebase holds the primary executable files, which are fundamental to the system's operation. These executables contain the main threads of execution that directly influence the functioning of the code. It is in these threads that all key functions are called at precisely timed intervals.

The configuration files located in the `targets` directory, including `cu_gnb.conf`, `du_gnb.conf`, and `ue.conf`, delineate the configurations for communication between the UE and

gNB. These files set up the parameters and operational settings required for interaction within the network components.

Furthermore, the `radio` directory contains the code for each available Software Defined Radio (SDR). This code connects the PHY layer and the radio frequency (RF) front end, ensuring proper signal transmission and reception. The drivers for various radios, including USRP, AW2S, and RFsim, are maintained here, facilitating the diverse hardware support required for the OAI system.

3.2 Problem Formulation and Approach

The network under study operates in the licensed band. For this reason, the main goal is to design and validate a configuration to enable the non-public network (NPN) to operate in a Standalone NR-U mode, operating solely on the unlicensed band. It is important to clarify that NR-U comprises a set of technologies and requirements that will not be implemented in our network due to the extensive complexity of that task. For this reason, we have simplified NR-U implementation in this project by focusing on the network's ability to operate in an unlicensed band alongside an effective coexistence mechanism.

The primary objective of this project was to extend the OAI codebase to support operations on an unlicensed frequency band. This involved designing and configuring the selected band to ensure proper integration and functionality. The second task consists of developing and integrating the Listen Before Talk (LBT) mechanism, ensuring compliance with 5G NR-U standards and enabling coexistence in shared spectra. The project culminates with a comprehensive evaluation of network performance and an exploration of various use cases to validate the effectiveness and operational viability of the developed configurations. Due to the limited practical implementations of LBT in 5G within the community, precise design and computation methods remain uncertain. We aim to address these ambiguities by detailing a possible approach and providing a sustained solution for the deployment of LBT.

3.2.1 Design and Configuration of the Unlicensed Band

For this study, which aims to support connected driving communications as detailed in Section 1.3, band 47 was chosen. This band, classified under the 3GPP TS 38.101, is allocated explicitly for Vehicle-to-Everything (V2X) communications and operates within the 5900 MHz range (5855 – 5925 MHz). Band 47 falls within the U-NII-4 category, as described in Section 2.3.1, and is often included as part of band 46, which spans from 5150 to 5925 MHz.

The integration process for band 47 into the OAI system initially appeared straightforward. Documentation and multiple code comments within OAI suggested compliance with the latest 3GPP TS 38.101 specifications, indicating support for band 47. However, a thorough analysis during the compilation phase revealed significant gaps. Contrary to initial expectations, it became evident that band 47 was not supported as presumed. This discrepancy necessitated further adjustments and configurations to allow the implementation of band 47 for this project.

This oversight can be attributed to two interrelated factors. Firstly, OAI primarily concentrates on licensed bands, which leads to less emphasis on unlicensed bands such as band 47. Secondly, band 47 is often included under the broader classification of band 46, which results in its specific requirements being overlooked during standard implementation processes.

Building on the updated OAI codebase to include support for band 47, the next step involved configuring the communication parameters exchanged during synchronization to allow the operation in the 5.9 GHz frequency range. This stage entails exchanging synchronization signals and physical broadcast channel information between the User Equipment (UE) and the base station (gNB). Successful execution of this phase ensures that the UE is correctly synchronized with the base station's timing and frequency, as designed and detailed in Section 2.2.4.1.

3.2.2 5G NR-U - LBT Design and Configuration

As outlined in Section 2.3.3, the LBT implementation encompasses four potential categories and must adhere to 3GPP and ETSI standards. While the core aspects of LBT are standardized to ensure consistency and interoperability across technologies sharing the spectrum, the practical implementation has scope for tailored adaptations. These adaptations can optimize the LBT to better align with specific network conditions such as duplexing schemes, user priorities, interference management strategies, and hardware limitations. In this study, we will customize the LBT configuration to enhance performance and tailor it to our network's unique characteristics, requirements, and project limitations.

The sensing phase is the first step in LBT. It determines whether the channel is occupied or available for transmission. The main challenges in this step are detailing when to detect the channel's energy and how to compute it. It is relevant to mention that, as detailed in Section 2.3.3.2, the sensing phase is not solely Clear Channel Assessment (CCA) but includes multiple parts such as the Short Interframe Space (SIFS), the CCA itself, and a random Contention Window (CW) to prevent simultaneous connections post-CCA. While some papers and standards differentiate these components, others treat the entire process as CCA. For simplification in this discussion, we will refer to the entire sensing period as CCA. Subsequently, in the next and final phase, we define a mechanism for when the channel is occupied.

3.2.2.1 Timing of Energy Detection

The first detail to consider is that LBT indicates the CCA phase to be performed before transmitting. However, capturing, processing, and computing signal energy involves delays in hardware and software. This means there will always be a small gap between when an OFDM symbol reaches the antenna and when it is analyzed, and the CCA being performed consists of analyzing the previous samples already captured.

Moreover, the duplexing scheme influences the practical implementation of LBT in 5G NR-U, especially with the Time Division Duplex (TDD) configuration. As previously explained in

Section 2.2.3, TDD devices have specific time slots to transmit. However, the typical TDD configurations only free the channel during the guard time inside the mixed slot, leaving a short period to perform the CCA and allow other devices to transmit. This process is detailed in Figure 3.3, and adopting TDD configurations with shorter periodicity could enhance the frequency of CCA attempts.

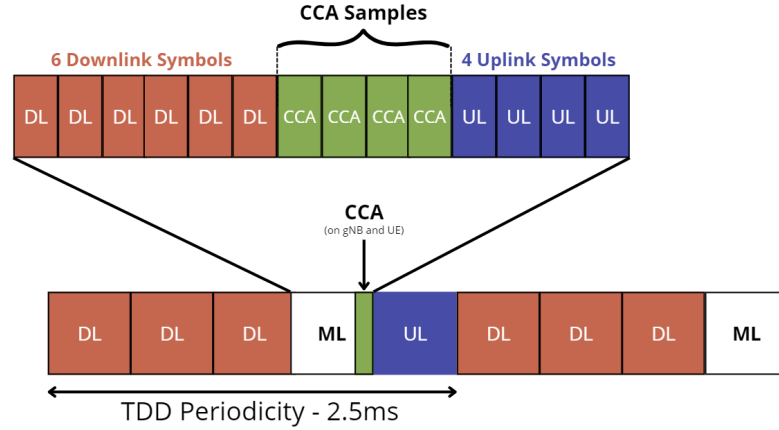


Figure 3.3: CCA timing in the mixed slot during guard time with a 2.5ms TDD periodicity.

In the gNB, if the channel is occupied during the mixed slot, CCA can be repeated during the UL slot to determine whether the channel is still occupied.

Another possible solution is performing the CCA in every slot, as detailed in Figure 3.4. This would require full-duplex (simultaneous RX and TX) or fast-switching capabilities in the Software Defined Radio (SDR) and a proper software implementation that continuously receives the data, even during transmission slots. This approach is only viable if the sampling frequency exceeds the minimum required to deliver the necessary samples within each slot period. Otherwise, the number of samples is precisely sent to occupy exactly the entire slot period. In such cases, only interference that does not respect the channel rules could be detected between consecutive transmission periods, as no time is left for another device to perform a CCA and initiate transmission.

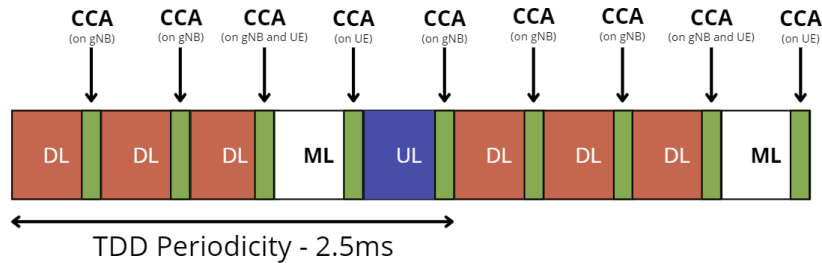


Figure 3.4: CCA timing in every slot with a 2.5ms TDD periodicity.

Additionally, with this implementation, the transition slots between downlink (DL) to mixed slot and uplink (UL) to DL slot will require a more complex CCA. It becomes challenging to differentiate whether the signal originates from the expected 5G device or an external source. To

address this, the process must involve a precise threshold setting or potentially more advanced signal analysis techniques in the upper layers of the protocol stack.

For this reason, implementing the first solution remains the primary option because it only performs the CCA during empty slots, is resilient to multiple types of hardware, and reduces the need for complex signal analysis during the transition slots. The main disadvantage is that it assumes all the devices sharing the channel comply with the channel access rules, performing all the LBT to detect if they can transmit. Additionally, in the UE, we should be able to access the CCA samples (empty period) before transmitting the UL symbols. This period involves only four symbols, though it could be modified to include only one symbol to minimize the limitation. However, even this reduced count still presents a limitation, as it can interfere with ongoing communication.

3.2.2.2 Energy Computation

Regarding the computation process, it is important to first detail the signal processing in 5G. As detailed in Section 2.2.1.1, the expected signal in the 5G NR architecture is structured based on Orthogonal Frequency Division Multiplexing (OFDM).

When the antenna captures an OFDM symbol, it is later digitized after RF processing (amplification, filtering, and down-conversion) and converted to a digital signal using an Analog-to-Digital Conversion (ADC). The cyclic prefix is removed to mitigate inter-symbol interference (ISI), and this signal represents the OFDM symbol in the time domain. During this stage, the energy can be computed through the following formula:

$$E_{\text{time}} = \sum_{n=0}^{N-1} |x[n]|^2$$

where $x[n]$ represents the time-domain samples, and N is the total number of samples within the OFDM symbol. It is crucial to note that N may be larger than the number of subcarriers, reflecting the number of Discrete Fourier Transform (DFT) points used in the Inverse Fast Fourier Transform (IFFT) process. Most commonly, the number of DFT points is chosen as a power of two because it allows for a more efficient implementation of the Fast Fourier Transform (FFT) algorithm, which underlies the IFFT.

Moreover, depending on the OAI implementation and the available buffer, the computation can also be performed in the frequency domain. The data is transformed using a DFT implemented through a FFT algorithm. The fundamental definition of the FFT follows the following equation:

$$X[k] = \sum_{n=0}^N x[n] \cdot e^{-i2\pi kn/N}.$$

where $X[k]$ represents the frequency-domain samples, and N is the total number of FFT points. Finally, the energy in the frequency domain is then computed as follows:

$$E_{\text{freq}} = \frac{1}{N} \sum_{k=0}^{N-1} |X[k]|^2$$

In this context, N represents the total number of points in the FFT. To compute E_{freq} , first, for each frequency bin k , calculate the magnitude squared of the FFT coefficient: $|X[k]|^2 = (\Re\{X[k]\})^2 + (\Im\{X[k]\})^2$, where $\Re\{X[k]\}$ and $\Im\{X[k]\}$ are the real and imaginary parts of $X[k]$, respectively. Then, sum these magnitude squared values across all frequency bins. Finally, normalize this sum by dividing by N to obtain the average energy per frequency bin.

This formula is derived from Parseval's theorem, which states that the total energy of the signal in the time domain is equal to the total energy in the frequency domain. Specifically, for a discrete-time signal $x[n]$ of length N , Parseval's theorem can be expressed as:

$$\sum_{n=0}^{N-1} |x[n]|^2 = \frac{1}{N} \sum_{k=0}^{N-1} |X[k]|^2.$$

The number of samples could differ depending on the practical implementation of CCA, the configurations performed in band 47, and the device that might interfere (which could have a significantly different sampling frequency).

3.2.2.3 Channel Occupancy Response Mechanism

The final step in configuring the LBT is establishing the conditions under which the device concludes the sensing phase upon detecting an occupied channel. This includes defining the number of attempts allowed before the sensing phase is terminated and specifying the subsequent actions to be taken once the channel is confirmed as occupied.

The standards for 3GPP do not specify the limit for the number of sensing attempts. This number should consider the number of samples and the time available for sensing. If the receiving samples buffer is updated once per slot, only one CCA can be performed, representing the channel samples over the last 0.5ms period. This CCA will differ slightly from the one explained in Section 2.3.3.1. Instead of gathering fewer samples every $9 \mu\text{s}$ multiple times, we will directly analyze the last slot samples and, with a proper offset, select the necessary symbols.

Regarding the next phase, when a device finds the channel occupied after several sensing attempts, it must implement a strategy to manage this situation effectively. One common approach is to delay the transmission. The device waits for a specified period before it attempts to sense the channel again. Alternatively, the device may abort the transmission if the channel remains occupied beyond the permitted number of sensing tries. This action avoids wasting system resources and causing excessive delays in data communication. Following an aborted attempt, the device usually informs the higher-level protocols of the issue. These protocols may take further steps, such as scheduling the transmission later or selecting an alternative communication channel.

In our case, detecting the channel occupied will cancel the next transmission because the communication is structured using a frame-based approach. Depending on the TDD configuration, this could correspond to one or multiple transmission slots.

Chapter 4

System Design and Implementation

This chapter will discuss the technical process of implementing the Non-Public Network (NPN) in band 47, following scenario C, detailed in Section 2.3.1, and outline the necessary adjustments to unforeseen limitations and obstacles beyond the initial planning phase.

The implementation will primarily focus on configuring the OpenAirInterface Radio Access Network (OAI-RAN) to support this unlicensed band and integrating the Listen Before Talk (LBT) to enable spectrum coexistence. We will delve into the technical aspects of the configuration and immediate operational challenges.

4.1 Setting up the NPN for Band 47

As mentioned in Section 3.2, OAI did not natively support band 47, and the design configuration for different bands of 78 was not fully understandable or updated.

4.1.1 Modifications for Band 47 Support

To support band 47 in the OAI codebase, specific modifications were made in both the User Equipment (UE) and the Distributed Unit (DU) code to the `nr_ssb_table` (located in `openair1/PHY/TOOLS/nr_bandtable.c`) and `sync_raster` (located in `openair2/GNB_APP/gnb_config.c`) array configurations. The OAI codebase supports these arrays by the 3GPP standards, particularly the synchronization raster and numbering section of Table 5.4.3.3-1 from the 38.101-1 and 38.101-2 documents. However, no configuration is defined for band 47 in both the referenced 3GPP documents and these arrays. Therefore, we needed to understand how the other values are configured and what they represent to add the new configuration for band 47.

Band 46, which encompasses band 47, has some descriptions in the 3GPP documents. From these descriptions and the current default band 78 configuration in OAI, we computed the necessary values for band 47.

4.1.1.1 Configuration of SSB

The `nr_ssb_table` is an array where each value follows the format: {78, 30, nr_ssb_type_C}. In each entry, the first index represents the band number, the second represents the sub-carrier spacing (SCS) in kHz, and the third indicates the synchronization signal block (SSB) type. Specifically, `nr_ssb_type_A` corresponds to numerology 0, `nr_ssb_type_B` corresponds to numerology 1, and `nr_ssb_type_C` encompasses multiple possible numerologies.

For band 47, the computation was straightforward as we planned to add band 47 with SCS of 15 or 30 kHz, resulting in the following values: {47, 15, nr_ssb_type_A}, {47, 30, nr_ssb_type_B}.

4.1.1.2 Calculation and Adjustment of GSCN Values

The `sync_raster` details the allowed interval and step for each band's GSCN (Global Synchronization Channel Number). As detailed in Section 2.2.4.1, the GSCN represents a frequency conversion that identifies the absolute position of the Synchronization Signal Block (SSB).

In the OAI code, each array value follows the format: {78, 1, 7711, 1, 8051}. The first and second indices represent the band and the numerology, respectively. The last three represent the first GSCN, the step, and the last GSCN.

We computed all the possible GSCN values for the band 47 frequency range (5855-5925) Mhz. According to TS 38.104, represented in Table 2.3, the formula for frequencies greater than 3000 MHz is $GSCN = 7499 + N$. To determine N , we utilize the relationship given by the expression $3000 \text{ MHz} + N \times 1.44 \text{ MHz}$, which equals the specific frequency of interest within the band. By setting this expression equal to the known frequency limits of the band, we can solve for N . This process is illustrated below, where we calculate the values of N_1 and N_2 by equating them to the lower and upper-frequency bounds of the band:

$$\begin{aligned} 3000 \text{ MHz} + N_1 \times 1.44 \text{ MHz} &= 5855 \text{ MHz} \Leftrightarrow N_1 = \frac{5855 - 3000}{1.44} \approx 1982, \\ 3000 \text{ MHz} + N_2 \times 1.44 \text{ MHz} &= 5925 \text{ MHz} \Leftrightarrow N_2 = \frac{5925 - 3000}{1.44} \approx 2032. \end{aligned}$$

Resulting in the adjusted GSCN values:

$$\begin{aligned} GSCN_1 &= 7499 + N_1 = 7499 + 1982 = 9481, \\ GSCN_2 &= 7499 + N_2 = 7499 + 2032 = 9531. \end{aligned}$$

Additionally, to ensure safety coverage for the entire frequency range, a guard band interval is considered: adding four units for lower frequencies results in a final GSCN of 9485 for N_1 , while subtracting four units for upper frequencies results in a final GSCN of 9527 for N_2 .

4.1.2 Design of the Communication Channel

After updating the OAI code to support band 47, the next step is to design the communication channel parameters to host the connection between the UE and the base station (gNB).

In the OAI codebase, the `du_gnb.conf` file defines the DU's communication protocols, emphasizing channel parameters and SSB configurations. To configure synchronization for band 47, it was crucial to review and understand the settings for band 78. This review provided a clear picture of current practices and helped clarify the significance of each parameter in the configuration file. Figure 4.1 was constructed during this development phase, visually representing the channel bandwidth configurations of band 78, designed by OAI, with the established positioning of the SSB and Point A.

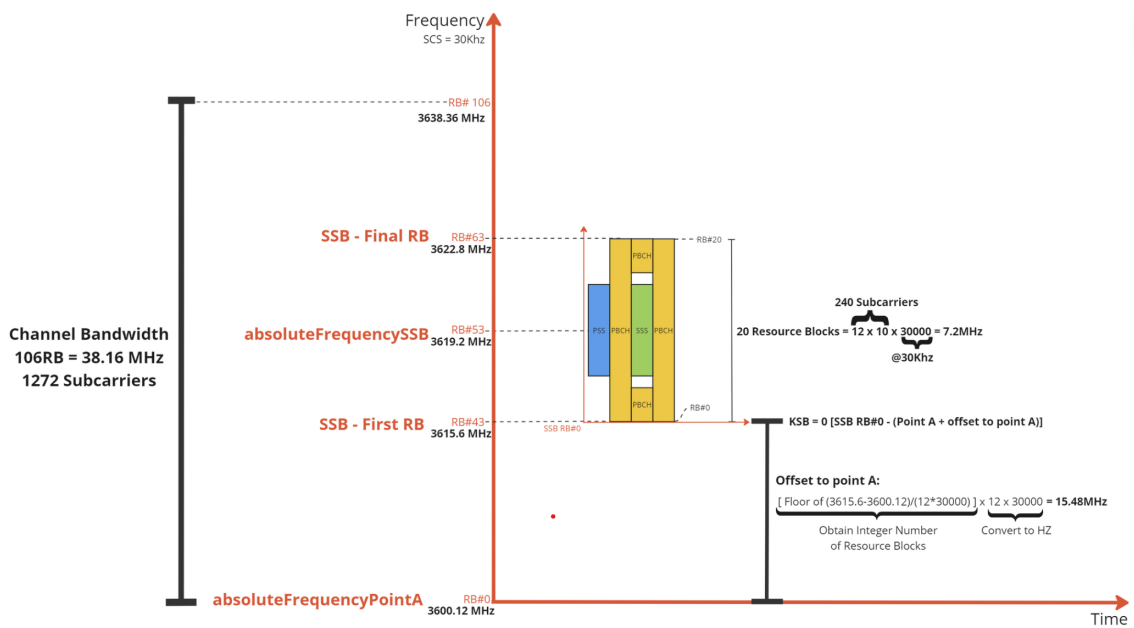


Figure 4.1: Channel Bandwidth Configurations for Band 78 by OAI.

The design of the new unlicensed band encompasses the computation of the following parameters:

- **Channel Bandwidth:** Determined by the formula $\text{Channel Bandwidth (Hz)} = N^{\circ} \text{ of RB} \times 12 \times \text{SCS (Hz)}$. This parameter defines the effective bandwidth.
- **Point A Frequency:** This is the reference frequency from which other channel measurements and settings are derived, ensuring alignment with the band's operational limits and regulatory standards.
- **SSB Frequency:** Used in the initial UE synchronization, the SSB's positioning within the frequency band is adjusted to comply with specific GSCN requirements and the operational constraints of the OAI codebase.

- **Bandwidth Part (BWP):** This defines the actual spectrum allocation for UL and DL, set through the RRC parameter *locationAndBandwidth* using the Resource Indication Value (RIV) formula.

4.1.2.1 Channel Bandwidth Configuration

Following these specifications, the first task was to define the channel bandwidth, which reflects the effective bandwidth size used for communication. Table 4.1 illustrates how the number of Resource Blocks (RBs) and Subcarrier Spacing (SCS) determine channel bandwidths in 5G NR, with values rounded to the nearest MHz and including guard bands to prevent interference. This table helps select a channel bandwidth that achieves at least 90% spectrum occupancy for efficiency while staying within the 70 MHz available band (5855-5925 MHz), accounting for guard bands.

Table 4.1: Resource Blocks (RBs) and spectrum utilization rates for different Subcarrier Spacing (SCS) and channel bandwidths in 5G NR.

SCS (KHz)	Channel bandwidth (MHz)									
	5	10	15	20	25	30	40	50	60	70
15	25	52	79	106	133	160	216	270	n/a	n/a
30	11	24	38	51	65	78	106	133	162	189
60	n/a	11	18	24	31	38	51	65	79	93

- Spectrum utilization: **>90%**, 90% and <90%

Additionally, as previously explained in Section 2.3, the 5GAA recommends a channel bandwidth of 10 MHz or 20 MHz for 5G NR applications. However, 3GPP proposes using also wider channel bandwidths of 30 MHz and 40 MHz for sidelink operations in NR Band 47. These specifications are detailed exclusively in the 3GPP standards, as in Table 2.5. Due to OAI limitations, numerologies (μ) higher than one and channel bandwidths of 30MHz are not supported, and no attention was given to fixing the issue due to it not being a priority.

Concerning hardware constraints, the selected channel bandwidth directly affects the transmission frequency, corresponding to the sampling rate. Not all sampling rates are compatible with USRP B210 or OAI software. Table 4.2 offers a comprehensive overview of channel bandwidth configurations. It explicitly delineates which configurations are supported or not.

Moreover, OAI supports the three-quarter sampling rate approach to overcome possible USRP issues, as exemplified in Table 4.2, where USRP B210 does not support the 61.44 MSamples/s

Table 4.2: Channel bandwidth values for the USRP B210 without three-quarter sampling.

Bandwidth, SCS x RB	Subcarriers (RB * 12)	OFDM Points	Samples Per Slot Without Cyclic Prefix (OFDM Points * 14)	Cyclic Prefix Samples	Total Samples (per slot)	Total Samples (per millisecond)	USRP Sampling rate (MSps)
10 MHz, 15 x 52	624	1024	14336	$1*80 + 13*72 = 1016$	15352	15352	15.36
10 MHz, 30 x 24	288	512	7168	$1*44 + 13*36 = 512$	7680	15360	15.36
20 MHz, 15 x 106	1272	1536	21504	$1*160 + 13*144 = 2032$	23536	23536	30.72
20 MHz, 30 x 51	612	768	10752	$1*88 + 13*72 = 1024$	11776	23552	30.72
30 MHz, 15 x 160	1920	2048	28672	$1*160 + 13*144 = 2032$	30704	30704	30.72
30 MHz, 30 x 78	936	1024	14336	$1*88 + 13*72 = 1024$	15360	30720	30.72
40 MHz, 15 x 216	2592	4096	57344	$1*320 + 13*288 = 4064$	61408	61408	61.44
40 MHz, 30 x 106	1272	2048	28672	$1*176 + 13*144 = 2048$	30720	61440	61.44

Not supported by USRP B210

Not supported by OAI

rate. It reduces the standard sampling rate to 75% of its normal value and introduces possible new configurations, as detailed in Table 4.3.

Table 4.3: Channel bandwidth values for the USRP B210 with three-quarter sampling enabled.

Bandwidth, SCS x RB	Subcarriers (RB * 12)	OFDM Points	Samples Per Slot Without Cyclic Prefix (OFDM Points * 14)	Cyclic Prefix Samples	Total Samples (per slot)	Total Samples (per millisecond)	USRP Sampling rate (MSps)
10 MHz, 15 x 52	624	768	10752	$1*60 + 13*54 = 762$	11514	11514	11.52
10 MHz, 30 x 24	288	384	5376	$1*33 + 13*27 = 384$	5760	11520	11.52
20 MHz, 15 x 106	1272	1536	21504	$1*120 + 13*108 = 1524$	23028	23028	23.04
20 MHz, 30 x 51	612	768	10752	$1*66 + 13*54 = 768$	11520	23040	23.04
30 MHz, 15 x 160	1920	3072	43008	$1*240 + 13*216 = 3048$	46056	46056	46.08
30 MHz, 30 x 78	936	1536	21504	$1*132 + 13*108 = 1536$	23040	46080	46.08
40 MHz, 15 x 216	2592	3072	43008	$1*240 + 13*216 = 3048$	46056	46056	46.08
40 MHz, 30 x 106	1272	1536	21504	$1*132 + 13*108 = 1536$	23040	46080	46.08

Not supported by USRP B210

Not supported by OAI

Although this method reduces the sampling rate to accommodate hardware limitations, it significantly increases the risk of aliasing because the sample rate is nearly equivalent to the channel bandwidth. Aliasing compromises signal reconstruction accuracy, potentially leading to data interpretation and processing errors. Therefore, we will apply the three-quarter sampling exclusively to 40 MHz bandwidth configurations with $\mu = 1$. While all the supported designed channel bandwidths that do not use the three-quarter sampling rate will be assessed, it's important to note that not every configuration complies with the subsequent OAI SSB Position limitations, which will be detailed further.

4.1.2.2 Point A and SSB Frequency Positioning

After determining the channel bandwidth, Point A's absolute frequency was set, which must meet various operational constraints and standards, including the band's operational limits and the regu-

latory and technical specifications defined by 3GPP. As detailed in Section 2.2.1.3, Point A represents the reference point and will be set at the channel's beginning to simplify future calculations by assigning the *OffsetToCarrier* value to 0. Therefore, this section will treat the requirements for the channel's beginning as synonymous with those for Frequency to Point A. However, it should be noted that in practical terms, Frequency to Point A serves merely as a reference and does not impose any specific requirements or must attend to some specific relation with other parameters. Considering this, to ensure compliance with 3GPP standards, the following constraints are applied to both the absolute SSB frequency (detailed in Section 2.2.4.1) and the frequency at Point A:

- **Band Operational Limits:** Point A and SSB Frequency must fall within the designated operational frequency band limits. The offset to Point A in hertz and the SSB subcarrier offset (K_{ssb}) in hertz must be divisible by the subcarrier spacing (SCS) to ensure an integer number of subcarriers.
- **GSCN Formula Compliance:** The SSB absolute frequency must be located into a valid Global Synchronization Channel Number (GSCN) with the formula $3000 \text{ MHz} + 1.44 \times N$, as referred in Table 2.3.

Additionally, in adherence to OAI code limitations, we should adhere to two other requirements:

- **K_{ssb} must be 0:** The SSB absolute frequency must align with an integer RB frequency, avoiding fractional offsets undetectable by the UE. For instance, if the channel bandwidth has 52 RBs, placing the SSB at RB 26 ensures an integer-based centering. In this case, the offset to Point A, the distance between the starting frequency point of the channel (Point A) and the first RB of the SSB (RB 16), must be an integer number of Resource Blocks (RBs). This will ensure the K_{ssb} , the distance between the offset to Point A and the first RB of the SSB, zero, which is essential because, in OAI, the UE cannot detect the SSB if K_{ssb} is not zero due to the complications arising from fractional offsets in frequency assignments.
- **SSB Placement:** The SSB should ideally be positioned in the middle of the channel to maintain simplicity and ensure effective synchronization. This placement is straightforward in scenarios where the channel has an even number of RBs. However, for a channel with an odd number of RBs (e.g., 51 RBs), positioning the SSB at the midpoint will make the K_{ssb} not zero. Consequently, for some configurations, meeting both the central placement and zero K_{ssb} requirements may not be possible, thus limiting the available design options.

To ensure this set of requirements, a Python script, `band_design.py`, detailed in Appendix A.1, was developed. This script receives the frequency band boundaries, the subcarrier spacing (SCS), and the number of resource blocks. It calculates multiple sets of valid configurations for Point A and SSB that satisfy all the necessary constraints.

4.1.2.3 Bandwidth Part (BWP) Configuration

Moreover, the location and bandwidth of a Bandwidth Part (BWP) inside the channel were specified with the Radio Resource Control (RRC) parameter called *locationAndBandwidth* for both UL and DL, defined as a Resource Indication Value (RIV), previously detailed in Section 2.2.4.3, which follows the formula:

$$\text{RIV} = \begin{cases} 275 \times (\text{max RB} - 1) + \text{RB start} & \text{if } \text{max RB} - 1 \leq \frac{N_{RB}}{2} \\ 275 \times (N_{RB} - \text{RB start} + 1) + (N_{RB} - 1 - \text{RB start}) & \text{otherwise} \end{cases}$$

Table 4.4 are the RIV calculations for different channel bandwidths (10, 20, and 40 MHz) at two different Subcarrier Spacings (SCS) of 15 kHz and 30 kHz. We utilize a single BWP occupying the allocated channel bandwidth in our configuration. This simplifies the RIV calculation as the BWP spans all available Resource Blocks (RBs) from the start to the end of the channel. Consequently, the RIV will indicate full channel bandwidth utilization, encapsulating the available spectrum.

Table 4.4: RIV Calculations for different SCS and Channel Bandwidths

SCS (kHz)	Channel Bandwidth (MHz)	Max RB	RIV Calculation	Location and Bandwidth (RIV)
15	10	52	$275 \times (52 - 1)$	14025
15	20	106	$275 \times (106 - 1)$	28875
15	40	216	$275 \times (216 - 1)$	59375
30	10	24	$275 \times (24 - 1)$	6325
30	20	51	$275 \times (51 - 1)$	13750
30	40	106	$275 \times (106 - 1)$	28875

Although, ideally, according to TS 38.214, for 5G NR, these configurations could be dynamically adjusted and scheduled during transmission to enhance efficiency and spectrum utilization, in OAI, this value is previously set and must be fixed during transmission. Depending on the designed channel bandwidth, we use the according RIV.

4.1.2.4 Final Design Choices and Hardware Limitations in 5.9 GHz

During the final stages of our project, practical tests revealed that the USRP B210 does not adequately support operations at 5.9 GHz, despite its theoretical operational limit of 6 GHz, as stated in the [USRP datasheet](#). Upon further investigation and corroborated by an important reference [39], it was found that the frequency response of the USRP B210 significantly attenuates at 5.9 GHz, as detailed in Figure 4.2. Given the time constraints, switching to a more capable SDR was not feasible. Therefore, we adjusted our frequency range to band 46 (5150 – 5925 MHz), which includes band 47 (5855 - 5925 MHz). We experimentally determined that the closest frequency

our USRP B210 could reliably support is around 5855 MHz. This adjustment effectively uses half of the bandwidth available in band 47 and the other half in band 46.

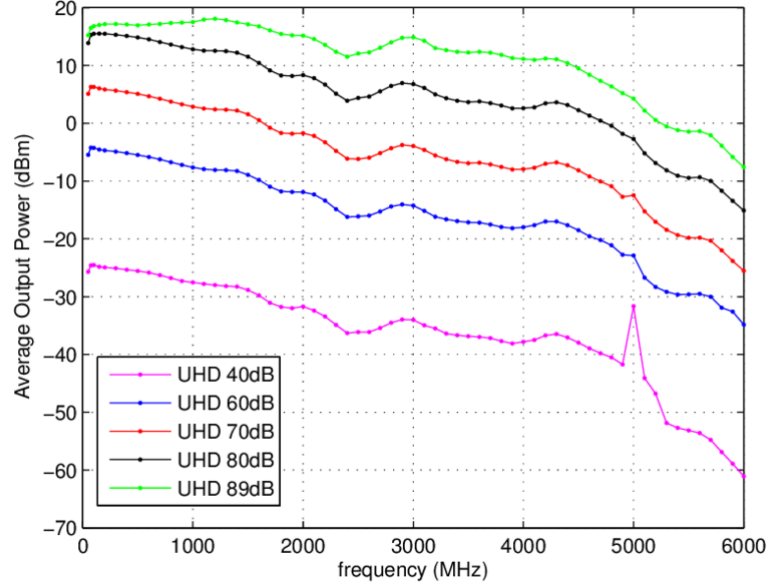


Figure 4.2: The measured frequency bandwidth of the MIMO B210 USRP board for different UHD G values. Source: [39].

Despite these modifications, we did the same steps detailed in Section 4.1.1 for band 46, as it is also not natively supported by OAI, and the essential channel parameters previously computed in Section 4.1.2 remained unchanged except for the SSB and Point A positions. Fortunately, the script `band_design.py` we previously mentioned can calculate these values for any band. This allowed us to acquire a new set of values tailored to the adjusted frequency range. As a result, this limitation did not significantly impact our configurations. After computing the latest values, we can select a set of design choices. Table 4.5 represents the final values we designed.

Table 4.5: Final design values for band 47 with different numerologies and channel bandwidths

Channel Bandwidth (MHz)	SCS x RB (KHz)	Point A (MHz)	SSB (MHz)	RIV	USRP Sampling Rate (MSps)
10	15 x 52	5849.4	5854.08	14025	15.36
10	30 x 24	5849.76	5854.08	6325	15.36
20	15 x 106	-	-	28875	30.72
20	30 x 51	-	-	13750	30.72
40	15 x 216	-	-	59375	46.08 (with 3/4)
40	30 x 106	5835	5854.08	28875	46.08 (with 3/4)

Among the available SSB and Point A value sets, we selected those where the SSB, corresponding to the channel's effective center frequency, closely matches the 5855 MHz. As mentioned in the table, some configurations did not meet all the requirements.

After exploring various configurations and channel bandwidths for the unlicensed band, it was decided that the 40MHz channel bandwidth configuration is the optimal choice. This bandwidth offers a significantly larger channel, which enhances both tolerance and performance compared to the other available options. Additionally, although we are using a three-quarter sampling rate in this specific case, there is no expected aliasing as we transmit and receive 23,040 samples/ms with a 46,080 Msamples/s rate in the USRP sampling rate, effectively supporting our system requirements without compromising performance or efficiency. Figure 4.3 represents this configuration, with a $\mu = 1$ (SCS of 30KHz) and 106 RB. In this configuration, the SSB frequency is marked by GSCN 9481, representing 5854.08 MHz, and Point A is at 5835 MHz, representing the channel's beginning.

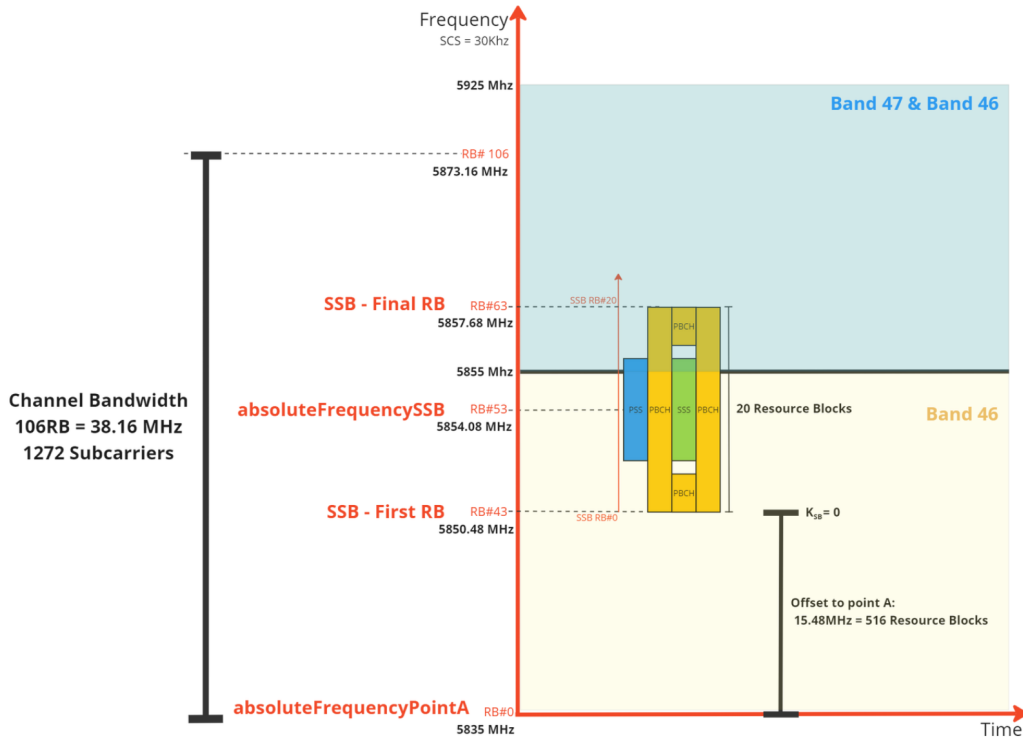


Figure 4.3: Configuration of the channel, located in bands 46 and 47, with a 38.16 MHz bandwidth and 106 RBs, showing Point A and SSB positioning.

The configuration file `du_gnb.conf`, which translates the design parameters into the OAI interface, is described in Appendix A.2. For the UE, the requisite configurations are specified within the execution command parameters as follows:

```
./nr-uesoftmodem -O \
../../../../targets/PROJECTS/GENERIC-NR-5GC/CONF/ue.conf --sa \
-r 106 --numerology 1 --band 46 -C 5854080000 --ssb 516 \
```

```
--ue-fo-compensation -E --ue-rxgain 120
```

In the above command, the `-r` parameter specifies the number of Resource Blocks (RBs), the `-C` option sets the center channel frequency, the `-E` flag activates the necessary three-quarter sampling rate, and `--sa` denotes the standalone mode of operation. Additionally, the `ssb` parameter represents the offset between Point A and the SSB's first Resource Block (RB).

4.2 Implementing the Listen Before Talk (LBT) mechanism

This section will explore the Listen Before Talk (LBT) practical implementation within the OpenAirInterface Radio Access Network (OAI-RAN) codebase.

4.2.1 Understanding RF Frontend Dynamics and Timing Advances in OAI

Before detailing the LBT's coding approach, it is important to understand the exact timing considerations of both the RF front end and OAI and how they will impact the implementation.

The initial point of focus is the precise moment data becomes accessible. While devices transmit at predefined intervals in the Time Division Duplex (TDD), this schedule is generally observed at the RF front end. At the Physical Layer (PHY), where data extraction and processing occur, additional timing considerations come into play. Figure 4.4 illustrates the precise time considerations and the relationship between the propagation time, the RF front-end reception, and the PHY processing. The transmitter accounts for propagation delays, and in OAI, it computes the data three slots in advance to ensure data delivery aligns with TDD configurations. The processing occurs only when the receiver obtains all the slot samples. This aspect is essential because when processing begins at any slot, the code where we will implement the LBT already has all the samples for that slot.

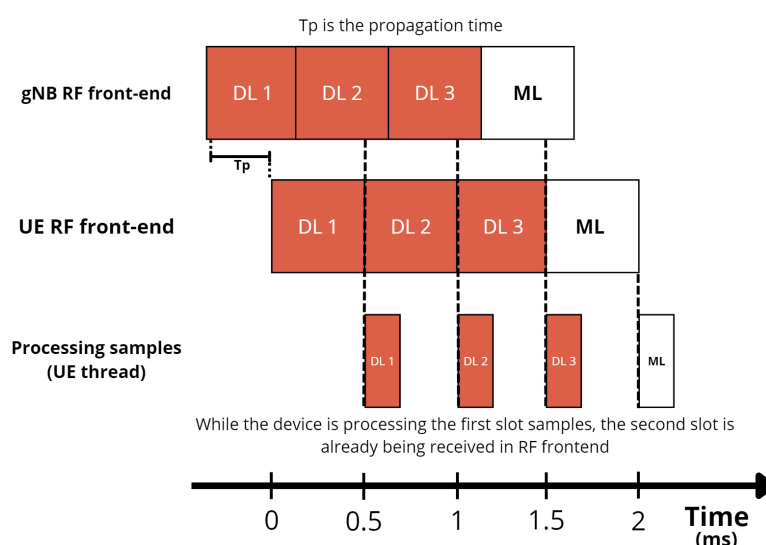


Figure 4.4: Interaction between the gNB and UE with timing advance and slot structure.

As previously mentioned in Section 2.2.4, the base station typically computed the timing advance for each UE to accommodate varying propagation times in the uplink due to differences in distances to the base station. In OAI, this timing advance is fixed and equal to three slots, as the processing slot advance. For this reason, in the UE, data is also sent three slots in advance, which contrasts with the gNB, where the advance in processing does not alter the data transmission timing. This discrepancy modifies the designed TDD structure, as represented in Figure 4.5. Yet, it proves advantageous for the LBT implementation, as it leaves one or more slots empty, depending on the specific TDD configuration, to perform the sensing phase.

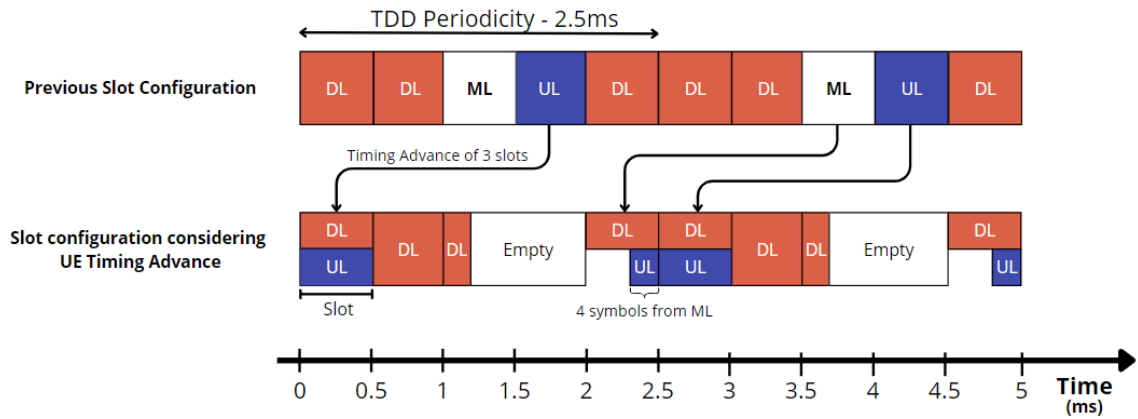


Figure 4.5: Impact of UE Timing Advance on TDD Slot Configuration in OAI.

4.2.2 Data Extraction and Code Integration

The first task was to compute the channel's energy from the previous slot at the beginning of the current slot for both the User Equipment (UE) and the base station (gNB). Placing this task at the start of the slot ensures adequate time to implement a hold-off if the channel is detected to be occupied, thereby preventing any potential interference with other transmissions.

In the base station, the approach focuses specifically on the Radio Unit (RU) thread within the OAI-RAN codebase, found in the source file `openairinterface5g/executables/nr-ru.c` at the function `void *ru_thread(void *param)`. Similarly, for the User Equipment, the implementation is centered around the UE thread, detailed in `openairinterface5g/executables/nr-ue.c` at the function `void *UE_thread(void *arg)`. Both threads are invoked at every slot period, processing each slot's data sequentially. The system to detect and compute the channel's energy should be employed at the beginning of these threads and after the initial synchronization.

Subsequently, we must access the samples after identifying the appropriate insertion points for the LBT code. Data is managed within the `RU_t *ru` structure on the RU side. The function `rx_rf`, linked to `ru->fh_south_in`, reads the samples of each slot.

Similarly, on the UE side, the structure is defined as `PHY_VARS_NR_UE`. Data is managed within this structure, and samples are read through the `trx_read_func` function of the `UE->rfdevice`. This function fills the `UE->common_vars.rxdata` array.

Both the `ru->common.rxdata` and `UE->common_vars.rxdata` arrays store the time-domain samples from the current slot as complex numbers of type `c16_t`, where `.r` is used to access the real part, and `.i` is used to access the imaginary part. These arrays are organized as two-dimensional, where the first index points to the antenna (only one in our case), and the second index corresponds to the sample position within the transmission slot.

4.2.3 Identifying Slot Types and Executing the Sensing Phase

As detailed in Section 4.2.1, the fixed timing advance of three slots in the OAI for the UL extends the Sensing Phase due to the increased duration during which devices are not transmitting. This extension is critical as it provides additional time to monitor the channel for potential conflicts, thereby enhancing the efficacy of the LBT mechanism.

Figure 4.6 illustrates how all Time Division Duplex (TDD) configurations incorporate an "empty phase" of 8 OFDM Symbols from the mixed slot. Depending on the TDD configuration, additional empty phases are observed. For instance, a TDD configuration with a periodicity of 2ms includes 10 OFDM symbols from the UL slot. In a TDD configuration of 2.5ms, the entire UL slot period remains empty, and for a TDD configuration of 5ms, two whole UL slots are devoid of transmission.

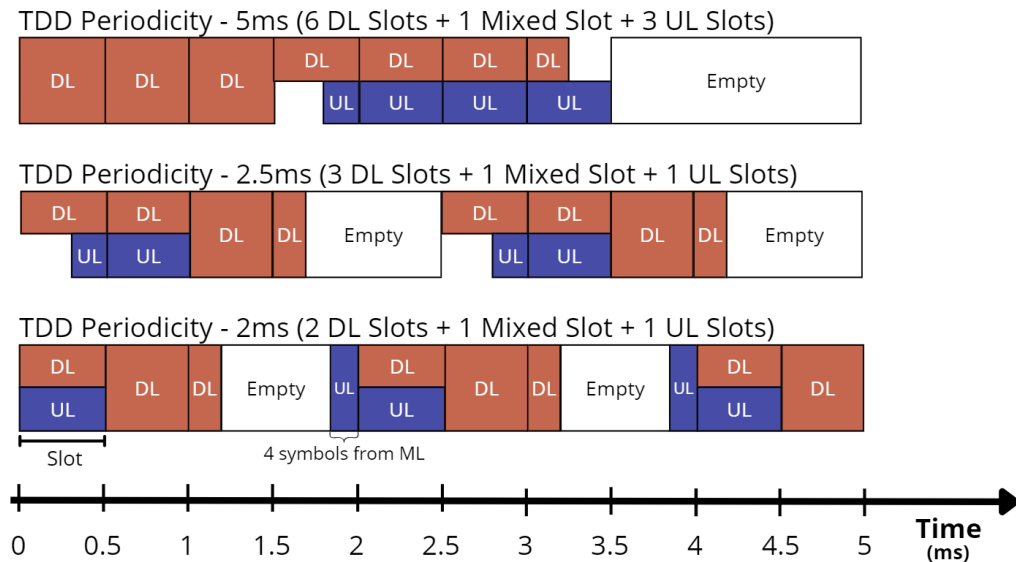


Figure 4.6: Overview of Time Division Duplex (TDD) configurations at a 30kHz Subcarrier Spacing (SCS), illustrating the arrangement and timing of DL, UL, and empty phases for different periodicities.

We can access the current slot type in the UE with the `UE_nr_rxtx_proc_t` structure.

Within this structure, `nr_slot_rx` and `nr_slot_tx` track the current slot positions for reception and transmission within the frame, respectively. The `rx_slot_type`, viewed from the perspective of the base station, and `tx_slot_type`, which refers to the perspective of the UE, determine the type of each slot, such as downlink, uplink, or mixed slots. The function `determine_slot_type()` computes the type of slot based on the TDD configuration, the timing advance, the current position in the frame, and the numerology.

For the gNB side, the identification of slot types is managed through the structure `RU_proc_t_s` that tracks the current slot and frame for transmission and reception. The variables `tti_rx` and `tti_tx` represent the current slot index for reception and transmission within the frame, similar to `nr_slot_rx` and `nr_slot_tx`. The function `nr_slot_select()` is used to determine the slot type based on the TDD configuration, similar to the UE function.

Finally, for both devices, we adhere to the perspective of the gNB slot type. This approach is encapsulated in the condition represented in Code Listing 4.1, determining whether to perform the sensing phase, ensuring that calculations are conducted only during the empty phases.

```
// UE
int slot_type = curMsg.proc.rx_slot_type;
if (slot_type == NR_UPLINK_SLOT || slot_type == NR_MIXED_SLOT) {
    channel_occupancy = update_channel_state(
        (cl6_t **)UE->common_vars.rxdata, UE->frame_parms.ofdm_symbol_size,
        curMsg.proc.nr_slot_rx, UE->energy_info.current_frame, slot_type);
}

// in gNB
int slot_type = nr_slot_select(cfg, proc->frame_rx, proc->tti_rx);
if (slot_type == NR_UPLINK_SLOT || slot_type == NR_MIXED_SLOT) {
    channel_occupancy = update_channel_state((cl6_t **)ru->common.rxdata, fp->
        ofdm_symbol_size, slot, frame, slot_type);
}
```

Listing 4.1: Updating Channel Occupancy State Based on Slot Type

4.2.4 Computing Channel Energy

After accessing the necessary samples and identifying the correct slot type, the next step involves computing the energy of the channel depending on the TDD configuration. The function should filter and compute the energy from specific symbols in the empty phase. As detailed in Section 3.2.2.2, the computation of energy is based on the magnitude of the complex numbers stored in the arrays `ru->common.rxdata` and `UE->common_vars.rxdata`.

As explained in Section 3.2.2.1, the process involves computing the magnitude of each symbol in the slot to determine their energy levels. As described in Code Listing 4.2, the computation is performed for each symbol, and the array `rxp` corresponds to the samples array.

```

int update_channel_state(c16_t **rxp, int symbol_size, int slot_in_frame, int frame
, int slot_type){
    int start_symbol = (slot_type == NR_MIXED_SLOT) ? 6 : 0;
    int end_symbol = 13; // should be 8 if in gNB and TDD with 2.5ms periodicity
    for (int sym = start_symbol; sym < end_symbol; sym++) {
        c16_t symbol_data[symbol_size];
        memcpy(symbol_data, &rxp[0][sym * symbol_size], sizeof(c16_t)*symbol_size);
        double symbol_energy_dB = 0;
        for (int i = 0; i < symbol_size; i++) {
            int real = symbol_data[i].r;
            int imag = symbol_data[i].i;
            symbol_energy_dB += real * real + imag * imag;
        }
        symbol_energy_dB = 10 * log10(symbol_energy_dB + 1e-10);
        (...)
    }
}

```

Listing 4.2: Computation of symbol energy

The symbol size, measured in samples, dictates the offset for each symbol computation, specifically identifying the starting sample of each symbol. This offset is dependent on the transmission configurations, and it is important to determine it accurately to filter the symbols correctly.

4.2.5 Channel Occupancy Determination

After computing the signal energy for the desired symbols, we should compare it with a threshold. Our testbed was connected to the USRPs during this phase through a coaxial cable. The interference was low, and we noticed a large energy difference between the symbols in the transmission and empty phases.

We focused on the mixed slot period to validate the TDD configurations. In particular, we measure the energy difference between the last downlink symbol (symbol 6) and the first empty symbol (symbol 7). For example, in a 5ms configuration, in a mixed slot, the energy significantly dropped from 83.20 dB in symbol 6 to 54.59 dB in symbol 7. A similar trend was observed in the 2.5ms configuration, where energy decreased from 90.20 dB to 52.93 dB. These results, obtained in the UE during a 5 MB download, confirm the clear distinction between active transmission and the TDD configuration's empty phase. Based on these findings, as detailed in Code Listing 4.3, we established a provisory threshold of 60 dB.

```

int update_channel_state(c16_t **rxp, int symbol_size, int slot_in_frame,
int frame, int slot_type){
    int start_symbol = (slot_type == NR_MIXED_SLOT) ? 6 : 0;
    int end_symbol = 13; // should be 8 if in gNB and TDD with 2.5ms periodicity
    for (int sym = start_symbol; sym < end_symbol; sym++) {
        (...)
        symbol_energy_dB = 10 * log10(symbol_energy_dB + 1e-10);
        if (symbol_energy_dB > 60) {

```

```

        return 1;
    }
}
return 0;
}

```

Listing 4.3: Code for determining channel occupancy by measuring and comparing symbol energy to a predefined threshold.

When at least one symbol energy exceeds the threshold, indicating significant recent activity, the function returns a value of 1. It considers the channel occupied, halting further energy analysis for the remaining symbols in the slot. This approach is adopted because a device that has just been transmitted is statistically more likely to do so again, and so, even if the most recent symbols have low energy, it is safe to consider the channel is occupied and cancel the subsequent transmission.

It is important to note that this threshold value established in our study is tailored explicitly for environments where the communication setup is wired. In the phase of the experiment, when we adapt the channel to be wireless, following the setup explained in the next Chapter, in Section 5.1, the appropriate threshold would need to account for the expected noise floor and possible interferences, which might significantly differ from those observed in a wired setup. This function's final code version of the `channel_occupancy` function with the proper threshold and final adaptations explained in the next Chapter is listed in Appendix A.3.

4.2.6 Transmission Cancellation in Occupied Channels

Having established a method to update the `channel_occupancy` variable based on detected symbol energy, the last step is propagating this state to the radio interface to manage transmissions effectively. The variable `channel_occupancy` is declared as an external integer (`extern int channel_occupancy;`) in the file `radio/COMMON/common_lib.h`, accessible in both UE and gNB contexts. This external declaration facilitates a global update and access mechanism for managing transmission states across different system components.

As previously detailed in Table 3.1, the `radio` directory contains drivers for software-defined radios, linking PHY functionalities to the RF frontend. The file `radio/USRP/usrp_lib.cpp` includes functions for sending and receiving samples. The operational logic for managing transmissions based on the channel occupancy is represented in Code Listing 4.4:

```

if (channel_occupancy == 0) {
    ret = (int)s->tx_stream->send(&(((int16_t *)buff_tx[0])[0]), nsamps, s->tx_md);
} else { ret = 0; }

if (ret != nsamps) {
    LOG_E(HW, "[xmit] tx samples %d != %d\n", ret, nsamps);
    return ret;
}

```

Listing 4.4: Code demonstrating the conditional management of transmissions based on channel occupancy, ensuring that data is only sent when the channel is clear.

This implementation transmits data only when `channel_occupancy` equals zero. If the channel is occupied, the transmission is canceled. This strategy ensures no transmission occurs during occupied channel states, preventing signal interference.

Chapter 5

Experiments, Results, and Discussion

This chapter outlines the experimental setup designed to validate operations within the unlicensed spectrum using the Listen Before Talk (LBT) mechanism in a 5G Non-Public Network (NPN) context and evaluate the inherent challenges of spectrum coexistence. A primary focus is the adaptation and enhancement of the testbed to include a new Software-Defined Radio (SDR) that simulates a secondary user or acts as a source of interference.

Following the new SDR installation, we conducted experiments to assess how 5G devices manage the mandatory coexistence mode in the unlicensed spectrum. This included testing whether the devices correctly sense channel energy, the operational efficiency of the LBT mechanism, and the impact on network performance due to the additional delays and potential degradation caused by sharing the spectrum. These experiments aimed to provide insights into how effectively the LBT strategy supports network stability and performance under varied interference levels.

5.1 Updating the Testbed for LBT Validation and Performance Evaluation

The testbed required a significant modification in the Radio Access Network (RAN) to advance our investigation of the LBT mechanism and assess network performance under simulated interference. This update facilitates the integration of a new device to act as a coexisting device or secondary user, generating traffic on the 5.85 GHz channel, also shared by the 5G network, as detailed in Section 4.1.2.4. The subsequent modifications are designed to simulate potential interference scenarios and evaluate the coexistence capabilities of our primary 5G standalone NPN with secondary users.

A wireless configuration will be tested and utilized, leveraging its closer resemblance to real-world V2X environments. We will use a Software-Defined Radio (SDR), specifically a Single-Board Computer (SBC) with a mini Peripheral Component Interconnect Express (mPCIe) to generate traffic up to 6 GHz. This SDR supports the creation of traffic patterns and interference conditions for assessing the LBT's performance and resilience. This setup involves replacing coaxial cables with antennas. This change introduces five new antennas: two receivers and three

transmitters, one each for the two USRP units in the testbed and another for the SBC to generate interference. The testbed setup is represented in Figure 5.1.

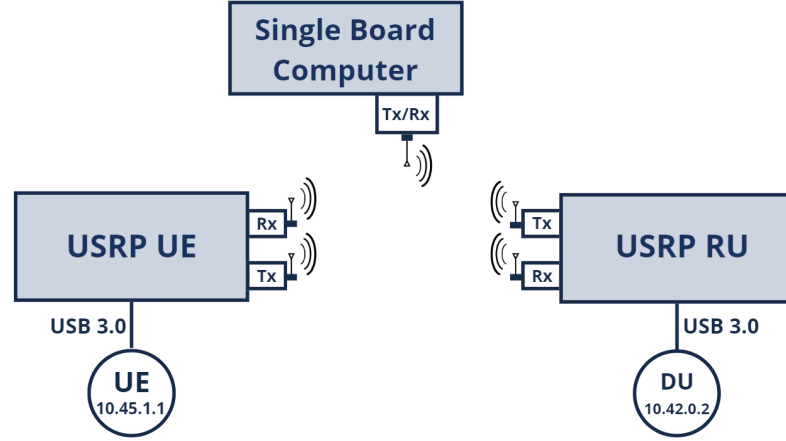


Figure 5.1: Wireless configuration testbed.

This configuration introduces challenges typical of real-world wireless communication systems. Continuous monitoring is required to maintain the testbed's integrity and ensure no external and unpredicted interference occurs during the experiments.

Furthermore, the proximity of transmitting and receiving antennas results in self-interference because our setup utilizes omnidirectional antennas, which operate close to each other on the same frequency band. Complex interference scenarios can also occur due to the OAI configuration when sending UL traffic three slots in advance. To minimize the risk of interference and effectively evaluate LBT, we strategically position the uplink and downlink antennas at a necessary minimum distance from each other, as represented in Figure 5.2.

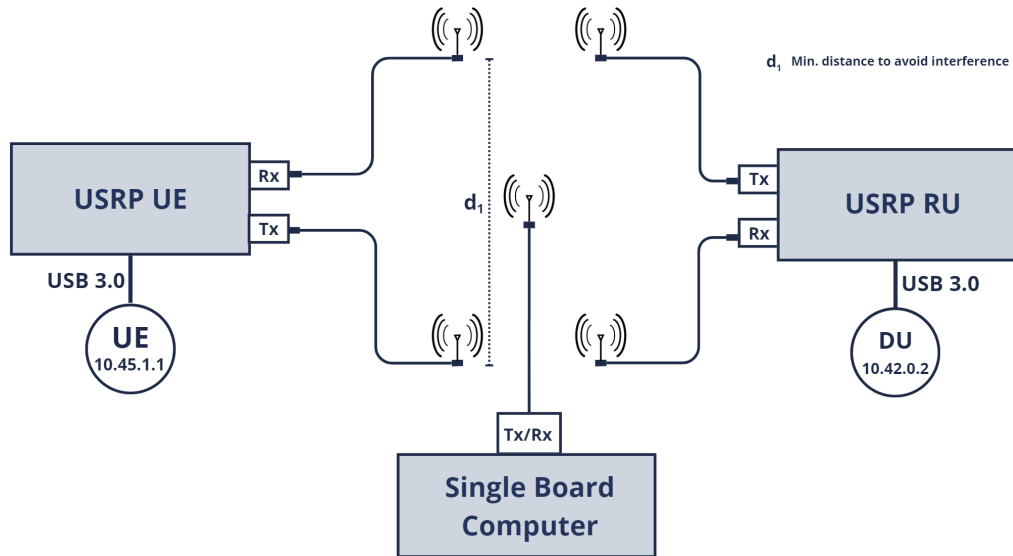


Figure 5.2: Wireless configuration testbed with proper distance to avoid interference.

In this updated testbed setup, we position the SBC centrally to simulate identical interference at the TX and RX antennas. This method allows for LBT evaluation, assuming that the only interference comes from our controlled setup. The setup's antennas have an approximate range of 1 meter, corresponding to the d_1 parameter. Regarding the specifications of the antennas, we have used the following antennas:

- **5G Devices Antennas - MobileMark OD5-2400/5500MOD2-BLK:** This antenna operates over frequency ranges of 2400-2485 MHz and 5150-5925 MHz, with a gain of 5 dBi. It is designed for harsh environmental conditions with omnidirectional coverage and is suited for marine and high-vibration settings like mining and construction. The design includes a powder-coated finish, stainless steel hardware, and conformal foam dampening.
- **Interference Antenna - TE Connectivity Linx ANT-W63WS5-SMA:** Covering a broad frequency range from 2.4 GHz to 2.5 GHz, 5.15GHz to 5.85GHz, and 5.925 GHz to 7.125 GHz, this antenna has variable gains, such as 4.0 dBi, 4.9 dBi, and up to 8.4 dBi, depending on the band. In 5.9 GHz, the value is 4.0 dBi.

The gains of each device are represented in Table 5.1. Antenna gains are denoted in decibel-isotropic (dBi), which quantifies the increase in power relative to an isotropic source, as opposed to dB, which is a general measure of gain. The USRP values are derived from the USRP Hardware Driver API logs. We could not adjust the RX gain at the gNB USRP due to the absence of a corresponding parameter in the OAI configuration. Consequently, the overall energy values at the gNB are expected to be lower than those at the UE.

Table 5.1: Antenna and Device Gain Specifications

Parameter	Value (dBi or dB)
Antenna for 5G Devices	5 dBi
Antenna for Interference	4 dBi
UE USRP B210 TX Gain	89.75 dB
UE USRP B210 RX Gain	76.00 dB
gNB USRP B210 TX Gain	89.75 dB
gNB USRP B210 RX Gain	36.00 dB

To investigate the anomalously high dB values observed in the USRP with the OAI configurations, we configured the SBC into monitor mode to detect the energy of the received signals. The 5G devices typically report energy values in negative dBm, which substantially deviate from those recorded in this project. The results from this investigation are illustrated in Figure 5.3. Analyzing the logs, it is possible to validate the hypothesis that the 5G network operates around -19 to -20 dBm.

Although utilized for comparative analysis, the dB values employed in this study should not be interpreted as direct energy indicators in linear terms. The abnormally high dB values recorded in the USRP with the OAI configurations remain unexplained, casting uncertainty on what these values represent and their impact on energy measurements. In the subsequent section, we will

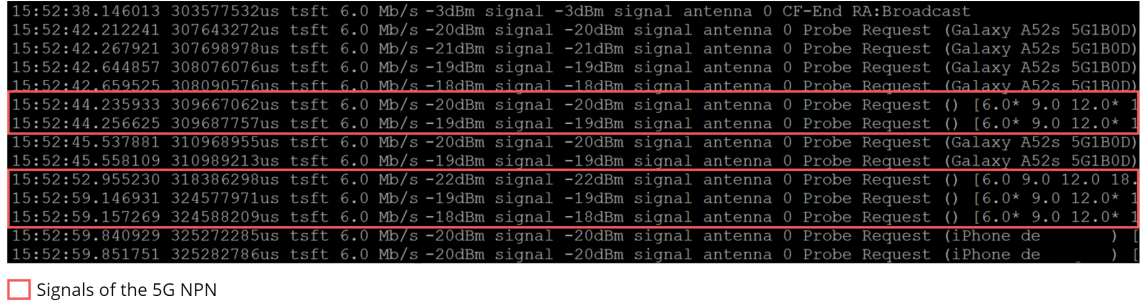


Figure 5.3: TCPdump logs from wlan0 on the SBC in monitor mode, confirming predicted energy values from the 5G NPN.

proceed with calculations based on these dB values; however, it is crucial to acknowledge that they do not precisely reflect actual energy levels.

5.2 Evaluating 5G Channel Energy and Interference without LBT

This section details the experimental evaluation of 5G channel conditions, focusing on energy measurement and interference impacts without implementing the LBT mechanism. In the first set of experiments, we aim to verify the proper operation of Time Division Duplex (TDD) configurations, confirming that the slot ratios align with the expected configurations. We assessed energy values under regular and heavy load traffic at the Downlink (DL) and Uplink (UL), increasing the traffic rate to evaluate the channel conditions without interference. In all the experiments, DL refers to the transmission from the 5G Core (5GC) to the User Equipment (UE), and the UL denotes transmission from UE back to the 5GC.

Subsequently, we introduced interference at different levels. At the same time, the 5G network maintained only control-plane activity, exchanging control information without generating additional traffic or performing demanding operational tasks at the user-plane level. This setup aimed to evaluate the impact of this interference on the channel's energy values. We also verified if the network operates at 5.85 GHz as expected by generating interference at the same frequency and detecting its impact on network performance. Given that the interference effects are symmetrical between the UE and the gNB, and we want to verify the interference presence during this set of experiments, we did most of the measurements only at the UE.

These experiments were configured to operate the 5G RAN network wirelessly, as represented in Figure 5.2, using a central channel frequency of 5854.08 MHz with an effective bandwidth of 40 MHz and 106 Resource Blocks (RB), employing a subcarrier spacing of 30 kHz as specified in Section 4.1.2.4. The TDD configuration has a periodicity of 2.5 ms, consisting of three DL slots, one mixed slot, and one UL slot.

5.2.1 Baseline Channel Energy Measurement

In the initial experiment, we generated downlink network traffic over 30s, using the *iperf* tool at various bitrates: 5 Mbits/s, 20 Mbits/s, and 40 Mbits/s. Adapting the code outlined in the previous chapter (described in Appendix A.3), we measure the energy of each symbol across every slot type, storing this data in the `samples.txt` file on the UE. The revised code is detailed in Appendix A.4. Each line in `samples.txt` records a timestamp, the absolute slot value, the energy of the slot, and the slot type. An example is illustrated below:

```
162800.000130448ns: Slot (DL) 1, Absolute_Slot: 15000, Symbol 0: 94.81dB
```

This setup achieves a sampling rate of 23,040 samples/ms. With such a high data capture rate, timestamps are meticulously recorded to ensure precise energy measurement accuracy.

Data processing was conducted using the `energy_measurements.py` script, listed in Appendix A.6. This script retrieves data from `samples.txt` and analyzes it to track channel energy fluctuations over time for each slot type. Each sample indicates the energy of a specific symbol inside a particular type of slot. The slot type indicates that the sample was acquired during a particular period. For instance, the red color samples are associated with the Downlink slot type, representing a symbol acquired during the Downlink slots of the TDD configuration. It also produces histograms depicting the average power ratio for each slot type. Gaussian Kernel Density Estimation (KDE) is applied to refine the statistical analysis of the data, offering a smooth approximation of the frequency distribution. This method concentrates the samples around prevalent values, alleviating the impact of outliers and resulting in a more reliable average representation of channel energies at any given time. Figures 5.4, 5.5, 5.6, and 5.7 illustrate the channel energy distributions under different network conditions, starting with only control-plane activity and progressing through increasing levels of data-plane DL traffic generated by *iperf*.

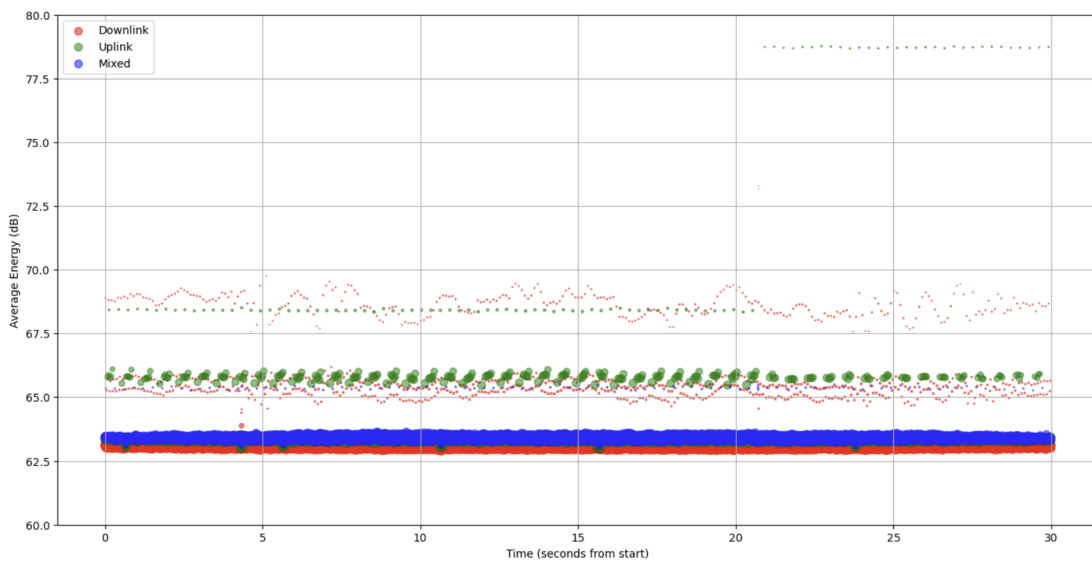


Figure 5.4: Channel energy distribution during idle mode with predominantly signaling (control-plane) activity, captured at the UE antenna.

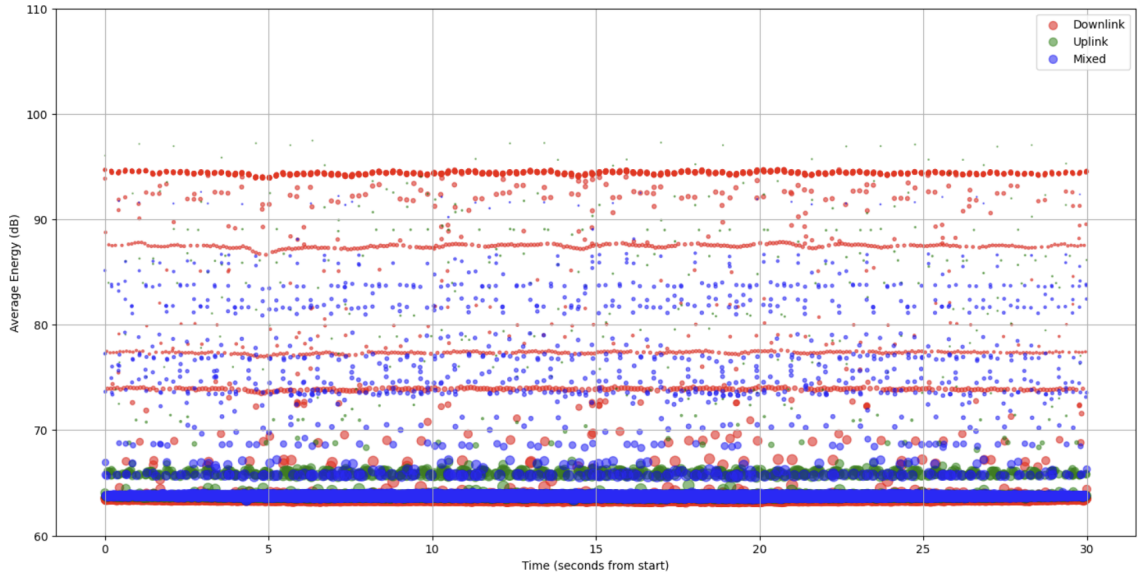


Figure 5.5: Channel energy distribution during active mode with a throughput of 5 Mbits/s generated using *iperf* for data-plane traffic in the downlink, captured at the UE antenna.

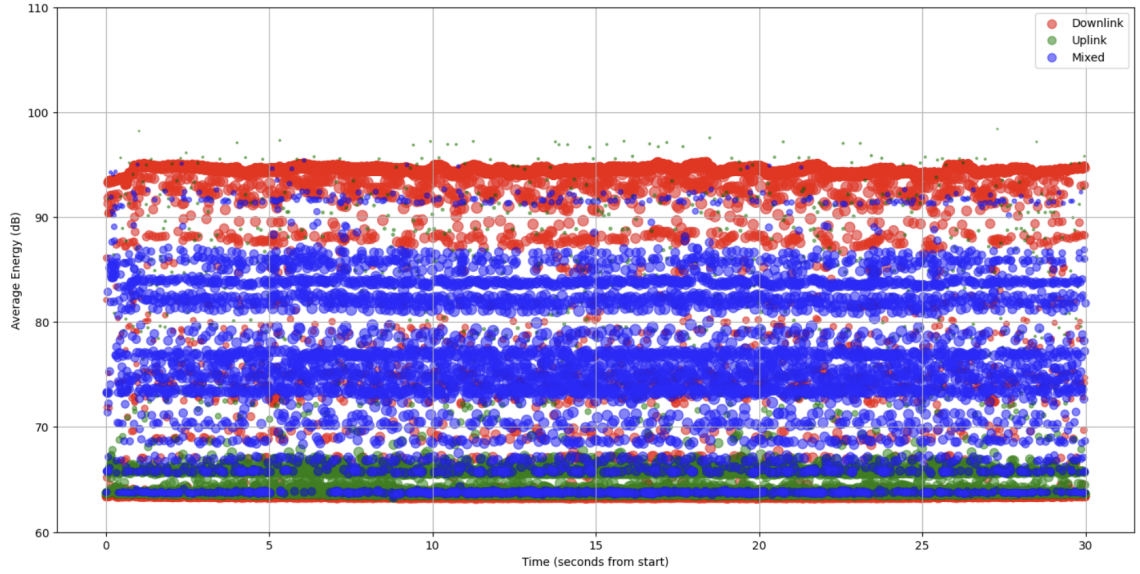


Figure 5.6: Channel energy distribution during active mode with a throughput of 20 Mbits/s generated using *iperf* for data-plane traffic in the downlink, captured at the UE antenna.

Additionally, we evaluated the average energy per slot during these transmission periods using the same script. Figure 5.8 shows the average energy with only control-plane activity, and Figure 5.9 demonstrates the energy with an added 40 Mbits/s of data-plane traffic in the downlink, generated with the *iperf* tool.

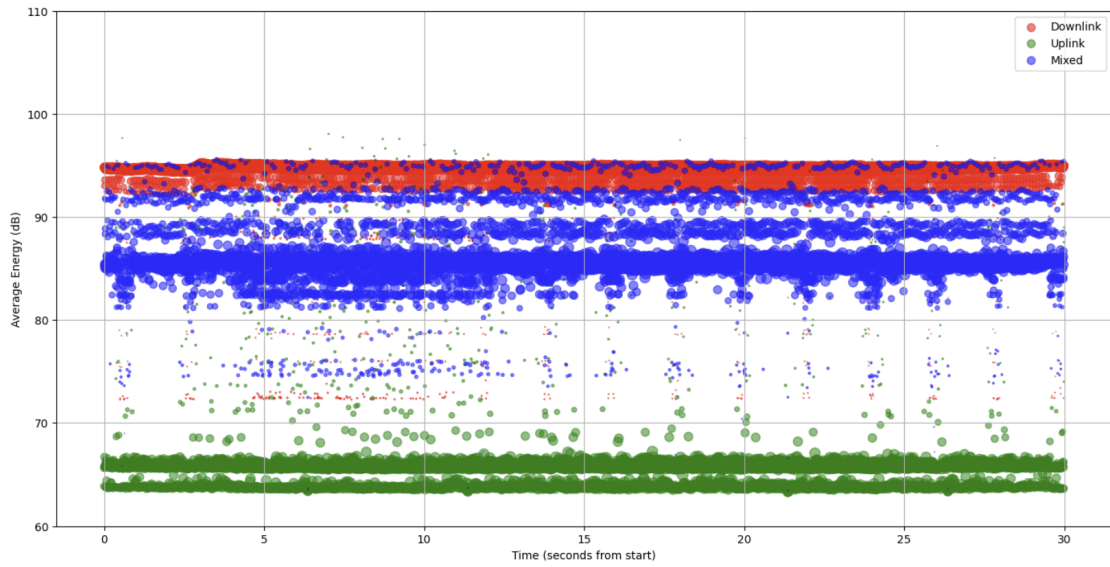


Figure 5.7: Channel energy distribution during active mode with a throughput of 40 Mbits/s generated using iperf for data-plane traffic in the downlink, captured at the UE antenna.

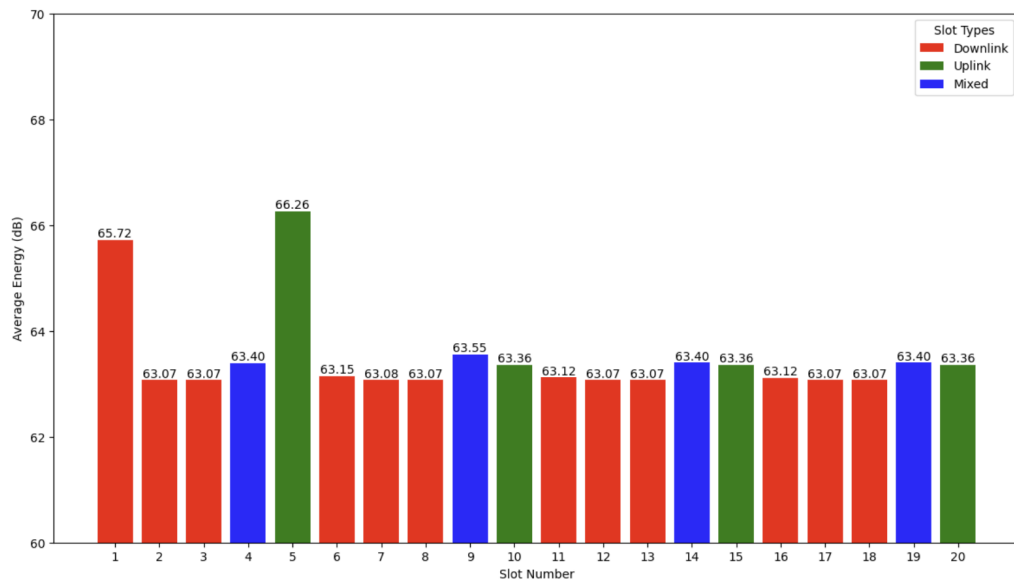


Figure 5.8: Average energy per slot with only control-plane activity, captured at the UE antenna.

The experimental results show that increases in bit rate significantly impact the energy levels in DL slots. The average energy values in DL slots rise from approximately 63–64 dB under low activity conditions to around 89 dB at higher bit rates. This demonstrates the direct relationship between data throughput and channel energy. Moreover, as illustrated in Figure 5.9, mixed slots exhibited higher energy levels than initially expected under heavy network load. Originally, it was anticipated that only six out of fourteen symbols in each mixed slot would be used for DL traffic, theoretically representing about 43% of the energy compared to full DL slots. Further analysis indicated that the UL symbols sent three slots earlier and expected to be empty are also being

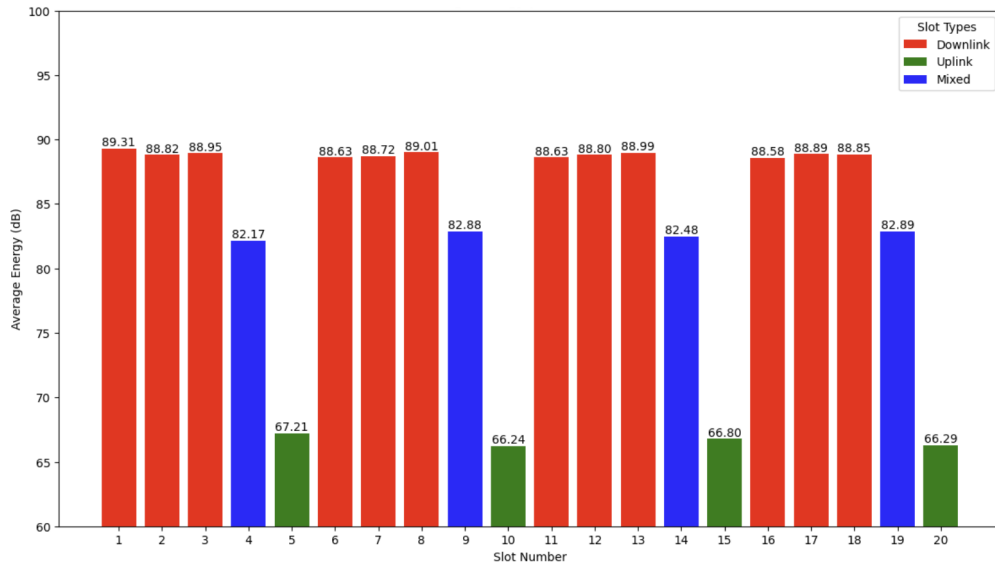


Figure 5.9: Average energy per slot at 40 Mbits/s in the downlink, captured at the UE antenna.

used for DL traffic. The four symbols intended to remain empty are respected, resulting in mixed slots having lower energy than full DL slots but still higher than expected, with nine symbols to transmit rather than six. Using designated UL slots for DL traffic suggests that LBT should not be performed in mixed slots, as the channel is not empty.

We did a similar experiment to verify the timing advance of three slots in the UE, detecting the energy values at the gNB with only control-plane activity, as shown in Figure 5.10 and with 8 MBits/s in the UL, as represented in Figure 5.11.

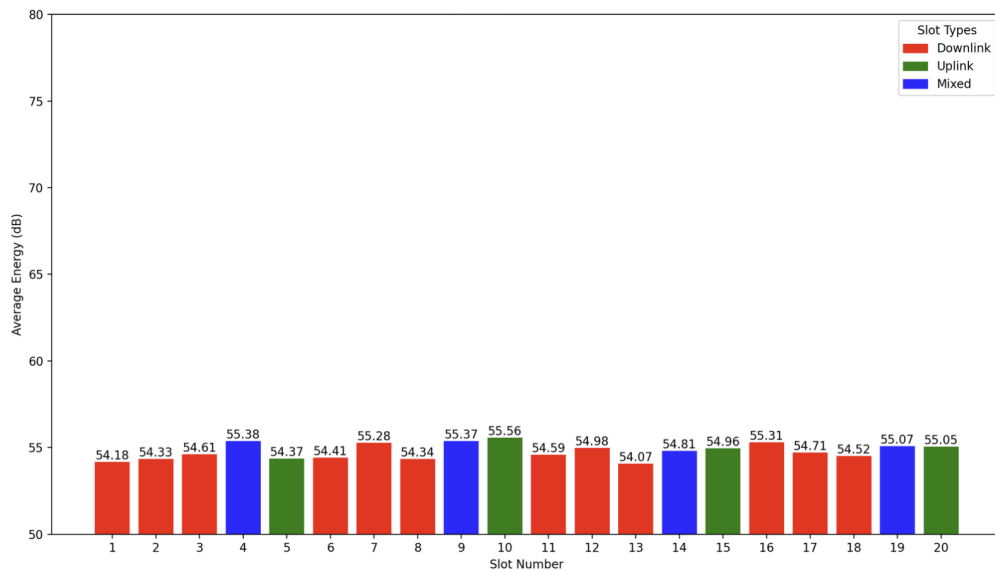


Figure 5.10: Average energy per slot with only control-plane activity, captured at the base station (gNB) RX antenna.

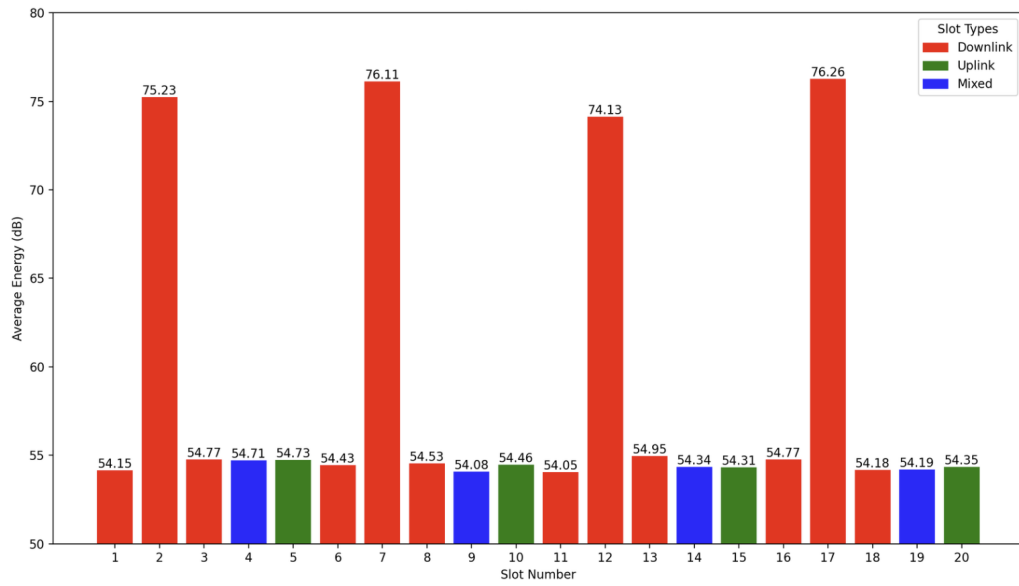


Figure 5.11: Average energy per slot with 8 Mbits/s uplink traffic, captured at the base station (gNB) RX antenna.

As previously explained, in OAI, UL data is transmitted three slots earlier, coinciding with the DL slots and leaving the UL slots empty. For this reason, it is predictable that at the gNB RX antenna, the UL traffic is captured in DL slots 2, 7, 12, and 17 (three slots before the UL slots).

Based on the experiments detailed above, we have successfully measured the energy of the channel signals, validated the TDD configuration, and confirmed the existence of the UE timing advance. We observe that the UL slots exhibit no traffic and thus serve as an optimal window for the sensing phase. As mentioned in table 5.2, the values for noise thresholds at both the UE and the gNB have been updated to manage interference more effectively. The lowest threshold values at the gNB are due to the different USRP gains, as previously mentioned in Table 5.1.

Table 5.2: Interference thresholds for UE and gNB based on interference levels.

Condition	UE Threshold (dB)	gNB Threshold (dB)
Baseline Noise Level	68	55
Maximum Network Activity	90	77

5.2.2 Impact of Interference on Channel Performance

In this set of experiments, we aim to introduce and detect interference in the 5G network to assess the capability of our current SBC configuration. This SBC is programmed to generate traffic at 5.8 GHz with 40 MHz bandwidth. The primary goal of these experiments is to validate if our interference signals are indeed impacting the 5G network as intended. This will test the network's response at the specific frequency and help us understand the feasibility of generating effective interference within this band.

Following the same approach as the previous set of experiences, we first measure the energy of the channel at the UE for 30 seconds, with the code listed in Appendix A.4 and registered the energy values in the `samples.txt` file. Then, we used the previous script `energy_measurements.py`, described in Appendix A.6, to process and plot the data. Our initial experiment focused on generating short bursts of high-energy signals within the 5G network using the SBC. This was achieved with the `generate_interference.sh` bash script that sends UDP packets at a given burst duration, with a given frequency, to increase the channel energy sporadically at a given rate. This code is detailed in Appendix A.9.

For these tests, we employed two burst frequencies—1 Hz and 2 Hz, each lasting 6 ms, the maximum allowed channel occupancy, according to Table 2.6. This setup was designed to simulate peak network conditions by momentarily injecting substantial data volumes into the network. The effects of these different interference frequencies on the 5G network are demonstrated in Figures 5.12 and 5.13, where the channel energy response is captured at the UE antenna.

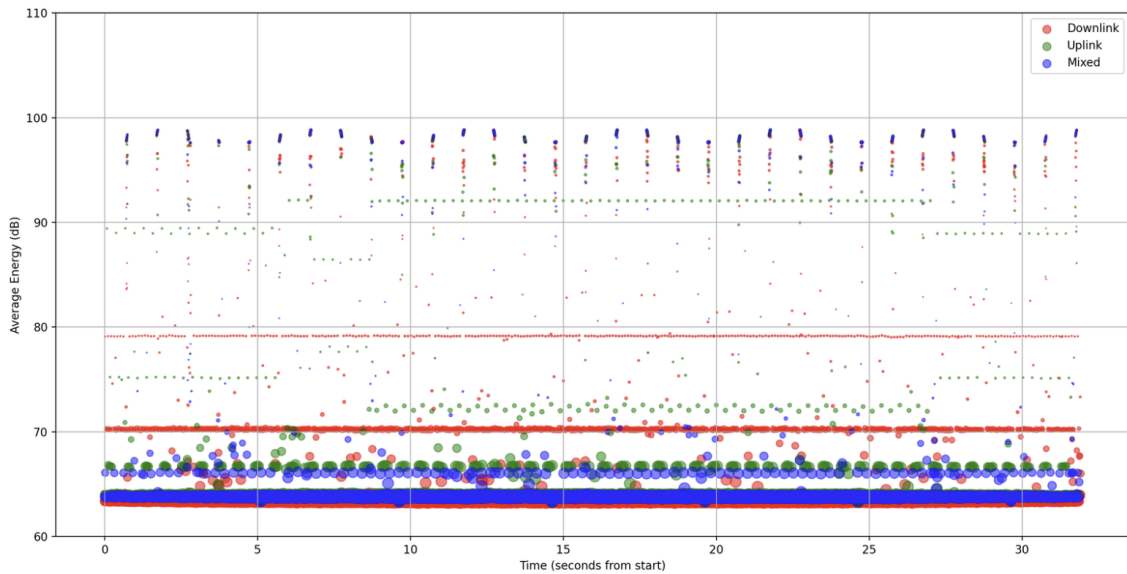


Figure 5.12: Channel energy distribution with episodic interference, showing peaks generated at 1 Hz, captured at the UE antenna.

The results demonstrated the presence of interference at the desired rates. Increasing the frequency of interference bursts to 2 Hz augmented the necessary downlink retransmissions, observed around a 78 dB threshold. This indicates that more frequent bursts of interference complicate the network’s ability to maintain uninterrupted downlink transmissions, directly impacting network performance and reliability.

In the subsequent experiments, we employed the *iperf* tool to generate traffic streams at rates of 5 Mbits/s and 20 Mbits/s, each lasting 10 seconds within a total experimental period of 30 seconds. This setup was designed to provide a consistent flow of data, intended to contrast with the episodic, high-intensity bursts of the earlier experiments. We limited our testing to these bitrates due to the network’s inability to handle traffic at 40 Mbits/s without overwhelming its operational

capabilities, which led to significant disruptions and compromised network stability.

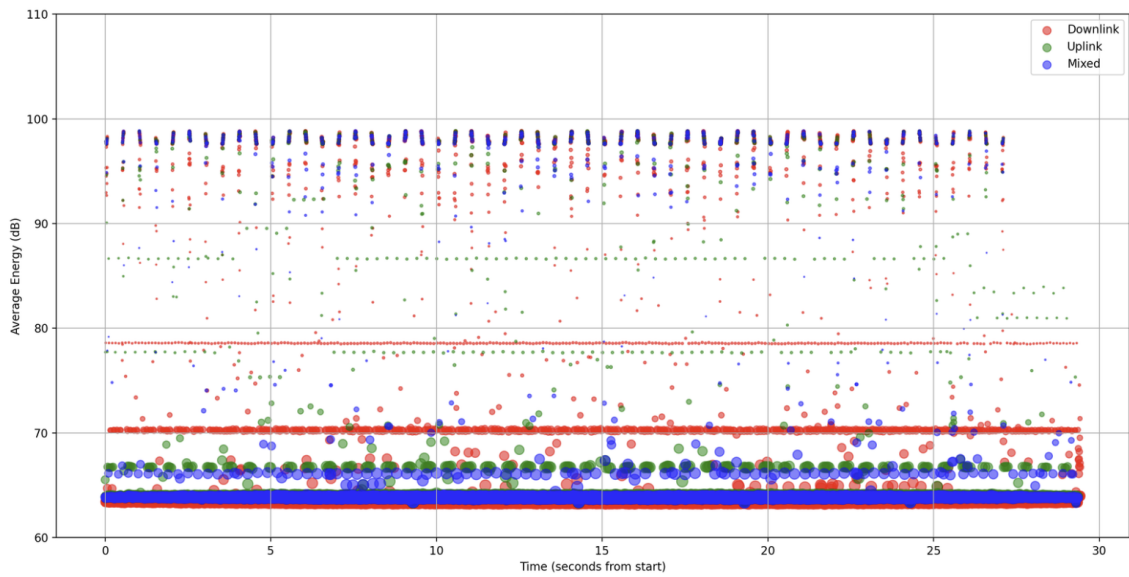


Figure 5.13: Channel energy distribution with episodic interference, showing peaks generated at 2 Hz, captured at the UE antenna.

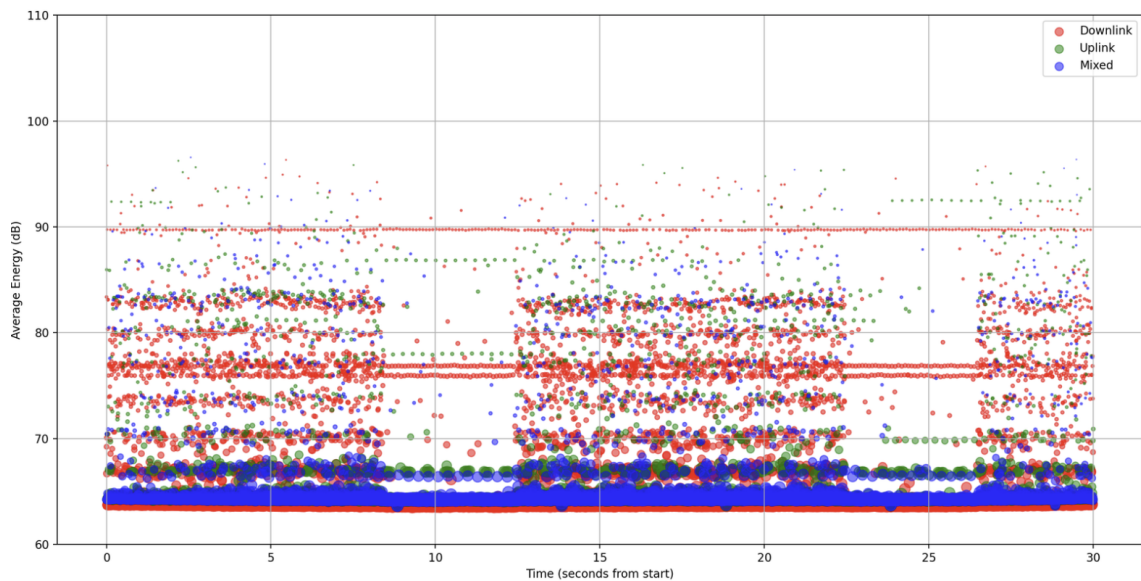


Figure 5.14: Channel energy distribution with 10-second data transmission streams at 5 Mbits/s, captured at the UE antenna.

After analyzing the results, it is possible to conclude that at 5 Mbits/s, the network showed resilience but with considerable operational stress, marked by numerous retransmissions. At 20 Mbits/s, the network experienced significant instability. It managed to function but with difficulty and frequent disruptions. This level of interference pushed the network's limits, causing multiple disruptions and revealing its constraints under sustained high-load interference. These sustained

interference trials show that attempting to perform the LBT under conditions where a device violates channel access rules is inadequate. The network struggled to maintain functionality without delays in access. Introducing mandatory wait times for a clear channel would render the network inoperable.

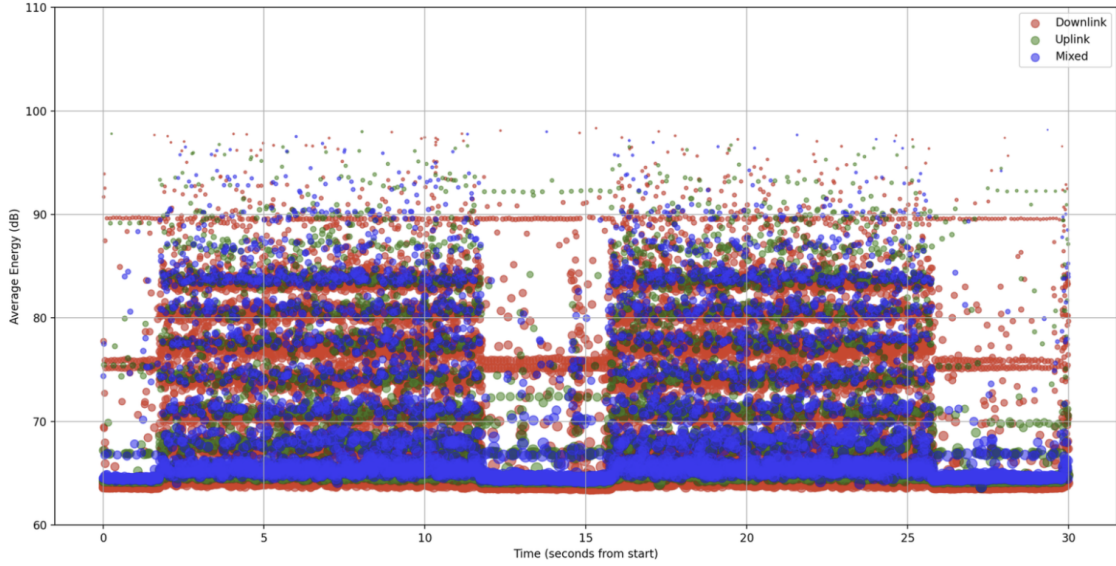


Figure 5.15: Channel energy distribution with 10-second data transmission streams at 20 Mbits/s, captured at the UE antenna.

This set of experiments has confirmed that both the 5G network and the SBC are operating within the desired frequency band, achieving the primary goal of our project. While validating and testing the LBT and network performance in the subsequent sections, we will limit interference to episodic occurrences that comply with established channel access parameters, as previously depicted in Table 2.6. This approach ensures a more realistic assessment of the network's capabilities and resilience under typical operational conditions.

5.3 LBT Validation and Network Performance Evaluation

This section describes a series of experiments conducted to validate the LBT mechanism under controlled interference conditions within the 5G network. The main goal is to assess the LBT's operational effectiveness in detecting and adapting to channel activity, thereby minimizing collisions.

The experiments are structured to introduce interference at various levels, mirroring the methodology used in earlier tests. Performance metrics such as throughput, latency, and block error rate (BLER) are analyzed to measure the impact of interference on network efficiency and reliability. This analysis aims to demonstrate the efficacy of LBT in maintaining optimal network performance and adherence to regulatory standards under various traffic loads and interference levels.

5.3.1 Validating LBT

The initial set of experiments was designed to validate the core capabilities of LBT by generating short, episodic interference traffic at both the gNB and the UE simultaneously. Interference bursts, lasting 30 ms each, were introduced at a rate of 1 Hz, creating peak energy values. This burst duration was chosen to improve the visualization of LBT operation. Threshold levels for LBT detection were adjusted based on the proximity of the interference-generating antenna to the receiving antennas of the 5G devices (95 dB for the UE and 80 dB for the gNB). The main objective is to visualize that, during interference periods, there was no activity from the 5G devices.

To align the data effectively between the gNB and UE, which were not synchronized by a clock, the use of the `absolute_slot` parameter was required. This approach allowed us to bypass issues related to time desynchronization and directly match data based on slot numbers. For instance, if peak energy was detected at absolute slot 2000, we could filter both devices' datasets to focus on samples around that specific slot. This method ensures that comparisons and analyses of data are synchronized despite the lack of inherent time alignment between the machines.

Regarding energy computation, we applied the same code as in the previous section but with a necessary modification. Upon detecting interference, we labeled the slot type of all symbols during the channel occupancy period as "Interference" in our data collection. As explained in Section 4.2.6, during this period, the gNB and UE were programmed to cancel all transmissions until the next sensing phase. This categorization of slot type as "Interference" ensures that the measured energy during these periods reflects solely the generated interference and any additional environmental noise. The updated code used in these experiments is detailed in Appendix A.5. Figures 5.16 and 5.17 illustrate the responses of the UE and gNB to these interference peaks.

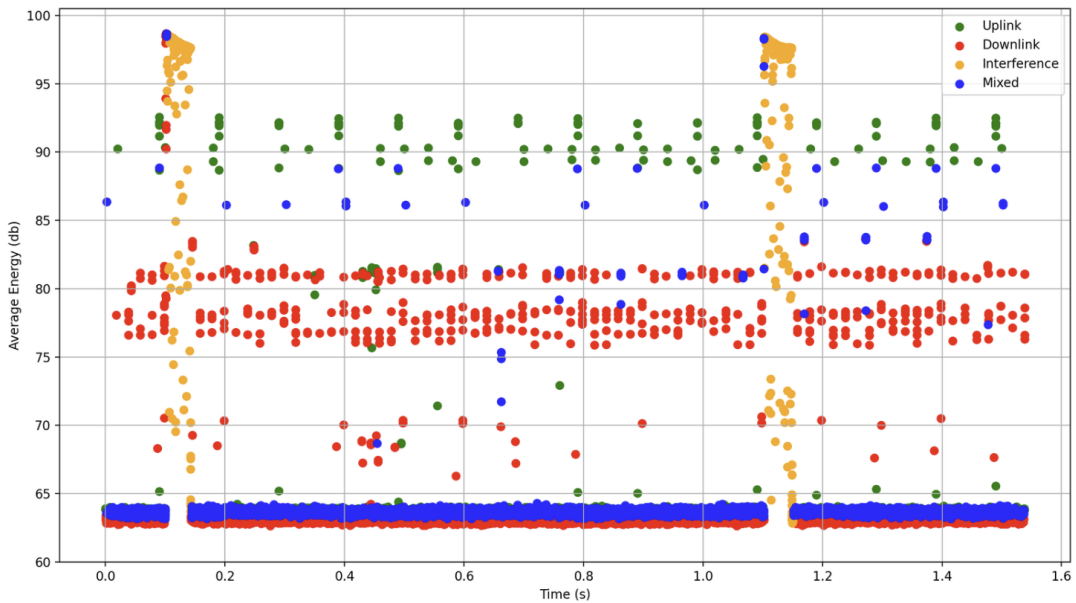


Figure 5.16: Channel energy distribution with episodic interference, showing peaks generated each second, captured at the UE antenna with the LBT mechanism enabled.

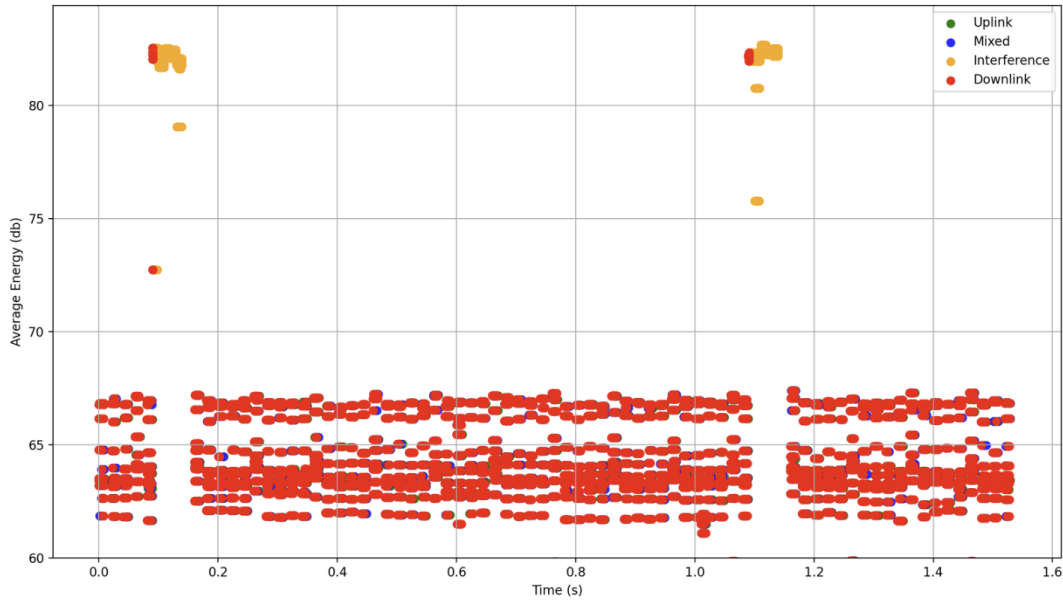


Figure 5.17: Channel energy distribution with episodic interference, showing peaks generated each second, captured at the gNB antenna with the LBT mechanism enabled.

Analyzing the results, we can conclude that the LBT mechanism was correctly implemented, as evidenced by the absence of activity from the UE and gNB during interference occurrences. Following the interference, the systems automatically resumed transmissions, confirming the LBT's effectiveness in managing and mitigating interference within the network.

5.3.2 Network Performance Evaluation

In this final set of experiments, we evaluated the network performance under the influence of LBT across various interference levels. The primary aim was to ascertain the potential delays introduced by LBT, which could impact key performance indicators such as latency, throughput, and Block Error Rate (BLER). Furthermore, the role of Time Division Duplex (TDD) configurations in influencing network performance is investigated using periodicities of 2 ms, 2.5 ms, and 5 ms. The 10ms TDD configuration in OAI did not allow more than three UL slots and was not possible to test because it was providing significant latency in the uplink; the slots available for the UE were all being used for ACK, resulting in the UE not having time to transmit.

5.3.2.1 Latency Evaluation

To evaluate network latency, we executed structured tests that involved sending 100 pings from the UE to the 5G core (5GC) for UL latency measurement. Conversely, pings were sent from the 5GC to the UE for DL. A bash script `ping_average.sh`, detailed in Appendix A.8, was developed to compute the average one-way latency from these pings. This script halves the round-trip time (RTT) to estimate one-way latency. This method is inherently limited because it assumes that the path latency is symmetrical between the forward and return paths. Thus, a more sophisticated

method that individually measures the latency of each direction would provide a more accurate reflection of network performance. Due to time constraints, developing the precise method was not possible.

We utilized the previously developed bash script, `generate_interference.sh`, detailed in Appendix A.9, to generate interference at specific burst durations and different rates. For these experiments, we specifically used burst durations of 3 ms and 6 ms with interference rates of 1 Hz, 2 Hz, and 10 Hz, respectively, to affect uplink and downlink communications. Table 5.3 presents the baseline one-way latency values for each TDD configuration operating in normal mode without interference but with the LBT mechanism implemented. These values represent the network's performance under optimal conditions and provide a benchmark for evaluating the impact of interference on network latency. Table 5.4 summarizes the one-way latency results for the 2 ms, 2.5 ms, and 5 ms periodicity TDD configurations under various interference scenarios.

Table 5.3: Baseline Uplink and Downlink latency for different TDD configurations with the LBT implemented, without interference.

TDD Periodicity (ms)	Uplink Latency (ms)	Downlink Latency (ms)
2	12.533	12.899
2.5	13.182	14.119
5	10.948	10.505

Table 5.4: Uplink and Downlink latency under different TDD configurations and interference Levels, with the LBT implemented.

TDD Periodicity (ms)	Interference Frequency (Hz)	Burst Duration (ms)	Uplink Latency (ms)	Downlink Latency (ms)
2	1	3	13.760	13.218
		6	13.859	14.155
	2	3	14.595	13.859
		6	14.719	14.413
	10	3	21.457	21.265
		6	23.221	22.661
2.5	1	3	13.543	16.253
		6	13.566	15.805
	2	3	14.595	18.738
		6	16.592	21.476
	10	3	22.557	28.861
		6	25.572	29.235
5	1	3	10.750	10.271
		6	10.880	10.725
	2	3	10.445	11.092
		6	11.203	11.334
	10	3	18.226	15.451
		6	18.915	17.592

The evaluation of network latency reveals that, as expected, both burst duration and interference frequency contribute to increased network latency. Specifically, the data indicate that as the burst duration and interference frequency increase, latency in both uplink and downlink channels also increases.

The TDD configuration also impacts channel performance. The 5 ms TDD configuration, featuring extended sequences of the same slot type, demonstrates the benefits of extended consecutive processing periods, enhancing the network's efficient data transmission and interference management. Conversely, the 2.5 ms configuration, despite having one more downlink slot than the 2 ms setup, results in higher uplink latency. This detriment arises because the added downlink slot increases the pressure on the UE, which struggles to manage the uplink efficiently due to the disproportionate downlink-to-uplink slot ratio of 3:1. The 2 ms configuration, with a more balanced downlink-to-uplink ratio of 2:1, performs better than the 2.5 ms setting, despite more frequent switching. These results, supported by the baseline values without interference, suggest that adding more downlink slots without a balanced approach can worsen performance and increase uplink pressure and overall latency.

In an additional experiment, the previous script was updated to incrementally increase network traffic over time following a controlled exponential distribution with a 1.02 growth rate, starting at 1 Hz (1 interference per second) and escalating to 100 Hz, with a fixed burst duration of 3 ms. The code is detailed in Appendix A.7. The experiments included an analysis of the interference frequency threshold that leads to network crashes, with results depicted in Figure 5.18 for the uplink and Figure 5.19 for the downlink. For benchmarking purposes, the same experiment was conducted in the uplink without the LBT mechanism, illustrated in Figure 5.20.

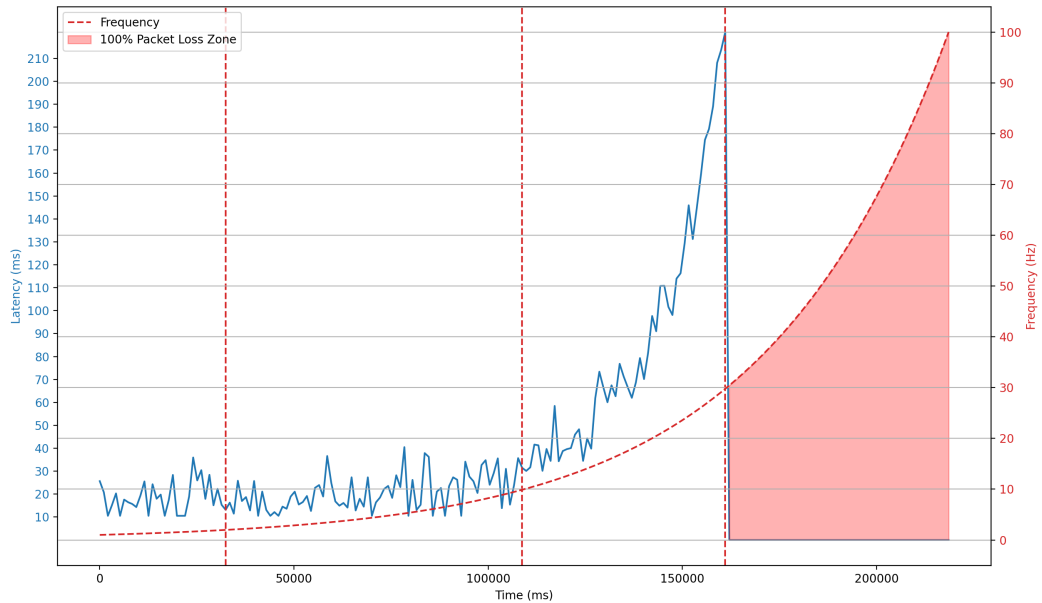


Figure 5.18: Uplink Latency with an exponential increase in the interference frequency of 3 ms bursts. Network operating in 5 ms TDD Configuration with LBT Mechanism.

Analyzing the results, it is possible to observe that the LBT mechanism increases network

latency under the tested conditions. The added delay causes this increased latency as the system waits for a clear channel before transmitting, which can be beneficial in avoiding collisions but detrimental to latency in environments with frequent or constant interference. Additionally, the concurrent delays also pressure the radio buffers. This pressure can lead to desynchronization and cause network crashes under smaller interference scenarios, which is evident in our experiments, with the implementation without LBT allowing the network to operate with a higher interference frequency.

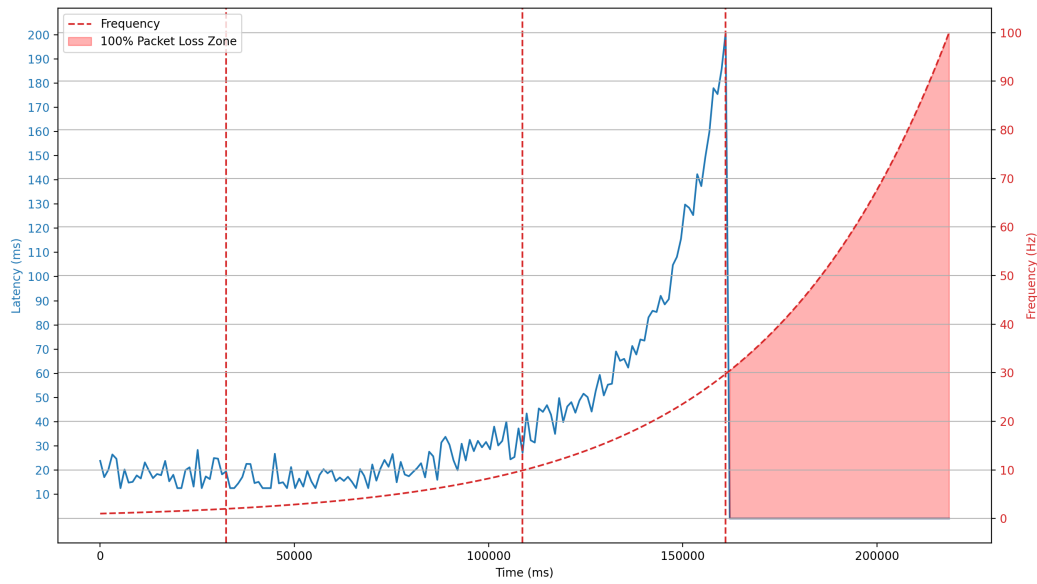


Figure 5.19: Downlink Latency with an exponential increase in the interference frequency of 3 ms bursts. Network operating in 5 ms TDD Configuration with LBT Mechanism.

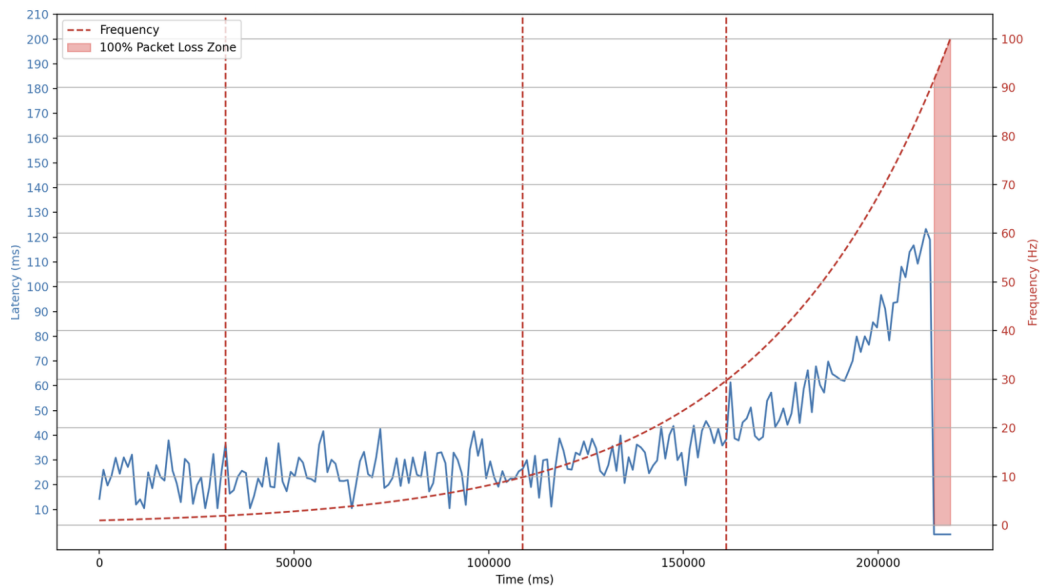


Figure 5.20: Uplink Latency with an exponential increase in the interference frequency of 3 ms bursts. Network operating in 5 ms TDD Configuration without the LBT Mechanism.

In conclusion, while the LBT mechanism aids in the coexistence of multiple communication technologies, its implementation under the tested conditions leads to increased latency and a higher probability of network failures under higher interference frequencies.

5.3.2.2 Throughput Evaluation

We extend our network performance analysis in the following experiments by examining throughput. Due to the implementation of LBT, a simple `iperf` test asking for maximum throughput during interference periods was causing the network to crash. These disruptions were only observed at frequencies of 2 Hz with 6 ms bursts and 10 Hz for both 3 ms and 6 ms bursts. This issue arises because the maximum throughput, coupled with the additional latency from interference, forced the OAI to deviate from the TDD configuration, leading to data being sent desynchronized in all slots. This data transmitted between the gNB and UE was not sent in the expected slot type, was misinterpreted as interference, and caused further disruptions in the network. This issue certainly presents a challenge for future work, as it necessitates further investigation into the OAI behavior and whether we can prevent these disruptions or modify the LBT approach in such scenarios.

For this reason, we implemented a systematic approach using the `iperf` tool, incrementally increasing the bandwidth in increments of 0.1 Mbits/s. Each increase was tested over 60 seconds to accurately determine the point at which the network would begin to fail. This testing protocol was applied across uplink and downlink paths in the three TDD configurations. The tests were conducted by simulating different interference levels with burst durations of 3 and 6 milliseconds and interference rates of 1 Hz, 2 Hz, and 10 Hz, respectively. Table 5.5 presents the baseline throughput values for each TDD configuration operating in normal mode with the LBT mechanism implemented and without interference. Table 5.6 summarizes the maximum throughput results observed that do not cause network crashes. For instance, a value of 40.1 Mbits/s indicates that an increase to 40.2 Mbits/s resulted in network failure.

Table 5.5: Baseline Uplink and Downlink throughput for different TDD configurations without interference and LBT implementation.

TDD Periodicity (ms)	Uplink Throughput (Mbits/s)	Downlink Throughput (Mbits/s)
2	9.44	40.93
2.5	8.21	42.91
5	10.52	46.12

Reviewing the throughput results under various interference conditions clearly shows a decline in network performance, with lower throughput rates observed across UL and DL as interference frequency and burst duration increase. Additionally, the experiments demonstrated the influence of TDD configuration and interference levels on network performance, corroborating the principles observed in latency assessments. Notably, the 5 ms TDD configuration demonstrates the highest throughput due to its extended sequences of the same slot type. Despite the higher uplink latency, the 2.5 ms configuration offers better downlink throughput than the 2 ms setup, indicating that the

Table 5.6: Uplink and Downlink throughput under different TDD configurations and interference Levels, with the LBT implemented.

TDD Periodicity (ms)	Interference Frequency (Hz)	Burst Duration (ms)	Uplink Throughput (Mbits/s)	Downlink Throughput (Mbits/s)
2	1	3	8.27	38.41
		6	7.98	38.22
	2	3	8.13	37.53
		6	7.10	35.10
	10	3	4.60	22.10
		6	3.80	20.20
2.5	1	3	7.56	40.12
		6	6.34	39.04
	2	3	5.23	38.41
		6	4.90	38.30
	10	3	2.50	26.50
		6	1.70	21.40
5	1	3	10.32	45.37
		6	10.12	44.18
	2	3	9.40	41.21
		6	8.30	40.80
	10	3	6.20	28.10
		6	5.10	24.40

additional downlink slot enhances the maximum throughput capability. This improvement occurs even though the disproportionate downlink-to-uplink slot ratio of 3:1 places more pressure on the uplink, reducing its overall throughput, especially when interference is introduced.

5.3.2.3 Block Error Rate (BLER) Evaluation

To finalize the experiments, we analyzed the Block Error Rate (BLER) for UL and DL transmissions. The BLER metric provides the ratio of erroneously received blocks to the total number of blocks. This value is computed for the Physical Uplink Shared Channel (PUSCH) and Physical Downlink Shared Channel (PDSCH) using the available OAI data that provides the number of errors and transmitted resource blocks during transmission. The specific formulas for the PUSCH and PDSCH are as follows:

$$\text{BLER (\%)} = \left(\frac{\text{Number of Erroneous Blocks}}{\text{Number of Erroneous Blocks} + \text{Number of Correct Blocks}} \right) \times 100\%$$

The BLER values from the gNB and the UE are accessible and computed by the Distributed Unit (DU). Each sample is obtained every 120 frames for PDSCH and PUSCH. We exported 100 BLER samples (1200 frames) for PUSCH and PDSCH during the experiments to a text file `samples_bler.txt`. Each pair of entries in `samples_bler.txt` follows the format:

UE 0fb7: dlsch_rounds 43/0/0/0 MEAN BLER 0.03988 | STDDEV BLER 0.03192
 UE 0fb7: ulsch_rounds 52/28/0/0 MEAN BLER 0.25640 | STDDEV BLER 0.16588

Subsequently, we computed the average BLER for each channel under the same interference scenarios described, generating interferences at 1 Hz, 2 Hz, and 10 Hz with burst durations of 3 ms and 6 ms. Table 5.7 illustrates the results.

Table 5.7: PDSCH and PUSCH Block Error Rate (BLER) under different TDD configurations and interference levels.

TDD (ms)	Interference Frequency (Hz)	Burst Duration (ms)	Downlink		Uplink	
			μ_{BLER}	σ_{BLER}	μ_{BLER}	σ_{BLER}
2	1	3	0.00513	0.01470	0.19841	0.06003
		6	0.01078	0.02290	0.26695	0.09660
	2	3	0.02555	0.06362	0.28736	0.09524
		6	0.09929	0.01961	0.28712	0.08906
	10	3	0.16969	0.07120	0.38611	0.01596
		6	0.21470	0.04328	0.41727	0.17792
2.5	1	3	0.00597	0.02849	0.21253	0.09615
		6	0.02973	0.04653	0.32437	0.10307
	2	3	0.04143	0.06640	0.26705	0.09792
		6	0.04361	0.07689	0.28990	0.10779
	10	3	0.26182	0.26370	0.39245	0.10081
		6	0.33521	0.35136	0.43790	0.10687
5	1	3	0.01305	0.01718	0.27127	0.09900
		6	0.06916	0.08234	0.32014	0.09499
	2	3	0.04849	0.05102	0.28482	0.08420
		6	0.08910	0.01465	0.31081	0.15380
	10	3	0.26251	0.25049	0.41745	0.17848
		6	0.38040	0.31124	0.50633	0.19387

The observed increase in BLER levels in the PUSCH compared to the PDSCH indicates an imbalance in transmission and reception configurations. This imbalance is directly related to the settings of the gNB and UE antennas, as evidenced by the USRP configurations. Specifically, the USRP gNB receiver is configured to 36 dB, unlike the UE set at 76 dB, as detailed in Table 5.1. Consequently, the UE experiences a higher rate of errors, pointing to an inadequately balanced gain configuration across the network components.

Moreover, our experiments continued to show the negative influence of interference, as both burst duration and interference frequency contribute to an increased average BLER of both the PUSCH and the PDSCH. Regarding the TDD configuration, we got a different relation than the latency and throughput measurements, where the TDD with 5 ms periodicity performs worst. Our results indicate that longer TDD configurations correlate with higher average BLER. The mechanics of LBT can explain this observation. During periods of interference, the number of transmission errors corresponds to the number of blocks scheduled for transmission that will not be sent (essentially, BLER equals one during interference periods). Furthermore, in configurations with shorter cycles, such as 2 and 2.5 ms, the sensing phase occurs more frequently compared to

the 5 ms configuration. This higher sensing rate in shorter TDD cycles could explain the variations in BLER for this interference observed across different configurations.

We did a second experiment to validate the LBT influence on the BLER, increasing the interference rate and analyzing the average BLER over a sequence of frames with and without the LBT mechanism, as represented in Figures 5.21 and 5.22, respectively. The code that reads the `samples_bler.txt` and plots the data is represented in Appendix A.10.

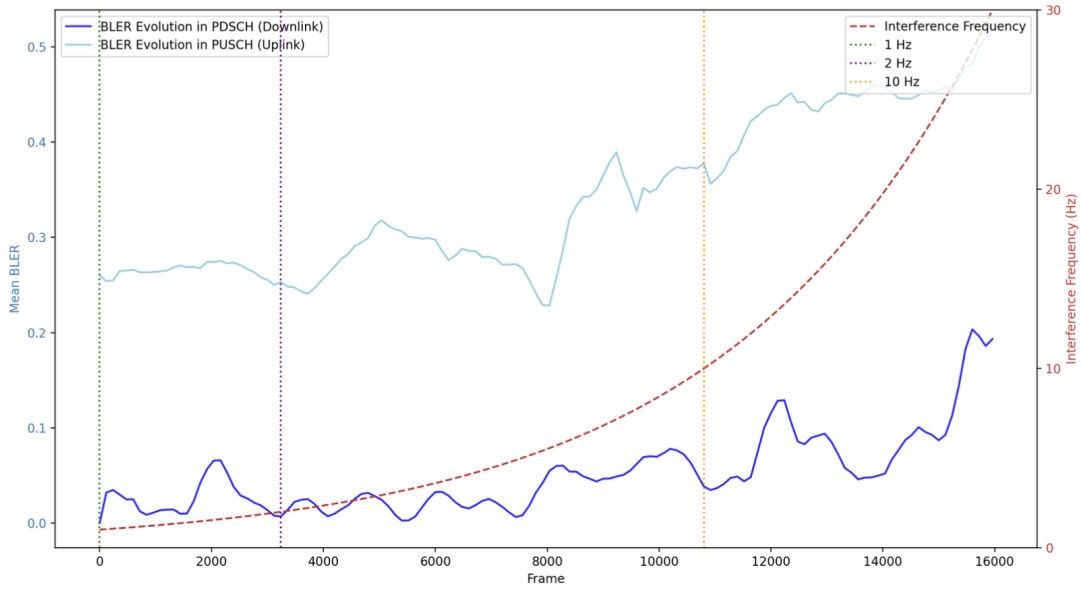


Figure 5.21: Average BLER with an exponential increase in the interference frequency of 3 ms bursts. Network operating in 2 ms TDD Configuration with LBT Mechanism.

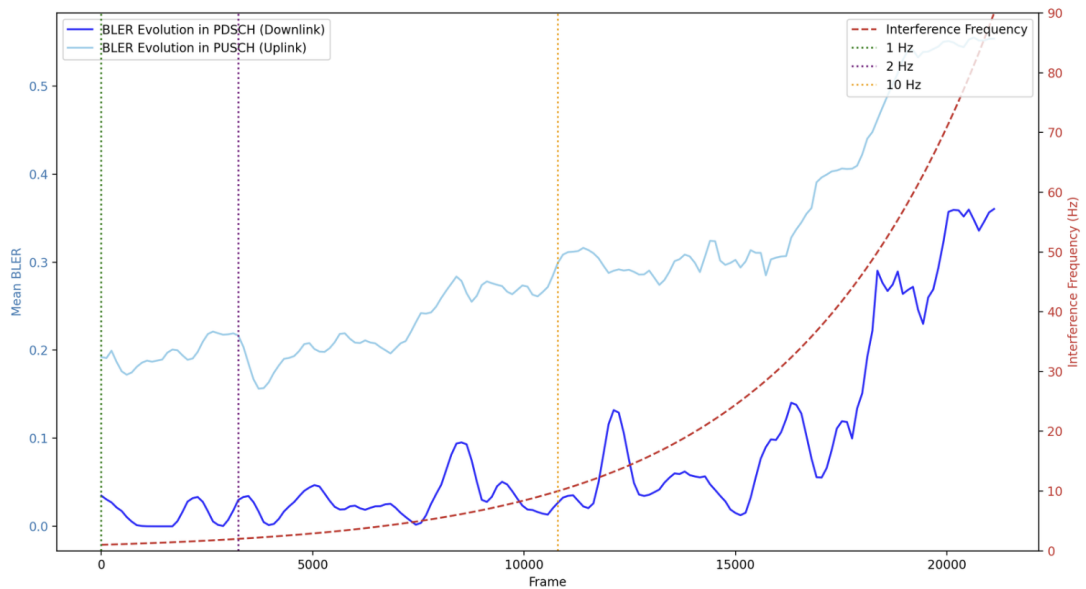


Figure 5.22: Average BLER with an exponential increase in the interference frequency of 3 ms bursts. Network operating in 2 ms TDD Configuration without LBT Mechanism.

Our observations confirmed that with the implementation of the LBT mechanism, the BLER was constantly higher as the system refrained from transmitting blocks under detectable interference levels. Intriguingly, only when interference rates exceeded 20 Hz did we begin to see an escalation in BLER in systems without LBT. This indicates that the level of interference the LBT was avoiding was not severe enough to be considered impactful to cause errors, which might suggest that BLER was not inherently higher due to interference but due to the non-transmission policy of LBT. Although this might appear to be a drawback for LBT, it reflects adherence to channel rules. LBT ensures that our transmissions do not contribute to the cumulative interference that could affect other network elements' BLER, throughput, or latency. Thus, while some of the interference avoided by LBT might not directly impact our channel's reception capability, the mechanism helps maintain a cleaner channel environment conducive to overall network quality, which is the primary goal of this mechanism.

Chapter 6

Final Remarks

6.1 Conclusion

The key findings of this work were successfully designing and implementing a version of NR-U by adapting a non-public network (NPN) to support operations in an unlicensed band. This encompassed two primary tasks: altering channel configurations at both software and hardware levels to support operation in the unlicensed band and implementing a coexistence mechanism, specifically Listen-Before-Talk (LBT), to adhere to channel access rules.

These objectives were successfully completed, and our network is now correctly operating in the unlicensed band. We conducted multiple performance evaluations, focusing on key aspects such as detecting potential interference within the unlicensed channel band and appropriately halting transmissions to mitigate any impact. Furthermore, we analyzed the interference effect and delineated how the network operates under different interference levels, enriching the details and understanding of this new NPN's capabilities and resilience. Main performance metrics such as throughput, latency, and Block Error Rate (BLER) were assessed to ensure the network's operational efficiency and robustness under various conditions.

6.2 Future Work

The successful deployment and evaluation of the NR-U highlight several areas for future research and development to enhance system performance and utility. A critical objective requiring further exploration is testing the network under Cooperative Intelligent Transportation Systems (C-ITS) requirements, aligning more closely with the Route 25 Project. Future studies should focus on adapting our network to meet these specialized demands and validate its performance in vehicular communication environments.

Another critical area of future work involves addressing the disparity between uplink (UL) and downlink (DL) performance observed during the project. Potential issues in gain configurations

and excessive acknowledgment (ACK) packets in the UL can significantly impact network efficiency. Investigating and resolving these discrepancies is crucial for effectively balancing UL and DL and improving the overall NPN performance.

Improvements to the LBT mechanism are also necessary. While effective under certain conditions, LBT has shown limitations during high traffic loads, leading to network crashes and buffer overflows. Developing a more sophisticated LBT implementation that can handle high loads without disrupting network operations is essential. This might include enhanced algorithms that better manage data transmission based on real-time network conditions and more effectively communicate with upper layers and the RF front-end about transmission readiness.

Furthermore, while the implemented coexistence mechanisms effectively prevent interference with the 5G network, they do not fully consider the performance of other communications within the same channel. Future experiments should include more detailed evaluations considering multiple transmitters, different priorities, and varied interference profiles. This approach should protect the 5G network from interference and enhance the overall communication environment, ensuring that coexistence mechanisms improve the performance of all users sharing the spectrum.

Addressing these areas will allow future developments to build on the current project's successes and further refine the integration of 5G NR-U technology in Non-Public Networks, particularly in contexts like C-ITS, where robust and reliable communication is critical.

References

- [1] 3GPP. System architecture for the 5g system (5gs). Technical Specification (TS) 23.501, 3GPP, 12 2017. Version 15.0.0, Under change control, Available at: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144>.
- [2] 3GPP. Release 16 description; summary of rel-16 work items. Technical Report 21.916, 3GPP, 07 2018. Available at: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3493>.
- [3] 3GPP. Study of separation of nr control plane (cp) and user plane (up) for split option 2. Technical Report 38.806, 3GPP, 01 2018. Version 15.0.0, Available at: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3307>.
- [4] 3GPP. Study on New Radio (NR) Access Technology (Release 15). Tech. Rep. TS 39.912 V15.2.0, 3GPP, Sophia Antipolis, France, 2018.
- [5] 3GPP. Open ran, 2021. Available at <https://www.3gpp.org/news-events/3gpp-news/open-ran>.
- [6] 3GPP. 5g system overview, 2022. Available at <https://www.3gpp.org/technologies/5g-system-overview>.
- [7] 3GPP. Summary of rel-16 work items. Technical Report TR 21.916 version 16.0.1 Release 16, 3GPP, 2023. Available at: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3493>.
- [8] 5G Americas. 5g evolution: 3gpp release 16 and release 17, 2020. Available at https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14680, Accessed: Dec. 26, 2023.
- [9] Muhammad Ali. Performance analysis of physical downlink shared channels for 5g new radio. 08 2019.
- [10] 5GAA Automotive Association. Deployment band configuration for c-v2x at 5.9 ghz in europe. *Position Paper*, 2021.
- [11] R. Bajracharya, R. Shrestha, and H. Jung. Future is unlicensed: Private 5g unlicensed network for connecting industries of future. *Sensors (Basel)*, 20(10):2774, May 2020.
- [12] Rojeena Bajracharya, Rakesh Shrestha, Syed Hassan, Haejoon Jung, Rafay Ansari, and Mohsen Guizani. Unlocking unlicensed band potential to enable urllc in cloud robotics for ubiquitous iot. *IEEE Network*, 35, 2021.

- [13] Volker Braun, Karol Schober, and Esa Tirola. 5g nr physical downlink control channel: Design, performance and enhancements. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6, 2019.
- [14] European Commission. 5g cross-border corridors for connected and automated mobility, 2024.
- [15] Roberto Maldonado Cuevas, Claudio Rosa, Frank Frederiksen, and Klaus I. Pedersen. On the impact of listen-before-talk on ultra-reliable low-latency communications. *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, 2018.
- [16] Erik Dahlman et al. *5G NR: The Next Generation Wireless Access Technology*. Academic Press, 2020.
- [17] EN ETSI. 5 ghz rlan; harmonised standard covering the essential requirements of article 3.2 of directive 2014/53/eu. *Harmonised Standard Covering the Essential Requirements of Article, 3*, 2017.
- [18] European Commission. Radio spectrum decisions. Available at <https://digital-strategy.ec.europa.eu/en/library/radio-spectrum-decisions>.
- [19] Mohammed Hirzallah, Marwan Krunz, Balkan Kecicioglu, and Belal Hamzeh. 5g new radio unlicensed: Challenges and evaluation. *IEEE Transactions on Cognitive Communications and Networking*, PP, 11 2020.
- [20] Richard Jacob, Nick Schwarzenberg, Friedrich Burmeister, and Gerhard Fettweis. Congestion-aware packet repetitions for ieee 802.11bd-based safety-critical v2v communications. pages 315–321, 05 2022.
- [21] Jeongho Jeon, Russell Ford, Vishnu Ratnam, Joonyoung Cho, and Jianzhong Zhang. Coordinated dynamic spectrum sharing for 5g and beyond cellular networks. *IEEE Access*, PP:1–1, 08 2019.
- [22] Yasin Kabalcı and Muhammad Ali. Throughput analysis over 5g nr physical uplink shared channels. In *2020 2nd Global Power, Energy and Communication Conference (GPECOM)*, 2020.
- [23] L. Kleinrock and F. Tobagi. Packet switching in radio channels: Part i - carrier sense multiple-access modes and their throughput-delay characteristics. *IEEE Transactions on Communications*, 23(12):1400–1416, 1975.
- [24] Katarzyna Kosek-Szott, Alice Lo Valvo, Szymon Szott, Pierluigi Gallo, and Ilenia Tinnirello. Downlink channel access performance of nr-u: Impact of numerology and mini-slots on coexistence with wi-fi in the 5 ghz band. *Computer Networks*, 195:108188, 2021.
- [25] Meik Kottkamp, Anil Pandey, Andreas Roessler, Reiner Stuhlfauth, and Daniela Raddino. *5G New Radio: Fundamentals, Procedures, Testing Aspects*. Rohde Schwarz GmbH Co. KG, Germany, 2019.
- [26] Lopamudra Kundu, Gang Xiong, and Joonyoung Cho. Physical uplink control channel design for 5g new radio. In *2018 IEEE 5G World Forum (5GWF)*, pages 233–238, 2018.

- [27] Sandra Lagen, Lorenza Giupponi, Sanjay Goyal, Natale Patriciello, Biljana Bojović, Alpaslan Demir, and Mihaela Beluri. New radio beam-based access to unlicensed spectrum: Design challenges and solutions. *IEEE Communications Surveys Tutorials*, 22(1):8–37, 2020.
- [28] Yonghui Li, Mahyar Shirvanimoghaddam, Rana Abbas, Changyang She, and Branka Vucetic. Urllc for 5g and beyond: Physical, mac and network solutions 2020 ieee wcnc tutorial, 08 2020.
- [29] Viacheslav Loginov, Evgeny Khorov, A. Lyakhov, and Ian Akyildiz. Cr-lbt: Listen-before-talk with collision resolution for 5g nr-u networks. *IEEE Transactions on Mobile Computing*, PP:1–1, 01 2021.
- [30] Mohammad Mozaffari, Y.-P. Eric Wang, and Kittipong Kittichokechai. Blocking probability analysis for 5g new radio (nr) physical downlink control channel. In *ICC 2021 - IEEE International Conference on Communications*.
- [31] 3GPP; Technical Specification Group Radio Access Network. Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation. 3GPP TS 36.211. Available online: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2425>.
- [32] Larry Peterson, Oguz Sunay, and Bruce Davie. *Private 5G: A Systems Approach*. Systems Approach LLC, U.S.A, 2023. Available at: <https://5g.systemsapproach.org/>.
- [33] José Pedro Nogueira Rodrigues. Open source non-public 5g networking in licensed and unlicensed bands. Universidade do Porto, Faculdade de Engenharia, 09 2023. Available at <https://hdl.handle.net/10216/153247>.
- [34] Gabor Soos, Dániel Ficzer, Roberto Padovani, Attila Frankó, Sándor Veress, and Pal Varga. 5g networks for industrial applications: the ecosystem of npns, 12 2021.
- [35] Spectrum-Tracker.com. 5g frequency bands in portugal. Spectrum-Tracker.com, 08 2023. Available at <https://spectrum-tracker.com>.
- [36] Gordon Sutton, Jie Zeng, Ren Liu, Wei Ni, Diep Nguyen, Beeshanga Jayawickrama, Xiaojing Huang, Mehran Abolhasan, and Zhang Zhang. Enabling ultra-reliable and low-latency communications through unlicensed spectrum. *IEEE Network*, 32:70–77, 2018.
- [37] Gordon J. Sutton, Jie Zeng, Ren Ping Liu, Wei Ni, Diep N. Nguyen, Beeshanga A. Jayawickrama, Xiaojing Huang, Mehran Abolhasan, and Zhang Zhang. Enabling ultra-reliable and low-latency communications through unlicensed spectrum. *IEEE Network*, 32(2):70–77, 2018.
- [38] Yonghong Zeng, Yuhong Wang, Sumei Sun, and Kun Yang. Feasibility of urllc in unlicensed spectrum. In *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, 2019.
- [39] Rafik Zitouni. Software defined radio for cognitive wireless sensor networks: A reconfigurable ieee 802.15.4 standard. 07 2016.

Appendix A

Code Listings

A.1 Band Configuration Code

```
1 import pandas as pd
2
3 def freq_to_arfcn(frequency_mhz):
4     return (frequency_mhz - 3000) / 0.015 + 600000
5
6 def arfcn_to_freq(arfcn):
7     return 0.015 * (arfcn - 600000) + 3000
8
9 def calculate_ssb_arfcn(N):
10     frequency_mhz = 3000 + 1.44 * N
11     return freq_to_arfcn(frequency_mhz)
12
13 def is_valid_gscn(ssb, min_frequency, max_frequency):
14     frequency_mhz = arfcn_to_freq(ssb)
15     return min_frequency <= frequency_mhz <= max_frequency
16
17 def valid_combinations(channel_bw_rb, min_arfcn, max_arfcn, subcarrier_subspacing):
18     valid_combinations = []
19
20     for point_a in range(min_arfcn, max_arfcn + 1):
21         point_a_mhz = arfcn_to_freq(point_a)
22         center_frequency_mhz = point_a_mhz + (channel_bw_rb * 12 * 0.5 *
23             subcarrier_subspacing)
24         N = (center_frequency_mhz - 3000) / 1.44
25         if N.is_integer():
26             ssb_arfcn = freq_to_arfcn(center_frequency_mhz)
27             ssb_mhz = arfcn_to_freq(ssb_arfcn)
28             if (ssb_arfcn - point_a) % 24 == 0 and is_valid_gscn(ssb_arfcn,
29                 point_a_mhz, ssb_mhz):
30                 abs_diff_mhz = abs(ssb_mhz - point_a_mhz)
31                 abs_diff_arfcn = abs(ssb_arfcn - point_a)
```

```

30         valid_combinations.append((point_a, int(ssb_arfcn), point_a_mhz,
31                                     ssb_mhz, abs_diff_mhz, abs_diff_arfcn, center_frequency_mhz,
32                                     ssb_arfcn))
33
34     return valid_combinations
35
36 channel_bw_rb = 106 # Value for Channel Bandwidth in Resource Blocks
37 # Band 46 range
38 min_arfcn = 743333 # Min Frequency of band in ARFCN 5150 MHz
39 max_arfcn = 795000 # Max Frequency of band in ARFCN 5925 MHz
40 subcarrier_subspacing = 0.030
41
42 valid_combinations = valid_combinations(channel_bw_rb, min_arfcn, max_arfcn,
43                                         subcarrier_subspacing)
44
45 if valid_combinations:
46     df_valid_combinations = pd.DataFrame(valid_combinations, columns=[
47         'Point A (ARFCN)', 'SSB (ARFCN)', 'Point A (MHz)', 'SSB (MHz)',
48         'Absolute Difference (MHz)', 'Absolute Difference (ARFCN)',
49         'Central Channel Frequency (MHz)', 'Central Channel Frequency (ARFCN)'])
50     filename = f"bandConfiguration_BW{channel_bw_rb}_MinARFCN{min_arfcn}_MaxARFCN{
51                 max_arfcn}_SCS_{subcarrier_subspacing:.3f}.xlsx"
52     df_valid_combinations.to_excel(filename, index=False)
53     print(df_valid_combinations[['Point A (MHz)', 'SSB (MHz)', 'Central Channel
54                                 Frequency (MHz)']])
55 else:
56     print("No valid combinations found.")

```

Listing A.1: 5G Channel design in a given band.

A.2 Distributed Unit Configuration File for Unlicensed Band

```

1  (...)
2  # downlinkConfigCommon
3      absoluteFrequencySSB                = 783744; # 5854.08 MHz
4      dl_frequencyBand                    = 46;      # (5150-5925) MHz
5      dl_absoluteFrequencyPointA          = 782472; # 5835 MHz
6      dl_offstToCarrier                    = 0;
7      dl_subcarrierSpacing                = 1;
8      dl_carrierBandwidth                  = 106;
9      initialDLBWPlocationAndBandwidth    = 28875;
10     initialDLBWPsubcarrierSpacing        = 1;
11     initialDLBWPcontrolResourceSetZero   = 12;
12     initialDLBWPsearchSpaceZero          = 0;
13
14 # uplinkConfigCommon
15     ul_frequencyBand                      = 46;

```

```

16     ul_offstToCarrier                = 0;
17     ul_subcarrierSpacing             = 1;
18     ul_carrierBandwidth              = 106;
19     pMax                             = 20;
20     initialULBWPlocationAndBandwidth = 28875;
21     initialULBWPSubcarrierSpacing    = 1;
22     (...)
23
24 # tdd-UL-DL-ConfigurationCommon
25     referenceSubcarrierSpacing        = 1;
26
27     # TDD 2ms
28     # dl_UL_TransmissionPeriodicity    = 4; # Periodicity: 2ms
29     # nrofDownlinkSlots                = 2;
30     # nrofDownlinkSymbols              = 6;
31     # nrofUplinkSlots                  = 1;
32     # nrofUplinkSymbols                = 4;
33
34     # TDD 2.5ms
35     # dl_UL_TransmissionPeriodicity    = 5; # Periodicity: 2.5ms
36     # nrofDownlinkSlots                = 3;
37     # nrofDownlinkSymbols              = 6;
38     # nrofUplinkSlots                  = 1;
39     # nrofUplinkSymbols                = 4;
40
41     # TDD 5ms - Default OAI configuration
42     dl_UL_TransmissionPeriodicity      = 6; # Periodicity: 5ms
43     nrofDownlinkSlots                  = 6;
44     nrofDownlinkSymbols                = 6;
45     nrofUplinkSlots                    = 3;
46     nrofUplinkSymbols                  = 4;
47
48     # TDD 10ms
49     # dl_UL_TransmissionPeriodicity    = 7; # Periodicity: 10ms
50     # nrofDownlinkSlots                = 13;
51     # nrofDownlinkSymbols              = 8;
52     # nrofUplinkSlots                  = 6;
53     # nrofUplinkSymbols                = 2;
54 }
55 );
56 (...)

```

Listing A.2: Configuration DU file (du_gnb.conf) for band 46 and 47 in OAI.

A.3 Listen Before Talk Function

```

1  int update_channel_state(c16_t **rxp, int symbol_size, int slot_in_frame, int frame
    , int slot_type) {
2      int end_symbol = 14;
3      for (int sym = 1; sym < end_symbol; sym++) {
4          c16_t symbol_data[symbol_size];
5          memcpy(symbol_data, &rxp[0][sym * symbol_size], sizeof(c16_t) * symbol_size
              ); // Copy symbol data to a local array
6          double symbol_energy_dB = 0;
7          for (int i = 0; i < symbol_size; i++) {
8              int real = symbol_data[i].r;
9              int imag = symbol_data[i].i;
10             symbol_energy_dB += real * real + imag * imag;
11         }
12         symbol_energy_dB = 10 * log10(symbol_energy_dB + 1e-10);
13         if (symbol_energy_dB > 90) {
14             LOG_E(PHY, "CANCEL NEXT TRANSMISSION (energy > 90 dB): %.2f, Slot(%s):
                %d, Symbol: %d, Frame: %d\n", symbol_energy_dB, "UPLINK",
                slot_in_frame + 1, sym, frame);
15             return 1;
16         }
17     }
18     return 0;
19 }

```

Listing A.3: Listen Before Talk Mechanism - Function to assess channel energy and determine occupancy state based on uplink slot energy measurements.

A.4 Network measurements and experiments

A.4.1 Channel Energy Computation by Slot Type Function

```

1  int compute_and_store_channel_energy(c16_t **rxp, int symbol_size, int
    slot_in_frame, int frame, int slot_type){
2
3      const char *slot_type_str = (slot_type == NR_MIXED_SLOT) ? "Mixed" :
4                                  (slot_type == NR_UPLINK_SLOT) ? "Uplink" :
5                                  "Downlink";
6      const char* filename = "/home/du/filipe-peixoto-experiments/nrL1_UE_stats.txt";
7      FILE* output_file = fopen(filename, "a");
8      if (output_file == NULL) {
9          printf("ERROR OPENING\n");
10         return -1;
11     }
12     struct timespec ts;
13     clock_gettime(CLOCK_REALTIME, &ts);
14     long int initial_ns = ts.tv_nsec;

```

```

15     for (int sym = 0; sym < 13; sym++) {
16         long int current_ns = initial_ns + (long int) (35.714 * (sym - 1)); //
            35.714 ns is the time of each symbol
17         c16_t symbol_data[symbol_size];
18         memcpy(symbol_data, &rxp[0][sym * symbol_size], sizeof(c16_t) * symbol_size
            );
19         double symbol_energy_dB = 0;
20         for (int i = 0; i < symbol_size; i++) {
21             int real = symbol_data[i].r;
22             int imag = symbol_data[i].i;
23             symbol_energy_dB += real * real + imag * imag;
24         }
25         symbol_energy_dB = 10 * log10(symbol_energy_dB + 1e-10);
26         fprintf(output_file, "%02d%02d%02d.%09ldns: Slot(%s) %d, Symbol %d: %.2f dB
            \n",
27
                (int) (ts.tv_sec / 3600) % 24, (int) (ts.tv_sec / 60) %
                    60, (int) ts.tv_sec % 60, ts.tv_nsec, slot_type_str,
                    slot_in_frame, sym, symbol_energy_dB);
28     }
29     fclose(output_file);
30     return 0;
31 }

```

Listing A.4: Function to Compute and Save Channel Energy.

A.4.2 Channel Energy Computation by Slot Type with Interference Function

```

1 int compute_and_store_channel_energy_with_interference(c16_t **rxp, int symbol_size
    , int slot_in_frame, int absolute_slot, int slot_type) {
2     int end_symbol = 14;
3     const char *slot_type_str;
4     int local_channel_occupancy = 0;
5     if (channel_occupancy == 1) {
6         slot_type_str = "Interference";
7     } else {
8         slot_type_str = (slot_type == NR_MIXED_SLOT) ? "Mixed" :
9             (slot_type == NR_UPLINK_SLOT) ? "Uplink" :
10                "Downlink";
11     }
12     const char* filename = "/home/ue/filipe-peixoto-experiments/nrL1_UE_stats.txt";
13     FILE* output_file = fopen(filename, "a");
14     if (output_file == NULL) {
15         printf("ERROR OPENING FILE\n");
16         return -1;
17     }
18     struct timespec ts;
19     clock_gettime(CLOCK_REALTIME, &ts);

```

```

20     long int initial_ns = ts.tv_nsec;
21     for (int sym = 1; sym < end_symbol; sym++) {
22         long int current_ns = initial_ns + (long int)(35.714 * (sym - 1));
23         c16_t symbol_data[symbol_size];
24         memcpy(symbol_data, &rxp[0][sym * symbol_size], sizeof(c16_t) * symbol_size
                );
25         double symbol_energy_dB = 0;
26         for (int i = 0; i < symbol_size; i++) {
27             int real = symbol_data[i].r;
28             int imag = symbol_data[i].i;
29             symbol_energy_dB += real * real + imag * imag;
30         }
31         symbol_energy_dB = 10 * log10(symbol_energy_dB + 1e-10);
32         if (symbol_energy_dB > 95 && slot_type == NR_UPLINK_SLOT) {
33             if (strcmp(slot_type_str, "Interference") != 0) {
34                 LOG_E(PHY, "CANCEL NEXT TRANSMISSION (energy > 95 dB): %.2f,
                        Absolute_Slot: %d, Slot(%s): %d, Symbol: %d\n",
                        symbol_energy_dB, absolute_slot, slot_type_str, slot_in_frame
                        + 1, sym);
35             }
36             fprintf(output_file, "%02d%02d%02d.%09ldns: Slot(Interference) %d,
                        Absolute_Slot: %d, Symbol %d: %.2f dB\n",
37                     (int)(ts.tv_sec / 3600) % 24,           // Hours
38                     (int)(ts.tv_sec / 60) % 60,           // Minutes
39                     (int)ts.tv_sec % 60,                  // Seconds
40                     current_ns,                           // Nanoseconds
41                     slot_in_frame,                         // Slot in frame
42                     absolute_slot,                         // Absolute Slot
43                     sym,                                   // Symbol
44                     symbol_energy_dB);                    // Symbol energy in dB
45             local_channel_occupancy = 1; // Interference
46             slot_type_str = "Interference"; // if one symbol is occupied during
                        sensing phase, all the following are Interference too
47         } else {
48             fprintf(output_file, "%02d%02d%02d.%09ldns: Slot(%s) %d, Absolute_Slot:
                        %d, Symbol %d: %.2f dB\n",
49                     (int)(ts.tv_sec / 3600) % 24,
50                     (int)(ts.tv_sec / 60) % 60,
51                     (int)ts.tv_sec % 60,
52                     current_ns,
53                     slot_type_str,
54                     slot_in_frame,
55                     absolute_slot,
56                     sym,
57                     symbol_energy_dB);
58         }
59     }
60     fclose(output_file);
61     // Update state only on UL Slot

```

```

62     return slot_type != NR_UPLINK_SLOT ? channel_occupancy :
        local_channel_occupancy;
63 }

```

Listing A.5: Function to compute and save channel energy.

A.4.3 Channel Energy Analysis and Visualization by Slot Type Code

```

1  import matplotlib.pyplot as plt
2  import numpy as np
3  from scipy.stats import gaussian_kde
4
5  def plot_slot_histogram(filename, window_size=500, y_min=30, y_max=80):
6      slot_data = {i: [] for i in range(20)}
7      slot_colors = {}
8      color_map = {'Downlink': 'red', 'Uplink': 'green', 'Mixed': 'blue'}
9      try:
10         with open(filename, 'r') as file:
11             for line in file:
12                 if 'Slot(' in line:
13                     slot_type = line.split('Slot(')[1].split(' ')[0]
14                     parts = line.split(':')
15                     slot_info = parts[1].strip()
16                     slot_number = int(slot_info.split(',')[0].split()[-1])
17                     db_value = float(parts[2].split('dB')[0].strip())
18                     if 0 <= slot_number < 20:
19                         slot_data[slot_number].append(db_value)
20                         if slot_number not in slot_colors:
21                             slot_colors[slot_number] = color_map[slot_type]
22
23     except FileNotFoundError:
24         print(f"File not found: {filename}")
25         return
26     except Exception as e:
27         print(f"An error occurred: {str(e)}")
28         return
29
30     averages = []
31     for i in range(20):
32         values = slot_data[i]
33         if len(values) >= window_size:
34             avg = np.mean([np.mean(values[j:j+window_size]) for j in range(0, len(
35                 values), window_size)])
36         else:
37             avg = np.mean(values) if values else 0
38         averages.append(avg)

```

```

39     colors = [slot_colors.get(i, 'gray') for i in range(20)]
40
41     plt.figure(figsize=(10, 5))
42     bars = plt.bar(range(1, 21), averages, color=colors)
43     plt.title('Average Energy per Slot Number')
44     plt.xlabel('Slot Number')
45     plt.ylabel('Average Energy (dB)')
46     plt.ylim(y_min, y_max)
47     plt.xticks(range(1, 21))
48     plt.grid(False)
49     for bar, avg in zip(bars, averages):
50         plt.text(bar.get_x() + bar.get_width() / 2, bar.get_height(), f'{avg:.2f}',
51                 ha='center', va='bottom')
52     from matplotlib.patches import Patch
53     legend_elements = [
54         Patch(facecolor=color_map['Downlink'], label='Downlink'),
55         Patch(facecolor=color_map['Uplink'], label='Uplink'),
56         Patch(facecolor=color_map['Mixed'], label='Mixed')
57     ]
58     plt.legend(handles=legend_elements, title="Slot Types")
59     plt.show()
60
61 def parse_time(time_str):
62     hours = int(time_str[:2])
63     minutes = int(time_str[2:4])
64     seconds = int(time_str[4:6])
65     nanoseconds = float(time_str[6:-2])
66     total_seconds = hours * 3600 + minutes * 60 + seconds + nanoseconds
67     return total_seconds
68
69 def read_data(filename, slot_type):
70     times = []
71     values = []
72     initial_time = None
73     with open(filename, 'r') as file:
74         for line in file:
75             if f'Slot({slot_type})' in line:
76                 parts = line.split(':')
77                 timestamp_ns = parts[0].strip()
78                 db_value = float(parts[-1].split('dB')[0].strip())
79                 current_time = parse_time(timestamp_ns)
80                 if initial_time is None:
81                     initial_time = current_time
82                 relative_time_ms = (current_time - initial_time) * 1000
83                 times.append(relative_time_ms)
84                 values.append(db_value)
85     return times, values
86
87 def average_data(times, values, window_size=10):

```

```

87     avg_times = []
88     avg_values = []
89     for i in range(0, len(times), window_size):
90         avg_times.append(np.mean(times[i:i+window_size]))
91         avg_values.append(np.mean(values[i:i+window_size]))
92     return avg_times, avg_values
93
94 def plot_data(times, values, slot_type, n):
95     plt.figure(figsize=(10, 5))
96     color_map = {'Downlink': 'red', 'Uplink': 'green', 'Mixed': 'blue'}
97     downsampled_times = times[::n]
98     downsampled_values = values[::n]
99     data = np.vstack([downsampled_times, downsampled_values])
100    density = gaussian_kde(data, bw_method=0.5)(data) # Adjust the bandwidth as
        needed
101    sizes = (density / np.max(density)) * 100 # Scale sizes between 0 and 100
102    seconds = np.array(downsampled_times) / 1000
103    plt.scatter(seconds, downsampled_values, marker='o', c=color_map[slot_type], s=
        sizes, alpha=0.5)
104    plt.title(f'Average Energy Evolution in {slot_type} Slots Over Time with n={n}'
        )
105    plt.xlabel('Time (seconds from start)')
106    plt.ylabel('Average Energy (dB)')
107    plt.ylim(20, 110)
108    plt.grid(True)
109    plt.tight_layout()
110    plt.show()
111    print(f"Plot for {slot_type} with n={n} displayed.")
112
113 def plot_combined_data(slot_data, n):
114     plt.figure(figsize=(10, 5))
115     color_map = {'Downlink': 'red', 'Uplink': 'green', 'Mixed': 'blue'}
116     for slot_type in slot_data:
117         times, values = slot_data[slot_type]
118         downsampled_times = times[::n]
119         downsampled_values = values[::n]
120         data = np.vstack([downsampled_times, downsampled_values]) # Calculate
            density using KDE
121         density = gaussian_kde(data, bw_method=0.5)(data)
122         sizes = (density / np.max(density)) * 100
123         seconds = np.array(downsampled_times) / 1000
124         plt.scatter(seconds, downsampled_values, s=sizes, c=color_map[slot_type],
            label=slot_type, alpha=0.5)
125     plt.title('Combined Average Energy Evolution Over Time with n={}'.format(n))
126     plt.xlabel('Time (seconds from start)')
127     plt.ylabel('Average Energy (dB)')
128     plt.ylim(60, 110)
129     plt.legend()
130     plt.grid(True)

```

```

131     plt.tight_layout()
132     plt.show()
133
134 filename = 'samples.txt'
135 plot_slot_histogram(filename)
136
137 slot_data = {}
138 for slot_type in ['Downlink', 'Uplink', 'Mixed']:
139     times, values = read_data(filename, slot_type)
140     avg_times, avg_values = average_data(times, values)
141     slot_data[slot_type] = (avg_times, avg_values)
142 plot_combined_data(slot_data, 3)

```

Listing A.6: Plotting of the slot histogram and energy evolution.

A.4.4 5.85GHz Channel Increasing Interference Generator Code

```

1 import socket
2 import time
3 import logging
4 import math
5 def generate_udp_traffic(target_ip, port, max_frequency_hz, initial_frequency_hz
    =1.0, scale_factor=1.02, burst_duration_ms=3, total_duration=60):
6     packet_content = b'a' * 1024
7     sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
8     start_time = time.time()
9     current_time = start_time
10    frequency = initial_frequency_hz
11    while current_time - start_time < total_duration:
12        wait_time = 1.0 / frequency
13        burst_end_time = time.time() + (burst_duration_ms / 1000.0)
14        while time.time() < burst_end_time:
15            sock.sendto(packet_content, (target_ip, port))
16            time.sleep(max(0, wait_time - (burst_duration_ms / 1000.0)))
17            frequency = min(max_frequency_hz, frequency * scale_factor)
18            current_time = time.time()
19    sock.close()
20    logging.info("Traffic generation complete.")
21 if __name__ == "__main__":
22     logging.basicConfig(level=logging.INFO)
23     generate_udp_traffic('172.254.0.2', 5005, 100)

```

Listing A.7: Interference generator on 5.85GHz band traffic.

A.4.5 One-Way Average Delay Code

```

1 #!/bin/bash
2 if [ "$#" -ne 2 ]; then
3     echo "Usage: $0 <IP_ADDRESS> <INTERFACE>"
4     exit 1
5 fi
6 IP_ADDRESS=$1
7 INTERFACE=$2
8 ping -I $INTERFACE -c 100 $IP_ADDRESS | tee /tmp/ping_results.txt
9 average_rtt=$(grep "avg" /tmp/ping_results.txt | awk -F'/' '{print $5}')
10 average_owd=$(echo "$average_rtt / 2" | bc -l)
11 echo "Average one-way delay to $IP_ADDRESS on interface $INTERFACE: $average_owd ms"

```

Listing A.8: Average one-way delay time over 100 attempts.

A.4.6 5.85GHz Channel Interference Generator Code

```

1 #!/bin/bash
2 TARGET_IP="172.254.0.2"
3 PORT="5005"
4 BANDWIDTH_MBPS="100"
5 DURATION="60" # Duration in seconds
6 PACKET_SIZE=$((125000 * $BANDWIDTH_MBPS)) # Packet size calculation
7 echo "Generating UDP traffic to $TARGET_IP:$PORT with bandwidth ${BANDWIDTH_MBPS}
8     Mbps for $DURATION seconds."
9 start=$(date +%s)
10 end=$((start + DURATION))
11 while [ $(date +%s) -lt $end ]; do
12     echo -n "$(head -c 1024 < /dev/zero | tr '\0' 'a')" | socat - UDP-DATAGRAM:
13         $TARGET_IP:$PORT,sourceport=50000
14     sleep 1 # Rate control for 1-second intervals
15 done
16 echo "Traffic generation complete."

```

Listing A.9: Interference generator on 5.85GHz band traffic.

A.4.7 Average Block Error Rate x Frame Plot

```

1 import numpy as np
2 import matplotlib.pyplot as plt
3 import re
4
5 max_frequency = 30 # manually adapted
6 def custom_smooth(data, window_size):

```

```

7     smoothed_data = np.zeros_like(data)
8     for i in range(len(data)):
9         if i < window_size - 1:
10             smoothed_data[i] = np.mean(data[:i+1])
11         else:
12             smoothed_data[i] = np.mean(data[i-window_size+1:i+1])
13     return smoothed_data
14
15 def find_nearest_index(array, value):
16     array = np.asarray(array)
17     idx = (np.abs(array - value)).argmin()
18     return idx
19
20 def read_and_plot(file_path, num_samples=10):
21     with open(file_path, 'r') as file:
22         lines = file.readlines()
23
24     ul_bler = []
25     dl_bler = []
26
27     for line in lines:
28         dl_match = re.search(r'dlsch_rounds.*?MEAN BLER ([\d\.]+)', line)
29         ul_match = re.search(r'ulsch_rounds.*?MEAN BLER ([\d\.]+)', line)
30
31         if dl_match:
32             dl_bler.append(float(dl_match.group(1)))
33         if ul_match:
34             ul_bler.append(float(ul_match.group(1)))
35
36     window_size_dl = 5
37     window_size_ul = 10
38     dl_bler_smooth = custom_smooth(dl_bler, window_size_dl)
39     ul_bler_smooth = custom_smooth(ul_bler, window_size_ul)
40
41     x = np.arange(len(dl_bler)) * 120 # Multiply by 120 to convert index to frame
        number
42
43     interference_frequency = np.exp(np.log(max_frequency) * np.linspace(0, 1, len(
        dl_bler)))
44     idx_1hz = find_nearest_index(interference_frequency, 1) * 120
45     idx_2hz = find_nearest_index(interference_frequency, 2) * 120
46     idx_10hz = find_nearest_index(interference_frequency, 10) * 120
47
48     fig, ax1 = plt.subplots(figsize=(14, 6))
49     ax1.set_xlabel('Frame') # Updated label
50     ax1.set_ylabel('Mean BLER', color='tab:blue')
51     ax1.plot(x, dl_bler_smooth, label='BLER Evolution in PDSCH (Downlink)', color='
        blue')

```

```

52     ax1.plot(x, ul_bler_smooth, label='BLER Evolution in PUSCH (Uplink)', color='
        skyblue')
53     ax1.tick_params(axis='y', labelcolor='tab:blue')
54     ax1.legend(loc='upper left')
55
56     ax2 = ax1.twinx()
57     ax2.set_ylabel('Interference Frequency (Hz)', color='tab:red')
58     ax2.plot(x, interference_frequency, label='Interference Frequency', color='tab:
        red', linestyle='--')
59     ax2.axvline(x=idx_1hz, color='green', linestyle=':', label='1 Hz')
60     ax2.axvline(x=idx_2hz, color='purple', linestyle=':', label='2 Hz')
61     ax2.set_ylim(0, max_frequency)
62     ax2.set_yticks(np.arange(0, max_frequency+1, 10))
63     ax2.axvline(x=idx_10hz, color='orange', linestyle=':', label='10 Hz')
64     ax2.tick_params(axis='y', labelcolor='tab:red')
65     ax2.legend(loc='upper right')
66     plt.title('BLER and Interference Frequency over Entries')
67     plt.show()
68     print("Last", num_samples, "samples of DL BLER (smoothed):", dl_bler_smooth[-
        num_samples:])
69     print("Last", num_samples, "samples of UL BLER (smoothed):", ul_bler_smooth[-
        num_samples:])
70
71 file_path = 'samples_bler.txt'
72 read_and_plot(file_path, 10)

```

Listing A.10: BLER Evolution Plot Across Frames with Variable Interference Frequencies.