Universidad de Málaga

Escuela Técnica Superior de Ingeniería de Telecomunicación

Programa de Doctorado en Ingeniería de Telecomunicación

TESIS DOCTORAL POR COMPENDIO

Performance assessment of mobile networks in Industry 4.0

Autor:

David Segura Ramos

Directores:

Emil Jatib Khatib

Raquel Barco Moreno

2024

AUTOR: David Segura Ramos

https://orcid.org/0000-0002-6898-0418

EDITA: Publicaciones y Divulgación Científica. Universidad de Málaga

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD DE LA TESIS PRESENTADA PARA OBTENER EL TÍTULO DE DOCTOR

D. **David Segura Ramos**

Estudiante del programa de doctorado en **Ingeniería de Telecomunicación** de la Universidad de Málaga, autor de la tesis presentada para la obtención del título de doctor por la Universidad de Málaga, titulada: **Performance assessment of mobile networks in Industry 4.0**.

Realizada bajo la tutorización de **Raquel Barco Moreno** y dirección de **Emil Jatib Khatib** y **Raquel Barco Moreno**.

DECLARO QUE:

La tesis presentada es una obra original que no infringe los derechos de propiedad intelectual ni los derechos de propiedad industrial u otros, conforme al ordenamiento jurídico vigente (Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia), modificado por la Ley 2/2019, de 1 de marzo.

Igualmente asumo, ante a la Universidad de Málaga y ante cualquier otra instancia, la responsabilidad que pudiera derivarse en caso de plagio de contenidos en la tesis presentada, conforme al ordenamiento jurídico vigente.

En Málaga, a **8** de **Noviembre** de **2024**.

Fdo.: David Segura Ramos Doctorando	Fdo.: Raquel Barco Moreno Tutor de tesis
Fdo.: Emil Jatib Khatib y Raquel Barco Moreno Directores de tesis	

AUTORIZACIÓN PARA LA LECTURA DE LA TESIS

Por la presente, la Dra. Raquel Barco Moreno, y el Dr. Emil Jatib Khatib, profesores del Departamento de Ingeniería de Comunicaciones de la Universidad de Málaga,

CERTIFICAN

Que D. David Segura Ramos, ha realizado en el Departamento de Ingeniería de Comunicaciones de la Universidad de Málaga bajo su dirección, el trabajo de investigación correspondiente a su TESIS DOCTORAL titulada:

"**Performance assessment of mobile networks in Industry 4.0**"

En dicho trabajo, se han propuesto aportaciones originales para la evaluación y análisis del rendimiento de las redes de comunicaciones móviles e inalambricas en el escenario industrial. Los resultados de dicha tesis han dado lugar a las diversas publicaciones en revista, así como a aportaciones a congresos, superando el requisito de 1 punto ANECA del programa de doctorado regulado por el Real Decreto 99/2011.

Por todo ello, y dada la unidad temática de las distintas contribuciones y la metodología común seguida en todas ellas, los directores consideran que esta tesis es apta para su presentación al Tribunal que ha de evaluarla y AUTORIZA la presentación de la tesis por COMPENDIO DE PUBLICACIONES en la Universidad de Málaga. Igualmente, certifica que las publicaciones que avalan la tesis no han sido empleadas en trabajos anteriores a la misma.

Málaga, 8 de Noviembre de 2024

Fdo.: Raquel Barco Moreno

Fdo.: Emil Jatib Khatib

Universidad de Málaga
Escuela Técnica Superior de Ingeniería de Telecomunicación
Programa de doctorado en ingeniería de telecomunicación

Reunido el tribunal examinador en el día de la fecha, constituido por:

Presidente: Dr. D./Dña. _____

Secretario: Dr. D./Dña. _____

Vocal: Dr. D./Dña. _____

para juzgar la Tesis Doctoral titulada *Performance assessment of mobile networks in Industry 4.0* realizada por D. David Segura Ramos, y dirigida por los doctores D. Emil Jatib Khatib y Dña. Raquel Barco Moreno, acordó por

_____ otorgar la calificación de

_____ y para que conste,

se extiende firmada por los componentes del tribunal la presente diligencia.

Málaga, a ____ de _____ de _____.

El Presidente:

Fdo.:_____

El Secretario: El Vocal:

Fdo.:_____ Fdo.:_____

Hold the vision, trust the process.

Acknowledgments

First of all, I would like to express my most sincere gratitude to my supervisors, Raquel and Emil. Thank you Raquel for giving me the opportunity to join the MobileNet research group where I had the opportunity to learn a lot. Thank you Emil for the time and effort you dedicated to this thesis, for your valuable advice and for being my guide during its development.

Moreover, I would like to express my gratitude to my colleagues in lab 1.3.1. They made it possible to work in a more enjoyable way, and made me able to learn a lot from them to be a better research. A special mention to Hao and Carlos Baena for their always willingness to help with questions that arose throughout the thesis. Also, to my colleagues Antonio, José Antonio and Sebastián, who joined me into the adventure of the research stay and we made a lot of travels together.

I would like to extend my gratitude to people at Aalborg University with whom I had the opportunity to collaborate during my research stay, Preben, Sebastian, Melisa, and Akif. Thank you all for making me feel integrated and welcome. I would like to make a special mention to Sebastian, for all his work, help and dedication involved during the research stay.

A special mention among these lines is for my family. Thanks to my parents, brother and sister for their unconditional support and for always believe in me. Finally, I would like to thank Ana for being my greatest support during these years, for your patience and for always making me laugh.

This thesis has been partially funded by the following projects:

- EDEL4.0: Seguridad y fiabilidad en las comunicaciones 5G/IoT para la Industria 4.0. Número de proyecto UMA18-FEDERJA-172, receiving funds from Junta de Andalucia and European Comission, within the framework of "Proyectos de I+D+i en el marco del Programa Operativo FEDER Andalucia 2014-2020".
- PENTA: Provisión de servicios PPDR a través de Nuevas Tecnologías de Acceso radio. Número de proyecto PY18-4647, receiving funds from Junta de Andalucía and European Comission, within the framework of "Plan Andaluz de Investigación, Desarrollo e Innovación (PAIDI 2020)".
- MAORI: Massive AI for the OpenRadIo b5G/6G network. Project number TSI-063000-2021-72, receiving funds from Ministerio de Asuntos Económicos y Transformación Digital and European Union - NextGenerationEU within the framework "Recuperación, Transformación, y Resiliencia".

Contents

Abstract

The world is currently undergoing a profound digital transformation across various socio-economic sectors, a shift often referred to as the *digital revolution*. In the context of the industrial sector, the advent of the fourth industrial revolution, commonly known as *Industry 4.0*, is transforming factories into smart factories. This revolution refers to the current trend of automation and integration of data exchange mechanisms in manufacturing processes, thereby making production and distribution processes more flexible, robust and efficient. To achieve this goal, Industry 4.0 relies on different enabler technologies such as the the integration of Cyber-Physical Systems (CPS), the use of the Internet of Things (IoT), cloud computing, Artificial Intelligence (AI), robotics, and Big Data analytics.

With the integration of these enabler technologies in the factory, new applications and use cases emerge to provide mobility and flexibility such as rearrangeable modules in production lines, Automated Guided Vehicles (AGVs), autonomous robots or connected worker solutions. These applications and use cases pose new challenges for their correct operation, such as requirements of low latency communications, high reliability, and high throughput. To adapt to the challenges launched by the new services and use cases contemplated in a smart factory, the Fifth Generation (5G) of mobile networks is emerging as an enabling technology for this transformation. This thesis addresses the integration of the 5G cellular network into the industrial scenario, by assessing and improving network performance for different Industry 4.0 use cases involved in a smart factory. In particular, this thesis has been divided into three parts where different techniques and optimizations of the 5G network are addressed.

The first part is focused on the assessment of the network performance for critical services. These services such as the communication of the AGVs impose requirements of low latency and high reliability in the network. In this part, the focus is set on the assessment of the latency. On the

one hand, a study of the numerologies introduced in 5G is performed in terms of latency. In addition, an empirical assessment and comparison of the scalability of the network with different technologies in an industrial environment is carried out.

The second part focuses on the development of optimization algorithms of the network. First, a dynamic algorithm for the activation of Packet Duplication (PD) when using Dual Connectivity (DC) is proposed. This algorithm is centered on the increase of the reliability for critical services while minimizing the waste of radio resources. Secondly, the Quality of Service (QoS) performance with different configurations of Network Slicing (NS) for the different traffic profiles involved within a distribution center is studied.

The third part of this thesis focuses on the evaluation of Cellular Internet of Things (CIoT) devices in the 5G network. In particular, the performance of the different optimizations proposed in the standard to reduce the signaling overhead in the data transmission of CIoT devices has been evaluated. In addition, an in-depth analysis of the security of the Early Data Transmission (EDT) optimization is provided, analysing its main vulnerabilities and providing a set of recommendations for manufacturers and researchers.

Resumen

El mundo está experimentando actualmente una profunda transformación digital en diversos sectores socioeconómicos, un cambio que a menudo se denomina revolución digital. En el contexto del sector industrial, la llegada de la cuarta revolución industrial, comúnmente conocida como Industria 4.0, está transformando las fábricas en fábricas inteligentes. Esta revolución se refiere a la tendencia actual de automatización e integración de mecanismos de intercambio de datos en los procesos de fabricación, haciendo así más flexibles, robustos y eficientes los procesos de producción y distribución. Para lograr este objetivo, la Industria 4.0 se apoya en diferentes tecnologías facilitadoras como la integración de sistemas ciberfísicos (*Cyber-Physical Systems*, CPS), el uso del internet de las cosas (*Internet of Things*, IoT), la computación en la nube, la Inteligencia Artificial (IA), la robótica y el análisis de Big Data.

Con la integración de estas tecnologías facilitadoras en la fábrica, surgen nuevas aplicaciones y casos de uso que aportan movilidad y flexibilidad, como módulos reorganizables en las líneas de producción, vehículos guiados automatizados (*Automated Guided Vehicles*, AGVs), robots autónomos o soluciones para trabajadores conectados. Estas aplicaciones y casos de uso plantean nuevos retos para su correcto funcionamiento, como los requisitos de comunicaciones de baja latencia, alta fiabilidad y alto rendimiento. Para adaptarse a los retos lanzados por los nuevos servicios y casos de uso contemplados en una fábrica inteligente, la quinta generación (5G) de redes móviles se perfila como una tecnología habilitadora de esta transformación.

Esta tesis aborda la integración de la red celular 5G en el escenario industrial, mediante la evaluación y mejora del rendimiento de la red para diferentes casos de uso de Industria 4.0 implicados en una fábrica inteligente. En concreto, esta tesis se ha dividido en tres partes donde se abordan diferentes técnicas y optimizaciones de la red 5G.

La primera parte se centra en la evaluación del rendimiento de la red para

servicios críticos. Estos servicios, como la comunicación de los AGV, requieren requisitos de baja latencia y alta fiabilidad en la red. En esta parte, la atención se centra en la evaluación de la latencia. Por un lado, se realiza un estudio de las numerologías introducidas en 5G en términos de latencia. Por otro lado, se realiza una evaluación empírica y una comparación de la escalabilidad de la red con diferentes tecnologías en un entorno industrial.

La segunda parte se centra en el desarrollo de algoritmos de optimización de la red. En primer lugar, se propone un algoritmo dinámico para la activación de la duplicación de paquetes (*Packet Duplication*, PD) cuando se utiliza la conectividad dual (*Dual Connectivity*, DC). Este algoritmo se centra en el aumento de la fiabilidad para los servicios críticos, minimizando al mismo tiempo el desperdicio de recursos radio. En segundo lugar, se estudia la calidad de servicio (*Quality of Service*, QoS) con diferentes configuraciones de *Network Slicing* (NS) para los diferentes perfiles de tráfico involucrados dentro de un centro de distribución.

La tercera parte de esta tesis se centra en la evaluación de los dispositivos IoT celulares (*Cellular IoT*, CIoT) en la red 5G. En particular, se ha evaluado el rendimiento de las diferentes optimizaciones propuestas en el estándar para reducir la sobrecarga de señalización en la transmisión de datos de los dispositivos CIoT. Además, se ofrece un análisis en profundidad de la seguridad de la optimización de la transmisión temprana de datos (*Early Data Transmission*, EDT), analizando sus principales vulnerabilidades y proporcionando un conjunto de recomendaciones para fabricantes e investigadores.

Acronyms

3GPP	Third Generation Partnership Project
5G	Fifth Generation of mobile networks
5GC	5G Core
5GS	5G System
AF	Application Function
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
AMR	Autonomous Mobile Robot
AR	Augmented Reality
ARQ	Automatic Repeat reQuest
AS	Access Stratum
APN	Access Point Name
ARPF	Authentication credential Repository and Processing Function
AUSF	Authentication Server Function
BPSK	$\pi/2$-Binary Phase Shift Keying
BWP	Bandwidth Part

CA	Carrier Aggregation
CC	Component Carrier
CE	Coverage Enhancement
CIoT	Cellular Internet of Things
CN	Core Network
CP	Control Plane
CPS	Cyber-Physical Systems
CU	Central Unit
DC	Dual Connectivity
DFT-s-OFDM	Discrete Fourier Transform-spread-OFDM
DoS	Denial/Degradation of Service
DRB	Data Radio Bearer
DRX	Discontinuous Reception
DU	Distributed Unit
DY	Dolev-Yao
E2E	End-to-End
eDRX	Extended Discontinuous Reception
EDT	Early Data Transmission
eMBB	Enhanced Mobile Broadband
en-gNB	Evolved-Next Generation NodeB
eNB	Evolved Node B
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EPC	Evolved Packet Core
EPS	Evolved Packet System

FL	Federated Learning
FR	Frequency Range
FTP	File Transfer Protocol
gNB	Next-generation NodeB
HARQ	Hybrid Automatic Repeat reQuest
HSS	Home Subscriber Server
InF	Indoor Factory
InF-DH	InF with Dense clutter and High base station height
InF-DL	InF with Dense clutter and Low base station height
InF-SH	InF with Sparse clutter and High base station height
InF-SL	InF with Sparse clutter and Low base station height
IoT	Internet of Things
IP	Internet Protocol
ITU	International Telecommunication Union
LOS	Line-of-Sight
LPWA	Low-Power Wide-Area
LTE	Long Term Evolution
LTE-M	LTE for Machine Type Communications
MAC	Medium Access Control
MitM	Man-in-the-middle
MCG	Master Cell Group
MCL	Maximum Coupling Loss
ME	Mobile Equipment
MEC	Mobile Edge Computing

MeNB	Master eNB
MIMO	Multiple-Input Multiple-Output
ML	Machine Learning
MME	Mobility Management Entity
mMTC	Massive Machine Type Communications
MN	Master Node
multi-RAT	Multi-Radio Access Technology
MR-DC	Multi-Radio Dual Connectivity
MTC	Machine Type Communications
NAS	Non-Access Stratum
NB-IoT	NarrowBand Internet of Things
NF	Network Function
NFV	Network Function Virtualization
ng-eNB	Next-generation eNB
NG-RAN	Next Generation Radio Access Network
NLOS	Non-Line-of-Sight
NR	New Radio
NS	Network Slicing
NSA	Non-Stand Alone
NSSF	Network Slice Selection Function
NSSAAF	Network Slice-specific and Authentication and Authorization Function
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access

P-GW	Packet Data Network Gateway
PAPR	Peak-to-Average Power Ratio
PCC	Primary Component Carrier
PCell	Primary Cell
PCF	Policy Control Function
PD	Packet Duplication
PDCCH	Physical Downlink Control Channel
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDU	Packet Data Unit
PHY	Physical
PRB	Physical Resource Block
PSM	Power Saving Mode
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RA	Random Access
RAI	Release Assistance Indication
RAN	Radio Access Network
RAR	Random Access Response
RAT	Radio Access Tecnology
RE	Resource Element
RedCap	Reduced Capability
RF	Random Forest

RLC	Radio Link Control
RRC	Radio Resource Control
RSRP	Reference Signal Received Power
S-GW	Serving Gateway
SA	Stand Alone
SBA	Service-Based Architecture
SC-FDMA	Single Carrier Frequency Division Multiple Access
SCC	Secondary Component Carrier
SCell	Secondary Cell
SCG	Secondary Cell Group
SCS	Subcarrier Spacing
SDAP	Service Data Adaptation Protocol
SDN	Software Defined Network
SDR	Software Defined Radio
SEAF	SEcurity Anchor Function
SeNB	Secondary eNB
SINR	Signal to Interference plus Noise Ratio
SMC	Security Mode Command
SMF	Session Management Function
SN	Secondary Node
SR	Service Request
SRB	Signaling Radio Bearer
TB	Transport Block
TBS	Transport Block Size

TDD	Time Division Duplex
TDMA	Time Division Multiple Access
TSN	Time Sensitive Network
TTI	Transmission Time Interval
UDM	Unified Data Management
UDP	User Datagram Protocol
UE	User Equipment
UP	User Plane
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communications
USIM	Universal Subscriber Identity Module
UWB	Ultra-Wide Band
VoIP	Voice over Internet Protocol
VoLTE	Voice over LTE
WISA	Wireless Interface to Sensors and Actuators

Part I

Background

Chapter 1

Introduction

This chapter provides an introduction to the work carried out during this thesis. First, Section 1.1 provides the motivation of this thesis, describing the fourth industrial revolution and indicating how cellular networks can be applied in this context. Next, the challenges identified and the objectives pursued in this thesis are outlined in Section 1.2. Finally, the structure of the document is described in Section 1.3.

1.1 Motivation

The advent of the fourth industrial revolution or Industry 4.0 [1] marks a transformative shift in manufacturing and the industrial sector. The term Industry 4.0 was used for the first time in 2011 in the assignment that the German government made to the Industry-Science Research Alliance for the consolidation of the leadership of the German Industry [2]. This initiative was subsequently extended to the rest of the European Union, and today, Industry 4.0 refers to the interconnection of machines and systems within production centers, as well as between them and the outside world. This digital revolution is transforming factories into smart factories, where digitization is key. In a connected factory, sensors, cloud storage and real-time data analysis are used to optimize production processes. Central to this revolution is the need for a robust, efficient, and improved flexibility of production and distribution processes. To achieve these needs, there are different enabler technologies that are in the core of Industry 4.0 (see Figure 1.1):

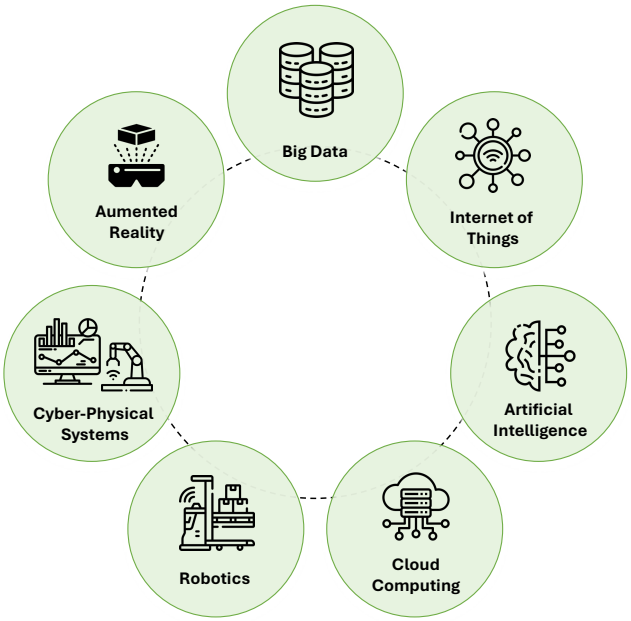


Figure 1.1: Industry 4.0 enabler technologies.

- Cyber-Physical Systems (CPS) [3, 4]. They integrate computing and network capacity into a physical process. CPS technologies enable the development of smart factories, where machinery and equipment are interconnected, allowing for real-time monitoring, control, and optimization.

- Internet of Things (IoT) [5]. IoT is a network of physical objects that have been embedded with sensors, software, and other technologies to enable them to connect and exchange data. In Industry 4.0, IoT facilitates the seamless flow of information across production lines, enhancing operational visibility and decision-making.

- Artificial Intelligence (AI) [6]. AI algorithms analyze vast amounts of data generated by CPS and IoT devices. This technology enables predictive maintenance, quality control, and adaptive manufacturing processes, reducing downtime and improving product quality.

- Cloud Computing [7]. Cloud computing plays a significant role in Industry 4.0 by providing the infrastructure and platform for storing, processing, and analyzing the large amounts of data generated by IoT devices and other sensors in the manufacturing process. In addition, cloud computing can provide the computing power needed to run AI algorithms.

- Augmented Reality (AR) [8]. The application of AR technology has the potential to enhance a range of processes, including training, maintenance, and design. By overlaying digital information onto the physical world, AR technology can provide workers with real-time data and instructions, thereby facilitating more efficient and effective workflows.

- Robotics [9, 10]. Robots and automation systems in Industry 4.0 are more intelligent, flexible, and collaborative. These systems can perform complex tasks alongside human workers, enhancing productivity and safety in manufacturing environments.

- Big Data analytics [11, 12]. The collection and analysis of large datasets allow for better forecasting, efficiency improvements, and the discovery of new insights. Data-driven decision-making is at the core of Industry 4.0, driving more responsive and agile manufacturing practices.

Although the Industry 4.0 concept is focused on manufacturing, the aforementioned technologies and principles are also applied across different industry sectors such as logistics, healthcare, agriculture or energy.

Traditional industrial networks are mainly based on wired connections and legacy wireless technologies. Some of the wired connections that have been used are ProfiNET [13], EtherCAT [14] and the set of Time Sensitive Networks (TSNs) protocols [15]. In the field of wireless technologies, the main technologies used are those based on the IEEE 802.11 family, commonly named Wi-Fi, but also customized solutions for factories based on IEEE 802.15.1 and 802.15.4, such as Wireless Interface to Sensors and Actuators (WISA) and WirelessHART [16]. Nevertheless, these networks often fall short in terms of scalability, flexibility, and real-time responsiveness required by modern industrial applications [17]. The dynamic nature of smart factories, autonomous systems, and complex supply chains needs a communication infrastructure that can seamlessly support a vast number of connected devices, facilitate real-time data exchange, and ensure high levels of security and reliability.

Cellular networks, with their widespread adoption, proven reliability, and continuous evolution, are uniquely positioned to address these needs, offering a foundational technology to propel Industry 4.0 forward. Cellular networks, particularly with the advent of the Fifth Generation of mobile networks (5G) and upcoming 6G technologies [18], offer unprecedented capabilities that align perfectly with the demands of

Industry 4.0. These include the support of use cases related to critical communications, that are known as Ultra-Reliable Low Latency Communications (URLLC), the massive use of machine-type devices, also known as Massive Machine Type Communications (mMTC), and Enhanced Mobile Broadband (eMBB). The ability to provide deterministic communication, support for a massive number of IoT devices, and high data throughput are critical enablers for applications such as predictive maintenance, remote monitoring, and autonomous robotics. Furthermore, the modular and scalable nature of cellular networks allows for tailored deployments in diverse industrial environments, from large-scale manufacturing plants to remote and isolated facilities. This flexibility supports the creation of private networks [19] dedicated to specific industrial needs, ensuring that the unique requirements of different sectors are met effectively.

The global push towards sustainability and efficiency in industrial operations [20] further underscores the importance of leveraging advanced communication networks. By enabling more efficient resource management, reducing downtime through predictive maintenance, and facilitating the seamless integration of renewable energy sources, cellular networks [21] contribute significantly to the sustainability goals of modern industries.

As the adoption and implementation of the cellular technology is progressively taking place in factories, especially the 5G technology [22], it is necessary to study its applicability, evaluating the network performance through the different services and use cases that are involved in a smart factory.

1.2 Challenges and objectives

The main objective of this thesis is to asses and improve cellular network performance in an indoor industrial environment. For this purpose, different techniques and optimizations to the network are addressed in this thesis. First, tasks related to the study of the latency performance of critical services and the scalability in the network are carried out. Secondly, different tools have been developed to assess network performance in an industrial environment and to improve the reliability of critical services through the use of the multi-connectivity solution. Thirdly, optimizations algorithms are developed and evaluated with the following purposes: to improve the reliability of critical services without resource wastage, and to enhance the Quality of Service (QoS) of the different traffic profiles involved in a factory. Finally, the performance of the different optimizations proposed by the Third Generation Partnership Project (3GPP)

for Cellular Internet of Things (CIoT) devices has been evaluated, also including a security analysis of the latest optimization.

In an indoor industrial scenario, there are many challenges present due to the characteristics of this particular scenario. First, in a factory, a harsh environment is present for radio propagation due to the presence of large metallic machines within crowded spaces [23]. This causes reflections and multi-path in the signal, making difficult the appropriate adjustment of the configuration in the network according to radio conditions. Another challenge regarding to the scenario that is also present is that the distribution can change from one day to another (i.e., moving and placing stock from one side of the factory to another), so network conditions and performance could vary. This is specially important for adjusting the appropriate configuration in the network to maximize the QoS of the different services and to fulfil service requirements.

As new use cases are introduced in the smart factory to enhance the flexibility, such as the mobility within the factory by using an Automated Guided Vehicle (AGV), it also introduces more demanding requirements in the network for the correct operation of these applications. In particular, the AGVs are vehicles that follow programmed paths to transport material and goods within the factory facility [24]. The AGVs communicate with a guidance control system from which they receive guidance commands. For the correct operation of the AGVs, the communication with the guidance control system needs to be in real-time with low latency and high reliability to avoid malfunctions or accidents in the factory. Therefore, these communications are considered as critical. In 5G, there are different approaches followed in the literature to reduce the latency of the communications in the Radio Access Network (RAN). The approaches encompass the use of mini-slots [25, 26], solutions in the scheduler [27–30], uplink grant free transmissions [31–34], and the use of a flexible numerology [35–38]. The numerology approach has been one of the mainly used techniques, with the use of a higher numerology to successfully reduce the latency for critical services. Despite the importance of this approach, the latency evaluation of the numerology in the literature only considers Line-of-Sight (LOS) conditions, and there are no studies that include the assessment in the industrial scenario. Given that Non-Line-of-Sight (NLOS) conditions are the most prevalent in a factory, it is necessary to conduct an assessment to study the numerology impact and identify the optimal configuration for critical services. Therefore, the first objective (Obj. 1) of this thesis consists in studying and assessing the impact of the different 5G numerologies on the latency experienced by an AGV in an indoor factory scenario under LOS and NLOS conditions.

Another aspect that must be taken into account in a smart factory is the network scalability. As many devices are connected in a smart factory and high traffic is coming from machinery, sensors, AGVs, etc., it may overload the network or decrease the performance, thereby not achieving the requirements of the different applications. In the case of critical services, this becomes even more important, as a low latency must be ensured despite an increase in the number of devices to maintain productivity and prevent accidents. Moreover, the technology selection in the factory is not clear for industrial manufacturers. Some will prefer low cost-technologies with lower performance, and others will prefer a very reliable network although this implies a higher cost. Different assessments of the network performance in an industrial scenario have been carried out in the literature with different technologies such as Long Term Evolution (LTE), 5G, Wi-Fi, and the use of Multi-Radio Access Technology (multi-RAT) connectivity [39–47]. However, the existing literature does not take into account the scalability of the network, with only one device attached to the network in the majority of the works. Therefore, following with this line, the second objective (Obj. 2) of this thesis is to assess and compare the scalability of the network with different technologies in an industrial environment. In this way, the study should provide a clear vision of which technology suits better the manufacturing sector.

Following the line started with Obj. 1, the critical services involved in the smart factory also have requirements of high reliability in the communication in addition to a low latency. In the 5G network, the use of multi-connectivity is proposed to enhance the reliability of critical communications. Multi-connectivity consists in establishing two or more links between a user and two or more radio access nodes, which are typically uncorrelated links. For instance, the two links can use different channels, different networks or even different network access technologies, namely multi-RAT [48]. Multi-connectivity is often adopted for improving communication aspects such as latency, reliability and throughput [49,50]. In the case of reliability, the most extended solution is the Packet Duplication (PD) approach [51,52]. This solution allows the transmission of the same data duplicated from different links. However, this solution comes at a cost in terms of network redundancy, as the duplication can lead to an inefficient use of network resources, resulting in a degradation of the overall network performance [53]. Thus, the third objective (Obj. 3) of this thesis consists in the enhancement of the reliability for critical communications, designing and developing a dynamic algorithm to control the activation of PD to avoid resource wastage in the network.

One of the industrial sectors where Industry 4.0 is adopted is smart logistics to add

flexibility and easily adapt to changes both at large and small volumes of moving stock. In smart logistics, distribution centers [54] play the role of nodes in the distribution network, where small batches of products (or even individual units) are received, stored for very short periods of time (days or hours), and redirected to the next distribution center. Within a distribution center, different traffic profiles with diverse requirements are present (i.e., workers with AR glasses, smart tags, and AGVs moving stock), which makes it challenging, as network resources need to be shared between these profiles and each traffic profile requires different network parameters such as the numerology. The application of the 5G network in smart logistics has been discussed in the literature in [55–59]. On the other hand, several works have been centered in optimizing the 5G network specifically for smart logistics, analyzing the specific particularities of the applications and the different environments where the processes take place [60–65]. One solution followed in the literature to tackle this challenge is the use of Network Slicing (NS), which allows the creation of subsets of the network for each traffic profile, with optimized configurations [66–68]. Despite that, the performance of the 5G network has not been assessed yet in a distribution center. Therefore, the fourth objective (Obj. 4) of this thesis is to evaluate the 5G network performance in a distribution center in terms of QoS for the different traffic profiles involved there.

CIoT devices are characterized by the transmission of small data to update information provided by sensors in the factory such as the temperature, the humidity, the state of a machine, an alarm, etc. These transmissions are characterized by a large transmission interval (i.e., one transmission per hour), and on each transmission a high signaling overhead is produced compared to the size of the data sent. Furthermore, the power constraints inherent to CIoT devices, which rely on batteries, underscore the importance of optimizing data transmission to save energy. To tackle with this challenge, many optimizations have been proposed in the standard by the 3GPP with two main objectives: to increase the battery life and to reduce the signaling overhead when transmitting data. These optimizations were first proposed in Release 13, namely Control Plane (CP) and User Plane (UP) CIoT optimizations; and a new optimization was introduced in Release 15 for infrequent and small data transmissions, namely Early Data Transmission (EDT). The enhancements to these optimizations in terms of battery life and the latency have been the subject of analysis in the literature, as evidenced by works such as [69–73]. Nevertheless, none of these employ the use of commercial equipment; rather, they employ analytical frameworks or simulators. Additionally, they operate under the assumption of different ideal scenarios, which do not

align with the actual implementation of the 3GPP standard. Thus, the fifth objective (Obj. 5) of this thesis consists in studying the latency impact of CIoT signaling optimizations in the network with commercial equipment.

Lastly, in relation with Obj. 5, much effort has been made in optimizing the transmissions of CIoT devices, however, it is of particular importance to also analyse the threats and vulnerabilities, and to ensure the security of these optimizations. As the security of the EDT optimization has not been studied in the state of the art, the sixth objective (Obj. 6) of this thesis consists in analyzing the security of the EDT optimization in the 5G network. In this way, the EDT optimization should be described in detail in its operation modes and the main vulnerabilities associated to this optimization must be analyzed.

In summary, the objectives that address the previous challenges are the following (see Figure 1.2):

Obj. 1. To study the impact of 5G numerologies on the latency for critical services.

The objective of this study is to analyse the behaviour of the different numerology configurations on the latency perceived by the users under different channel conditions and packet sizes. In this way, this study aims to lay the foundations for future optimizations to reduce the latency, as the appropriate numerology can be selected according to the radio conditions experienced.

Obj. 2. To assess and compare network scalability with different technologies in an industrial environment.

The aim of this objective is to empirically assess and compare the network performance in terms of latency and packet loss with different technologies in an indoor industrial scenario. In particular, the assessment should take into account different packet sizes and scenarios with varying number of devices transmitting data. As a result, this study should provide a clear vision of which technology suits better the manufacturing sector.

Obj. 3. To propose a mechanism to enhance reliability for critical services.

This objective refers to the design and development of an algorithm to fulfil reliability requirements for critical services. Thus, the proposed algorithm should be able to dynamically adapt and control the activation of PD to avoid resource wastage in the network.

Obj. 4. To evaluate the network performance in a distribution center.
The aim of this objective is to perform an assessment of the 5G network in a distribution center scenario, taking into account the different traffic profiles involved in this scenario. In particular, this work should compare the QoS of these traffic profiles under different logistics activities with different NS approaches.

Obj. 5. To study the impact of CIoT signaling optimizations in the network.
The objective of this study is to analyse the behaviour of the different CIoT signaling optimizations on the latency perceived by the user when transmitting infrequent small data into the network.

Obj. 6. To analyze the security of 5G EDT optimization for CIoT.
This objective is related to Obj. 5 and refers to an in-depth analysis of the security of the EDT optimization, describing in detail its operation modes and analyzing the main vulnerabilities associated to this optimization. As a result, a set of recommendations for vendors should be derived from the security analysis.

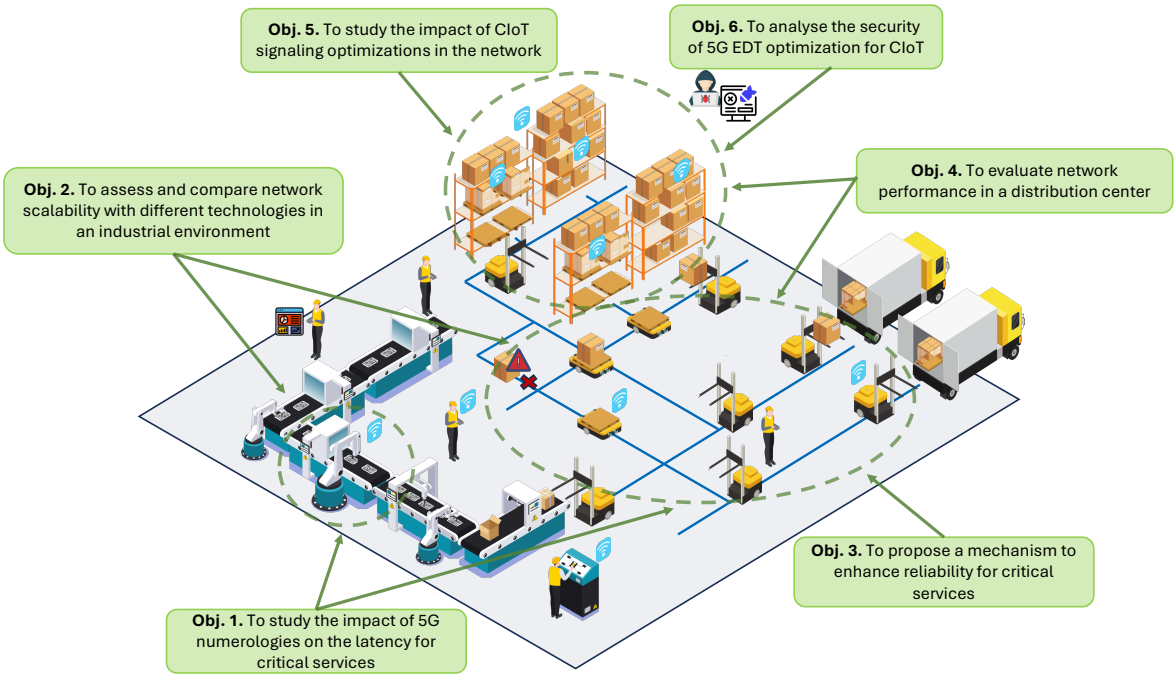


Figure 1.2: Conceptual scheme of the objectives addressed.

1.3 Document structure

This document has been structured in seven chapters grouped into three blocks for an easier understanding, as shown in Figure 1.3. The first block contains the background and knowledge required to understand the rest of the thesis and it is composed of two chapters. Chapter 1 consists in an introduction to the thesis, detailing the motivation that led to the research conducted and setting out the objectives to be addressed. Chapter 2 provides the technical background necessary to understand the content of the thesis. In this chapter, first the cellular technologies involved in this thesis are described: LTE, 5G and CIoT. In particular, their main characteristics and features are described for each of these technologies. Next, an overview of multi-connectivity in 5G is provided, presenting the different architectures and the benefits and challenges of this feature. Finally, this chapter ends with a description of the 5G network security, in particular, it is focused on the security architecture and procedures, along with the threat model and main attacks.

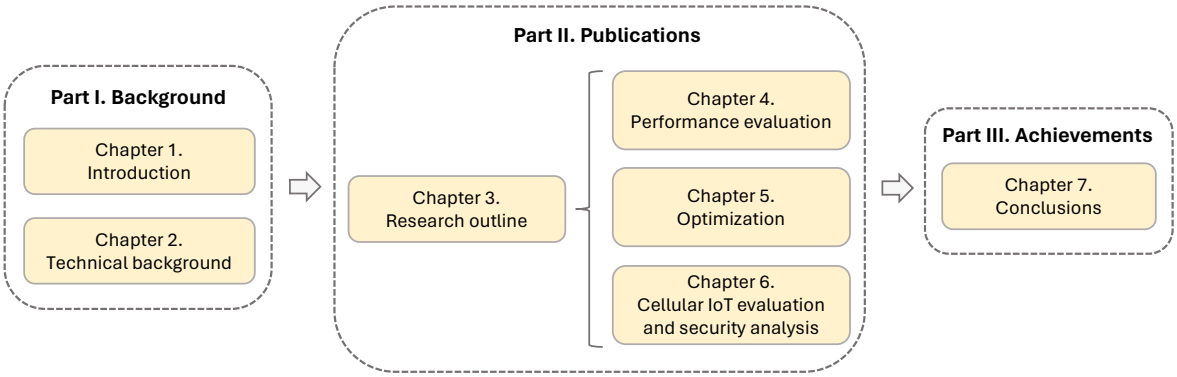


Figure 1.3: Document structure.

The second block corresponds to the publications that support this thesis. This block has been divided into different chapters according to their topic. This block includes a first chapter (Chapter 3) in which the research outline is presented. In particular, this chapter details the relationship between the publications and the challenges, objectives and chapters of this thesis. The research methodology followed in the development of this thesis is also presented in this chapter. The rest of the chapters included in this second block correspond to the publications that are directly related to the objectives established in Section 1.2.

Chapter 4 contains the results related to the performance of the cellular network and is associated with Obj. 1 and 2 of this thesis, including two publications. Specifically,

the first publication addresses the latency evaluation of the new numerologies introduced in 5G under different channel conditions. The second one provides an empirical comparison of the scalability performance of 5G, Wi-Fi 6, and multi-connectivity in terms of latency and packet loss. For that, measurement campaigns were performed in an indoor industrial scenario with commercial equipment.

Chapter 5 covers the work related to the development of algorithms that aims to improve the performance in the network. This chapter is related to Obj. 3 and 4 of this thesis and includes two publications. The first publication proposes a dynamic packet duplication algorithm in multi-connectivity scenarios for latency-constraint services in order to improve the reliability and reduce the resource consumption. In particular, the solution proposed is based on Machine Learning (ML), and a latency predictor is trained and evaluated. The second one introduces a novel open-source simulator with a realistic representation of a distribution center scenario. In particular, the floorplan, activities and applications have been developed and the 5G network performance is evaluated by comparing two NS strategies (static and dynamic). This comparison have been performed for all traffic profiles involved in a distribution center (eMBB, URLLC and mMTC).

Chapter 6 is related to the evaluation and the security analysis of CIoT in the context of 5G. This chapter is associated with Obj. 5 and 6 of this thesis and includes two publications. Specifically, the first publication evaluates and compares the different transmissions modes for CIoT, such as Release 13 optimization and EDT with commercial equipment. The evaluation takes into account different coverage levels and packet sizes and focuses on the latency performance. The second one describes in detail the EDT feature for CIoT devices and analyzes its main vulnerabilities with a set of recommendations.

Finally, the third block consists of Chapter 7, which provides an overview of the main results and conclusions of this thesis and the future lines of research are discussed.

This document also includes two appendices. Appendix A describes the evaluation tools and testbeds used for research. Finally, the summary of the thesis in Spanish is provided in Appendix B.

Chapter 2

Technical background

This chapter provides a review of the technical background necessary to follow the content of this thesis. The first section describes the cellular technologies involved in this thesis: LTE, 5G, and CIoT. More specifically, it describes the architecture and main components, along with the radio access technology. Section 2.2 describes the multi-connectivity feature for 5G networks, along with the benefits and challenges. Finally, Section 2.3 describes the security in cellular networks, in particular, it is focused on the security architecture and procedures for the 5G network. Moreover, the threat model along with the main attacks are also described.

2.1 Cellular technologies

This section aims to provide an overview of the cellular technologies that are the basis of this thesis. Section 2.1.1 describes the LTE network. Section 2.1.2 describes the 5G network, including its architecture and protocol stack. The new radio access technology in 5G is described in Section 2.1.3. Finally, Section 2.1.4 makes an overview of CIoT focused on Low-Power Wide-Area (LPWA) technologies.

2.1.1 LTE

The Evolved Packet System (EPS), also known as LTE, was first introduced in Release 8 as a mobile communication standard by the 3GPP [74]. The system differs from its predecessor technology, 3G, by using packet-switched networks for the delivery of all services, also including voice, which is commonly referred as Voice over Internet

Protocol (VoIP) and, in the LTE network, as Voice over LTE (VoLTE). LTE evolved in Release 10 with the introduction of LTE-Advanced, which provides an increased data rate and enhancements in multi-antenna techniques. At this point, the standard met the requirements of a 4G network [75].

Regarding the transmission in LTE, Orthogonal Frequency Division Multiple Access (OFDMA) is used in the downlink, while in the uplink Single Carrier Frequency Division Multiple Access (SC-FDMA) is used.

Network architecture

The architecture of LTE is divided into two parts [76]: the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and the Evolved Packet Core (EPC), as depicted in Figure 2.1. The EPC performs functions such as mobility management, network access control or the connection with external networks. The following elements compose the EPC:

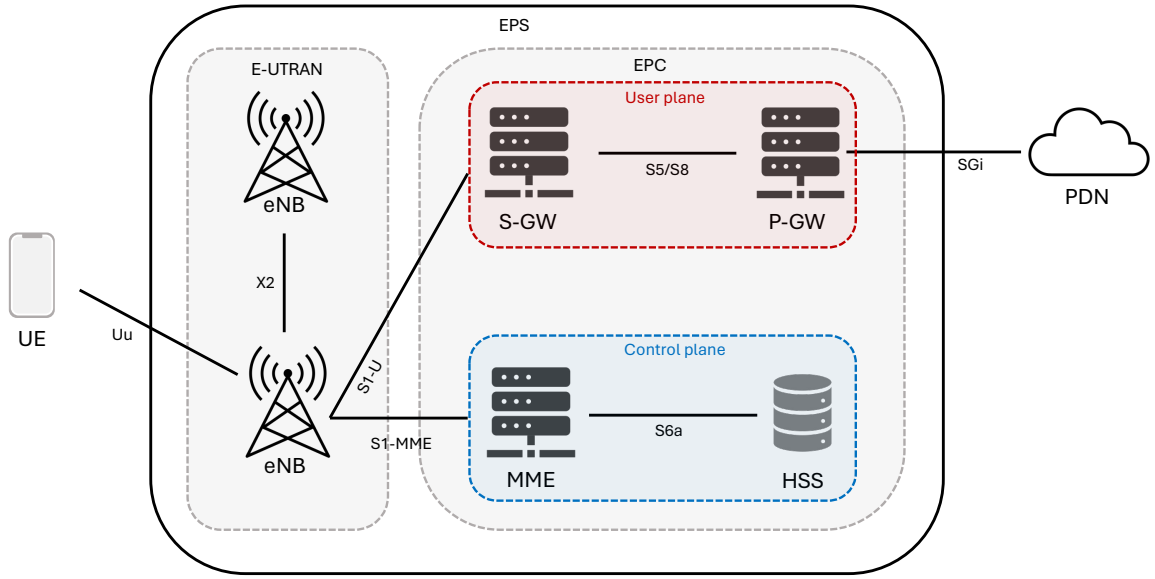


Figure 2.1: LTE architecture.

- Mobility Management Entity (MME): this element manages the CP between the User Equipment (UE) and the Core Network (CN). Its main functions are:
  - Non-Access Stratum (NAS) signaling and security.
  - Access Stratum (AS) security control.
  - EPS bearer control.

  - Roaming and authentication.
  - Idle state handling.

- Serving Gateway (S-GW): this element manages the UP between the UE and the CN. This element performs the following functions:
  - Local mobility anchor point for inter-eNB handover.
  - Mobility anchoring for inter-3GPP mobility.
  - E-UTRAN idle mode downlink packet buffering and initiation of network triggered service request procedure.
  - Packet routing and forwarding.
  - Transport level packet marking in the uplink and the downlink.

- Packet Data Network Gateway (P-GW): this element connects the EPC to external Internet Protocol (IP) networks. The main functions of the P-GW are the following:
  - Per-user based packet filtering.
  - UE IP address allocation.
  - Transport level packet marking in the uplink and downlink.

- Home Subscriber Server (HSS): database that stores users subscription data such as the QoS profile, roaming access restrictions or Access Point Name (APN) of Packet Data Network (PDN) to which the user can connect.

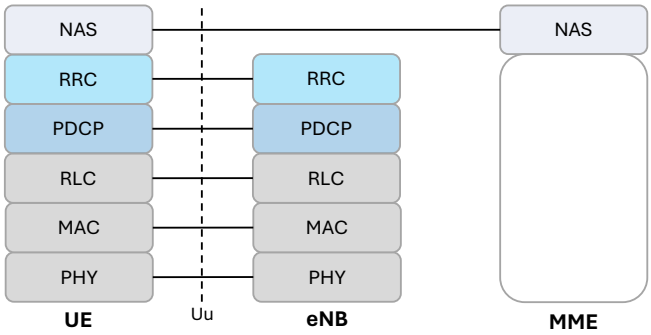
The E-UTRAN consists of base stations, providing E-UTRA UP and CP protocols terminations towards the UE. The E-UTRAN is composed with only one kind of element, the Evolved Node B (eNB), which establishes communication with the UEs via radio signal and with the CN elements. Its main functions are:

- Radio Resource Management functions (e.g., Radio Bearer Control, Admission Control, etc.).
- IP and Ethernet header compression.
- Selection of an MME at UE attachment.
- Routing of UP data towards S-GW.
- Scheduling and transmission of broadcast information and paging.

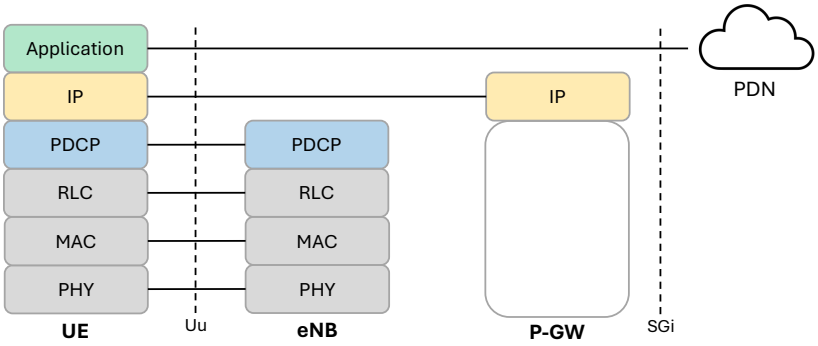
Protocol stack

The communication in LTE between the network elements is done by using a protocol stack. The protocol stack is different for the UP and the CP, along with the network core elements involved, as shown in Figure 2.2.

The UP is used for data transmission between the UE and the network. On the other hand, the CP is used between the network elements to establish connections and authentication. A brief description of the different layers is provided below.



(a) Control Plane.



(b) User Plane.

Figure 2.2: LTE protocol stack.

- Physical layer (PHY): the main function of this layer is the transmission of the signal over the radio channel. This layer includes the use of channel coding, modulation, resource element mapping and mapping to antennas.
- Medium Access Control (MAC): the main purpose of this layer is the allocation of radio resources. This layer also performs functions such as physical channel error corrections using the Hybrid Automatic Repeat reQuest (HARQ) technique or the control of the Random Access (RA) procedure to establish connection from the UE to the network.

- Radio Link Control (RLC): this layer provides a radio connection with an error detection and recovery with Automatic Repeat reQuest (ARQ). This layer also manages packet segmentation and reassembly.
- Packet Data Convergence Protocol (PDCP): this layer provides functions such as header compression and decompression, applies security functions, sequential delivery and data duplicated detection.
- Radio Resource Control (RRC): this layer manages the broadcast of system information (i.e., paging); establish, modify and release RRC connections; performs handover between cells; and encapsulates NAS messages in RRC messages.
- NAS: this layer manages direct signaling between the UE and the MME to establish and maintain communication sessions with the UE as it moves through the network.
- IP layer: this layer is a network protocol that provides bidirectional data transfer, ensuring that data packets are routed and delivered correctly across the network.

Radio Access technology

The physical layer of LTE is based on two multiple access technologies over the air interface: OFDMA and SC-FDMA for downlink and uplink transmissions, respectively. OFDMA allows multiple users to transmit data simultaneously on different subcarriers within the same frequency band. This is done by dividing the channel into a set of narrow subcarriers that are divided into groups according to the needs of each user. This parallel transmission enhances spectral efficiency and enables LTE to achieve higher data rates compared to previous technologies. However, the combination of a high number of subcarriers leads to a high Peak-to-Average Power Ratio (PAPR), which causes a high power consumption in the radio transceivers. In the uplink, this multiple access increases the battery consumption in the UEs. For this reason, OFDMA is not suitable for uplink and SC-FDMA is used instead. SC-FDMA utilizes a single-carrier transmitting signal, transmitting the data symbols in series over one wideband signal, with higher rate and more bandwidth.

Regarding the modulation scheme, in downlink each subcarrier is modulated using from Quadrature Phase Shift Keying (QPSK) to 1024-Quadrature Amplitude Modulation (QAM), whereas the modulation used in uplink ranges from $\pi/2$-Binary Phase Shift Keying (BPSK) to 256-QAM [77].

In terms of system bandwidth, the following values are available in LTE: 1.4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz and 20 MHz. The physical radio resources can be thought of as a set of subcarriers in the frequency domain and a set of opportunities for modulated symbols in the time domain. The smallest resource unit in the physical layer of LTE is called Resource Element (RE), which consists of one symbol in the time domain and one subcarrier in the frequency domain. The REs are grouped together into logical structures that can be used for transmission and reception, called Physical Resource Block (PRB). A PRB is the smallest unit of resources that can be allocated to a user. The PRB consists of 180 kHz in the frequency domain and one slot (0.5 ms) in the time domain. In frequency, PRBs are either $12 \cdot 15$ kHz subcarriers or $24 \cdot 7.5$ kHz subcarriers wide, depending on the Subcarrier Spacing (SCS). The number of subcarriers used per PRB for most channels and signals is 12. On the other hand, the number of symbols per PRB varies depending on the length of the cyclic prefix used, with the common practice being the use of 7 symbols per time slot. In the time domain, LTE is composed of frames with a duration of 10 ms and there are ten subframes per frame with a duration of 1 ms and each subframe contains two slots. An overview of the LTE frame structure is depicted in Figure 2.3.

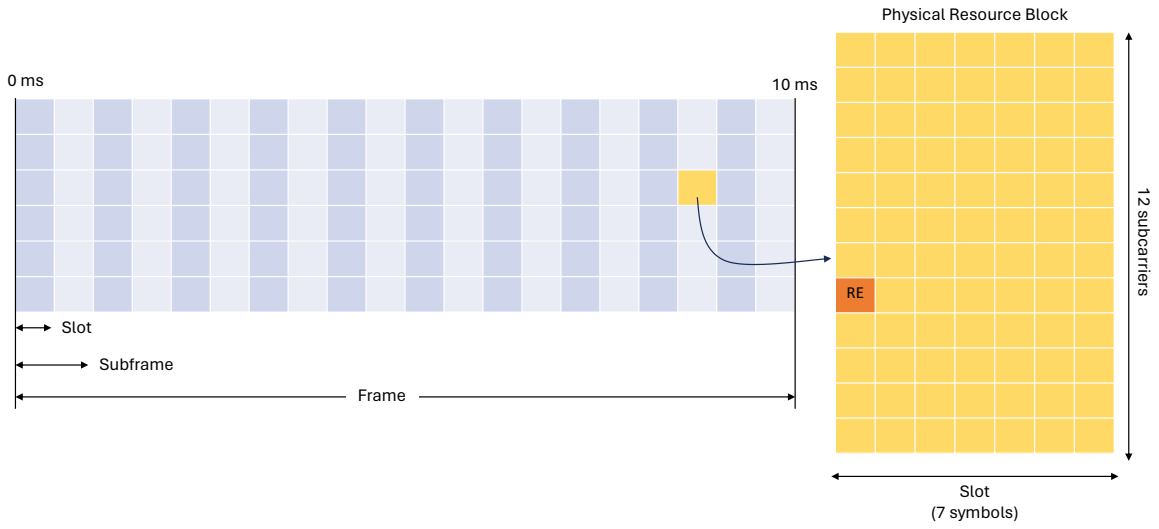


Figure 2.3: LTE frame structure.

2.1.2 5G

The 5G network was first introduced in Release 15 with the aim to provide more flexibility to support new services and applications. Unlike previous technologies that were focused on traditional mobile broadband, in 5G the services have been classified

into three categories according to their requirements [78]:

- eMBB: this service category is an evolution of traditional mobile broadband, with higher data rates and bandwidth. This category encompasses traditional human use cases such as web browsing or streaming multimedia content.
- URLLC: this service category aims to cover critical communications, with low latency and high reliability requirements. Some examples of this category include industrial automation, self-driving car or remote medical surgery.
- mMTC: this category covers massive connection of devices with low bandwidth requirement and non-critical delay. It is mainly focused on the IoT.

An overview of the requirements for the different services is depicted in Figure 2.4.

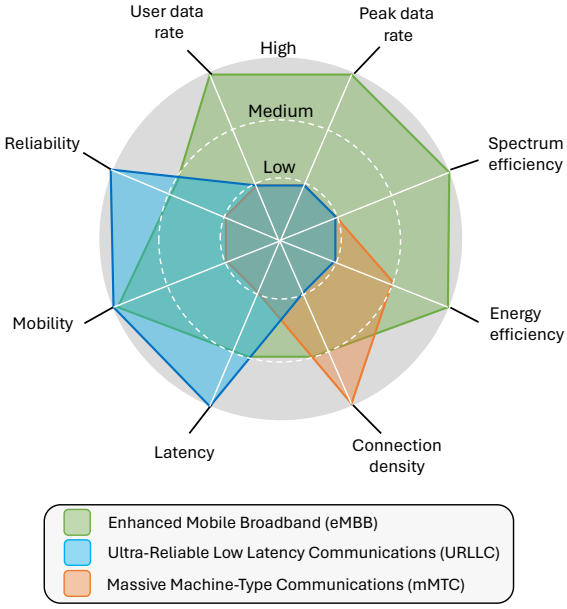


Figure 2.4: Requirements for the different 5G service categories.

To support these traffic profiles and add more flexibility to the network, the following key features have been introduced in 5G:

- Beamforming: this technique allows to transmit the signal directly in one or more specific directions by changing the phase and amplitude of the transmission when using multiple antennas.
- Multiple-Input Multiple-Output (MIMO): this technique allows to transmit different data streams multiplexed on the same spectral resources by using different

antennas, with the aim of improving the channel spectral efficiency. This technique is evolved from LTE MIMO and in 5G the number of antennas is increased.

- Numerologies: 5G provides flexibility in the frame configuration, that is, the SCS and the cyclic prefix. The main purpose of the numerology is to reduce the latency by reducing the slot duration in the frame structure. A more in depth detail of this feature is explain in Section 2.1.3.

- Network Slicing (NS): this technique allows to divide the physical network into different logical networks, commonly known as slices. Each slice can be configured with different parameters to be optimized for a specific application. The implementation of NS is simplified by using Software Defined Network (SDN) and Network Function Virtualization (NFV).

- Mobile Edge Computing (MEC): applications servers are moved to the network edge, thus, reducing the path that a packet must travel.

- Multi-connectivity: consists in establishing multiple radio links between the UE and the network. These links can be established using different components carriers in one node, using different nodes of a network or a combination of both. This feature can be used to improve the throughput if different information is transmitted or to improve the reliability if the same information is transmitted in all links. More details of this feature is explained in Section 2.2.

Network architecture

The 3GPP introduced in Release 15 the first specification of the 5G technology, where two deployment options are defined [79]: the Non-Stand Alone (NSA) and Stand Alone (SA). In the NSA architecture (see Figure 2.5), the 5G RAN is used in conjunction with the existing LTE and EPC infrastructure. This configuration provides the same services as LTE, but with improvements offered by the 5G New Radio (NR) such as lower latency. In this case, a new network element has been introduced in the RAN, the Evolved-Next Generation NodeB (en-gNB). The en-gNB is a network node that provides NR UP and CP towards the UE and it is connected to the EPC.

On the other hand, the SA architecture (see Figure 2.6) operates using the 5G System (5GS). The 5GS is divided into the Next Generation Radio Access Network (NG-RAN) and the 5G Core (5GC). Under this architecture, the different services

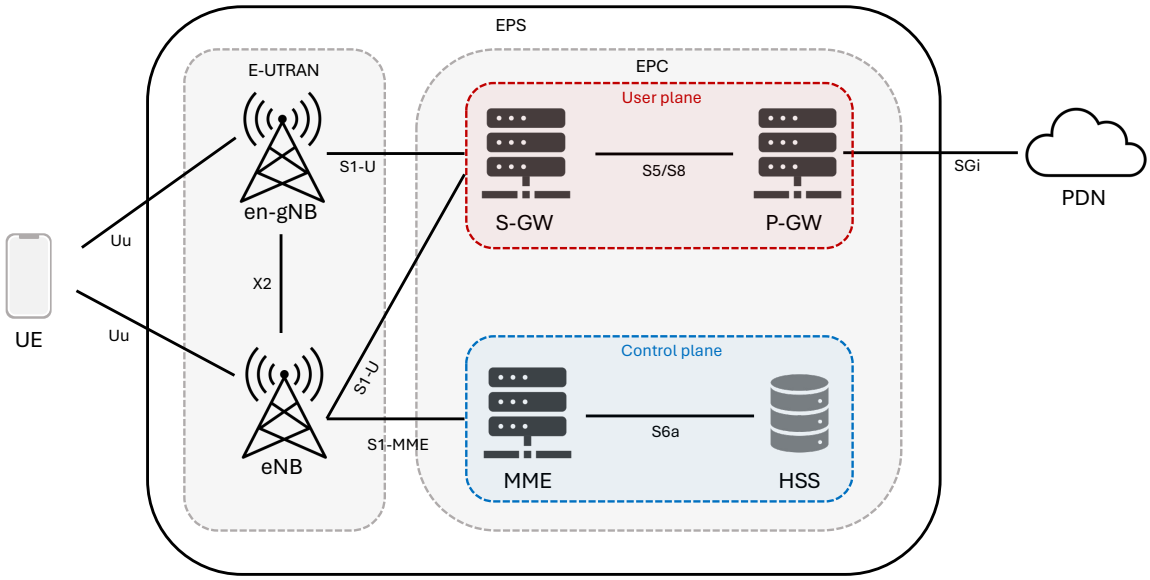


Figure 2.5: 5G NSA architecture.

introduced in 5G are offered. The new elements defined in 5G SA in the RAN part are described below [80, 81].

- Next-generation eNB (ng-eNB): network node that provides E-UTRA UP and CP towards the UE with capabilities to connect to the 5G core.
- Next-generation NodeB (gNB): network node that provides NR UP and CP towards the UE and it is connected to the 5GC. Its main functions are:
  - Radio resource management functions (e.g., radio bearer control, radio admission control or connection mobility control).
  - Selection of an Access and Mobility Management Function (AMF) at UE attachment.
  - Routing of UP data towards User Plane Function (UPF) and CP towards AMF.
  - Scheduling and transmission of paging messages and system broadcast information.
  - Connection setup and release.
  - Session management.
  - Support of NS.
  - Dual connectivity.

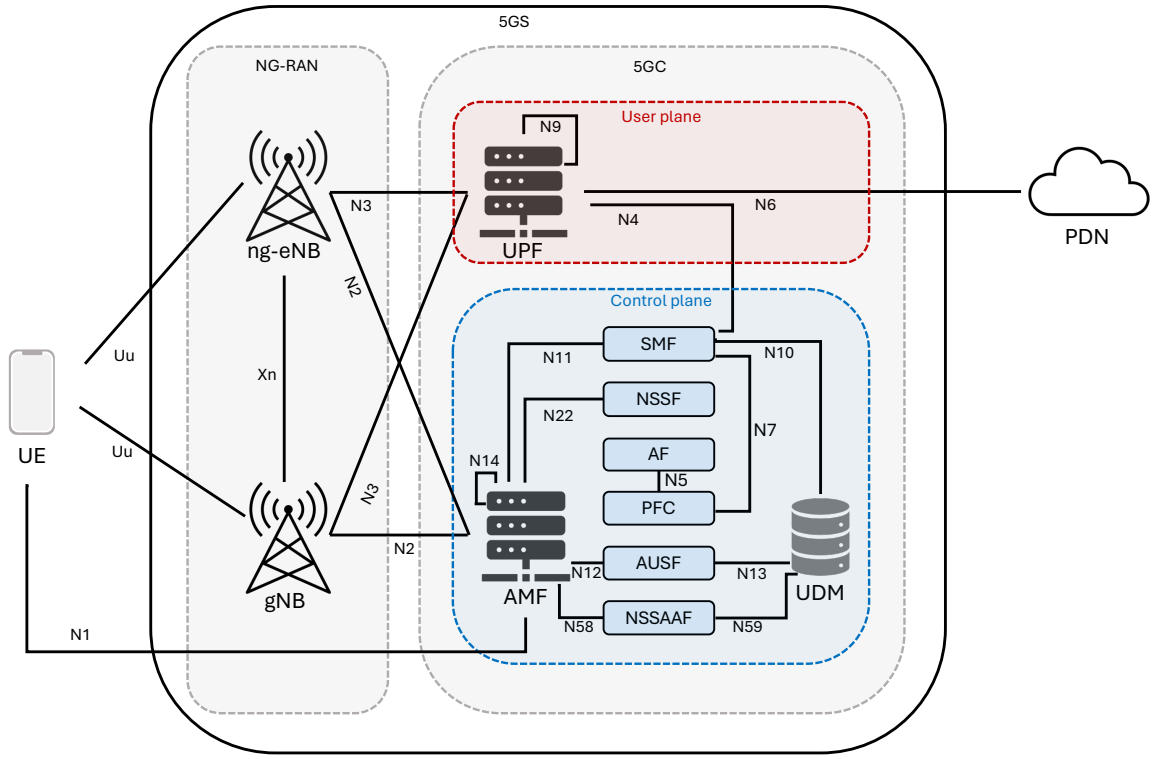


Figure 2.6: 5G SA architecture.

– QoS flow management and mapping to Data Radio Bearer (DRB).

The 5GC architecture relies on a Service-Based Architecture (SBA), where the different mobile CN functionalities (authentication, mobility management, etc.) are defined in terms of Network Functions (NFs) rather than by traditional network entities. This allows an open and modular service platform. A description of the different 5GC NFs is provided below [81].

- AMF: it performs the access, authentication and mobility in the network. The main functions of the AMF are the following:
  - NAS signaling termination and security.
  - AS security control.
  - Access authentication and authorization.
  - Mobility management control.
  - NS support.
  - Session Management Function (SMF) selection.

- SMF: it is in charge of the session management of the UEs. Its main functions are:
  - Session management.
  - UE IP address allocation and management.
  - Control part of policy enforcement and QoS.
  - Configuration of traffic steering at UPF.
  - Downlink data notification.
- UPF: it connects the UP between the NG-RAN and the 5GC; and connects the 5GC to external IP networks. The UPF performs the following functions:
  - Anchor point for intra-/inter-Radio Access Tecnology (RAT) mobility.
  - Packet routing and forwarding.
  - Packet inspection and UP part of policy rule enforcement.
  - QoS handling for the UP.
  - Downlink packet buffering and downlink data notification triggering.
- Authentication Server Function (AUSF): this function is in charge of the authentication in the network. In particular, it executes the following functions:
  - Authentication for 3GPP access and untrusted non-3GPP access.
  - Authentication of the UE.
- Policy Control Function (PCF): this function is in charge of the policy of the network. It performs the following functions:
  - Supports unified policy framework.
  - Provides policy rules to CP functions.
- Application Function (AF): interacts with the CN in order to provide services such as application influence on traffic routing, time synchronization service or interacting with the policy framework for policy control.
- Unified Data Management (UDM): the main functions of this element are the following:

  - Generation of 3GPP authentication credentials.
  - User identification handling.
  - Access authorization.
  - Support to service continuity.
  - Subscription management.

- Network Slice Selection Function (NSSF): this function selects the set of NS instances serving the UE.
- Network Slice-specific and Authentication and Authorization Function (NSSAAF): this function supports for NS specific authentication and authorization.

Protocol stack

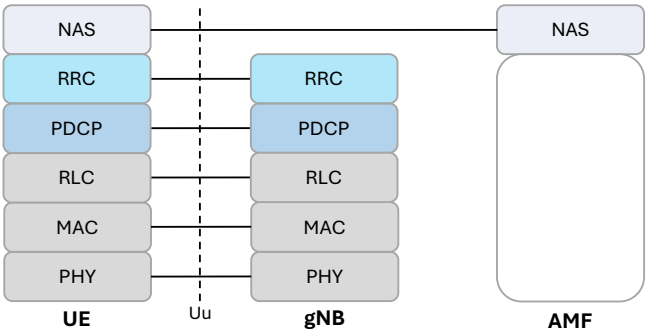
The protocol stack in 5G is based on previous LTE technology and it is depicted in Figure 2.7. However, an additional layer is included in the UP on top of the PDCP layer. This layer is called Service Data Adaptation Protocol (SDAP). The purpose of this layer is to map QoS flows to radio bearers and to provide QoS marking on data packets in the RAN for traffic prioritization purposes.

Moreover, some changes in many layers have been made in 5G:

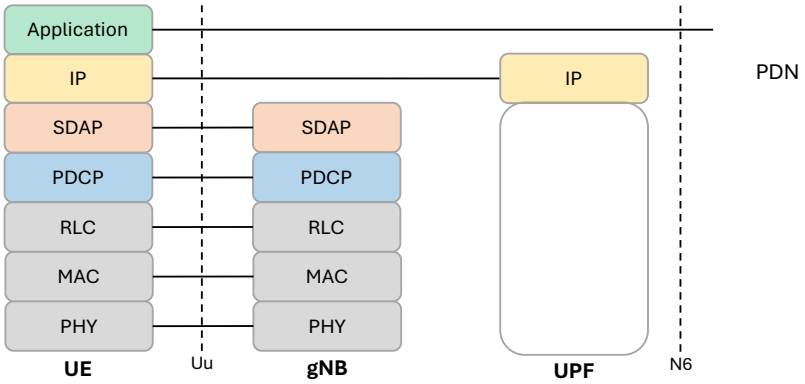
- RRC layer: support of a new RRC state with the aim of reducing the energy consumption and latency for devices that transmit small data with low frequency. This new state is namely RRC Inactive.
- PDCP layer: data integrity protection is added to the UP. Duplication is also added, mapping Packet Data Units (PDUs) to more than one logical channel and sending them over different component carriers.
- RLC/MAC layer: support for beam management procedures and transmission modes that use different numerologies and Transmission Time Intervals (TTIs).

2.1.3 New Radio access technology

As previously explained, the 5G technology was first standardized in Release 15 by the 3GPP. Its radio access technology has suffered changes compared to LTE with the aim



(a) Control Plane.



(b) User Plane.

Figure 2.7: 5G protocol stack.

to provide more flexibility and meet requirements such as lower latency and improved throughput in the communications. This radio access technology is known as NR.

5G NR is based on a flexible Orthogonal Frequency Division Multiplexing (OFDM) system, allowing it to operate in a wide range of bands, address different use cases and operate under multiple spectrum access. Regarding the waveform, OFDM with a cyclic prefix is used for the downlink while for the uplink, unlike LTE, it is possible to use OFDM with cyclic prefix or Discrete Fourier Transform-spread-OFDM (DFT-s-OFDM), the last one with the aim of minimizing the PAPR and to improve the uplink coverage [79].

With respect to the frequency operation in 5G, Release 15 allows frequencies up to 52.60 GHz. Moreover, two Frequency Ranges (FRs) are defined [82]:

- FR1: it covers frequencies from 410 MHz to 7.125 GHz.
- FR2: encompasses frequencies in the range of 24.25 GHz to 52.60 GHz. In this range, directional antennas are necessary due to propagation losses and interference.

Higher frequencies are considered in Release 17. In fact, a new FR has been defined, the FR2-2, which encompasses frequencies in the range of 52.60 GHz to 71 GHz.

Regarding the bandwidth for a component carrier, a maximum value of 100 MHz is supported for FR1, while for FR2 the maximum value is 400 MHz. Note that for the FR2-2 in Release 17, the maximum bandwidth value is increased up to 2 GHz. Nevertheless, the bandwidth configuration will differ depending on the SCS for data transmission configured in the network [82].

Numerology concept and frame structure

5G NR introduces a flexible SCS in its design. The SCS is formed as $15 \cdot 2^{\mu}$ where μ can adopt values of 0, 1, 2, 3 or 4, which results in SCS of 15, 30, 60, 120 and 240 KHz. This is commonly known as numerology (μ), defined by a SCS and the cyclic prefix, which can be normal or extended [79].

However, not all numerologies are suitable for each FR. The reason is that as the SCS increases, the symbol duration decreases, also reducing the cyclic prefix and this can led to inter-symbol interference due to OFDM signal characteristics. This will affect in FR1, since multi-path is present. However, as the frequency is increased, the multi-path problem is reduced, since propagation is predominantly LOS. Therefore, higher SCS are suitable for higher frequencies.

In the standard, the use of a numerology has been divided into the FR used and into data and synchronization channels [80]. In terms of data channels, $\mu = \{0, 1, 2\}$ is supported in FR1 and $\mu = \{2, 3\}$ in FR2. On the contrary, for synchronization channels, $\mu = \{0, 1\}$ is supported in FR1 and $\mu = \{3, 4\}$ in FR2. In Release 17, two numerologies have been introduced for FR2-2 (5 and 6), which corresponds to a SCS value of 480 and 960 kHz and they are supported by data and synchronization channels. The different 5G numerologies defined in the Release 17 are summarized in Table 2.1.

Numerology (μ)	**SCS (kHz)**	**Slots per subframe**	**Slot duration (ms)**	**Symbol duration (μs)**
0	15	1	1	71.42
1	30	2	0.5	35.71
2	60	4	0.25	17.85
3	120	8	0.125	8.92
4	240	16	0.0625	4.46
5	480	16	0.03125	2.26
6	960	16	0.015625	1.115

Table 2.1: 5G numerology configurations (Release 17).

With respect to the radio frame structure, in 5G NR the number of subcarriers is 12 for all numerologies. Moreover, with the aim of maintain compatibility with LTE, the frame duration remains fixed with a duration of 10 ms and the frame is divided into 10 subframes with a duration of 1 ms. Each subframe is composed of slots, which will vary depending on the numerology selected. In fact, the number of slots per subframe is defined as 2^{μ} and the slot duration as $1/2^{\mu}$ ms. Finally, each slot is composed of 14 OFDM symbols, with a symbol duration of $1/(14 \cdot 2^{\mu})$ ms.

An overview of the 5G radio frame in the time domain with different numerologies when using Release 15 is depicted in Figure 2.8.

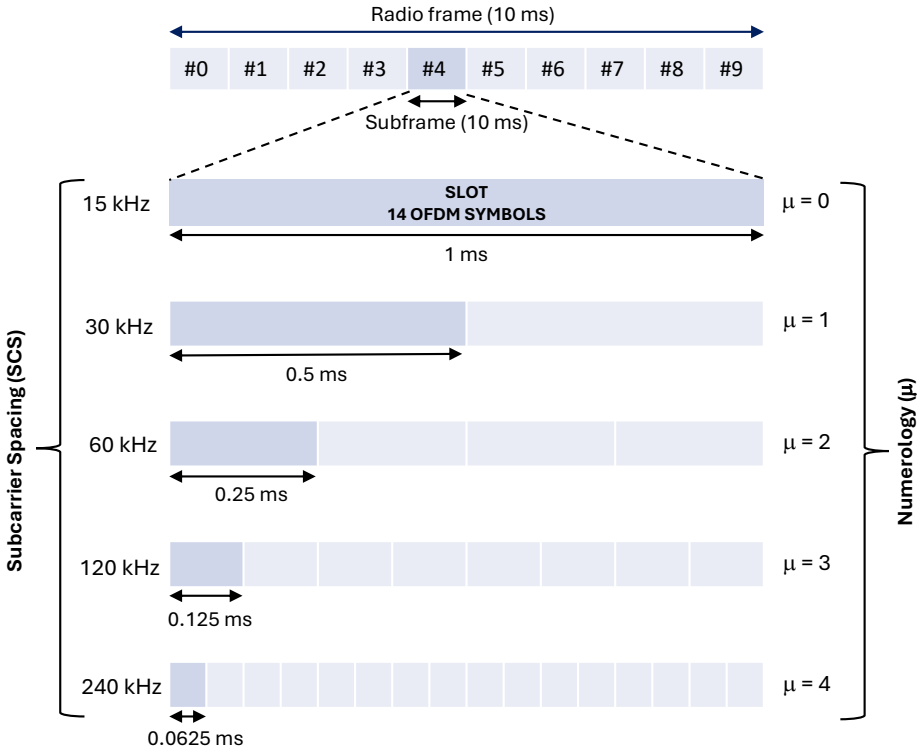


Figure 2.8: 5G numerologies scheme in the time domain (Release 15/16).

2.1.4 Cellular IoT

The 3GPP introduced in Release 13 two Machine Type Communications (MTC) solutions over cellular networks, commonly known as CIoT. In particular, these solutions were LTE for Machine Type Communications (LTE-M) and NarrowBand Internet of Things (NB-IoT), both based on LTE technology.

These technologies emerged to cover MTC use cases, characterized by low throughput requirements, support of massive connections, low power consumption, coverage

enhancements and low cost devices [83]. While LTE-M is intended for mid-range IoT applications with support of voice and video services, NB-IoT provides very deep coverage and support ultra-low-cost devices.

Although these technologies were introduced in Release 13, enhancements have been made in following releases to include new features. An important remark in Release 16 is that CIoT devices are allowed to connect to the 5GC by using a ng-eNB. This implies the support of 5G NAS messages and the 5G security framework, except data integrity protection.

The 3GPP has initiated Release 17 activities on NR Reduced Capability (RedCap) devices, also namely NR-Light [84]. The approach of NR RedCap devices is to address use cases (wearables, video surveillance, industrial IoT) in IoT with requirements that cannot be met using NB-IoT or LTE-M. This devices will offer lower cost, lower complexity, and longer battery life than NR eMBB and wider coverage than URLLC. In this thesis, the focus is set on LPWA technologies and therefore, a brief description of LTE-M and NB-IoT technologies is provided below.

LTE-M

As previously mentioned, LTE-M [85] was first introduced in Release 13 within a new UE category, namely Cat-M1. Cat-M1 enables a coverage enhancement of 15 dB with respect to LTE. Regarding its radio design, Cat-M1 operates like LTE but with a reduced radio frequency bandwidth of 1.08 MHz, which is equivalent to 6 PRBs. Cat-M1 was designed to operate with only one receive antenna, eight HARQ processes and a maximum Transport Block Size (TBS) of 1000 bits. Additional features from LTE that are supported in LTE-M are discontinuous reception, mobility, connection suspend/resume and data transmission via the CP.

LTE-M supports two Coverage Enhancement (CE) modes: CE mode A and CE mode B. Both CE modes enable coverage enhancement using repetition techniques for both data channels and control channels. CE mode A supports up to 32 repetitions, while CE Mode B supports up to 2048 repetitions. The default mode of operation for LTE-M is CE Mode A, which provides an efficient operation in coverage scenarios where moderate coverage enhancement is needed. On the other hand, CE Mode B is an optional extension which provides even further coverage enhancement at the expense of throughput and latency.

LTE-M category has evolved throughout following releases since its first definition.

In each release, enhancements in data rates, device capacities, and energy-efficient solutions have been integrated. In Release 14, support of high peak data rates, multicast transmission, voice enhancements and location services were introduced [86]. In addition, UE Cat-M2 was defined, which supports a radio frequency bandwidth of 5 MHz and higher data rates compared to Cat-M1. Moreover, the maximum TBS for uplink was increased to 2984 bits.

In Release 15, features such as increased spectral efficiency, sub-PRB resource allocation and transmission during the RA procedure were introduced to reduce the latency and power consumption [79]. In Release 16, 5G integration has been realized to share 5G capabilities, CE for non-bandwidth reduced low complexity, standalone development, and mobility improvements. Finally, Release 17 introduced a maximum downlink TBS of 1736 bits, 14 HARQ processes, and traffic management capabilities [87, 88].

NB-IoT

NB-IoT is a narrowband system which operates with a channel bandwidth of 180 kHz with support for multi-carrier operation [89]. NB-IoT is based on LTE technology, therefore, NB-IoT inherits part of its design such as channel codification, numerology, modulation scheme and higher protocols layers. Nevertheless, to reduce the complexity and the cost of these devices, some features are removed such as mobility in connected mode (handover).

NB-IoT supports three different operation modes:

- Stand-alone: using a dedicated carrier.
- In-band: using one PRB withing a normal LTE carrier.
- Guard-band: using unused resource blocks within an LTE carrier guard-band.

Regarding its radio design, in downlink, OFDMA is used with a SCS of 15 kHz over 12 subcarriers with 14 OFDM symbols. Same as LTE, the subframe duration is 1 ms. In the uplink, SC-FDMA is used, where two SCS are supported: 3.75 kHz and 15 kHz [90]. In addition, to reduce the PAPR in the uplink, the modulation is limited in the transmissions, where BPSK and QPSK schemes are adopted.

To operate with NB-IoT devices, only one antenna is necessary and one HARQ process is supported in Release 13 for uplink and downlink. Moreover, two classes of maximum output power are supported by NB-IoT devices: 20 and 23 dBm. In terms

of TBS, a maximum TBS size of 1000 bits for uplink and 680 bits for downlink is supported in Release 13.

NB-IoT supports a Maximum Coupling Loss (MCL) of 164 dB and uses the concept of repetitions and signal combining techniques to improve coverage extension [91]. To serve UEs with different coverage conditions, up to three CE configuration can be set in the network, and each UE will belong to a CE depending on its distance to the base station (see Figure 2.9). The CE is determined by the UE based on a Reference Signal Received Power (RSRP) threshold set by the network, where on each CE different transmission repetitions on physical channels, modulation and radio resources are used.

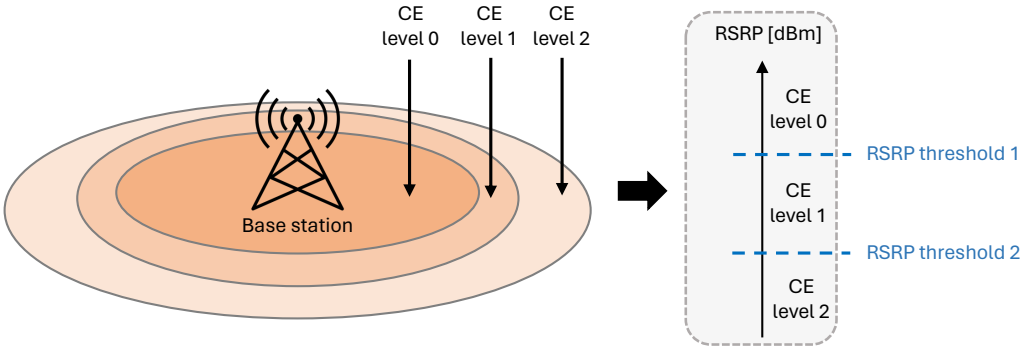


Figure 2.9: Relation between the CE levels and the RSRP thresholds.

Same as LTE-M, enhancements have been incorporated into NB-IoT which each subsequent release. The support of new bands, multicast transmission and positioning were introduced in Release 14. Furthermore, up to two HARQ processes are supported and the maximum TBS was enhanced to 2536 bits in the uplink and downlink [90]. A new NB-IoT category was also introduced, namely Cat NB2. Cat NB2 provides higher data rates and a new power class with a reduced output power of 14 dBm [86].

In Release 15, the focus was mainly set on enhancements on power consumption and latency reduction, with the introduction of data transmission during the RA procedure, Time Division Duplex (TDD) support and higher spectral efficiency [79]. Release 16 introduced coexistence with NR, improved energy and transmission efficiency, and scheduling enhancements. Finally, Release 17 enables data transmission in RRC Inactive state and introduced enhancements such as intra-UE multiplexing, positioning targeting factory automation, extended peak data rate, 16-QAM for uplink and downlink transmission, and time synchronization enhancements [87, 88]

Power saving techniques for CIoT

CIoT communications are usually characterized as sensors that transmit small data reporting the temperature, humidity, etc., with a low frequency. Due to the nature of these communications, it is important to ensure an efficient battery consumption, particularly while the devices are not transmitting any data, which is most of the time. This is quite important, since the International Telecommunication Union (ITU) and the 3GPP have defined a battery life requirement for CIoT devices in extreme coverage of beyond 10 years, with a desirable target of 15 years [92].

To address this, different power saving techniques have been introduced for CIoT devices (see Figure 2.10):

- Extended Discontinuous Reception (eDRX): defines a cycle where the UE monitors the Physical Downlink Control Channel (PDCCH) during a short period of time and sleeps the remaining time of the cycle. This mechanism is an extension of LTE Discontinuous Reception (DRX), where longer sleep periods are supported (DRX cycle is extended from 2.56 seconds to minutes or hours) [93]. The duration of the eDRX phase is defined by the active timer (T3324).
- Power Saving Mode (PSM): this feature was designed for CIoT devices to conserve more battery, where the UE enters in deep sleep mode. During the PSM, the device turns off its radio components completely, but maintains the registration in the network [94]. This means that there is no transmission or reception for any kind of channel or signal, and the UE is not reachable by the network. The advantage of this approach is that the UE can wake-up from PSM without reattaching the connection, thus, avoiding extra power consumption. The duration of the PSM is defined by the difference between the tracking area update timer (T3412) and the active timer (T3324) [95, 96].
- Release Assistance Indication (RAI): before the UE switches from RRC Connected state to RRC Idle state, it has to wait for receiving the RRC Release message from the network. If this message is not received, the UE has to wait until the expiry of an inactivity timer. To avoid this, the 3GPP introduced in Release 14 the RAI feature [97]. The RAI feature allows the UE to indicate to the network that it has no more uplink data or it does not expect to receive any data. This feature improves the battery by releasing the RRC connection without waiting for the inactivity timer expiration.

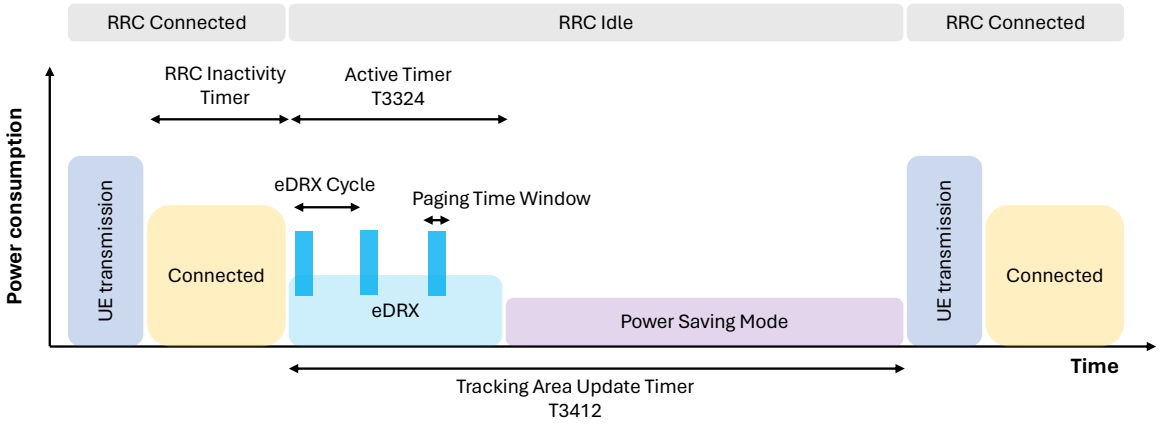


Figure 2.10: Overview of the RRC connection states and energy consumption with eDRX and PSM for a CIoT device.

CIoT signaling optimizations

In LTE and 5G, it is required to establish an RRC connection for the transmission of data from a UE to the network. This process is called Service Request (SR) and is shown in Figure 2.11. Since no RRC connection is active at the beginning, the first communication with the network is made using the RA procedure. The RA procedure consists of four steps: the preamble transmission (Msg1), the preamble response (Msg2), the connection establishment request (Msg3) and the connection establishment (Msg4). When receiving Msg4, the UE moves to RRC Connected state. After that, the AS security is configured. Once this process is finished, DRBs are created and the UE can transmit its data to the network. Finally, after an inactivity period, the UE receives a message from the network to release the connection and the UE returns to RRC Idle state. At the same time, DRBs and UE context are deleted in the CN. To further optimize this process for CIoT devices, two methods were introduced in Release 13 (see Figure 2.11): CP and UP CIoT optimizations.

The CP CIoT optimization consists in performing data transmission using the CP. The support of this mode is mandatory for NB-IoT devices and optional for LTE-M. In this case, data is encapsulated in NAS signaling messages that are sent to the CN. When using this procedure, the UE avoids the establishment of UP bearers and AS security each time it requires to send data.

The UP CIoT optimization is based on the concept of connection suspension and resume introduced in Release 13. This optimization requires a previous RRC connection establishment, where AS security and DRBs are created. Once this process is done, it is possible to suspend the connection and the UE moves to RRC Idle state. However,

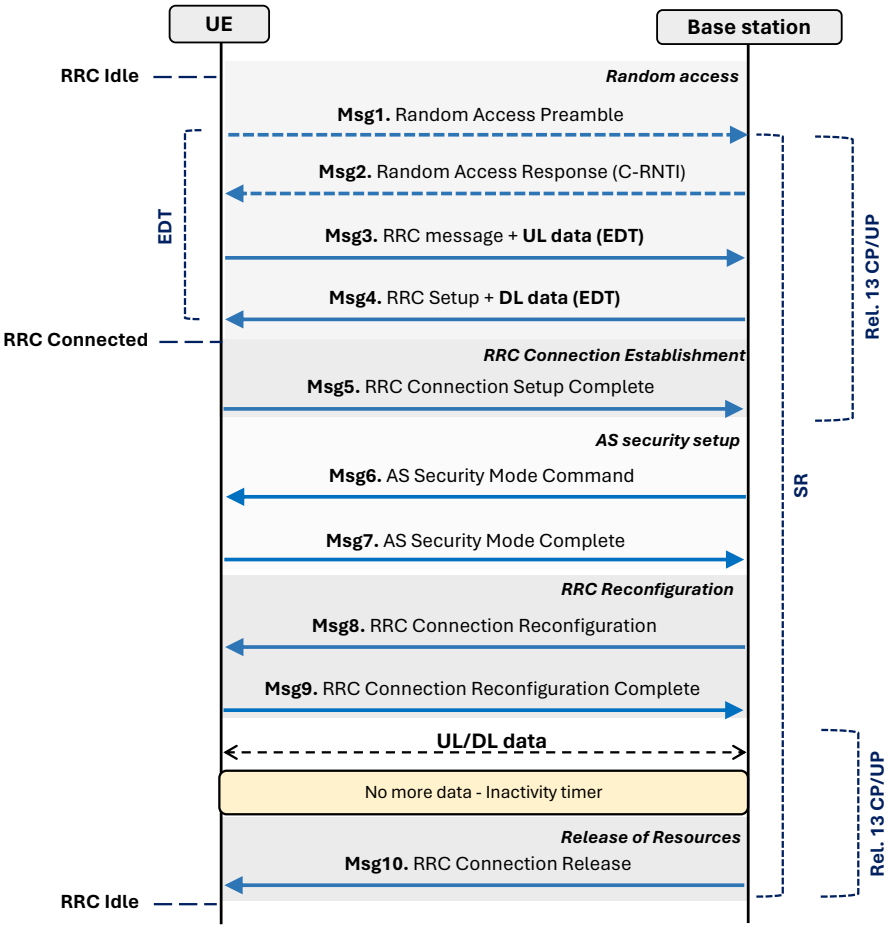


Figure 2.11: Signaling diagram of mobile originated data transport between the UE and the base station for SR, Release 13 CP/UP optimizations and EDT.

the suspension keeps the UE connection and security context in the entities involved (UE, base station and core). Therefore, when the UE needs to send data again, it can resume the previous context using for that a connection identifier provided in the suspension message. As the UE context is maintained in the network, it is not necessary to reconfigure the RRC connection with new DRBs and the AS security.

Although Release 13 CIoT optimizations reduce the signaling exchange between the UE and the network with respect to the SR procedure, a new mechanism was introduced in Release 15 to further reduce the latency and battery consumption of the UEs. This mechanism is known as EDT and is intended particularly for infrequent and small data transmissions. EDT allows the transmission of data during the RA procedure (see Figure 2.11) and is supported for the CP and UP. EDT was created to send uplink data in Msg3, without further need for the establishment of an RRC connection and a state change in the UE; significantly reducing both signaling and wake-up time in the UE. Moreover, the UE can also receive small data in Msg4 if

necessary.

To be able to use this optimization, a special preamble is used in Msg1, which lets the base station know that the UE has small data to transmit. Then, in Msg2, the base station returns a TBS, which indicates the maximum size of the Msg3 (RRC message and user data). For EDT, the maximum TBS allowed in Msg3 is 1000 bits, whereas the minimum is 328 bits [91]. On the other hand, the maximum TBS allowed in Msg4 is 680 bits. A more detailed description of EDT is provided in Chapter 6, along with a security analysis of this feature.

2.2 Multi-connectivity in 5G

Multi-connectivity consists in simultaneously establishing two or more links between the UE and the radio access nodes. In 5G, multi-connectivity inherits from two concepts introduced for LTE networks: Carrier Aggregation (CA) and Dual Connectivity (DC).

2.2.1 Carrier aggregation

CA was first introduced in Release 10 by the 3GPP for LTE networks [74]. In CA, two or more Component Carriers (CCs) are aggregated in order to support wider transmission bandwidths and thereby increase the bitrate. This aggregation is made from a single network node. Two types of CA are defined, which depend on the frequency of the aggregated CCs: (1) inter-band, and (2) intra-band with its two sub-modes, intra-band contiguous and intra-band non-contiguous. Inter-band means that the aggregated carriers are in different frequency bands while intra-band means that the aggregated CCs reside in the same frequency band. In the case of non-contiguous, however, the carriers are not co-located. The bandwidth of the aggregated CCs and the number of CCs used in downlink and uplink can be different, with a maximum of 16 CCs for 5G operation in both cases [80].

When CA is configured there are a number of serving cells, one for each CC. Although the different number of serving cells, the RRC connection is only handled by one cell, the Primary Cell (PCell), served by the Primary Component Carrier (PCC). The other CCs are all referred to as Secondary Component Carriers (SCCs), serving the Secondary Cells (SCells). The SCCs are added and removed as required, while the PCC is only changed in a handover procedure. A high-level diagram of CA with one UE that is served with two CCs in the same gNB is depicted in Figure 2.12.

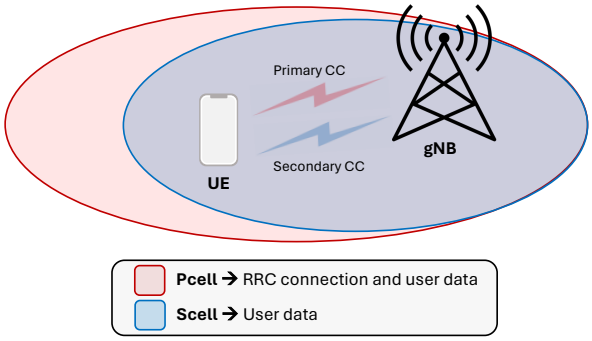


Figure 2.12: High-level CA diagram in 5G.

When using CA, the user traffic is split between the CCs in the MAC layer, and this layer must be able to handle scheduling on a number of CCs. For each serving cell, one HARQ entity is required. Also, one Transport Block (TB) is generated per TTI for each serving cell in the absence of spatial multiplexing [80]. Figure 2.13 shows the 5G layer-2 structure for downlink with CA configured and highlights the main changes.

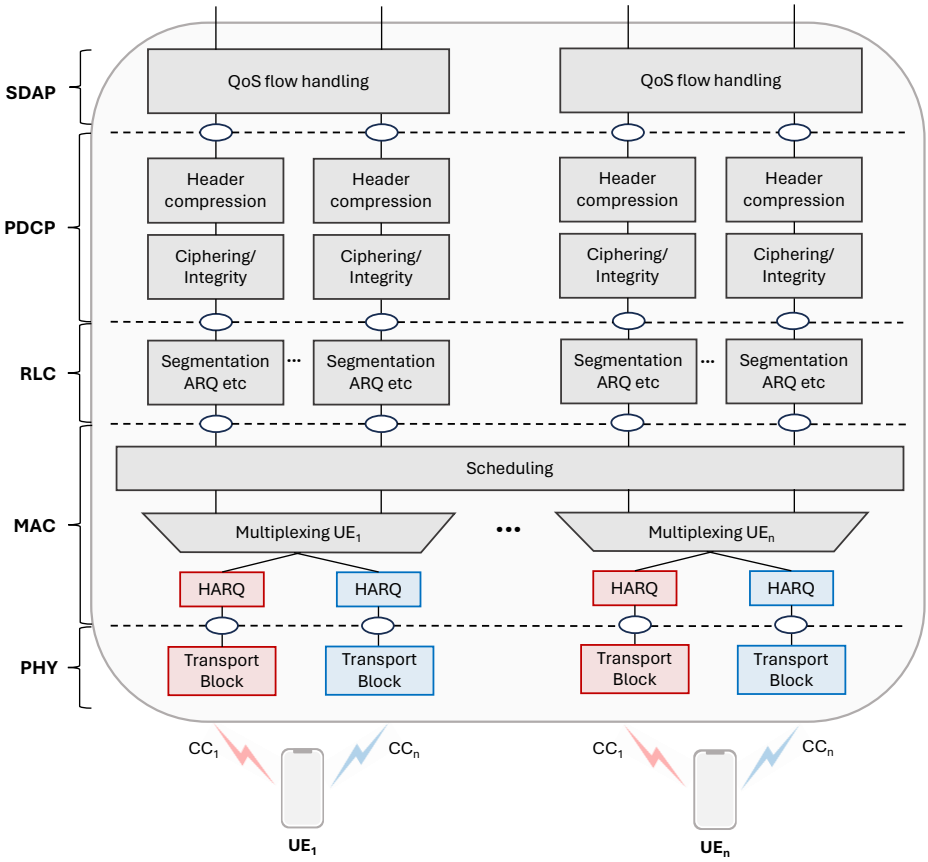


Figure 2.13: Layer-2 structure for downlink with CA configured in 5G.

2.2.2 Dual connectivity

DC feature was first introduced in Release 12 for LTE [74] and allowed UEs to simultaneously receive and send data from two eNBs that are connected via a non-ideal backhaul. In particular, DC allows to aggregate different CCs using two different network nodes, one acting as a Master eNB (MeNB) and the other one as a Secondary eNB (SeNB). The MeNB is in charge of the signaling between the E-UTRAN and the EPC, also managing the DC signaling. The DC signaling between the MeNB and the SeNB is performed via the X2 interface. This feature was first introduced to boost LTE throughput using different network nodes [98].

Release 15 introduced the support of DC with NR and LTE nodes as an extension of existing DC in LTE. In fact, this type of DC was specified for 5G NSA networks and it is known as Multi-Radio Dual Connectivity (MR-DC) [80]. In MR-DC, the UE is connected to one eNB that acts as a Master Node (MN), carrying the signaling between the UE and the EPC; and to a gNB that acts as a Secondary Node (SN). Moreover, in Release 16 DC was introduced for 5G SA deployments, namely as NR-NR DC. In NR-NR DC (see Figure 2.14), the UE is connected to two gNBs, one acting as a MN and another as a SN, and both connected via a non-ideal backhaul over the Xn interface.

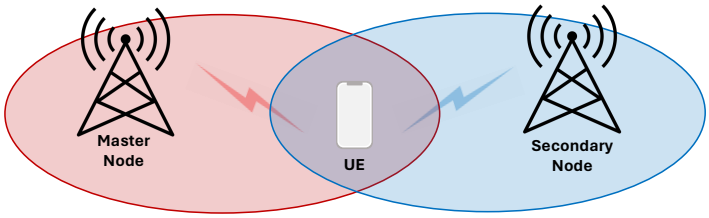


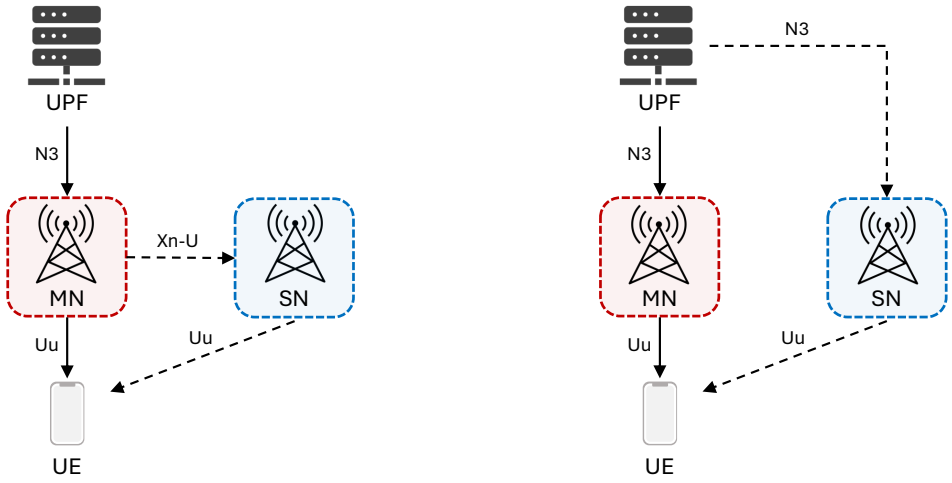
Figure 2.14: Dual Connectivity in 5G.

The 3GPP has defined two UP architectures for DC (see Figure 2.15). In the first architecture, the UP is split in the MN. When using this architecture, the UP data is transferred to the SN over the Xn-U interface. In the second architecture, both MN and SN have a UP connection to the UPF.

In DC, two different radio bearers exist:

1. Direct bearer: uses radio resources from one node. Direct bearers are divided into Master Cell Group (MCG) and Secondary Cell Group (SCG), depending on which node are located, MN or SN.

2. Split bearer: uses radio resources from both, MN and SN.



(a) UP split in the MN. (b) UP split in the CN.

Figure 2.15: 5G Dual Connectivity UP architectures.

Signaling Radio Bearer (SRB) are always configured as MCG, while DRBs can be configured as MCG, SCG or split bearers. Contrary to CA, in DC the user data is split at PDCP layer of the MN. Figure 2.16 shows the layer-2 structure for 5G DC in the downlink direction.

Packet duplication

One of the main changes introduced in the split in MR-DC with respect to LTE DC was the possibility of duplicating user data to further increase the reliability. This DC approach is known as Packet Duplication (PD). When PD is activated, the duplication is made in the PDCP entity of the MN. In the receiver, the PDCP entity is responsible for detecting and removing duplicated packets. Figure 2.17 depicts how the UP bearers can be split in a DC architecture, also including data duplication.

When using PD, the PDCP entity of the MN duplicates the PDU and adds the same sequence number in the PDCP header of both. This avoids performing twice functions such as ciphering, integrity and header compression. Then, the packet is sent from the MN to the SN via the Xn-U interface and the packet will undergo through independent RLC, MAC and Physical (PHY) layers as it can be seen in Figure 2.16.

Multiple copies of the packet are received on the receiver side, and the first successfully received packet is forwarded to the higher layers and the duplicated packets received later are discarded based on the PDCP sequence number.

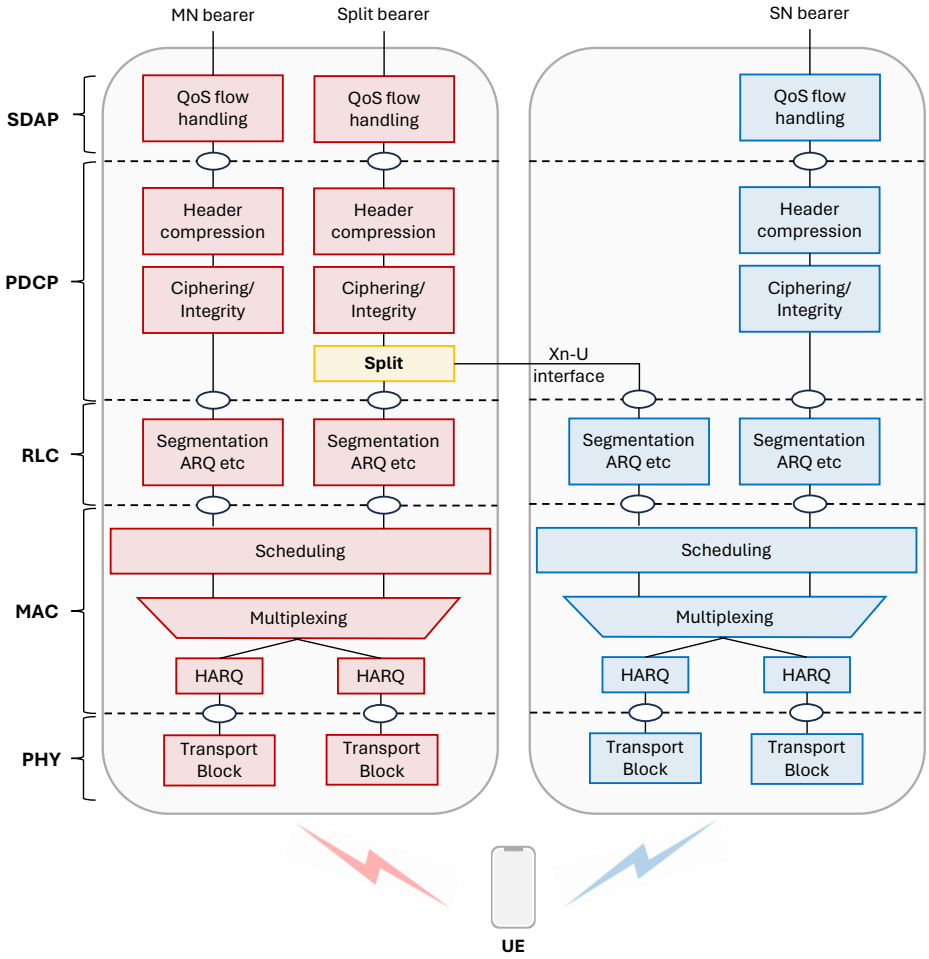


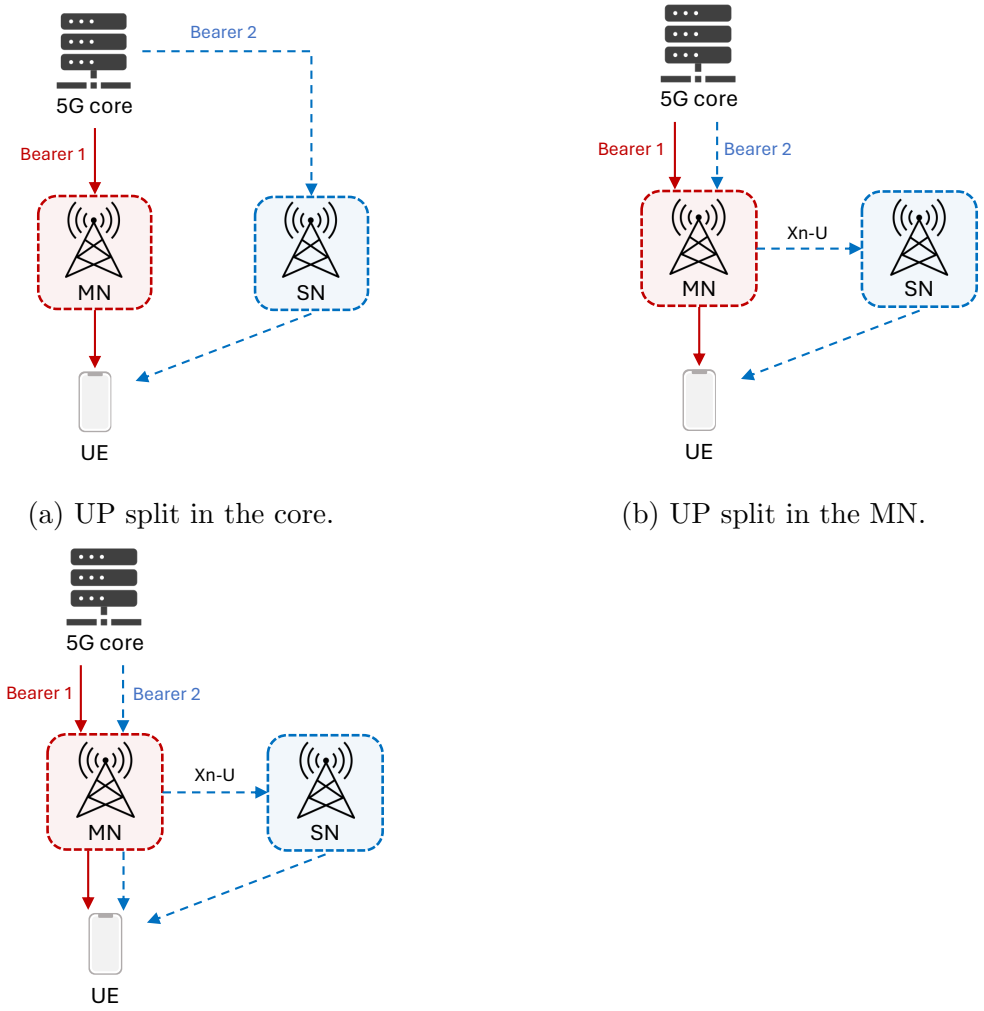
Figure 2.16: Layer-2 structure for 5G DC.

2.2.3 Multi-connectivity benefits and challenges

The use of multi-connectivity techniques offers different benefits, as demonstrated during the last few years by several research works, including [99]: (1) improved reliability, sending redundant data using different links, which also reduce the packet loss rate; (2) improved data rate, combining multiple data streams from different links into a single data stream; (3) service segregation, by segregating services with different requirements to different links; (4) mobility robustness, reducing the interruption time and the amount of signaling required.

Nevertheless, despite the benefits previously mentioned, some challenges are also present when using multi-connectivity [99]:

- Flow control: under- or over-utilized links might be created by an inadequate flow control logic, which results in a degradation of the service (i.e., out-of-order



(a) UP split in the core.

(b) UP split in the MN.

(c) Data duplication in the MN.

Figure 2.17: 5G DC UP bearers split architectures.

packet arrivals or poor overall system performance). The solution of this issue is to use a dynamic control of multi-connectivity that takes into account radio link conditions and radio resources instead of a static approach.

- Packet reordering: packets may arrive out of order due to different radio link conditions and communication path delays. To address this issue, the 3GPP has defined a reordering method for DC and MR-DC, which uses a static reordering timeout [100]. A special care should be taken in the decision of this timeout value, where aspects such as backhaul latency, radio link conditions, traffic type and QoS requirements should be considered.

- Multi-connectivity operation management: the decision of when to use multi-connectivity instead of single connectivity, the CCs involved or which base sta-

tions should be used is not trivial. Therefore, this decision is of a great importance since it has an impact on the overall system performance.

- Number of network nodes: only two network nodes are considered in the current standard. The use of a higher number of network nodes could provide more versatility for traffic aggregation if one of the nodes fails.

2.3 Security in 5G

2.3.1 Security architecture

The security architecture of 5G is divided into two domains [101]: the subscriber and the network domain. The subscriber domain is composed of the UE, while the network domain is composed of two elements, the home network and the serving network. Each of them contains different modules and subsystems, with the most important for the security aspects depicted in Figure 2.18.

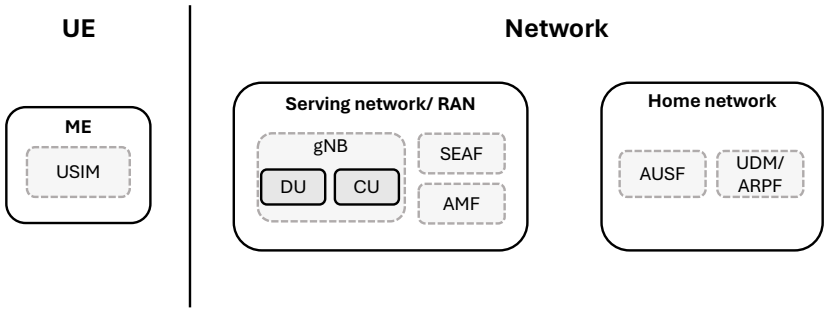


Figure 2.18: 5G security domains and submodules.

The UE contains the Mobile Equipment (ME) of the subscriber, and it is equipped with a Universal Subscriber Identity Module (USIM), which has cryptographic capabilities and stores the subscriber's credentials provided by the network operator.

The home network belongs to the subscribers' operator, manages subscriber information at the UDM and is in charge of verifying subscribers' authentication requests, using the Authentication credential Repository and Processing Function (ARPF) and the AUSF.

On the other hand, the serving network receives and stores the anchor key in the SEcurity Anchor Function (SEAF), and connects the UE with the home network, providing access to the UEs through the gNBs. It also manages the registration, mobility and reachability through the AMF. The gNB functionality is split into two

functional units: the Distributed Unit (DU), which contains the physical layer and the antenna; and the Central Unit (CU), which controls different DUs.

2.3.2 Security procedures between the UE and the 5G network

The security procedures between the UE and the 5G network are performed during the UE registration in the network, which allows the UE to transmit data if successfully registered. Before the UE being able to securely communicate, 5G requires an authentication process. This authentication is mandatory and is named primary authentication. The purpose of the primary authentication is to enable mutual authentication between the UE and the network and provide keying material that can be used between the UE and the serving network in subsequent security procedures [101]. For the primary authentication, the 3GPP proposes a novel Authentication and Key Agreement (AKA) protocol, namely 5G-AKA [102]. Alternatively, the previous EAP-AKA' from LTE can still be used [103]. While these two protocols share similarities, differences exist in the key derivation and the inclusion of new messages. The details of 5G-AKA protocol is described in detail in Chapter 6.

Once the primary authentication is done, the UE and the network share an anchor key called K_{SEAF}. From this anchor key, session keys for the communication between the subscriber and the home network are derived, as depicted in Figure 2.19. However, this authentication is implicit between the parties (UE, serving network and home network) according to the 3GPP. Therefore, upon successful completion of the primary authentication, a Security Mode Command (SMC) procedure is initiated by the AMF with the UE and at the end of this procedure, both are mutually authenticated.

Security Mode Command procedure

The SMC procedure is implemented for NAS and AS to establish the security of these domains, that is, the ciphering/integrity algorithms to be used and to derive the keys from K_{SEAF}. This procedure also checks the security capabilities of the UE to prevent bidding-down attacks [104].

The first one to execute after the primary authentication is the NAS SMC procedure (see Figure 2.20), in which the NAS security context is established between the UE and the AMF.

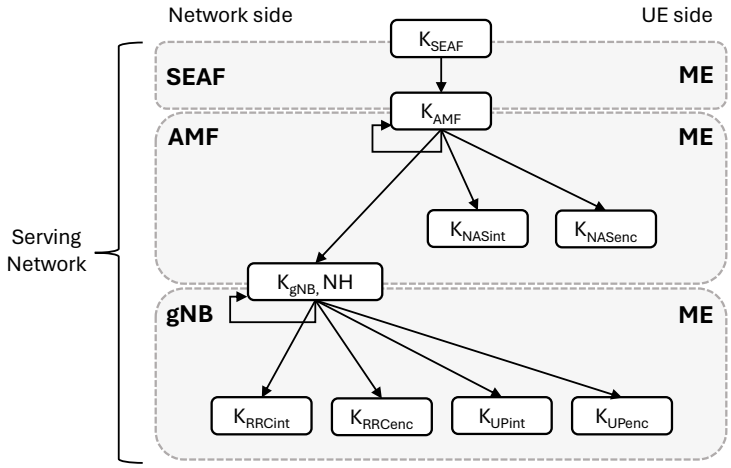


Figure 2.19: Key hierarchy generation.

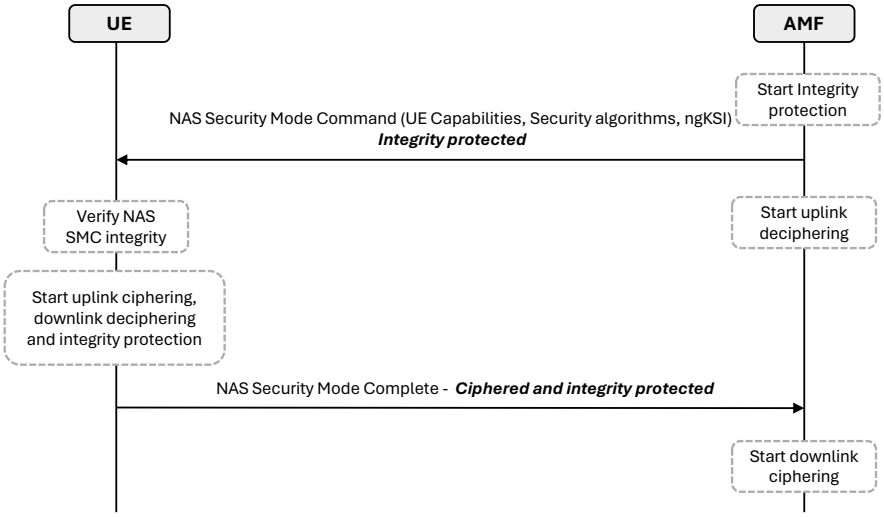


Figure 2.20: NAS Security Mode Command procedure.

The procedure consists of two messages and is initiated by the AMF. Before sending the first message, the AMF activates the NAS integrity protection. Then, the "NAS Security Mode Command" message is sent from the AMF to the UE. This message is integrity protected with K_{NASint} and contains the UE security capabilities (previously transmitted by the UE in the "NAS Registration Request" message), the selected NAS algorithms and the ngKSI for identifying the K_{AMF}. Upon reception of this message, the UE verifies its content. This includes checking that the UE security capabilities sent by the AMF match the ones stored in the UE to ensure that these were not modified by an attacker and verifying the integrity protection using the indicated NAS integrity algorithm and NAS integrity key based on the K_{AMF} indicated by the ngKSI. If the verification of the integrity of the message is successful, the UE starts NAS integrity protection and ciphering/deciphering with the security context indicated by the ngKSI

and sends the "NAS Security Mode Complete" message to the AMF ciphered and integrity protected with K_{NASenc} and K_{NASint}. Finally, the AMF deciphers and check the integrity protection of the "NAS Security Mode Complete" message using the key (K_{NASenc}, K_{NASint}) and algorithm indicated in the "NAS Security Mode Command" message and activates NAS downlink ciphering.

Once the NAS SMC procedure is successfully executed, the AS SMC procedure is triggered by the gNB (see Figure 2.21). Similar to the NAS SMC procedure, the AS SMC procedure aims to negotiate RRC and UP security algorithms and activate RRC security. First, the gNB sends the "AS Security Mode Command" message, which contains the selected RRC and UP ciphering and integrity algorithms and is integrity protected with K_{RRCint} (based on the current K_{gNB}). The UE then verifies the integrity of the message and if successful, starts RRC integrity protection and RRC downlink deciphering. Moreover, the UE sends the "AS Security Mode Complete" message to the gNB, which is integrity protected with the selected RRC algorithm indicated in previous message and the key K_{RRCint}. Finally, the gNB verifies the message sent by the UE and RRC uplink deciphering starts at the gNB.

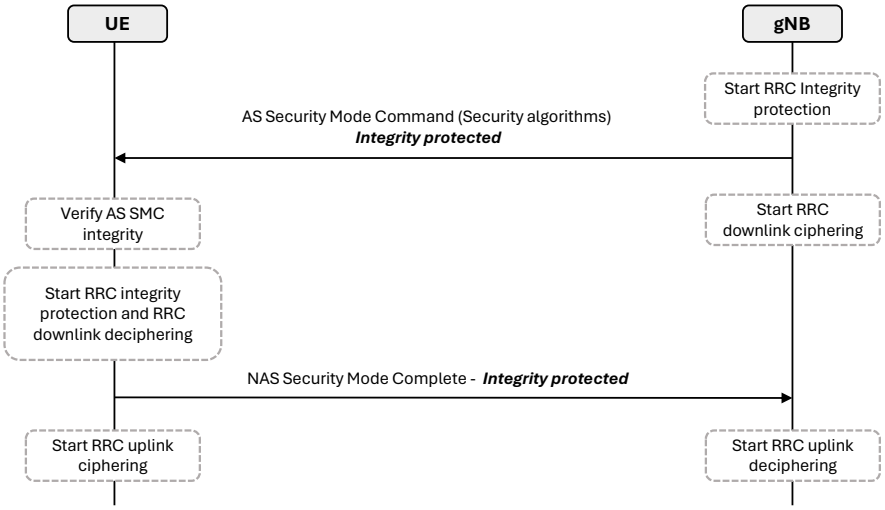
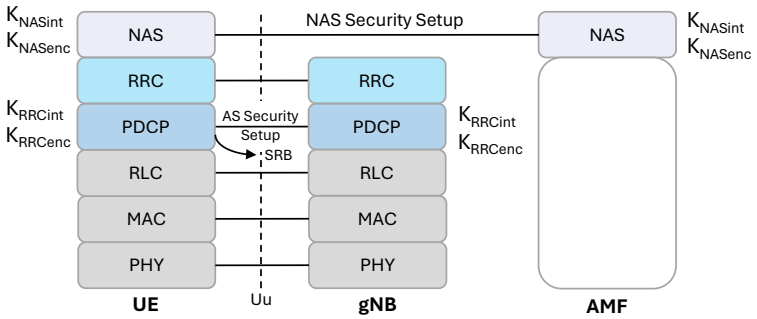


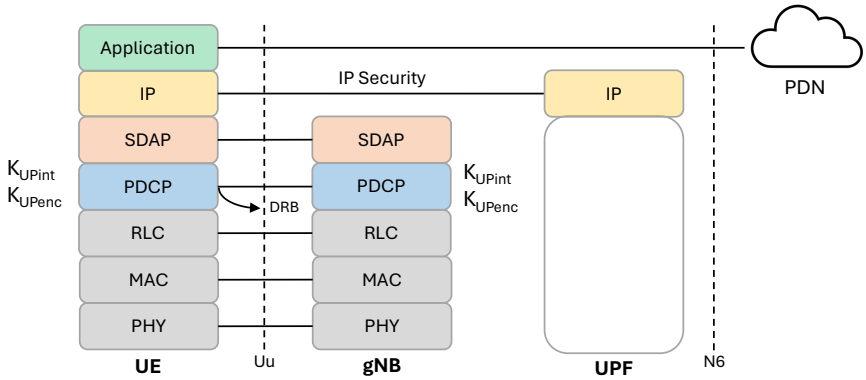
Figure 2.21: AS Security Mode Command procedure.

Ciphering and integrity protection of UP downlink and uplink, at the UE and the gNB, starts when configuring the DRBs, with the "RRC Connection Reconfiguration" and "RRC Connection Reconfiguration Complete" messages [101].

At the end of both procedures (NAS and AS SMC procedures), the UE and the network shares the CP and UP keys that are used to securely communicate the UE with the network and Figure 2.22 summarizes the layer where the key is used and the security contexts.



(a) Control Plane.



(b) User Plane.

Figure 2.22: Control and user plane keys and security contexts.

To summarize all the security procedures performed in the 5G registration, Figure 2.23 depicts the messages exchanged between the UE and the network for establishing a 5G communication. It comprises six phases:

1. The UE gets physical access to the gNB by using the RA procedure [105].
2. UE is authenticated with the network (primary authentication) using the 5G-AKA protocol and K_{SEAF} is derived.
3. NAS security context is created with NAS SMC procedure.
4. AS security context is created with AS SMC procedure.
5. RRC Connection Reconfiguration procedure is performed between the gNB and the UE to add DRBs and activate the UP security.
6. Finally, data exchanged in the network is ciphered and integrity protected using the keys derived in previous phases and the communication between the UE and network is secure.

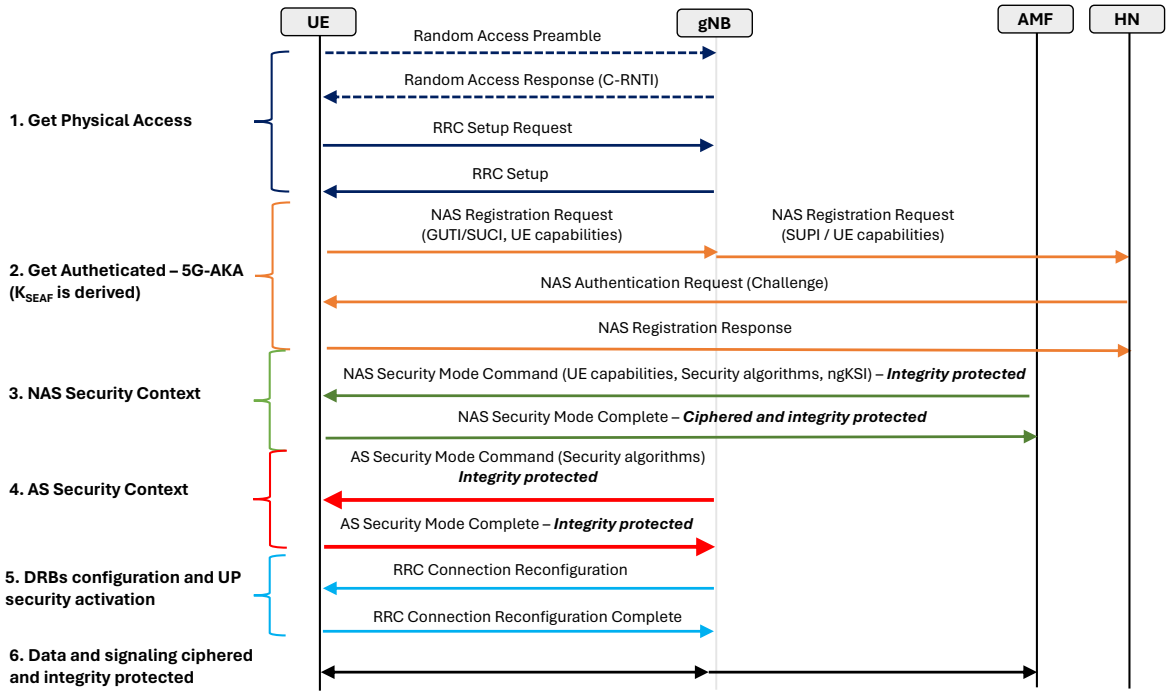


Figure 2.23: 5G registration and security initialization process.

2.3.3 Threat model and main attacks

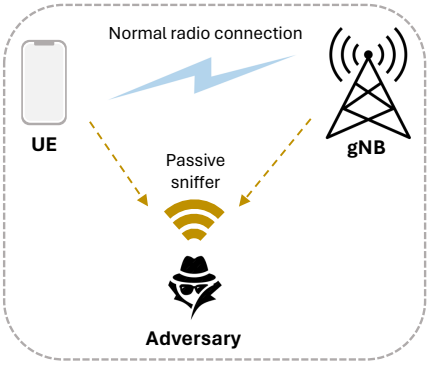
In general, threat models assume that the UE and the serving network are connected over an untrusted wireless channel, whereas serving network and home network communicate using a trusted channel [101]. Under this model, for the UE-Serving network channel, the ability of adversaries is usually modeled using the Dolev-Yao (DY) model [106]. In the DY model, the network is controlled by the adversary; where passive adversaries can eavesdrop on the communication and active adversaries can also intercept, inject, manipulate or drop messages. Thus, attacks on the radio interface can be classified into three different categories depending on the attacker capabilities [107] (see Figure 2.24):

- Passive attacker: plays an eavesdropper role that has the ability to receive, save and decode radio signals within a specific range and further extract concerned information without being noticed. Thus, a passive attacker can passively sniff the transmissions between the UE and the base station in the air interface.

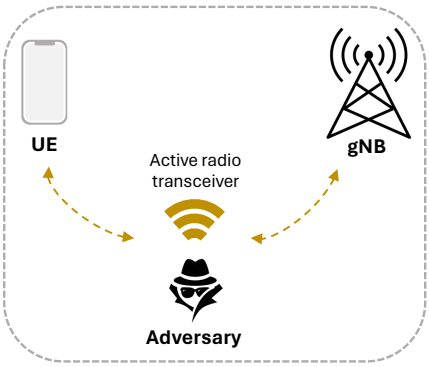
- Active attacker: in addition to the ability of a passive attacker, the active attacker can also send radio signals (e.g., spoofed signals or noise) into the open wireless channels. This type of adversary can launch radio jamming attacks, set up fake

base stations, or impersonate a UE towards the cellular network.

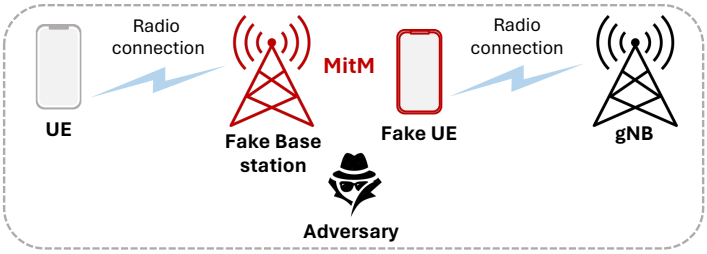
- Man-in-the-middle (MitM) attacker: it is considered as an online-version of the active attacker, where the attacker simultaneously impersonates a UE towards the network and a base station towards the UE. Therefore, the MitM attacker can establish and maintain an attacker-controlled relay transmission between the UE and the network.



(a) Passive attacker.



(b) Active attacker.



(c) MitM attacker.

Figure 2.24: Attacker models with different capabilities.

Depending on the aim of the attack, these can be classified into four main categories:

- Traceability: the adversary is able to determine the participation of a device in a specific communication and thus infer certain information about that device, i.e., location, type of exchanged information, communication frequency, etc.
- Impersonation: the adversary manages to impersonate one of the parties and communicate with the other on behalf of it.
- Denial/Degradation of Service (DoS): the adversary aims to compromise the availability of the system by interrupting temporarily or completely the service, or decreasing its performance.

- Bidding-down: the adversary tries to make UE and network entities believe that the other side does not support a security feature, even when both sides do support it. By indicating that a certain function, or a version of a function, is not supported, another function is used that may already have known vulnerabilities and exploits.

Although there are many attack variants depending on the attacker capability and aim of the attack [107], Table 2.2 summarizes the most important.

Attack	Description	Attacker	Type	Victim
Eavesdropping	An adversary could decode the essential UE information and network configuration details by sniffing the RAN	Passive	Traceability	UE/Network
RAN spoofing	An adversary is spoofing the RAN signals by transmitting a fake signal meant to pretend as an actual signal	Active	Impersonation	UE
Radio jamming	An adversary could disrupt the communication by deliberately jamming, blocking, or creating interference with the authorized wireless network	Active	DoS	UE/Network
Signaling storm	The adversary uses standard mechanism of the network CP to cause DoS, e.g., flooding the network with registration requests or the RA procedure	Active	DoS	Network
Replay attacks	The adversary first intercepts legitimate messages sent by one of the parties and later replays these messages with no or slight modifications to the other party	Active/ MitM	Impersonation/ DoS	UE/Network

Table 2.2: Summary of main existing threats and attacks against 5G network.

Part II

Publications

Chapter 3

Research outline

This chapter is structured in two sections. The first section describes the publications that support this thesis and associates them with the identified challenges and the thesis objectives. For each publication, their contributions to the state of the art are highlighted.

The second section presents the research methodology followed during the development of this thesis. This section also indicates the tools and equipment used in the research. For more details on the implementations made with these tools, refer to Appendix A.

3.1 Description of the publications

This section outlines the outcomes (research papers) arising from this thesis. These papers address the challenges identified and the objectives established in Section 1.2. Figure 3.1 illustrates the relationship between the challenges, the objectives and the corresponding outcomes. Each publication is represented as an individual block in the figure, indicating the chapter of this thesis in which it is included.

A brief summary of each of the papers that support this thesis is provided in the following subsections.

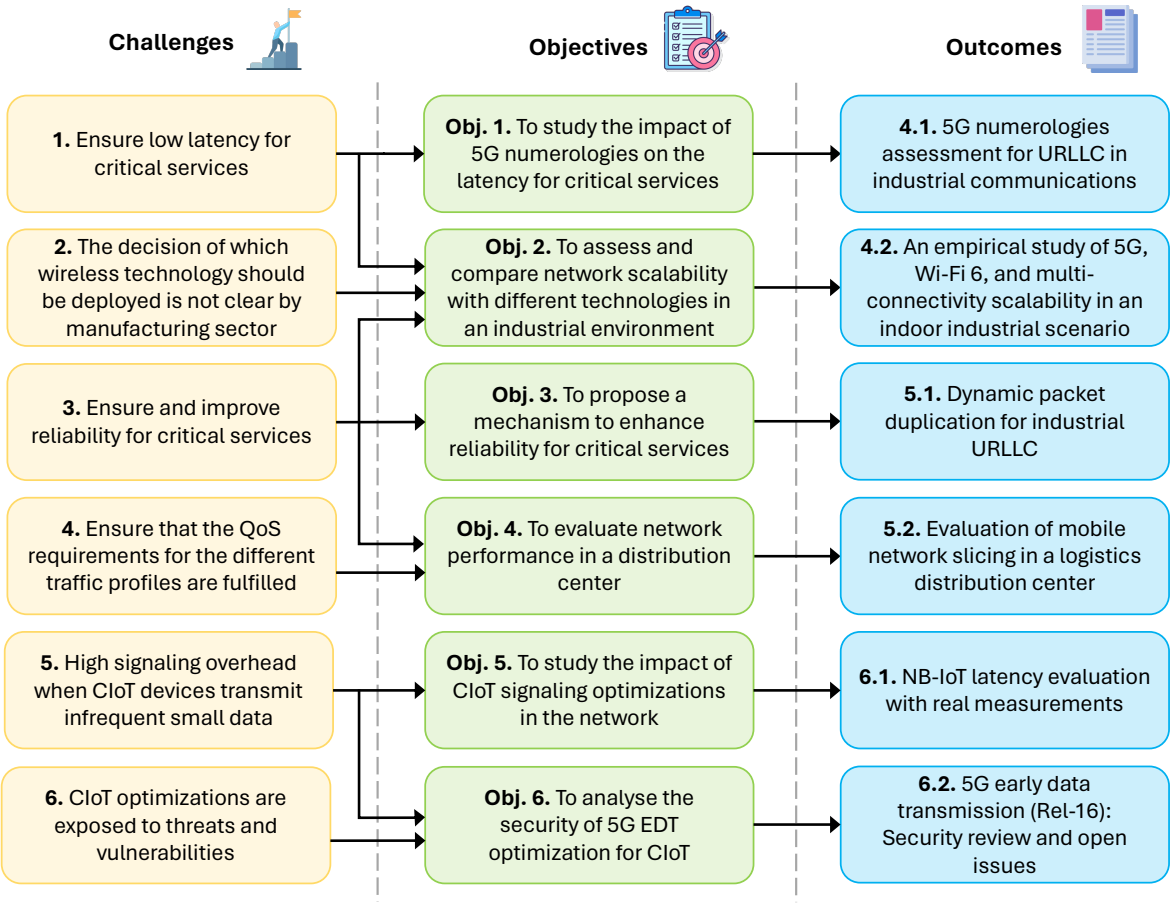


Figure 3.1: Challenges, objectives and outcomes.

3.1.1 5G numerologies assessment for URLLC in industrial communications

The advent of the 5G network has facilitated the introduction of novel features, enabling the development of new use cases and services. One of these features is the numerology, which allows a faster resource allocation process due to the use of shorter time slots. This feature is of particular importance for latency-constrained services such as those employed in the operation of AGVs, as it enables a reduction in the latency of their communications.

However, in industrial scenarios, the main challenge arises from the presence of concrete walls and large metallic machinery and structures, which can result in interference and multi-path propagation. Consequently, selecting an appropriate numerology is a challenging task, and it should be adapted to the radio conditions experienced.

Therefore, the first article presented in Chapter 4 is focused on assessing the impact of the numerology on the delay experienced at the radio link for a remote-control service

(AGVs communication), thus covering Obj. 1 of this thesis. More specifically, this study encompasses the assessment with varying packet sizes and channel conditions in a simulated factory environment, with a particular focus on identifying and analysing the outliers.

The results demonstrate that the assumption that a higher numerology leads to lower delay is not always true, particularly in NLOS conditions. In such cases, an intermediate numerology may be more suitable for this type of service.

3.1.2 An empirical study of 5G, Wi-Fi 6, and multi-connectivity scalability in an indoor industrial scenario

The manufacturing sector is adopting Industry 4.0 to enhance flexibility and reduce installation costs through the use of wireless connectivity. However, the question remains as to which wireless technology should be deployed in the factory to fulfil the requirements for next-generation applications such as Autonomous Mobile Robots (AMRs). While Wi-Fi technology is the most prevalent and easily deployed, the 5G network has been designed to support these industrial needs. It is therefore important to compare both technologies from a performance point of view, especially under different load conditions and with different number of devices. The use of multi-connectivity with different radio access technologies is also considered as a key enabler to fulfil the requirements of the most critical real-time applications.

Therefore, the second article presented in Chapter 4 is focused on the empirical assessment and comparison of the network scalability of 5G, Wi-Fi 6, and multi-connectivity in terms of latency and packet loss, thus covering Obj. 2 of this thesis. The work was carried out in the "5G Smart Production Lab" in Aalborg (Denmark), where different measurement campaigns were performed for different scenarios (static and mobility) and packet sizes.

The results obtained showed lower latencies with Wi-Fi in general, but large tails in the latency distribution, with a higher packet loss compared to 5G. On the other hand, 5G latency is very consistent with bounded tails, and low packet loss is obtained. With regard to scalability, 5G scales better than Wi-Fi, the latter being very affected by the number of devices transmitting data. Finally, the multi-connectivity solution showed an improved reliability and lower latencies in all evaluated cases.

3.1.3 Dynamic packet duplication for industrial URLLC

This work follows the line started with the first publication of Chapter 4. That is, when selecting an appropriate numerology to reduce the latency, the second step is to enhance the reliability for critical communications. One of the ways to improve the reliability of these communications is the use of multi-connectivity, particularly with the PD approach. Nevertheless, this solution comes at a cost in terms of redundancy, which can lead to an inappropriate use of network resources.

Therefore, to reduce the wastage of network resources, the first article of Chapter 5 proposes a dynamic PD algorithm based on ML, which determines whether PD is required at a specific data transmission to successfully send a critical message (Obj. 3). In particular, a latency estimator based on Random Forest (RF) was trained and evaluated, which decides when to duplicate a packet based on a latency threshold. The methodology presented was evaluated in a 5G simulator and the network performance was compared to different approaches: no duplication and a pure static PD.

The evaluation results demonstrated that the proposed dynamic PD algorithm reduced the number of duplicated packets sent by 81% while maintaining the same level of latency (i.e., the latency below the threshold) as a static PD technique. This reduction in the number of duplicated packets results in a more efficient usage of the network resources.

3.1.4 Evaluation of mobile network slicing in a logistics distribution center

The second article included in Chapter 5 addresses the problem of optimizing network resources for the different traffic profiles involved within a logistics distribution center scenario. In particular, these traffic profiles correspond to eMBB, URLLC, and mMTC, with distinct requirements in terms of latency, reliability, throughput, etc.

Specifically, this article first introduce a developed novel open-source simulator based on the ns-3 platform, with a realistic representation of a distribution center scenario, where different logistics activities are present. The communications of these activities have been modeled and used to estimate the performance of the different traffic profiles. As a result, the developed simulator serves as the foundation for evaluating the 5G network performance on smart logistics scenarios (Obj. 4).

Secondly, under the developed simulator, this work evaluates and compares the role of two 5G NS strategies in smart logistics: the use of a static slice with a balance division of network resources and the use of a dynamic slice that adapts the resources based on the traffic load, depending on the activity taken place. More specifically, this work evaluates these strategies in terms of QoS for the different traffic profiles, resulting in the following metrics: throughput for eMBB traffic, reliability for URLLC traffic, and the RA channel for mMTC traffic.

The results obtained show that a dynamic slice makes a more efficient usage of the network resources, improving the QoS for the different traffic profiles, even when there is a traffic peak on a specific profile. This improvement ranges from 6.48% to 95.65%, depending on the specific traffic profile and the evaluated metric.

3.1.5 NB-IoT latency evaluation with real measurements

Many optimizations have been proposed by the 3GPP for CIoT devices in order to improve the battery life and reduce the signaling exchange in the network. These optimizations started with the arrival of the Release 13, where the transmission via the CP was introduced. This optimization allowed to transmit data using the CP instead of the UP, thus avoiding the establishment of DRBs of the UP.

Moreover, with the arrival of Release 15, EDT optimization was introduced to support infrequent small data transmissions, supporting both the CP and UP transmission modes. The latter optimization allows the transmission of data during the RA procedure, with a significant reduction in the signaling exchange between the UE and the network, and without the need of an RRC state change (i.e., the UE transmits data in RRC Idle state).

Thus, the fist article of Chapter 6 is focused on the assessment and comparison of the aforementioned CIoT optimizations proposed by the 3GPP via the CP in terms of latency performance using the NB-IoT technology, covering Obj. 5 of this thesis. In particular, in this work a measurement campaign was performed with Amarisoft equipment (AMARI Crowdcell and AMARI UE Simbox) under different packet sizes and coverage levels.

The evaluation results showed lower latencies for EDT, particularly in the case of small packets, where a reduced TB is used, thereby being more efficient from a network perspective. Furthermore, it was demonstrated that EDT, in contrast to Release 13

optimization, fulfils the 3GPP latency requirement (10 seconds) for extreme coverage.

3.1.6 5G early data transmission (Rel-16): Security review and open issues

This section presents the second of the works carried out in relation to Chapter 6 of this thesis. In this case, this work extends the line started in the first publication of Chapter 6 by offering an in-depth description of the EDT optimization along with a security analysis of this mechanism. Thus, this work covers Obj. 6 of this thesis.

As mentioned above, EDT optimization was introduced in Release 15 to allow the transmission of data during the RA procedure. This optimization, intended particularly for infrequent and small data transmissions, aims to reduce the latency and the power consumption of the UEs. Nonetheless, despite the importance of this novelty and the general agreement about its effectiveness, there are few works in the literature that provide insight into its implementation and analyze the advantages and disadvantages of its two different implementation options (CP and UP).

Moreover, although security is recognized as a crucial aspect for the correct deployment of this technology, the literature lacks a review of the security issues and features of this mechanism. As a consequence of such a lack of works and the complexity of mobile network protocols, there is a divide between security experts and EDT researchers, that prevents the easy development of security schemes.

To overcome this important gap, this article offers a tutorial of EDT and its security, analyzing its main vulnerabilities and concluding with a set of recommendations for researchers and manufacturers. In particular, due to the simplifications in the protocols done by EDT, vulnerabilities such as packet injection, replay attacks and injection of fake values to disable EDT have been found.

3.2 Research methodology

The contributions reported in this thesis were conducted following a structured research methodology composed of different stages. Figure 3.2 depicts the different stages, which are described below.

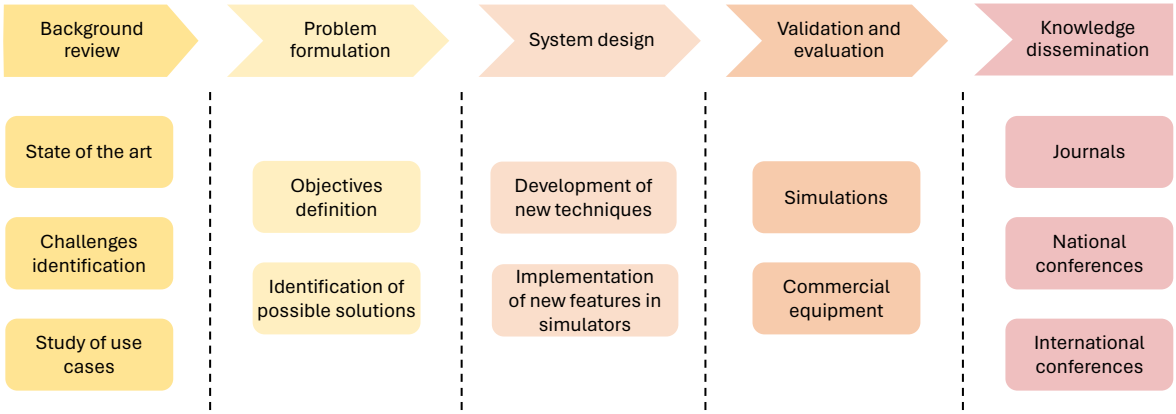


Figure 3.2: Research methodology.

1. **Background review**
   In the first stage of the research methodology, an exhaustive review of the background in the field of cellular network was performed, to clearly define which problems need to be solved. That is, the existing literature of the performance of cellular network focused on Industry 4.0 was reviewed. This resulted into the definition of the main challenges to be addressed and the study of different use cases in a factory.

2. **Problem formulation**
   In the second stage, the problem formulation is carried out for each challenge previously defined in the first stage. This stage comprises the definition of the objectives and the approaches to solve them.

3. **System design**
   The third stage of the methodology consisted in the development of the system and new techniques to overcome the challenges and objectives of the thesis, including the design and the implementation of new features in simulators.

4. **Validation and evaluation**
   Once the system has been designed, the proposed solutions and optimizations

were evaluated and validated either via simulations and with commercial equipment, in terms of network performance indicators:

- Simulations: For those works that require a controlled environment for the validation and evaluation of the features and methods designed, simulations were performed in the ns-3 simulator [108]. In particular, the 5G-LENA [109] module of the ns-3 simulator has been used in this thesis. 5G-LENA is an open-source module that provides a 5G NSA network and closely follows the 3GPP NR specifications, including features such as numerology support, frequency division multiplexing of numerology, beamforming, among others. Under the ns-3 framework and this module, many features were implemented focused on the particular environment of this thesis, which is the industrial scenario. Features such as the industrial channel and propagation loss in all its variants (3GPP 38.901) [110], the 5G DC feature with PD approach, slices with dedicated resources and assignation according to traffic requirements, a distribution center scenario with a realistic representation including its activities and applications, and the RRC Idle state, among others. A more in-depth detail of these contributions made to the simulator is provided in Appendix A. This resulted in a developed open-source simulator based on the ns-3 platform and the 5G-LENA module that can be found in [111].
- Commercial equipment: This thesis also evaluated the performance of the cellular network with different testbeds done with commercial equipment. In particular, Amarisoft equipment such as AMARI Callbox Classic [112] and AMARI UE Simbox [113] were used to evaluate the latency performance of CIoT signaling optimizations for NB-IoT under different radio conditions. On the other hand, measurement campaigns were performed in the "5G Smart Production Lab" [114] in Aalborg (Denmark), comparing the scalability performance of 5G, Wi-Fi 6, and multi-connectivity in terms of latency and packet loss in an indoor industrial scenario. These testbeds are described in detail in Appendix A.

During this phase it is necessary to analyze the results obtained from an statistical point of view. That is, to identify any unexpected effects that were not previously considered and, if necessary, make readjustment or reformulate the hypothesis. To this end, Python libraries and tools such as Scikit-learn [115–117], Pandas [118] or Numpy [119] have been used for data pre-processing.

5. **Knowledge dissemination**

   Finally, the most relevant results obtained during the thesis have been published in high impact journals and presented at national and international conferences.

Chapter 4

Performance evaluation

4.1 5G Numerologies Assessment for URLLC in Industrial Communications

D. Segura, E.J. Khatib, J. Munilla, and R. Barco, "5G Numerologies Assessment for URLLC in Industrial Communications," *Sensors*, vol. 21, no. 7, p. 2489, Apr. 2021. DOI: 10.3390/s21072489.

Abstract: The fifth-generation (5G) network is presented as one of the main options for Industry 4.0 connectivity. Ultra-Reliable and Low Latency Communications (URLLC) is the 5G service category used by critical mechanisms, with a millisecond end-to-end delay and reduced probability of failure. 5G defines new numerologies, together with mini-slots for a faster scheduling. The main challenge of this is to select the appropriate numerology according to radio conditions. This fact is very important in industrial scenarios, where the fundamental problems are interference and multipath propagation, due to the presence of concrete walls and large metallic machinery and structures. Therefore, this paper is focused on analyzing the impact of the numerology selection on the delay experienced at radio link level for a remote-control service. The study, which has been carried out in a simulated cellular factory environment, has been performed for different packet sizes and channel conditions, focusing on outliers. Evaluation results show that not always a higher numerology, with a shorter slot duration, is appropriate for this type of service, particularly under Non-Line-of-Sight (NLOS) conditions.

4.2 An Empirical Study of 5G, Wi-Fi 6, and Multi-Connectivity Scalability in an Indoor Industrial Scenario

D. Segura, S.B. Damsgaard, A. Kabaci, P. Mogensen, E.J. Khatib, and R. Barco, "An Empirical Study of 5G, Wi-Fi 6, and Multi-Connectivity Scalability in an Indoor Industrial Scenario," *IEEE Access*, vol. 12, pp. 74406-74416, May. 2024. DOI: 10.1109/ACCESS.2024.3404870.

Abstract: Industry 4.0 is being adopted by the manufacturing sector to improve the flexibility and reduce installation costs by the use of wireless connectivity. There is an open question of which wireless technology deployment should be used in the factory to fulfil the requirements for next-generation applications such as autonomous mobile robots. Wi-Fi technology is the most extended and easy to deploy, while the fifth generation of mobile networks (5G) has been designed to support these industrial needs. Therefore, it is important to compare both technologies from a performance point of view, especially under different load conditions and number of devices. The use of multi-connectivity between 5G and Wi-Fi can also be an option to fulfil the requirements for the most critical real-time applications. In this paper, we empirically measure the scalability of 5G, Wi-Fi and multi-connectivity in the "Aalborg University 5G Smart Production Lab" and compare them in terms of latency and packet loss with different packet sizes. We found that in general Wi-Fi obtains lower latencies but large tails in the distribution, with a higher packet loss compared to 5G. On the other hand, 5G latency is very consistent with bounded tails, and low packet loss is obtained. In terms of scalability, 5G scales better than Wi-Fi, the latter being very affected by the number of devices transmitting data. Finally, multi-connectivity showed an improved reliability and lower latencies in all evaluated cases.

Chapter 5

Optimization

5.1 Dynamic Packet Duplication for Industrial URLLC

D. Segura, E.J. Khatib, and R. Barco, "Dynamic Packet Duplication for Industrial URLLC," *Sensors*, vol. 22, no. 2, p. 587, Jan. 2022. DOI: 10.3390/s22020587.

Abstract: The fifth-generation (5G) network is presented as one of the main options for Industry 4.0 connectivity. To comply with critical messages, 5G offers the Ultra-Reliable and Low latency Communications (URLLC) service category with a millisecond end-to-end delay and reduced probability of failure. There are several approaches to achieve these requirements; however, these come at a cost in terms of redundancy, particularly the solutions based on multi-connectivity, such as Packet Duplication (PD). Specifically, this paper proposes a Machine Learning (ML) method to predict whether PD is required at a specific data transmission to successfully send a URLLC message. This paper is focused on reducing the resource usage with respect to pure static PD. The concept was evaluated on a 5G simulator, comparing between single connection, static PD and PD with the proposed prediction model. The evaluation results show that the prediction model reduced the number of packets sent with PD by 81% while maintaining the same level of latency as a static PD technique, which derives from a more efficient usage of the network resources.

5.2 Evaluation of Mobile Network Slicing in a Logistics Distribution Center

D. Segura, E.J. Khatib, and R. Barco, "Evaluation of Mobile Network Slicing in a Logistics Distribution Center," *IEEE Transactions on Network and Service Management*, Under review, 2024.

Abstract: Logistics is a key economic sector where any optimization that reduces costs or improves service has a great impact on society at large. Network Slicing (NS) is a technique that allows the creation of different independent networks with different dedicated resources on a shared physical infrastructure. This is particularly useful in scenarios where different applications with different requirements coexist. In this paper, a novel open-source simulator based on NS-3 has been developed with a realistic representation of a distribution center scenario, including the logistics activities that take place there. Under this developed simulator, the role of two 5G NS strategies in Smart Logistics is studied: the use of a static slice with a balance division of network resources and the use of a dynamic slice. These strategies have been evaluated in terms of Quality of Service (QoS) for different traffic profiles via simulations. Results show that a dynamic slice makes a more efficient usage of the network resources, improving the QoS for the different traffic profiles, even when there is a traffic peak. This improvement ranges from 6.48% to 95.65%, depending on the specific traffic profile and the evaluated metric.

Chapter 6

Cellular IoT evaluation and security analysis

6.1 NB-IoT latency evaluation with real measurements

D. Segura, E.J. Khatib, J. Munilla, and R. Barco, "NB-IoT latency evaluation with real measurements," in *2022 IEEE Workshop on Complexity in Engineering (COMPENG)*, Florence (Italy), Jul. 2022. DOI: 10.1109/COMPENG50184.2022.9905471.

Abstract: In the 3GPP LTE Release 13, NB-IoT was standardized to provide wide-area connectivity for IoT. To optimize network signaling and power consumption, control plane (CP) optimization was introduced. In Release 15, to support infrequent small data transmissions, Early Data Transmission (EDT) was also included, in which the data are sent during the random access procedure. Thus, this paper analyses the latency performance of the different NB-IoT optimizations for the CP. The study, carried out in a real device, has been performed for different packet sizes and coverage levels. Evaluation results show lower latencies for EDT, particularly with small packets, where a reduced transport block is used, being more efficient from a network point of view. Additionally, we verify that EDT, unlike Release 13 optimization, fulfills 3GPP latency requirement for extreme coverage.

6.2 5G Early Data Transmission (Rel-16): Security Review and Open Issues

D. Segura, J. Munilla, E.J. Khatib, and R. Barco, "5G Early Data Transmission (Rel-16): Security Review and Open Issues," *IEEE Access*, vol. 10, pp. 93289–93308, Sep. 2022. DOI: 10.1109/ACCESS.2022.3203722.

Abstract: The fifth-generation technology is called to support the next generation of wireless services and realize the "Internet of Everything" through Machine-Type Communications and Cellular Internet of Things optimizations. As part of these optimizations, Release 15 introduced a new mechanism, known as Early Data Transmission (EDT), that allows the transmission of data during the Random Access procedure. This feature, intended particularly for infrequent and small data transmissions, aims to reduce the latency and the power consumption of user equipments. Nonetheless, despite the importance of this novelty and the general agreement about its effectiveness, there are few papers in the literature that provide insight into its implementation and analyze the advantages and disadvantages of its two different implementation options (Control and User Plane). Moreover, although security is recognized as a crucial aspect for the correct deployment of this technology, we have not found any paper that reviews the security issues and features of this mechanism. As a consequence of such a lack of papers and the complexity of mobile network protocols, there is a divide between security experts and EDT researchers, that prevents the easy development of security schemes. To overcome this important gap, this paper offers a tutorial of EDT and its security, analyzing its main vulnerabilities and concluding with a set of recommendations for researchers and manufacturers. In particular, due to the simplifications in the protocols done by EDT, vulnerabilities such as packet injection, replay attacks and injection of fake values to disable EDT have been found.

Part III

Achievements

Chapter 7

Conclusions

This chapter provides a summary of the research conducted during this thesis. For this purpose, this chapter is divided into three sections. Section 7.1 provides a review of the objectives pursued in this thesis, highlighting the main contributions of each of them. Section 7.2 suggests some lines of future work related to the research carried out. Finally, Section 7.3 shows a list of publications as well as other activities related to this thesis.

7.1 Contributions

This thesis aims at assessing and improving the performance of mobile networks in the Industry 4.0 paradigm. To this end, a set of challenges in the industrial scenario have been identified and required objectives to solve these challenges have been defined. A total of six objectives have been established through this work, which are distributed as follows. Obj. 1 and 2 are related to the performance assessment of the network in an indoor industrial environment. Obj. 3 and 4 refer to the development of optimization algorithms to improve network performance. Finally, Obj. 5 and 6 aim to cover CIoT signaling optimizations, first assessing the impact of these optimizations in the network and then providing a security analysis of the latest optimization proposed by the 3GPP. The contributions related to each of these objectives are presented below:

Obj. 1. To study the impact of 5G numerologies on the latency for critical services.

- An analysis on the impact of the different 5G numerology configurations on

users' latency has been performed. In this analysis, a more detailed study than in those found in the state of the art has been performed. The 5G numerologies have been evaluated under two different channel conditions (LOS and NLOS) and with different packet sizes for an AGV use case.

– The study has been carried out in a 5G simulated environment. The results showed that the numerology selection is not trivial, and an intermediate value is more suitable under NLOS conditions. This study opens the way to algorithms that can be used to dynamically adjust the numerology configuration in the network for a better performance.

Obj. 2. To assess and compare network scalability with different technologies in an industrial environment.

– Following this objective, an empirical assessment has been carried out with different number of devices, packet sizes and scenarios to evaluate the network performance in terms of latency and packet loss. In particular, the technologies selected to compare their performance have been 5G, Wi-Fi 6, and the use of multi-connectivity between both with a PD approach.

– More specifically, measurement campaigns were performed with commercial equipment in the "5G Smart Production Lab" at Aalborg University (Denmark), which consists of a small-scale indoor industrial factory environment composed of two halls and a wide range of industrial manufacturing and production equipment.

– As a result of the measurement campaigns, it has been demonstrated that the 5G technology provides lower tails in the latency distribution and is more reliable than Wi-Fi 6. On the other hand, the multi-connectivity solution demonstrated a significant reduction in the latency tails and a zero packet loss, being very effective to fulfil the use cases with very restrictive latency and reliability requirements.

Obj. 3. To propose a mechanism to enhance reliability for critical services.

– To meet this objective, an algorithm based on ML to dynamically activate PD in an industrial environment has been designed. This algorithm relies on network metrics such as the Signal to Interference plus Noise Ratio (SINR), the modulation index, and the HARQ feedback to predict the latency. The

output of the predictor is used for the PD decision in the downlink direction, based on a latency threshold.

- The latency predictor was trained with the RF algorithm, and the performance of the proposed algorithm has been validated under different tests conducted in a 5G simulated environment. Under this simulator, the DC feature with PD approach was implemented, as described in Appendix A.
- The performance of the algorithm has been compared with other approaches in the state of the art, thus demonstrating that the proposed solution is able to achieve better results and minimize resource wastage in the network.

Obj. 4. To evaluate the network performance in a distribution center.

- The contributions corresponding to this objective are, firstly, the design and implementation of an open-source simulator based on the ns-3 framework and the 5G-LENA module which includes new features to support the assessment of the network in a distribution center. In particular, features such as a distribution center scenario, the activities involved there, the resource allocation per slice, and the industrial channel and propagation loss model have been implemented.
- Secondly, once the above features were implemented, two NS strategies using the 5G network have been evaluated under different logistics activities. These NS strategies consist in the use of a static slice with a balanced division of network resources, and the use of a slice that dynamically adjust its size depending on the activity taken place.
- Finally, the QoS performance provided by these NS strategies across various traffic profiles have been evaluated via simulations, and the results demonstrated that a dynamic slice improves the QoS especially under high traffic load, whereas the static slice performs well when the traffic load is low.

Obj. 5. To study the impact of CIoT signaling optimizations in the network.

- In relation to this objective, an analysis on the impact of the different CIoT signaling optimizations proposed by the 3GPP on user's latency has been performed. Specifically, in this study the NB-IoT technology has been used for the evaluation of these optimizations via the CP.

- The study has been carried out with commercial equipment from Amarisoft, with which several measurement campaigns were performed under different coverage levels and packet sizes.
- From the results of these measurements, it has been demonstrated that EDT, unlike Release 13 optimization, fulfils the 3GPP latency requirement for infrequent small data transmissions under extreme coverage level.

Obj. 6. To analyse the security of 5G EDT optimization for CIoT.

- A comprehensive study of the EDT optimization in CIoT has been provided as a final contribution. In this study, the EDT feature has been described in detail for both supported operation modes, CP and UP.
- Moreover, a security analysis of this feature has been provided, extracting the main vulnerabilities found in each of its operation modes. Specifically, vulnerabilities such as packet injection, replay attacks and the injection of fake values to disable EDT have been found.
- Finally, after the exhaustive security analysis, a set of recommendations for researchers and manufacturers have been provided, which include solutions to patch these vulnerabilities in future 3GPP releases, and which operation mode is more suitable to use.

7.2 Future work

Possible lines of research that might continue the work in this thesis are the following:

- Regarding the 5G numerologies assessment, this thesis has conducted a study that aims to serve as a guide for a better understanding of which numerology configuration is more suitable in an industrial environment for critical services. One of the main lines to be addressed in this context would be the study of other mechanisms such as preemptive scheduling and resource reservation to complement the numerology selection. Another line would be the developing of algorithms to dynamically select the proper numerology according to radio conditions.
- In this thesis, a study of the network scalability with different technologies have been conducted in an indoor industrial scenario, making it easier for the manufacturing sector to opt for one technology or another based on the network

performance and their business use case. A possible future line to extend this work would be the integration of spectrum interference on the study, to better provide and compare the performance of the network with and without interference. Another line would be the enhancement of the multi-RAT tool to take into account network metrics, thereby enabling the PD only when necessary. This would result in a more efficient usage of network resources.

- The proposed algorithm based on ML to dynamically duplicate packets has been evaluated and has demonstrated its effectiveness in reducing resource wastage while improving the reliability. Some aspects that have not been covered in this thesis and could be the subject of future study are the implementation of this algorithm in a commercial network, the selection of the proper SN, the required model update frequency due to network or environment changes, and the study of using Federated Learning (FL) for the creation and enrichment of the model.

- The performance of the network in a distribution center has been evaluated in this thesis with a customized open-source simulator. One of the main lines to be addressed in this context would be the study of linking wireless performance with the production performance. This would further demostrate the impact of network optimizations on the vertical scenario.

- Regarding the optimization of CIoT transmissions, this thesis has covered CIoT optimizations up to Release 16, the latest one corresponding to the EDT feature. A similar mechanism to EDT has been proposed in native 5G, namely two-step RACH. A possible future line to extend this work would be the comparison of these two features from an analytical and a performance point of view. Moreover, a new type of device has been proposed by the 3GPP in the Release 17, namely NR RedCap. These devices are focused on use cases such as wearables, video surveillance and industrial IoT. A future line would be to consider RedCap devices to further study the performance and the energy saving in the network.

- Finally, in terms of network security, multiple future lines of research can be launched. First, with the arrival of Open-RAN networks, where NFs are virtualized and standard open interfaces between virtualized network elements are used, new security challenges that need to be analyzed and solved arise. Secondly, the massive use of AI algorithms expected in future networks posses new threats into the models such as data poisoning, model evasion or model inversion that need

to be analysed, and defense mechanisms need to be developed and deployed in the network.

7.3 Publications and projects

The following subsections present the publications and activities related to this thesis.

7.3.1 Journals

Publication arising from this thesis

The work carried out in this thesis has resulted in four papers published in high impact journals plus one in the process of revision, listed as follows.

[I] D. Segura, E.J. Khatib, J. Munilla, and R. Barco, "5G Numerologies Assessment for URLLC in Industrial Communications," *Sensors*, vol. 21, no. 7, p. 2489, Apr. 2021. DOI: 10.3390/s21072489.

[II] D. Segura, E.J. Khatib, and R. Barco, "Dynamic Packet Duplication for Industrial URLLC," *Sensors*, vol. 22, no. 2, p. 587, Jan. 2022. DOI: 10.3390/s22020587.

[III] D. Segura, J. Munilla, E.J. Khatib, and R. Barco, "5G Early Data Transmission (Rel-16): Security Review and Open Issues," *IEEE Access*, vol. 10, pp. 93289–93308, Sep. 2022. DOI: 10.1109/ACCESS.2022.3203722.

[IV] D. Segura, E.J. Khatib, and R. Barco, "Evaluation of Mobile Network Slicing in a Logistics Distribution Center," *IEEE Transactions on Network and Service Management*, Under review, 2024.

[V] D. Segura, S.B. Damsgaard, A. Kabaci, P. Mogensen, E.J. Khatib, and R. Barco, "An Empirical Study of 5G, Wi-Fi 6, and Multi-Connectivity Scalability in an Indoor Industrial Scenario," *IEEE Access*, vol. 12, pp. 74406-74416, May. 2024. DOI: 10.1109/ACCESS.2024.3404870.

7.3.2 Conferences and Workshops

Conferences arising from this thesis

Several works have also been presented at national and international conferences, as shown below.

[VI] D. Segura, E.J. Khatib, and R. Barco, "Evaluación de numerologías 5G para URLLC," in *XXXV Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2020)*, Málaga (España), Sept. 2020.

[VII] D. Segura, E.J. Khatib, J. Munilla, and R. Barco, "Evaluación de los modos de conexión para NB-IoT," in *XXXVI Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2021)*, Vigo (España), Sept. 2021.

[VIII] D. Segura, E.J. Khatib, J. Munilla, and R. Barco, "NB-IoT latency evaluation with real measurements," in *2022 IEEE Workshop on Complexity in Engineering (COMPENG)*, Florence (Italy), Jul. 2022.
DOI: 10.1109/COMPENG50184.2022.9905471.

[IX] D. Segura, E.J. Khatib, J. Munilla, and R. Barco, "Evaluación de la latencia de NB-IoT con medidas reales," in *XXXVII Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2022)*, Málaga (España), Sept. 2022.

[X] D. Segura, S.B. Damsgaard, P. Mogensen, E.J. Khatib, and R. Barco, "Comparativa empírica del rendimiento de 5G y Wi-Fi en un escenario industrial de interior," in *XXXVIII Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2023)*, Cáceres (Spain), Sep. 2023.

[XI] D. Segura, H.Q. Luo-Chen, C. Baena, E.J. Khatib, S. Fortes, and R. Barco, "Testbed para la evaluación de los ataques de envenenamiento y evasión en un servicio E2E," in *XXXIX Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2024)*, Cuenca (España), Sept. 2024.

Conferences related to this thesis

[XII] J. Llanes, E.J. Khatib, D. Segura, and R. Barco, "Seguridad en B5G/6G," in *XXXVII Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2022)*, Málaga (Spain), Sep. 2022.

[**XIII**] S.B. Damsgaard, D. Segura, M.F. Andersen, S.A. Markussen, S. Barbera, I. Rodríguez, and P. Mogensen, "Commercial 5G NPN and PN Deployment Options for Industrial Manufacturing: An Empirical Study of Performance and Complexity Tradeoffs," in *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Toronto (Canada), Sep. 2023. DOI: 10.1109/PIMRC56721.2023.10293869.

[**XIV**] H.Q. Luo-Chen, D. Segura, C. Baena, E.J. Khatib, and R. Barco, "Detection of anomalous samples based on automatic thresholds," in *2024 IEEE Workshop on Complexity in Engineering (COMPENG)*, Florence (Italy), Jul. 2024.

[**XV**] H.Q. Luo-Chen, D. Segura, C. Baena, E.J. Khatib, S. Fortes, and R. Barco, "Alteración de datos E2E: impacto de un ataque de envenenamiento y evasión en una red celular," in *XXXIX Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2024)*, Cuenca (España), Sept. 2024.

[**XVI**] C.S. Álvarez-Merino, D. Segura, C. Baena, E.J. Khatib, and R. Barco, "Infraestructura para la monitorización del consumo energético en redes b5G/6G," in *XXXIX Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2024)*, Cuenca (España), Sept. 2024.

[**XVII**] E.J. Khatib, D. Segura, A. Tarrías, and R. Barco, "Estudio del ataque de cadena de suministro sobre XZ utils y sus consecuencias en telecomunicaciones," in *XXXIX Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2024)*, Cuenca (España), Sept. 2024.

7.3.3 Related projects

This thesis has contributed to the following projects:

- National projects:
  - EDEL4.0: Seguridad y fiabilidad en las comunicaciones 5G/IoT para la Industria 4.0. Número de proyecto UMA18-FEDERJA-172, receiving funds from Junta de Andalucia and European Comission, within the framework of "Proyectos de I+D+i en el marco del Programa Operativo FEDER Andalucia 2014-2020".

– PENTA: Provisión de servicios PPDR a través de Nuevas Tecnologías de Acceso radio. Número de proyecto PY18-4647, receiving funds from Junta de Andalucía and European Comission, within the framework of "Plan Andaluz de Investigación, Desarrollo e Innovación (PAIDI 2020)".

– MAORI: Massive AI for the OpenRadIo b5G/6G network. Project number TSI-063000-2021-72, receiving funds from Ministerio de Asuntos Económicos y Transformación Digital and European Union - NextGenerationEU within the framework "Recuperación, Transformación, y Resiliencia".

7.3.4 Research stay

This thesis involved a five-month stay in Aalborg (Denmark), collaborating with Aalborg University on several measurement campaigns with 5G, Wi-Fi 6, and multi-connectivity in an industrial environment. The stay took place between February 2023 and June 2023 and was supervised by Preben E. Mogensen.

Appendices

Appendix A

Assessment tools and testbeds

A.1 5G LENA ns-3 simulator

NS-3 is an open-source network simulation software with discrete events, and it is composed of different modules developed in C++, each of them providing a particular function [108]. Among the functionalities implemented with this simulator is the 5G-LENA module [109], which is oriented to 5G NSA networks.

The 5G-LENA module is focused on the new 5G NR specifications of the 3GPP standard, particularly on the Release 15. This module adds some functionalities adapted to 5G in the PHY and MAC layers. It supports both the millimeter FR (FR2) and the non-millimeter FR (FR1), as well as beamforming, modulation schemes and error recovery (HARQ) implementations, among others. The most important features of this module are listed:

- Support of 5G numerologies. It is possible to select the numerologies from 0 to 4, which corresponds to Release 15 specification.

- Multiplexing of different Bandwidth Parts (BWPs). Allows to divide the total bandwidth into different parts, with different configurations (e.g., different numerology). This is useful for multiplexing different services with different requirements.

- Scheduler based on OFDMA and Time Division Multiple Access (TDMA), with the typical scheduling algorithms such as round robin, proportional fair, etc.

- Propagation and channel model based on the 3GPP 38.901 standard [110]. Implements the propagation and channel models for rural, urban and office scenarios.

A.1.1 Author's contribution

Throughout the development of this thesis, many features have been included using as a baseline the NS-3 simulator and the 5G-LENA module, with the aim to assess network performance in an industrial environment for those works carried out with simulations. This resulted in an open-source simulator with the code available on Github [111]. The different enhancements and features developed are described below.

1. Industrial channel model and propagation loss

The 5G-LENA module does not provide the industrial scenario. Therefore, the first feature added to the simulator was the inclusion of the industrial channel and propagation loss model defined in the Release 16 of the 3GPP standard [110]. The Indoor Factory (InF) scenario focuses on factory halls of varying sizes and with varying levels of density of clutter, e.g., machinery, assembly lines, storage shelves, etc. In particular, four different industrial scenarios are defined based on the clutter density and base station height:

- InF with Sparse clutter and Low base station height (InF-SL). It is characterized by having a factory ceiling height of between 5-25 meters composed of large machinery with regular metal surfaces (e.g., several mixed production areas with open spaces and storage/commissioning areas). The typical size of these machinery is 10 meters and the base station is located at a height below the average height of the machinery.

- InF with Dense clutter and Low base station height (InF-DL). It is characterized by having a factory ceiling height of between 5-15 meters and, composed of small and medium-sized machinery, and metal objects with irregular structure (e.g., assembly and production lines surrounded by small mixed machinery). The typical size of these machinery is 2 meters and the base station is located at a height below the average height of the machinery.

- InF with Sparse clutter and High base station height (InF-SH). Same scenario as InF-SL, but with the base station height being above the height of the machinery.

- InF with Dense clutter and High base station height (InF-DH). Same scenario as InF-DL, but with the base station height being above the height of the machinery.

With the aim of providing maximum flexibility to perform simulations and allowing to recreate different scenarios, all InF scenarios were implemented and Table A.1 shows the different parameters that can be modified in the simulator.

Scenario	Parameter	Value	Description
All	**InFTotalSurface**	Any	Represents the total area of the factory in squared meters
All	**InFVolume**	Any	Represents the total surface of the factory in cubic meters
InF-SL, InF-SH	**LowClutterDensity**	0 to 0.39	Percentage of area occupied by clutter
InF-DL, InF-DH	**HighClutterDensity**	0.4 to 1	Percentage of area occupied by clutter
InF-SH, InF-DH	**ClutterHeight**	0 to 10	Clutter height in meters

Table A.1: Configurable simulator parameters according to the industrial scenario.

2. RRC Idle state

In 5G-LENA, by default, when starting a simulation, all UEs move from RRC Idle state to RRC Connected state, performing the RA procedure and establishing a DRB, even when there are UEs that are not going to transmit any data. This causes radio resources to be consumed, which could be used by other UEs that are transmitting data. In order to make the simulations more realistic, the possibility of establishing the connection later (just when the UE has data to send) was implemented in the simulator and, in addition, the inclusion of the transition from RRC Connected to RRC Idle state after an inactivity period of the UE.

To achieve this goal, the code associated to the RRC layer have been modified, both in the UE and base station, together with the NAS layer and part of the network core. Figure A.1 shows the different states through which the UE transits and the modifications made are highlighted in red:

1. When the RRC Idle connection mode is activated, the UE remains in the IDLE_CAMPED_NORMALLY state, without sending the preamble.

2. The UE switches to CONNECTED_NORMALLY state when alerted from the NAS layer that the UE has data to transmit. When this occurs, the RA preamble is sent, in addition to performing the steps from IDLE_CAMPED_NORMALLY state to CONNECTED_NORMALLY state, where, once the RRC connection is established, the packet shall be sent over the corresponding DRB.

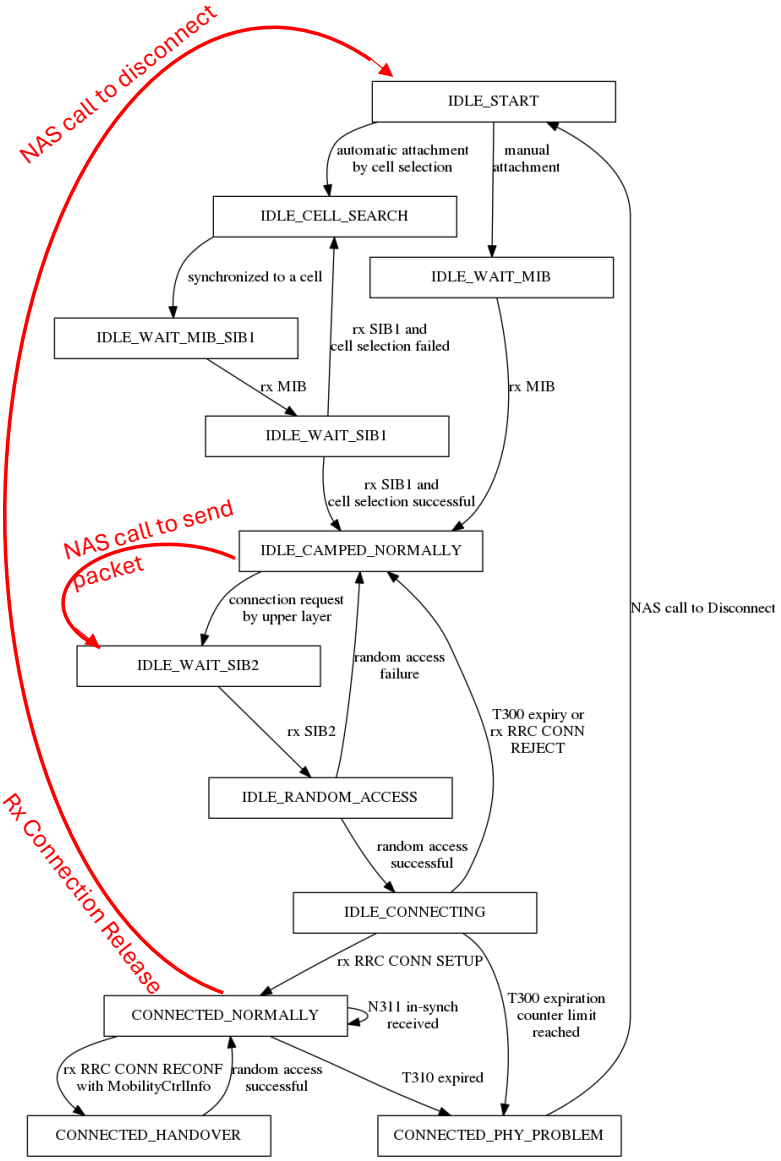


Figure A.1: RRC layer state machine at the UE.

3. The NAS layer accumulates user packets in a buffer while the RRC connection is being established.

4. When the UE does not transmit any data during a time period, it receives a signaling message from the network (RRC Connection Release), which causes the UE context in the network core, the SRBs (SRB0, SRB1) and DRBs to be removed. It also forces the UE to go to IDLE_START state and to remain in the IDLE_CAMPED_NORMALLY state.

5. In case of reconnection from the UE, the same process will be repeated from step 2.

Figure A.2 shows the different states that the UE context stored in the base station goes through each time a connection establishment request is received, with the implemented modifications highlighted in red. In this case, only the UE inactivity detection has been implemented, which causes its context to be removed. In general, the steps to be followed are:

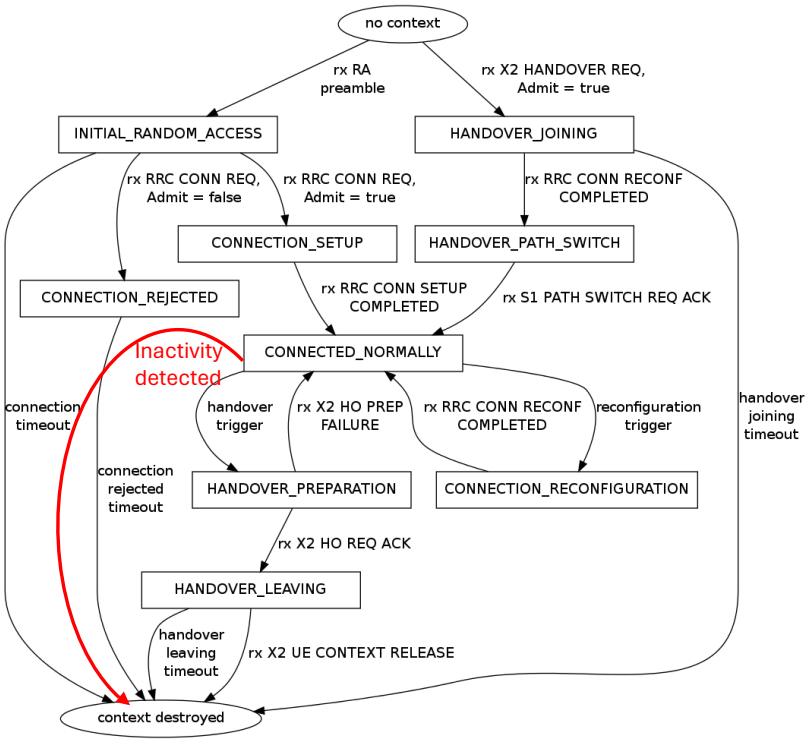


Figure A.2: RRC layer state machine at the base station for each UE.

1. When a packet is received in the CONNECTED_NORMALLY state (this state is reached after a successful establishment of the RRC connection), an inactivity timer is started and its value is configurable.

2. In case the network continues receiving packets from the UE, this timer value is reset. Otherwise, when the inactivity timer expires, the UE context is removed.

3. Before proceeding to remove the UE context, the network sends an RRC Connection Release message to the UE, which moves the UE from RRC Connected to RRC Idle state.

4. Finally, the base station communicates with the network core and all bearers associated with that UE are deleted.

Table A.2 shows the different configurable parameters to activate RRC Idle mode and to set the inactivity timer.

Parameter	Value	Description
UseIdealConnection	**Boolean** (True, False)	Indicates whether the mode used is the original simulator mode (True) or the one implemented with RRC Idle mode (False)
InactivityTimer	**TimeValue** (Value in seconds)	Indicates the inactivity time configured in the gNB to switch a UE to RRC Idle state when the timer expires

Table A.2: Configurable parameters to activate RRC Idle mode.

3. Dual Connectivity and Packet Duplication feature

The DC feature has been implemented in the simulator. This feature allows the UE to be connected with two base stations simultaneously. In order to support this feature in the simulator, two 5G network devices have been inserted in the same node, each of them associated and connected to the corresponding gNB and with their respective band configuration. On the other hand, the possibility of connecting a UE with two different technologies simultaneously, in this case LTE and 5G, has also been included. The implementation is equivalent to MR-DC, allowing to test different DC configurations, such as LTE as MN and 5G as SN, or both nodes being 5G.

Once DC has been inserted in a node, it is essential to implement an application that is capable of managing two sockets (each of them connected to the target application), otherwise, the UE will only send data over the primary socket and one of the links will be completely unusable. The implementation details of this application are described in the next subsection. On the other hand, the DC solution with the PD approach for the downlink has been included with the 5G technology, being used in a journal article of this thesis ([**II**]) corresponding to Chapter 5. The operation and implementation of this approach is described below.

1. Upon arrival of a packet for a UE at the MN from the network core, it is processed and a PDCP header is added, as indicated in the standard. Thus, both packets will contain the same identifier and the duplication can be detected at the receiver.

2. Once the PDCP header has been processed and added, the duplicated packet is sent thought the Xn interface to the SN. MN and SN are always the same throughout the simulation and the necessary functions have been added so that in the simulation configuration file the pairing (i.e., who acts as MN and who as

SN, as well as activating the Xn interface between them) is carried out prior to the start of the simulation. These parameters are described in Table A.3.

3. Both packets are processed independently by the lower layers (RLC, MAC, and PHY) at each node. Upon arrival at the UE, the first packet received is sent to the upper layers and, when the duplicate packet is detected (based on the sequence number), it is discarded and not sent to the upper layers.

4. Finally, the packet reaches the application layer, where it is processed and the corresponding traces are obtained.

Function	Parameter	Description
SetMasterGnb	**Boolean** (True, False)	Indicates whether the gNB acts as a master node in the case of DC
SetSecondaryGnb	**Boolean** (True, False)	Indicates whether the gNB acts as a secondary node in the case of DC
ActivatePacketDuplication	**sourceRnti**: UE RNTI in master node; **sourceCellId**: master cell identifier; **targetCellId**: secondary cell identifier; **targetRnti**: UE RNTI in secondary node	The master node activates PD for the indicated RNTI
DeActivatePacketDuplication	**sourceRnti**: UE RNTI in the master node	The master node deactivates PD for the indicated RNTI

Table A.3: Simulator functions implemented at RRC layer for the establishment of DC and PD.

4. Application module for DC

Two new modules have been included in the simulator, which are responsible for providing a User Datagram Protocol (UDP) uplink application with two different sockets, each one connected with the corresponding interface when DC feature is used. These modules are namely DualSocket and DualSocket5G.

This application allows the user data to be sent to the network, either via one interface or the other, or via both network interfaces. In this case, the operation of both modules is equivalent, with the only difference being the type of connection of the network interface (LTE-5G in DualSocket module and 5G-5G in the DualSocket5G module).

Figure A.3 depicts a visual scheme of the application. When a new packet arrives, an algorithm with a set of functions determines which network interface is selected.

In this case, if a number of conditions are met, the selected interface will be the best between the primary and secondary ones. Alternatively, the packet could be sent duplicated on both interfaces. Once the decision has been made, the packet will be sent to the lower layers.

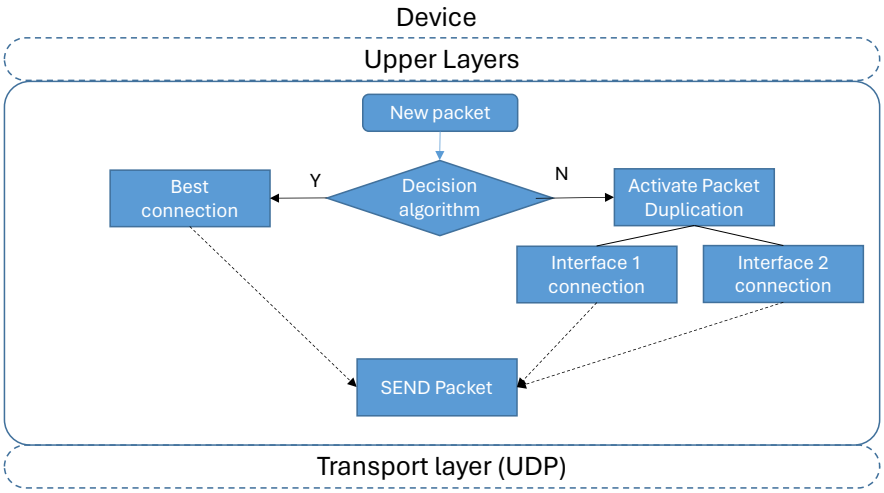


Figure A.3: Visual scheme of the UDP application.

On the other hand, Figure A.4 shows the operation of the decision algorithm to send the packet through one interface or another. The algorithm uses ML techniques to predict whether it is necessary to activate PD or, on the contrary, to choose the best connection. This algorithm has a number of inputs that are updated based on how packets arrive on that interface from the network (e.g., SINR, modulation used, delay obtained, etc.). In addition, feedback is provided on how the packet arrived at its destination (End-to-End (E2E) feedback).

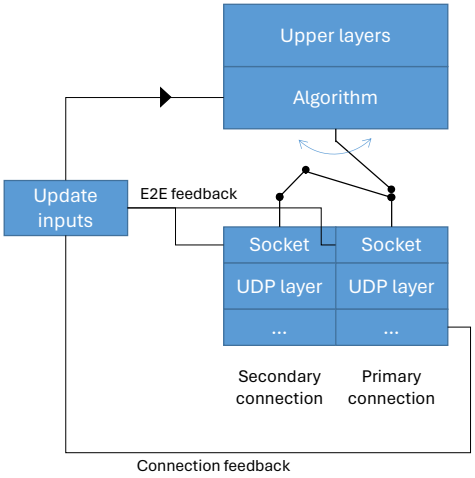


Figure A.4: Visual scheme of the decision algorithm.

5. A distribution center scenario

The enhancements made to the simulator also includes a realistic representation of a distribution center scenario, including the logistics activities that take place there. The details of this implementation are described in Chapter 5, corresponding to a journal article of this thesis ([**IV**]).

A.2 Random access simulator for cellular devices

As part of the journal publication [**IV**] of this thesis, a RA simulator for cellular devices has been developed, resulting in an open-source simulator with the code available on Github [120].

This simulator has been implemented on Python and enables the evaluation of the performance of the contention-based RA channel for 5G cellular networks. The implementation is based on the 3GPP standard [121–123] and the parameters that can be modified are described in Table A.4.

Parameter	Type	Description
PRACH Configuration Index	**Integer** ([0, 1, 2, 3, 4, 5])	Defines the periodicity of the RA slots. The periodicity ranges between a maximum of one RA slot per subframe to a minimum of one RA slot every two frames
Number of available preambles	**Integer**	Corresponds to the number of preambles reserved for the contention-based procedure
preambleTransMax	**Integer**	Maximum number of preamble attempts for a device before declaring RA failure
RAR Window Size	**Integer**	Time window to monitor the RA response
Backoff Indicator	**Integer**	Random backoff that is used by the UEs to wait a time when a preamble collision occurs before retrying a new access attempt. This backoff is intended to disperse the access attempts and thus, reduce the probability of preamble collision

Table A.4: Simulator parameters.

The simulator extracts the following metrics from the simulations:

- Blocking probability: probability that a device reaches the maximum number of transmission attempts (*preambleTransMax*) and is unable to complete an access

process.

- Average number of preamble retransmissions: measure the average number of preamble retransmissions required to have a success access.
- Access delay: time elapsed between the transmission of the first preamble and the reception of the Random Access Response (RAR) by the device. Only for devices that do not reach the maximum number of transmission attempts.

A.3 AAU 5G Smart Production Lab

The AAU 5G Smart Production Lab consists of a small-scale industrial factory environment of approximately 1250 m^2 and a wide range of industrial manufacturing and production equipment from different vendors, such as robotics arms, welding machines, production lines, AMRs, etc. The lab is equipped with multiple networks from different wireless technologies, such as private deployments of LTE, 5G NR, and Wi-Fi 6; and dedicated operator-managed network slices of LTE and 5G NR. The lab also contains a dedicated positioning system based on Ultra-Wide Band (UWB).

As part of the measurement campaigns performed in publication **[V]** of this thesis, a testbed was created to perform latency measurements with 5G SA and Wi-Fi 6 technologies. The testbed was composed of an Intel NUC [124], equipped with an Intel M2 Wi-Fi 6 AX200 card, and running Arch Linux; and with a 5G modem (Simcom SIM8202G-M2 [125]) connected to the NUC through a M2 to USB3 adapter. Figure A.5 illustrates the equipment used and the data path for each technology.

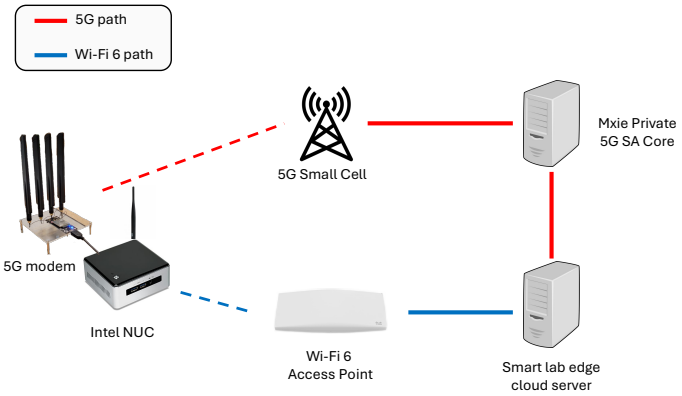


Figure A.5: Testbed in the AAU 5G Smart Production Lab.

For mobility measurements, a MiR200 AMR [126] was used, with the aforementioned equipment placed on top of the AMR. The AMR allowed to perform different

reproducible mobility tests within the AAU 5G Smart Production Lab, which guarantees a consistency on the measurements.

For the latency assessment, the Linux ping tool was used on the NUC, in which the interface for data transmission was indicated via command line. Python scripts were developed to automate the process of configuring devices and interfaces, launching multiple measurements to obtain statistical data, controlling the AMR robot path and collecting the data from the logs.

A.3.1 Mpconn tool

For the multi-connectivity measurements performed in the journal article [**V**] of this thesis, a tool developed at Aalborg University was used, namely mpconn [127]. This tool duplicates the packets at Layer 3 and sends them over IP in Layer 4 (UDP) packets through 5G and Wi-Fi technologies. An overview of the functionality of this tool is provided in Figure A.6, where a ping request packet is sent from a NUC to a server.

First, a virtual tunnel IP address is created in the NUC and in the server, where an instance of mpconn is running. This virtual tunnel IP address is used to communicate the mpconn instance running in the NUC with the mpconn instance running in the server. Then, for each packet sent by the NUC, a custom UDP packet adding a sequence number is created, and the packet is duplicated and sent via both interfaces. At the receiver side (server), the first packet received from the client is decapsulated, while the duplicated packet received is discarded based on the sequence number. In the example illustrated in Figure A.6, the packet duplication process for the ping reply will be the same but inverted.

A.4 Testbed for the evaluation of CIoT optimizations

The measurement campaigns in publications [**VIII**] and [**IX**] of this thesis were performed using a testbed with Amarisoft equipment. Specifically, the AMARI Callbox Classic and AMARI UE Simbox solutions from Amarisoft were used, and Figure A.7 illustrates these solutions and the different configurations that can be used.

Both devices have a completely software-based network implementation, where different network elements are deployed in a virtualized way. In the case of the Callbox,

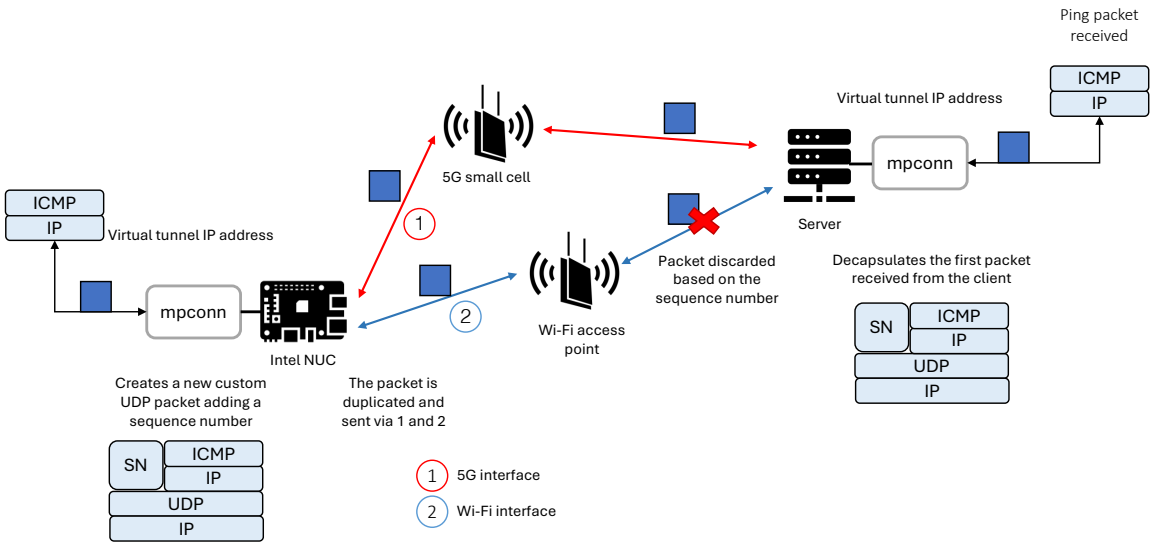


Figure A.6: An example of mpconn tool when transmitting a ping request.

the type of base station and the core network elements are virtualized. On the other hand, in the UE Simbox a UE terminal and its components are virtualized. The virtualization on these devices allows the configuration of different networks in the same physical device, thereby adding more flexibility. With respect to the Callbox, it allows the implementation of many LTE/NR network elements, such as the MME/AMF, as well as a large number of protocols and interfaces of these networks, thereby creating a virtual core. Similarly, the software allows to create different number of instances of eNB/ng-eNB/gNB, through which it is allowed to manage the Software Defined Radio (SDR) card of the device. All of this is implemented on a PC running on top of the Linux operating system.

Same as the Callbox, the UE Simbox allows a software implementation of a virtualized UE, where the different network elements of the UE are implemented along with its protocol layers. In this case, the UE Simbox allows the configuration of LTE, NB-IoT/LTE-M and NR devices. The entire implementation of both devices is based on the 3GPP standard with support up to Release 17.

Under this testbed, first, the configuration files for testing the CIoT optimizations were created. This involves configuring the scripts to define the network elements in both (Crowdcell and UE Simbox), the antennas, the spectrum and bandwidth, and the applications that run on top of the UE with the Amarisoft script format. In this case, the technology was configured as NB-IoT with support of EDT and the base station was configured as a ng-eNB connected to a 5GC. Furthermore, the Linux ping tool was implemented on top of the UE to evaluate the latency performance.

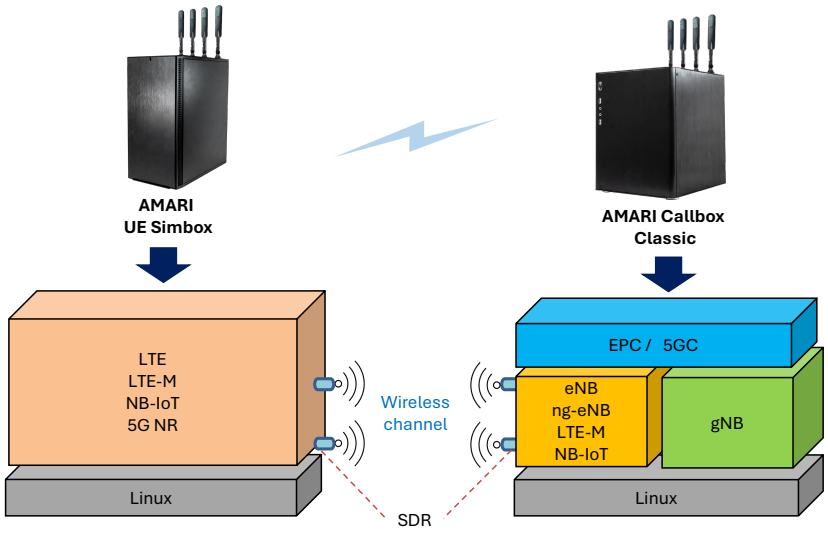


Figure A.7: Testbed with Amarisoft equipment.

Finally, a Python script was developed to automate the process of launching multiple measurements to obtain statistical data. In particular, the script was in charge of changing network conditions such as the cell gain, launching the tests and collecting the data from the logs. A diagram of the testbed for the latency evaluation of CIoT optimizations is depicted in Figure A.8.

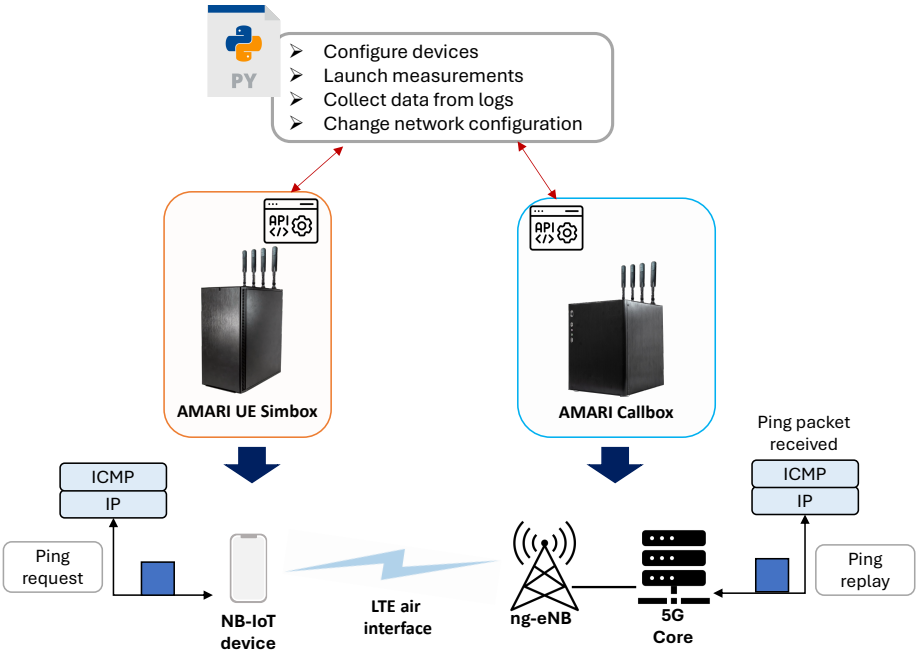


Figure A.8: Diagram of the testbed for the latency evaluation of CIoT optimizations.

A.5 Testbed for the evaluation of poisoning and evasion attacks in an E2E service

As part of publications [**XI**], [**XIV**] and [**XV**] of this thesis, a testbed for the evaluation of poisoning and evasion attacks in an E2E service has been used. More specifically, the testbed allows the extraction of metrics from the network and from the service, thus allowing the generation of datasets with radio and service parameters in situations with and without attack. The testbed has been implemented under a 5G network and the E2E service provided is the download of video on demand from the Youtube platform.

The physical architecture of the testbed is composed of different blocks, as depicted in Figure A.9. The testbed is partly inherited from the one proposed by the authors of [128], but with slight differences. First, a new block to include background traffic has been introduced, thereby providing a more realistic network scenario. Furthermore, a new block for the generation of attack samples is also included, thus allowing the generation of samples with altered values. These new blocks are marked in Figure A.9. Each of the different blocks that compose the testbed are detailed below.

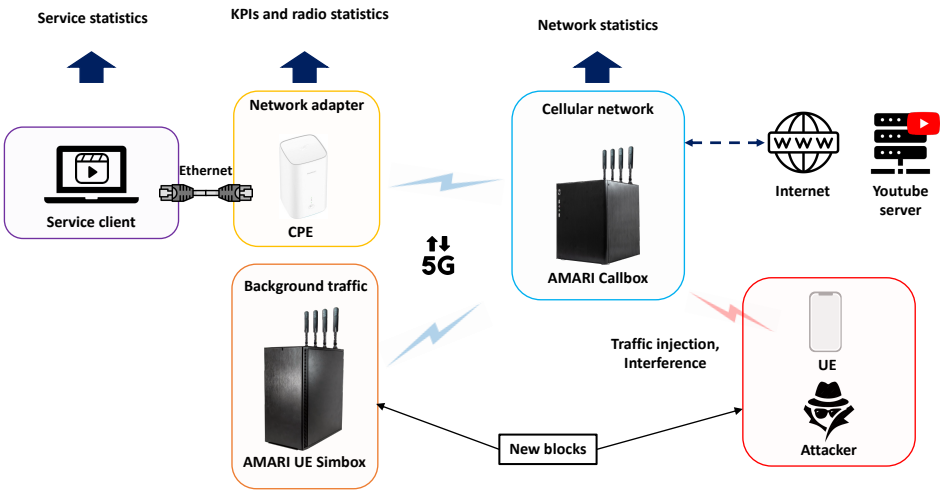


Figure A.9: An overview of the physical architecture of the testbed.

- **Service client**: the E2E service used is a video on demand service from the Youtube platform that is executed in a laptop. The video download is automated with different Python scripts that make use of the Selenium web driver. This block allows the collection of service metrics such as the buffer health, the initial time or freeze events.

- **Network adapter**: this block provides network connectivity to the client. For that purpose, the Huawei CPE PRO 2 has been used as a network adapter, which provides connectivity to the client via Ethernet connection, and backhaul connection with the cellular network.

- **Cellular network**: this block provides cellular connectivity to the users. It is composed of an AMARI Callbox Classic equipment, which creates a virtualized RAN and core network, providing 5G cellular service and internet access to the users.

- **Background traffic**: this new block adds background traffic in the network, thus generating a realistic scenario for the collection of network and service metrics. The equipment used in this block is the AMARI UE Simbox, that allows the emulation of multiple users (up to 64) connected to the AMARI Callbox. Each emulated user is able to run independent traffic, such as video content services, File Transfer Protocol (FTP), ping, etc.

- **Attacker**: this new block allows the collection of metrics in attack situation. In this block, the adversary can be considered as a legitimate user in the network, with its own identity and connected to the cellular network, injecting traffic into the network; or as an external adversary performing an attack to the legitimate network, such as an interference attack. The aim of this block is to alter network and service metrics collected.

Appendix B

Summary (Spanish)

B.1 Introducción

B.1.1 Motivación

La llegada de la cuarta revolución industrial o Industria 4.0 [1] marca un cambio en la fabricación y el sector industrial. El término Industria 4.0 fue usado por primera vez en 2011 en el encargo que el Gobierno alemán hizo a la *Industry-Science Research Alliance* para la consolidación del liderazgo de la industria alemana [2]. Posteriormente, esta iniciativa se extendió al resto de la Unión Europea y en la actualidad, la Industria 4.0 hace referencia a la interconexión de máquinas y sistemas dentro de los centros de producción, así como entre estos y el mundo exterior. Esta revolución digital está transformando las fábricas en fábricas inteligentes, donde la digitalización es clave. En una fábrica conectada, los sensores, el almacenamiento en la nube y el análisis de datos en tiempo real se utilizan para optimizar los procesos de producción. Un aspecto central de esta revolución es la necesidad de que los procesos de producción y distribución sean robustos, eficientes y más flexibles. Para alcanzar estas necesidades, existen diferentes tecnologías facilitadoras que están en el núcleo de la Industria 4.0:

- Sistemas ciberfísicos (*Cyber-Physical Systems*, CPS) [3, 4]. Integran la capacidad de computación y de red en un proceso físico. Las tecnologías CPS permiten el desarrollo de las fábricas inteligentes, donde las máquinas y los equipos están interconectados, lo que permite su monitorización, control y optimización en tiempo real.

- Internet de las cosas (*Internet of Things*, IoT) [5]. IoT es una red de objetos físicos a los que se han incorporado sensores, *software* y otras tecnologías que les permiten conectarse e intercambiar datos. En la Industria 4.0, el uso de IoT facilita el flujo continuo de información a través de las líneas de producción, mejorando la visibilidad operativa y la toma de decisiones.

- Inteligencia Artificial (IA) [6]. Los algoritmos de IA analizan grandes cantidades de datos generados por los CPS y los dispositivos IoT. Esta tecnología permite el mantenimiento predictivo, el control de calidad y la adaptación de los procesos de fabricación, reduciendo el tiempo de inactividad y mejorando la calidad del producto.

- Computación en la nube [7]. La computación en la nube desempeña un papel importante en la Industria 4.0 al proporcionar la infraestructura y la plataforma para almacenar, procesar y analizar las grandes cantidades de datos generados por los dispositivos IoT y otros sensores en el proceso de fabricación. Además, la computación en la nube puede proporcionar la potencia de cálculo necesaria para ejecutar algoritmos de IA.

- Realidad Aumentada (RA) [8]. La aplicación de la tecnología de RA puede mejorar una serie de procesos, como la formación, el mantenimiento y el diseño. Al superponer información digital al mundo físico, la tecnología de RA puede proporcionar a los trabajadores datos e instrucciones en tiempo real, facilitando así flujos de trabajo más eficientes y eficaces.

- Robótica [9, 10]. Los robots y los sistemas de automatización en la Industria 4.0 son más inteligentes, flexibles y colaborativos. Estos sistemas pueden realizar tareas complejas junto a los trabajadores, aumentando la productividad y la seguridad en los entornos de fabricación.

- Análisis de grandes datos [11, 12]. La recopilación y el análisis de grandes conjuntos de datos permiten mejorar las previsiones, mejoras en la eficiencia y descubrir nuevos conocimientos. La toma de decisiones basada en datos se encuentra en el núcleo de la Industria 4.0, impulsando prácticas de fabricación más ágiles y con mayor capacidad de respuesta.

Aunque el concepto de Industria 4.0 se centra principalmente en la industria de producción, las tecnologías y principios mencionados también se aplican en distintos sectores industriales, como la logística, la sanidad, la agricultura o la energía.

Las redes industriales tradicionales se basan principalmente en conexiones cableadas y tecnologías inalámbricas heredadas. Algunas de las conexiones cableadas que se han utilizado son ProfiNET [13], EtherCAT [14] y el conjunto de protocolos de redes sensibles al tiempo (*Time Sensitive Networks*, TSN) [15]. En el campo de las tecnologías inalámbricas, las principales tecnologías utilizadas son las basadas en la familia IEEE 802.11, comúnmente denominada Wi-Fi, pero también soluciones personalizadas para fábricas basadas en IEEE 802.15.1 y 802.15.4, como *Wireless Interface to Sensors and Actuators* (WISA) y WirelessHART [16]. Sin embargo, estas redes a menudo se quedan cortas en términos de escalabilidad, flexibilidad y capacidad de respuesta en tiempo real que requieren las aplicaciones industriales modernas [17]. La naturaleza dinámica de las fábricas inteligentes, los sistemas autónomos y las cadenas de suministro complejas requieren una infraestructura de comunicación que pueda soportar sin problemas un gran número de dispositivos conectados, facilitar el intercambio de datos en tiempo real y garantizar altos niveles de seguridad y fiabilidad.

Las redes celulares, con su adopción generalizada, fiabilidad demostrada y evolución continua, se encuentran en una posición única para satisfacer estas necesidades, ofreciendo una tecnología fundamental para impulsar la Industria 4.0. Las redes celulares, especialmente con la llegada de la quinta generación (5G) de redes móviles y las próximas tecnologías 6G [18], ofrecen capacidades sin precedentes que se alinean perfectamente con las demandas de la Industria 4.0. Entre ellas se incluye el soporte de casos de uso relacionados con comunicaciones críticas, que se conocen como comunicaciones ultra fiables de baja latencia (*Ultra-Reliable Low Latency Communications*, URLLC), el uso masivo de dispositivos de tipo máquina, también conocido como comunicaciones masivas de tipo máquina (*massive Machine-Type Communications*, mMTC), y los servicios mejorados de banda ancha (*enhanced Mobile Broadband*, eMBB). La capacidad de proporcionar una comunicación determinista, la compatibilidad con un número masivo de dispositivos IoT y un alto caudal de datos son habilitadores críticos para aplicaciones como el mantenimiento predictivo, la monitorización remota y la robótica autónoma. Además, la naturaleza modular y escalable de las redes celulares permite despliegues a medida en diversos entornos industriales, desde plantas de fabricación a gran escala hasta instalaciones remotas y aisladas. Esta flexibilidad admite la creación de redes privadas [19] dedicadas a necesidades industriales específicas, garantizando que se cumplan eficazmente los requisitos únicos de los distintos sectores.

El impulso mundial hacia la sostenibilidad y la eficiencia en las operaciones industriales [20] subraya aún más la importancia de aprovechar las redes de comunicación

avanzadas. Al permitir una gestión más eficiente de los recursos, reducir el tiempo de inactividad mediante el mantenimiento predictivo y facilitar la perfecta integración de las fuentes de energía renovables, las redes celulares [21] contribuyen significativamente a los objetivos de sostenibilidad de las industrias modernas.

Dado que la adopción e implantación de la tecnología celular se está llevando a cabo de manera progresiva en las industrias, especialmente la tecnología 5G [22], es necesario estudiar su aplicabilidad, evaluando el rendimiento de la red a través de los diferentes servicios y casos de uso involucrados en la fábrica inteligente.

B.1.2 Objetivos

El objetivo principal de esta tesis es evaluar y mejorar el rendimiento de la red celular en un entorno industrial de interior. Para ello, en esta tesis se abordan diferentes técnicas y optimizaciones de la red. En primer lugar, se realizan tareas relacionadas con el estudio de la latencia de servicios críticos y la escalabilidad en la red. En segundo lugar, se desarrollan diferentes herramientas para evaluar el rendimiento de la red en un entorno industrial y mejorar la fiabilidad de los servicios críticos mediante el uso de la solución de multiconectividad. En tercer lugar, se desarrollan y evalúan algoritmos de optimización con los siguientes propósitos: mejorar la fiabilidad de los servicios críticos sin desperdiciar recursos, y mejorar la calidad de servicio (*Quality of Service*, QoS) de los diferentes perfiles de tráfico involucrados en una fábrica. Por último, se ha evaluado el rendimiento de las distintas optimizaciones propuestas por el *Third Generation Partnership Project* (3GPP) para dispositivos IoT celulares (*Cellular IoT*, CIoT), incluyendo también un análisis de seguridad de la última optimización. Específicamente, las líneas de investigación abordadas en esta tesis se pueden resumir en los siguientes objetivos:

Obj. 1. Estudiar el impacto de las numerologías 5G en la latencia de los servicios críticos.

El objetivo de este estudio consiste en analizar el comportamiento de las diferentes configuraciones de numerología en la latencia percibida por los usuarios bajo diferentes condiciones de canal y tamaños de paquete. En este sentido, este estudio pretende sentar las bases para futuras optimizaciones en la reducción de la latencia, ya que una numerología adecuada puede seleccionarse en función de las condiciones radio experimentadas.

Obj. 2. Evaluar y comparar la escalabilidad de la red con diferentes tecnologías en un entorno industrial.

El propósito de este objetivo es el de evaluar y comparar empíricamente el rendimiento de la red respecto a la latencia y las pérdidas de paquetes con distintas tecnologías en un escenario industrial de interior. En concreto, la evaluación debe tener en cuenta diferentes tamaños de paquete y escenarios con distintos número de dispositivos transmitiendo datos. Como resultado, este estudio debería proporcionar una visión clara sobre qué tecnología se adapta mejor al sector industrial.

Obj. 3. Proponer un mecanismo para mejorar la fiabilidad de los servicios críticos.

Este objetivo se refiere al diseño y desarrollo de un algoritmo que cumpla los requisitos de fiabilidad de los servicios críticos. Así, el algoritmo propuesto debería ser capaz de adaptar y controlar dinámicamente la activación de la duplicación de paquetes para evitar el malgasto de los recursos en la red.

Obj. 4. Evaluar el rendimiento de la red en un centro de distribución.

La finalidad de este objetivo es la de realizar una evaluación de la red 5G en un escenario correspondiente a un centro de distribución, teniendo en cuenta los diferentes perfiles de tráfico implicados en este escenario. En concreto, en este trabajo se debería comparar la QoS de estos perfiles de tráfico bajo diferentes actividades logísticas con diferentes enfoques de *Network Slicing* (NS).

Obj. 5. Estudiar el impacto de las optimizaciones de señalización para CIoT en la red.

El objetivo de este estudio es el de analizar el comportamiento de las diferentes optimizaciones de señalización de CIoT en la latencia percibida por el usuario cuando transmite de forma infrecuente pequeños datos en la red.

Obj. 6. Analizar la seguridad de EDT en 5G para CIoT.

Este objetivo se relaciona con el Obj. 5 y se refiere a un análisis en profundidad de la seguridad de la optimización de la transmisión temprana de datos (*Early Data Transmission*, EDT), describiendo en detalle sus modos de operación y analizando las principales vulnerabilidades asociadas a esta optimización. Como resultado, un conjunto de recomendaciones para los proveedores debería ser derivado del análisis de seguridad.

B.2 Descripción de los resultados

En esta sección se presentan los resultados derivados de esta tesis. Estos trabajos abordan los retos identificados y los objetivos definidos en la Sección 1.2. La Figura B.1 ilustra la relación entre los retos, los objetivos y los resultados obtenidos. En la figura, cada publicación se representa como un bloque individual, indicando el capítulo de la tesis en el cual se incluye.

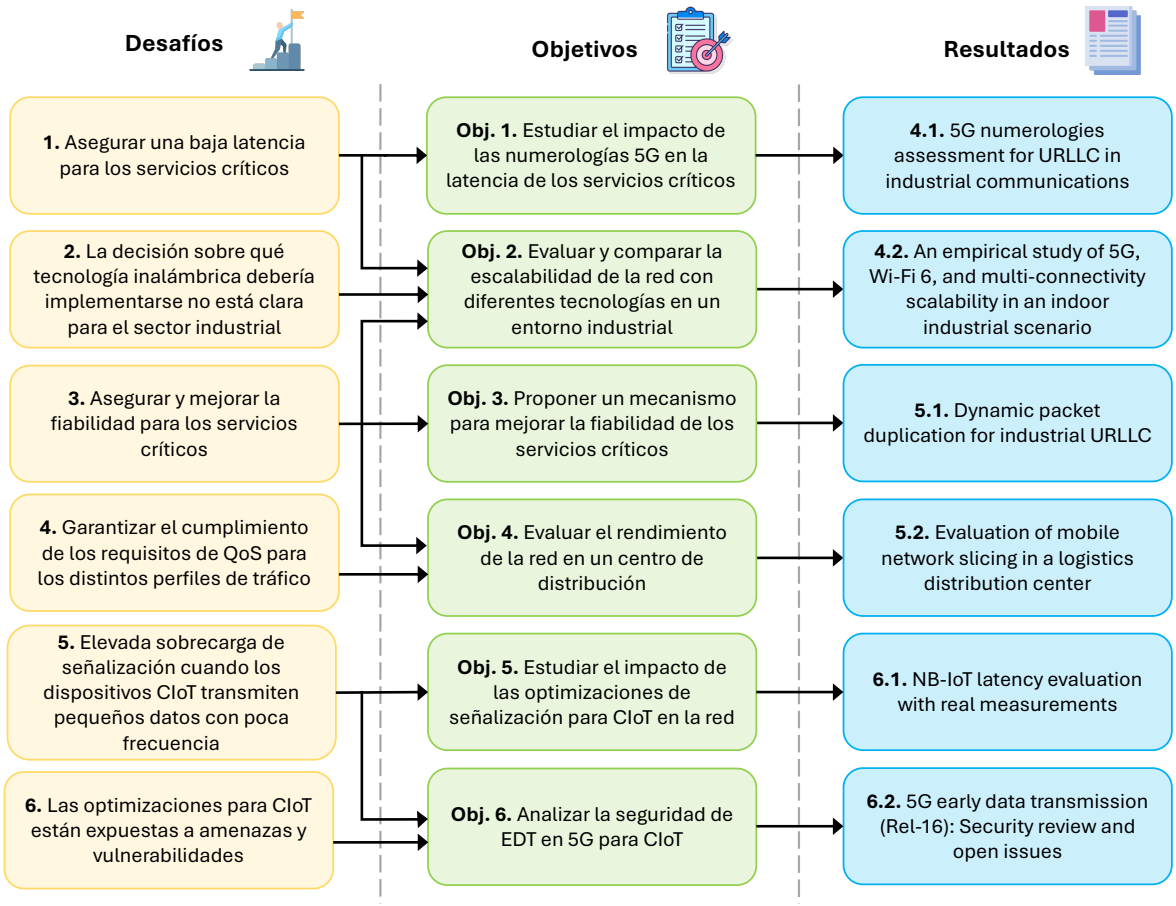


Figura B.1: Desafíos, objetivos y publicaciones.

B.2.1 Evaluación de las numerologías 5G para URLLC en comunicaciones industriales

La llegada de la red 5G ha facilitado la introducción de características novedosas, permitiendo el desarrollo de nuevos casos de usos y servicios. Una de estas características es la numerología, que permite un proceso de asignación de recursos más rápido debido al uso de *slots* de tiempo más cortos. Esta característica es de particular importancia

para servicios con restricción de latencia, como los empleados en la operación de los vehículos guiados automatizados (*Automated Guided Vehicles*, AGVs), ya que permite una reducción de la latencia.

Sin embargo, en los escenarios industriales, el principal desafío proviene de la presencia de muros de hormigón y de las grandes estructuras y máquinas metálicas, lo que da lugar a interferencia y propagación multicamino. Como consecuencia, seleccionar una numerología apropiada es una tarea desafiante, y esta debe adaptarse a las condiciones de radio experimentadas.

Por ello, el primer artículo presentado en el Capítulo 4 se enfoca en la evaluación del impacto de la numerología en el retardo experimentado en el enlace radio para un servicio de control remoto (comunicación de AGVs), cubriendo con ello el Obj. 1 de esta tesis. Específicamente, este estudio abarca la evaluación con distintos tamaños de paquete y condiciones de canal en un entorno de industria simulado, con un foco especial en la identificación y el análisis de los valores anómalos.

Los resultados demuestran que la premisa de que una alta numerología tiende a un menor retardo no siempre se cumple, particularmente en condiciones de no línea de visión directa (*Non-Line-of-Sight*, NLOS). En estos casos, una numerología intermedia es más adecuada para este tipo de servicio.

B.2.2 Estudio empírico de la escalabilidad de 5G, Wi-Fi 6 y multiconectividad en un escenario industrial de interior

El sector industrial está adoptando la Industria 4.0 para mejorar la flexibilidad y reducir los costes de instalación mediante el uso de la conectividad inalámbrica. Sin embargo, persiste la pregunta sobre qué tecnología inalámbrica debería implementarse en la fábrica para cumplir con los requisitos de las aplicaciones de próxima generación, como los robots móviles autónomos (*Autonomous Mobile Robots*, AMRs). Mientras que la tecnología Wi-Fi es la más prevalente y fácil de desplegar, la red 5G ha sido diseñada para soportar las necesidades del sector industrial. Por lo tanto, es importante comparar ambas tecnologías desde el punto de vista del rendimiento, especialmente bajo diferentes condiciones de carga y con diferentes número de dispositivos. El uso de la multiconectividad con diferentes tecnologías de acceso radio también se considera un habilitador clave para satisfacer los requisitos de las aplicaciones en tiempo real más

críticas.

Por lo tanto, el segundo artículo presentado en el Capítulo 4 se centra en la evaluación empírica y comparación de la escalabilidad de la red 5G, Wi-Fi 6 y multiconnectividad desde el punto de vista de la latencia y las pérdidas de paquetes, cubriendo con ello el Obj. 2 de esta tesis. Este trabajo se ha llevado a cabo en el laboratorio "5G Smart Production Lab" en Aalborg (Dinamarca), donde se han realizado diferentes campañas de medidas para diversos escenarios (estático y movilidad) y tamaños de paquete.

Los resultados obtenidos muestras en general latencias bajas con Wi-Fi, pero largas colas en la distribución de la latencia, con unas pérdidas de paquetes mayores en comparación con 5G. Por otro lado, la latencia de 5G es muy consistente con colas acotadas y obteniendo una baja pérdida de paquetes. En términos de escalabilidad, 5G escala mejor que Wi-Fi, viéndose esta última muy afectada por el número de dispositivos transmitiendo datos. Finalmente, la solución de multiconectividad mostró una mayor fiabilidad y menores latencias en todos los casos evaluados.

B.2.3 Duplicación de paquetes dinámica para URLLC industrial

Este trabajo sigue la línea comenzada con la primera publicación del Capítulo 4. Esto es, una vez se selecciona una numerología apropiada para reducir la latencia, el segundo paso consiste en mejorar la fiabilidad de las comunicaciones críticas. Una de las formas de mejorar la fiabilidad de estas comunicaciones es mediante el uso de la multiconectividad, particularmente con el enfoque de duplicación de paquetes. No obstante, esta solución lleva consigo un aumento de la redundancia en la red, lo que puede llevar a un uso inapropiado de los recursos de red.

Por ello, para reducir el malgasto de los recursos de red, el primer artículo del Capítulo 5 propone un algoritmo de duplicación de paquetes dinámico basado en aprendizaje automático (*Machine Learning*, ML), que determina cuando la duplicación de los paquetes es requerida en una transmisión específica de datos para enviar un mensaje crítico de manera exitosa (Obj. 3). En concreto, un estimador de latencia basado en bosque aleatorio (*Random Forest*, RF) fue entrenado y evaluado, el cual decide cuando realizar la duplicación basándose en un umbral de latencia. La metodología presentada fue evaluada en un simulador 5G y el rendimiento de la red fue comparado con distintos

enfoques: no duplicar los paquetes y, una duplicación estática de los paquetes.

Los resultados de la evaluación demostraron que el algoritmo dinámico de duplicación de paquetes propuesto reduce en un 81% el número de paquetes duplicados enviados mientras que mantiene el mismo nivel de latencia (esto es, la latencia obtenida se encuentra por debajo del umbral) que la técnica de duplicación estática. Esta reducción en el número de paquetes duplicados resulta en un uso más eficiente de los recursos de la red.

B.2.4 Evaluación de *Network Slicing* de la red móvil en un centro de distribución logística

El segundo artículo incluido en el Capítulo 5 aborda el problema de optimizar los recursos de la red para los diferentes perfiles de tráfico involucrados dentro de un centro de distribución de logística. En concreto, estos perfiles de tráfico corresponden a eMBB, URLLC y mMTC, con distintos requisitos de latencia, fiabilidad, *throughput*, etc.

Específicamente, este artículo primero introduce un novedoso simulador de código abierto desarrollado, basado en el *framework* de ns-3, con una representación realista de un escenario de centro de distribución, donde están presentes diferentes actividades logísticas. Las comunicaciones de estas actividades han sido modeladas y usadas para estimar el rendimiento de los diferentes perfiles de tráfico. Como resultado, el simulador desarrollado sirve como base para evaluar el rendimiento de la red 5G en un escenario de logística inteligente (Obj. 4).

En segundo lugar, bajo el simulador desarrollado, este trabajo evalúa y compara el rol de dos estrategias de NS en 5G para la logística inteligente: el uso de una *slice* estática con una división balanceada de los recursos de red y el uso de una *slice* dinámica que adapta los recursos basándose en la carga del tráfico, dependiendo de la actividad que se esté realizando. En concreto, este trabajo evalúa estas estrategias en términos de QoS para los diferentes perfiles de tráfico, resultando en las siguientes métricas: *throughput* para el tráfico eMBB, fiabilidad para el tráfico URLLC y el canal de acceso aleatorio (*Random Access*, RA) para el tráfico mMTC.

Los resultados obtenidos muestran que una *slice* dinámica realiza un uso más eficiente de los recursos radio, mejorando la QoS de los diferentes perfiles de tráfico, incluso cuando hay un pico de tráfico en un perfil específico. Esta mejora va desde el

6.48% a el 95.65%, dependiendo del perfil de tráfico específico y la métrica evaluada.

B.2.5 Evaluación de la latencia de NB-IoT con medidas reales

Diferentes optimizaciones han sido propuestas por el 3GPP para dispositivos CIoT con el objetivo de mejorar la vida de la batería y reducir la señalización con la red. Estas optimizaciones comenzaron con la llegada de la *Release* 13, donde la transmisión por el plano de control (*Control Plane*, CP) fue introducida. Esta optimización permite la transmisión de datos utilizando el CP en lugar del plano de usuario (*User Plane*, UP), evitando con ello el establecimiento de las portadoras radio de datos (*Data Radio Bearers*, DRBs) del UP.

Además, con la llegada de la *Release* 15, la optimización de EDT fue introducida para soportar las transmisiones infrecuentes de datos pequeños, soportando tanto el modo de transmisión por el plano de control CP como por el UP. Esta última optimización permite la transmisión de datos durante el procedimiento de RA, con una reducción significativa en la señalización entre el UE y la red, y sin la necesidad de realizar un cambio de estado de la capa *Radio Resource Control* (RRC). Esto es, el UE transmite los datos en el estado RRC *Idle*.

De este modo, el primer artículo del Capítulo 6 se centra en la evaluación y comparativa de las optimizaciones propuestas por el 3GPP para CIoT previamente mencionadas a través del CP en términos de rendimiento de latencia con la tecnología NB-IoT, cubriendo con ello el Obj. 5 de esta tesis. En concreto, en este trabajo se ha realizado una campaña de medidas con equipos de Amarisoft (AMARI Crowdcell y AMARI UE Simbox) bajo diferentes tamaños de paquetes y niveles de cobertura.

Los resultados evaluados mostraron bajas latencia para EDT, particularmente en el caso de paquetes pequeños, donde se utiliza un *transport block* reducido, siendo así más eficiente desde una perspectiva de la red. Además, se ha demostrado que EDT, al contrario que la optimización de la *Release* 13, logra el requisito de latencia definido por el 3GPP (10 segundos) bajo cobertura extrema.

B.2.6 EDT en 5G: revisión de seguridad y problemas abiertos

Esta sección presenta el segundo de los trabajos llevado a cabo en relación con el Capítulo 6 de esta tesis. En este caso, este trabajo extiende la línea comenzada con la primera publicación del Capítulo 6, ofreciendo una descripción detallada de la optimización de EDT junto a un análisis de la seguridad de este mecanismo. Por tanto, este trabajo cubre el Obj. 6 de esta tesis.

Como se ha mencionado anteriormente, la optimización de EDT fue introducida en la *Release* 15 para permitir la transmisión de datos durante el proceso de RA. Esta característica, destinado especialmente para transmisiones infrecuentes y con tamaños pequeños, trata de reducir la latencia y el consumo de los UEs. No obstante, a pesar de la importancia de esta novedad y el acuerdo general sobre su efectividad, existen pocos trabajos en la literatura que proporcionen información sobre su implementación y analicen las ventajas y desventajas de sus dos diferentes opciones de implementación (CP y UP).

Además, a pesar de que la seguridad es reconocida como un aspecto crucial para el correcto despliegue de esta tecnología, la literatura carece de una revisión de los problemas de seguridad y las características de este mecanismo. Como consecuencia de esta falta de trabajos y la complejidad de los protocolos de redes móviles, existe una división entre los expertos en seguridad y los investigadores de EDT, que impide el fácil desarrollo de esquemas de seguridad.

Para combatir esta importante brecha, este artículo ofrece un tutorial de EDT y su seguridad, analizando las principales vulnerabilidades y concluyendo con un conjunto de recomendaciones para investigadores y fabricantes. En concreto, debido a las simplificaciones en los protocolos llevado a cabo por EDT, se han encontrado vulnerabilidades como la inyección de paquetes, ataques por repetición y la inyección de valores falsos para deshabilitar EDT en la red.

B.3 Conclusiones

B.3.1 Contribuciones

Esta tesis tiene como objetivo evaluar y mejorar el rendimiento de las redes móviles en el paradigma de la Industria 4.0. Para ello, se han identificado un conjunto de desafíos en el entorno industrial y se han definido los objetivos necesarios para resolver estos desafíos. A lo largo de este trabajo se han establecido un total de seis objetivos, los cuales están distribuidos de la siguiente manera. Los Obj. 1 y 2 están relacionados con la evaluación del rendimiento de la red en un entorno industrial de interior. Los Obj. 3 y 4 se refieren al desarrollo de algoritmos de optimización para mejorar el rendimiento de la red. Finalmente, los Obj. 5 y 6 pretenden cubrir las optimizaciones de señalización de CIoT, primero evaluando el impacto de estas optimizaciones en la red y luego proporcionando un análisis de la seguridad de la última optimización propuesta por el 3GPP. A continuación se presentan las contribuciones relacionadas con cada uno de estos objetivos:

Obj. 1. Estudiar el impacto de las numerologías 5G en la latencia de los servicios críticos.

- Se ha realizado un análisis del impacto de las diferentes configuraciones de numerología 5G en la latencia de los usuarios. En este análisis, se ha llevado a cabo un estudio más detallado que los encontrados en el estado del arte. Se han evaluado las numerologías 5G bajo diferentes condiciones de canal (LOS y NLOS) y con diferentes tamaños de paquete para el caso de uso de un AGV.
- El estudio se ha llevado a cabo en un entorno 5G simulado. Los resultados mostraron que la selección de la numerología no es trivial, siendo un valor intermedio más adecuado bajo condiciones NLOS. Este estudio abre la puerta a algoritmos que puedan ser utilizados para dinámicamente ajustar la configuración de la numerología en la red para un mejor rendimiento.

Obj. 2. Evaluar y comparar la escalabilidad de la red con diferentes tecnologías en un entorno industrial.

- Siguiendo este objetivo, se ha llevado a cabo una evaluación empírica con diferente número de dispositivos, tamaños de paquete y escenarios para eval-

uar el rendimiento de la red respecto a la latencia y las pérdidas de paquetes. En concreto, para realizar esta comparativa de rendimiento, se han seleccionado las tecnologías 5G, Wi-Fi 6 y el uso de multiconectividad entre ambas con un enfoque de duplicación de paquetes.

- Específicamente, se han llevado a cabo campañas de medidas con equipo comercial en el laboratorio "5G Smart Production Lab" de la Universidad de Aalborg (Dinamarca), que consiste en un entorno de fábrica industrial de interior a pequeña escala compuesto por dos salas y una amplia gama de equipos de fabricación y producción industrial.
- Como resultado de las campañas de medida, se ha demostrado que la tecnología 5G proporciona menor latencia en las colas y es más fiable que Wi-Fi 6. Por otro lado, la solución de multiconectividad demostró una significativa reducción en las colas de la latencia y cero paquetes perdidos, siendo esta solución muy efectiva para lograr los casos de uso con requisitos de latencia y fiabilidad muy restrictivos.

Obj. 3. Proponer un mecanismo para mejorar la fiabilidad de los servicios críticos.

- Para cumplir este objetivo, se ha diseñado un algoritmo basado en ML para activar dinámicamente la duplicación de paquetes en un entorno industrial. Este algoritmo se basa en métricas de red como la relación señal/interferencia más ruido (SINR), el índice de modulación y la retroalimentación *Hybrid Automatic Repeat reQuest* (HARQ) para predecir la latencia. La salida del predictor se utiliza para la decisión de duplicación de paquetes en el enlace descendente, basándose en un umbral de latencia.
- El predictor de latencia se entrenó con el algoritmo de RF y el rendimiento del algoritmo propuesto se validó mediante diferentes pruebas realizadas en un entorno simulado 5G. En este simulador, se implementó la función de conectividad dual (*Dual Connectivity*, DC) con un enfoque de duplicación de paquetes, tal y como se describe en el Apéndice A.
- Se ha comparado el rendimiento del algoritmo con otros enfoques en el estado del arte, demostrando así que la solución propuesta es capaz de obtener mejores resultados y de minimizar el desperdicio de recursos en la red.

Obj. 4. Evaluar el rendimiento de la red en un centro de distribución.

- Las contribuciones correspondientes a este objetivo son, en primer lugar, el diseño e implementación de un simulador de código abierto basado en el *framework* de ns-3 y el módulo 5G-LENA, que incluye nuevas características para soportar la evaluación de la red en un centro de distribución. En concreto, se han implementado características como el escenario de un centro de distribución, las actividades involucradas allí, la asignación de recursos por *slice*, y el modelo de propagación y canal industrial.
- En segundo lugar, cuando las características anteriores fueron implementadas, se han evaluado dos estrategias de NS utilizando la red 5G. Estas estrategias consisten en el uso de una *slice* estática con una división de los recursos de red balanceada, y el uso de una *slice* que dinámicamente ajusta su tamaño dependiendo de la actividad que se esté llevando a cabo.
- Finalmente, se ha evaluado mediante simulaciones el rendimiento de QoS proporcionado por esas estrategias de NS sobre distintos perfiles de tráfico, y los resultados han demostrado que una *slice* dinámica mejora la QoS especialmente con alta carga de tráfico, mientras que la *slice* estática rinde bien cuando la carga de tráfico es baja.

Obj. 5. Estudiar el impacto de las optimizaciones de señalización para CIoT en la red.

- En relación con este objetivo, se ha llevado a cabo un análisis del impacto en la latencia de los usuarios de las diferentes optimizaciones de señalización en CIoT propuestas por el 3GPP. Concretamente, en este estudio se ha utilizado la tecnología NB-IoT para la evaluación de las distintas optimizaciones por el CP.
- El estudio se ha llevado a cabo con equipo comercial de Amarisoft, con el cual se han realizado varias campañas de medidas bajo diferentes niveles de cobertura y tamaños de paquete.
- A partir de los resultados de estas mediciones, se ha demostrado que EDT, a diferencia de la optimización de la *Release* 13, cumple con el requisito de latencia definido por el 3GPP para transmisiones de datos pequeños y poco frecuentes bajo un nivel de cobertura extremo.

Obj. 6. Analizar la seguridad de EDT en 5G para CIoT.

- Como contribución final se ha llevado a cabo un estudio de la optimización de EDT en CIoT. En este estudio, la optimización de EDT se ha descrito en detalle para sus dos modos de operación soportados, el CP y el UP.
- Además, se ha proporcionado un análisis de seguridad de esta optimización, extrayendo las principales vulnerabilidades encontradas en cada uno de sus modos de operación. Concretamente, se han encontrado vulnerabilidades como la inyección de paquetes, los ataques por repetición o la inyección de valores falsos para deshabilitar EDT.
- Finalmente, tras un análisis de seguridad exhaustivo, se ha proporcionado un conjunto de recomendaciones para investigadores y fabricantes, que incluyen soluciones para remediar estas vulnerabilidades en futuras versiones del estándar 3GPP, y que modo de operación es más recomendable de utilizar.

B.3.2 Publicaciones

Revistas

Publicaciones derivadas de esta tesis

El trabajo realizado en esta tesis ha dado lugar a cuatro artículos publicados en revistas de alto impacto más otra en proceso de revisión, que se enumeran a continuación.

[**I**] D. Segura, E.J. Khatib, J. Munilla, and R. Barco, "5G Numerologies Assessment for URLLC in Industrial Communications," *Sensors*, vol. 21, no. 7, p. 2489, Abr. 2021.

[**II**] D. Segura, E.J. Khatib, and R. Barco, "Dynamic Packet Duplication for Industrial URLLC," *Sensors*, vol. 22, no. 2, p. 587, Ene. 2022.

[**III**] D. Segura, J. Munilla, E.J. Khatib, and R. Barco, "5G Early Data Transmission (Rel-16): Security Review and Open Issues," *IEEE Access*, vol. 10, pp. 93289–93308, Sep. 2022.

[**IV**] D. Segura, E.J. Khatib, and R. Barco, "Evaluation of Mobile Network Slicing in a Logistics Distribution Center," *IEEE Transactions on Network and Service Management*, Bajo revisión, 2024.

[**V**] D. Segura, S.B. Damsgaard, A. Kabaci, P. Mogensen, E.J. Khatib, and R. Barco, "An Empirical Study of 5G, Wi-Fi 6, and Multi-Connectivity Scalability in an Indoor Industrial Scenario," *IEEE Access*, vol. 12, pp. 74406-74416, May. 2024.

Conferencias

Conferencias derivadas de esta tesis

También se han presentado varios trabajos en congresos nacionales e internacionales, como se muestra a continuación.

[**VI**] D. Segura, E.J. Khatib, and R. Barco, "Evaluación de numerologías 5G para URLLC," en *XXXV Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2020)*, Málaga (España), Sept. 2020.

[**VII**] D. Segura, E.J. Khatib, J. Munilla, and R. Barco, "Evaluación de los modos de conexión para NB-IoT," en *XXXVI Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2021)*, Vigo (España), Sept. 2021.

[**VIII**] D. Segura, E.J. Khatib, J. Munilla, and R. Barco, "NB-IoT latency evaluation with real measurements," en *2022 IEEE Workshop on Complexity in Engineering (COMPENG)*, Florencia (Italia), Jul. 2022.

[**IX**] D. Segura, E.J. Khatib, J. Munilla, and R. Barco, "Evaluación de la latencia de NB-IoT con medidas reales," en *XXXVII Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2022)*, Málaga (España), Sept. 2022.

[**X**] D. Segura, S.B. Damsgaard, P. Mogensen, E.J. Khatib, and R. Barco, "Comparativa empírica del rendimiento de 5G y Wi-Fi en un escenario industrial de interior," en *XXXVIII Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2023)*, Cáceres (España), Sept. 2023.

[**XI**] D. Segura, H.Q. Luo-Chen, C. Baena, E.J. Khatib, S. Fortes, and R. Barco, "Testbed para la evaluación de los ataques de envenenamiento y evasión en un servicio E2E," en *XXXIX Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2024)*, Cuenca (España), Sept. 2024.

Conferencias relacionadas con esta tesis

[**XII**] J. Llanes, E.J. Khatib, D. Segura, and R. Barco, "Seguridad en B5G/6G," in *XXXVII Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2022)*, Málaga (España), Sept. 2022.

[**XIII**] S.B. Damsgaard, D. Segura, M.F. Andersen, S.A. Markussen, S. Barbera, I. Rodríguez, and P. Mogensen, "Commercial 5G NPN and PN Deployment Options for Industrial Manufacturing: An Empirical Study of Performance and Complexity Tradeoffs," en *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Toronto (Canada), Sept. 2023.

[**XIV**] H.Q. Luo-Chen, D. Segura, C. Baena, E.J. Khatib, and R. Barco, "Detection of anomalous samples based on automatic thresholds," en *2024 IEEE Workshop on Complexity in Engineering (COMPENG)*, Florencia (Italia), Jul. 2024.

[**XV**] H.Q. Luo-Chen, D. Segura, C. Baena, E.J. Khatib, S. Fortes, and R. Barco, "Alteración de datos E2E: impacto de un ataque de envenenamiento y evasión en una red celular," en *XXXIX Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2024)*, Cuenca (España), Sept. 2024.

[**XVI**] C.S. Álvarez-Merino, D. Segura, C. Baena, E.J. Khatib, and R. Barco, "Infraestructura para la monitorización del consumo energético en redes b5G/6G," en *XXXIX Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2024)*, Cuenca (España), Sept. 2024.

[**XVII**] E.J. Khatib, D. Segura, A. Tarrías, and R. Barco, "Estudio del ataque de cadena de suministro sobre XZ utils y sus consecuencias en telecomunicaciones," en *XXXIX Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2024)*, Cuenca (España), Sept. 2024.

B.3.3 Proyectos relacionados

Esta tesis ha contribuido a los siguientes proyectos:

- Proyectos nacionales:
  - EDEL4.0: Seguridad y fiabilidad en las comunicaciones 5G/IoT para la Industria 4.0. Número de proyecto UMA18-FEDERJA-172, recibiendo fondos de la Junta de Andalucia y la Comisión Europea, perteneciente a la convocatoria "Proyectos de I+D+i en el marco del Programa Operativo FEDER Andalucia 2014-2020".
  - PENTA: Provisión de servicios PPDR a través de Nuevas Tecnologías de Acceso radio. Número de proyecto PY18-4647, recibiendo fondos de la Junta de Andalucía y la Comisión Europea, perteneciente a la convocatoria del "Plan Andaluz de Investigación, Desarrollo e Innovación (PAIDI 2020)".
  - MAORI: Massive AI for the OpenRadIo b5G/6G network. Número de proyecto TSI-063000-2021-72, recibiendo fondos del Ministerio de Asuntos Económicos y Transformación Digital y la Unión Europea - NextGenerationEU dentro del marco de "Recuperación, Transformación, y Resiliencia".

B.3.4 Estancia de investigación

Como parte de esta tesis se ha realizado una estancia de investigación de cinco meses en Aalborg (Dinamarca), colaborando con la Universidad de Aalborg en la realización de varias campañas de medidas con 5G, Wi-Fi 6 y multiconectividad en un entorno industrial. La estancia tuvo lugar entre febrero de 2023 y junio de 2023, y fue supervisada por Preben E. Mogensen.

Bibliography

[1] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, "Industry 4.0," *Business & information systems engineering*, vol. 6, pp. 239–242, 2014.

[2] European Commission, "Digital Transformation Monitor. Germany: Industrie 4.0," 2017, (accessed June 2024). [Online]. Available: https://de.sistematica.it/docs/379/Germay_Industrie_4.0.pdf

[3] D. G. Pivoto, L. F. de Almeida, R. da Rosa Righi, J. J. Rodrigues, A. B. Lugli, and A. M. Alberti, "Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review," *Journal of manufacturing systems*, vol. 58, pp. 176–192, 2021.

[4] S. J. Oks, M. Jalowski, M. Lechner, S. Mirschberger, M. Merklein, B. Vogel-Heuser, and K. M. Möslein, "Cyber-physical systems in the context of Industry 4.0: A review, categorization and outlook," *Information Systems Frontiers*, pp. 1–42, 2022.

[5] M. Soori, B. Arezoo, and R. Dastres, "Internet of things for smart factories in Industry 4.0, a review," *Internet of Things and Cyber-Physical Systems*, 2023.

[6] I. Ahmed, G. Jeon, and F. Piccialli, "From artificial intelligence to explainable artificial intelligence in Industry 4.0: A survey on what, how, and where," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 8, pp. 5031–5042, 2022.

[7] A. Sunyaev and A. Sunyaev, "Cloud computing," *Internet computing: Principles of distributed systems and emerging internet-based technologies*, pp. 195–236, 2020.

[8] P. Fraga-Lamas, T. M. Fernández-Caramés, O. Blanco-Novoa, and M. A. Vilar-Montesinos, "A review on industrial augmented reality systems for the Industry 4.0 shipyard," *IEEE Access*, vol. 6, pp. 13 358–13 375, 2018.

[9] J. Wen, L. He, and F. Zhu, "Swarm robotics control and communications: Imminent challenges for next generation smart logistics," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 102–107, 2018.

[10] R. Goel and P. Gupta, "Robotics and Industry 4.0," *A Roadmap to Industry 4.0: Smart Production, Sharp Business and Sustainable Development*, pp. 157–169, 2020.

[11] J. Lee, H.-A. Kao, and S. Yang, "Service innovation and smart analytics for Industry 4.0 and big data environment," *Procedia cirp*, vol. 16, pp. 3–8, 2014.

[12] M. Khan, X. Wu, X. Xu, and W. Dou, "Big data challenges and opportunities in the hype of Industry 4.0," in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1–6.

[13] R. Pigan and M. Metter, *Automating with PROFINET: Industrial communication based on Industrial Ethernet.* John Wiley & Sons, 2008.

[14] D. Orfanus, R. Indergaard, G. Prytz, and T. Wien, "Ethercat-based platform for distributed control in high-performance industrial applications," in *2013 IEEE 18th Conference on Emerging Technologies & Factory Automation (ETFA)*, 2013, pp. 1–8.

[15] F. Zezulka, P. Marcon, Z. Bradac, J. Arm, T. Benesl, and I. Vesely, "Communication systems for Industry 4.0 and the IIoT," *IFAC-PapersOnLine*, vol. 51, no. 6, pp. 150–155, 2018.

[16] V. K. Huang, Z. Pang, C.-J. A. Chen, and K. F. Tsang, "New trends in the practical deployment of industrial wireless: From noncritical to critical use cases," *IEEE Industrial Electronics Magazine*, vol. 12, no. 2, pp. 50–58, 2018.

[17] M. Alabadi, A. Habbal, and X. Wei, "Industrial internet of things: Requirements, architecture, challenges, and future research directions," *IEEE Access*, vol. 10, pp. 66 374–66 400, 2022.

[18] L. Qiao, Y. Li, D. Chen, S. Serikawa, M. Guizani, and Z. Lv, "A survey on 5G/6G, AI, and robotics," *Computers and Electrical Engineering*, vol. 95, p. 107372, 2021.

[19] J. Ordonez-Lucena, J. F. Chavarria, L. M. Contreras, and A. Pastor, "The use of 5G Non-Public Networks to support Industry 4.0 scenarios," in *2019 IEEE*

Conference on Standards for Communications and Networking (CSCN), 2019, pp. 1–7.

[20] European Commission, "Industry and the Green Deal," (accessed June 2024). [Online]. Available: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/industry-and-green-deal_en

[21] M. Attaran, "The impact of 5G on the evolution of intelligent automation and industry digitization," *Journal of ambient intelligence and humanized computing*, vol. 14, no. 5, pp. 5977–5993, 2023.

[22] A. Mahmood, S. F. Abedin, T. Sauter, M. Gidlund, and K. Landernäs, "Factory 5G: A review of industry-centric features and deployment options," *IEEE Industrial Electronics Magazine*, vol. 16, no. 2, pp. 24–34, 2022.

[23] M. Cheffena, "Propagation channel characteristics of industrial wireless sensor networks [wireless corner]," *IEEE Antennas and Propagation Magazine*, vol. 58, no. 1, pp. 66–73, 2016.

[24] E. A. Oyekanlu, A. C. Smith, W. P. Thomas, G. Mulroy, D. Hitesh, M. Ramsey, D. J. Kuhn, J. D. Mcghinnis, S. C. Buonavita, N. A. Looper *et al.*, "A review of recent advances in automated guided vehicle technologies: Integration challenges and research areas for 5G-based smart manufacturing applications," *IEEE Access*, vol. 8, pp. 202 312–202 353, 2020.

[25] Z. Li, M. A. Uusitalo, H. Shariatmadari, and B. Singh, "5G URLLC: Design challenges and system concepts," in *2018 15th international symposium on wireless communication systems (ISWCS)*, 2018, pp. 1–6.

[26] M. Darabi, V. Jamali, L. Lampe, and R. Schober, "Hybrid puncturing and superposition scheme for joint scheduling of URLLC and eMBB traffic," *IEEE Communications Letters*, vol. 26, no. 5, pp. 1081–1085, 2022.

[27] K. Pedersen, G. Pocovi, J. Steiner, and A. Maeder, "Agile 5G scheduler for improved E2E performance and flexibility for different network implementations," *IEEE Communications Magazine*, vol. 56, no. 3, pp. 210–217, 2018.

[28] A. A. Esswie and K. I. Pedersen, "Multi-user preemptive scheduling for critical low latency communications in 5G networks," in *2018 IEEE Symposium on Computers and Communications (ISCC)*, 2018, pp. 00 136–00 141.

[29] H. Yin, L. Zhang, and S. Roy, "Multiplexing URLLC traffic within eMBB services in 5G NR: Fair scheduling," *IEEE Transactions on Communications*, vol. 69, no. 2, pp. 1080–1093, 2020.

[30] A. A. Esswie and K. I. Pedersen, "Opportunistic spatial preemptive scheduling for URLLC and eMBB coexistence in multi-user 5G networks," *IEEE Access*, vol. 6, pp. 38 451–38 463, 2018.

[31] T. Jacobsen, R. Abreu, G. Berardinelli, K. Pedersen, P. Mogensen, I. Z. Kovács, and T. K. Madsen, "System level analysis of uplink grant-free transmission for URLLC," in *2017 IEEE Globecom Workshops (GC Wkshps)*, 2017, pp. 1–6.

[32] C. Wang, Y. Chen, Y. Wu, and L. Zhang, "Performance evaluation of grant-free transmission for uplink URLLC services," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, 2017, pp. 1–6.

[33] N. H. Mahmood, R. Abreu, R. Böhnke, M. Schubert, G. Berardinelli, and T. H. Jacobsen, "Uplink grant-free access solutions for URLLC services in 5G new radio," in *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*, 2019, pp. 607–612.

[34] Y. Liu, Y. Deng, M. Elkashlan, A. Nallanathan, and G. K. Karagiannidis, "Analyzing grant-free access for URLLC service," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 3, pp. 741–755, 2020.

[35] A. A. Zaidi, R. Baldemair, H. Tullberg, H. Bjorkegren, L. Sundstrom, J. Medbo, C. Kilinc, and I. Da Silva, "Waveform and numerology to support 5G services and requirements," *IEEE Communications Magazine*, vol. 54, no. 11, pp. 90–98, 2016.

[36] J. Flores de Valgas, J. F. Monserrat, and H. Arslan, "Flexible numerology in 5G NR: Interference quantification and proper selection depending on the scenario," *Mobile Information Systems*, vol. 2021, no. 1, p. 6651326, 2021.

[37] A. Hossain and N. Ansari, "5G multi-band numerology-based TDD RAN slicing for throughput and latency sensitive services," *IEEE Transactions on Mobile Computing*, vol. 22, no. 3, pp. 1263–1274, 2023.

[38] N. Patriciello, S. Lagen, L. Giupponi, and B. Bojovic, "5G new radio numerologies and their impact on the end-to-end latency," in *2018 IEEE 23rd Inter-*

national Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2018, pp. 1–6.

[39] S. Senk, S. A. W. Itting, J. Gabriel, C. Lehmann, T. Hoeschele, F. H. P. Fitzek, and M. Reisslein, "5G NSA and SA campus network testbeds for evaluating industrial automation," in *European Wireless 2021; 26th European Wireless Conference*, 2021, pp. 1–8.

[40] J. Rischke, P. Sossalla, S. Itting, F. H. P. Fitzek, and M. Reisslein, "5G campus networks: A first measurement study," *IEEE Access*, vol. 9, pp. 121 786–121 803, 2021.

[41] S. B. Damsgaard, D. Segura, M. F. Andersen, S. Aaberg Markussen, S. Barbera, I. Rodríguez, and P. Mogensen, "Commercial 5G NPN and PN deployment options for industrial manufacturing: An empirical study of performance and complexity tradeoffs," in *IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2023, pp. 1–7.

[42] I. Rodriguez, R. S. Mogensen, A. Fink, T. Raunholt, S. Markussen, P. H. Christensen, G. Berardinelli, P. Mogensen, C. Schou, and O. Madsen, "An experimental framework for 5G wireless system integration into industry 4.0 applications," *Energies*, vol. 14, no. 15, p. 4444, 2021.

[43] J. Ansari *et al.*, "Performance of 5G trials for industrial automation," *Electronics*, vol. 11, no. 3, p. 412, 2022.

[44] A. Fink, R. S. Mogensen, I. Rodriguez, T. Kolding, A. Karstensena, and G. Pocovi, "Empirical performance evaluation of enterprise Wi-Fi for IIoT applications requiring mobility," in *European Wireless 2021; 26th European Wireless Conference*, 2021, pp. 1–8.

[45] V. Sathya, L. Zhang, and M. Yavuz, "A comparative measurement study of commercial WLAN and 5G LAN systems," in *2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall)*, 2022, pp. 1–7.

[46] V. Sathya, L. Zhang, M. Goyal, and M. Yavuz, "Warehouse deployment: A comparative measurement study of commercial Wi-Fi and CBRS systems," in *2023 International Conference on Computing, Networking and Communications (ICNC)*, 2023, pp. 242–248.

[47] A. Emami, H. Frank, W. He, A. Bravalheri, A.-C. Nicolaescu, H. Li, H. Falaki, S. Yan, R. Nejabati, and D. Simeonidou, "Multi - RAT enhanced private wireless networks with intent-based network management automation," in *2023 IEEE Globecom Workshops (GC Wkshps)*, 2023, pp. 1789–1794.

[48] S. Chandrashekar, A. Maeder, C. Sartori, T. Höhne, B. Vejlgaard, and D. Chandramouli, "5G multi-RAT multi-connectivity architecture," in *2016 IEEE International Conference on Communications Workshops (ICC)*, 2016, pp. 180–186.

[49] N. H. Mahmood, M. Lopez, D. Laselva, K. Pedersen, and G. Berardinelli, "Reliability oriented dual connectivity for URLLC services in 5G New Radio," in *2018 15th International Symposium on Wireless Communication Systems (ISWCS)*. IEEE, 2018, pp. 1–6.

[50] M. Agiwal, H. Kwon, S. Park, and H. Jin, "A survey on 4G-5G dual connectivity: Road to 5G implementation," *IEEE Access*, vol. 9, pp. 16 193–16 210, 2021.

[51] J. Rao and S. Vrzic, "Packet duplication for URLLC in 5G: Architectural enhancements and performance analysis," *IEEE Network*, vol. 32, no. 2, pp. 32–40, 2018.

[52] A. Aijaz, "Packet duplication in dual connectivity enabled 5G wireless networks: Overview and challenges," *IEEE Communications Standards Magazine*, vol. 3, no. 3, pp. 20–28, 2019.

[53] E. J. Khatib, D. A. Wassie, G. Berardinelli, I. Rodriguez, and P. Mogensen, "Multi-connectivity for ultra-reliable communication in industrial scenarios," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, 2019, pp. 1–6.

[54] A. Alicke, J. Rachor, and A. Seyfert, "Supply chain 4.0–the next-generation digital supply chain, mckinsey & company," *Supply Chain Management June*, 2016.

[55] Y. Ding, M. Jin, S. Li, and D. Feng, "Smart logistics based on the internet of things technology: An overview," *Int. J. Logist. Res. Appl.*, vol. 24, no. 4, pp. 323–345, Apr. 2021.

[56] Y. Song, F. R. Yu, L. Zhou, X. Yang, and Z. He, "Applications of the internet of things (IoT) in smart logistics: A comprehensive survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4250–4274, Mar. 2020.

[57] Z. Yang, R. Wang, D. Wu, H. Wang, H. Song, and X. Ma, "Local trajectory privacy protection in 5G enabled industrial intelligent logistics," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2868–2876, Apr. 2022.

[58] G. Li, "Development of cold chain logistics transportation system based on 5G network and internet of things system," *Microprocess. Microsyst.*, vol. 80, p. 103565, Feb. 2021.

[59] J. M. Marquez-Barja, S. Hadiwardoyo, B. Lannoo, W. Vandenberghe, E. Kenis, L. Deckers, M. C. Campodonico, K. dos Santos, R. Kusumakar, M. Klepper, and J. Vandenbossche, "Enhanced teleoperated transport and logistics: A 5G cross-border use case," in *Proc. IEEE Eur. Conf. Netw. Commun. (EuCNC) & 6G Summit*, Jun. 2021, pp. 229–234.

[60] E. J. Khatib and R. Barco, "Optimization of 5G networks for smart logistics," *Energies*, vol. 14, no. 6, p. 1758, Mar. 2021.

[61] J. Zhan, S. Dong, and W. Hu, "IoE-supported smart logistics network communication with optimization and security," *Sustain. Energy Technol. Assess.*, vol. 52, p. 102052, Aug. 2022.

[62] S. Iranmanesh, F. S. Abkenar, R. Raad, and A. Jamalipour, "Improving throughput of 5G cellular networks via 3D placement optimization of logistics drones," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1448–1460, Feb. 2021.

[63] M. Savic, M. Lukic, D. Danilovic, Z. Bodroski, D. Bajović, I. Mezei, D. Vukobratovic, S. Skrbic, and D. Jakovetić, "Deep learning anomaly detection for cellular IoT with applications in smart logistics," *IEEE Access*, vol. 9, pp. 59 406–59 419, 2021.

[64] J. Cheng, Y. Yang, X. Zou, and Y. Zuo, "5G in manufacturing: a literature review and future research," *The International Journal of Advanced Manufacturing Technology*, pp. 1–23, 2022.

[65] B. S. Khan, S. Jangsher, A. Ahmed, and A. Al-Dweik, "URLLC and eMBB in 5G Industrial IoT: A survey," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 1134–1163, 2022.

[66] S. Zhang, "An overview of network slicing for 5G," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 111–117, 2019.

[67] Y. Wu, H.-N. Dai, H. Wang, Z. Xiong, and S. Guo, "A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1175–1211, 2022.

[68] T. Umagiliya, S. Wijethilaka, C. De Alwis, P. Porambage, and M. Liyanage, "Network slicing strategies for smart industry applications," in *2021 IEEE Conference on Standards for Communications and Networking (CSCN)*, 2021, pp. 30–35.

[69] A. Hoglund, D. P. Van, T. Tirronen, O. Liberg, Y. Sui, and E. A. Yavuz, "3GPP release 15 early data transmission," *IEEE Commun. Standards Mag.*, vol. 2, no. 2, pp. 90–96, Jun. 2018.

[70] *Evaluation for early data transmissions*, TSG-RAN WG2 #100, document R2-1713058, 3GPP, Nov. 2017.

[71] O. Liberg, J. Bergman, A. Höglund, T. Khan, G. A. Medina-Acosta, H. Rydén, A. Ratilainen, D. Sandberg, Y. Sui, T. Tirronen, and Y. P. E. Wang, "Narrowband internet of things 5G performance," in *Proc. IEEE 90th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2019, doi: 10.1109/VTCFall.2019.8891588.

[72] F. J. Dian and R. Vahidnia, "A simplistic view on latency of random access in cellular internet of things," in *Proc. 11th IEEE Annu. Inf. Technol. Electron. Mob. Commun. Conf. (IEMCON)*, Nov. 2020, pp. 0391–0395.

[73] R. Barbau, V. Deslandes, G. Jakllari, and A.-L. Beylot, "An analytical model for evaluating the interplay between capacity and energy efficiency in NB-IoT," in *Proc. Int. Conf. on Comput. Commun. and Netw. (ICCCN)*, Jul. 2021, doi: 10.1109/ICCCN52240.2021.9522178.

[74] 3GPP TS 36.300, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall Description; Stage 2 (Release 17)," 3rd Generation Partnership Project, Tech. Rep. V17.5.0, 2023.

[75] 3GPP TR 36.913, "LTE; Requirements for further advancements for Evolved Universal Terrestrial Radio Access (E-UTRA) (LTE-Advanced) (Release 10)," 3rd Generation Partnership Project, Tech. Rep. V10.0.0, 2011.

[76] 3GPP TS 23.401, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 17)," 3rd Generation Partnership Project, Tech. Rep. V17.9.0, 2023.

[77] 3GPP TS 36.211, "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation (Release 17)," 3rd Generation Partnership Project, Tech. Rep. V17.4.0, 2023.

[78] J. Navarro-Ortiz, P. Romero-Diaz, S. Sendra, P. Ameigeiras, J. J. Ramos-Munoz, and J. M. Lopez-Soler, "A survey on 5G usage scenarios and traffic models," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 905–929, 2nd Quart., 2020.

[79] 3GPP TR 21.915, "Release 15 Description; Summary of Rel-15 Work Items (Release 15)," 3rd Generation Partnership Project, Tech. Rep. V15.0.0, 2019.

[80] 3GPP TS 38.300, "NR; NR and NG-RAN Overall Description; Stage 2 (Release 17)," 3rd Generation Partnership Project, Tech. Rep. V17.5.0, 2023.

[81] 3GPP TS 23.501, "5G; System architecture for the 5G System (5GS) (Release 17)," 3rd Generation Partnership Project, Tech. Rep. V17.10.0, 2023.

[82] 3GPP TS 38.104, "5G; NR; Base Station (BS) radio transmission and reception (Release 15)," 3rd Generation Partnership Project, Tech. Rep. V15.19.0, 2023.

[83] 3GPP TS 22.368, "Service Requirements for Machine-Type Communications (MTC); Stage 1 (Release 13)," 3rd Generation Partnership Project, Tech. Rep. V13.2.0, 2016.

[84] TSG RAN Meeting 86, "New SID Support Reduced Capability NR Devices," 3rd Generation Partnership Project, Tech. Rep. RP-193238, 2019.

[85] S. R. Borkar, "Long-term evolution for machines (LTE-M)," in *LPWAN technologies for IoT and M2M applications*. Elsevier, 2020, pp. 145–166.

[86] 3GPP TR 21.914, "Release 14 Description; Summary of Rel-14 Work Items (Release 14)," 3rd Generation Partnership Project, Tech. Rep. V14.0.0, 2018.

[87] 3GPP TR 21.917, "Release 17 Description; Summary of Rel-17 Work Items (Release 17)," 3rd Generation Partnership Project, Tech. Rep. V17.0.1, 2023.

[88] G. Medina-Acosta, L. Zhang, J. Chen, K. Uesaka, Y. Wang, O. Lundqvist, and J. Bergman, "3GPP Release-17 physical layer enhancements for LTE-M and NB-IoT," *IEEE Communications Standards Magazine*, vol. 6, no. 4, pp. 80–86, 2022.

[89] M. Chen, Y. Miao, Y. Hao, and K. Hwang, "Narrow band internet of things," *IEEE Access*, vol. 5, pp. 20 557–20 577, 2017.

[90] M. Kanj, V. Savaux, and M. Le Guen, "A tutorial on NB-IoT physical layer design," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 4, pp. 2408–2446, 2020.

[91] 3GPP TS 36.213, "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures (Release 16)," 3rd Generation Partnership Project, Tech. Rep. V16.6.0, 2021.

[92] 3GPP TR 38.913, "5G; Study on scenarios and requirements for next generation access technologies (Release 17)," 3rd Generation Partnership Project, Tech. Rep. V17.0.0, 2022.

[93] 3GPP TS 23.682, "Architecture enhancements to facilitate communications with packet data networks and applications (Release 16)," 3rd Generation Partnership Project, Tech. Rep. V16.10.0, 2021.

[94] 3GPP TS 24.301, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 16)," 3rd Generation Partnership Project, Tech. Rep. V16.8.0, 2021.

[95] GSMA, "NB-IoT deployment guide to basic feature set requirements," Groupe Speciale Mobile Association (GSMA), Tech. Rep., 2019, (accessed June 2024). [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2019/07/201906-GSMA-NB-IoT-Deployment-Guide-v3.pdf

[96] ——, "LTE-M deployment guide to basic feature set requirements," Groupe Speciale Mobile Association (GSMA), Tech. Rep., 2019, (accessed June 2024). [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2019/08/201906-GSMA-LTE-M-Deployment-Guide-v3.pdf

[97] 3GPP TS 36.321, "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification (Release 14)," 3rd Generation Partnership Project, Tech. Rep. V14.9.0, 2019.

[98] C. Rosa, K. Pedersen, H. Wang, P.-H. Michaelsen, S. Barbera, E. Malkamäki, T. Henttonen, and B. Sébire, "Dual connectivity for LTE small cell evolution: functionality and performance aspects," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 137–143, 2016.

[99] C. Pupiales, D. Laselva, Q. De Coninck, A. Jain, and I. Demirkol, "Multi-connectivity in mobile networks: Challenges and benefits," *IEEE Communications Magazine*, vol. 59, no. 11, pp. 116–122, 2021.

[100] 3GPP TS 36.323, "Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification (Release 17)," 3rd Generation Partnership Project, Tech. Rep. V17.2.0, 2023.

[101] 3GPP TS 33.501, "Security architecture and procedures for 5G System (Release 17)," 3rd Generation Partnership Project, Tech. Rep. V17.11.1, 2023.

[102] J. Munilla, A. Hassan, and M. Burmester, "5G-compliant authentication protocol for RFID," *Electronics*, vol. 9, no. 11, p. 1951, 2020.

[103] J. Arkko, V. Lehtovirta, and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')," IETF RFC 5448, May 2009, (accessed June 2024). [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5448

[104] B. Karakoc, N. Fürste, D. Rupprecht, and K. Kohls, "Never let me down again: Bidding-down attacks and mitigations in 5G and 4G," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 97–108. [Online]. Available: https://doi.org/10.1145/3558482.3581774

[105] 3GPP TS 38.213, "5G; NR; Physical layer procedures for control (Release 17)," 3rd Generation Partnership Project, Tech. Rep. V17.7.0, 2023.

[106] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[107] C. Yu, S. Chen, F. Wang, and Z. Wei, "Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers," *Computer Networks*, vol. 201, p. 108532, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128621004576

[108] "NS-3-A Discrete-Event Network Simulator for Internet Systems," https://www.nsnam.org/, (accessed June 2024).

[109] N. Patriciello, S. Lagen, B. Bojovic, and L. Giupponi, "An E2E simulator for 5G NR networks," *Simul. Model. Pract. Theory*, vol. 96, Nov. 2019, Art. no. 101933.

[110] *Study on Channel Model for Frequencies from 0.5 to 100 GHz*, document TR 38.901, V17.1.0, 3GPP, Jan. 2024.

[111] "5G-simulator: Extended 5G-simulator based on NS-3 and 5G-LENA," https://github.com/dsr96/5g-simulator, (accessed June 2024).

[112] "Amarisoft - AMARI Callbox Classic," https://www.amarisoft.com/test-and-measurement/device-testing/device-products/amari-callbox-classic, (accessed June 2024).

[113] "Amarisoft - AMARI UE Simbox," https://www.amarisoft.com/test-and-measurement/network-testing/network-products/amari-ue-simbox-e-series, (accessed June 2024).

[114] I. Rodriguez *et al.*, "5G swarm production: Advanced industrial manufacturing concepts enabled by wireless automation," *IEEE Communications Magazine*, vol. 59, no. 1, pp. 48–54, 2021.

[115] L. Breiman, "Random forests," *Machine learning*, vol. 45, pp. 5–32, 2001.

[116] G. Hackeling, *Mastering Machine Learning with scikit-learn*. Packt Publishing Ltd, 2017.

[117] E. Bisong and E. Bisong, "Introduction to scikit-learn," *Building machine learning and deep learning models on google cloud platform: a comprehensive guide for beginners*, pp. 215–229, 2019.

[118] W. McKinney *et al.*, "Pandas: a foundational python library for data analysis and statistics," *Python for high performance and scientific computing*, vol. 14, no. 9, pp. 1–9, 2011.

[119] C. R. Harris, K. J. Millman, S. J. Van Der Walt, R. Gommers, P. Virtanen, D. Cournapeau, E. Wieser, J. Taylor, S. Berg, N. J. Smith *et al.*, "Array programming with numpy," *Nature*, vol. 585, no. 7825, pp. 357–362, 2020.

[120] "RA-simulator - A random-access channel simulator for cellular networks," https://github.com/dsr96/ra-simulator, (accessed June 2024).

[121] 3GPP TS 38.211, "NR; Physical channels and modulation," 3rd Generation Partnership Project, Tech. Rep. V16.10.0, 2022.

[122] 3GPP TS 38.321, "NR; Medium Access Control (MAC) protocol specification," 3rd Generation Partnership Project, Tech. Rep. V16.10.0, 2022.

[123] 3GPP TS 38.331, "NR; Radio Resource Control (RRC); Protocol specification," 3rd Generation Partnership Project, Tech. Rep. V16.10.0, 2022.

[124] Intel NUC Kit NUC5i3MYHE. (accessed June 2024). [Online]. Available: https://www.intel.co.uk/content/www/uk/en/products/sku/84860/intel-nuc-kit-nuc5i3myhe/specifications.html

[125] Simcom SIM8202G-M2. (accessed June 2024). [Online]. Available: https://www.simcom.com/product/SIM8202X_M2.html

[126] MiR200 Data Sheet. (accessed June 2024). [Online]. Available: https://www.ics-id.de/mir.html?file=files/ics-id.de/downloads/MIR200/Technische%20Daten%20MiR%20200%20%28EN%29.pdf

[127] Mpconn - The open source multi-path connectivity tool. (accessed June 2024). [Online]. Available: https://github.com/drblah/mpconn

[128] C. Baena, O. S. Peñaherrera-Pulla, L. Camacho, R. Barco, and S. Fortes, "Video streaming and cloud gaming services over 4G and 5G: A complete network and service metrics dataset," *IEEE Communications Magazine*, vol. 61, no. 9, pp. 154–160, 2023.