UNIVERSITÀ
DEGLI STUDI
DI PADOVA

UNIVERSITY OF PADOVA

DEPARTMENT OF INFORMATION ENGINEERING

Master degree in ICT for Internet and Multimedia

Evaluation of performance and security of 5G for IEC 61850 based communications in power grids

Supervisor
Professor Stefano Vitturi

Co-supervisor
Michele Luvisotto
Hitachi Energy

Master Candidate
Francesco Trolese
Student ID: 2050698

Academic Year
2022–2023

To those who stand by me every day.

Abstract

The rapid advancement of wireless telecommunication technologies, particularly the emergence of 5G networks, sparked significant interest in their potential applications in various scenarios, among which critical infrastructure communications. In particular, the power grid sector is undergoing a massive evolution with the adoption of standards like IEC 61850, which could facilitate efficient and standardized communication within substations and across power networks. This thesis serves as a bridge between these two domains, investigating the synergy between cutting-edge telecommunication technologies and modern power grid architectures. The integration of 5G technology with IEC 61850 standard holds promise for optimizing the real-time monitoring, control, and management of power systems, contributing to increased operational efficiency, reduced deployment costs and improved fault management. This study offers an evaluation of the performance of applying 5G to IEC 61850-based communications in power grids. In parallel, as power grids evolve into "smart grids," the importance of secure and resilient communication becomes paramount. By investigating potential vulnerabilities and countermeasures, this thesis aims to provide insights that help the industry to deploy 5G-enabled communication networks while upholding the highest standards of data protection and system integrity.

Contents

Listing of figures

Listing of tables

1 Introduction

Telecommunications play a crucial role in critical infrastructure, defined as systems and assets essential for the functioning of society and the economy. These systems include power grids, transportation networks, and water treatment plants, among others. Without reliable and secure communication networks, often referred to in this context as mission-critical networks, the functioning of critical infrastructure can be severely compromised, leading to disastrous consequences for public safety and national security. Telecommunications for critical infrastructure are designed to meet the unique needs of these systems. To ensure the highest performance and security, networks used in this context are often closed systems which are heavily optimized for a specific application. The term OT (operational technology) is often used to refer to such systems, in contrast with the more versatile solutions used in consumer-based applications which are often generally referred to as IT (information technology).

As shown in Fig. 1.1, the evolution of communication protocols used in IT and OT applications has followed different paths. While IT protocols have evolved towards more open and versatile solutions, OT protocols have been optimized for specific applications, resulting in a wide range of different standards. However in recent years, the continuous release of new OT protocols has slowed down, while IT protocols have continued to evolve.

There exist currently two trends in the industrial-grade communication landscape that motivate this behaviour: the first one consists in refining OT network capabilities to improve their performance (latency, reliability, determinism, etc.). The second one is to progressively harmonize IT and OT networks, aiming at re-using the same technologies in both fields. The two trends are somehow conflicting: although the best performance is typically achieved by closed systems, integrated systems would greatly simplify organization challenges allowing vertical integration across multiple levels and horizontal integration across different industrial sectors. The shift from IT to OT protocols entails significant challenges, such as ensuring that the adopted IT solutions can provide the levels of performance and security required by critical infrastructure applications.

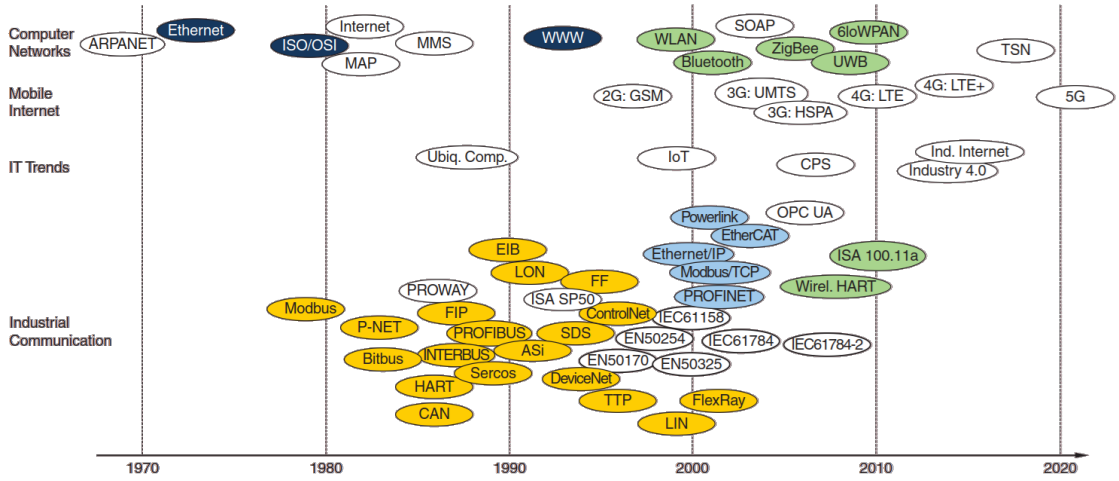


Figure 1.1: IT and OT protocols over the years. Source: [1]

The increased complexity of critical infrastructure, coupled with the growing capabilities of IT solutions calls for a convergence between IT and OT solutions. In this vision, technologies typically used in IT contexts (e.g. wireless cellular communication networks) are adapted to applications typically relying on OT solutions, with significant benefits in terms of versatility, interoperability and cost.

A particular segment of critical infrastructure is represented by power grids. The path to de-carbonization and sustainable development involves massive integration of renewable energy sources in power grids. Such a goal would significantly benefit from a more pervasive deployment of communications in power grids, which would improve their observability and controllability. Currently, critical control and protection applications in power grids either avoid any use of communications, with consequent performance limitations, or rely on dedicated communication infrastructure, with high cost and limited scalability. There is hence a strong interest to explore to which extent emerging wireless networking technologies, such as 5G, could be applied in this scenario, facilitating the integration of renewables, and simplifying the path to a sustainable future.

One of the most significant challenges in this direction is ensuring the reliability and availability of the communication network. In power grids, for example, disruptions in communications can have severe consequences, including power outages and system failures. Additionally, wireless communication devices deployed in power grid applications will face harsh environments characterized by extreme temperatures, heavy electromagnetic interference, significant presence of metallic obstacles, etc., which will further challenge the reliability of wireless communications. Another significant challenge that can be expected is connected to latency. Low latency in the order of few milliseconds is required in the most advanced control applications, and it is notoriously challenging to achieve over wireless networks, especially if combined with high reliability.

Besides the challenges related to performance of 5G-based power grid applications, their se-

curity is also a pressing concern for grid operators. Moving from closed OT systems to more interconnected IT solutions corresponds to an increase in exposure to cyber-attacks. Due to their strategic importance, critical infrastructure networks such as those used in power grids are particularly vulnerable to cyber-attacks and there is significant evidence of real-world attacks on this infrastructure. The first acknowledged successful cyberattack targeting a power grid took place in 2015 and caused a 6 hours power outage for about 230.000 customers in and around Ukraine's capital city of Kiev [2]. More recently (2023), security researchers discovered a Russian industrial control system malware, never exploited in a cyberattack but potentially able to disrupt critical infrastructure systems and electric grids in the ongoing Russo-Ukrainian War [3]. In this context, the introduction of any new technology, especially if concerned with exchange of critical data between remote locations, has to be carefully considered and designed. Moreover, wireless networks present specific security risks compared to wired ones, such as increased likelihood of eavesdropping and jamming.

To summarize, wireless communications in critical infrastructure and power grids present a range of challenges, including performance and security. However, with the right technical solutions, these challenges can be addressed and wireless networks can provide significant benefits to critical infrastructure environments, including increased flexibility, reduced cost, and improved scalability from a business perspective.

The focus of this work is the study of 5G applied to communications based on IEC 61850, one of the main international standards for data exchange used in the electrical power grid. This will in turn enable grid operators to pervasively deploy communications in a more flexible and cost-effective manner, compared to today's solutions based on wired networks, improving the observability and controllability of power grids and ultimately contributing to a faster energy transition.

This thesis contributes to the literature by providing a comprehensive evaluation of the performance and security aspects of 5G technology in the context of IEC 61850-based communications in power grids. First, we implement a simulation testbed to analyze the performance of different 5G network topology for IEC 61850 traffic, focusing on two types of messages defined by the IEC standard: MMS (Manufacturing Message Specification) and SV (Sampled Values). Furthermore, we analyze the security implications of 5G networks in power grid environments, considering potential vulnerabilities and countermeasures. Our findings highlight the potential of 5G to enhance communication in power grids while emphasizing the importance of robust security measures for safeguarding critical infrastructure.

This document is organized as follows. Chapter 2 provides a literature review on wireless communication for IEC 61850, low-latency communications over 5G and cybersecurity considerations for both 5G and IEC 61850. In Chapter 3 we provide background information on IEC 61850 and 5G. Then we delve into the methodologies and tools used to carry out the simulations. Chapter 4 describes the applications and topologies considered. Chapter 5 presents the results of our performance evaluation. Chapter 6 provides an overview of the security implications of 5G networks in power grids, including potential vulnerabilities and countermeasures. Finally, Chapter 7 concludes the thesis and provides an outlook on future work.

2

Related works

Although literature in wireless telecommunications and mission-critical communications for power grids considered separately is very advanced, it does not appear that the joint study of the two topics has yet been dealt with in depth. Ever since the introduction of IEC 61850 as an international standard for substation communications in power grids there has been academic interest in the possibility of replacing wired Ethernet links commonly used in IEC 61850 networks with wireless technologies, which would further reduce the cost and facilitate the deployment. However, given the challenging requirements of some IEC 61850 traffic classes (especially in terms of latency) and the relatively low performance offered by wireless technologies in this aspect, practical evaluations have been limited so far. This chapter provides an overview of the literature related to wireless communications for IEC 61850, low latency communications over 5G and cybersecurity measures both for 5G and IEC 61850.

2.1 Wireless communications for IEC 61850

A few papers have explored the possibility of introducting different wireless technologies in IEC 61850 networks. [4] reports an extended investigation of WLAN (Wireless LANs, commonly known as WiFi) for various smart distribution substation applications, as tap changer control and monitoring and feeder over current protection. The paper focuses on the IEC 61850 communication standard which is the main standard used for communications in power grids. The work starts by identifying the potential smart distribution substation applications, for which wireless LAN can be used. The performance of wireless LAN is then assessed with respect to the latency requirement criteria specified in the standard. This investigation using laboratory and field tests demonstrate suitability of an industrial WLAN for some of the presented innovative smart-distribution substation applications. [5] further expands this direction by providing a comprehensive review of several wireless technologies e.g. ZigBee, WiMAX, WLAN, Wireless HART, etc., with regard to

their features, suitability for substation communications and need for research.

Although some of these wireless technologies present interesting possibilities, a fundamental concern is related to latencies. IEC 61850, in fact, defines an upper bound on the end-to-end latency for each type of message it defines. For some applications, this latency must be in the order of a few milliseconds (e.g. 3 ms). For this reason, wireless networks need to be optimized to process and transmit packets with minimal low latency. Another common issue of wireless communication protocols regards the additional cybersecurity measures required with respect to wired protocols. In mission-critical applications such as power grids security is a fundamental requirement and the use of wireless technologies can introduce new vulnerabilities.

2.2 Low-latency communications over 5G for power grids applications

One of the primary goals of 5G since its introduction has been the possibility to achieve URLLC (Ultra-Reliable and Low-Latency Communications) to support mission-critical applications, which is fully in line with the demands of IEC 61850-based power grids. Several research works have been published describing techniques that can be used for URLLC over 5G. [6] presents a survey on some of the challenges and possible solutions for delivering end-to-end, reliable, ultra-low-latency services in mmWave cellular systems regarding the MAC layer, congestion control, and core network architecture. Both [7] and [8] report some results obtained through simulations that show different techniques are used to achieve URLLC. However, none of these works deals specifically with the requirements and constraints of power grid applications. A few recent works have started evaluating 5G networks with URLLC capabilities for usage in power grids applications and proposing improvements. [9] offers a possible solution to the problem of IEC 61850 based data packet sizes, which are not optimal for wireless communication networks. To decrease packet loss, the authors propose an innovative solution to aggregate multiple IEC 61850 messages in a single Ethernet frame. The results show that aggregating small packets can decrease packet loss in the wireless communication channel. Additionally, packet aggregation can be implemented by network engineers without extensive knowledge on IEC 61850. [10] proposes a smart grid cyber-physical testbed for protection systems. It consists of power system applications and a 5G communication network modelled in ns-3. A Permissive Underreaching Transfer Trip (PUTT) protection scheme was demonstrated on the testbed and its performance was evaluated using a 5G network scenario. In [11] the author analyze IEEE 802.11g, 4G LTE and 5G NR performances for handling SV traffic in a digital substation scenario. IEEE 802.11g as well as 4G LTE were tested in a laboratory environment. IEEE 802.11g resulted in a significant packet loss compared to the sending cycle, thus excluding the possibility of using this technology for SV data transmission. 4G LTE achieved limited success with a round-trip latency of 19.25 ms. On the contrary, significant improvements were observed in a simulated 5G network, for which the latency was within the desired range of 3 ms. This thesis work expands the directions above by carrying out extensive simulations of different IEC 61850 traffic types over a state-of-the-art 5G network simulators, exploring the

impact of different architectural choices. A key innovative is the usage of a recognized open-source IEC 61850 library (further described in Chapter 3) to feed the simulation model with real IEC 61850 traffic, thus ensuring higher confidence on the conclusions.

2.3 Cybersecurity considerations for IEC 61850

Network security is one of the greatest concerns in power grids, a critical infrastructure whose operation must be protected from intentional attacks. In the recent years, as reported in [2] and [3], cyber attacks against power grids have been reported. This fact shows how nowadays even people life can depend on the security of critical infrastructure networks making it a crucial concern not only for manufacturers but also for states and governments. Historically, isolated networks and proprietary protocols have been widely used in power grids, so the "security by obscurity" approach was sufficient. However, with the standardization of communication protocols for power systems, the increasing need for openness and interconnection of the network infrastructure, and the growing number of intentional attacks targeting power grids, this assumption no longer holds. For this reason, different studies have been carried out about the security of IEC 61850. In 2007 the IEC released the IEC 62351 standard, which provides guidelines and recommendations for ensuring the confidentiality, integrity, and availability of data exchanged in power system automation and control applications. [12] provides a comprehensive examination of security risks, potential attacks, and the security needs related to IEC 61850 communication. Additionally, the security measures outlined in IEC 62351, aimed at safeguarding various IEC 61850 message types like GOOSE (Generic Object-Oriented Substation Events), SV, R-GOOSE (Routable-GOOSE), R-SV (Routable-SV) and MMS messages are discussed. In [13] the authors point out some vulnerabilities in the algorithms or parameters chosen in parts of the IEC 62351. On the other hand, they note that the need for backward compatibility has led to some design choices that provide less security and conclude that the standard can significantly improve security in power systems if applied holistically. Apart from IEC 62351, also other efforts have been made to provide security to IEC 61850 communications. In [14] for example is presented an open source IEC 61850 MMS Traffic Parser, which can be integrated into Intrusion Detection Systems (IDS) in order to identify cyberattacks. The use of wireless communication technologies such as 5G instead of Ethernet introduces new vulnerabilities in IEC 61850 networks, e.g. the disruption of the communication or the eavesdropping of the data on the radio channel therefore it is important to consider the security implications of these technologies.

2.4 Cybersecurity considerations for 5G

Security considerations for MTC (Machine Type Communication) applications in 5G are crucial due to the potential impact of any compromise in these interconnected systems. In [15] the authors show the key security advancements in terms of user plane security termination, authentication and authorization, RAN (Radio Access Network) security, security for UE and network slicing security. It also introduces security for IoT. In [16] the authors provide an overview of 5G security issues

and the existing and newly proposed technologies designed to overcome them. They categorize security technologies using Open Systems Interconnection (OSI) layers. Their focus relies on the physical layer between the base stations and users' devices which presents great opportunities for attacks such as eavesdropping and data fabrication. [17] provides an overview on security for Public-Network Integrated Non-Public Networks (NPNs) and Standalone NPNs. The main focus was set on summarizing requirements, architecture and authentication considering alternative authentication methods without the need for USIM in the UE. Finally, [18] focuses on the secure deployment of 5G in a smart grid. It contributes by presenting a threat model and showing how 5G network security features, according to the released 3GPP standard, can support the needs of a smart grid scenario. This work contributes to the literature by presenting a threat model of the power grid communication scenarios we considered. Then, we show how IEC 61850, together with 5G security features, according to the released 3GPP standard, can provide countermeasures to the highlighted threats. Finally, we propose a security feature to overcome the vulnerabilities not yet addressed by the standards.

3
Background and tools

This chapter provides an overview of the background technologies and tools involved in this work. First of all the standard IEC 61850 for substation automation is explained. Then, we dig into 5G details and give an overview of ns-3 network simulator. Finally, we explain the methodologies used to carry out the performance evaluation.

3.1 IEC 61850

IEC 61850 is an international standard for communication protocols and data models used in the electrical power grid. It was developed by the International Electrotechnical Commission (IEC) to address the need for interoperability and communication between various IEDs (Intelligent Electronic Devices) used in power systems. Before the introduction of IEC 61850, communication in power systems relied on proprietary protocols that often lacked interoperability. This meant that devices from different manufacturers were not able to communicate and exchange information. This also hindered the integration of advanced functionalities and automation in the power grid. In the 1990s, there was a growing demand for a standardized communication protocol that could facilitate seamless interaction between devices from different vendors. In response to this need, the IEC initiated the development of IEC 61850, which began in 1995 and culminated in the release of the first edition of the standard in 2003. The primary benefits introduced by IEC 61850 to the power industry are:

- Interoperability and vendor independence: The standard aims to ensure interoperability between IEDs from different manufacturers. This allows utilities and system integrators to choose devices from various vendors without worrying about compatibility issues.
- Flexibility and Scalability: IEC 61850 provides a flexible framework that supports both current and future requirements of power systems. It can adapt to changes in technology

and evolving grid architectures, making it suitable for diverse applications.

- Advanced Functionality: The standard enables the integration of advanced functionalities, such as protection, automation, control, and monitoring, into power systems. It supports real-time data exchange and provides a standardized approach for implementing complex applications. Its design allows it to accommodate future advancements in power system technology and provides a foundation for the integration of renewable energy sources, energy storage systems, and smart grid functionalities.

IEC 61850 introduces also the SCL (Substation Configuration Language): an XML-based language used to describe the configuration of IEDs and their communication relationships within a substation. It enables the exchange of configuration information between different tools and systems.

Overall, IEC 61850 has become the leading standard for communication in electrical substations and power systems. Its widespread adoption has transformed the way devices communicate and collaborate, enabling more efficient and reliable operation of the modern power grid.

3.1.1 Standard structure and content

IEC 61850 is divided into several parts, each covering specific aspects of the standard. The standard is continuously evolving, and new parts are added or existing parts are revised to address emerging requirements and technologies. Here is an overview of the structure and content of some key parts of IEC 61850 relevant to this work.

- IEC 61850-1: Introduction and Overview. This part provides an introduction to the standard and an overview of its objectives, scope, and key concepts. It explains the principles of communication and data modelling in IEC 61850 and sets the foundation for understanding the other parts of the standard.

- IEC 61850-2: Glossary. This part defines the terms, abbreviations, and acronyms used in IEC 61850. It serves as a reference for consistent understanding and usage of terminology throughout the standard.

- IEC 61850-3: General Requirements. It outlines the general requirements for the communication networks and systems used in power utility automation. It covers aspects such as system architecture, communication protocols, data modelling, and security.

- IEC 61850-4: System and Project Management. This part provides guidelines for the management of IEC 61850-based systems and projects. It includes recommendations for system engineering, configuration management, testing, and documentation.

- IEC 61850-5: Communication Requirements for Functions and Device Models. It focuses on the communication requirements for specific functions and device models within the power system. It defines the communication services, data objects, and services required for functions such as protection, control, measurement, and monitoring.

- IEC 61850-6: Configuration Language and Data Models. Part 6 introduces the SCL and the data models used for describing the configuration of IEC 61850-based systems. It defines the XML-based syntax and structure of SCL and provides guidelines for creating and exchanging SCL files.

- IEC 61850-7: Basic Communication Structure for Substation and Feeder Equipment. Part 7 specifies the basic communication structure for substation and feeder equipment. It defines the services, protocols, and communication profiles to be used for the exchange of data between IEDs in a substation. In particular, IEC 61850-7-2 defines the ACSI (Abstract Communication Service Interface) that forms the basis for the communication between IEC 61850 devices. It specifies the service operations and parameters used for exchanging information, such as reading and writing data, controlling devices, and reporting events. IEC 61850-7-3: Common Data Classes standardizes the common data classes used for representing various types of data in power utility systems. It includes classes for voltage, current, status, measurement values, control commands, and more. These data classes provide a consistent and interoperable way of representing information across different devices and systems. IEC 61850-7-4 introduces compatible logical node classes and compatible data classes. Compatible logical node classes group related logical nodes and provide a standardized way of organizing functionality. Compatible data classes define standardized data objects for specific functionality or equipment types.

- IEC 61850-8: SCSM (Specific Communication Service Mapping). Part 8 focuses on the mapping of IEC 61850 communication services to specific communication protocols and technologies. It provides mappings for protocols among which Ethernet. In particular, IEC 61850-8-1 provides the methodology to map from the IEC 61850-7-2, IEC 61850-7-3, and IEC 61850-7-4, all detailed above, into MMS.

- IEC 61850-9: Specific Communication Service Mapping for Mappings Over Serial Unidirectional Multidrop Point-to-Point Links. It specifies the mapping of IEC 61850 communication services over serial unidirectional multidrop point-to-point links. In particular, IEC 61850-9-2 defines the communication requirements for the transmission of SV over Ethernet-based networks in the context of substation automation systems. This standard focuses on the communication between MU (merging units) and PBI (process bus interfaces) in electrical substations. SV are the digitized versions of analog signals, such as voltage and current measurements, and are used for real-time monitoring, control and protection of substation equipment.

- IEC 61850-90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118. It specifically deals with the communication between substations and control centers, often referred to as PMUs (Phasor Measurement Units). The standard specifies the requirements for exchanging synchrophasor data, which includes measurements of voltage, current, and phase angle, among others.

These are just few of the parts of IEC 61850. There are additional parts that cover topics such as conformance testing and system configuration tools which have not been reported above because they are not relevant for this thesis. It is important to note that the structure and content of each part may evolve over time as the standard is revised and updated to address industry requirements and technological advancements.

3.1.2 IEC 61850 protocols with performance requirements

In IEC 61850 every message function correspond to an interface type. Table 3.1 shows the correspondence between the 11 interface types and their respective function.

Interface type	Function
IF1	Protection-data exchange between bay and station level
IF2	Protection-data exchange between bay level and remote protection
IF3	Data exchange within bay level
IF4	Current and voltage transformers instantaneous data exchange (especially samples) between process and bay level
IF5	Control-data exchange between process and bay level
IF6	Control-data exchange between bay and station level
IF7	Data exchange between substation (level) and a remote engineer's workplace
IF8	Direct data exchange between the bays especially for fast functions such as interlocking
IF9	Data exchange within station level
IF10	Control-data exchange between substation (devices) and a remote network control centre (beyond the scope of IEC 61850)
IF11	Control-data exchange between different substations

Table 3.1: Interface types and their function

As reported in Fig 3.1 different interfaces are exploited at different levels for substation communication. IF 1, 3, 6, 8, 9 are used for communication in the station bus, between station level and bay level. Similarly, IF4 and IF5 support the communication in the process bus, used for data exchange between bay and process level.

The standard defines seven types of messages, each one supporting specific interfaces. The types of messages and their relation with interfaces are schematized in Table 3.2. The table shows also the mapping of these messages to the communication stack, better represented in Fig. 3.2.

The two most relevant message types for this work are SV and MMS, referred to by Fig. 3.2 as Client-Server. SV are analog or digital measurements sampled at a specific rate and sent by IEDs to the MUs in a substation with a publisher/subscriber communication model. This enables the transfer of real-time data for applications such as protection and control. To achieve lower latency this protocol is mapped directly to Ethernet. On the other hand, MMS is a server/client type communication. This protocol is used for information exchange between IEDs and higher-level devices (i.e. SCADAs). As shown in Fig. 3.2, the protocol is mapped on TCP/IP and enables the client to read/write data, read configuration and exchange files with the server.

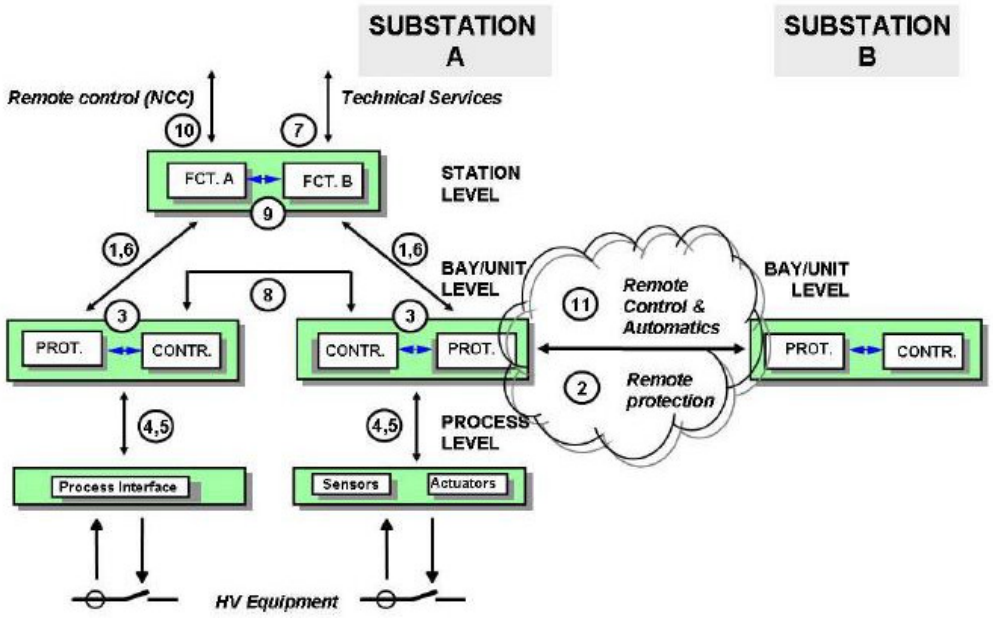


Figure 3.1: Interface model for inter and intra-substation communication

IEC 61850 also defines, for each message type, requirements on the latency or transfer time, defined as the time elapsed from the moment the sender (IED) puts the data content on top of its transmission stack up to the moment the receiver (IED) extracts the data from its transmission stack [4]. For this thesis the focus is on Type 4 SV messages, which have, according to the standard, a latency requirement of less than 3 ms for the protection functions. This thesis studies also Client-Server MMS communication, characterized by less strict requirements on latency which vary with the application. The latency requirement for MMS considered for this work is less than 100 ms, as it is for the most time critical MMS message type.

3.1.3 libIEC61850: an open source IEC 61850 implementation

libIEC61850 is an open-source software library that implements the communication protocols and data models defined in the IEC 61850 standard [19]. It provides a set of functions and utilities that enable the development of IEC 61850-compliant applications and systems. It is written in C language and available under the GPLv3 license.

The libIEC61850 library offers a programming interface that allows software developers to interact with devices in an IEC 61850-based power system. It provides the necessary functions to establish communication connections, send and receive messages, and access the data objects defined in the standard.

The key features of libIEC61850 are the following:

1. Communication Protocol Implementation: The library implements the communication protocols specified in IEC 61850, providing the APIs for IEC 61850/MMS server and client, IEC

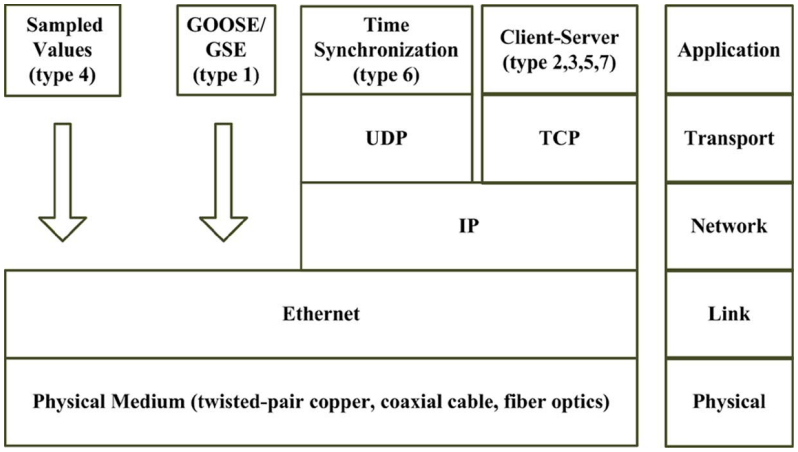


Figure 3.2: Message communication stack of IEC 61850

Message type	Communication protocol	Interface support
Type 1 1a – Trip 1b – Others Message	Direct on Ethernet Link Layer	IF 3,5,8
Type 2: Medium Speed Message	Client Server (TCP/IP)	IF 3,8,9
Type 3: Low Speed Message	Client Server (TCP/IP)	IF 1,3,4,5,6,8,9
Type 4: Raw Data Message	Direct on Ethernet Link Layer	IF 4
Type 5: File Transfer	Client Server (TCP/IP)	IF 1,3,4,6
Type 6: Time Synchronization Message	UDP/IP	IF 1,3,4,5,6,8,9
Type 7: Command Message with Access Control Message	Client Server (TCP/IP)	IF 1,6,7

Table 3.2: Message types and their interface support

61850/GOOSE and IEC 61850-9-2/SV publisher and subscriber. It handles the underlying network communication, including the establishment of connections and message parsing.

2. Data Model Access: libIEC61850 provides functions to access the data objects defined in the IEC 61850 data model. It allows reading and writing data attributes, subscribing to data changes, and handling events and alarms. This enables applications to interact with IEDs and retrieve real-time information from the power system.

3. SCL Parsing and Configuration: The library includes utilities for parsing and handling SCL files. SCL defines the configuration of IEC 61850-based systems, and libIEC61850 allows developers to read SCL files, extract configuration information, and configure IEC 61850 devices accordingly.

4. Integration with Existing Systems: libIEC61850 can be integrated into existing software applications and systems to add IEC 61850 communication capabilities. It provides APIs

and interfaces for different programming languages, including C, C++, and Python, making it flexible and accessible for developers.

5. Cross-Platform Compatibility: The library is designed to be cross-platform and can be used on various operating systems, such as Windows, Linux, and macOS. It supports different network protocols, including Ethernet and serial communication, enabling communication with a wide range of devices and systems.

libIEC61850 is widely used by researchers, system integrators, and developers working in the field of power system automation and control. It simplifies the implementation of IEC 61850-compliant solutions and accelerates the development of applications that leverage the capabilities of the standard.

3.2 5G

Fifth Generation (5G) wireless technology is the latest advancement in cellular networks, improving on the previous generations of mobile communication systems. It represents a significant leap forward in terms of speed, capacity, and connectivity compared to its predecessors, enabling a wide range of innovative applications and services. The first generation of mobile networks (1G) introduced analog cellular technology, which was primarily focused on voice communication. Subsequent generations witnessed significant advancements, with 2G bringing digital communication and text messaging, 3G enabling mobile internet access, and 4G enhancing data speeds to support video streaming and other data-intensive applications. The development of 5G technology aimed to address the increasing demand for faster and more reliable wireless communication. Its aim is to deliver significantly higher data rates, lower latency, improved capacity, increased network flexibility, and enhanced user experience compared to 4G networks. 5G is expected to provide a platform for transformative technologies such as the IoT (Internet of Things), autonomous vehicles, AR (Augmented Reality), VR (Virtual Reality), and smart cities. International organizations, such as the 3GPP (3rd Generation Partnership Project), have been instrumental in defining the specifications and standards for 5G. The 3GPP's Release 15, completed in 2018, introduced the first set of 5G functionalities, also known as NSA (Non-Standalone) 5G, which relied on existing 4G infrastructure. Subsequent releases, including Release 16 and Release 17, expanded these standards, enabling SA (Standalone) 5G networks and introducing further enhancements and capabilities. Release 16, among the other features, focuses on massive MTC, ultra-reliable critical machine communication, NPN, time sensitive communication and 5G LAN.

3.2.1 5G features and technologies

The above mentioned features are building blocks for enabling support for Industrial IoT [17]. Non-Public Networks enable the deployment of 5G systems for private use. There are two deployment models: SNPN (Stand-alone Non-Public Network) and Public Network Integrated NPN (PNI-NPN). SNPN is operated by an NPN operator and doesn't rely on functions from a PLMN

(Public Land Mobile Network). PLMN ID and NID combinations identify SNPNs, and the SNPN RAN broadcasts this information for network selection and access control.

These advancements will play a crucial role in enabling 5G for various Industry 4.0 and factory automation use cases, contributing to the growth and integration of 5G technology in diverse industrial settings, including power grids.

To achieve its ambitious goals, 5G incorporates several key technological advancements [20].

- mmWave (Millimeter Wave) Spectrum: compared to previous generations, 5G introduced the capability of utilizing higher-frequency bands, including the mmWave spectrum, which offers greater bandwidth for faster data transmission. However, mmWave signals have a shorter range and can be affected by obstacles, requiring the deployment of more small cells and advanced beamforming techniques.

- Massive MIMO (Multiple-Input, Multiple-Output): 5G networks employ massive MIMO technology, which utilizes a large number of antennas at the base station and user devices to increase network capacity, enhance spectral efficiency, and improve signal quality.

- Network Slicing: This concept allows the division of a single physical network infrastructure into multiple virtual networks, each tailored to specific applications or services. Network slicing enables customized quality of service (QoS), security, and latency requirements for diverse use cases simultaneously on the same infrastructure.

- Edge Computing: 5G aims to bring computing resources closer to the network edge, reducing latency and enabling real-time processing for applications that require instantaneous response times. This facilitates services such as autonomous vehicles, remote surgery, and smart infrastructure management.

- Network Function Virtualization (NFV) and Software-Defined Networking (SDN): 5G networks leverage NFV and SDN technologies to enable flexible and dynamic network management. NFV allows network functions to be virtualized and run on general-purpose hardware, while SDN enables centralized control and management of the network.

As 5G continues to be deployed worldwide, its impact on various sectors and the realization of its full potential are yet to be fully realized. However, the technological advancements and possibilities it presents make 5G an essential pillar of the ongoing digital revolution.

3.2.2 Architecture of 5G networks

The architecture of a 5G network is designed to support the next generation of wireless communication technology, providing higher data rates, lower latency, increased capacity and improved reliability compared to previous generations.

Below is reported a high-level overview of the key components and architectural elements of a typical 5G network, schematized in Fig. 3.3.

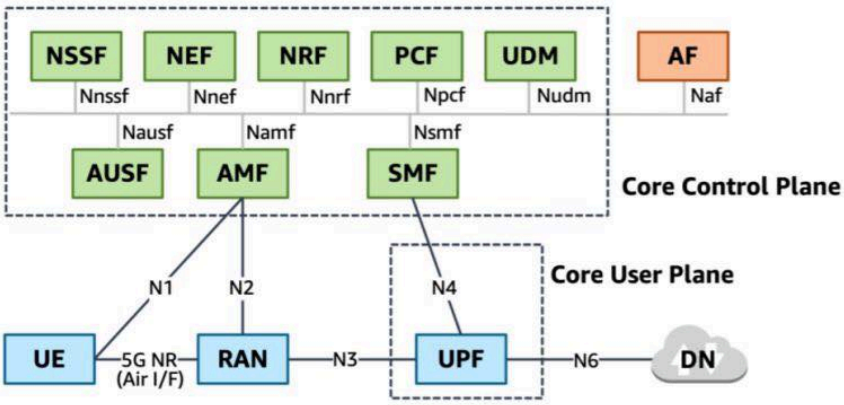


Figure 3.3: 5G network architecture. Source: [21]

User Equipment (UE) It refers to the end-user devices such as smartphones, tablets, IoT devices, and other devices capable of connecting to the 5G network.

Radio Access Network (RAN) The RAN is responsible for establishing a wireless connection between the UE and the core network. It consists of base stations, which are called gNBs (Next Generation NodeB) in 5G, and associated equipment. The RAN provides the air interface for communication, manages radio resources, and handles tasks like authentication, encryption, and modulation/demodulation.

Core Network (CN) Provides the central intelligence and management for the 5G network. It includes several key elements. The AMF (Access and Mobility Management Function) manages access and mobility-related functions, including session management, mobility management, and connection management. The SMF (Session Management Function) handles session-specific tasks such as session establishment, IP address assignment and Quality of Service (QoS) management. The UPF (User Plane Function) manages the user data and handles tasks like packet routing, forwarding, and deep packet inspection. It plays a crucial role in ensuring low latency and high-speed data transmission. NSSF (Network Slice Selection Function) is responsible for selecting the appropriate network slice based on user requirements and network conditions. The AUSF (Authentication Server Function) handles user authentication and security functions. The PCF (Policy Control Function) manages policy-related decisions, such as QoS enforcement, network access rules, and resource allocation. The UDM (Unified Data Management) handles user-related data and functions like subscriber authentication, authorization, and user profile management. Finally the NEF (Network Exposure Function): enables third-party applications and services to access specific network functions and services.

It's important to note that the architecture of a 5G network can vary slightly depending on the specific implementation and deployment scenario. However, the general concepts and components mentioned above provide a foundation for understanding the key elements of a typical 5G network

architecture.

3.2.3 Configurations and parameters

In a 5G network, several parameters can influence the performance of the system. This section provides an overview of some key parameters, mainly within the 5G RAN, that play a role in shaping the performance characteristics of a 5G network and have been evaluated in this thesis.

Central Frequency The central frequency refers to the carrier frequency used for transmitting signals in the 5G network. It influences the coverage range, propagation characteristics, and available bandwidth. Different frequency bands, such as sub-6 GHz (also defined as FR1) and mmWave (also defined as FR2), have different characteristics in terms of coverage area and data rate capabilities.

Numerology Numerology refers to the subcarrier spacing and symbol duration used in 5G waveform design. It determines the bandwidth and time resolution of the signals transmitted over the air interface. Different numerology options are available in 5G, such as 15 kHz, 30 kHz, 60 kHz, and 120 kHz. The choice of numerology affects the data rate, latency, and spectral efficiency of the system.

Modulation and Coding Scheme (MCS) MCS determines the modulation scheme and coding rate used for data transmission. It defines how information is encoded into symbols and transmitted over the air interface. Higher MCS values indicate more complex modulation schemes with higher data rates but potentially more susceptible to errors. The selection of the appropriate MCS depends on channel conditions, SNR (Signal-to-Noise Ratio), and desired data rate. AMC (Adaptive Modulation and Coding) is a technique used to optimize the transmission parameters based on the current channel conditions, which is subject to varying levels of noise, interference, and fading. AMC continuously monitors the channel conditions and selects the appropriate MCS based on the observed SNR. In good channel conditions, it might use higher-order modulation and less error correction coding to achieve higher data rates. In poor channel conditions, it might switch to lower-order modulation and stronger error correction coding to maintain reliable communication.

Error correction techniques are employed to enhance the reliability and robustness of wireless communication. FEC (Forward Error Correction) coding schemes, such as Turbo codes and LDPC (Low-Density Parity Check) codes, are used to add redundancy to transmitted data, allowing for error detection and correction. The choice of coding schemes impacts the system's resilience to channel impairments and noise.

Scheduling Scheduling is the process of allocating radio resources, such as time and frequency slots, to different users in the network. Effective scheduling algorithms and strategies are crucial for managing the allocation of resources and optimizing system performance. Various scheduling techniques, including proportional fair scheduling, round-robin scheduling, and opportunistic

scheduling, are employed to balance the requirements of different users and improve overall network efficiency. 5G-NR introduces dynamic and semi-static scheduling for supporting different communication requirements and traffic patterns. With dynamic scheduling, the gNB allocates radio resources on-the-fly for each packet transmission in both the DL (downlink) and UL (uplink). However, the signaling exchange between the UE and the gNB to request or inform about the allocated resources introduces a non-negligible latency. This latency can potentially impact services that demand low latencies, especially in the UL, where two messages need to be exchanged between the UE and the gNB. In order to minimize this latency, 5G NR implements semi-static scheduling techniques known as semipersistent scheduling (SPS) for DL transmissions and configured grant (CG) for UL transmissions. Through SPS and CG, radio resources are pre-assigned periodically to the UE. As a result, when a packet is generated, it can be immediately transmitted using the pre-allocated resources. This approach eliminates the necessity of exchanging signaling messages to request or grant resources for each packet, leading to a reduction in transmission latency.

Duplexing schemes This term refers to the methods used to enable two-way communication between devices over the radio interface. These schemes rules how the UL and DL transmissions are organized, allowing devices to send and receive data simultaneously or in separate time slots. The duplexing schemes are crucial for ensuring efficient and reliable communication between the UE and the gNB in a 5G network. There are two duplexing schemes in 5G. In TDD (Time Division Duplexing) both the UL and DL transmissions share the same frequency band, but they are separated by different time slots within the same radio frame. This means that during a specific time interval, the device can either transmit data to the base station (UL) or receive data from the base station (DL). The allocation of time slots for UL and DL can be dynamically adjusted based on the traffic demand. TDD is often preferred in scenarios where UL and DL traffic can vary significantly, as it allows for more flexible use of the spectrum. In FDD (Frequency Division Duplexing) instead, separate frequency bands are allocated for UL and DL transmissions. Devices use one frequency band to transmit data to the base station and another frequency band to receive data from the base station. This simultaneous use of distinct frequency bands ensures that UL and DL transmissions do not interfere with each other. FDD is typically chosen in scenarios where there is a need for constant and symmetrical traffic between the UE and the BS, as it provides a predictable separation between the UL and DL channels.

Frame Structure The frame structure defines the organization of time and frequency resources within a transmission frame. In 5G the length of a radio frame is always 10 ms and the length of a subframe is always 1 ms so a frame always contains 10 subframes. The only parameter that can change is the number of slots within one subframe. This value is defined by the numerology chosen. The higher the numerology, the more slots are contained in the subframe. Frame structure includes parameters like the frame duration, slot duration, and subframe structure. These parameters determine the granularity of resource allocation and the time division for different types of data transmission, such as control information, user data, and synchronization signals.

Channel scenario Modelling propagation in a wireless channel is a complex yet important task, as it greatly impact the network performance. As part of 5G standardization, 3GPP introduced different channel models that are defined by the technical report TR 38.901 [22]. The TR 38.901 standardizes a set of channel models to simulate various real-world propagation environments, representing different use cases and deployment scenarios. Here are brief definitions of the 5G channel scenarios as defined by TR 38.901. Urban Macro (UMa) represents a densely populated urban area with tall buildings where the base station is mounted on a high tower, providing wide-area coverage. Urban Micro (UMi) scenario simulates a densely populated urban environment with smaller cells to enhance capacity in high-demand areas. UMi-Street Canyon represents a street canyon where small cells are deployed at street level. Rural Macro (RMa) models a rural environment with large macrocells and open spaces. Indoor Office (InH) deals with indoor office environments where 5G small cells are deployed within buildings.

The selection of the channel scenario and the configuration of parameters within a scenario impacts the network capacity and coverage and available spectrum resources.

3.2.4 Simulation tools for 5G networks

Network simulators are essential tools for studying and analyzing network behaviour in a controlled environment. The evolution of network simulators can be traced back to the early days of computer networking research. Initially, simple analytical models were used, but as networks grew in complexity, researchers turned to simulation tools to replicate real-world network scenarios and evaluate protocol performance.

Many options are available for simulating 5G networks. MATLAB provides the Vienna simulator for 5G networks, useful for research addressing PHY and MAC layers. OPNET Modeler is a commercial network simulator option that supports many network topologies, OMNeT++ is an open-source network simulator that supports 5G user plane simulation.

However, this thesis used ns-3 (network simulator–3), one of the most used network simulators in academic environments, with a comprehensive module for 5G networks [23].

ns-3

ns-3 is an open-source discrete-event network simulator widely used for academic and research purposes. It provides a platform for simulating and evaluating various network protocols, scenarios, and applications. Developed as a successor to ns-2, ns-3 offers several enhancements and features that make it a valuable tool for network researchers and developers. The ns-3 project aimed to create a modern and more flexible simulator that supported newer programming languages like C++ and Python. Over the years, ns-3 has gained popularity among network researchers due to its robustness, extensibility, and accurate modeling capabilities.

ns-3 was designed according to several key principles.

- Modularity: ns-3 is built on a modular architecture, allowing researchers to easily extend and customize the simulator for specific requirements. Modules encapsulate various network protocols, devices, and applications, promoting code reusability and maintainability.

- Realism: The simulator strives to emulate real-world network behaviour as accurately as possible. This includes modelling network latency, packet loss, link capacities, and other factors that affect network performance.

- Accuracy and Validation: ns-3 emphasizes accurate representation and validation of protocol implementations. Developers and researchers meticulously review and validate the simulator against known benchmarks and existing implementations to ensure its fidelity.

- Protocol Support: ns-3 supports a wide range of network protocols, including TCP/IP, UDP, ICMP, Routing protocols (e.g., OSPF, BGP), MAC protocols (e.g., IEEE 802.11, Ethernet), and more. This allows researchers to simulate and evaluate the behaviour of these protocols under different network conditions.

- Application Support: The simulator provides support for simulating various network applications, such as web browsing, video streaming, VoIP, and custom application development.

- Integration and Extensibility: ns-3 can be integrated with external tools and libraries, allowing researchers to incorporate additional functionality or custom modules into their simulations. It also provides an extensive set of APIs for easy integration and extension.

For the simulation of 5G networks with ns-3 two different modules have been considered, namely 5G-mmWave and 5G-LENA. 5G-mmWave [24] is a module for the simulation of non-standalone 5G cellular networks operating at mmWaves. 5G-LENA [23] is a fork of the former project providing in addition a 3GPP-compliant NR (New Radio) module working in the bands above and below 6 GHz, aligned with 3GPP NR Release-15.

The 5G-LENA module is the one used for the simulations carried out for this thesis. For this reason, the following section will focus on its description.

5G-LENA

This simulator is the evolution of LENA, a 4G LTE/EPC ns-3 pluggable module. There are many features that make it the best choice for the study carried out in this thesis.

5G-LENA is a versatile module that facilitates the modeling and simulation of scheduling algorithms, beamforming, power control, and interference management.

Furthermore, 5G-LENA allows for the effective representation of the entire network architecture of 5G systems, including core network elements, base stations, UE, and network slicing. It implements and simulates the 5G protocol stack, allowing the simulation of both the control plane (responsible for managing the setup, configuration, and control of network resources) and user plane (responsible for forwarding actual user data) protocols.

In addition to these capabilities, 5G-LENA provides a wide array of performance evaluation metrics and tools that effectively analyze and measure the performance of 5G networks. These metrics include throughput, latency, packet loss, and quality of service (QoS) parameters, making it a comprehensive tool for researchers and practitioners in the 5G domain.

The main downside of this module is that, being compliant with 3GPP Release 15, it does not support the Standalone (SA) architecture, which is the most suitable one for MTC application. However, the module is under active development and the SA architecture is expected to be supported in the future.

3.3 Methodology

The simulations have been implemented by using ns-3 for the network part and libIEC61850 for the emulations of IEDs. This thesis pursued a network emulation approach, integrating the simulation realised with ns-3 with real hosts running IEC 61850 applications.

This approach was adopted because it brings two main advantages. First, it avoids modelling IEC61850 in ns-3, by using an existing and widespread library, i.e. libiec61850. In addition, it guarantees the possibility in future work to replace the network simulated in ns-3 with a real 5G network without modifying the application. On the other hand, however, integrating real hosts in the simulation introduces latencies due to the scheduling of operating system processes as detailed in section 5.1.

In the following, the methodology is explained in detail.

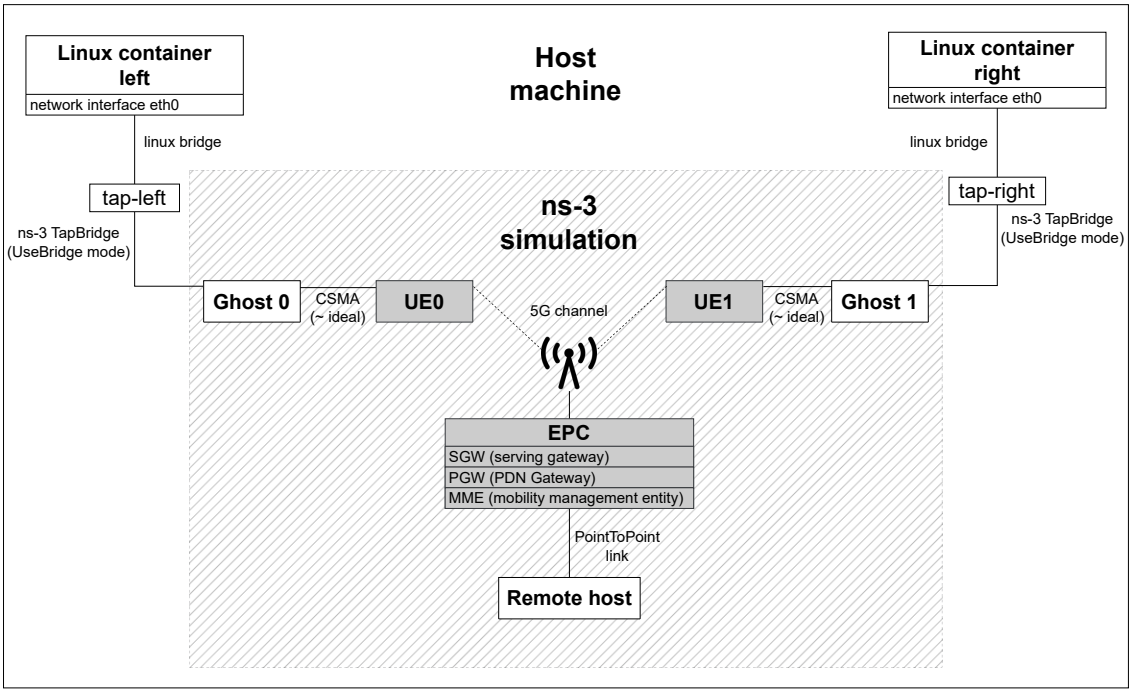


Figure 3.4: 5G simple network setting

3.3.1 Network simulation

The basic setup we started experimenting with is sketched in fig. 3.4. The 5G network topology implemented within the ns3 simulator, consists of 2 UEs connected to the same gNB, connected to the core network. The 5G network nodes correspond to the grey boxes in the figure. As it can be noticed the core network consists of the EPC (Evolved Packet Core). In fact, to the best of our knowledge, there does not exist an open source 5G network simulator implementing stand-alone 5G architecture. The core network is connected via a point-to-point link to a remote host. With some variations, this scheme is the base to build the other network topologies described in section 4.2. The hatched rectangle contains all the nodes within the ns-3 simulation while the external rectangle represent the physical machine used to carry out the simulations. To integrate IEC 61850 devices into the simulation, we used TapBridge [25], an ns-3 module that allows real hosts to appear as local hosts in the simulation. TapBridge connects the inputs and outputs of an ns-3 network device to the inputs and outputs of a Linux Tap net device, hence the name Tap Bridge. It is important to note that a real host in this case means a host virtualized via LXC (Linux Container) on the same machine running the ns-3 simulation. As can be observed from the network topology, each one of the two UE is connected via a CSMA channel to a "ghost node", whose net device is used to bridge with the tap device of the LXC host. The addition of the CSMA link is forced because in ns-3 not all net devices offer tap bridge functionality, and a literature survey has shown that using a dummy CSMA link is the most common solution to overcome this problem. Furthermore, this solution does not affect the performance significantly, as the bandwidth and link latency can be set arbitrarily high and low respectively.

The advantages of the emulation approach over a purely simulative alternative are mainly two. First of all, it avoids modelling the IEC61850 communication in ns-3, by using an existing and widespread library. The other advantage comes from the opportunity, in future work, to replace the simulated network in ns-3 with a real 5G network without changing the application. On the other hand, this approach also has disadvantages, most importantly the latency due to the operating system, which is further detailed in Chapter 5.

3.3.2 IEC 61850 devices emulation

The LXC hosts described in the previous section are used to make the simulation more realistic. Indeed, their purpose is to run IEC 61850 applications used to send and receive packets over the network. The applications chosen for the simulations are MMS and SV. The libIEC61850 APIs were used to create two pairs of applications: an MMS client/server and an SV publisher/subscriber. These were then installed on the LXCs and used to simulate IEC 61850 traffic on the 5G network. The major obstacle encountered during the implementation of this solution comes from the fact that the SV protocol, as explained in Sec. 3.1.2 is mapped directly to the Ethernet layer, making impossible packets routing outside of a LAN. Since ns-3 does not allow 5G LANs to be simulated, despite the fact that this concept was introduced by 3GPP for IoT applications [26], an alternative solution had to be used. The workaround considered is inspired by the R-SV protocol introduced in IEC 61850-90-5, which involves encapsulating SV packets by adding UDP/IP headers to send

them through the network. The mapping on the network stack of R-SV messages is shown in

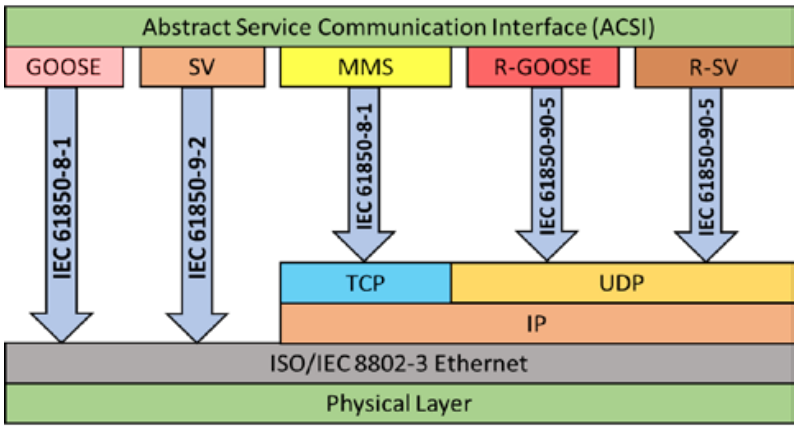


Figure 3.5: Mapping of IEC 61850 messages to network stack. Source: [12]

Fig. 3.5

Since the solution to the SV messages routing problem we mentioned above is not straightforward and libIEC61850 does not provide APIs for R-SV, we report here the details of the functioning of our ns-3 simulation during the transmission of SVs. The following steps are schematized also in Fig. 3.6.

1. The SV packet enters the simulations sent by the LXC host through its ghost node on broadcast on the CSMA LAN.

2. A callback is invoked at the reception of the packet at the CSMA net device of the sender UE. The callback purpose is first of all to serialize the packet. The serialized SV packet is then sent through the 5G channel to the receiver node exploiting a UDP socket. In this case with the term receiver node we are referring to the node on the side of the 5G network which, according to fig. 3.4, can be a UE or a remote host.

3. At the receiver another callback is called when the serialized UDP packet is received. Its purpose is to remove the UDP and IP header from the packet, deserialize it and send it through the CSMA channel to the other ghost node.

4. This allow the ghost node and the LXC host to finally receive the packet.

Although this solution solves the problem of routing SV packets, it introduces an overhead on the packet size to which the UDP and IP headers must be added. In particular, the original SV packet length is 119 bytes, while the transmitted packet is 198 bytes long. The 79 bytes overhead is due to the added UDP and IP headers and to the serialization of the packet.

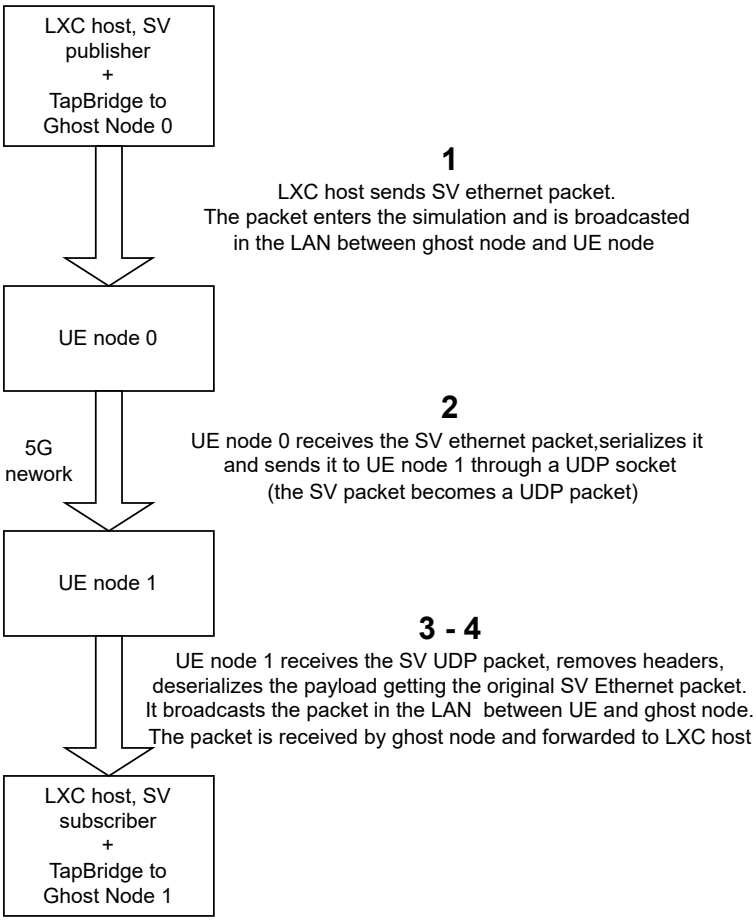


Figure 3.6: Flowchart of the SV packet transmission

4 Scenarios

In this chapter, we detail the scenarios that were chosen to be simulated for this thesis. Three network topologies and three traffic-generating applications have been defined. The combination of these applications and topologies allows to cover a wide range of practical scenarios in 5G-based IEC 61850 communications. The applications employed are presented in section 4.1, while details on the chosen topologies are given in the section 4.2.

4.1 Applications

The details about the 3 applications defined to test our topologies are reported in this section.

4.1.1 Ping

Ping is a network utility that employs the ICMP (Internet Control Message Protocol) to evaluate the accessibility and reachability of a specific host or network node over an IP network. It involves the transmission of a small data packet from the originating source to the target destination, which sends back a response packet to the source. The primary objective of this diagnostic procedure is to assess the existence of a viable communication path and to gauge the round-trip time it takes for the data packet to travel to the destination and back to the source. By measuring this round-trip time, commonly referred to as ping latency, the utility aids in determining the responsiveness and quality of the network connection, while also facilitating the identification of potential network issues or connectivity problems.

In this thesis, ping has been used as a smoke test to verify the correct functioning of the simulated network. For every topology simulated we used ping first to determine if the transmitter and the receiver are able to communicate. Then we used it to measure the latency of the simulated network. The procedure used involves first using the ns-3 `V4PingHelper` to create an IPv4

application to ping between the two hosts inside the simulation. Once we have established that this is working correctly, we move on to ping the two Linux containers connected to transmitter and receiver via TapBridge to check that also this link is working correctly. Although the ping application provided by ns-3 could be sufficient for this test, we decided to use the standard Linux ping because it is more reliable and it provides a more similar setting to the one target of this study.

4.1.2 MMS

This application is used to evaluate the communication between a client and a server running on two emulated hosts using MMS, one of the protocols defined in IEC 61850. The client and server applications have been implemented starting from the code of the examples provided by libIEC61850 [19].

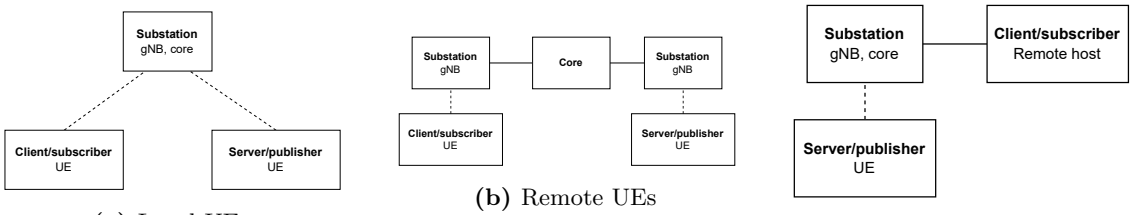
Server First of all, a new IedServer object is created according to an IEC model description. This object is responsible for managing the complete MMS protocol stack and the IEC 61850 data model. After invoking the starting function the server starts listening for client connections on its port 102, i.e. the default TCP port of MMS. For every new incoming client connection a dedicated thread is started to handle this connection. In the main loop the application periodically updates the MMS values. When the application is stopped all the client connections are closed and the memory is cleaned up.

Client The client application first of all creates a connection to the server. After having established the connection the client starts a loop in which it periodically sends MMS read requests to the server. The client then waits for the response and prints the value of the MMS variable and the value of the round trip time between the sending of the request and the reception of the reply. After having sent 100 requests the application prints the statistics about maximum, minimum, average and standard deviation of the round trip time. Then it closes the connection and cleans up the memory.

4.1.3 SV

This application target is to tests the SV publisher/subscriber communication. Also in this case the two applications, publisher and subscriber, have been implemented by exploiting libIEC61850 APIs.

Publisher The application first creates a SV publisher and then create 2 ASDU (Application Service Data Unit) objects. The application then starts the main loop in which, with a tunable period, the values of the ASDUs data points are updated and published on the network interface eth0. When the application is stopped the memory is cleaned up.



(a) Local UEs **(b)** Remote UEs **(c)** UE and host

Figure 4.1: Network topologies

Subscriber The subscriber application simply creates a subscriber listening to SV messages with APPID 4000h on network interface eth0. Each time it receives a message it prints the ASDUs values. When the application is stopped the memory is cleaned up.

4.2 Topologies

We defined 3 network topologies to implement with ns-3 and the 5G LENA module that resemble 3 different substations scenarios.

4.2.1 Local UEs

Client/subscriber and server/publisher are UEs connected to the same gNB in the same substation. This scenario, schematized in Fig. 4.1a, mainly refers to the case where the communicating IEDs are located in the same substation and exchange either SVs (IEC 61850 interface IF4) or MMS traffic (interfaces IF1/IF3/IF5/IF6/IF8/IF9). The topology can also cover the case of IEDs located in geographically close substations that are within the coverage radius of the same gNB, exchanging either SVs (interface IF2) or MMS traffic (interface IF11). Eq. 4.1 reports the components of the data plane latency (T_{e2e}) for this topology.

$$T_{e2e} = T_{RAN_{UL}} + 2T_{core} + T_{RAN_{DL}} \tag{4.1}$$

In this topology each packet goes through the core two times: first from the sending UE to the core (UL) and then from the core to the receiving UE (DL). For this reason T_{core} is considered two times in the computation of the total latency.

The only fixed latency is the one of the core network, T_{core} whose value is fixed to 200 μs in this thesis. This low latency is due to the fact that in this scenario the core network is considered to be located close to the gNB, often in the same substation, thus allowing a fast and reliable communication between the core network and the RAN. The other two components, i.e. $T_{RAN_{UL}}$ and $T_{RAN_{DL}}$, depend on the configuration of the RAN.

4.2.2 Remote UEs

Client/subscriber and server/publisher are UEs connected to different gNB in different substations. Fig. 4.1b shows this topology which is a possible deployment used when IEDs are located in different substations and exchange either SVs (interface IF2) or MMS traffic (interface IF11).

$$T_{e2e} = T_{RAN_{UL}} + 2T_{core} + T_{RAN_{DL}} \tag{4.2}$$

The only fixed end-to-end latency component, as shown in Eq. 4.2, is the core latency T_{core}, which in these cases take values of 1/2/5 ms. This latency is higher than the one of Local UEs and UE and host topologies because in this scenario the core network is deployed in a different location, potentially far from the substations in which the gNBs and UEs are located. Increasing T_{core} values aims at simulating increasing distances between the gNBs and the core. For this reason we expect to obtain higher latency values in this scenario. The other two components, i.e. $T_{RAN_{UL}}$ and $T_{RAN_{DL}}$, as in the previous topology depends on the configuration of the RAN.

4.2.3 UE and host

The server/publisher is a UE while the client/subscriber is a remote host located in the same substation, meaning that only one gNB is deployed. Fig. 4.1c schematize this topology which refers to cases when communicating IEDs are located in the same substation and one of the IEDs is directly interfaced to a local 5G core via a point-to-point link, exchanging either SVs (interface IF4) or MMS traffic (interfaces IF1/IF3/IF5/IF6/IF8/IF9) with the other IED.

$$T_{e2e} = T_{RAN_{UL}} + T_{core} + T_{host} \tag{4.3}$$

In this scenario, as shown in Eq. 4.3, the end-to-end latency is composed by $T_{RAN_{UL}}$, i.e. the RAN UL latency depending on the channel configuration, the subsequent core latency T_{core} of 200 μs, which is low for the same reasons explained in Sec. 4.2.1 and by the remote host latency T_{host}, of 1 ms. This value has been chosen to simulate a remote host close to the core network.

4.3 Parameters

In Sec. 3.2.3 we provided an overview of the principal 5G configurations and parameters that affect the performance of the system with particular attention to the RAN. This section provides more details about which of these parameters can be configured and which values they can assume in ns-3 5G-LENA [27] in order to optimize the performance in the simulated scenarios.

Frequency 5G-LENA provides the flexibility to work from 400 MHz to 100 GHz. This allows to test the system in both FR1 (sub 6GHz) and FR2 (above 6GHz) i.e. mmWaves.

Numerology Numerology, often referred to with the greek letter μ, defines the configuration of subcarrier spacing and the duration of radio slots used in the 5G wireless communication

system. Subcarrier Spacing (SCS) refers to the frequency separation between adjacent subcarriers used for transmitting data. By adjusting numerology parameters, 5G can adapt to different channel conditions, user requirements, and deployment scenarios, making it a versatile technology that can accommodate a wide range of use cases, including enhanced mobile broadband, massive MTC, and URLLC. Numerology defines the time duration of a radio slot, which is the basic time unit for scheduling data transmissions and resource allocation. Different numerology values influence the time granularity and efficiency of 5G communication. The 5G standard supports multiple numerology configurations to optimize the network's performance for various scenarios and applications. The numerology values defined in 3GPP Release-15 and available in the 5G-LENA simulator are shown in Table 4.1 with their respective SCS and Cyclic prefix type.

Numerology	Subcarrier spacing in kHz	Cyclic prefix
0	15	Normal
1	30	Normal
2	60	Normal, Extended
3	120	Normal
4	240	Normal

Table 4.1: Numerologies defined in 3GPP NR Release-15

Duplexing scheme and frame structure 5G-LENA supports both TDD and FDD modes. For the TDD model the module allows different slot types: "DL", "UL" and "F" slots. The DL slots are used for downlink transmission, the UL slots are used for uplink transmission and the F (Flexible) slots are used for both downlink and uplink transmission. Also LTE slot type can be emulated through the use of "S" slot type. The pattern of slots of each type can be configured by the user. There are no limitation in the implementation of the pattern size and structure. However, a too large gap between two UL or DL symbol can cause a timeout in the RRC (Radio Resource Control), HARQ or CQI (Channel Quality Indicator) timers compromising the performances. The FDD duplexing is implemented using two paired bandwidth parts. One bandwidth part is exclusively allocated for transmitting DL data and control, while the other is designated for UL data and control transmission. To achieve this, users configure each bandwidth part with either a DL-only or UL-only pattern and establish a connection between the two parts to ensure proper routing of control messages. For instance, the HARQ feedback for a DL transmission is sent through the UL-only bandwidth part, even though it pertains to the DL-only bandwidth part. This configuration is essential to correctly direct the message from one bandwidth part to the other. It is important to note that this FDD model only allows pairing between bandwidth parts configured with the same numerology.

MCS The 5G-LENA module offers two methods for link adaptation in 5G simulations. With fixed MCS configuration the user can set a predetermined value for the MCS independently for both DL and UL transmissions. The second method exploits AMC Models: the module supports two AMC models for link adaptation: Error Model-Based AMC in which the MCS index is

dynamically selected to achieve a target Transport Block Error Rate (BLER) and Shannon-Based AMC that selects the highest MCS that provides a spectral efficiency lower than the one achieved by the Shannon rate. The user can configure the desired AMC model using the "AmcModel" attribute. For the Error model-based AMC, the "ErrorModelType" attribute specifies the type of error model used, which must match the one configured for error modeling. On the other hand, for the Shannon-based AMC, the "Ber" value sets the desired bit error rate for MCS selection. In the 'NR' module, link adaptation occurs at the UE side. The UE selects an MCS index (quantized by 5 bits) and communicates it to the gNB using a CQI index (quantized by 4 bits). It's worth noting that in the simulator, gNB's DL data transmissions start with MCS0 in the case of adaptive MCS. This initial MCS is used until there is CQI feedback from the UE.

HARQ The NR module supports two HARQ methods: Chase Combining (HARQ-CC) and Incremental Redundancy (HARQ-IR). In HARQ-CC, every retransmission contains the same information and coding bits. Therefore, the effective code rate (ECR) after the q-th retransmission remains the same as after the first transmission. In HARQ-IR instead, every retransmission contains different coded bits than the previous one. The different retransmissions typically use a different set of coding bits. Therefore, both SINR and ECR need to be recomputed after each retransmission.

Error model The 5G-LENA module includes a PHY abstraction model for error modeling that is compliant with the latest NR specifications, including LDPC coding, MCS up to 256-QAM using MCS Table1 and MCS Table2, and NR transport block segmentation. In the NR case, the HARQ method and MCS table are configured according to the selected error model, e.g. ns3::NrEesmCcT1 uses HARQ-CC and MCS Table 1.

Scheduler 5G-LENA implements natively only the dynamic scheduling both for UL and DL. For the down-link OFDMA scheduling is exploited in a round robin (RR), proportional fair (PF) and max rate (MR) manner. In the UL, the scheduling is done by the TDMA schedulers with the same variants as OFDM schedulers (RR, PF and MR). A study shows that introducing a semi-static scheduling technique for UL, called Configured Grant (CG) [28], leads to a significant decrease in latency. For this reason, in future works it can be interesting to integrate the CG in our simulation in order to further increase the performances.

Channel scenario For the propagation environment simulation, 5G-LENA provides all the scenarios defined by TR 38.901 [22]. Unfortunately, as some previous analysis point out [29] [30] these scenarios are developed for generic applications and may not represent well the propagation environment in electrical substations, which is very peculiar. For this reason we decided to implement our own scenario based on the measurements reported in [29] and [30] which we called "HVSubstation", aiming to simulate the environment conditions of a High Voltage Substation. The path loss model we exploited is the Close-In one, in which the intercept is determined by

the path loss at a reference distance of 1 m in the 3D space. Eq. 4.4 shows the formula used to compute the path loss for this scenario.

$$PL(f_0, d) = 10 \log_{10} \left(\frac{4\pi f_0}{c} \right)^2 + 10n \log_{10}(d) + X_\sigma \tag{4.4}$$

Where n is the path loss exponent, f_0 is the carrier frequency, d is the distance between transmitter and receiver in the 3D space and X_σ is the shadow fading which follows a Gaussian distribution with zero mean and σ exponent. The values of n and σ used are different according to the carrier frequency of the radio channel and have been defined according to the values obtained by [29] for FR1 (<6 GHz) and [30] for FR2 (>6 GHz). Table 4.2 reports the numeric values which are different for FR1 and FR2 and depending on LoS (Line of Sight) or NLoS (Non-Line of Sight) conditions.

	FR1 (3.5 GHz) [29]		FR2(28 GHz) [30]	
	LoS	NLoS	LoS	NLoS
n	1.62	2.43	2.46	3.36
σ	2.76	2.76	4.12	2.95

Table 4.2: Path loss and shadowing exponent for different scenarios

5 Performance evaluation

5.1 Ping

This section reports the results obtained for the first application, i.e. the ping application. The main goal of this section is to evaluate the latency introduced by the 5G channel simulated by ns-3 and the one caused by the Tap Bridge between the ghost nodes in the simulation and the real hosts. The results obtained in this section are used as a baseline for the other applications.

5.1.1 Ping with ideal CSMA channel

The first tests were carried out on a ns-3 network scenario with 2 UEs, connected by an ideal CSMA channel (i.e. a channel configured with no errors, latency close to zero, high data rate). These 2 UEs are called ”ghost nodes” because their role is just to connect via the ns-3 TapBridge module to linux containers, allowing to integrate real hosts in the ns-3 simulation. This scenario is similar to the one showed in Fig. 3.4 with a CSMA channel instead of a 5G network between the 2 UEs. In fact we exploited this simplification to study the effectiveness of TapBridge emulation for our requirements.

After implementing the simulated network, the scenario was tested first by pinging one UE from the other inside the simulation and then pinging between the two LXCs as explained in Sec. 4.1.1 to test the end to end connectivity. In both cases 100 ping packets were sent with an interval of 1 second between each other. The traffic generated by the simulation was analyzed with Wireshark along with the traffic sniffed on the two tap interfaces ”tap-left” and ”tap-right” shown in Fig. 3.4. In the following we present the results obtained.

- We experienced a big decrease in latency outside the simulation when using the optimized build of ns-3. In fact, ns-3 provides the possibility to build its code in debug and optimized

mode. While debug mode is more suitable for producing logs and troubleshooting application, optimized build is for certain scenarios way faster. In our experiments the ping RTT was 10 ms in the debug setting and 0.5 ms in the optimized setting.

- The first packet injected in the simulation always takes more time because of the ARP protocol overhead.
- With the optimized version of the simulator the ping RTT operating at the LXCs is around 0.5 ms. This latency is probably irreducible and is introduced by latencies in the operating system scheduling. In fact in this scenario the latency in the simulation is negligible because of the ideal channel.

5.1.2 Ping with 5G network (Local UEs)

After testing the effectiveness of the TapBridge connection, we moved to the 5G network emulation scenario. The first test was carried out with the local UEs topology, i.e. the communication between 2 UEs connected to the same gNB.

5G network parameter tuning

In order to obtain the lowest latency possible, we performed the tuning of the parameters for the 5G network. The values of the parameters used for the simulation are reported in Table 5.1.

Parameter	Value
Carrier frequency	3.5 GHz (FR1)
Bandwidth	200 MHz
TX power	6 dBm
Channel scenario	HVSubstation LoS
HARQ	HARQ-CC
MCS	AMC, Table 1
Duplexing scheme	TDD
Numerology	4
Subframe pattern	DDUUDDUUDDUUDDUU
Scheduling	Dynamic
2D distance UE-gNB	20 m
UE height	1.5 m
gNB height	5 m

Table 5.1: 5G-LENA channel parameters for the simulation

Following the findings reported in [7] and [6] we focused especially on the numerology and the subframe pattern. The numerology is the parameter that defines the duration of a slot in the 5G frame. The subframe pattern is the sequence of slots in the frame. In particular, we used the numerology 4 and the subframe pattern DDUUDDUUDDUUDDUU. In fact, with this numerology and subframe pattern, the distance between subsequent UL and DL slots is always small, guaranteeing a small interval between the reception of a packet and its transmission.

Although these values have been initially tested with the local UEs topology and ping application, they have been used also for all the other scenarios because they proved to be always the best ones for achieving URLLC.

Results

The results obtained with the ping application inside the simulation show a deterministic RTT of 2.9 ms. As expected this value is higher than the one obtained with the ideal channel because of the latency introduced by the 5G channel. When we try to ping between the LXCs, we notice a big increase in the RTT which is around 6 ms with significant fluctuations between 10 and 3 ms. This increment is much higher in this scenario with respect to the CSMA channel. The cause could be the unpredictable latency introduced by the operating system that conflicts with channel scheduling and TDD subframe pattern. Motivated by this observation, in the rest of the thesis we only report results related to the latency measured inside the simulation, not the end-to-end latency between the LXCs. This allows to focus the analysis on the latency introduced by 5G network. In future works, a real-time operating system or other setups ensuring deterministic latency should be used in order to optimize the end-to-end transfer time that would be seen in a real-world IEC 61850 application.

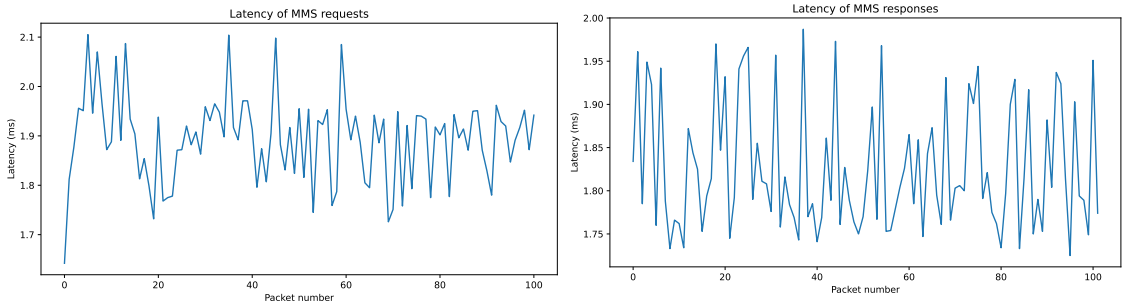
5.2 MMS

The tests with ping allowed to evaluate the latency introduced by the 5G channel and by the Tap Bridge link with the real hosts. In this section we present the results obtained with the second application, i.e. MMS client/server communication.

5.2.1 MMS with local UEs

The evaluation of this application was restricted to topology local UEs, in which the 2 UEs are connected to the same gNB. The parameters of the channel are the same as in Table 5.1. Since the MMS is a symmetric protocol we decided to compute separately latencies of requests and responses. In Fig. 5.1 are plotted the latencies of 100 MMS requests and responses. Fig. 5.2 compares the two distributions. The average latency of the requests is 1.89 ms while the average latency of the responses is 1.83 ms. This results show that the latency of the responses is slightly lower than the one of the requests but this difference is negligible. The maximum latency observed is 2.1 ms, which is well above the requirements for MMS traffic.

Fig. 5.3 shows the round-trip latencies measured at the client tap interface for each request + response. These values include both the latency of the 5G network and that introduced by Tap Bridge and operating system scheduling. By comparing this latency, on average 5 ms, with the one obtained with the ping experiment, we can observe that the latter predicted quite well the former.



(a) MMS responses

Figure 5.1: Plot of the latency measured for MMS requests and responses

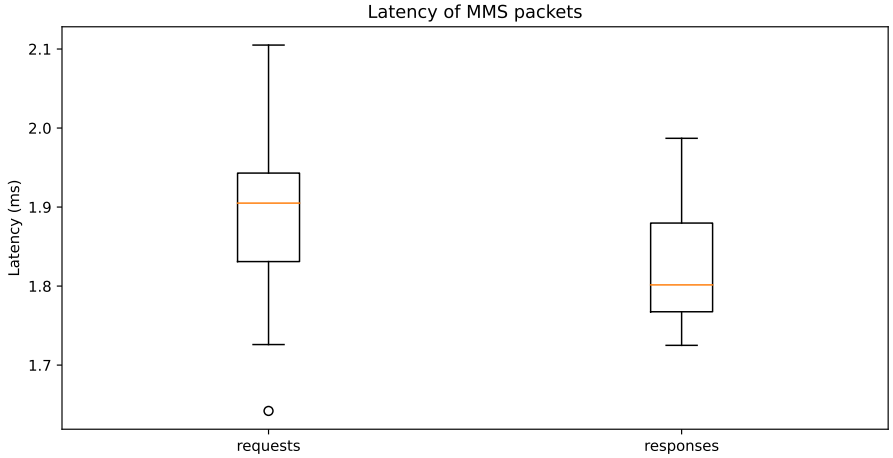


Figure 5.2: Comparison of the latency measured for MMS requests and responses

5.3 SV

The last application tested is the SV publisher/subscriber. The results obtained with this application are the most interesting because the SV is the most time sensitive application and the one with the strictest latency requirements within IEC 61850.

5.3.1 SV with Local UEs, Remote UEs and UE and host

We carried out performance tests on SV with each one of the topologies we defined. For every topology we used the channel configuration reported in Table 5.1. The tests consisted in sending SV messages with a fixed period for 1 second from the publisher to the subscriber and measuring the end-to-end latency of each SV message within the simulation.

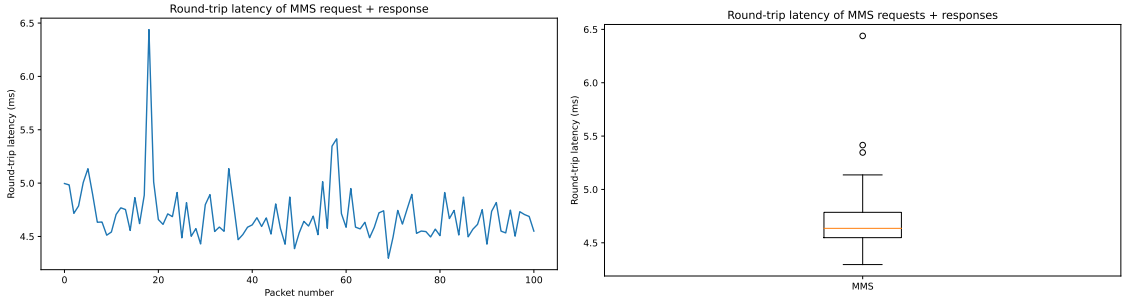


Figure 5.3: Round-trip latency measured for MMS requests + responses at client

Impact of SV transmission rate

Typical values considered for the SV publish frequency in protection applications are 80 samples per power cycle, which corresponds to 4000 samples per second (or 250 μs transmission rate) in 50 Hz power systems. To provide a comprehensive analysis, we tested the impact of different SV transmission rates on the end-to-end latency. Fig. 5.4 shows a comparison of the latency obtained with SV rate of 250 μs, 1, 2, 5, 10 and 20 ms.

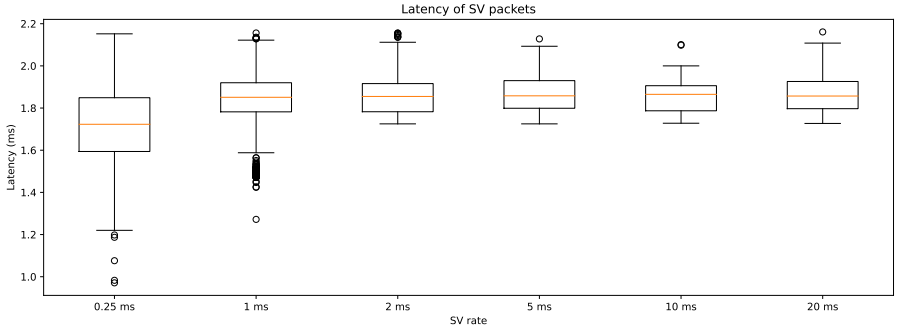
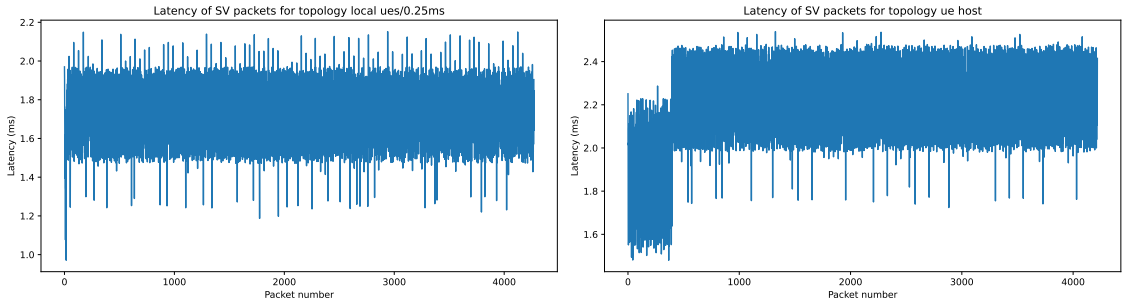


Figure 5.4: Comparison of the latency for different SV rate with local UEs topology

As can be seen, the latency is not highly affected by the SV rate. This is due to the fact that the SV is a periodic application and the 5G channel is configured with a subframe pattern that guarantees a small interval between the reception of a packet and its transmission. The only observable difference between the rates consists in a higher variance of the latency for the highest rate of 250 μs. This is due to the fact that the higher the rate, the higher the probability that some packets are sent through the channel exactly when they are created by the publisher, thus decreasing the minimum possible latency and resulting in a higher variability.

Impact of topology

The results obtained with local UEs and UE and host topologies and SV rate of 250 μs are reported in Fig. 5.5a and Fig. 5.5b respectively.



(a) Local UEs **(b)** UE and host

Figure 5.5: Latencies of SV with local UEs and UE and host topologies

Fig. 5.6 compares the latency of these 2 topologies. The average latency obtained is 1.72 ms for local UEs and 2.19 ms for UE and host topology. Furthermore, all the packets are delivered within 2.2 ms for local UEs and 2.6 ms for UE and host, respecting the 3 ms bound imposed by IEC 61850.

Fig. 5.5b highlights the fact that the first packets take less time to be delivered. The increase of the latency after about 500 packets is due to AMC that changes the MCS to adapt to the channel conditions. We noticed that this effect can be observed when a base station transmits packets only in a direction (UL or DL) and it tends to disappear with the increasing of the core latency.

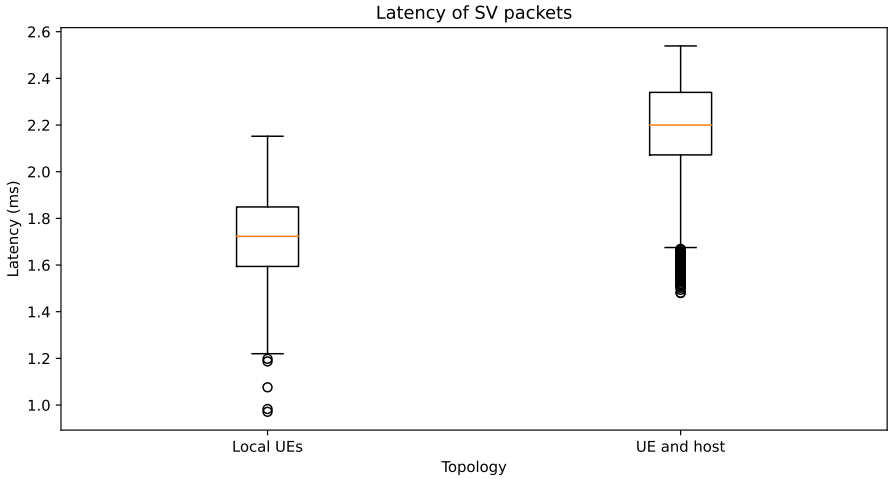
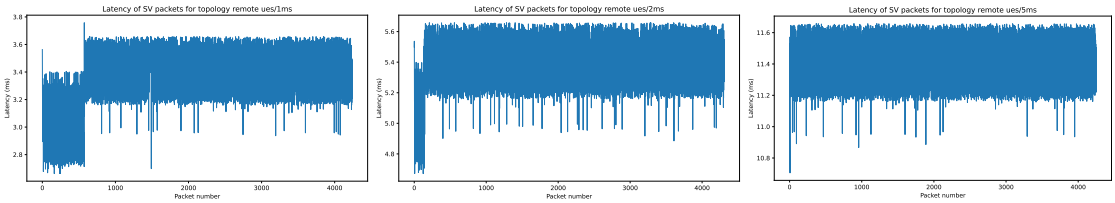


Figure 5.6: Comparison of the latency of SV with local UEs and UE and host topologies

Impact of core latency

For the remote UEs topology, different scenarios have been tested by changing the core latency of the 5G channel. This variation represents different distances between the 2 gNB of the scenario and the core network. In fact the gNB could be deployed in different substations potentially very

far one from the other. The results obtained are reported in Fig. 5.7. Also in this case we notice the same trend of the latency as in the UE and host topology: the first packets are delivered with lower latency and when the MCS is changed the latency increases. However, this phenomena tends to disappear with the increasing of the core latency.



(a) 1 ms **(b)** 2 ms **(c)** 5 ms

Figure 5.7: Latency measured for remote UEs topology with different core latencies

The average latency obtained is 3.4 ms with core latency of 1 ms, 5.4 ms for core latency of 2 ms and 11.4 ms with core latency of 5 ms. It is worth noting that the core latency contributes twice to the end-to-end latency (once in UL and once in DL), hence adding a constant core latency of 1 ms results in an average latency increase of 2 ms. In this scenario, as can be noticed in Fig. 5.8, all the 3 variants don't allow to deliver packet within the time limit of 3 ms. This allows to conclude, as expected, that core latency is a critical component of end-to-end latency in 5G applications and should be kept low (e.g. to less than 1 ms) if the most critical IEC 61850 applications are to be targeted.

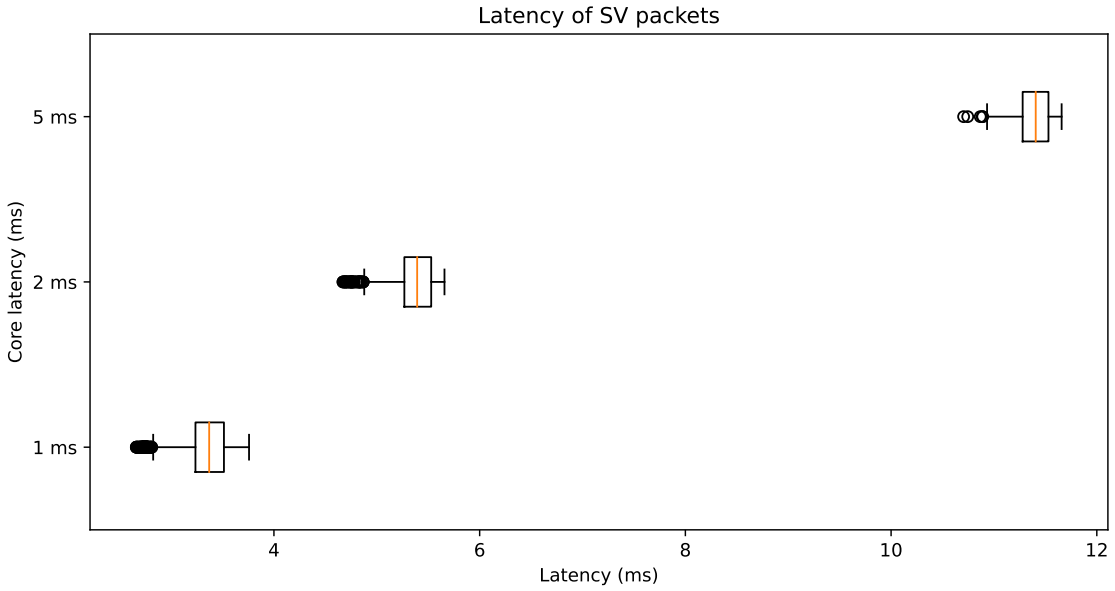


Figure 5.8: Comparison of the e2e latency measured in remote UEs topology for SV with different core latencies

Table 5.2 summarizes the statistics obtained with the 3 topologies, showing the minimum, maximum, average and standard deviation of the latency measured for each topology.

Scenario	Latency			
	Min	Max	Avg	Stdev
Local UEs	0.97 ms	2.15 ms	1.72 ms	0.16 ms
UE and host	1.48 ms	2.54 ms	2.19 ms	0.19 ms
Remote UEs, core latency 1 ms	2.66 ms	3.76 ms	3.35 ms	0.20 ms
Remote UEs, core latency 2 ms	4.67 ms	5.66 ms	5.39 ms	0.17 ms
Remote UEs, core latency 5 ms	10.71 ms	11.66 ms	11.40 ms	0.15 ms

Table 5.2: Latency statistics for SV with the 3 topologies

5.3.2 Impact of the propagation environment

After testing all the topologies and applications, further experiments have been carried out to evaluate the impact of the propagation environment and of the carrier frequency on the latency. We focused on SV and local UEs topology because it is the topology that best satisfies the latency requirements of IEC 61850. The following conditions have been evaluated.

FR1 NLoS As a first experiment we tested the same frequency of the previous experiments (FR1, 3.5 GHz) but switching from HVSubstation LoS to NLoS channel scenario. The average latency obtained is 1.87 ms, which is very similar to the one obtained with the LoS scenario. Also in this case all the packets are delivered correctly without packet loss thus allowing a reliable communication. This result shows that the absence of Line of Sight at FR1 frequencies doesn't affect the performances of the channel.

FR2 LoS In this case we used a frequency of 28 GHz (FR2) with the HVSubstation LoS channel scenario. The average latency obtained is 1.87 ms, which is again the same obtained in the reference scenario. Also in this case all the packets are delivered correctly without packet loss allowing a reliable communication. This result shows that FR2 frequencies doesn't affect the performances of the channel when the gNB and UEs are in Line of Sight.

FR2 NLoS This experiment is similar to the previous one but in this case we used the HVSubstation NLoS channel scenario. In this case, keeping fixed all the parameters shown in Table 5.1, no packet can arrive to the destination, due to the too high path loss caused by the Non Line of Sight condition at such high frequency. In this case the SINR measured by the simulation is negative, meaning that the communication is not feasible at all.

FR2 NLoS with lower distance between UEs and gNB Once acknowledged the results of the previous experiments, we decided to test the same frequency FR2 in NLoS conditions with a lower horizontal distance between the UEs and the gNB. In fact, being the distance directly

proportional to the path loss (Eq. 4.4), we expected that at a certain point, by decreasing the distance, we would have being able to achieve communication. The turning point was found at 5 m, where the subscriber was able to receive all the SVs sent by the publisher. However in this case the average latency measured is of 309.0 ms, which is way higher than the one obtained with the same distance and NLoS condition at FR1, as shown in Fig. 5.9. This large increase of the latency shows that, at comparable distances, using mmWave frequencies results in worse channel conditions that shows as increased latency (likely due to the effect of HARQ or AMC in low SNR conditions and channel variations due to shadowing). Table 5.3 summarizes the latency statistics obtained with the 3 different propagation environments and frequencies.

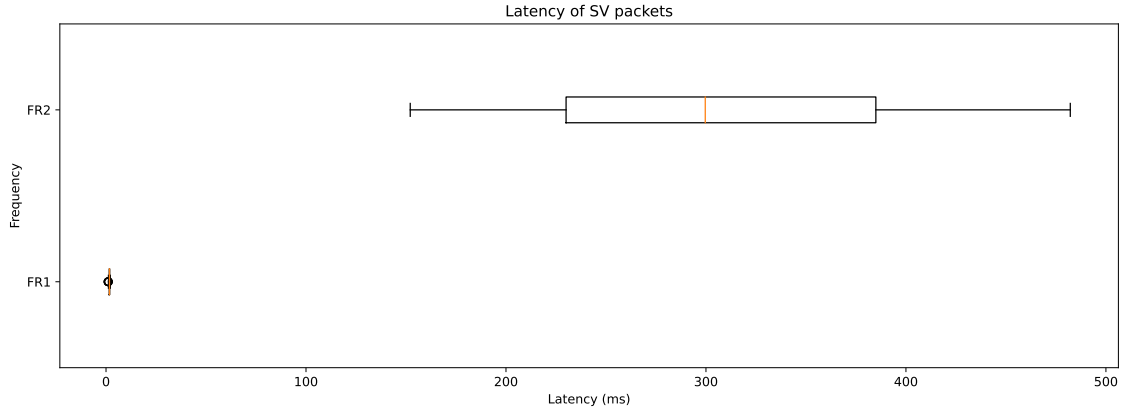


Figure 5.9: Comparison of the latency measured in local UEs topology for SV using FR1 and FR2

Scenario	Latency			
	Min	Max	Avg	Stdev
FR1 NLoS	0.93 ms	2.21 ms	1.73 ms	0.18 ms
FR2 LoS	0.99 ms	2.25 ms	1.76 ms	0.13 ms
FR2 NLoS	152.12 ms	482.18 ms	309.04 ms	89.43 ms

Table 5.3: Latency statistics for SV with local UEs topology and different propagation environments and frequencies

5.4 Summary

The results obtained with the ping application allowed to evaluate the latency introduced by the 5G channel and by the TapBridge link with the real hosts. The results obtained with the MMS application showed that 5G introduces a low and bounded latency, allowing to satisfy the latency requirements for MMS traffic. The results obtained with the SV application showed that the latency is still within the IEC 61850 requirements when the two communicating UEs are connected to the same gNB and the core latency is kept low (0.2 ms). The same occurs when one

communicating device is implemented in a remote host connected to a local core. However, when communicating IEDs are connected to different gNBs and core latencies are higher (1 ms or more), the end-to-end latency exceeds the requirement of 3 ms. This points at the need to minimize core latency when critical IEC 61850 applications are considered over wide areas.

Furthermore, the results showed that the propagation environment and the carrier frequency have a significant impact on the latency of the channel. In particular, Non Line of Sight condition at high frequency (28 GHz) highly affects the performance of the channel. This result is in line with the literature which highlights how the high frequency bands (mmWaves) are more sensitive to the propagation environment and struggle to provide good results in presence of obstacles between the transmitter and receiver.

As reported above, besides frequency and channel scenario, the other parameters that according to our experiments influenced the most the latency of the channel is the numerology and subframe pattern. This confirms the findings of previous works [7] [6] which show how higher numerologies and subframe patterns in which the distance between subsequent UL and DL slot is always small guarantees lower latency.

6 Cybersecurity review

In this chapter we provide first of all a summary of the cybersecurity-related background relevant for this thesis. In Sec. 6.1 we offer an overview of IEC 61850 security measures while in Sec. 6.2 we report the details on 5G security focusing on industrial IoT scenarios. In Sec. 6.3 we first define a threat model, then list the countermeasures provided by 5G and IEC 61850, we proceed by showing the vulnerabilities introduced by the IEC 61850 communication on a 5G channel and finally present some countermeasures to be considered in future research in order to mitigate these vulnerabilities.

6.1 IEC 61850 security

Although some independent approaches for cybersecurity in IEC 61850 have been studied in the literature, as reported in Sec. 2.3, these solutions are nowadays not applied in real-word scenarios. Therefore, we decided to focus on the official solutions offered by the International Electrotechnical Commission. In the following sections, we summarize the most important ones.

6.1.1 Summary of IEC 62351

IEC 62351 standard has been published to provide security measures for different power system communication protocols including IEC 61850. The standard is divided into many parts. The most relevant for the scope of this thesis are listed below. What follows is a summary of the information found in the IEC 62351 standard, integrated with [12] and [13] that provide some review of the standard.

IEC 62351-1 Introduction which covers the background of security for power system operations and provides overview information on the IEC 62351 series. It also briefly describes concepts such

as risk assessments, key management and security processes, among other things.

IEC 62351-2 The second part of the IEC 62351 standard is a glossary, explaining terms such as Access Control, Data Security, etc.

IEC 62351-3 Specifies how to achieve message-level authentication for protocols that make use of TCP/IP as a message transport layer when cyber-security is required. This part of IEC 62351 specifies how to secure TCP/IP-based protocols through constraints on the specification of the messages, procedures, and algorithms of TLS (Transport Layer Security) so that they are applicable to the specific features of IEC applications, such as TLS version, session resumption, renegotiation, MAC (message authentication code), CA (Certification authorities), signing, key exchange. IEC 62351-3 protects against different threats:

- Eavesdropping through TLS encryption.
- Man-in-the-middle security risk through message authentication.
- Spoofing through Security Certificates (Node Authentication).
- Replay, again through TLS encryption.

There are however some specific threats that are not covered, such as denial of service. This type of security attack needs to be guarded against through implementation-specific measures.

IEC 62351-4 IEC 62351-4 provides application-layer security measures for MMS messages and derivatives. The combination of IEC 62351-3 and IEC 62351-4 provides end-to-end security through the application layer, including authentication, confidentiality, data integrity and non-repudiation.

This part defines 2 security profiles:

- A-Profile Security. Security for the A-Profile (the application level) is achieved through certificate-based peer entity authentication during association setup.
- T-Profile Security. For TCP T-Profiles, the standard recommends the use of TLS.

The main issue of IEC 62351-4 security for the A-Profile is that it does not cover message integrity or confidentiality. It only covers the initial authentication, but the authentication does not extend to the subsequent messages within the session. Therefore, unless transport-level security (i.e., TLS for the T-Profile) is also used, the security provided by A-Profile security mechanism is minimal.

IEC 62351-6 This part of the standard covers three IEC 61850 protocols (GOOSE, GSE, and SV) that are multicast datagrams and not routable, designed to run on a substation LAN or other non-routed network. In this environment, the messages need to be transmitted within 3 milliseconds, therefore most encryption techniques or other security measures which affect latency are not acceptable. In fact, many cybersecurity techniques exploit complex algorithms that require long

elaboration times, heavily impacting packets transmission time. For this reason, authentication through a digital signature is the only security measure included. Some of the key elements of the security measures for GOOSE and SV are:

- Authentication is the primary security measure.
- Encryption is not included because it causes too much delay to packets transmission and is not considered that important. (In the future, some hardware encryption might be added.)
- Key renegotiation is not supported "in-band" because it could disrupt the highly critical, high-speed flow of information.

The standard suggests the use of RSA signatures for providing authenticity and integrity of extended packets, which makes it unsuitable for applications where a 3 ms response time is required (GOOSE), as RSA signatures are relatively expensive in terms of computation power required. An HMAC (hash-based message authentication code) on the other hand can be implemented in hardware, requiring only around 10µs for generating an HMAC for a typical IP packet. For backward compatibility, a reserved field is now used for length, so that an extension can be added to the end of the GOOSE/SV message. This extension contains the authentication value (Digital Signature – HMAC). Non-secure clients would simply ignore this extension. This adds about 20 bytes. The IEC 61850 SCL is extended in order to support the exchange of certificates.

IEC 62351-7 Power systems operations are increasingly reliant on information infrastructures, including communication networks, IEDs, and proprietary communication protocols. Therefore, management of the information infrastructure is crucial to provide the necessary high levels of security and reliability in power system operations. IEC 62351-7 has therefore developed abstract Network and System Management (NSM) data objects for the power system operational environment These NSM data objects reflect what information is needed to manage the information infrastructure as reliably as the power system infrastructure is managed. The ISO CMIP and the IETF SNMP standards for Network Management can provide some of this management. In SNMP, Management Information Base (MIB) data is used to monitor the health of networks and systems, but each vendor shall develop their own set of MIBs for their equipment. For power system operations, SNMP MIBs are only available for common networking devices, such as routers. No standard MIBs have been developed for IEDs, so vendors use ad hoc or proprietary methods for monitoring some types of equipment health. This standard thus provides MIB-like data objects (termed NSM data objects) for the power industry.

IEC 62351-8 The scope of this part of IEC 62351 is to facilitate RBAC (Role-Based Access Control) for power system management. RBAC assigns human users, automated systems, and software applications (collectively called "subjects" in this document) to specified "roles", and restricts their access to only those resources, which the security policies identify as necessary for their roles.

IEC 62351-9 This part of IEC 62351 specifies cryptographic key management, namely how to generate, distribute, revoke, and handle public-key certificates and cryptographic keys to protect digital data and its communication. Included in the scope is the handling of asymmetric keys (e.g. private keys and public-key certificates) and symmetric keys for groups (GDOI). These keys are used in different algorithms specified in other parts of IEC 62351 standards such as 3, 4 and 6.

IEC 62351-10 This part of IEC 62351, which is a Technical Report, targets the description of security architecture guidelines for power systems based on essential security controls, i.e. on security-related components and functions and their interaction. Furthermore, the relation and mapping of these security controls to the general system architecture of power systems are provided as a guideline to support system integrators to securely deploy power generation, transmission, and distribution systems applying available standards.

6.1.2 IEC 61850-90-5

The security model for R-GOOSE and R-SV messages, i.e. the GOOSE and SV variant designed for being routed is not provided by IEC 62351 but by IEC 61850-90-5, which is the part of the standard that also introduces these types of messages. Considering the security threats and functions given in IEC 62351-1, the IEC 61850-90-5 states that for R-GOOSE and R-SV, exactly as with the non-routed variant, the information authenticity and integrity is a mandatory requirement, while confidentiality is left as optional. The IEC 61850-90-5 recommends the use of MAC algorithms to generate digital signatures for APDU authentication and integrity.

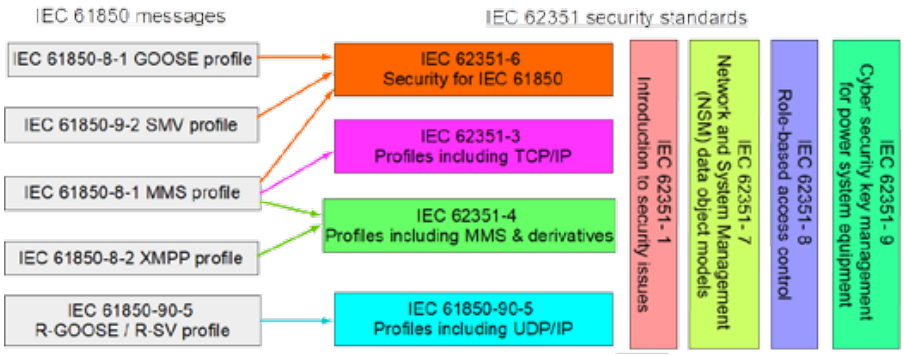


Figure 6.1: Mapping between security mechanisms and IEC 61850 messages

To summarize, as represented in Fig. 6.1, IEC 62351-6 specifies the security mechanisms to secure the IEC 61850-8-1 GOOSE and IEC 61850-9-2 SV messages, whereas IEC 62351-4 and 3 provide the security mechanisms required to secure the IEC 61850-8-1 MMS messages and IEC 61850-8-2 XMPP messages. Cybersecurity guidelines for R-SV and R-GOOSE are not provided by IEC 62351 but by IEC 61850-90-5.

6.2 Summary of 5G security architecture

The fifth generation of mobile networks, 5G introduces significant advancements in terms of speed, capacity, and latency, enabling a wide range of applications, including MTC. MTC applications involve communication between machines or devices, often without human intervention. These applications include IoT devices, smart grids, industrial automation, connected cars, and more. Security considerations for MTC applications in 5G are crucial due to the potential impact of any compromise in these interconnected systems [15].

The 5G Alliance for Connected Industries and Automation (5G-ACIA) was founded in 2018 for tackling, discussing, and evaluating relevant aspects of 5G for the industrial domain. The primary focus of telecommunication operators has never been industrial vertical architectures and, on the other hand, the main priority of OT industry vendors is not telecommunications. As a consequence, there existed a lack in the representation of OT needs in 3GPP, both generally and in terms of security, which is presently being addressed via a collaboration between 3GPP and 5G-ACIA. The requirements for OT security from 5G are now being discussed, looking at various use cases and using a risk-based approach to security. In particular, 3GPP released TS 33.501 [31], a technical specification addressing security architecture and procedures for 5G Systems which contains three annexes on security requirements and solutions for vertical industry-related features. One of these annexes specifically deals with NPN which, according to a 5G-ACIA white paper [32] are fundamental for industrial use cases. It is important to note that the main focus of 5G-ACIA is on industrial automation applications and power grid applications are not represented in the alliance. However, since NPNs are fundamental in power grids as well, most considerations in TS 33.501 apply to this domain as well.

NPNs are designed for usage by private service providers such as industries. The advantages of NPNs with respect to networks accessible to the general public consist of high QoS, high security standards, isolation from other networks and accountability. NPNs, as stated in [32], can be deployed in many ways, leveraging both virtual and physical elements. The standard deployment options are two: SNPN (Standalone Non-Public Network) and PNI-NPN (Public Network Integrated Non-Public Network). The NPN deployment scenarios are shown in Fig. 6.2.

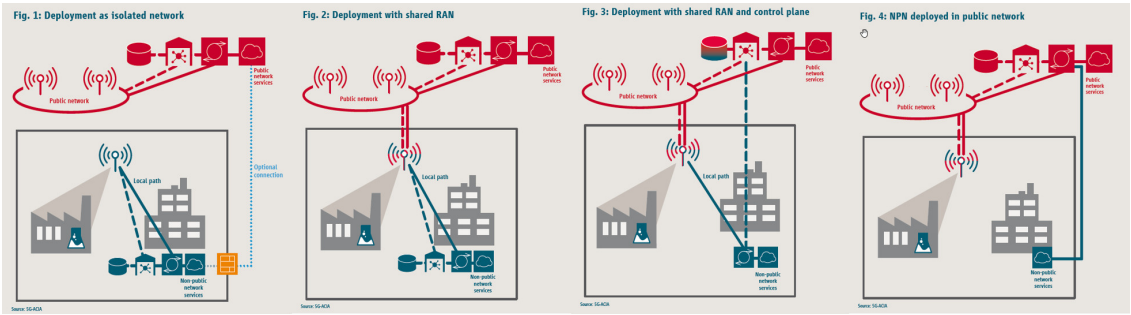


Figure 6.2: NPN different deployment scenarios

A SNPN is assumed to be run by an SNPN operator who does not rely on network functionalities

provided by the public network. A firewall is the only optional communication link between the NPN and the public network. On the other hand, A public network is required to deploy a PNI-NPN. Network slices, Closed Access Group (CAG) cells or a mix of the two techniques is exploited to implement it. A PNI-NPN can share with the public network only the RAN, both RAN and control plane or be deployed in public network.

6.2.1 5G security for industrial application

Here are the key aspects of 5G security with a focus on MTC applications and NPN.

Authentication and Access Control

AKA (Authentication and Key Agreement) is a fundamental security protocol that ensures the confidentiality, integrity, and authenticity of communication between a user device (UE) and the 5G network. It plays a vital role in establishing a secure connection, preventing unauthorized access, and protecting sensitive data from interception or tampering. AKA provides mutual authentication between the UE and the network, generates temporary session keys for encryption, and ensures the freshness, confidentiality, and integrity of exchanged information. The authentication process involves the UE sending a request to the network, receiving a challenge, responding with a calculated response, and undergoing verification. The standardization of AKA by 3GPP enables global interoperability. Additionally, AKA supports continuous authentication and periodically revalidating the user's access. For MTC applications, this includes secure provisioning and registration of IoT devices, as well as secure authentication protocols to prevent unauthorized access and protect against spoofing or impersonation. The 5G Authentication and Key Agreement (AKA) protocol enhances the 4G/LTE/EPS by assuring the home network that the UE has authenticated and avoiding forged roaming costs.

EAP (Extensible Authentication Protocol) is the other important authentication framework in 5G. In EAP there are three key entities: the server is responsible for concluding the authentication process with the peer. The peer is the endpoint that provides responses to the authenticator. The authenticator is the entity that initiates the EAP authentication procedure. Translating this framework to 5G architecture, the AUSF located in the home operator network serves as the equivalent of the EAP server. The UE takes on the role of the peer, offering responses during the authentication process. The Security Anchor Function (SEAF), which is a component within the AMF of the serving network, assumes the responsibility of a pass-through authenticator.

When AKA isn't the primary choice for authentication, the 5G architecture relies on the EAP framework. In release 16, one of the primary differences between PNI-NPN and SNPN deployments lies in the requirement for AKA methods. In a PNI-NPN, as in a public network deployment, AKA and EAP methods must be supported in both the UE and the network. However, in a SNPN, supporting 5G AKA or EAP-AKA is not mandatory [17].

Encryption

5G incorporates strong encryption algorithms to protect data transmission between devices and the network. Encryption ensures that sensitive information remains confidential and cannot be intercepted or tampered with during transit. In MTC applications, encryption is vital to safeguard data transmitted between IoT devices and the backend systems. Some of the key encryption algorithms used in 5G include the Advanced Encryption Standard (AES), a widely used symmetric encryption algorithm exploited in 5G for encrypting user data. On the other hand, SNOW 3G, a stream cipher and Elliptic Curve Cryptography (ECC) are used for securing control plane data. In comparison with LTE, where the long-term credentials was still sent in the clear through the radio channel during initial registration of the UE with the serving network, in 5G it is never exposed in clear over the air [17]. According to Release 15, it's a requirement that the privacy feature involves the USIM (Universal Subscriber Identity Module). When the Home Network Public Key isn't present within the USIM, no privacy protection can be applied although EAP TLS, an EAP variant, does not imply the need of a USIM, since no long-term key needs to be shared in advance.

Network Slicing and Isolation

5G introduces the concept of network slicing, which allows the partitioning of a single physical network infrastructure into multiple virtual networks. This isolation provides an added layer of security for MTC applications, as it ensures that different applications or services are logically separated and protected from potential threats within the network.Network slicing is one of the key enabler of PNI-NPN.

Overall, securing MTC applications in 5G networks requires a holistic approach that combines secure authentication, encryption, network isolation, and proactive threat detection. By implementing robust security measures, organizations can protect against unauthorized access, data breaches, and disruptions to critical infrastructure, thereby enabling the safe and reliable deployment of MTC applications in the 5G era.

6.3 Sketch of security architecture

6.3.1 Threat model

We used the threat modelling approach exploited in [18] to create a threat model. The STRIDE mnemonic (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) was then used to highlight the primary potential risks of the system.

The threat model identified for IEC 61850 traffic on a 5G network is summarised in Table 6.1.

The threats are then mapped to the security requirements of the system, such as authentication, integrity, confidentiality, etc. Then, security requirements are mapped to the countermeasures provided by 5G and IEC 62351. This mapping is summarised in Table 6.2. The colours in the table represent the effectiveness of the countermeasure. Green means that the countermeasure is considered strong, yellow means that the countermeasure is considered weak and red means that

STRIDE	Threat
Spoofing	Spoofing of IEDs or MU
Tampering	Change measurement of IEDs
Repudiation	Lack of logging, can't detect cause of incident
Information disclosure	Get access to measurements from IED or MU
Denial of Service	Jamming, buffer overflow
Elevation of privilege	Gain administrator access to IEDs

Table 6.1: Threat model based on STRIDE

Threat	Security requirement	5G countermeasure	IEC 62351 countermeasure
Spoofing	Authentication	Mutual authentication with USIM or certificates and message authentication	Message authentication is compulsory for SV and MMS
Tampering	Integrity	Message integrity through AKA and/or EAP	Message integrity protection is always guaranteed
Repudiation	Accountability	SNPN access, network slicing	Role-Based Access Control
Information disclosure	Confidentiality	AKA/EAP enables encrypted communication	Encryption not necessary for SV, enabled for MMS
Denial of Service	Availability	SNPN and network slicing for security and reliability	Network system management
Elevation of privilege	Accountability		Role-Based Access Control

Table 6.2: Threat countermeasures provided by 5G and IEC 62351

the countermeasure is not provided. The prevailing colour is green, meaning that the majority of the countermeasures are considered strong. In the majority of the threats, separate countermeasures are, provided by both 5G and IEC 62351. The only red cell in the table is the corresponds to accountability for 5G as no countermeasure of this type is provided by the standard. However, the threat associated to this requirement, i.e. elevation of privilege, is a threat related to the specific application so 5G is not expected to provide a countermeasure for this threat.

We will now analyze the countermeasures provided by 5G and IEC 62351 in more detail. As regards authentication, both 5G and IEC 62351 provide strong countermeasures. As highlighted in the previous sections, 5G provides mutual authentication through USIM or certificates, while IEC 62351 provides compulsory message authentication both for SV and MMS. Also integrity of the messages is guaranteed by both 5G and IEC 62351.

Accountability is achieved first by 5G with SNMP and network slicing, which guarantees a limited network access and then by the Role-Based Access control provided by IEC 62351-8.

Confidentiality is guaranteed by 5G through AKA and/or EAP, which enables encrypted communication. On the contrary, as explained above, IEC 62351 provides encryption for MMS messages but not for SV messages. However, this is not a problem because confidentiality is not considered necessary for SV messages. For these reasons the cell in the table is represented as

yellow. It is important to mention that also in SNPN encryption can be disabled when not needed, in order to increase the performance and meet the requirements of the most low-latency requiring messages.

Availability is guaranteed by 5G through network slicing and SNPN and by IEC 62351 through network system management (IEC 62351-7). It is important to notice that radio jamming attacks to compromise channel availability are still possible in 5G, so the cell is coloured in yellow. Finally, IEC 62351 provides an effective Role-Based Access Control to prevent elevation of privilege.

6.3.2 List of possible vulnerabilities

According to the analysis presented in the previous sections the vulnerabilities of a 5G network used for IEC 61850 communication consist in denial of service through jamming and metadata disclosure.

Denial of Service attacks involve disrupting the normal functioning of a system, making it inaccessible or unusable for legitimate users. In the context of 5G networks used for IEC 61850 communication, jamming attacks specifically target the radio frequency (RF) spectrum used for wireless communication between devices and base stations. By emitting interference signals in the same frequency bands, attackers can disrupt the communication links between IEC 61850 devices, leading to communication failures and potentially causing critical infrastructure operational disruptions, potential safety hazards, and financial losses.

Metadata in the context of 5G networks refers to information about the communication itself rather than the actual content. Attackers can intercept network traffic to obtain metadata associated with IEC 61850 communication. This metadata may include details such as the source and destination addresses, communication session duration, packet timing, and patterns of communication between devices. While metadata may not contain the actual data payload being transmitted, it can still reveal crucial information about the network's structure, the devices connected, and communication patterns. This information can be valuable for attackers in planning further, more targeted attacks on critical infrastructure systems, potentially leading to data exfiltration, device manipulation, or other malicious activities.

There exist some mitigations that could solve the issues highlighted above. These mitigations could be the subject of future research.

Jamming Protection is a complex challenge for wireless networks but there are some possible workarounds that can be considered. Frequency hopping techniques can be used to dynamically change the operating frequencies to avoid prolonged disruptions from jamming attacks. Directional antennas and beamforming technologies can be leveraged to focus the communication signal and reduce the impact of interference from jamming sources. Intrusion detection systems (IDS) can be deployed to detect and respond to jamming attempts in real-time, enabling swift countermeasures. A good Jamming Protection system needs to combine all these techniques and perhaps other ones to solve this challenging problem.

Metadata protection can be achieved by padding traffic by adding additional data to communications, making it challenging for attackers to discern actual communication patterns and extract

meaningful metadata. This technique can help obfuscate the true nature of communication and increase the difficulty of metadata analysis.

However, both these countermeasures, although theoretically feasible to implement, are not provided by 5G specifications. Therefore, they require further research and development.

7 Conclusions

The application of 5G to IEC 61850-based communications has been explored as one step towards improving the power system infrastructure and facilitating the energy transition. This study provided a comprehensive evaluation of the usage of 5G in power grids communications, considering both performance and security aspects. Using advanced simulation tools, we were able to create realistic models of power substation network scenarios, simulate network traffic and analyze network behavior under different conditions. We studied the security implications of 5G networks in power grid environments, highlighting potential vulnerabilities and, when available, possible countermeasures. Our outcomes highlight the potential of 5G for power grids applications while emphasizing the importance of robust security measures for safeguarding critical infrastructure. The following sections reports the results obtained and the envisioned future work.

7.1 Summary of main findings

Notably, our analysis of MMS and SV IEC 61850 message types showed that in 5G the contribution of the RAN to the end-to-end latency is typically less than 2 ms in the simulations considered. Consequently, when the core latency is limited (e.g. in topologies with local UEs or remote hosts), the 3 ms threshold is respected. On the other hand, when the core latency is 1 ms or more (e.g. in topologies with remote UEs), the threshold is not met.

Furthermore, our research highlighted the complex relation between latency, propagation environment, and carrier frequency. It's clear that high-frequency bands, such as mmWaves, are sensitive to factors like propagation conditions and obstacles, prompting the need for thoughtful engineering to ensure reliable communication.

The other parameters related to the RAN that according to our findings influenced the most the latency of the channel is the numerology and frame structure. In our tests the employment of a higher numerology and a subframe pattern in which the distance between subsequent UL and

DL slots is always small guarantees lower latency.

According to the threat model presented in the previous chapter the only vulnerabilities of a well deployed 5G network used for IEC 61850 communication consist in denial of service through jamming and metadata disclosure. However these threats are present in almost all wireless communication protocols and are due to the nature of the wireless communications. What's more, these flaws can be solved by applying changes to 5G protocol. In the evolving landscapes of telecommunications and power systems, this study adds to the growing body of knowledge shaping the future of critical infrastructure. As power grid systems continue to evolve alongside technological progress, our hope is that these insights will encourage further research and innovation, ensuring the resilience, sustainability, and security of the systems driving our modern world.

7.2 Envisioned future work

The findings and insights generated from this study lay the foundation for several potential directions of future research and development, which could further enhance the understanding and practical implementation of this thesis. The following outlines potential directions for future work.

To further validate the findings of this research, conducting simulations with more realistic network traffic loads, in particular with more UEs connected to the RAN, is fundamental. This extension will provide insights into the scalability of the 5G-enabled communication infrastructure under higher demands and help identify potential bottlenecks.

Future research is aimed at tackling the persistent challenge of latency induced by the integration of real hosts by performing the tests with a real-time operating system. This entails refining the synchronization between the simulation and actual devices, eliminating the latency that currently affects responsiveness. Minimizing this latency will allow to create an end-to-end testing framework that mirrors real-world conditions with unparalleled fidelity.

Given the critical nature of power grid communication systems, a deeper investigation into cybersecurity measures is compulsory. Specifically, the evaluation through simulation of the overhead caused by the use of Transport Layer Security (TLS) and 5G radio channel encryption will show how much these security measures impact on the performances of low latency traffic, especially SV. This research could delve into varying encryption algorithms, key exchange methods, and authentication mechanisms to identify the most suitable configurations for power grid applications.

Experimental research is a crucial contribution to the field of wireless networks for mission-critical communication in power grids. Conducting experiments in real-world settings allows researchers to evaluate the performance of the network under real-world conditions and validate the results obtained through theoretical and simulative research. For this reason one of the next step of this work will be to carry out experiment with real hardware components instead of software simulations for the network part.

As our cybersecurity investigation highlighted, the integration of 5G in power grids introduces new security risks connected to DoS attacks through radio channel jamming and metadata disclosure. Currently, the 5G specification doesn't address this problems. Therefore, it is essential to

develop new security solutions to protect the network from cyber-attacks.

This research area aims also to use data-driven approaches, such as Machine Learning (ML), to improve network performance and security. One possible way to exploit ML is by developing algorithms that can automatically tune the network configuration based on real-time assessments of the network conditions and external factors. This approach enables networks to adapt to changing conditions and optimize their performance without human intervention. Additionally, ML can be used to develop intrusion detection systems that can identify and mitigate cyber threats in mission-critical networks. By analyzing network traffic and behavior patterns, these systems can detect anomalies and alert network administrators of potential security breaches.

References

[1] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17–27, 2017.

[2] J. E. Sullivan and D. Kamensky, "How cyber-attacks in ukraine show the vulnerability of the us power grid," *The Electricity Journal*, vol. 30, no. 3, pp. 30–35, 2017.

[3] TechCrunch. "Researchers uncover russia-linked malware that could immobilize electric grids." (2023), [Online]. Available: `https://techcrunch.com/2023/05/25/mandiant-russia-malware-immobilize-electric-grids/`. (accessed: 08.07.2023).

[4] P. P. Parikh, T. S. Sidhu, and A. Shami, "A comprehensive investigation of wireless lan for iec 61850–based smart distribution substation applications," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1466–1476, 2012.

[5] A. Sen and S. Bakka, "A study of wireless communication for substation automation," in *2021 5th International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, 2021, pp. 606–612.

[6] R. Ford, M. Zhang, M. Mezzavilla, S. Dutta, S. Rangan, and M. Zorzi, "Achieving ultra-low latency in 5g millimeter wave cellular networks," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 196–203, 2017.

[7] 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, 2021.

[8] X. Jiang, M. Luvisotto, Z. Pang, and C. Fischione, "Latency performance of 5g new radio for critical industrial control systems," in *2019 24th IEEE International conference on emerging technologies and factory automation (ETFA)*, IEEE, 2019, pp. 1135–1142.

[9] P. Raussi, H. Kokkoniemi-Tarkkanen, and K. Ahola, "Methodology to decrease packet loss in iec 61850 substation communication over wireless 5g communication," *CIGRE Science and Engineering*, vol. 26, CSE–026, 2022.

[10] C. M. Adrah, M. K. Katoulaei, T. Amare, and D. Palma, "A real-time cyber-physical testbed to assess protection system traffic over 5g networks," in *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, IEEE, 2022, pp. 71–75.

[11] N. Kumari, *Feasibility study for substation communication using parallel redundant wireless technology*, 2018.

[12] S. S. Hussain, T. S. Ustun, and A. Kalam, "A review of iec 62351 security mechanisms for iec 61850 message exchanges," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5643–5654, 2019.

[13] R. Schlegel, S. Obermeier, and J. Schneider, "A security evaluation of iec 62351," *Journal of Information Security and Applications*, vol. 34, pp. 197–204, 2017.

[14] H. C. Tan, V. Mohanraj, B. Chen, D. Mashima, S. K. S. Nan, and A. Yang, "An iec 61850 mms traffic parser for customizable and efficient intrusion detection," in *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, IEEE, 2021, pp. 194–200.

[15] X. Zhang, A. Kunz, and S. Schröder, "Overview of 5g security in 3gpp," in *2017 IEEE conference on standards for communications and networking (CSCN)*, IEEE, 2017, pp. 181–186.

[16] S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, "5g security challenges and solutions: A review by osi layers," *IEEE Access*, vol. 9, pp. 116 294–116 314, 2021.

[17] A. Jerichow, B. Covell, D. Chandramouli, A. Rezaki, A. Lansisalmi, and J. Merkel, "3gpp non-public network security," *Journal of ICT Standardization*, pp. 57–76, 2020.

[18] R. Borgaonkar, I. Anne Tøndel, M. Zenebe Degefa, and M. Gilje Jaatun, "Improving smart grid security through 5g enabled iot and edge computing," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 18, e6466, 2021.

[19] MZ Automation GmbH. "Libiec61850: Open source library for iec 61850." (), [Online]. Available: `https://libiec61850.com/`. (accessed: 07.07.2023).

[20] 3GPP. "5g system overview." (2022), [Online]. Available: `https://www.3gpp.org/technologies/5g-system-overview`. (accessed: 07.07.2023).

[21] T. A. N. do Amaral, R. V. Rosa, D. F. C. Moura, and C. E. Rothenberg, "An in-kernel solution based on xdp for 5g upf: Design, prototype and performance evaluation," in *2021 17th International Conference on Network and Service Management (CNSM)*, IEEE, 2021, pp. 146–152.

[22] 3GPP. "Study on channel model for frequencies from 0.5 to 100 ghz (3gpp tr 38.901 version 15.0.0 release 15)." (2018), [Online]. Available: `https://www.etsi.org/deliver/etsi_tr/138900_138999/138901/15.00.00_60/tr_138901v150000p.pdf`. (accessed: 07.07.2023).

[23] N. Patriciello, S. Lagen, B. Bojovic, and L. Giupponi, "An e2e simulator for 5g nr networks," *Simulation Modelling Practice and Theory*, vol. 96, p. 101 933, 2019.

[24] M. Mezzavilla, S. Dutta, M. Zhang, M. R. Akdeniz, and S. Rangan, "5g mmwave module for the ns-3 network simulator," in *Proceedings of the 18th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2015, pp. 283–290.

[25] ns-3. "Tap bridge model." (), [Online]. Available: `https://www.nsnam.org/docs/release/3.9/doxygen/group___tap_bridge_model.html`. (accessed: 07.07.2023).

[26] 3GPP. "5g for industry 4.0." (2020), [Online]. Available: `https://www.3gpp.org/technologies/tsn-v-lan`. (accessed: 07.07.2023).

[27] OpenSim CTTC/CERCA. "Nr module manual." (2023), [Online]. Available: `https://cttc-lena.gitlab.io/nr/nrmodule.pdf`. (accessed: 07.07.2023).

[28] A. Larrañaga Zumeta, M. C. Lucas-Estañ, S. Lagén, Z. Ali, I. Martinez, and J. Gozalvez, "An open-source implementation and validation of 5g nr configured grant for urllc in ns-3 5g lena: A scheduling case study in industry 4.0 scenarios," *Available at SSRN 4201881*,

[29] R. M. Sandoval, A.-J. Garcia-Sanchez, J.-M. Molina-Garcia-Pardo, F. Garcia-Sanchez, and J. Garcia-Haro, "Radio-channel characterization of smart grid substations in the 2.4-ghz ism band," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1294–1307, 2016.

[30] Z. Fu, Y. Zhang, X. Zhao, *et al.*, "An ann-based channel modeling in 5g millimeter wave for a high-voltage substation," *IET Communications*, vol. 15, no. 19, pp. 2425–2438, 2021.

[31] 3GPP. "3gpp ts 33.501: Security architecture and procedures for 5g system." (2020), [Online]. Available: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf. (accessed: 07.07.2023).

[32] 5G-ACIA. "5g non-public networks for industrial scenarios." (2021), [Online]. Available: https://5g-acia.org/wp-content/uploads/5G-ACIA_5G_Non-Public_Networks_for_Industrial_Scenarios_09-2021.pdf. (accessed: 07.07.2023).

Acknowledgments

I express my gratitude to my supervisor, Prof. Stefano Vitturi, for his support and guidance throughout my thesis journey. I am thankful for the opportunities you provided me to learn and grow as a researcher.

I am truly thankful to my co-supervisor, Michele Luvisotto, for his invaluable expertise, encouragement and mentorship. Your contributions have shaped this thesis and broadened my perspective. Thank you very much for making my internship at Hitachi Energy possible. This experience enriched me both professionally and personally

To my parents, Luigi and Veronica and my sister, Elena, I am forever grateful for your unconditional love, support and belief in my abilities. Your encouragement and support motivated my academic pursuits, and I dedicate this work to you.

I want to extend my heartfelt appreciation to my girlfriend, Alessandra, for her unwavering support, understanding, and patience during this challenging journey. Your love and encouragement have been my constant motivation, and I am lucky to have you by my side.

To my dear friends, I am thankful for their friendship, laughter, and moral support. Your presence has given me strength over the years. The countless shared experiences made this journey more enjoyable.

Thank you to all those who played a role in this journey; your support and encouragement made this path unique.