Analysis of Security in Railway Communication Networks based on 5G and WiFi

António Manuel Angeja Filipe

Thesis to obtain the Master of Science Degree in

Computer Science and Engineering

Supervisors: Prof. Luís Manuel De Jesus Sousa Correia
Prof. Ricardo Chaves

Examination Committee

Chairperson: Prof. Pedro Tiago Gonçalves Monteiro
Members of the Committee: Prof. Luís Manuel De Jesus Sousa Correia
Prof. Fernando Manuel Valente Ramos
Eng. Fernando Santana

May 2024

I declare that this document is an original work of my own authorship and that it fulfils all the requirements of the Code of Conduct and Good Practices of the Universidade de Lisboa.

Acknowledgments

I would like to thank my family who always supported me and pushed me to achieve this milestone in my life. A special thanks to my parents for helping me anytime they could.

I would like to thank my friends as well that never allowed me to give up and encouraged me to finish. For those who were closer to me during this process, thank you especially for the patience throughout those months.

I would also like to thank professors Luis and Ricardo for all the support throughout this difficult process, it could not have been easy.

Abstract

This thesis investigates the security implications of integrating 5G and WiFi technologies into modern railway communication networks. The research employs a multidimensional analytical approach, including a comprehensive 'Tree of Threats' model, to perform a security analysis of the network servicing the train's services and respective components which allow it to function. This study strives to identify key vulnerabilities and formulate targeted mitigation strategies. The analysis reveals that while 5G and WiFi technologies significantly enhance network efficiency and user experience, they simultaneously introduce an array of new security risks demanding robust solutions. The investigation identifies specific network nodes requiring better security measures and proposes various effective mitigation techniques. It also analyses the security of each service used by the train and applies the same method as for the nodes. This research provides a roadmap for stakeholders in the railway industry. The study concludes with a call for ongoing vigilance and adaptive strategies to safeguard against evolving threats in railway communication systems.

Keywords

Network Security, Railway Communication, Vulnerability Assessment, Threat Mitigation, 5G, WiFi.

Resumo

Esta tese investiga as implicações de segurança da integração das tecnologias 5G e WiFi nas redes de comunicação ferroviária modernas. O estudo utiliza uma abordagem analítica multidimensional, incluindo um modelo abrangente de 'Árvore de Ameaças', para realizar uma análise de segurança da rede que presta serviços ao comboio e os respetivos componentes que permitem o seu funcionamento. Este estudo procura identificar vulnerabilidades chave e formular estratégias de mitigação específicas. A análise revela que, embora as tecnologias 5G e WiFi melhorem significativamente a eficiência da rede e a experiência do utilizador, elas introduzem, no entanto, uma série de novos riscos de segurança que exigem soluções robustas. A investigação identifica nós específicos da rede que exigem melhores medidas de segurança e propõe várias técnicas de mitigação eficazes. Analisa também a segurança de cada serviço utilizado pelo comboio e aplica o mesmo método que para os nós. Esta pesquisa fornece um guia para os intervenientes na indústria ferroviária. O estudo conclui com um apelo à vigilância contínua e estratégias adaptativas para proteger contra ameaças em evolução nos sistemas de comunicação ferroviária.

Palavras Chave

Segurança de Rede, Comunicações ferroviárias, Avaliação de vulnerabilidades, Mitigação de ameaças, 5G, WiFi.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

2FA	Two-Factor Authentication
3GPP	Third Generation Partnership Project
AKA	Authentication and Key Agreement
AP	Access Point
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATS	Automatic Train Supervision
BS	Base Station
BSS	Base Station Subsystem
CC	Control Centre
CCTV	Closed-Circuit Television
CS	Circuit Switched
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DPI	deep packet inspection
DREAD	Damage, Reproducibility, Exploitability, Affected Users, Discoverability
EDGE	Enhanced Data Rates for GSM Evolution
ERA	European Union Agency for railways
ERTMS	European Rail Traffic Management System
ETSI	European Telecommunications Standards Institute
FRMCS	Future Railway Mobile Communication System
GMSC	Gateway Mobile Switching Centre
GS	Gateway Server
GSM	Global System for Mobile Communication
GSM-R	Global System for Mobile Communications - Railway
HMAC	Message Authentication Code
IDS	Intrusion Detection System

IMSI International Mobile Subscriber Identity
IP Internet Protocol
LTE Long term evolution
LTE-R Long term evolution Railways
MAC Media Access Control
MSC Mobile Switching Centre
MT Mobile Terminal
NMS Network Management System
NR New Radio
NSA Non Stand-Alone
NSS Network Switching Subsystem
OSS Operating Support System
PGW Packet Data Network Gateway
PS Packet Switched
PTC Positive Train Control
QKD Quantum Key Distribution
QoS Quality of Service
RAA Risk Assessment Average
RS Ruggedized Switch
SA Stand-alone
SGW Serving Gateway
SIM Subscriber Identity Module
SLG Service Layer Gateway
SMS Short Message Service
SSL Secure Socket Layer
STRIDE Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TCP Trasnmission Control Protocol
TLS Transport Layer Security
TLS/SSL Transport Layer Security / Secure Sockets Layer
TOTP Time-based One-Time Passwords
UDP User Datagram Protocol
UIC International Union of Railways
UMTS Universal Mobile Telecommunications System
UMTS/HSPA Universal Mobile Telecommunications System/High Speed Packet Access

VoIP Voice over Internet Protocol

VMC Video Management Centre

VPN Virtual Private Network

1

Introduction

This chapter serves as an introduction to the role of railways in a country's infrastructure and the need to improve current conditions. It starts with a brief overview of railway passenger's data. The narrative then moves on to describe the problem statement where a central dilemma arises: How can 5G technology be incorporated globally while railway communications remain reliant on 2G? This issue motivates the thesis, particularly as trains become increasingly crucial for efficient and sustainable travel.

The goals and requirements section highlights the project's aim towards enhancing the security of the railway infrastructure communication systems. The chapter concludes by providing an overview of the report's structure.

Contents

1.1 Overview

Railways are a crucial infrastructure in any country. They are an effective way of transportation used by people and cargo. Even though the use of trains has decreased these past years due to the Covid-19 pandemic, prior to that, the use of this transport had been increasing. Now, numbers are slowly climbing again since the pandemic is starting to come to an end.

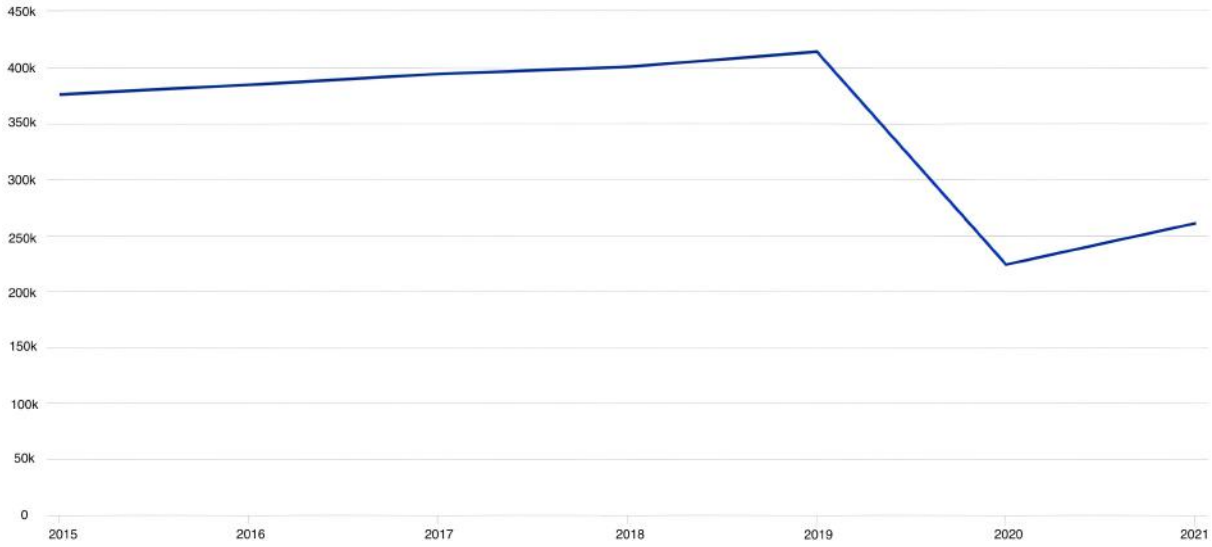

Figure 1.1: Millions of passengers transported per Kilometer every year since 2015 in Europe [1].

Despite the anomaly in 2020, Figure 1.1 clearly shows that trains are still very much in use throughout Europe. Railways are a growing industry with new improvements to the infrastructure every year. Even though trains are becoming faster every year and with a a large number of circulating trains every day, the standardised communications network system supporting most railways is still very obsolete and reliant on old technologies, such as 2G. These technologies are a thing of the past, as they do not fit in the current state of the world. They are slow, vulnerable to security threats, not that effective anymore.

The communication technology in question is Global System for Mobile Communications - Railway (GSM-R) [7], which is mostly an adaptation, to fit railway specifications and requirements, of the very well-known system Global System for Mobile Communication (GSM) / Enhanced Data Rates for GSM Evolution (EDGE). It relies on 2G telecommunication technology that ruled the telecommunications world from approximately 1990 to 2000. After that, Universal Mobile Telecommunications System/High Speed Packet Access (UMTS/HSPA), 3G technology, came to be.

The first technical specification for the GSM network architecture was approved in 1987 and was formulated to be a standard system for digital telecommunications, something to supplant the analogue 1G system in place at the time. The original *Groupe Spécial Mobile* GSM succeeded. Being created

so long ago, it can be asserted that this technology did not take into consideration the problems and technological advances of nowadays [8]. Also, it did not have a strong enough foundation to be evolved and modified to the current world [9]. Some modifications were made to it so it could, for example, be able to support IP-based communications with the EDGE technology.

GSM was the base from which the new system that came to replace it was created, UMTS/HSPA. Universal Mobile Telecommunications System (UMTS) was designed to bring higher speeds and more secure channels. It based its architecture on GSM/EDGE. Long term evolution (LTE), 4G, started a new dawn as fourth-generation technology [10]. This revolutionary system brought all sorts of innovations, increased speed for wireless networks, a whole new spectrum of radio frequencies incompatible with previous generations, reduced latency and many more. This was, and still is in many places, the most advanced telecommunications technology.

Shifting to trains and railways telecomunications history, as mentioned, the railway communication system is ruled by GSM-R. GSM is the main character of this system but it was not the easiest of adaptations. Only in 2000 the final specifications for this system were finalised and put into action. It unified most of Europe's railway communications as the European Rail Traffic Management System (ERTMS) [11].

Of course, all this evolution in communications was also accompanied by an evolution in the security measures implemented. The security of GSM networks was extremely poor, whilst it got a bit better with the EDGE evolution, it is still not a very good solution. Like every evolving thing, the security scope kept evolving with every new generation of communications. Despite communications security in more recent communication systems, like 5G, being much more evolved, GSM-R, as it relies on GSM, is still extremely poor regarding security.

1.2 Problem Statement

How can 5G technology be implemented in telecommunications around the world and still be using 2G in railway communications? Trains are only getting faster and with cars being a big source of pollution trains become a commodity when it comes to travelling long distances or commuting to work. There is a need for trains to evolve and provide more reliable transportation and the current communications system presents a bottleneck in this evolution.

This problem is the main motivation of this thesis. Although specifications have been developed and proposed to use Long term evolution Railways (LTE-R) with 4G networks described in this technical report [12], and even used on real trains, it is not a standard yet. Even so, 3G and 4G present their own security issues in communications that are already solved with next-generation technology. The purpose is mainly focused on what 5G technology has to offer to LTE-R, as there are not many specifications for

a system with these qualities, and analyse security issues that may arise in this system. The goal is to come up with a communications system that will provide railways, which are now relying on GSM-R, a more secure and faster alternative.

One very important concept to grasp in order to understand the topic at hand is the security of a network. GSM-R has a lot of issues when it comes to security. 2G networks are extremely hard to secure. Due to their old protocols and outdated security measures, it has a lot of design flaws and it is not even IP-based, i.e., it does not follow the internet protocol rules, including the ones that prevent security breaches. When adapted to an EDGE network, GSM/EDGE became IP-based but still has its design flaws.

LTE-R is a completely different concept. LTE has been around for quite a while, being available to the public worldwide since approximately 2010. LTE came to replace GSM (2G) and UMTS/HSPA (3G) and offered a wide range of improvements from these technologies, such as faster download and upload speeds, and safer and more reliable communications. 4G technology was created to adapt to the problems of the world, new in a lot of ways. An analysis of some security issues of this network is made in the next chapter but the main focus is the 5G New Radio (NR) technology. Despite LTE-R being a major breakthrough compared to GSM-R, there is still room for improvement, now that 5G is available to everyone and an infrastructure to support it is in place. The aim is to inspect security issues when adapting 5G technology to railways, to use the most recent technological advances in railway communications.

This is the main focus of this thesis, making sure the railway communication system can be improved to more recent technologies without compromising communications **security**.

1.3 Goals and Requirements

The main goal of this thesis was to study a secure way to bring the current railway infrastructure to a more sophisticated era. Providing a secure way to expand the existing infrastructure means exploring security hazards and potential critical points where communications security can be in jeopardy. By reducing the security risk in an evolved system, the infrastructure could, theoretically, be updated to use a more advanced communication system. Thus, the purpose of this thesis is to explore the security implications that evolving the railway communication system to a more sophisticated version would have on the infrastructure itself.

As mentioned, the main goal is to evolve the railway system to have better infrastructure for communications and other services. This opens a lot of possibilities such as:

- Onboard live feed of train cars and platform (if the train is stopped);

- Onboard entertainment systems and user WiFi;
- Perform instant train monitoring remotely from an operations centre;
- Use sensors to provide a safer journey being used to prevent collisions.

Among the most exciting features that an evolved railway system could benefit is Automatic Train Operation (ATO), which is a system that automates the control of trains, allowing them to operate without a human driver, and Positive Train Control (PTC), which is a system that is designed to improve the security of railway operations by automatically controlling the movement of trains.

To achieve these goals, one can apply 5G to railways and modify it to fit. This would allow data rates of hundreds of Mbps and just a few milliseconds of latency. To achieve this progress, 5G infrastructure needs to be extended into the railway system. The speeds provided by 5G technology are sufficient to catalyse all the new changes herein discussed. 5G is already secure, but an analysis of how it would perform, in terms of security, on the railway system still needs to be performed. This leads us to the main requirements:

- Increase the data rates of communications.
- Increase the throughput of railway communications system.
- Decrease latency in communications.
- Keep the system as secure as possible against threats.
- Remove critical points of failure in the system.

While trying to meet these requirements, the objective is to keep the system as secure as possible. There is no way to ensure total security in a system, so the analysis in the thesis focuses more on providing an analysis so that companies can assess the report and perform informed choices for their system's security measures.

In order to make it abundantly clear, the disruptive factor of this work is to take a small step into a new era of telecommunications. It aims to help bring the new 5G radio technology into railways, performing a security analysis of the whole infrastructure's communication. This work also provides possible architectures to bring this reality to life and uses those architectures to examine the potential threat that would prevent these innovative measures to take place.

1.4 Structure

This thesis is divided into four chapters besides the introduction.

- Chapter 2, Fundamental Concepts: Introduction to technologies, and the state of the art of said technologies, needed to understand and comprehend this thesis.
- Chapter 3, Model Development: Description of railway architecture for a 5G network based on ex-

isting railway networks. In this chapter, the network architecture is outlined with all its components and services intended to operate in this new infrastructure.

- Chapter 4, Model Analysis and Reflections: Takes the architecture and studies possible weaknesses and vulnerabilities that may compromise the system using threat analysis models. It then provides different methodologies that can prevent those vulnerabilities from being exploited.
- Chapter 5, Conclusion: This chapter focuses on summarising the most important parts of the thesis.

2

Fundamental Concepts

This Chapter provides a comprehensive exploration of the foundational elements of railway communication networks. This chapter delves into the intricate details of network architecture and technologies, laying the groundwork for understanding their functionality and role in the broader context of modern railway systems and in this thesis.

Contents

2.1 General Considerations

There are a few important organisations in railway infrastructure development. They provide international standards that countries should follow when applying new technologies.

The International Union of Railways (UIC) is an international organisation that represents the railways of the world. It promotes cooperation and interoperability between railways, and develops standards and recommendations for various aspects of railway operation, including communication systems.

European Telecommunications Standards Institute (ETSI) is a non-profit organisation that develops and publishes telecommunications standards for a wide range of industries, including the railways one. It works in close cooperation with the European Union and other standardisation bodies to develop standards that are consistent with EU policies and regulations.

Third Generation Partnership Project (3GPP) is a collaboration between telecommunications standard development organisations, which develops standards for the third generation (3G) of mobile communication systems and beyond. It is responsible for the development of the LTE (Long-Term Evolution) standard, which is the basis for LTE-R (LTE for Railways), a communication system specifically designed for use in railway environments.

The European Union Agency for railways (ERA) is in charge of unifying Europe's rail tracks and has done so with the European Rail Traffic Management System (ERTMS), which is currently employing GSM-R technology but is looking for improvement.

2.2 Security Basic Concepts

The main emphasis of this thesis is on the security of railway telecommunications. Therefore, one of the most important items to provide some background on is cyber security.

When talking about cyber security the CIA (confidentiality, integrity and availability) properties are at the centre of it all, being the key pillars of any secure system. There are other important properties, such as non-repudiation and authenticity that are approached later. Confidentiality means that no one can read the message but its recipient(s), integrity means no one can change the message, and availability means that the message is available to the recipient(s) at all times. If a system can account for all these properties, it means it is secure. However, being able to ensure all these properties is not trivial, as shown later.

One of the most important mechanisms behind secure communications over a network is cryptography. There are two main cypher approaches, asymmetric ciphers, which require a public and private key, and symmetric ciphers, which only require one private key. A common cipher over networks is a combination of both types where mostly the asymmetric cipher is used to share the private key of the

symmetric cipher that will be used from that moment on. For the asymmetrical cipher algorithm, two keys are needed, a public and a private ones. The public key is known by everyone and the private key is known only by its owner. Each person should have a private and public keys. When encrypted with one key (public / private), a message can only be decrypted with the other (private/public). Very basically explained, to send messages over a network someone would use the other person's public key to encrypt the communications symmetric key and therefore only the owner of that public key could decrypt the message with its own private key. After that, the symmetric key is used for the communications. There are many variations to this simple key exchange protocol to ensure authenticity, non-repudiation and other properties, but this simple exchange is at the core of secure key entitlement over a network.

This exchange ensures confidentiality in future communications, nevertheless it had some problems regarding some security properties, like integrity. One crucial addition to it was the incorporation of a Message Authentication Code (HMAC), preventing tempering with the message and guaranteeing integrity. A HMAC is generated using a HASH function, which generates a different output for every message. Depending on the size you want the HMAC to be, the HASH function takes a message and generates a code with that length unique to that message. It is impossible to recreate the message with the HASH of that message.

A person could say that they are another and give a public key to someone. This way, one can think he is encrypting the message with his friends' public key when he is actually encrypting with the malefactors' public key. Hence, the creation of certificates. Certificates allow people to be sure that the public key actually belongs to whom it says it belongs to. This is based on a hierarchy of certificates that can be traced by a chain to a certification authority. There are other ways to ensure that the public key belongs to the right person, but certificates that give you a digital signature are the most standard approach.

Security Analysis Models

The STRIDE model stands as a pivotal framework in the realm of cyber security, primarily designed to systematically identify and address potential security threats in information systems. Developed by Microsoft, STRIDE is an acronym representing six categories of security threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [13]. Each category encapsulates a specific type of threat, enabling a structured approach to security analysis.

- Spoofing Identity: This threat involves an attacker impersonating a user or a device, aiming to gain unauthorised access to systems or information, challenging the integrity of user authentication systems.
- Tampering with Data: This refers to unauthorised alterations made to data, the integrity of data

being at risk.

- Repudiation Threats: These involve an entity denying their actions, lacking non-repudiation mechanisms.
- Information Disclosure: This threat pertains to unauthorised access to confidential information.
- Denial of Service (DoS): This attack aims to disrupt the availability of services, rendering them inaccessible to legitimate users.
- Elevation of Privilege: This involves an attacker gaining higher access levels than initially granted, often exploiting system vulnerabilities.

In essence, the STRIDE model provides a comprehensive method through which potential security vulnerabilities can be identified, analysed, and mitigated. Its application is crucial in developing robust security strategies, ensuring the protection of information systems against diverse and evolving cyber threats.

The DREAD model is another significant tool in the field of cyber security, particularly in the context of risk assessment. An acronym for Damage, Reproducibility, Exploitability, Affected Users, and Discoverability, DREAD is part of a risk assessment methodology that helps in quantifying, prioritising, and comparing various types of threats in software applications and systems. Each component of the DREAD model evaluates a different aspect of the potential risk posed by a security threat.

- Damage Potential: This factor assesses the potential damage if a security breach occurs. It considers the extent of harm a successful exploit could cause, ranging from data loss to financial or reputational damage.
- Reproducibility: This element measures how easily a threat can be replicated once discovered. A higher reproducibility rate implies a greater risk, as it increases the likelihood of widespread exploitation.
- Exploitability: This aspect gauges the ease with which a vulnerability can be exploited. Factors such as the level of technical skill required and the availability of tools to exploit the vulnerability are considered.
- Affected Users: This criterion estimates the proportion of users that would be impacted by the exploit. A threat that affects a larger user base is considered more severe.
- Discoverability: This measures the likelihood of the vulnerability being discovered by potential attackers. High discoverability increases the risk of an exploit being attempted.

By evaluating each threat against these five criteria, the DREAD model assists in prioritising risks based on their potential impact and likelihood. This prioritisation is crucial for efficient allocation of resources towards mitigating the most significant threats. The DREAD model's structured approach to risk assessment makes it an invaluable tool in the development of comprehensive security strategies and in ensuring the resilience of information systems against diverse security threats [13]. For each

component of the table, there is a value assigned to be between one and ten. After every aspect of the vulnerability is considered, a mean of the values is constructed and the result gives the Risk Assessment Average (RAA) that dictates the overall risk of the vulnerability in question.

While other models focus either on threat identification or risk assessment, the combination of STRIDE and DREAD delivers a dual-faceted approach. This integration ensures not only that all potential threats are identified but also that they are evaluated for their severity and likelihood, providing a robust basis for informed decision-making. By addressing both the identification and prioritization of threats, the use of STRIDE and DREAD together offers a more complete and actionable security analysis framework than using any other model alone.

2.3 Network Basic Concepts

A network is composed of many layers. Using the internationally known 7-layer OSI model, a network is built with the following layers: physical, link, network, transport, session, presentation, and application. Only 5 layers are considered rather than the OSI 7 ones, because the layers between the transport and application layers are not relevant to train's communications.

Each of these layers has protocols and each protocol has its own security measures. A good example is depicted in Figure 2.1 where different components added to data received from its upper layer can be seen. For example, application sends a message, when it gets to the transport layer, new information needs to be added so it becomes a segment, then it becomes a datagram on the network layer, and so on. In terms of protection, the physical layer requires physical protection, like locking your screen or monitoring your links, which is the only type of security that is not based on software. Security protocols can vary from MAC filtering in the link layer to https in the application one. The most relevant protocols, like IPSec and TCP, are explained in Section 2.5 where security over a network is discussed. The information in this section can be found and further explored in [14].

2.4 Cellular and Wireless Communications

There are several technologies that are involved in the topics herein discussed. At the foundation of it all are radio communications, which are the core that allows us to communicate. Radio waves travel from device to device, transmitting signals that later, in the device, translate to either voice or an internet connection in the form of data packets. WiFi is used to provide internet in small environments while cellular communications are used for wider ranges and provide voice and internet services.

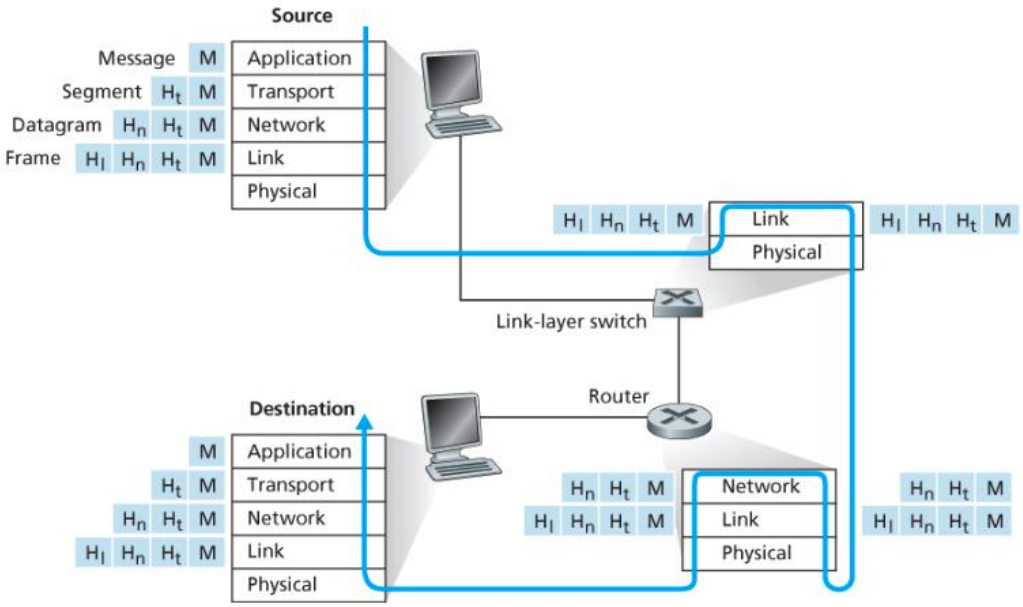

Figure 2.1: Changes made to message throughout some OSI layers [2].

2.4.1 GSM-R

GSM-R is an adaptation of GSM. The full official technical specification can be found in [15], an overview being provided in what follows. The network architecture can be seen in Figure 2.2, which is built on three major subsystems, the Base Station Subsystem (BSS), the Network Switching Subsystem (NSS), and the OSS, also known by its main component of Operations and Maintenance Centre (OMC).

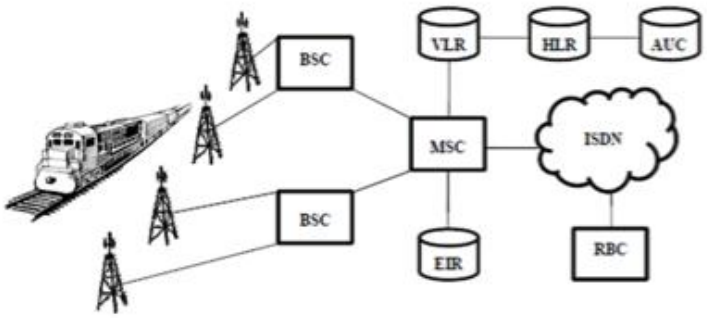

Figure 2.2: Basic GSM-R Architecture with BSS and NSS components [3].

The BSS is composed of base stations, which primarily receive signals from the terminals and relay those signals to controllers. Base station controllers handle channel setups and other logistic matters for the base stations and are also the link to the NSS. In the centre of the NSS is the Mobile Switching

Centre (MSC). The MSC makes use of other NSS components to perform all its functions, such as registration and authentication, but its main purpose is switching and path routing for the signals to reach their correct destination. The other systems in the NSS are the Home Location Register to store and manage subscriptions, the Visitor Location Register to hold temporary information, the Authentication Centre that is a protected database with private keys, and Equipment Identity Reader that helps with network mobile validity. The MSC is responsible for switching and routing messages but the Gateway Mobile Switching Centre (GMSC) is the one responsible for forwarding the signals to the public network being also an extremely important subsystem of the NSS. The NSS can also be split into the Circuit Switched (CS) domain and Packet Switched (PS) domain. The CS handles voice communications and the PS handles internet packets and instead of the MSC and GMSC, it has Serving General Packet Radio Service Support Node and Gateway General Packet Radio Service Support Node, which are basically the same but for packets. The OCM is connected to all subsystems and is used to perform maintenance on those systems and allow them to run without any issues.

There are three major frequency band slots used by GSM-R.

- 4.75-5.00 GHz: This band is used for data services, such as train control and onboard Internet access, having a relatively high frequency, which allows to support high data rates, but has the disadvantage of having lower coverage and penetration than lower frequency bands.
- 876-960 MHz: This band is used for voice communications, as well as for data services such as train control and passenger information, having a lower frequency than the 4.75-5.00 GHz band, which allows it to provide better coverage and penetration but at the expense of lower data rates.
- 1435-1519 MHz: This band is also used for voice communication, as well as for data services such as train control and passenger information, having a similar frequency to the 876-960 MHz band and provides similar coverage and penetration characteristics.

2.4.2 LTE-R

Long Term Evolution for Railways (LTE-R) has not yet been formally specified to be standardised. GSM-R is foreseen to be replaced by LTE-R, whose architecture can be found in Figure 2.3, and like with GSM-R, LTE-R is based on LTE. LTE was developed by the 3rd Generation Partnership Project (3GPP). The development of LTE-R by the acknowledged organisation ETSI is specified in [12].

The LTE architecture is comprised of two main subsystems. The evolved terrestrial Radio Access Network (E-UTRAN) and the Evolved Packet Core (EPC), which is the main and only relevant component of the System Architecture Evolution (SAE).

The E-UTRAN is formed by:

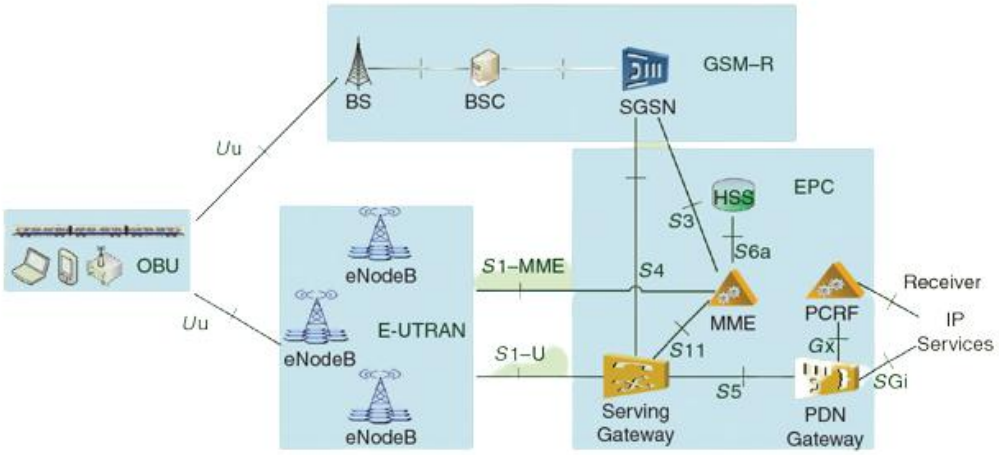

Figure 2.3: LTE-R Architecture [4].

- The Evolved Node B (eNodeBs) are the base stations that provide radio access to the network, being responsible for managing radio resources and providing connection to the core network.
- Evolved Universal Terrestrial Radio Access (E-UTRA) is the radio access network (RAN) that is used to provide high-speed wireless broadband access to mobile devices, such as smartphones, tablets, and laptops.

There are a few key differences between LTE and LTE-R. Because trains move through areas with not such good coverage and at high speeds, LTE-R had to add a whole new component for the radio interface of the railway network. The railway network consists of a series of base stations and antennas that are placed along the railway track, while the core network connects the railway network to the wider communications network. New software also had to be added to LTE to provide better Quality of Service (QoS) and protocols for railways applications. New base stations had to be installed along the railways, since the GSM-R legacy infrastructure cannot be used. The rest of the system remains as LTE.

In terms of cyber security, LTE-R networks face many of the same threats as other wireless communication systems, such as unauthorised access, denial of service attacks, and spoofing. To address these threats, it needs to implement robust security measures.

There are different implementations of LTE-R, one approach to securing LTE-R networks is to use encryption to protect data transmitted over the network. This can include the use of secure protocols such as SSL/TLS for data transmission, as well as the use of encryption algorithms, such as AES or RSA to protect data at rest [16]. Another important aspect of cyber security for LTE-R networks is the use of strong authentication methods to prevent unauthorised access. Some propose using techniques such as Subscriber Identity Module (SIM) authentication or Authentication and Key Agreement (AKA). Also,

this can include the use of multi-factor authentication [17], which requires users to provide multiple forms of evidence to verify their identity. In addition to these measures, it is important for railway operators to regularly update and patch their systems to fix vulnerabilities and prevent exploits.

2.4.3 5G

Fifth-generation cellular networks, better known as 5G, are the latest technology available. It is faster and more secure than LTE and provides several other improvements, such as higher data rates, lower latency, improved reliability, and better spectrum efficiency.

5G networks have two major implementations: Non Stand-Alone (NSA) and Stand-alone (SA). NSA makes use of the existing LTE existing architecture and combines it with 5G NR technology in order to get better coverage and performance. The NSA architecture makes use of advanced radio technologies, such as Massive MIMO (Multiple Input Multiple Output), which allows for the simultaneous transmission of multiple data streams, resulting in improved coverage and reduced interference.

5G SA is an end-to-end 5G network architecture that does not rely on any existing 4G network infrastructure, unlike NSA. 5G SA is expected to provide a wide range of services and features, such as higher data rates, lower latency, improved reliability, and better spectrum efficiency. The 5G NSA architecture allows the implementation of the concept of "network slicing", which allows for the creation of multiple virtual networks on a single physical network. This enables the deployment of different services and applications on different slices of the network, in an efficient use of network resources and ensures that each service or application has the necessary resources to perform optimally.

The 5G SA architecture consists of several components, including the radio access network (RAN), core network, and service layer. The RAN is responsible for providing the physical layer connection between the user equipment (UE) and the core network, and includes the base stations. The core network is responsible for establishing the connection between the user and the service layer, consisting of the mobility management entity, the Serving Gateway (SGW), and the Packet Data Network Gateway (PGW). The MME is responsible for managing the mobility of the user and the SGW is responsible for providing the user with access to the services. The PGW is responsible for providing the user with access to the internet.

The service layer consists of the application server and the Service Layer Gateway (SLG). The application server is responsible for providing the user with the services they require, such as video streaming, gaming, and Voice over Internet Protocol (VoIP). The SLG is responsible for providing access to the services, such as authentication, authorisation, and accounting.

Finally, 5G SA has a network slicing layer which allows for tailoring the network slices to the user's needs, [18].

In the heart of 5G are two very important breakthroughs, New Radio technology and network slicing. The first one, New Radio, works by using a combination of new radio technologies, such as advanced antenna systems, beamforming, Massive MIMO, and carrier aggregation, to increase the capacity and performance of cellular networks. It also uses higher frequency spectrum bands, which includes millimetre waves, to provide faster speeds and more capacity. Network slicing is a technology that allows network operators to divide a single physical network into multiple virtual networks, each with its own set of characteristics and requirements. Each virtual network is referred to as a "slice", being isolated from the other slices, and has its own set of network resources and characteristics. This allows the network operator to customise each slice to meet the specific needs of the customer or application as depicted in Figure 2.4. It also allows for individual slice monitoring.

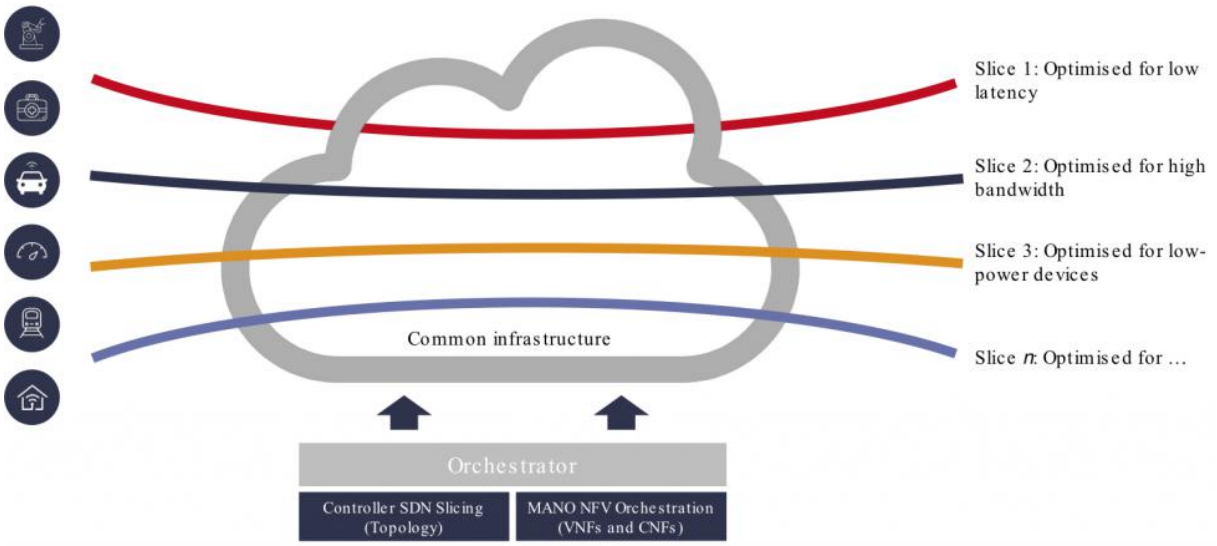

Figure 2.4: Multi purposed network slices [5].

2.4.4 WiFi

For a long period of time, the only explored bands for WiFi were around 2.4 GHz [2]. They were the only ones monitored by the IEEE standards and so they were the only bands allowed to be used. These bands had a major bottleneck because they only possessed a few available channels. Because close channels interfere with each other, there were only about 3 channels one could make use of. Multiple Access Points close to each other with WiFi signals on the same channel cannot be used, because they interfere with each other. Now that 5 GHz bands are able to be explored, that problem has been solved. 5 GHz bands have a much larger number of available channels to explore and channels do not clash with each other. This way, one person can have multiple Access Points in a house and have them not interfere with each other easily. Of course, the range of 5 GHz bands is lower than 2.4GHz, but that is a

trade-off.

The radio interface in a WLAN includes techniques such as frequency hopping and spread spectrum to minimise interference with other devices and ensure that the network operates efficiently. Access Points are an essential component of a WLAN, providing coverage, with improved security and better performance.

WiFi Client Server Protocol is a type of networking protocol used to enable communication between two or more computers, devices, or other networked systems. It is essential in the communication between devices and Access Points. The protocol works by allowing a client device to send a request to a server device, which then responds with the requested data. It is designed to be secure, reliable, and efficient. It uses encryption and authentication and authorisation infrastructures to ensure security.

2.5 Security over network communications

Basic network security and architecture have been described as well as communications architecture and evolution. However, the combination of both is the main point of this thesis, i.e., security over communications. Communication between two points is done over a network. This network is comprised of links and for a message to go from one user to another it usually goes through a few links along the way, i.e., the path or route, the links that the message goes through to reach the recipient. The recipient has an Internet Protocol (IP) address used to identify the message's destination. Each network interface has a Media Access Control (MAC) address that identifies it.

Deploying 5G networks for railways requires a specialized security analysis due to unique operational, environmental, and regulatory demands. Unlike general 5G networks, railway 5G systems support critical infrastructure for safe train operations. This demands heightened reliability, safety, and regulatory compliance. Railway 5G networks handle safety-critical applications like signalling and emergency communication. A breach could lead to accidents or loss of life, necessitating robust security measures. Network segmentation protects operational communications from cyber threats, minimizing the risk of attacks. Compliance with stringent railway safety standards like ETCS is mandatory. This requires tailored security analysis to ensure legal compliance and operational safety.

There are ways to keep information safe from attacks. Each telecommunications generation offers a better security package than the previous one. 5G being the most recent one, it is natural that it would have the most advanced security measures. However, all security measures provided by the communications technologies trace back to the network internet protocol stack model, Fig. 2.1, and security protocols in its layers. Each layer has different security measures, the most relevant ones being the link, network and transport layers.

IPsec provides encryption of data transmitted over the network at a Layer 3 level, using a variety of encryption algorithms such as AES, as well as having systems like firewalls and access control lists. It also includes mechanisms for authenticating the identity of the communicating parties, to ensure that the communication is not being spoofed or tampered with [19]. IPsec nowadays also supports the concept of tunnelling, which allows a secure connection to be established between two parties even if they are communicating over an untrusted network [20]. Some recent adjustments to IPsec include enhancing the encryption by using algorithms such as AES-GCM that provides both encryption and authentication [21]. Ipsec is one supporting algorithm for a VPN. The integration of TLS channels and IPv6 rather than the normal IPv4 also provides better security in these communications. TLS also allows the creation of a VPN at an application layer level rather than a network layer level like IPsec.

A VPNs is essentially a tunnel between networks that can help achieve end-to-end security. These constitute an exciting opportunity in the world of communications security. To achieve a perfectly secure tunnel between sender and receiver is something revolutionary and provides a whole new perspective. There are still a few issues with VPNs as discussed in [22], however, it is still positively good. Because VPNs are a product of the IPsec protocol most of the advances in the protocol will be reflected in this technology such as the encryption algorithms and quantum-resistant algorithms. However, there are also a few features unique to VPNs like enhancing an individual's anonymity to be able to bypass censorship for example. Even though it is more of a traffic analysis, this paper talks about recent VPN and traffic protocol technology which is quite relevant for network security [23].

The link can be a switch, a router, or a computer, among other devices. Securing the link layer of the network means keeping these links safe from attacks. There are several protocols to keep this from happening such as MAC address filtering, Dynamic Host Configuration Protocol (DHCP) snooping and other more technical ones that help keep the link secure. The network layer is a bit more complex because it houses the IP information of the sender and recipient. It uses the IP protocol to run and is vulnerable to more attacks than the previous layers. Whereas in the previous layer the concern is only in the link, the network layer, similarly to the transport layer, can be attacked throughout the entire connection between the sender and receiver. To secure the IP layer one protocol exists, the IPsec. It provides authentication, integrity, and confidentiality of data exchanged between two or more devices over a network. It is used to secure IP communications by authenticating and encrypting each IP packet of a communication session. It has many features such as internal key exchange crucial to solving authenticity problems like the one described in Section 2.2. The most interesting and relevant aspect of this protocol is the tunnel model, which allows for the creation of virtual private networks, enabling users to access private networks and share data securely over public networks as if their computing devices were directly connected to the private network.

Lastly, the transport layer. Transport layer protocols are responsible for providing reliable communi-

cations from user to user between two systems. They are responsible for ensuring that data is delivered in the correct order and that any lost or corrupted data is re-transmitted. The most common transport layer protocols are Trasnmission Control Protocol (TCP) (Transmission Control Protocol) and User Datagram Protocol (UDP) (User Datagram Protocol). TCP provides reliable, connection-oriented communication, while UDP provides connectionless, best-effort delivery. These protocols pave the way for the Secure Socket Layer (SSL). This security protocol is important because it is a cryptographic network protocol used for secure communication between two networked computers. It provides secure remote login, secure file transfer, and secure tunnelling capabilities, just like the ones used in a VPN.

Transport Layer Security (TLS) is a protocol situated between the application layer and the transport layer and it provides a good level of security in communications over the internet. However, it is mostly used in web browsers and application layer services so its application to the railway system communications is still to be determined [2].

Different types of security can be offered. The most important ones are link-to-link, end-to-end, and point-to-point security [14]:

- Link-to-Link security is used to protect data as it is sent between networks. It is implemented at the link layer of the OSI model and is based on the concept of encrypting data as it passes through the links connecting different networks. One commonly used protocol for this purpose is MACsec, which provides integrity, authentication, and confidentiality on Ethernet links. This ensures that data transmitted over the link are secure and cannot be intercepted or tampered with by unauthorised parties.
- Point-to-Point security is used to protect data that is sent between two specific points, such as between two computers or networks. While IPsec is a commonly used protocol for this purpose, it is not limited to point-to-point connections and can also be used for network-to-network connections. Point-to-Point Protocol with encryption can also be employed, especially for direct connections like those in a WAN. This ensures that data are encrypted and unreadable to anyone who may intercept it.
- End-to-End security is used to protect data that are sent from one device to another, ensuring that they is encrypted at the source and decrypted only at the destination. It is based on the concept of encrypting data at the beginning of the transmission and only decrypting it at the end in the recipient's device. It is generally implemented at the application layer. While TLS is commonly used for web traffic, other protocols can be used. This ensures that even if the data are intercepted during transit, they remain unintelligible to unauthorised parties.

In summary, point-to-point security is concerned with the protection of communication between two specific devices, link-to-link security is concerned with the protection of communication between two devices connected by a link, and end-to-end security is concerned with the protection of communication

between two devices from start to finish.

2.6 State of the Art

LTE-R, described in the previous section, has the main components of the Radio Access Network in LTE-R [24], and the Evolved Packet Core providing the core network. The High Speed Railways (HSR) using LTE-R have been extensively detailed and is seen as a very reliable step in the evolution of railway communications. The use of LTE-R to provide reliable communication for HSR systems has several applications and has been proven to be a reliable solution for communications in transportation [24]. The paper focuses on the use of MIMO-DPD (Multiple Input Multiple Output - Digital Pre-Distortion) to improve the performance of LTE-R communication in HSR environments.

3GPP has released a number of technical specifications specifically for the use of LTE in railway systems, LTE-R (Release 14) and LTE-R2 (Release 15). These specifications cover a range of topics, including the physical layer, radio resource management, mobility management, and **Qos!**, [25]. Not only 3GPP but the European Telecommunications International Institute (ETSI) has also released some specifications [26]. Among them, [27] is a good example explaining how LTE can be adapted to a rail environment.

In terms of deployment status, LTE-R is currently being deployed in a number of countries around the world, such as, Japan, South Korea, China, and Germany. In these countries, LTE-R is being used to provide high-quality voice and data communication services to passengers and staff on trains, as well as support for mission-critical communications for railway operations.

5G being the most recent telecommunications technology available, hence, there are few specifications for it, e.g., a technical specification made by ETSI and 3GPP together [28]. 5G-Railways SA is a project that aims to bring the benefits of 5G to the railway sector, including improved connectivity, better safety and maintenance, and also to improve passenger experience.

ETSI has released a few technical reports detailing, among other things, the usage of 5G in railways [6] and its roll in the new Future Railway Mobile Communication System (FRMCS) [29]. These reports have a big impact on the development of this technology. There are also a few other insightful papers on the subject, some describing very extensively the fundamental technologies for a 5G railway system, such as MIMO [30]. Others focus more on just reviewing the current state of the next-generation developments for railways providing good information as [31]. The paper [32], although old, gives a breakdown of characteristics and requirements for communications, those requirements being of the critical and non-critical types. In 2019, Nokia started working with Deutsche Bahn to produce 5G SA systems for automated rail operations [33]. Also, in 2022 Ericsson announced that they were working

with InnoTrans in order to deploy FRMCS using 5G [34].

Despite there being a lot of work required to apply 5G to railways, it is still important to analyse the state of 5G in terms of security and how it is progressing. There are not a lot of reviews on security in a 5G railways system. However, security in 5G regular network can be shifted to a 5G railways system and so 5G security reviews are also considered relevant. The work in [35] goes through the current state of 5G and alerts to the issues of hackers and how telecommunication networks are not safe from vulnerabilities and then moves on to review the technologies used to enable 5G and what level of security they provide. Vehicle to everything (V2X) is another interesting project that although not entirely related to railways, also focuses on real-time data transmission on a moving vehicle. Developments on this project could have applications in railways as well. Issues with 5G deployment on the internet and on projects like this, lift security requirements to fight vulnerabilities like Denial of Service (DoS). This is what is approached in [36].

Regarding security in the railway itself, key management is an important topic and needs to be implemented in a proper way. The paper [37] describes the challenges in key management in a future railway system using recent technology. Overall, the state of the art of security in 5G is still being developed and refined, as the technology continues to evolve and new threats emerge. However, significant progress has been made in addressing the security challenges of 5G, and it is expected that the security of 5G networks will continue to improve as the technology matures.

5GHz frequency WiFi is already widely used as it provides a much better alternative to 2.4 GHz. WiFi can be a crucial way to communicate on the railways. A few examples are communications between train sensors and command control, these can be optimised with WiFi connections, communications when the train is stopped in the platform, the train could connect to the station WiFi to transmit any data or transmit live feed video to the station. Besides these applications, it can also serve to provide commodities to the passengers such as an entertainment system or just basic onboard WiFi. 5GHz WiFi can help an automatic train control system by providing real-time data transmission faster than 5G due to its larger bandwidth. It can help increase the accuracy of the data transmissions and can even increase reliability and efficiency of the train.

The 6 GHz frequency band, also known as the 5.9 GHz band, has been identified as a potential band for next-generation WiFi, also known as WiFi 6E. The 6 GHz band is particularly attractive because it offers a large amount of bandwidth (1.2 GHz) that is not currently being used for other purposes. This bandwidth is expected to be able to support very high data rates, making it ideal for applications such as virtual and augmented reality, as well as other high-bandwidth applications [38]. In 2019, the Federal Communications Commission in the United States approved the use of the 6 GHz band for unlicensed use, paving the way for the deployment of WiFi 6E. Since then, a number of technology companies have announced the development of WiFi 6E products, including routers, access points, and devices such

as laptops and smartphones. This article [39] describes the impact of these frequencies of WiFi on a vehicular environment.

Some of the benefits of WiFi 6E include higher data rates, lower latency, and improved performance in crowded environments. It is expected to be particularly useful in dense urban environments, where there is a high demand for wireless bandwidth [40]. However, there are also a number of challenges to the deployment of WiFi 6E, including the need to ensure that it does not interfere with other uses of the 6 GHz band, such as satellite communications. In addition, there is a need to ensure that the deployment of WiFi 6E is done in a way that is fair and equitable, so that all users have access to the benefits it offers.

Like other WiFi networks, 6GHz frequency WiFi will provide safety features. Amongst them are basic encryption, authentication access using the WiFi Protected Access (WPA3) . Firewalls, intrusion detection systems and network segmentation can also be employed in aiding with network security. Overall, 6GHz WiFi is still in early development despite already a lot of work being put on it.

There have been several recent developments in the field of network security, particularly in the area of communication security. One major advancement has been the widespread adoption of end-to-end encryption (E2EE) for messaging and other forms of communication. This ensures that the contents of a message can only be read by the intended recipient, and cannot be intercepted or accessed by any third parties. To ensure E2EE there are a few important aspects like key exchange mechanisms and public key infrastructures which are systems that use a combination of public and private keys to secure communication [41]. There are a few developments regarding this aspect such as the use of Quantum Key Distribution (QKD) for secure communication. QKD uses the principles of quantum mechanics to generate and distribute a secret key that can be used to encrypt and decrypt messages [42]. This is particularly useful for secure communication over long distances, as it is extremely difficult for an attacker to intercept or compromise the key. There is work in place to expand the range of security established by the QKD protocol using different methods such as Wavelength-Multiplexed time-bin encoding as is described in the article [43]

There has also been a growing focus on the use of machine learning and artificial intelligence for network security. Machine learning algorithms can analyse patterns of network traffic and identify anomalies that may indicate an attempted cyber attack [44]. This allows for more effective and efficient detection and prevention of cyber threats.

Methods of authentication are very relevant as well and the most recent ones would have to be multi-factor authentication. It is not particularly recent but there are interesting papers on new authentication protocols like the one explored in [45] using only XOR and one-way hash operations. People are even discussing and even creating new authentication protocols as is evidenced by an experimental algorithm proposed in the research paper [46] called ”Patiyoot”. This algorithm has just a small twist

by the modification of the Nonce and Timestamp rather than their normal user in more conventional authentication protocols.

3

Architecture Development

This chapter is dedicated to the proposed examination of the Network Service Architecture and Railroad Infrastructure, both of which are integral components of the railway communication network. Understanding these elements is crucial for identifying vulnerabilities and formulating mitigation strategies, aligning with this research's objectives. This chapter focuses on the Network Service Architecture, dissecting its various layers and components. The flow of data through this architecture is explored, and potential vulnerable points are identified such as MTs and routers. Upon completion of this chapter, a comprehensive understanding of the architecture that supports railway communication networks is established. This foundational knowledge is vital for the analyses and evaluations conducted in the subsequent chapter.

Contents

3.1 Network Services

A service is a specific functionality or resource provided so that users can fulfil a particular need or requirement. A service can be rendered in multiple ways, one of which is the internet, or more specifically, over a network. A few of these services are mentioned in Table 3.1. The values in this table represent the standard for a railroad network [6].

Table 3.1: Network Services and KPIs [6].

			End to End Latency (ms)	Reliability	Max Speed Limit (km/h)	Data Rate (kbps)	Payload
Operational	critical	Voice	≤100	99,9%	≤500	100-300	small
		Video	≤100	99.9%	≤500	10000-20000	medium
		Data	≤100	99.9999%	≤500	10-500	small
	non critical	Messages	-	99.9%	≤500	100	small
		Voice	≤100	99.9%	≤500	100-300	small
		Video	≤100	99.9%	≤500	10000	medium
		Data	≤500	99.9%	≤500	1000-10000	large

There are multiple factors to characterise and evaluate a service. A few of those factors are: criticality, fallibility, reliability, and service level.

Criticality refers to the level of importance or significance that a telecommunications service holds for its users. Different services have varying degrees of criticality based on the purpose and the impact they have on individuals and businesses. For example, emergency communication services like 112 are considered highly critical due to their role in saving lives.

Fallibility relates to the potential for errors, disruptions, or failures within the telecommunications service. No service is completely immune to issues, and fallibility recognises the inherent possibility of technical glitches, network failures, or other unforeseen problems that can affect service's performance. It is essential for telecommunications providers to have robust measures in place to minimise fallibility.

Reliability is closely tied to fallibility but focuses on the consistency and dependability of the telecommunications service over time. A reliable service ensures that users can consistently access and use the service without experiencing frequent outages, disruptions, or performance degradation. Reliability is typically achieved through robust infrastructure, redundancy measures, backup systems and other mechanisms.

Service level refers to the stress or demand placed on the telecommunications channel or network to deliver a certain level of service. It encompasses factors such as bandwidth, capacity, latency, and responsiveness. Service levels can vary based on the specific requirements of different applications or users. For instance, a high-speed internet service used for streaming video content may require a higher service level with greater bandwidth compared to a basic email service. The service level must be carefully determined and optimised to meet user needs and expectations.

These values can also be used to understand service's requirements according to the situation it is deployed. For a voice service to be used to order a pizza there is no real need to prevent that connection from being interrupted by any external factor, however, if the communication is between a car crash victim and an emergency service operator, the connection being lost could cost the life of the victim. Therefore, the characteristics above described will vary not only from service to service but also within the service depending on its application. The following services are used in railway systems.

- VoIP: This service allows users to transmit their voice in real-time between two or more people. There are three main ways of providing voice services to users, landline calls, regular cellular calls and VoIP calls. Traditional landline phones use circuit-switched networks to transmit voice data. Mobile phones, on the other hand, use circuit- or packet-switched networks to transmit voice over cellular networks, depending on the generation. VoIP calls use the internet to transmit voice as packets in packet-switched networks. The user's voice is converted into digital data packets, which are then transmitted over to the recipient's device. As the name implies, this service uses the internet protocol (IP) to transmit packets. VoIP calls can be made using a variety of devices, including computers, smartphones, and dedicated VoIP phones.
- Video Surveillance: A video surveillance system is composed of multiple cameras, a Video Management Centre (VMC) and the infrastructure that connects both. The infrastructure connecting cameras and VMC tends to be secure and the flow of information is encrypted so that it cannot be tampered with. The footage is then monitored in real-time (either with automated software or by a real person) and potential security or safety incidents can be avoided. The images can also be stored if the purpose is not continuous monitoring. Cameras can be either analogue or IP. IP cameras offer better results in video capture but the files they produce are larger than analogue. In an IP network cameras can be a better option because they are directly linked to the network.
- Data: A data service is a bit of a vague concept, it mainly describes sending packets of data through the network from one place to another. It can be anything. Internet uses a variety of protocols to ensure that data are transmitted reliably and efficiently. These data can be anything from signalling and control information to a YouTube video. Internet data services are available through a variety of devices. Internet data exchange services also use cloud-based solutions for data storage and transfer. Cloud-based services, such as Dropbox, Google Drive, and Microsoft OneDrive, allow users to store and share files over the internet. Overall, internet data exchange services use different protocols and technologies to transfer data between devices or networks, in a secure way.
- Messages: Messaging services can be used to send a wide variety of message types, including text, images, videos, audio, and documents. They use different technologies to transmit messages over the network. One of the most common technologies used is the Short Message Ser-

vice (SMS), which is a standard protocol for sending text messages between mobile devices. Messaging services also use Internet-based protocols such as Instant Messaging (IM) and social media messaging. These protocols use the internet to transmit messages between devices, rather than relying on cellular networks.

- Video Calls: This service enables users to have real-time, face-to-face communication using video and audio streams. To manage video call service, it dynamically adjusts the quality of the video call based on the available bandwidth, ensuring that the call remains stable and clear.
- Video Stream: Enables users to watch video content on their devices in real-time. There are several video streaming services. For the video to reach the users there are some steps involving encoding and compressing said video. To have a good user experience there are a few techniques used such as adaptive bitrate streaming, buffering and caching.

3.2 Railroad Infrastructure

Now that the railway services have been described, it is time to describe what supports them, in this case, the infrastructure. The subsequent architectures describe this infrastructure in detail and as previously stated, later helping to evaluate network security. These figures are based on diagrams provided by Thales and seen in Appendix A.

3.2.1 General Architecture

The infrastructure of a train network is fourfold. All parts work together and exchange information so trains can operate smoothly and safely. The general architecture in Figure 3.1 is a high-level description and includes the main components of the railroad infrastructure. These components are complex and with infrastructures of their own. The components communicate either by an optical fibre network or by radio links. As depicted in the figure, the train can be in a static position (stat) when it is stopped at a station or in a moving position (mov) when it is in transit. A moving train cannot connect to the train station for more than a few seconds when it is arriving or departing the station and it is still in reach of the station's antennas. The following infrastructures and architectures are based on information provided by Thales, Appendix A.

- Control Centre: It is the brain of the network. It manages and controls trains and stations from a distance sending and receiving information. It is a complex system with multiple functionalities and is capable of controlling and monitoring multiple trains and stations.
- Base Station: Standard base stations that relay information between trains and the control centre, to which they are connect via an optical fibre. The connection between Base Station (BS) and Control Centre (CC) is secure as long as neither end is compromised. There are multiple BSs on

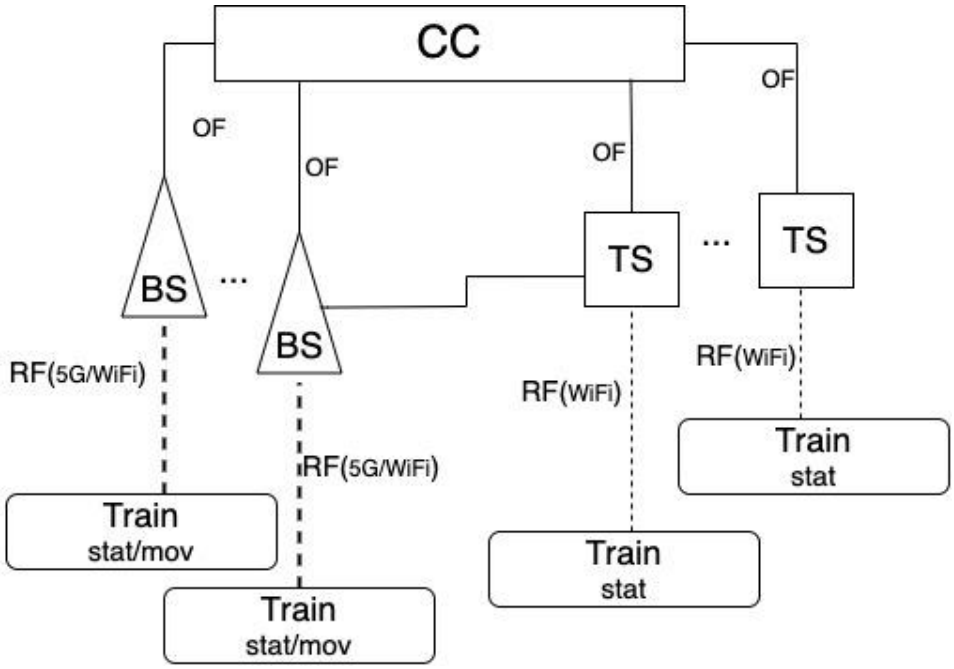

Figure 3.1: High-level railroad infrastructure communications network architecture.

the network and spread across the railroads. This way the train can maintain a firm connection throughout the journey.

- Train Stations: It usually has two states, i.e., when a train is in the station and when the station is empty. It communicates with the CC via optical fibre and with the train via radio links. The services at the train station are non-related to the ones on the train and on the CC. However, the TS can assist train services when it is docked.
- Train: A very important component of the whole system. It can have the ability to self-navigate. It communicates with the base stations via radio links.

3.2.2 Train Architecture

The train is one of the most important entities of the whole system. It is the actual physical place that moves passengers from one place to another. The network presented in Figure 3.2 has a very simple logic behind it. There are three main service types and each has a sub-network servicing them. The passenger services channel is completely separated from the train services channel for security and availability, among other reasons.

In the following list, highlighted in blue are points of access to the network on the train, excluding physical access to any hardware, for instance plugging a laptop into a switch. If physical access is not possible an outsider could only gain access to the network through a wireless connection and the only wireless devices on the train are the passenger's router, the 5G MT and the Wi-Fi access point. The

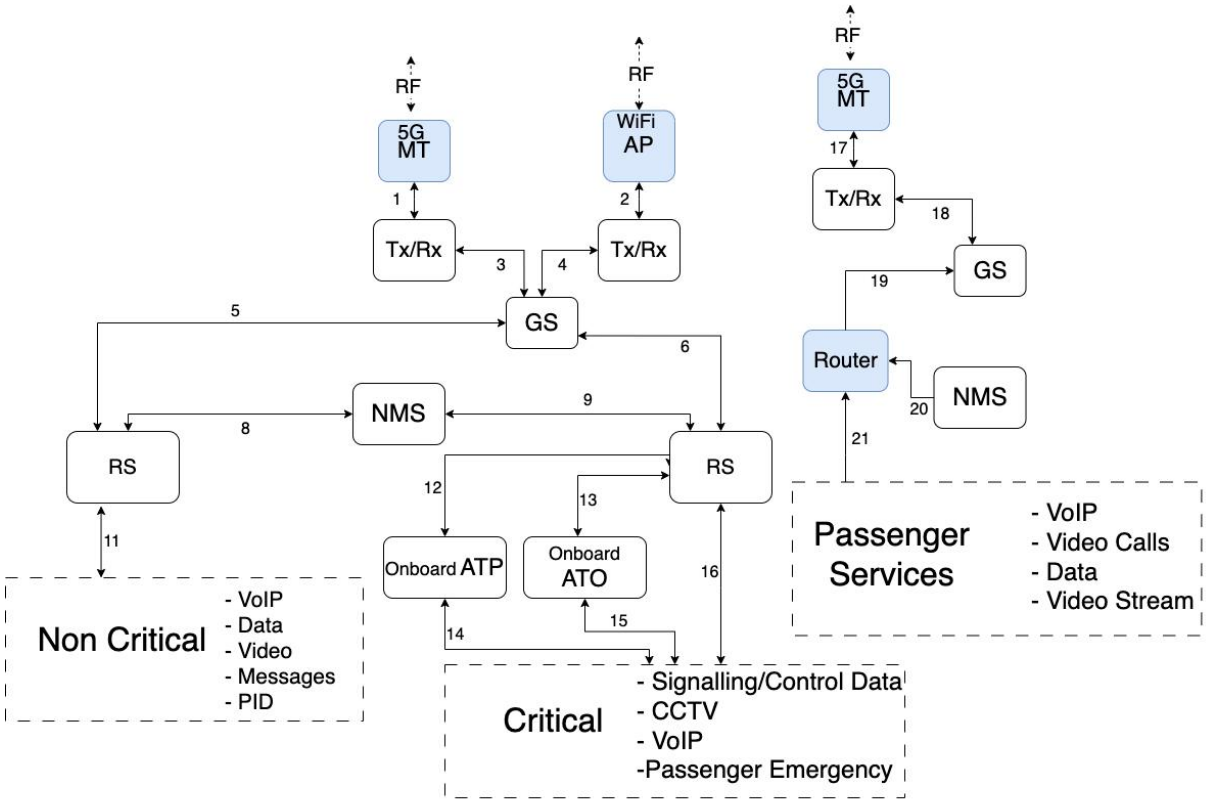

Figure 3.2: Train Network Architecture.

train services can be seen in the following bullet list.

In the following list, the train components are briefly introduced.

- Access Point: It serves for incoming and outgoing communications using short range radio frequencies.
- Mobile Terminal: It is used so that the train and the base station can communicate.
- Gateway Server: The GS serves as an initial barrier for communications arriving at the train.
- Network Management System (NMS): The objective of the NMS is to evaluate the performance of the network, monitor, and manage it.
- ATO: The ATO computer takes control over specific functions of the train, reducing the reliance on manual operation.
- Automatic Train Supervision (ATS): The ATS system aims to receive readings from the train's control services and process this information in real-time.
- Ruggedized Switches: The RS offers an extra layer of protection once it has extra security software installed.
- Router: The router provides internet access to the passengers on board the train.

The access point bridges the gap between wired and wireless networks. There should be at least 1 Access Point per carriage on the train. This component exists to provide Wi-Fi communications mostly when it is faster and more efficient than using the standard 5G terminal. It is more of a complementary measure to the underlying 5G infrastructure.

The Mobile Terminal (MT) works as a communication hub, enabling real-time data exchange between the train and control centres, ensuring efficient and safe operations. It can transmit onboard diagnostics and performance data, aiding in proactive maintenance and quick response to any emergency.

The gateway server's purpose is to serve as a filter and firewall for unwanted, unauthenticated, or unreliable communications. It will also be useful for messages leaving the train to be routed to the control centre in the most efficient way possible. Additionally, its functionality includes distinguishing the packets arriving at the train between data intended for a public Wi-Fi access point for customers, and data for services related to the train. It also serves as a bridge between networks so it helps translate packets that may be operating on different networking protocols or models.

Logically, there are two NMS onboard, one focusing on train communications and the other focusing on passenger communications. This can be accomplished with only one physical NMS as long as operations are logically separated. They each aim to protect different things but they are equally important. One aims more at controlling the passenger's access to the passenger router and the other aims at protecting the services the train needs to properly operate.

The ATO allows for different levels of automation, which are indicated by the Grade of Automation table. The computers use sensor sets to gather data and make informed decisions regarding train operation. The information is processed in real time and action is taken according to the received readings.

Unlike the ATO, the Automatic Train Protection (ATP) system incorporates warning systems and safety measures to prevent collisions, overspeeding, and other hazardous situations. It focuses more on the safety of the train rather than basic operations.

The RS is the last barrier between the CC and the train services and the first barrier between the services and the Control Centre. Its protection aids in finding problems with incoming or outgoing communications. The switch helps create an internal network inside the train connecting the devices and the different services in question. Whereas the gateway server will focus more on connecting the different networks (the critical, non-critical, passengers and then the exterior network), the switches will focus on forwarding packets to the different devices and creating a network. Because there are some security aspects that will not be able to be approached in the GS, the RS is important.

This router protected by a NMS is responsible for granting the passengers the services in the image.

It functions as a normal router using radio frequency waves of 2.4 GHz and 5 GHz for its communications.

- Critical: The critical services are serviced directly by a RS, being monitored by a network management system. The switch is connected to a gateway server which, with specialised hardware, connects to the base stations along the track.
  - VoIP: It is used to convey emergencies or critical information for the proper functionality of the train, via verbal communication.
  - Closed-Circuit Television (CCTV): This is used for critical video that cannot have very big latency values.
  - Data: This data is used for the signalling and control of the train so good speed and latency values are of the essence.
- Non-Critical: The non-critical services are also serviced directly by a RS, being monitored by the same NMS as the critical ones. The switch is connected to a gateway server which in turn will forward the message to the destination.
  - Messages: It is a bi-directional communication that uses terminals on the train and on the CC to function.
  - VoIP: It is very similar to the voice service described in the critical areas, however, the nature of the information that will be transmitted will be different and therefore, the performance of this communication needs not to be as efficient as the critical.
  - Video: Like the voice service, it is identical to its critical counterpart in terms of points of access and communication specifications but varies in performance requirements.
- Passenger Services
  - VoIP: Voice communications for the passengers will be provided by voice over IP services.
  - Video Calls: Same as voice, this service is ensured by the onboard router.
  - Video Stream: The onboard router will ensure this service.
  - Data: The data service includes messaging services like WhatsApp and other internet-dependent apps such as games.

Due to the critical nature of VoIP communications, a special voice channel has to be available at all times and requires an extremely high reliability. This communication is performed either by the staff or passengers. The staff passes on emergencies and critical train information whereas passengers should only use this channel for emergencies. Critical information for the train may constitute non-responsiveness of onboard controls and remote control action may be required, obvious faulty gauges readings and others. This communication is majorly bidirectional. This communication equipment consists of microphones and speakers that will be the input and output points of the communications.

The CCTV is more of a unidirectional type of communication rather than bidirectional. This system is completely automated and needs no intervention from staff. The communications are between the

train and CC. Examples of critical video may be front train cameras of tracks to scan for irregularities and live video of the onboard control cabin. Cameras are responsible for capturing the images on the train side whereas the display shows the footage on the other side, these are what make up this service.

Data communication is done between train and CC just like video communication is. The connection is bidirectional and this way the CC can control the train at a distance using ATP and ATO technology which is already developed. Entry points and output of this service constitute the sensors and train actuators and on the CC side just the control and signalling computers which should be heavily protected.

Non critical messaging is used for standard communication between staff and control centre; this non-critical communication helps to monitor information like passenger count and other information that is not fundamental to the good function of the train.

Examples of non-critical voice communication include a disorderly passenger on board that needs to be removed at the next stop, a malfunction with an onboard toilet and this sort of information.

Passengers VoIP will be available via the router on board and should be available to passengers with no interruptions.

For passengers video calls and video stream, the train needs to have necessary performance requirements to accomodate those needs. This means sharing enough bandwidth and throughput to the passenger router. Examples for video streaming services are Netflix, Disney Plus and others.

3.2.3 Control Centre Architecture

The control centre is a centralised location that monitors and manages the various systems and operations in real-time. It is also a very vital part of the system. Its main purposes are to coordinate and manage resources, control operations, respond to incidents and emergencies, and improve performance and efficiency. It plays a crucial role in ensuring the smooth and safe functioning of complex systems and processes. As seen in Figure 3.3, the CC can be seen as divided into a few main subsystems. The ATS system aims at controlling and monitoring the train, the NMS system focuses on ensuring the security of the communications and of the CC. The segregation between systems in the train spreads to the CC to ensure maximum separation and keep the two networks without any points of contact. Because there are no Wi-Fi connections and physical access is not being considered, there is no way for an attacker to have access to the control centre unless they gain access through an outside source such as a train.

- CC infrastructure
  - Core Network: The information flows and arrives at CC and are first received by the CN.
  - Network Switching System: It serves as a support to the CN and has some of the same functions.
  - Automatic Train Supervision: The ATS sub-system is responsible for the monitoring and con-

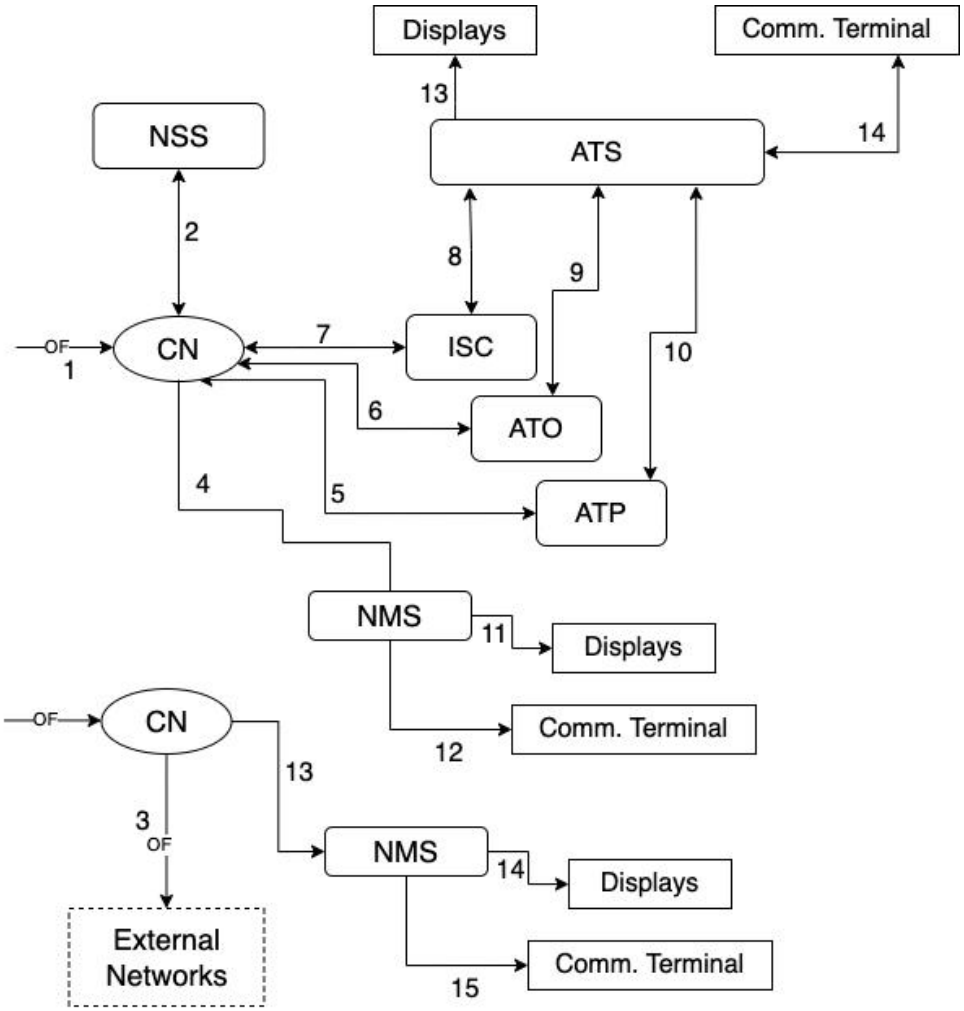

Figure 3.3: Rails Control centre internal architecture.

trol of train traffic, providing train drivers with information on train movements, track occupancy, and speed limits.

- Automatic Train Operation: ATO sub-system automates the train's acceleration, cruising, and deceleration functions to maintain the scheduled timetable and improve energy efficiency.
- Automatic Train Protection: The ATP sub-system ensures that the train operates safely within the defined speed limits and that the train stops automatically in the event of an emergency or violation of safety rules.
- Interlocking System Centre: The ISC is a safety-critical component of a railway signalling system that helps to prevent train collisions and other accidents.
- Network Management System: In the CC, the NMS is a software platform used to monitor, manage, and maintain computer networks.

• CC services support

- Control Services - These services will be the other end of the services described on the train and train station.
- Security Services - They will monitor the network for strange activity, validate base stations and trains, and authenticate them as well when needed.
- External Networks - External networks are all public services that are used or can be used to help the control centre.

The core network is a crucial component of the communications system, which connects different devices to facilitate seamless and secure transmission of voice and data traffic across the various networks. With the aid of the network switching system, it performs functions such as routing and switching, authentication and authorisation, mobility management, and QoS management. Its main purpose is to ensure the reliable and secure transmission of communication services. From this component, the information flows to the rest of the control centre.

The network switching system is also a critical component of the communication system. It performs functions such as packet forwarding, network segmentation, traffic control, and QoS management. It is crucial for managing and directing the flow of data across the railway's communication network. It enables the efficient routing of critical information, such as train locations, signalling data, and operational commands, between various components of the railway system, including trains, trackside equipment, and control centre systems.

Most functions will be performed automatically but there are displays and terminals as well to support other train services like voice and CCTV. This system is primarily responsible for the management and oversight of train movements across the network. It ensures optimal train scheduling, manages traffic flow, and minimises delays by dynamically adjusting train operations in response to real-time conditions

The ATO focuses on the automated control of the train's movements, including starting, stopping, speed control, and door operations. This automation enhances operational efficiency and consistency, reducing the likelihood of human error and ensuring precise adherence to the scheduled timetable. ATO systems can vary in the level of automation, ranging from partial automation, where the driver is responsible for some tasks, to full automation, where the train operates completely driverless.

The primary function of ATP is to ensure train safety by preventing collisions, overspeeding, and other dangerous situations. It continuously monitors train speed and enforces compliance with speed limits and signal aspects. If a potential safety breach is detected, such as exceeding the permitted speed, the ATP system can automatically apply brakes to prevent accidents.

The system works by establishing a set of rules and logic that must be followed before signals can be set to allow train movements. These rules create a safety mechanism designed to prevent conflicting

movements through an arrangement of tracks such as junctions, crossings, and switches. It ensures that signals and switches operate in a coordinated manner to allow the safe passage of trains, preventing collisions and derailments.

The purpose of the network management systems is to ensure the availability, reliability and security of network services and resources, as well as to optimise network performance. There are terminals and displays for staff to perform the monitoring and defence of communications.

The first supporting service of the OCC are the control services. The CC has to have staff monitoring the camera feeds, on the comm. terminal to aid train staff and the software on the CC has to provide indications on speed reduction/increase according to the information received by the train.

As for the security services, the services of this subsystem will handle the security of the communications on the CC side by implementing sets of rules, encrypting the communications and other strategies to help further secure every connection.

For the external networks, if there is a need or if it is better to use a PSTN to communicate with a train or to communicate with whatever is needed for a reason, it is possible. It is dangerous to connect the centre to public networks and all data received from these will need to be examined very thoroughly.

3.2.4 Train Station Architecture

The Train Station is another part of the global environment being described. It is where people wait to get on the train and has a whole life to it as well as its own infrastructure separate from the train. Its architecture can be seen in Figure 3.4. The services there are also independent of the train. There are two major states of a TS, with a train or without a train. Most of the time there will be no train at the station. The station will have an Access Point dedicated to the train's services which can be connected via WiFi if there are communications requiring large amounts of bandwidth. This Access Point allows the train to connect directly to a control room that will provide the train with instructions. To isolate the passengers from the main network, the communications channels are isolated as well.

- Train Station Infrastructure
  - GS - Much like on the train, the GS will serve as an initial barrier for communications arriving at the station. Additionally, its functionality includes distinguishing the packets arriving between data intended for passenger services, and critical or non-critical services. It also serves as a bridge between networks so it helps translate packets that may be operating on different networking protocols or models.
  - RS- The RSs offer an extra layer of protection once it has extra security software installed.
  - Aggregation Router - The aggregation router helps manage the communications.
  - Router - The router will be a series of simple devices spread across the station that will provide

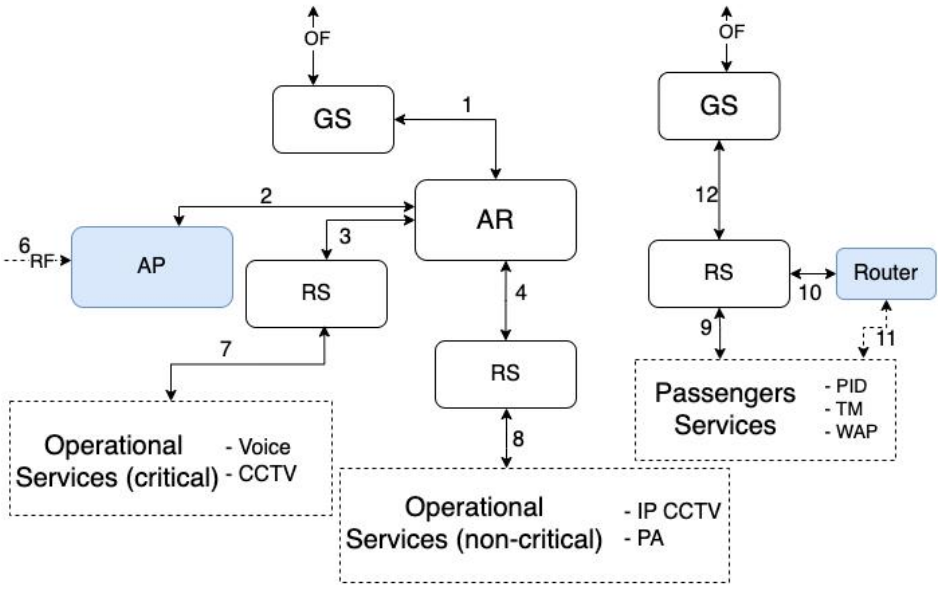

Figure 3.4: Train Stations' internal communications network architecture.

the passengers with a public Wi-Fi network.

- Access Point - The Access Point in the TS has the purpose of serving as a sort of base station for the train services to help when the train is in the station.

- Train Station Services
  - Non Critical
    - IP CCTV - There are some places on the station that do not need a critical channel to communicate due to its not having such high importance.
    - Public Announcements - The public announcement system should be used by staff members or if need be, by controllers in the CC.
  - Passenger Services
    - Public information Display - The PIDs service has the goal of giving passengers basic visual information such as train location, estimation of arrival, delays, weather conditions and others.
    - WAP - The Wi-Fi will be divided into staff and passengers.
    - Ticket Machines - TMs allow the users to buy tickets and help the system record the expected occupancy for the train.

The GS's purpose is to serve as a filter and firewall for unwanted, unauthenticated, or unreliable communications.

The RS helps create an internal network inside each service. The switches will focus on forwarding packets to the different devices and creating a network within the station's larger network. Because there

are some security aspects that will not be able to be approached in the GS such as error checking, the RS is important.

The AR aggregates multiple network connections into a single high-speed link. Collecting data from multiple sources, processing it, and sending it out over a single connection to its destination, improves network efficiency, reduces costs, and increases overall network performance.

The router will be connected to the passenger services RS which will in turn connect to the other passenger services.

In case of the train being static in a station, the train instead of using the nearest base station will use the train station's Access Point and connect more easily with the CC.

The CCTV monitors the platform, stairs, and other places in the station.

Public announcements should refer to standard information like lost baggage or arriving trains. These announcements can even be automatized and played periodically.

There should be two networks and the routers on the station should be equipped to support this feature. For the employer's network, a login is required for access to be granted and for the passengers, the network access should be open to grant easier access.

3.3 Architectures and Services Summary

This chapter's main goal is to describe thoroughly a railway infrastructure that supports the use of a 5G network. There is more than one way to design an architecture as such, however, securing a network starts as early as designing its architecture. Therefore, this network is carefully detailed and designed so it can be as secure as possible and support all kinds of systems to deal with potential threats. Also, to perform a security analysis, such as the one coming in the next chapter, there is a need to have something to analyse other than a hypothetical network, hence this network description.

There are a few points of access in the previous section's diagrams. Because this thesis falls under the assumption that there is no physical access to the network by an attacker, these points of access are the most important components of the infrastructure. In the next chapter, the security analysis focuses towards the systems on the train and the connection between the train and the base station, since there should not be any WiFi devices plugged into the network on the CC, therefore it is not directly susceptible to attacks that do not originate with physical access or social engineering. Also, the problems with the infrastructure on the train can also be replicated in the train station with a few tweaks so a different analysis for both would be a bit redundant. And last, the train is the physical place where the passengers deposit their trust and even their lives, so for that reason, it needs as much scrutiny, when it comes to security, as possible. For these reasons, only train components and train services are

being subjected to the security analysis that will be made up of STRIDE and DREAD analysis.

There is more than one way to design an architecture and there is also more than one way to choose how to implement the infrastructure. For example with the imminent standardisation of the FRMCS using a 5G stand-alone network for communications, the use of public antennas can be explored to service railroad communications instead of railway operators having to implement their own communications infrastructure. Then the subject of communication segregation arises. There are a few schools of thought on the matter and they all vary on the level of segregation that there should be. Furthermore, there are several ways to accomplish network segregation like using VLANs or even with more recent technology, different network slices.

Throughout this chapter, a meticulous exploration of the various components and functionalities that underpin the railway system, emphasising its robustness and adaptability to potential threats, was exercised. These services, encompassing critical and non-critical functions, passenger services, and control services, constitute the lifeblood of this technological ecosystem. Delving into the security analysis in the upcoming chapter, the focus will gravitate towards safeguarding these services, particularly those aboard the train and the link between the train and the base station. These are the services that will receive the most attention due to the assumptions that will be explained later on.

4

Architecture Analysis and Evaluation

In this chapter, a security analysis of the communication system introduced in Chapter 3 unfolds, using the DREAD and STRIDE models. The road map offers a preview of the analysis from top to bottom. Assumptions, crucial to the study's scope, are established at the beginning of this section. The following discussions scrutinise the security of core components like Routers, followed by an exploration of service-level vulnerabilities. The chapter concludes by unveiling mitigation strategies for both components and services.

Contents

4.1 Road map

In this chapter, a meticulous cyber security analysis of the railway communication systems described in Chapter 3 is conducted. This examination is performed using DREAD and STRIDE models described in Section 2.2. Each criterion from DREAD is graded from one to ten and the value's mean is used to calculate an overall risk score referred to as RAA. This structured approach should allow organisations to prioritise security vulnerabilities efficiently.

Figure 4.1 explains the flow of this analysis. Firstly, an analysis of the component's vulnerabilities is made. This analysis is not focused on how attacks are made or on how the network was breached. Instead, it revolves around identifying, listing, and assessing the impact of possible attacks, which aim to compromise a network node. Then, the analysis expands to the provided services. The same DREAD evaluation applied to the components follows now to services. The main difference is that, leveraging some of these attacks, there is the possibility that a component may already be compromised by a previously mentioned attack. As before, this analysis does not focus on the how of these attacks.

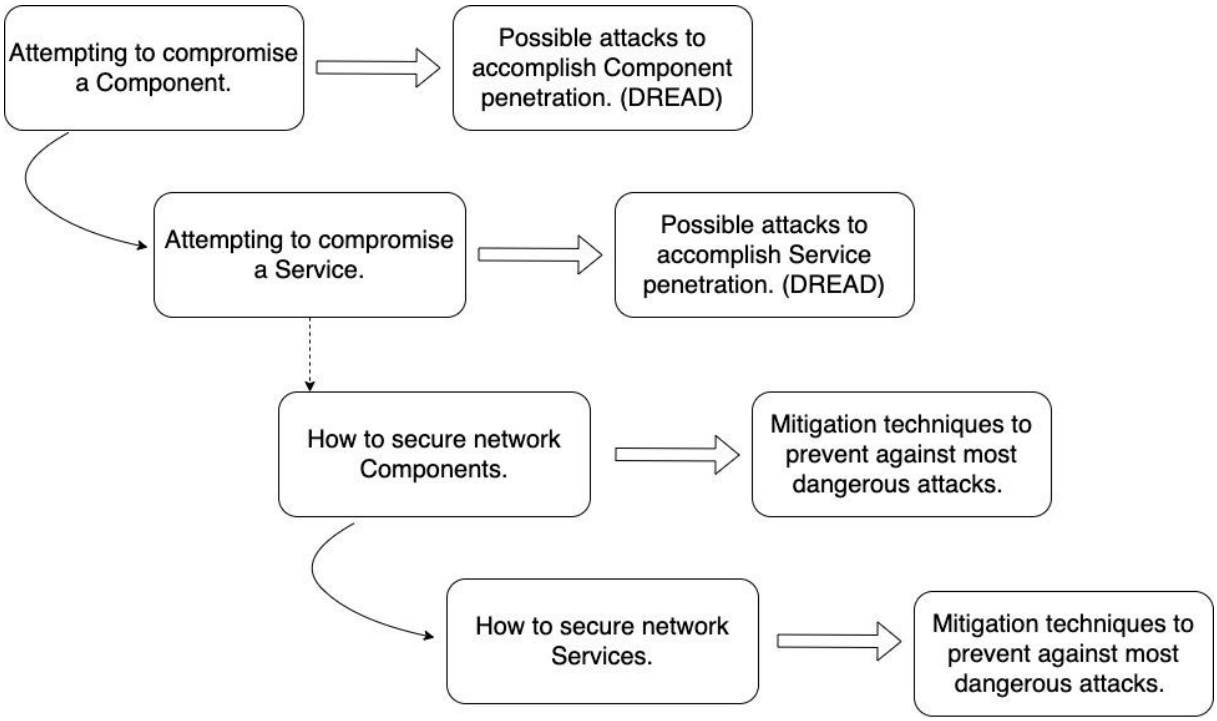

Figure 4.1: Security Analysis Roadmap.

After the different scopes of attacks are explored, the focus shifts to the "How" of the most dangerous attacks (deemed so by the DREAD analysis). The different ways to mitigate those vulnerabilities are approached.

There are several assumptions, central to this analysis, that serve as pillars for this analysis. The

way the attacks will be made takes into consideration assumptions that are intrinsic to the scope and depth of this study, being the following:

- Services use different channels with different levels of security. However, the way a channel is protected can be applied to other channels as well.
- Passenger communications are not very relevant.
- The internal and external networks are entirely isolated from each other.
- Implementing and managing a segregated network is inherently complex and requires meticulous planning.
- The system's standard security configurations could potentially be weak enough to allow impersonation attacks, affecting the integrity of communications.
- There is no physical access to the network nodes, thereby eliminating the risk of direct hardware tampering. Even though there is no physical access to nodes, there is equipment, in the network, communicating via radio waves, which can be exploited.

These assumptions will be intrinsic to the analyses and evaluations in the following chapter. They provide the framework within which the study operates. There may be a few occasions outside the scope of these assumptions but they are detailed and explained as isolated situations.

4.2 Components Analysis

The building blocks for the communications system are 5G and WiFi, which by themselves assure security measures such as strong encryption and mutual authentication amongst others. Nevertheless, a large part of the security provided by 5G and WiFi stands on proper implementation decisions made to the system in question.

When designing the architecture of the systems that make up the railroad, a few points of access were identified. These points of access are devices that can be accessed via a wireless connection. The devices in question are the passenger WiFi Routers onboard the train, the Access Point (AP) on the train and the MT on the train. Some vulnerabilities can be exploited if the network is not properly secured and other components can be compromised through these points of access.

The following analysis focuses on compromising the network through the devices that make up the network. The devices that are analysed are:

- Router.
- Mobile Terminal/Access Point.
- Gateway Server.
- Ruggedized Switch.

- Base Station.

The chosen architecture for the railway network is segregated. However, non-segregated architectures are a viable option and in these subsections, a brief comparison of both is done.

4.2.1 Router

The Router for passengers is in an isolated part of the network as seen in Figure 3.2. This division offers some protection to the rest of the train services in case the router is compromised. Nevertheless, if the router is compromised, the attacker still has access to all passengers connected to that device and, if skilled, will be able to explore the router's connections with the GS and potentially the CC. It is not a major point of access to the internal network as the information on this channel pertains mostly to passengers, but there is always the possibility that something was poorly configured in the network isolation and the attacker will gain access to the internal train network, but the assumption is that networks are completely segregated. Due to that fact, this point of access has a low damage potential to the train itself but high to passengers on board. The DREAD table for this node is shown in Figure 4.1.

Table 4.1: Router Vulnerabilities.

Device	Attack	D	R	E	A	D	Consequences	RAA
Router	Flooding	3	7	5	7	8	Router shutdown or reset.	6.0
	Brute Forcing	2	2	8	8	5	Elevation of privilege to router's admin.	5.0
	Spoofing	2	8	2	8	5	Elevation of privilege to router's admin.	5.0
	Firmware Exploits	4	8	5	8	7	Manipulation of router according to exploit.	6.4

The first attack is flooding the router. This attack will overwhelm the router with an amount of traffic larger than the router can withstand, which can cause the router to fall back to default configurations dropping some security protocols. This would allow an attacker to gain control of the router. This type of attack is considered to be a DoS attack and it would affect the router's processes, inputs and outputs and data flow. Because the attacker cannot access any critical information (passenger information is not considered critical for the proper function of the train) to the train, its damage potential is very limited. It is not a very hard attack to perform therefore its reproducibility is high. This attack would require knowledge to understand how to deploy, so the exploitability is medium. Everyone using this router, not using a local VPN on their devices, would be vulnerable to multiple attacks so the percentage of affected users would be very high. The discoverability of this attack will be high because the router is a public point of access to users and anyone can access it and also because there are many ways to perform

this attack so it is more likely for anyone to find information or an exploit for this attack..

Another possible attack on the router is brute forcing to get admin control over the device. This constitutes an elevation of privilege attack. The consequences of this attack, like most of the other attacks to the router that are described, will not vary from the ones described above. The router is compromised, the GS may be compromised as well and so the internal train network is exposed. There are a few differences in the way the attack is performed though. Because it is a very hard attack to perform its reproducibility is very low. The exploitability is high once this attack consists of running a script. The damage potential and percentage of affected users are the same as a flooding attack but the discoverability changes slightly. The discoverability will be lower than a flooding attack because gaining access to the admin portal is harder than just flooding router channels. Whereas in a flooding attack, it is easy to spot an unusual amount of traffic, in a brute force attack, if the script is properly written, this attack can be undetected.

For now, social engineering attacks will not be considered and therefore spoofing attacks become harder to perform in this situation. If a phishing attack were to be successful on a network admin the attacker would have unauthorised access to the router configuration settings. In other ways to perform this attack, the attacker would need the IP address of an admin, and change their IP to match the admins so the router would grant him access. They would have to search the network topology, explore the user's IPs and probably try and guess which ones were admin. This process could take a lot of time and effort just so the attacker could gain access to the passenger's information.

Lastly, another compromising type of attack on the router is firmware exploits. These can grant elevation of privilege to the attacker, and let him tamper with the device in many ways like installing back doors or another kind of malware. Depending on how the vulnerabilities are exploited the impact on the network can vary. For an elevation of privilege, the risk assessment is similar to that of a brute force attack but with a slightly higher reproducibility. The discoverability will depend on the type of exploit. If the vulnerability only needs the attacker to be connected to the network, which is the most common and the scenario which will be considered, the discoverability is high. On the other hand, if the exploit needs to be deployed inside the router's settings it is much harder to reach. There will, like on the others before, be a very high percentage of affected users. The exploitability would be medium because some knowledge of the router firmware is still needed to exploit a vulnerability and the reproducibility would be medium as well. The damage potential would stay very high for the users but pertaining to the control and train security it remains low due to the network's separation. As previously said, the routers in the train and in the train station are very similar. The changing component is the internal network, therefore this analysis can be applied to the train station router.

4.2.2 Mobile Terminals and Access Points

The MTs on the train allow it to communicate with the BSs via a 5G network. This is a crucial piece of equipment, communicating via radio links, which makes it vulnerable to wireless attacks. Because this is the link used to connect with the CC, it cannot be compromised otherwise the security of the train is as well.

There are a number of attacks that could be performed in order to disrupt this connection, as shown in Table 4.2. Attacking the MT does not mean directly attacking the terminal itself but it can also mean attacking its connections. For instance, the first attack in the list is a man-in-the-middle attack (MitM). This attack targets the connection between MT and BS and not the MT itself.

Table 4.2: MT and AP Vulnerabilities.

Device	Attack	D	R	E	A	D	Consequences	RAA
MT/AP	MitM (Tampering)	10	3	4	10	5	Information being manipulated.	6.4
	MitM (Eavesdropping)	6	6	4	10	5	Information being compromised.	6.2
	DoS	8	4	6	10	7	Communications become unavailable.	7.0
	Spoofing	8	7	7	10	5	Lost of control of communications.	7.4
	Firmware Exploits	9	8	4	10	4	Manipulation of the device according to exploit.	7.0

Tampering and Eavesdropping are a common type of MitM attacks. These attacks fall under repudiation attacks, information disclosure attacks and tampering attacks from STRIDE categories.

Having a nefarious individual control the connection out of the train can be catastrophic. The information arriving cannot be trusted, CCTV footage is compromised and all the communications are compromised. Being in control of the MT could lead to the internal network of the train's compromise. The information contained in the packets such as origin, addresses and other headers could be enough for an experienced attacker to gain control of the onboard computers. This is a worst-case scenario and difficult to happen with these proportions nowadays.

For MitM, the damage potential would be the highest possible. The reproducibility of an eavesdropping attack is high but that of an actively tampering situation is low. The exploitability of eavesdropping is high and tampering is low. The percentage of affected users is medium and the discoverability for eavesdropping and tampering is medium.

The DoS attack was discussed previously as a flooding attack on the router. In this case, it is similar to that one but instead of flooding the router, the MT is the one being overwhelmed with traffic.

It can also just have the purpose of disrupting the train's communications with the outside. If the 5G communications get overwhelmed and the same is done to the backup 4G network, the train would have to communicate using GSM-R leaving itself more exposed to other attacks. It is a very hard attack to defend against. The damage potential of this attack is high, the reproducibility is low, exploitability medium, affected users very high and discoverability is low because the MT even if using radio frequency, is not open to the public and there are multiple channels to find and flood.

As the routers, the MTs can also have vulnerabilities in their firmware. These vulnerabilities can be exploited just like the routers can and the consequences would be similar. Installing back doors, malware, and gaining admin access are all possible depending on the vulnerabilities of the device. There is a big market on the dark web with rootkits and exploits on existing software and hardware that can facilitate these types of attacks.

There is a type of spoofing attack that can be very dangerous to the train. It is called a rogue base station attack and, as the name implies, it consists of an attacker posing as a BS and the train is unaware of this situation. The attack can be as simple as spoofing the BSs ID, and the train, if authentication protocols are not properly configured, will think that the attacker is a BS. This attack can have the same repercussions as a MitM attack. The communications become unreliable, the attacker can have control over the train if he wants. The risk assessment of this attack resembles the risk assessment of an MitM attack with tampering purposes.Attacks performed on the MT on the train can as easily be performed on the train's AP. Because they have such similar functions, the consequences with also be similar.

There are also a few vulnerabilities to the MT and its connections associated with 5G networks. For instance, improper configuration of network slices can leave the system vulnerable. If the train is using a public 5G BS, and there are other slices dedicated to the public there, it is likely for the BS to become a weak link in the network. A couple of of attacks on the BS such as this can be seen in Table 4.5 It would, therefore, compromise the MT, the train and the communications in question. Further issues with 5G security will not be approached here. The premise here is for the attacker to gain access to the network through an infrastructure component. If the network is compromised, the 5G security measure will become redundant.

4.2.3 Gateway Server

The points of access described above, MTs, APs and routers, can be attacked individually. Nevertheless, they can be just a way for the attacker to gain access to a more internal part of the system. For example, in Table 4.3 we see attacks relevant to be studied regarding the GS. The gateway server can be a main objective for someone who targets either the MT or the Router.

Because the GS is located in such a vital part of the internal train network, the damage potential

of it being compromised is massive. Despite the existence of other layers of security inside systems, outgoing and incoming communications would become untrustworthy, even though self-reliant internal service would continue to operate unaffected, as these systems don't need outside inputs to work.

The presented values in Table 4.3 all track back to mostly the same reasons as seen in the former tables. To avoid repetition, and because all attacks on the GS have to come from another element, there will not be a deep dive into the values for this table. This will also be the case for the next components to not have too dense of a text.

Table 4.3: Gateway Server Vulnerabilities.

Device	Attack	D	R	E	A	D	Consequences	RAA
GS	Elevation of privilege	8	7	2	10	7	Access to trains internal network.	6.8
	DoS	10	4	7	10	7	Communications come to a stop.	7.6
	Malware injection	10	7	2	10	7	GS becomes compromised.	7.2

4.2.4 Ruggedized Switch

The RS is a simple piece of equipment connected to the GS. There are 2 RSs to consider, the non-critical, and the critical. If the critical RS is compromised, the attacker would be able to remotely control the train. To access the RSs an attacker would have to penetrate 3 devices in total, either the MT or the Router, the GS and then the RS. Added up, it is an expensive and complicated process for an attacker to break all devices. Later on, this is taken into consideration, for a more simplistic analysis, Table 4.4 considers that the GS is already compromised and not take into account the costly work of compromising it, or the points of access. If the GS can mask that it has been compromised, the attacker would not need to control the RS directly for the device to do its bidding. Firmware exploits can lead to unwanted elevations of privilege by the attacker.

Table 4.4: Ruggedized Switch Vulnerabilities.

Device	Attack	D	R	E	A	D	Consequences	RAA
RS	Flooding	6	7	7	1	5	RS shutdown or reset.	5.2
	Spoofing	10	7	3	1	5	RS controlled by compromised GS .	5.2
	Firmware Exploits	10	7	3	1	5	Manipulation of RS according to exploit.	5.2

The NMS is a crucial part of the defence of the devices onboard the train. It monitors and maintains

the devices. If it were to be compromised, it would not itself give the attackers access or control over the communications, but it would escalate the possible attacks to other elements.

Because this is the last line of defence between the exterior, and self-reliant internal services, a simple switch is not enough to secure this connection. Controlling the train is the ultimate service that needs protection and should be secure at all costs.

4.2.5 Base Station

The base station is where all communications from trains around the railway are first received and then forwarded to the control centre. For this reason, it is an extremely important link in the network. Also, as discussed, it relies on radio frequencies to communicate with the train and therefore it is a possible point of access for an attacker to be listening in or performing malicious attacks.

In order to not extend a lot the components analysis, just like the GS, there is no deep dive into this component as well. In the coming Section 4.3, attacks on services are mainly focused on communications between MT and BS. In those descriptions, the values on Table 4.5, which represents the values of a DREAD analysis to the BS, can be better understood. Furthermore, the attacks on the table do not fall outside those already previously mentioned in this chapter, so consulting the previous explanations can also be enlightening about the tables values.

Table 4.5: Base Station Vulnerabilities.

Device	Attack	D	R	E	A	D	Consequences	RAA
Base Station	Access control	6	6	3	10	9	Communications are unreliable.	6.8
	Tampering	10	7	4	10	4	Attacker has control over all communications to and from the train.	7.0
	Spoofing	9	8	6	10	5	Attacker can impersonate a base station or a train.	7.6
	DoS	7	3	4	10	10	Communications are interrupted.	6.8

4.2.6 Segregated versus Non segregated

To segregate a network into a few others is a decision made by each company based on how they want to manage their network. This choice impacts on costs of configuration and monitoring, changes the attack surface and overall can increase the system's protection.

There are two ways to split a network, physically and logically. Physical segregation means having

different infrastructures for each network and logical means the networks can share resources but the resources are logically split into two non-communicating parts. Simply put one is the separation of hardware and the other is the separation of software. From a cyber security approach, a segregated network is generally considered more secure. The isolation provided helps mitigate the risk of data breaches, malware propagation, and unauthorised access. Even if one part is compromised, attackers find it harder to pivot across the network, buying valuable time for security measures to detect and contain threats. However, implementing and managing a network as such can be more complex and require careful planning to avoid hindering legitimate communication and hindering user productivity. Proper segregation requires a deep understanding of an organisation's assets and their interconnections. Providing a flat network is cheaper and easier to manage and implement. Communication among systems becomes much easier as well as resource sharing. Managing the network security is centralised and becomes easier to monitor the network from one system. Even though it has its benefits, a segregated network will always offer a type of security intrinsic to the architecture that cannot be replaced by monitoring or algorithms.

The architectures presented in Section 3.2 show segregation between passenger services and train controls and communications. This segregation can be either physical or logical being the first option the most secure and expensive. There is also the alternative of separating the critical systems from the non-critical systems with a logical separation to ensure total isolation for the train's command and control communications. The segregation can also be total or partial. For example, the channels can merge at some point during the connection on a BS or entering the CC. Partial is not as safe as total and for that reason, the segregation presented in Figure 3.2 can be seen as well in the CC in Figure 3.3. This shows that there are no points of contact between those communications. This however poses a problem in case the systems from the train control need to access some of the passenger's information. This resource-sharing bridge would have to be well configured otherwise the security gained by segregating the network would be weakened.

4.3 Services analysis

To provide a broader analysis, the incoming attacks can also be analysed from the perspective of the services rather than the components. The services under analysis will be:

- VoIP.
- Control and Signalling.
- Data.
- CCTV.
- Messaging.

The services make use of all components and different infrastructures of the network. This provides a better security analysis of the communications flow rather than individual points of access. It helps to identify vulnerabilities unrelated to components as well. In the following analysis, the assumption that the network has very few security protocols in place will be made. Therefore, the starting point is that the attacker has already some access to the train's network. Those vulnerabilities are approached later on. Because all communications are similar, it may seem strange to analyse each service individually. The important aspect to notice is the different impact which similar attacks have on different services

4.3.1 Control and Signalling

The next service is the most critical of the entire infrastructure. Control and Signalling attacks have the power to crash and derail trains, so extra care is required. The DREAD analysis of this service is present in Table 4.6.

Table 4.6: Control and Signalling Vulnerabilities.

Service	Attack	D	R	E	A	D	Consequences	RAA
Control and Signalling	Eavesdropping	3	9	4	1	3	Communications are exposed.	4.0
	Tampering	10	6	4	10	8	Communications can be manipulated.	7.6
	Repudiation	10	5	2	10	4	Communications source is unknown.	6.2
	DoS	9	4	4	10	10	Communications are interrupted.	7.4
	Spoofing	10	7	5	10	9	Communications source is not CC.	8.2

The first attack someone can perform is eavesdropping. If someone has the ability to listen in on communications containing navigation instructions for the train there is little they can do with that information. They can maybe use the communications metadata to perform other attacks such as replicating commands but this attack itself is not very dangerous. It is more of a gateway attack. The damage potential is low, reproducibility and exploitability are high and low, affected users are low because just seeing the commands affects no one by itself and the discoverability is still high but because it is in a more isolated part of the system, not as many information available will apply to this case.

A tampering attack has a very high damage potential. It is not relevant how the attacker is able to perform it, if he is able to tamper with the control and signalling instructions it is extremely dangerous. This attack's reproducibility is going to be average tending to high because for this type of attack, the hard part is usually the setting up, once you are able to perform it once it should be easy to replicate.

However, all communications have variable circumstances to which the attack will have to adapt and thus the reproducibility will not be extremely high. This is not a very easy attack to perform and even exploring a vulnerability would require some network and communications knowledge. Also, some sort of relay to the messages either in the middle, source or destination is required and that consumes time. Therefore, the exploitability of this attack will be considered low. The affected users are all people on board the train. This attack's discoverability will be rated as high. There can be a lot of information on tampering attacks, an attacker would not have to search very much to find reliable and effective tools. However, if the network employs recent defence mechanisms, most tools will be ineffective.

Spoofing attacks are just as dangerous as tampering. If in a tampering attack the information needed to be changed, in this attack, only the information about who is sending needs to be changed. Damage potential is extremely high. If credentials are compromised or the attacker can mask the origin to match the CC then it has high reproducibility. It requires effort but not as much as tampering so the exploitability is higher. The affected users once again would be everyone on the train and the discoverability is quite high as well.

Being able to perform prohibited operations on the train's connection to the CC has a high damage potential, repudiation is an attack in which the reproducibility would be low and the exploitability would be very low. The affected users would the entire train and the discoverability is also low.

As mentioned, these are very critical communications. Therefore, if they are not able to get through, then the train will either be forced to stop or something worse. Thus, the damage potential of DoS is deemed as high. It is a hard attack to reproduce, it involves a lot of computer power and so its reproducibility will be on the low end. In terms of exploitability, it is going to be on the low side as well because it requires a lot of effort. The affected users will consist of the entire train. There is a high discoverability for this type of attack and on a standard network, the information available would most likely be efficient.

4.3.2 Voice over IP

Voice over IP is both in the critical and non-critical batch of services. There are several attacks that could be performed from the STRIDE threat list and a few ways those attacks could be performed. The DREAD analysis of this service can be seen in Table 4.7.

The first attack is Eavesdropping which can be seen as a form of information disclosure. An attacker listening in on voice communications can gain access to information which can be leveraged to perform a bigger attack. An eavesdropping attack where passwords, IPs, and privileged information are shared can lead to spoofing attacks and attacks in the access control domain. The damage potential of this attack is low because the information gained is not harmful itself, only if it is used. It is most likely

that critical information will not be conveyed over the phone in trivial conversations (non-critical) or in emergency conversations. If the attacker is inside the communications channel and the session IDs do not change frequently or the attacker has a way to decipher which session IDs they are using then the attack's reproducibility is very high. It is easy to perform this attack on a network with low levels of security. Since that is the starting point of this analysis the amount of effort to perform this attack is very low translating into a high exploitability. The affected users will consist of all the people involved in this communication therefore a small amount. This is a very common attack and with minimal protection it will be very easy to find information on how to listen in on a communications channel.

Spoofing, in contrast with eavesdropping, can have serious damage potential. For example, someone posing as a control centre orders the train conductor to speed up or perform an emergency stop. It can also go both ways, an attacker posing as a train conductor provides false information to the CC which then overrides the navigation computers and gives control and signalling information that will crash the train. If the attacker has the information needed to impersonate someone else, if those credentials are not often changed, then the reproducibility is high. The exploitability however will be average once credentials of the sort are closely guarded, and the effort to make a communication appear to come from another place will vary on the system. The affected users could be from just the train staff to all the passengers and therefore it is average. The discoverability of a vulnerability leading to a spoofing attack is average tending to be high because there is information about impersonating someone by masking headers or eavesdropping communications for credentials.

With the denial of the voice service, neither critical nor non-critical channels are available. The damage potential is average because in the best-case scenario, the train stops and the passengers are delayed indefinitely, and in the worst-case scenario there is an emergency on board which cannot be communicated. Either way, the train should be able to proceed because the control and signalling communications are still up and running. The attack's reproducibility and exploitability are average and low because if there is a way to flood the communications it can be done over and over again until the security problem is resolved. Creating a way to flood those communications can be very hard. However, to flood an entire channel is an expensive job, so it takes time and therefore it is not very easy

Table 4.7: VoIP Vulnerabilities.

Service	Attack	D	R	E	A	D	Consequences	RAA
VoIP	Eavesdropping	1	9	9	1	9	Information gets exposed.	5.8
	Spoofing	10	9	4	5	7	Bad information is transmitted.	7.0
	DoS	5	6	3	3	6	Communications are interrupted.	5.2

to reproduce. The number of affected users is also not high, only the communication operators or a passenger with an emergency will be affected.

4.3.3 CCTV

CCTV services can be considered either non-critical or critical, that choice falls into the company implementing it and therefore the assumption is that the service is critical. Its DREAD table is seen in Table 4.8. Further on, explanations will be shorter or non existing to avoid repeating what has already been said.

There is not a lot of damage someone can cause by spying on a camera feed of the train cars. Because the passenger's privacy is not a priority, this attack has little impact on the train. Like other on other services, gaining access to the service can be used in other attacks, but itself alone, has very little damage potential. The reproducibility is high, it does not require much effort to replicate the attack, however, it is not that easy to exploit a vulnerability which leads to CCTV feed interception nor it is easy to find an exploit that allows that so exploitability and discoverability are reduced. The affected users are the passengers who represent the majority of the train but because passenger privacy is not very relevant the value will be low.

Table 4.8: CCTV service Vulnerabilities.

Service	Attack	D	R	E	A	D	Consequences	RAA
CCTV	Eavesdropping	3	9	4	2	3	Communications become exposed.	4.2
	Tampering	6	9	5	6	3	Communications can be manipulated.	5.8
	DoS	7	3	7	5	9	Communications are interrupted.	6.2

Tampering and DoS attacks can be more damaging than eavesdropping. Whereas in an eavesdropping attack, the CC continues to have access to the camera feeds, in these attacks the video is either interrupted or corrupted and the people in charge of monitoring cannot report any security hazards. For example, if a window gets broken and the security CCTV is offline or non-responsive, it could prove to be dangerous for the people in the car and even for the train. Therefore the damage potential for a DoS and tampering attack is high. For a tampering attack, the reproducibility is high and exploitability is average. For the DoS, the values for these attributes are inverted. The affected users are the same for both, the average and the discoverability will be low and high for tampering and DoS respectively.

4.3.4 Data

The data service is not a very critical one. It can be used as a transition point to other services or a starting point for another attack, but it is not a very damaging one by itself. The communications of the different services are similar in many ways and therefore many of the attacks are similar as well. The values that vary with the services will be the damage potential and the affected users. Because a data service is similar to a voice service in the sense that people are on both ends of the communication and are exchanging information using a similar channel, the analysis is going to be very similar. The DREAD table for this service can be seen in Table 4.9.

Table 4.9: Data service Vulnerabilities.

Service	Attack	D	R	E	A	D	Consequences	RAA
Data	Eavesdropping	1	9	9	1	9	Communications become exposed.	5.8
	Spoofing	10	9	4	5	7	Communications source is not CC.	7.0
	Repudiation	4	5	2	4	4	Communication's source is unknown.	3.8
	Tampering	4	6	4	4	8	Communications can be manipulated.	5.2
	DoS	5	6	3	3	6	Communications are interrupted.	5.2

The damage potential of an eavesdropping attack on a data service is the same as for a voice service for the same reasons. All the values remain the same as the VoIP service. The values for a spoofing and DoS attack are equal to the VoIP for the same reasons but applied to data exchange.

There is no possibility of a tampering or repudiation attack on a voice service. However, the repudiation values on an attack like this will be similar to the Control and Signalling except for the damage potential and affected users, which will be lower. The same goes for a tampering attack.

4.3.5 Messaging

The analysis of the messaging service is the same as for the data service and the associated DREAD table is Table 4.10.

Table 4.10: Message Service Vulnerabilities.

Service	Attack	D	R	E	A	D	Consequences	RAA
Messages	Eavesdropping	1	9	9	1	9	Communications become exposed.	5.8
	Spoofing	10	9	4	5	7	Communications source is not CC.	7.0
	Tampering	4	6	4	4	8	Communications can be manipulated.	5.2
	DoS	5	6	3	3	6	Communications are interrupted.	5.2

4.4 Threats Mitigation

4.4.1 Initial Considerations

After performing the risk analysis and asserting which threats are the most dangerous, comes the need to discuss how to deal with those threats. An attack originates from a vulnerability in the system. The vulnerability can be something varying from a person, to a bad configuration of a database. The trade-off between what a company is willing to spend and the level of security it aims to acquire is very important. The key is to have a good balance between the two.

There are several vectors of approach when dealing with network security. The architecture should be constructed incorporating security by design. This means that the architecture is though with the systems security in mind implementing things such as a good amount of isolation between components. The more isolation between components, the higher the cost. It is vital to understand that not all vulnerabilities are worth preventing as that would require a tremendous amount of money and resources. Sometimes, it can be better to recover from an attack rather than wasting resources trying to prevent it. These protection measures (isolation and good architecture) are fundamental however, they are insufficient. Other measures such as firewalls, encryption and others need to be put in place to prevent more specific attacks and problems.

There are some vulnerabilities which are out of the scope of this analysis such as an attacker having physical access to the network, like an attacker being plugged in a switch. Other cases such as social engineering attacks will not be addressed as well. These are detailed in the assumptions made at the beginning of this Chapter.

For this analysis, it is also important to distinguish between compromising a service and compromising a component. As seen in the previous section, these two received separate risk analyses and therefore, despite being related to each other, will receive different mitigation analyses and different trees

of threats. Compromising a component would mean that the attacker now has control over a part of the network, big or small, which is harder to accomplish in theory than performing an attack on a service. An attack on a service can be launched from a compromised component, hence the risk analysis being related, but it can also be done independently, or from a temporarily compromised component.

The network at hand is a closed and private network. There is no contact with so-called public internet other than for passengers. This means public internet service providers will not be used. The train communications are segregated from the passengers. There are, however, ways to tap into the frequencies using specialised equipment, ways to listen in on channels and install malware, even in a private and closed network. Those cases are the ones being dealt with in this Chapter.

To aid in the mitigation process, a few trees of threats were elaborated and can be seen in Figures 4.2, 4.4 and 4.3. These figures are analysed in the next paragraphs.

4.4.2 Mitigating Component vulnerabilities

There are several components in this private 5G network. All of them are vulnerable as discussed in the previous sections. This section is dedicated to mitigating prominent ways in which one of those network nodes could be compromised. These issues could vary from human error to 5G exploits that have not yet been addressed in a totally effective way and are depicted in the tree of threats in Figure 4.2.

First up is IMSI cracking. 5G IMSI cracking refers to the illicit process of intercepting and deciphering International Mobile Subscriber Identity (IMSI) numbers within a 5G network. The IMSI is a unique identifier associated with a subscriber's SIM card and is crucial for establishing communication between a mobile device and the network.

The ramifications of 5G International Mobile Subscriber Identity (IMSI) cracking are vast. Firstly, it enables malicious actors to track users' movements and gather sensitive location data. Secondly, it can facilitate various cyberattacks, including man-in-the-middle attacks and SIM swapping, thereby putting the train's MTs at risk of being impersonated by an attacker. Moreover, IMSI cracking undermines the security and integrity of the network itself, potentially leading to service disruptions and data breaches. This could lead to the potential infiltration, replication or replacement of one of the 5G nodes in our network such as MTs or BSs.

To safeguard against 5G IMSI cracking, the implementation of strong encryption protocols for communication between mobile devices and the network is needed. Employ algorithms like AKA to protect IMSI transmission. Also, companies could use Two-Factor Authentication (2FA) and biometric authentication methods to add an extra layer of security during user authentication processes to aid in the process.

5G Packet Reflection Vulnerability is a security flaw that enables malicious actors to manipulate and

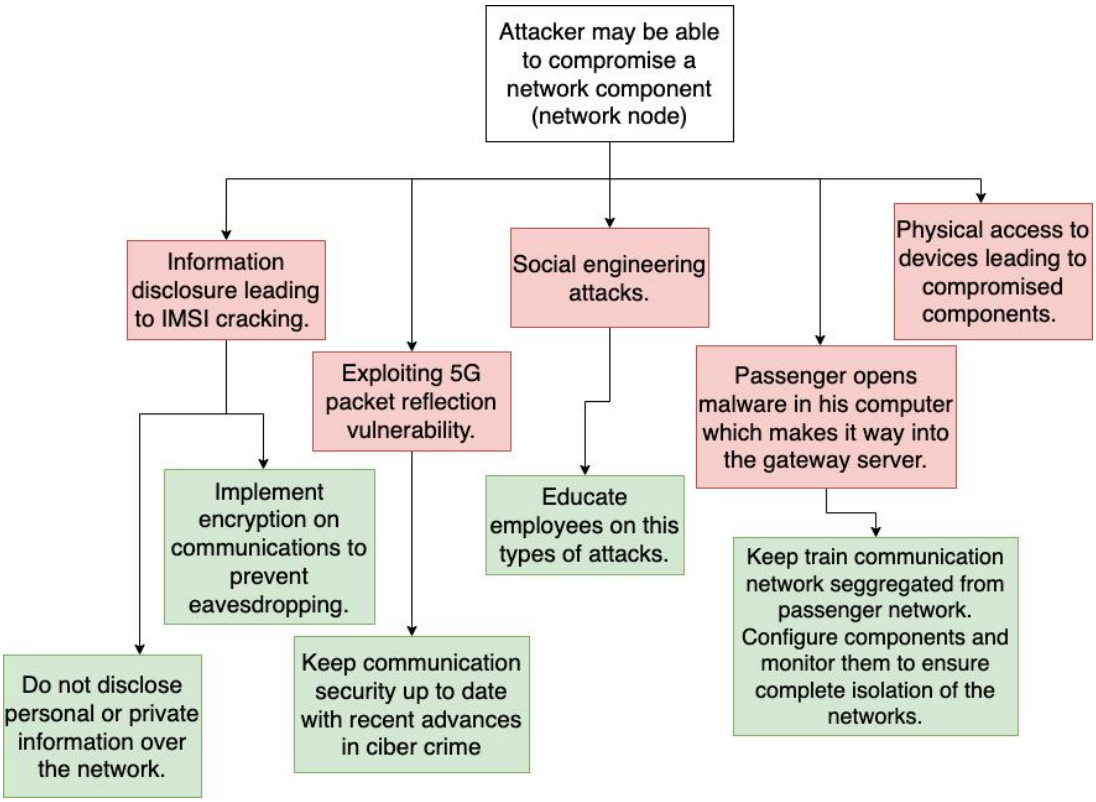

Figure 4.2: Network Component's Tree of Threats.

redirect data packets within a 5G network. These attackers can intercept legitimate data packets, alter their destination, and redirect them to unintended recipients. In essence, it creates an avenue for data interception, manipulation, and potential exploitation within the 5G ecosystem.

This vulnerability opens up many doors, especially for man-in-the-middle activity enabling eavesdropping and other malicious attacks. It can allow data tampering, permitting attackers to modify information in transit, leading to misinformation or service disruption. It can be used to install malware into any node of the network.

Known measures that can prevent this are of course the implementation of end-to-end encryption to protect data packets from interception and tampering. Encryption keys should be securely managed to prevent unauthorized access. Employ DPI techniques to scrutinize data packets for anomalies and malicious patterns before they reach any important component. This allows for the identification and isolation of suspicious traffic. Also, an Intrusion Detection System (IDS) can help clean any malicious code that was able to reach the network.

As has been previously mentioned, social engineering attacks are not in the scope of this thesis, however, the simplest and easiest way to deal with these sorts of situations is to educate the employees on the matter.

The train's architecture offers a level of segregation between passenger and train communications. This allows for a less exposed attack surface on the most important communications channels. There is, nevertheless, the possibility of this segregation being flawed for any number of reasons such as bad configuration, hardware malfunction or new exploits being released. When disparate parts of an organisation's network are not properly isolated, it becomes easier for attackers to move laterally across the network once they gain access to a channel, for example, the passenger's communications channel.

The consequences of poor network segregation manifest in several ways. One of those ways is the exposure of network components to users with nefarious intentions. There are other consequences such as critical systems may be exposed to unnecessary network traffic, increasing the attack surface and leaving them susceptible to exploitation. However, the focus is currently on the compromise of the network nodes, not channels.

For these reasons, it is important to prevent these scenarios where segregation is not one hundred per cent effective. To do so, there are a couple of measures that can be enforced such as

- Enforce strict access controls and role-based permissions to ensure that users and devices can only access the network resources necessary for their roles.
- Continuously monitor network traffic to detect anomalous or unauthorised activities. IDSs and security information and event management solutions can help identify potential security breaches.
- Conduct regular network audits to ensure that network segmentation remains effective and that any changes to the network are appropriately secured.

Just as social engineering attacks, physical access to components is out of the scope of the project. The easiest way to address the issue is physically securing the nodes with padlocks and monitoring them with CCTV.

4.4.3 Mitigating service vulnerabilities

There are a few types of attacks that can be very damaging to the services described in section 4.3. Each of those types of attacks can be fulfilled in different ways as will be described. The Tree of Threats in Figure 4.3 shows a few ways some attacks can be performed.

Spoofing attacks constitute a formidable weapon in cybercrime, posing significant threats to the integrity and security of digital systems. These attacks leverage various techniques to achieve their nefarious goals, often involving the manipulation of source addresses or identifiers. Amongst these techniques there are some more persistent and effective:

- Boosted by an eavesdropping attack, the malefactor can gain access to sensitive data that can be used to perform spoofing attacks.
- In spoofing attacks targeting information disclosure, attackers forge the source of communication

Figure 4.3: Spoofing and Tampering Tree of Threats.

to gain unauthorised access to sensitive data. This can include masquerading as a trusted entity to trick users or systems into divulging credentials, personal information, or proprietary data. The sensitive data can then be used to impersonate someone and this way trick systems or users into opening malicious content.

- Bad packet filtering spoofing involves the manipulation of packet headers to bypass security filters or firewalls. Attackers may alter source IP addresses to circumvent network security measures, thereby gaining unauthorised access to systems or initiating malicious activities undetected. Packet spoofing can be relatively straightforward or quite complex.
- Firmware spoofing entails the tampering of device firmware to impersonate legitimate devices. Attackers can exploit vulnerabilities in firmware to replace legitimate firmware with malicious versions, allowing them to assume control over the device and execute various malicious actions, often without the user's knowledge.

Just like Spoofing, Tampering is a big potential risk to the railroad infrastructure. Some ways spoofing attacks can be executed can be seen in Figure 4.3. These are:

- Eavesdropping, or passive interception, is a tampering method where attackers surreptitiously listen in on communication channels to gain access to sensitive information. This information may include session IDs or credentials, allowing attackers to impersonate legitimate users or escalate their privileges.
- Tampering attacks can involve overloading network resources to disrupt their normal functioning. By saturating a network with excessive traffic or requests, attackers can lower its defences, creating opportunities for further exploitation.
- Weak or flawed authentication protocols can pave the way for man-in-the-middle attacks. In these scenarios, attackers position themselves between legitimate parties, intercepting and potentially altering data in transit. This type of tampering can lead to data manipulation or unauthorised access.

Mitigating against spoofing and tampering attacks can be mostly performed by employing the same mitigation techniques.

An effective way to protect a communication channel is to deploy an end-to-end Transport Layer Security / Secure Sockets Layer (TLS/SSL) channel in the network. TLS and SSL are cryptographic protocols that provide secure communication over networks by encrypting data transmissions between a client and a server. A TLS/SSL channel establishes a secure, encrypted connection that ensures data integrity, confidentiality, and authenticity during transmission. TLS/SSL requires both the client and server to authenticate each other before establishing a connection. In a private network, this authentication ensures that devices within the network are genuine and not subject to spoofing. TLS/SSL encrypts data exchanged between devices, rendering it unintelligible to malicious actors attempting to intercept

or manipulate data packets. This encryption safeguards against eavesdropping and data tampering, common tactics in spoofing attacks. By using digital certificates, TLS/SSL enables devices within the network to verify the authenticity of other devices.

TLS/SSL channels fortify private networks against spoofing attacks by mitigating the risks associated with impersonation, data interception, and unauthorised access. The use of cryptographic protocols and digital certificates ensures that communication within the network is secure and authenticated.

Similar to TLS/SSL channels is a VPN. It protects the communication as well providing a few extra features. VPNs are cryptographic technologies that establish secure and encrypted communication channels over untrusted or public networks, such as the Internet. These channels, often referred to as tunnels, serve as virtual conduits for data transmission, safeguarding it against eavesdropping, interception, and manipulation. A VPN creates a virtual tunnel making it virtually impossible to access the content of the transmissions inside the tunnel without access to the VPN servers. In closed private networks, VPNs can be seamlessly integrated to fortify the network's security:

- VPNs enable secure communication between remote users, devices, or branch offices and the closed private network. All data traffic passing through the VPN tunnel is encrypted, ensuring data confidentiality and integrity.
- VPNs require authentication before granting access to the closed private network. Users and devices must authenticate themselves, ensuring that only authorised entities can establish a connection.
- VPNs create an isolated and segmented environment within the larger network. This segmentation restricts the visibility of network resources to external entities, reducing the attack surface for potential adversaries.
- VPNs employ cryptographic techniques to verify data integrity, making it extremely difficult for attackers to tamper with data in transit without detection.

The inclusion of VPNs within closed private networks yields several notable advantages in mitigating spoofing and tampering attacks:

- VPNs encrypt data traffic, thwarting eavesdropping attempts. Even if attackers intercept data, it remains encrypted and indecipherable.
- VPNs enhance authentication mechanisms, reducing the risk of credential spoofing attacks. Users and devices must undergo robust authentication processes before gaining access.
- By ensuring data integrity, VPNs deter tampering attacks. Any unauthorized modifications to data during transit are detected and rejected.
- VPNs isolate the closed private network from the external, untrusted network, reducing the risk of spoofing attempts and limiting potential attack vectors.

Usually, VPNs are a service provided by a company looking to protect your communications. This way, the railway company is placing a lot of trust in the VPN provider. However, this risk can be mitigated if the company decides to implement the VPN themselves. It is a more expensive option, however not outsourcing this kind of service would provide extra security.

Firewalls are security devices or software applications that serve as the first line of defence in protecting a network from unauthorised access, malicious traffic, and cyber threats. They operate by inspecting and controlling incoming and outgoing network traffic based on a set of predefined security rules.

In closed private networks, firewalls can be thoughtfully integrated to enhance security:

- Firewalls enforce access control policies, allowing or denying network traffic based on defined rules. This restricts unauthorised access and filters out potentially malicious traffic.
- Firewalls inspect packets and data flows, scrutinising them for anomalies or known attack patterns. This enables the detection and prevention of suspicious activities, including spoofing and tampering attempts.
- Firewalls can segment the network into security zones, creating barriers that limit the lateral movement of attackers within the network. This containment strategy reduces the impact of successful spoofing or tampering attacks.
- Advanced firewalls often include deep packet inspection (DPI) capabilities, allowing them to inspect traffic at the application layer. This provides more granular control and protection against sophisticated attacks.

While both advanced and basic firewalls serve as effective security measures, each approach comes with its own set of advantages and limitations. Advanced firewalls offer more granular control, often including features like intrusion detection and prevention, application-layer filtering, and enhanced threat intelligence integration. They provide robust protection against a wide range of cyber threats. Advanced firewalls are typically more complex to configure and maintain. They may require a higher level of expertise and financial resources. Basic firewalls are easier to set up and manage, making them suitable for smaller organisations or less complex network environments. They still provide essential protection against common threats. Basic firewalls may lack the depth of protection and advanced features found in more sophisticated solutions. They may not be as effective against highly targeted or sophisticated attacks. Through access control, traffic inspection, network segmentation, and application layer filtering, firewalls fortify the network's security posture. While both advanced and basic firewalls offer valuable protection, the choice between them should be based on the organisation's specific needs, resources, and the complexity of the threat landscape

IDS are security mechanisms designed to monitor and analyse network traffic and system activities for signs of suspicious or malicious behaviour. They operate by comparing observed activities to pre-

defined rules or patterns, identifying potential threats and alerting administrators when anomalies are detected. IDS constantly analyse network traffic, inspecting packets and data flows to identify patterns indicative of spoofing or tampering attempts. When suspicious activities are detected, IDS generate alerts or notifications to promptly notify network administrators of potential threats. This facilitates timely responses to mitigate risks. Advanced IDS employ machine learning and behaviour-based analysis to detect previously unseen threats or subtle deviations from normal network behaviour, including zero-day attacks. Some IDS are equipped with the capability to correlate data from multiple sources, providing a holistic view of network activities and enhancing the accuracy of threat detection.

While both advanced and basic IDS offer valuable threat detection capabilities, each approach comes with its own set of advantages and limitations. Advanced IDS typically provide more sophisticated threat detection mechanisms, including behavioural analysis, machine learning, and real-time threat intelligence integration. They offer comprehensive protection against a wide range of known and emerging threats. Advanced IDS solutions may be more complex to configure, manage, and maintain. They often require a higher level of expertise and resources. Basic IDS solutions are typically easier to set up and manage, making them suitable for smaller organisations or less complex network environments. They still provide essential threat detection capabilities. Basic IDS may lack the depth of protection and advanced features found in more sophisticated solutions. They may not be as effective against highly targeted or advanced attacks. IDSs play an indispensable role in safeguarding closed private networks against spoofing and tampering attacks. Through continuous traffic analysis, alert generation, anomaly detection, and correlation capabilities, IDS fortify the network's security posture. The choice between advanced and basic IDS should be based on the organisation's specific needs, resources, and the complexity of the threat landscape.

The act of updating software, firmware, and hardware is not merely a routine maintenance task but a strategic operation aimed at fortifying the network against known and emerging vulnerabilities. Security patches are designed to fix specific vulnerabilities that have been discovered either through internal testing or external reporting. These patches are critical because they close the loopholes that attackers could exploit. For instance, an unpatched router can be susceptible to a Denial of Service (DoS) attack, crippling the entire railway communication network. In this network, a centralised patch management system can be implemented. There is software which can be used to automate the distribution of patches to all network nodes, ensuring uniformity and reducing the risk of a weak link.In the railway communication network, each node—whether it's a control centre, a signal box, or an onboard communication system—can be scheduled for updates during off-peak hours to minimise service disruption. This ensures that all components are uniformly secure, thereby maintaining the integrity of the entire network.

When discussing railway communications, where data integrity and confidentiality are paramount,

encryption stands as an indispensable pillar. It serves not merely as a tool but as a foundational element in the architecture of secure communications within a closed, private network. Encryption algorithms such as AES-256 offer a high level of security, making it computationally infeasible for unauthorised entities to decrypt intercepted data. This is particularly crucial for protecting sensitive operational data, such as train schedules, cargo manifests, and control commands. The absence of strong encryption could expose the system to risks ranging from data theft to catastrophic operational failures, such as derailments or collisions. Given the critical nature of the data being transmitted, encryption at the Transport Layer of the OSI model is highly recommended. TLS, as previously discussed, can be implemented to secure the communication channels. TLS offers several advantages, including mutual authentication, data integrity, and data confidentiality. For instance, OpenSSL can be used to implement TLS, providing both server-side and client-side communication encryption.

In this specific context of a private railway communication network, acsTLS can be used to secure API calls between the centralised control centre and the individual trains. This ensures that operational commands are securely transmitted and authenticated, thereby mitigating the risk of man-in-the-middle attacks. Moreover, the encryption keys can be managed centrally, allowing for quick rekeying in case of suspected key compromise.

Authentication transcends beyond mere identity verification. It serves as a multi-faceted security measure that establishes a trusted relationship among network nodes, thereby forming the bedrock upon which other security measures can be reliably implemented. 2FA involves the use of two independent means of evidence to verify an entity's identity. In a high-stakes operational environment like a railway system, the implementation of 2FA can prevent unauthorised access even if one factor (e.g., a password) is compromised. This is crucial because unauthorised access to control systems could lead to catastrophic outcomes, including loss of life and severe economic impact. For implementing robust 2FA, a server can be deployed in conjunction with hardware tokens. The server would handle the first factor of authentication (something the user knows, like a password), while the hardware token would provide the second factor (something the user has). Technologies like RSA SecurID could be used for this purpose, which generates Time-based One-Time Passwords (TOTP) as the second factor. In the railway communication network, 2FA could be implemented at various levels, including control centre access, machine-to-machine communications, and even emergency override systems. For instance, a train should only obey a stop command from the control centre if the command is authenticated using 2FA, thereby ensuring that the command is legitimate and not a result of a compromised system.

Given the assumptions in this chapter, the likelihood of DoS attacks is relatively limited. However, due to the high stakes involved, especially in critical sectors like railway communications, it's crucial to dedicate a section to mitigation strategies for these types of attacks as they are very common. In Figure 4.4 the different ways to perform the attack are a bit out of the scope of this architecture's assumptions.

Nevertheless, these mitigation measures help deal with potential DoS attacks.

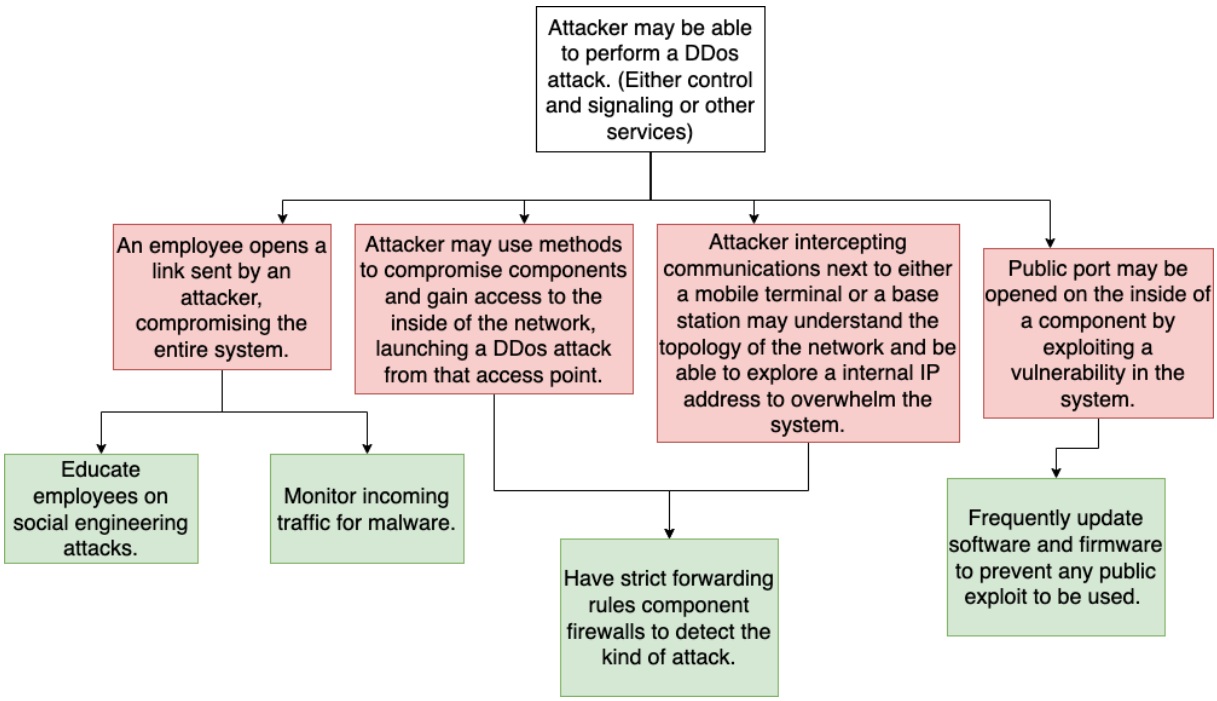

Figure 4.4: Distributed denial of service Tree of Threats.

Rate limiting is a foundational tool that controls the frequency of incoming network requests, serving not just as a gatekeeper but also as a strategic resource allocator. Setting a limit on the number of requests from a single source prevents resource exhaustion and ensures that legitimate traffic isn't overwhelmed by malicious attempts. This is particularly important for interfaces that handle critical control commands in a closed, private railway communication network.

Beyond mere monitoring, intelligent traffic analysis is employed to scrutinise network patterns and differentiate between legitimate and malicious requests. Deep Packet Inspection allows the system to identify abnormal patterns and filter out malicious traffic, preserving network resources for legitimate operations. This serves as a frontline defence mechanism against attacks targeting critical systems.

Infrastructure resilience goes beyond merely having backup systems; it involves creating a robust network architecture that can withstand high-stress scenarios. By deploying redundant resources, the system can continue to function even when some components are compromised. Load balancers distribute incoming traffic across multiple servers, mitigating the impact of an attack while optimising resource utilisation. In the context of a railway network, this means deploying redundant control centres and signalling systems to ensure service continuity under adverse conditions.

Lastly, anomaly-based detection systems add an advanced layer of security by leveraging machine learning to identify deviations from established network behaviour. Continuous monitoring allows these

systems to detect unusual spikes in traffic or irregular access patterns, enabling proactive mitigation measures. This is particularly effective for monitoring data traffic between trains and control centres, as any unusual activity can trigger an immediate investigation and remedial action.

5

Conclusion

Chapter five serves as the culmination of this thesis, synthesising the key findings and insights gained from the comprehensive study of railway communication networks. It not only reflects on the critical aspects explored in previous chapters but also looks forward, discussing the implications of these findings for future developments in the field. This chapter aims to provide a cohesive conclusion, drawing together the research threads to offer a clear perspective on the path ahead in railway communication technology.

Contents

5.1 Main Conclusions

The central issue this thesis addresses is the manifold security vulnerabilities that have emerged with the modernisation of railway communication networks, particularly through the integration of 5G and WiFi technologies. Railways serve as a critical infrastructure, and their secure and efficient operation is of paramount importance. The existing communication systems, which are primarily based on older technologies like GSM-R, have become increasingly inadequate to meet the demands of modern railway operations. The situation is further complicated by the rapid technological advancements in communication networks, which, while offering numerous benefits, also introduce new vulnerabilities. This requires a comprehensive study to identify and mitigate these vulnerabilities.

At the beginning of this project, an exploration of the current landscape in railway communication networks is performed, emphasising the integration of 5G and WiFi technologies. Chapter one lays the groundwork by presenting the background and introducing the core concepts. Chapter two delves deeper into the intricacies of railway communication networks, detailing their evolution and current state. In Chapter three, the focus shifts towards the Network Service Architecture, dissecting its layers and pinpointing potential vulnerabilities like mobile terminals and routers. This chapter is instrumental in identifying the weak points within the system. Chapter four builds upon this by proposing robust mitigation strategies and solutions to address the vulnerabilities identified earlier. Through a detailed analysis and practical approach, this chapter provides a clear road map for enhancing the security and reliability of railway communication networks. Collectively, these chapters offer a holistic understanding of the complexities involved in securing modern railway networks and lay a solid foundation for future advancements in this critical field.

This thesis approach has enabled the identification of key vulnerabilities in various components of the railway communication network, including Network Service Architecture, and Train Network Architecture. For example, the study reveals that routers, gateway servers, and base stations are particularly susceptible to a range of security threats. The research also provides a road map for mitigating some of these vulnerabilities, emphasising the need for a multi-layered security approach. The study also proposes targeted mitigation strategies. These strategies are not just theoretical suggestions but are grounded in some practical considerations. The research also quantifies the risks associated with each identified vulnerability using a DREAD model approach.

The mitigation model used in this thesis helped perform the identification and categorisation of vulnerabilities in railway communication networks with the chance of being used in a more in-depth approach. The model allowed for a structured approach to vulnerability assessment, enabling the prioritisation of threats and allocation of resources more effectively for mitigation efforts. The conclusions drawn from this model aim to give a future company, whose goal is to create a network fitting the thesis

model description, a variety of security measures to employ and help guide them into making the right choices for their network. Chapter four ties the work together explaining which attacks are the most dangerous, why, and a few ways to prevent those attacks. This allows a network designer to evaluate which of the mitigation techniques, which architecture and other network implementation decisions, are best for their system. In Chapter four, the study meticulously explores and addresses the intricate vulnerabilities within the Network Service Architecture and Train Network Architecture of railway communication networks. The chapter highlights that components such as routers, gateway servers, and base stations are especially vulnerable to a spectrum of security threats. By employing a systematic approach, key mitigation strategies are proposed, emphasising the need of a layered security framework. These strategies are not mere theoretical constructs but are anchored in practical applications, designed to effectively counter identified risks. The chapter plays a crucial role in constructing an understanding of the threat landscape, thereby guiding future network designers in making informed decisions on the implementation of robust security measures. This comprehensive analysis underscores the complexity of securing railway communication networks in the era of 5G and WiFi technologies, paving the way for future advancements in network security protocols and practices.

Despite its comprehensive nature, the research has its limitations, which are important to acknowledge for a balanced understanding of its contributions and shortcomings. One of the primary constraints was the limited time available for the study, which restricted the scope of the research to certain aspects of railway communication network security. For instance, the study could not delve into a detailed analysis of WiFi security aspects, focusing more on the 5G network vulnerabilities.

In summary, the thesis serves as a preliminary work in the field of railway communication network security, particularly in the context of modern technologies like 5G and WiFi. It not only identifies key vulnerabilities but also proposes practical solutions for their mitigation. The research aims to contribute to academic discourse and practical applications in railway network security, offering a roadmap for stakeholders in the railway industry. The thesis stands as a way to understand the complexities and challenges of securing modern railway communication networks, and it sets the stage for future research that can build upon its findings to develop even more robust security solutions.

5.2 Future Work

The scope of this thesis was primarily focused on identifying and analysing security vulnerabilities in railway communication networks that incorporate 5G and WiFi technologies. While the research has been comprehensive in its approach, it has also revealed several areas that require further investigation or which were not approached due to other constraints.

One of those areas for future research is a more detailed analysis of WiFi security aspects. The

current study was somewhat limited in this regard, focusing more on the vulnerabilities associated with 5G networks. Given that WiFi is often used in conjunction with 5G in modern railway systems, a separate and more in-depth study on WiFi security is crucial.

Another significant avenue for future work is the exploration of defence mechanisms against physical access to network nodes. The current study operated under the assumption that there would be no physical access to these nodes, but this is an assumption that may not hold in real-world scenarios. Therefore, future research should consider the implications of unauthorised physical access to network components like routers, switches, and servers, and propose hardware-level security measures to mitigate such risks.

The security of the control centre and train stations also presents a fertile ground for further investigation. While the current thesis touched upon these aspects, it did not delve into the specific types of attacks that could be launched against these critical points in the network. Future research could focus on identifying potential attack vectors that could compromise the integrity of the control centre and train stations, and propose countermeasures to defend against them.

Denial of Service (DoS) attacks were another area which could use a more thorough approach. While software-level solutions were discussed, there is a need for a more comprehensive approach that goes beyond software to include hardware and network-level defences. This could involve the development of algorithms that can detect and mitigate DoS attacks in real-time, as well as implementing redundant systems to ensure continued service availability in the event of an attack.

There is also potential to explore relying on public networks using 5G slicing technology rather than creating an infrastructure from scratch. This would entail a different type of approach and would have other network security challenges. It would however be beneficial in a substantial number of aspects.

There was no time in this project for practical measurements and performance checks and that would also be an interesting angle to follow. The effects of different types of security implementations on the performance of a network pose an interesting vector for future approaches.

Lastly, the potential for social engineering attacks should not be overlooked. While technological solutions are essential, the human element remains a significant vulnerability in any security system. Future research could explore the types of social engineering attacks that could be employed to compromise railway communication networks and propose educational and training programs to raise awareness among staff and users.

In summary, while the current thesis provides a robust foundation for understanding the security vulnerabilities in modern railway communication networks, there is a wealth of opportunities for future research. These areas not only extend the scope of the current study but are also critical for developing a comprehensive and multi-faceted approach to securing railway communication networks.

A

Architecture Images

This Annex shows images provided by Thales of projects involving train infrastructure and aims to help the reader understand the foundation of the architectures presented in Chapter 3.

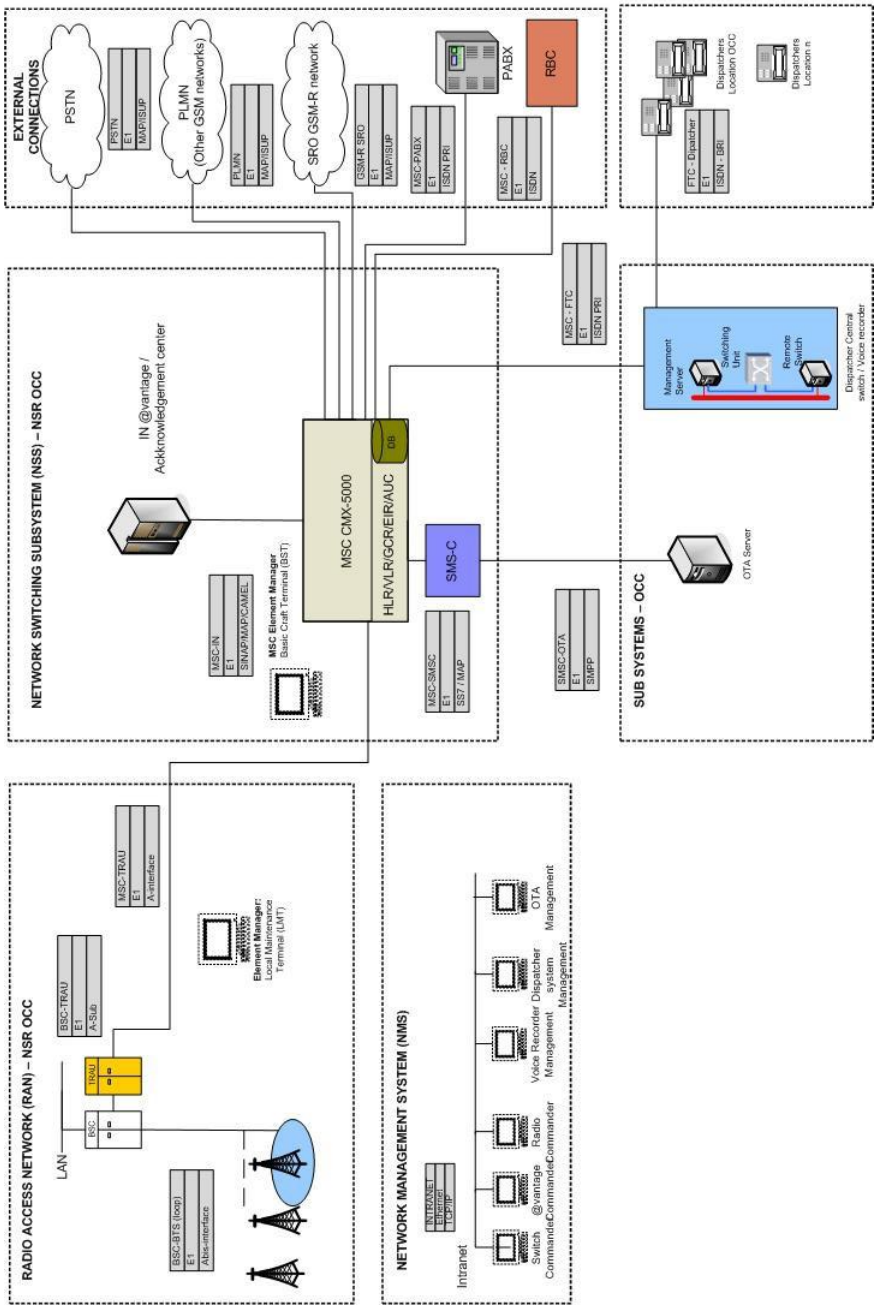

Figure A.1: Thales: Train Network Architecture.

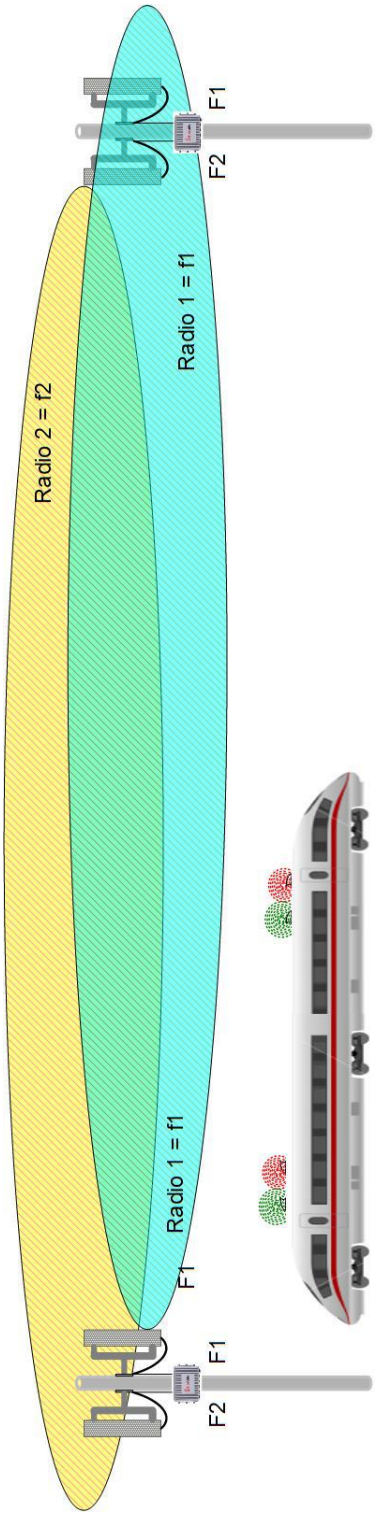

Figure A.2: Thales: WiFi train Architecture.

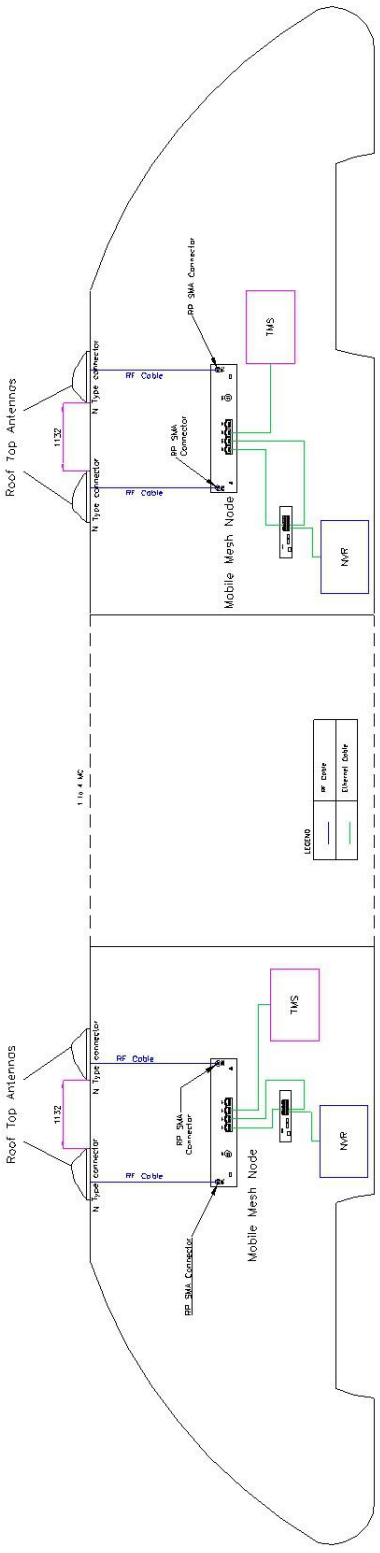

Figure A.3: Thales: WiFi train Architecture, onboard equipment.

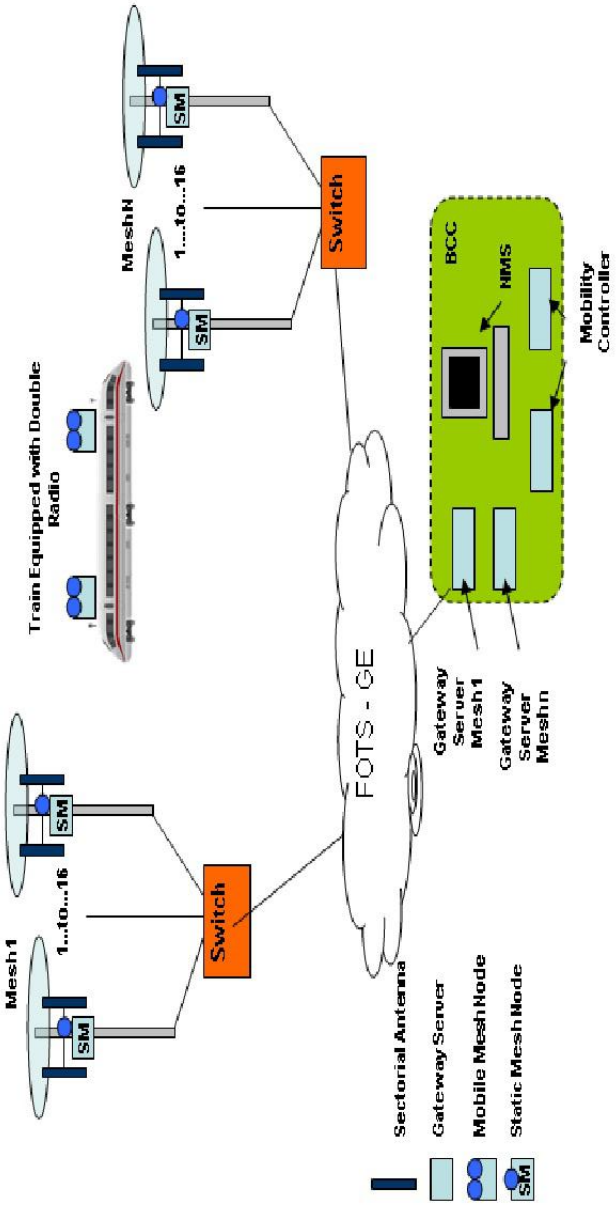

Figure A.4: Thales: General Train Network Architecture, FOTS-GE component.

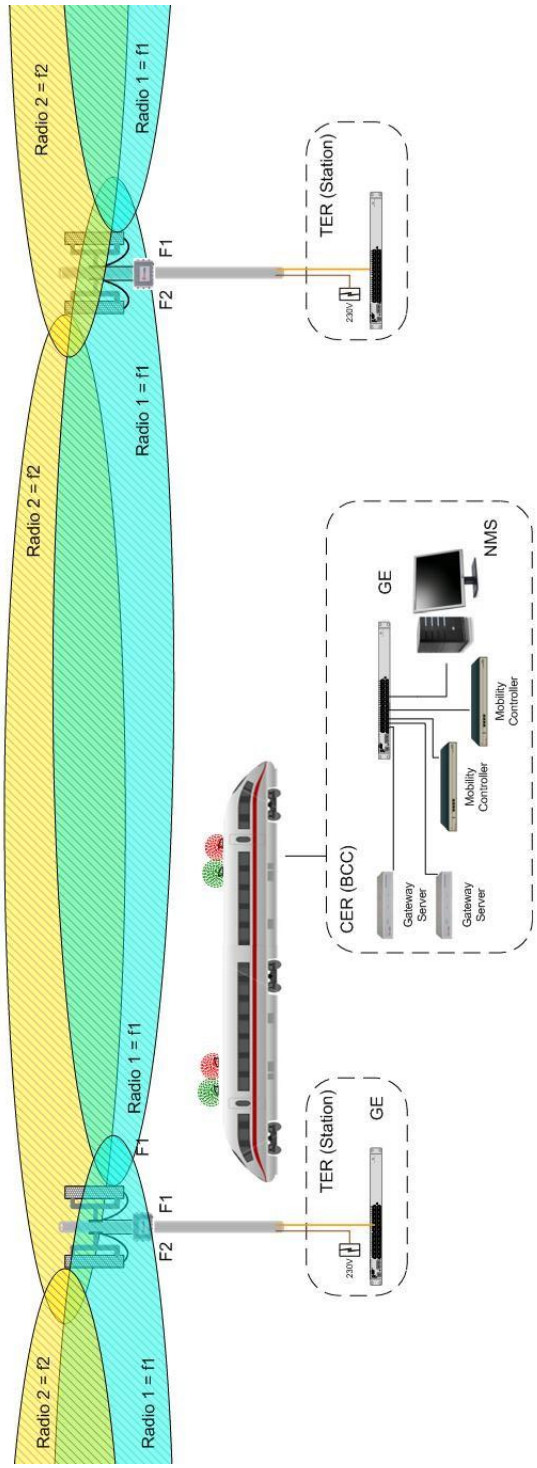

Figure A.5: Thales: Train General Network Components.

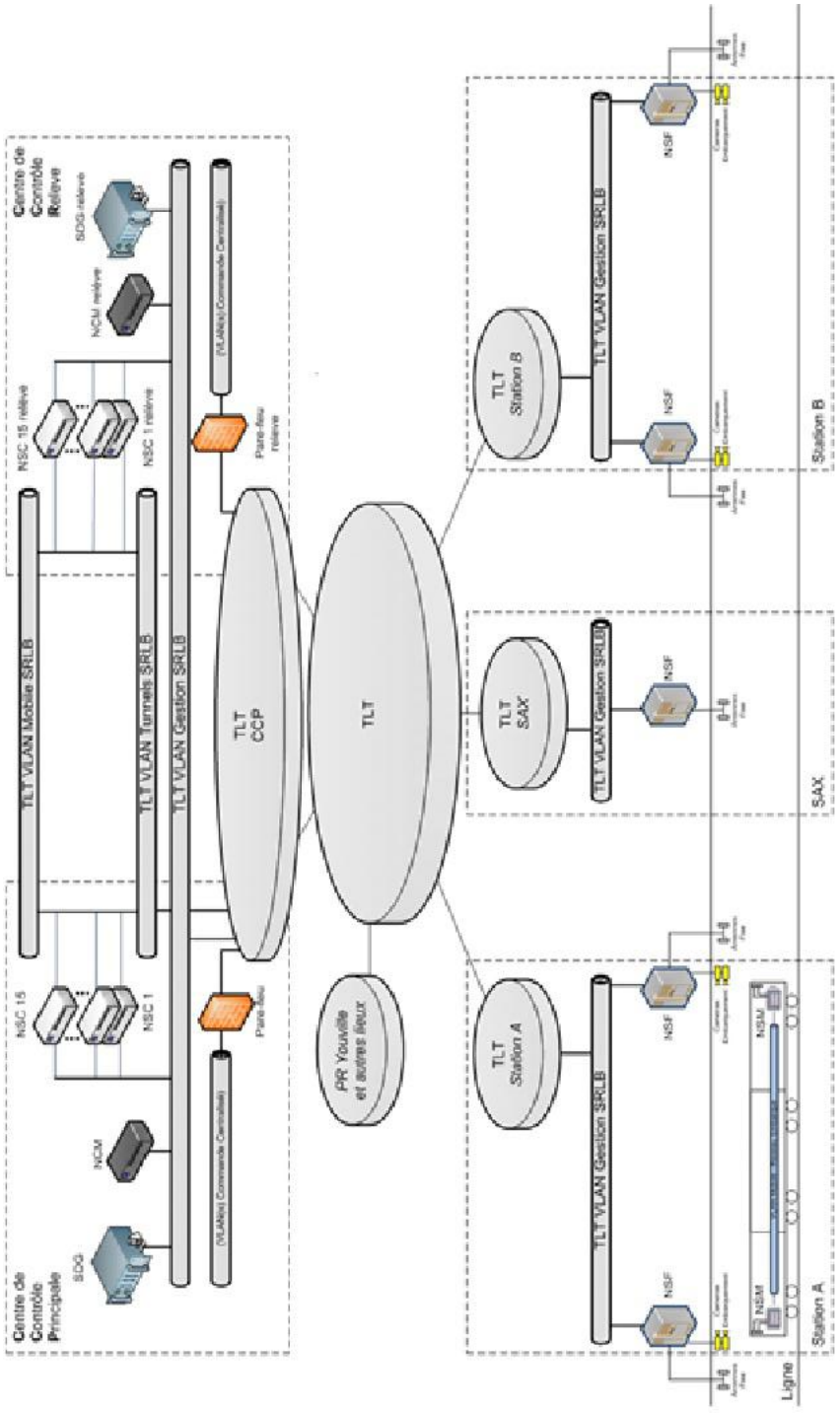

Figure A.6: Thales: High-level Network Description.

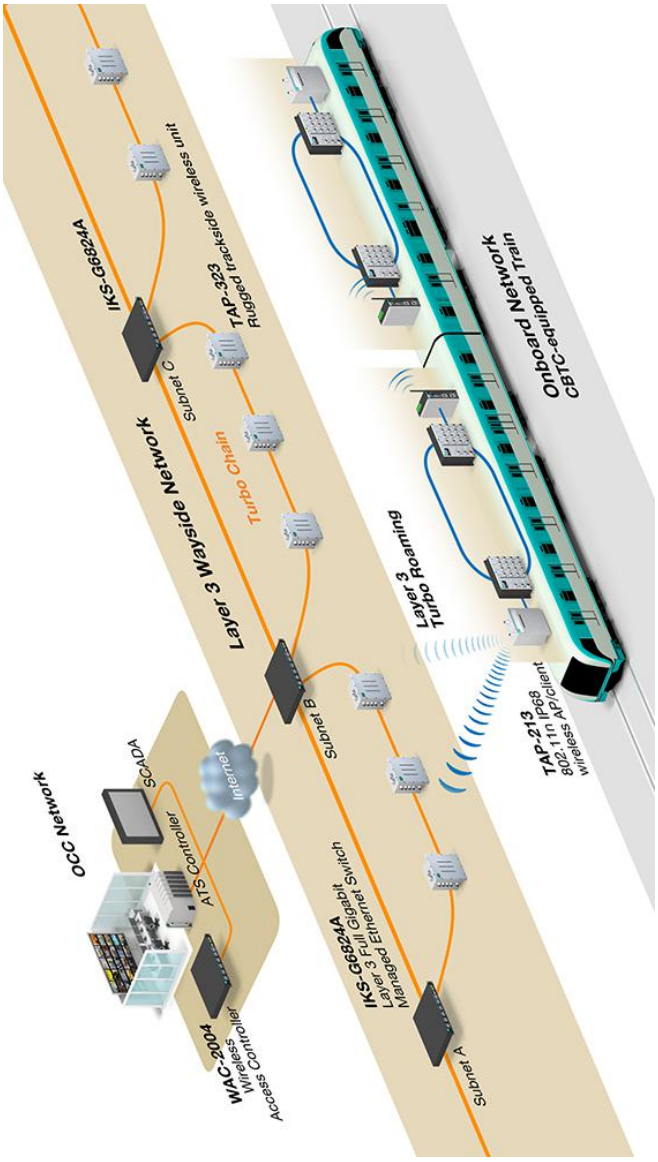

Figure A.7: Thales: Train-Station Network Architecture with static train.

References

[1] Eurostat – Rail Transport of Passengers, https://ec.europa.eu/eurostat/databrowser/view/TTR00015/default/line?lang=en&category=rail.rail_pa, Dec. 2023.

[2] J. F. Kurose and K. W. Ross, *Computer networking : a top-down approach*. Pearson, New Jersey, USA, 2017.

[3] ERTMS/ETCS – The signalling system, www.railwaysignalling.eu, 2013.

[4] R. He, B. Ai, G. Wang, K. Guan, Z. Zhong, A. F. Molisch, C. Briso-Rodriguez, and C. P. Oestges, "High-speed railway communications: From gsm-r to lte-r," *IEEE Vehicular Technology Magazine*, vol. 11, pp. 49–58, 2016, (https://ieeexplore.ieee.org/document/7553613).

[5] STL Partners – What is 5G Network Slicing, https://stlpartners.com/articles/private-cellular/what-is-5g-network-slicing/, Jan. 2017.

[6] E. T. S. Institute, "TS 122 289 - V16.1.0 - LTE; 5G; Mobile communication system for railways (3GPP TS 22.289 version 16.1.0 Release 16)," 2020, (https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx).

[7] European Union Agency for Railways – European Rail Traffic Management System Radio Communication, https://www.era.europa.eu/domains/infrastructure/european-rail-traffic-management-system-ertms/radio-communication_en, 2024.

[8] 3GPP – GSM Specifications, https://www.3gpp.org/specifications-technologies/specifications-by-series/gsm-specifications, 2024.

[9] European Telecommunications Standards Institute – 2G Mobile Technology, https://www.etsi.org/technologies/mobile/2g, 2024.

[10] European Telecommunications Standards Institute – 4G Mobile Technology, https://www.etsi.org/technologies/mobile/4G, 2024.

[11] International Union of Railways – GSM-Railway , https://uic.org/rail-system/gsm-r/, 2024.

[12] E. T. S. Institute, "TR 103 554 - V1.1.1 - Rail Telecommunications (RT); Next Generation Communication System; LTE radio performance simulations and evaluations in rail environment," 2018.

[13] OWASP (Larry Conklin) – Threat Modeling Process, https://owasp.org/www-community/Threat_Modeling_Process, 2024.

[14] W. Stallings, *Network security essentials : applications and standards*. Prentice Hall, Whashingthon, USA, 2011.

[15] E. T. S. Institute, "TS 102 281 - V3.0.0 - Railways Telecommunications (RT); Global System for Mobile communications (GSM); Detailed requirements for GSM operation on Railways," 2016, (https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx).

[16] D. Rupprecht, K. Kohls, T. Holz, and C. Popper, "Breaking lte on layer two," in *Proceedings - IEEE Symposium on Security and Privacy*, vol. 2019-May, San Francisco, USA, 5 May. 2019, pp. 1121–1136.

[17] Y. Wang, W. Zhang, and X. Wang, "A lightweight and secure authentication protocol for space-ground integrated network of railway," in *Proc. of IEEE 3rd International Conference on Communications, Information System and Computer Engineering (CISCE)*, Beijing, China, May. 2021, pp. 30–35.

[18] E. T. S. Institute, "TS 123 501 - V16.6.0 - 5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 16.6.0 Release 16)," 2020, (https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx).

[19] C. Sridevi, "A survey on network security," *Global Journal of Computer Science and Technology*, p. 33–38, Oct. 2017, (https://computerresearch.org/index.php/computer/article/view/1624).

[20] R. Khelf and N. Ghoualmi-Zine, "Ipsec/firewall security policy analysis: A survey," in *2018 International Conference on Signal, Image, Vision and their Applications (SIVA)*, Nov. 2018, pp. 1–7, (https://ieeexplore.ieee.org/document/8660973).

[21] A. Mbiriki, C. Katar, and A. Badreddine, "Improvement of security system level in the cyber-physical systems (cps) architecture," in *Proceeding of 2018 30th International Conference on Microelectronics.*, Sousse, Tunisia, Dec. 2018.

[22] R. Bansode and A. Girdhar, "Common vulnerabilities exposed in vpn – a survey," in *Journal of Physics: Conference Series*, vol. 1714, Jan. 2021.

[23] Y. Wang, G. Yu, W. Shen, and L. Sun, "Deep learning based on byte sample entropy for vpn encrypted traffic identification," in *Proceedings - 2022 5th International Conference on Advanced Electronic Materials, Computers and Software Engineering, AEMCSE 2022*, Wuhan, China, Apr. 2022, pp. 293–296.

[24] A. V. Agrawal and M. Rawat, "Green HSR Reliable Communication With LTE-R Using MIMO-DPD," *IEEE Access*, pp. 105 118–105 130, 2021, (https://ieeexplore.ieee.org/document/9493167).

[25] 3GPP – Documents in 36-series, https://www.3gpp.org/dynareport?code=36-series.htm, 2024.

[26] ETSI – European Telecommunications Standards Institute, https://www.etsi.org/, 2024.

[27] E. T. S. Institute, "TR 103 554 - V1.1.1 - Rail Telecommunications (RT); Next Generation Communication System; LTE radio performance simulations and evaluations in rail environment," 2018.

[28] E. T. S. Institutes, "TS 123 501 - V16.6.0 - 5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 16.6.0 Release 16)," 2018, (https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx).

[29] E. T. S. Institute, "TR 103 768 - V1.1.1 - Rail Telecommunications (RT); Future Rail Mobile Communication System (FRMCS); Interworking study with legacy systems," 2022, (https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx).

[30] B. Ai, A. F. Molisch, M. Rupp, and Z. D. Zhong, "5g key technologies for smart railways," in *Proceedings of the IEEE*, Jun. 2020, pp. 856–893, (https://ieeexplore.ieee.org/document/9103348).

[31] R. He, B. Ai, Z. Zhong, M. Yang, R. Chen, J. Ding, Z. Ma, G. Sun, and C. Liu, "5g for railways: Next generation railway dedicated communications," *IEEE Communications Magazine*, pp. 130–136, 2022, (https://ieeexplore.ieee.org/document/9895381).

[32] A. Gonzalez-Plaza, J. Moreno, I. Val, A. Arriola, P. M. Rodriguez, F. Jimenez, and C. Briso, "5g communications in high speed and metropolitan railways," in *2017 11th European Conference on Antennas and Propagation, EUCAP 2017*, Paris, France, Mar. 2017, pp. 658–660, (https://ieeexplore.ieee.org/document/7928756).

[33] Nokia – Nokia wins Deutsche Bahn tender to deliver and test the world's first 5G-based network for automated rail operation, https://www.nokia.com/about-us/news/releases/2019/12/12/nokia-wins-deutsche-bahn-tender-to-deliver-and-test-the-worlds-first-5g-based-network-for-automated-rail-operation/, Dec. 2019.

[34] Ericsson – InnoTrans 2022, https://www.ericsson.com/en/events/innotrans-2022, 2022.

[35] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys and Tutorials*, vol. 22, pp. 196–248, Jan. 2020.

[36] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A survey on security aspects for 3gpp 5g networks," *IEEE Communications Surveys and Tutorials*, vol. 22, pp. 170–195, Jan. 2020.

[37] M. Kiviharju, C. Lassfolk, S. Rikkonen, and H. Kari, "A cryptographic and key management glance at cybersecurity challenges of the future european railway system," in *International Conference on Cyber Conflict, CYCON*, Tallinn, Estonia, May. 2022, pp. 265–284.

[38] Dynamic Spectrum Alliance – Homepage, http://dynamicspectrumalliance.org/wp-content/uploads/

2019/03/, 2019.

[39] B. Yuan and J. tong da xue, “Icsp2018 : 2018 14th ieee international conference on signal processing proceedings,” in *IEEE International Conference on Signal Processing*, Beijing, China, Aug. 2018.

[40] A. Li, B. Feng, and X. Ding, “A wideband omnidirectional mimo antenna for wifi-6e applications,” in *2022 IEEE 5th International Conference on Electronic Information and Communication Technology, ICEICT 2022*, Hefei, China, 2022, pp. 834–836, (https://ieeexplore.ieee.org/document/9909106).

[41] S. Shin and T. Kwon, “A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5g-integrated internet of things,” *IEEE Access*, pp. 67 555–67 571, 2020.

[42] A. Aji, K. Jain, and P. Krishnan, “A survey of quantum key distribution (qkd) network simulation platforms,” in *Proc. 2nd Global Conference for Advancement in Technology*, Oct. 2021.

[43] X. Cheng, M. C. Sarihan, K.-C. Chang, C. Chen, F. N. C. Wong, and C. W. Wong, “Secure high dimensional quantum key distribution based on wavelength-multiplexed time-bin encoding; secure high dimensional quantum key distribution based on wavelength-multiplexed time-bin encoding,” in *2021 Conference on Lasers and Electro-Optics (CLEO)*, San Jose, CA, USA, May. 2021.

[44] L. Yan, X. Liu, C. Du, and J. Pei, “Research on network attack information acquisition and monitoring method based on artificial intelligence,” in *IEEE Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, Chongqing, China, Jun. 2022, pp. 2129–2132.

[45] X. Wu, J. Xu, W. Huang, and W. Jian, “A new mutual authentication and key agreement protocol in wireless body area network,” in *Proceedings - 2020 IEEE International Conference on Smart Cloud, SmartCloud 2020*, Washington, DC, USA, Nov. 2020, pp. 199–203.

[46] D. Patiyoot, “’patiyoot’ cryptography authentication protocol for computer network,” in *Proceedings of the 2022 International Electrical Engineering Congress, iEECON 2022*, Khon Kaen, Thailand, Mar. 2022.