Net-Zero self-adaptive activation of distributed self-resilient augmented services

D5.1 Physical layer threat modelling

Lead beneficiary	ISRD	**Lead author**	Maria B. Safianowska
Reviewers	Ioannis Markopoulos, Angelos Lampropoulos (NOVA), Roberto González (NEC)		
Type	R	**Dissemination**	PU
Document version	V1.0	**Due date**	30/06/2025

Co-funded by the European Union

6GSNS

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

UKRI UK Research and Innovation

Project information

Project title	Net-Zero self-adaptive activation of distributed self-resilient augmented services
Project acronym	NATWORK
Grant Agreement No	101139285
Type of action	HORIZON JU Research and Innovation Actions
Call	HORIZON-JU-SNS-2023
Topic	HORIZON-JU-SNS-2023-STREAM-B-01-04 Reliable Services and Smart Security
Start date	01/01/2024
Duration	36 months

Document information

Associated WP	WP5
Associated task(s)	T5.1
Main Author(s)	Maria B. Safianowska (ISRD)
Author(s)	Antonios Lalas, Alexandros Papadopoulos, Eleni Chamou, Aristeidis Papadopoulos, Virgilios Passas, Konstantinos Nikiforidis, Evgenia Vogiatzi, Nikolaos Makris, Donatos Stavropoulos, Thanasis Korakis, Anastasios Drosou (CERTH), Jorge Pose, Julio Suárez, Joaquín Escudero (GRAD), Gürkan Gür (ZHAW), Leonardo Padial (HES-SO), Nasim Nezhadsistani, Andy Aidoo (UZH), Ioannis Markopoulos, Angelos Lampropoulos (NOVA)
Reviewers	Ioannis Markopoulos, Angelos Lampropoulos (NOVA), Roberto González (NEC)
Type	R — Document, report
Dissemination level	PU — Public
Due date	M18 (30/06/2025)
Submission date	03/07/2025

Document version history

Version	Date	Changes	Contributor (s)
v0.1	03/12/2024	Table of contents, sections assignment	Maria B. Safianowska (ISRD)
v0.2	17/03/2025	Draft contributions for sections 2, 3, 4 and 5	Alexandros Papadopoulos, Eleni Chamou, Aristeidis Papadopoulos, Evgenia Vogiatzi (CERTH), Jorge Pose, Julio Suárez, Joaquín Escudero (GRAD), Gürkan Gür (ZHAW), Leonardo Padial (HES-SO)
v0.3	07/05/2025	Draft contributions for sections 2, 3, 4 and 5	All authors
v0.4	09/06/2025	Complete first version without executive summary, introduction and conclusions	All authors
v0.5	10/06/2025	Complete executive summary, introduction and conclusions	Maria B. Safianowska (ISRD)
v0.6	11/06/2025	Complete draft, ready for review	Maria B. Safianowska (ISRD)
v0.7	13/06/2025	Review complete and feedback to co-authors	Ioannis Markopoulos, Angelos Lampropoulos (NOVA), Roberto González (NEC)
v0.8	24/06/2025	Revisions complete, ready for quality review	Alexandros Papadopoulos, Eleni Chamou, Aristeidis Papadopoulos (CERTH), Jorge Pose, Julio Suárez, Joaquín Escudero (GRAD), Gürkan Gür (ZHAW), Leonardo Padial (HES-SO), Maria B. Safianowska (ISRD)
v0.9	25/06/2025	Quality review complete	Joachim Schmidt, Leonardo Padial (HES-SO)
v0.9.5	30/06/2025	Final review and refinements	Antonios Lalas, Alexandros Papadopoulos, Evangelos V. Kopsacheilis (CERTH)
v1.0	03/07/2025	Final version for submission	Antonios Lalas (CERTH)

Disclaimer

Copyright message

Contents

List of acronyms and abbreviations

Abbreviation	Description
3GPP	3rd Generation Partnership Project
5G-GUTI	5G Globally Unique AMF identifier
5G SA	5G Standalone
5GSC	5G Standalone Security Category
AI	Artificial Intelligence
AES	Advanced Encryption Standard
AMF	Access and Mobility Management Function
ANN	Artificial Neural Network
ARP	Address Resolution Protocol
AoA	Angle of Arrival
APN	Access point Name
AUSF	Authentication Server Function
AV	Autonomous Vehicle
BER	Bit Error Rate
BLE	Bluetooth Low Energy
BS	Base Station
BSGLRT	Bayesian Structured Generalized Likelihood Ratio Test
BUGLRT	Bayesian Unstructured Generalized Likelihood Ratio Test
CAN	Controller Area Network
CFO	Carrier Frequency Offset
CNN	Convolutional Neural Network
CRADA	Cooperative Research and Development Agreement
CSI	Channel State Information
DHCP	Dynamic Host Configuration Protocol
DL	Deep Learning
DM-RS	Demodulation Reference Signal
DNN	Deep Neural Network
DoA	Direction of Arrival
DoS	Denial of Service
DRL	Deep Reinforcement Learning
DSP	Digital Signal Processing
EM	Electro Magnetic
EO	Earth Observation
ERA	Environment Reconfiguration Attack
FDA	Frequency Diverse Array
FH	Frequency-Hopping
FMCW	Frequency-Modulated Continuous Wave
FPGA	Field-Programmable Gate Array
FSO	Free-Space Optical

Abbreviation	Description
GLRT	Generalized Likelihood Ratio Test
GMM	Gaussian Mixture Model
gNB	gNodeB
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GTP-U	GPRS Tunneling Protocol User
HAPS	High-Altitude Platform Station
ICI	Inter-Carrier Interference
IE	Information Element
IEC	International Electrotechnical Commission
ILP	Integer Linear Programming
IoT	Internet of Things
IRIS	Illegal Reconfigurable Intelligent Surface
ISC	Infrastructure Security Category
ISMS	Information Security Management System
ISO	International Organization for Standardization
JS	Jamming Suppression
JSON	JavaScript Object Notation
KGR	Key Generation Rate
LEO	Low Earth Orbit
LIDAR	Light Detection and Ranging
LR	Legitimate Receiver
LS	Least Squares
LTE	Long-Term Evolution
LU	Legitimate User
MAC	Medium Access Control
MEC	Mobile Edge Computing
MIB	Master Information Block
MIMO	Multiple Input Multiple Output
ML	Machine Learning
MMSE	Minimum Mean Squared Error
MMT	Multi-Metric Telemetry
mmWave	millimetre-wave
NAS	Non-Access Stratum
NASA	National Aeronautics and Space Administration
NCCoE	National Cybersecurity Centre of Excellence
Near-RT	Near Real-Time
NEF	Network Exposure Function
NIST	National Institute of Standards and Technology
NR	New Radio
MEC	Multi-access Edge Computing

Abbreviation	Description
MSE	Mean Square Error
OAM	Operations & Maintenance
OEM	Original Equipment Manufacturer
O-RAN	Open radio access network
PBCH	Physical Broadcast Channel
PBL	Primary Boot Loader
PCA	Pilot Contamination Attack
PCB	Printed Circuit Board
PDCCH	Physical Downlink Control Channel
PHY	Physical layer
PIN	Positive-Intrinsic-Negative
PKG	Physical-layer Key Generation
PLMN	Public Land Mobile Network
PLS	Physical Layer Security
PRACH	Physical Random Access Channel
PSA	Pilot Spoofing Attack
PSS	Primary Synchronization Signal
PTP	Precision Time Protocol
PUCCH	Physical Uplink Control Channel
PWE	Programmable Wireless Environment
P4	Packet Processing Platform
QoS	Quality of Service
RAN	Radio access network
RB	Resource Block
RF	Radio Frequency
RFID	Radio-Frequency Identification
RIA	Research Innovation Action
RIC	Radio Intelligent Controller
RIS	Reconfigurable Intelligent Surface
ROM	Read-Only Memory
SBA	Service-Based Architecture
SBL	Sparse Bayesian Learning
SCAS	Security Assurance Specifications
SDN	Software-Defined Networking
SDR	Software-Defined Radio
SER	Symbol Error Rate
SHA-256	Secure Hash Algorithm 256-bit
SIB	System Information Block
SINR	Signal to Interference and Noise Ratio
SKG	Secret Key Generation
SLS	Scaled Least Squares

Abbreviation	Description
SMF	Session Management Function
SNR	Signal to Noise Ratio
S-NSSAI	Single - Network Slice Selection Assistance
SoC	Systems on a Chip
SPARTA	Space Attack Research and Tactic Analysis
SSB	Synchronization Signal Block
SSS	Secondary Synchronization Signal
STC	Secrecy Transmission Capacity
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.
SUCI	Subscription Concealed Identifier
TDD	Time-domain Duplex
TPM	Trusted Platform Module
UDM	Unified Data Management
UE	User Equipment
UP	User Plane
UPF	User Plane Function
URLLC	Ultra-Reliable Low-Latency Communications
USRP	Universal Software Radio Peripheral
UWB	Ultra-Wideband
VM	Virtual Machine
VPN	Virtual Private Network
V2X	Vehicle-to-everything
XBL	Extended Bootloader
XR	EXtended Reality
ZF	Zero Force
ZFJS	Zero-Forcing Jamming Suppression

List of figures

List of tables

Executive summary

This deliverable, part of the NATWORK project, presents a comprehensive framework for threat modelling at the physical layer of next-generation wireless systems, particularly in the context of 5G and emerging 6G technologies.

The report begins by analysing existing threat models and methodologies relevant to the physical layer. Notably, it examines the IEEE SA P3349 Secure-by-Component approach, which emphasizes decomposing complex communication systems into secure, modular building blocks. The ISO/IEC 27005 risk management framework is also reviewed for its systematic process of identifying, assessing, and mitigating risks. Furthermore, the O-RAN Security Threat Modelling and Risk Assessment is considered, highlighting the relevance of open, disaggregated network architectures to PHY layer vulnerabilities.

Informed by these foundations, the deliverable defines the NATWORK Physical Layer Threat Modelling Methodology. This methodology builds upon recognised best practices but extends them to capture the evolving threat landscape of 5G/6G networks, characterized by virtualization, multi-vendor environments, AI-enhanced signal processing, and advanced physical-layer technologies like Reconfigurable Intelligent Surfaces and Massive MIMO. The methodology aligns with secure-by-design principles and emphasizes a proactive, adaptive approach to mitigating risks at the physical layer.

The core of the deliverable is the application of this methodology to develop the NATWORK Physical Layer Threat Model. The model systematically identifies key assets, potential adversaries, and vulnerabilities, followed by a threat characterisation across four primary categories: jamming, eavesdropping, spoofing, and physical tampering. The report presents a detailed analysis of vulnerabilities, distinguishing between those inherent to protocols and standards, technology-specific risks (such as those related to RIS and MIMO), and emerging AI-driven threats that exploit PHY-layer identifiers or control signals.

Furthermore, the report incorporates a layered risk and impact assessment that considers both the likelihood of threat occurrence and the potential consequences for system confidentiality, integrity, and availability. This assessment provides a clear basis for prioritising mitigation efforts across different technologies and threat vectors.

To address these challenges, the deliverable outlines key mitigation methods. Recommendations include established countermeasures, such as secure pilot authentication and beam randomization, as well as novel approaches targeting AI-assisted attacks and vulnerabilities introduced by virtualization and multi-vendor ecosystems. For RIS systems, the document proposes specific security controls for configuration integrity and unauthorised signal

manipulation prevention. For MIMO systems, obfuscation and advanced signal processing techniques are discussed to strengthen resilience.

In conclusion, this deliverable establishes a strategic foundation for adopting secure-by-design practices at the PHY layer. These practices are essential for realising the NATWORK project's vision of resilient, self-adaptive, and secure next-generation communication networks. Specifically, it directly supports Operational Objective #4: Provide Physical Layer Security that supports encryption-free, perennial self-resilience of wireless links. By addressing vulnerabilities early in the system design and development lifecycle, and by promoting the standardisation and harmonisation of security controls, NATWORK contributes to advancing Europe's leadership in secure, trustworthy 6G services.

This report also lays the groundwork for future work within NATWORK, including validation of proposed mitigations, integration of threat modelling outcomes into system architecture, and continuous updates of the threat landscape to reflect technological advances and evolving adversarial tactics.

1 Introduction

The evolution of wireless communication technologies, from 5G to the upcoming 6G, introduces new dimensions of complexity and a significantly expanded threat surface, especially at the physical (PHY) layer. Traditional threat modelling approaches have often focused on higher network layers, leaving the PHY layer underexplored despite its foundational role in ensuring secure and reliable connectivity. The NATWORK project addresses this critical gap by systematically analysing vulnerabilities and emerging threats at the PHY level, particularly those relevant to advanced technologies like Massive MIMO, Reconfigurable Intelligent Surfaces (RIS), and AI-enhanced signal processing. This deliverable (D5.1), the outcome of the work conducted in task T5.1, builds upon established methodologies—including ENISA's threat landscape, ISO/IEC 27005, and the O-RAN threat model—to develop a robust, context-specific threat modelling framework that considers both conventional and cutting-edge attack vectors.

This document also considers the multi-vendor and virtualized deployment environments that are increasingly prevalent in modern radio access networks, introducing risks that cannot be mitigated solely through conventional security techniques. The NATWORK physical layer threat modelling approach incorporates insights from multiple stakeholders across academia and industry to identify key assets, potential adversaries, and context-aware vulnerabilities. It emphasizes the need for proactive and adaptive mitigation strategies to guard against AI-assisted spoofing, pilot contamination, RIS manipulation, and other advanced tactics. Through this work, NATWORK contributes to a secure-by-design paradigm for the physical layer, ensuring that foundational security considerations are embedded early in the design lifecycle of future wireless networks.

1.1 Purpose and structure of the document

The purpose of the D5.1 Physical layer threat modelling is to inform the NATWORK consortium and its stakeholders by offering an integrated analysis of existing threat models, adapting them to physical-layer components, and proposing a new methodology aligned with project goals. It supports the secure-by-design paradigm and lays the groundwork for proactive risk assessment and countermeasure implementation across multi-vendor, AI-driven, and hardware-converged environments in the wireless domain.

Following the Introduction, which sets the stage for the document's purpose, audience, and its interconnections within the project's framework, the structure continues as follows:

Sections:

2. **Analysis of Existing Threat Models and Methodologies:** Provides a comparative analysis of several established threat modelling frameworks relevant to wireless systems physical layer.
3. **NATWORK Physical Layer Threat Model:** First presents the custom methodology developed by the NATWORK consortium for physical layer threat analysis. It then applies the proposed methodology to build a detailed threat model for the PHY layer.
4. **Key Mitigation Methods:** Proposes mitigation strategies to address the previously identified threats and vulnerabilities.
5. **Conclusions:** Wraps up the document, reflecting on the project's strategic orientation and establishing expectations for future milestones.

1.2 Intended Audience

The NATWORK D5.1 Physical layer threat modelling is devised for public use, including, but not limited to the NATWORK consortium, comprising members, project partners, and affiliated stakeholders. This document mainly focuses on the physical layer modelling of the project, thereby serving as a referential tool throughout the design, testing and validation of physical layer security solutions across the project's lifespan.

1.3 Interrelations

The NATWORK consortium integrates a multidisciplinary spectrum of competencies and resources from academia, industry, and research sectors, focusing on user-centric service development, robust economic and business models, cutting-edge cybersecurity, seamless interoperability, and comprehensive on-demand services. The project integrates a collaboration of fifteen partners from ten EU member states and associated countries (UK and CH), ensuring a broad representation for addressing security requirements of emerging 6G Smart Networks and Services in Europe and beyond.

NATWORK is categorised as a "Research Innovation Action - RIA" project and is methodically segmented into 7 WPs, further subdivided into tasks. With partners contributing to multiple activities across various WPs, the structure ensures clarity in responsibilities and optimizes communication amongst the consortium's partners, boards, and committees. The interrelation framework within NATWORK offers smooth operation and collaborative innovation across the consortium, ensuring the interconnection of the diverse expertise from the various entities (i.e., Research Institutes, Universities, SMEs, and large industries) enabling scientific, technological, and security advancements in the realm of 6G.

The D5.1 Physical layer threat modelling is the main output of T5.1 Threat modelling for Physical layer and is closely interrelated with the following project components and deliverables:

1. **D5.2** - Energy efficient AI-based security processes: D5.2 focuses on another aspect of security related to AI. While the PHY Threat Model developed in D5.1 includes the AI generated threats, D5.2 complements this research by further focusing on the intrinsic security of AI based solutions. Additionally, D5.2 presents energy-efficient security methods which are the answer to selected threats from D5.1.
2. **D5.3** - AI-powered Anti-jamming & RIS Defence mechanisms: D5.1 lays ground to the anti-jamming and RIS Defence mechanisms developed in D5.3 by thoroughly analysing the jamming and RIS related threats within the systematic physical layer threat model.
3. **WP2:** D5.1 is based on the SOTA of radio attacks performed in D2.1 - SoA analysis & benchmark assessment and provides a rationale for UC2 described in D2.2 - 6G Use Cases scenarios and requirements, which showcases physical layer security solutions.
4. **WP6:** D5.1 provides input to future integration and validation work in WP6.

2 Analysis of existing threat models and methodologies

The development of an effective, context-specific threat modelling framework for the NATWORK project requires a systematic evaluation of established methodologies as a first step. Existing threat modelling approaches provide essential foundations for understanding vulnerabilities, adversarial capabilities, and risk mitigation in complex, multi-layered communication environments. However, given the unique characteristics of physical-layer technologies in 5G and beyond—such as Massive MIMO, Reconfigurable Intelligent Surfaces (RIS), and AI-enhanced signal processing—traditional methodologies must be critically assessed and selectively adapted.

This section provides a structured analysis of relevant threat modelling frameworks that either directly address wireless and physical-layer security or contain transferable elements applicable to NATWORK's objectives. The reviewed methodologies, including the IEEE 3349 framework, ISO/IEC 27005 risk management standard, and sector-specific models such as O-RAN and ENISA's threat assessments, serve as technical baselines for building a robust, tailored PHY-layer threat modelling approach. By identifying their strengths, limitations, and relevance to emerging wireless systems, this analysis ensures that the NATWORK methodology is grounded in best practices while addressing the evolving threat landscape specific to physical-layer security.

2.1 Threat Modelling Methodologies

The development of a reliable and adaptable physical layer threat model relies on well-tailored methodologies that promote secure-by-design principles. This subsection explores key threat modelling approaches relevant to wireless systems, emphasizing their structure, practical application, and relevance to 6G and advanced 5G use cases. Particular attention is given to the IEEE Space System Cybersecurity Working Group methodology and the ISO/IEC 27005 standard, both of which advocate a systematic, component-focused approach to identifying vulnerabilities and mitigating risks across complex, distributed communication infrastructures.

2.1.1 Threat modelling and Secure-by-Design principles for Wireless Systems: IEEE 3349 Methodology

The rapid evolution of communication technologies, compounded by recent geopolitical events such as the Viasat cyberattack [1] in February 2022, has highlighted the urgent need for fast and reliable satellite missions for military and civil security operations. Consequently, the IEEE SA P3349 Space System Cybersecurity Working Group [2] has been working on a secure system engineering methodology, employing a secure-by-component design strategy. This approach begins by defining the scope of technical security engineering, decomposing the system into components and data flows, and enumerating attack surfaces. *It then* proceeds by identifying threats to low-level components, applying secure-by-design principles. This leads to a redesign

of components into secure blocks, and the crafting of SHALL statements to refactor the system design, with a particular focus on improving the security of the link segment [3].

In this section, we describe this methodology with a focus on threat modelling and analysis aspects to support the NATWORK's WP5 efforts. To provide concrete and practical input, we examine an Earth observation (EO) mission utilizing a single low Earth orbit (LEO) satellite and illustrate the design and decomposition of its components for enhanced security engineering purposes. We also enumerate potential attacks in optical networks and identify potential attack surfaces from a link perspective [4]. Please note that this scenario can easily be replaced with different 6G use cases following the methodology and the following description also serves as an example from the perspective of how to apply a threat analysis and modelling for 6G RAN regarding different physical layer technologies.

2.1.1.1 EO through a single LEO satellite

EO satellites are designed to observe various events occurring on Earth from space. They are equipped with different sensors tailored to specific purposes, including monitoring natural phenomena, tracking disasters, and documenting changes to the Earth. In this subsection, we focus on a LEO satellite that observes Earth and transmits the collected data to a ground station. In this scenario, we utilize both uplink and downlink communications. The downlink primarily handles the transmission of collected data back to Earth, including images and sensor outputs, thus requiring higher data rates and bandwidth. Conversely, the uplink sends commands from Earth for parameter adjustments, necessitating lower data rates and frequencies. Both radio frequency (RF) and free-space optical (FSO) communications are viable options and will be discussed further in the following section.

2.1.1.2 Security challenges and proposed approach

Potential vulnerabilities in wireless optical links. The security of communication channels is crucial when designing a network for EO, as these channels are susceptible to potential attacks. These channels are vital for transmitting the data gathered by the network. Two primary communication technologies in the physical layer are employed in this scenario: RF and FSO. However, each technology has unique characteristics, security challenges, and vulnerabilities.

Future satellite constellations are expected to increasingly rely on optical communication in the physical layer due to its higher data rates and inherent security features, as optical communication is generally considered more difficult to intercept. A study [5] considers optical communication as a defensive scheme in satellite networks. However, optical networks are vulnerable to various attacks, including eavesdropping, high-power jamming, physical infrastructure attacks, denial of service, and tapping attacks that allow unauthorized access for eavesdropping and traffic analysis. Most attacks on optical networks target the channel side, emphasizing the need for a secure-by-design approach to the communication link, even when

using FSO. For instance, the work in [6] demonstrated potential information leaks in satellite networking using optical communication. They proposed a model where a satellite communicates with a high-altitude platform station (HAPS) node through optical communication. In this model, an attacker positioned close to or on top of the satellite could eavesdrop on the transmitted signals. While inter-satellite communication is critical to the satellite system, its security remains underexplored.

Moreover, advances in FSO technology, while enhancing performance, introduce new security concerns. Attackers could inject signals to alter communications, degrading the signal-to-noise ratio (SNR) at the legitimate receiver and thus decreasing the overall secrecy capacity. Pointing errors and beam divergence caused by beam wander further exacerbates security risks by causing misalignment between the transmitter and receiver, lowering the main channel's adequate received power and SNR. Empirical data from NASA demonstrate that larger receiver apertures can reduce the bit error rate (BER) and aid in managing variable weather conditions. However, they also enable jammers to exploit this feature by transmitting disruptive optical pulses, making it difficult to differentiate legitimate signals from interference. This poses substantial risks to communication integrity, especially in high-security scenarios such as military applications [7].

This highlights the importance of designing secure communication systems in the physical layer from the outset to ensure the integrity and confidentiality of data transmission in optical communication networks. Special attention must be given to potential vulnerabilities, such as pointing errors and signal injection, which can degrade the main user channel and reduce the overall secrecy capacity. Additionally, beam divergence and alignment issues must be managed to maintain the reliability and availability of the communication link, particularly over long distances.

Secure-by-component approach. The secure-by-component approach was implemented in the work [8] to address these challenges for this specific scenario. This approach builds from secure building blocks to mission-level security and complements traditional top-down methods. We ensure a robust security framework by decomposing the system into secure components. Our methodology is mapped to specific phases, as shown in Figure 1. Furthermore, we considered SPARTA [9] to list attack techniques and secure-by-design principles, though other frameworks can also be applied.

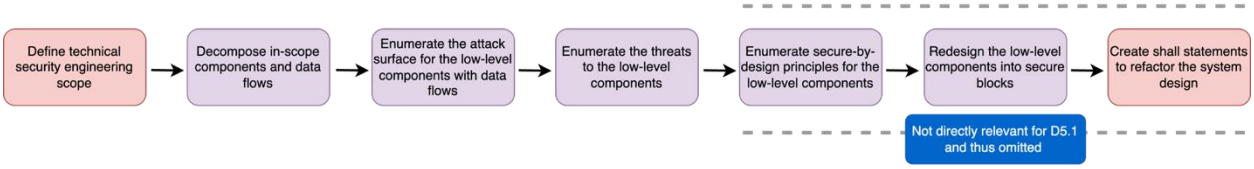

Figure 1 Secure-by-component design strategy.

As a first step, we define our technical scope as limited to the link segment, which encompasses the link capabilities required for ground-to-space, space-to-ground, and, in the case of our EO scenario, space-to-space communications. Applying this methodology to each segment, e.g., space vehicles or ground stations, separately is essential for a comprehensive security strategy to ensure thorough security coverage. However, they are not directly relevant for physical layer threat modelling and are not covered in this document.

Decomposition of in-scope components and data flows. This section decomposes the use case into functional blocks to analyse the associated data flows.

The workflow for a single LEO satellite starts with the ground station sending a manually or automatically scheduled command containing image schedule data. This data flow is received by the payload control system, which directs the camera to capture images through the image generation process, as shown in Figure 2. There are also other components, such as payload control and attitude determination on a satellite platform, which are not directly related to the physical links.

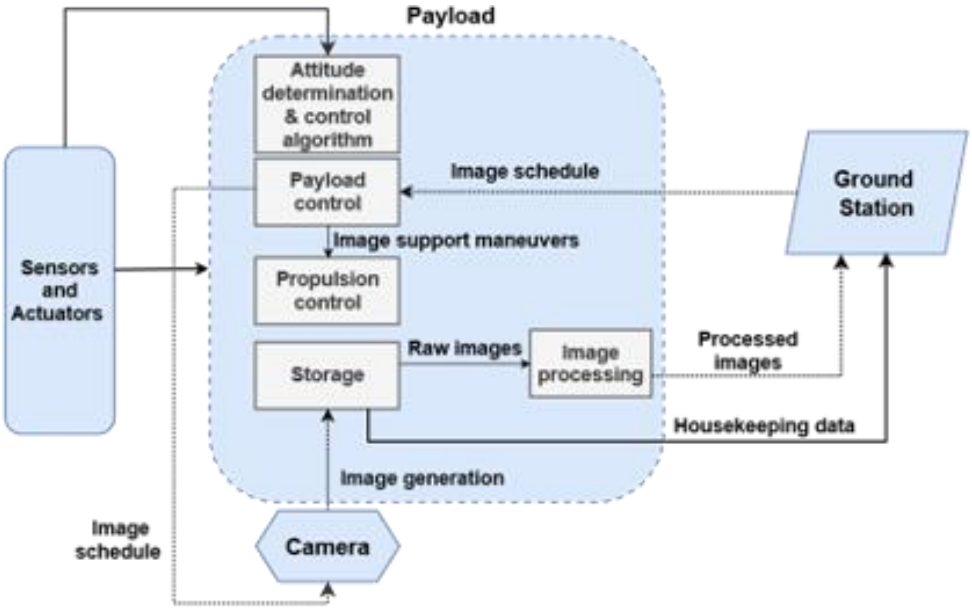

Figure 2 Decomposition of the systems for the EO through a single LEO satellite.

Attack surfaces and techniques. The attack surface for our link capabilities was defined and aligned with the engineering scope. The component inventory, related input, related processing, and related output with data flow were used to identify relevant adversarial techniques (Table 1). This approach allowed the demonstration of how to apply SPARTA as a threat source during the application of the technical security engineering process. Space-focused adversarial capabilities continue to evolve, especially in military operations. EO missions must be engineered

with intrinsic security and a military-hardened mindset. This is especially important based on the convergence of commercial operators into a hybrid military landscape for space operations.

Table 1 Attack surfaces outline for a single LEO satellite.

Component	Input	Processing	Output	Related data flow
Ground station	Processed images	Image service	Image product	Processed images
Image processing	Raw images	Image service	Processed images	Processed images
Payload control	Image schedule	Scheduling service	Scheduled commands	Image schedule
Camera	Image schedule command	Image acquisition service	Image data	Image generation
Storage	Image data	Data storage service	Raw images	Image generation
Image processing	Raw image data	Image processing service	Processed images	Processed images

The commercial space data system attack surface area has become a military surface area, so commercial security becomes military security. In addition, adversaries are constantly seeking to exploit attack surfaces further left, namely software-focused, in both commercial and hybrid government space data systems. Accelerating the “shift left” mindset for commercial, military, and other critical space data system operations requires a paradigm shift. This shift, centred on component-level secure-by-design, represents the attack surface reduction military advantage needed to protect national and allied assets.

EO through a Single LEO Satellite In our threat enumeration, we employ a strategic approach that involves mapping the sequence of operations to the most critical attack techniques delineated by the SPARTA framework. However, we first identify our attack surfaces by decomposing the inputs, processing, outputs, and data flow for each low-level component, as presented in Table 1.

1. **Ground-to-Space Trust - [SPARTA Attack Technique: IA-0009 Trusted Relationship]:** The trust relationship established between a ground station component and a payload control element on the satellite in the uplink consists of the image schedule data flow, which is crucial for maintaining integrity and resilience. An adversary could exploit this trust, gain unauthorized access, and inject incorrect commands and

schedules. This could lead to manipulating the timing or content of scheduled image captures. Alternatively, they could prevent uplink data transmission by disrupting the command flow, preventing essential commands from reaching the payload control element, thereby leading to operational disruptions.

2. **Image Acquisition Process - [SPARTA Attack Technique: IA-0009 Trusted Relationship]:** The trust relationship resides within the satellite's components, including the attitude determination and control algorithm, propulsion control, sensors, and actuators. It is crucial to ensure that malicious commands or error values do not impact the lone space vehicle's ability to support the primary mission's image schedule data flow. From an adversary's viewpoint, manipulating the attitude determination and control algorithm could lead to misalignment, affecting image quality. Similarly, compromising propulsion control systems could disrupt satellite manoeuvrability, impacting image capture locations and schedules. Sensors and actuators, if compromised, can result in inaccurate data collection, affecting the overall mission objectives. Furthermore, the interconnectedness of these components increases the risk, as a single compromise could lead to broader system vulnerabilities and potentially grant unauthorized access to critical functions.
3. **Image Storage - [SPARTA Attack Technique: IA-0006Compromise Hosted Payload]:** When considering the hosted payload, our focus extends to the components of the camera, camera storage, image processing, and housekeeping data flow. From an adversary's perspective, the camera's attributes, such as focus and scale, are vulnerable, as a compromise in technical integrity could be exploited to manipulate or distort images for deception. Additionally, once images are acquired and stored, adversaries may attempt to exploit vulnerabilities in the transmission of the housekeeping data by manipulating it to simulate operational failures, aiming to deceive ground operations and compromise mission objectives.
4. **Image Delivery to Ground Station- [SPARTA Attack Technique: IA-0009 Trusted Relationship and DE-0002 Prevent Downlink]:** The trust relationship is critical in the downlink, ensuring the ground station receives EO-processed image data exclusively from the satellite's storage element.

An adversary could prevent downlink data transmission, resulting in significant data loss and disrupting real-time monitoring and decision-making processes. This disruption would affect operational tasks reliant on timely data updates, necessitating manual intervention or rescheduling.

The next step would map the attack techniques identified above to *secure-by-design* principles. However, this is not provided since our focus is physical layer threat analysis. For further information on that topic, please refer to [2].

2.1.2 ISO/IEC: 27005

ISO/IEC 27005 [10] is a standard by International Organization for Standardization that provides guidance on managing information security risks. It helps organizations implement and maintain an Information Security Management System (ISMS) by offering a structured approach to identifying, assessing, and treating security risks. It outlines a cyclical process for identifying, analysing, evaluating, treating, and monitoring information security risks.

Key Stages in the ISO 27005 Risk Management Process:

1. **Context Establishment**: Defines the scope of the risk management process, including identifying the organization's objectives, assets, and vulnerabilities.
2. **Risk Assessment**: This involves identifying, analysing, and evaluating information security risks. It can be further broken down into:
    a. **Risk Identification**
    b. **Risk Analysis**
    c. **Risk Evaluation**
3. **Risk Treatment**: Implementing measures to mitigate or reduce identified risks.
4. **Residual Risk**: Risk not addressed in the risk treatment step needs to be continuously monitored and evaluated.
5. **Risk Communication and Consultation**: Communicating risk information to relevant stakeholders and seeking their input.

The framework is illustrated in Figure 3 ISO/EIC 27005 risk management process [15]Figure 3.

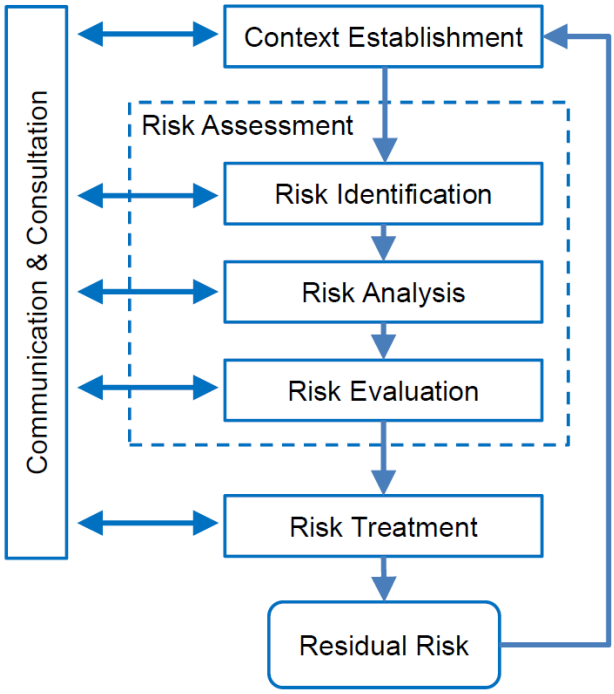

Figure 3 ISO/EIC 27005 risk management process [15]

ISO 27005 is a well-established and widely adopted by the industry. The advantages of using ISO 27005 include providing a structured, repeatable approach to identifying and managing information security risks, enabling organizations to make informed, prioritized decisions. The standard supports alignment with ISO/IEC 27001[11], which is the world's best-known standard for ISMS, facilitating ISMS compliance and audit readiness. Furthermore, ISO 27005 enhances risk visibility across the asset lifecycle, promotes proactive threat mitigation, and ensures consistency in risk evaluation. It is adaptable to diverse environments, including cloud-native and telecom systems, and integrates effectively with methodologies like STRIDE and Zero Trust, helping organizations build security by design and maintain resilience against evolving threats. Taking all of the above into account, it proves a good choice for the framework on which to base the threat modelling methodology for physical layer in NATWORK.

2.2 Threat Models

Beyond general methodologies, existing threat models provide domain-specific insights into potential attack vectors, vulnerabilities, and adversarial behaviours affecting wireless networks. This subsection introduces a comparative overview of several prominent threat models, including the O-RAN Security Threat Modelling and Risk Assessment framework and the ENISA 5G Threat Landscape. Additional models, informed by 5G networks, are also discussed to broaden the understanding of evolving threats in multi-vendor, AI-driven, and virtualization-heavy deployment scenarios. These models collectively inform the NATWORK consortium's approach

to securing the physical layer of future networks. The section identifies the elements which can be transferable to NATWORK while also outlines their limitations, which are then addressed in following sections to build comprehensive NATWORK PHY Threat Model.

This section, designed to help the comparison between the analysed models, is organized as follows:

1. Sections 2.2.1 and 2.2.2. follow a structure where first a brief **description** of the threat model is provided. The **scope** of the model provides insight into the area of wireless networking that the model is applicable to. The **methodology** used by the model is then summarized to identify potential gaps or drawbacks. Next the core of the analysis of the given model is given in the subsection describing elements related to Physical Layer that were identified by the model in question. Namely, **assets, vulnerabilities** and finally **threats** are identified. These will serve as transferable elements to the NATWORK PHY Threat Model Finally the **limitations** of each model are identified.
2. Section 2.2.3 serves as a container for two additional threat models and follows the same logic in a briefer way, focusing on identifying the limitations of the discussed models to further inform the construction of NATWORK PHY Threat Model.

2.2.1 O-RAN Security Threat Modelling and Risk Assessment 4.0

2.2.1.1 Description

The O-RAN Security Threat Modelling and Risk Assessment document [12] provides a comprehensive and methodical evaluation of potential security threats across the O-RAN architecture. This document serves as a technical report produced by O-RAN Alliance Work Group 11, focusing on:

1. Identifying security threats in O-RAN architecture
2. Performing threat modelling using the STRIDE framework
3. Assessing risk levels (impact and likelihood)
4. Recommending principles and controls to mitigate risks

It includes only components and interfaces explicitly specified by O-RAN.

2.2.1.2 Scope

The threat model spans the following O-RAN Architecture elements:

1. **Key O-RAN components**: SMO, Near-/Non-RT RIC, O-DU, O-CU-CP/UP, O-RU, xApps/rApps, O-Cloud
2. **Interfaces**: A1, O1, O2, E2, Open Fronthaul (CUS-Plane, M-Plane), Y1
3. **Protocols**: TLS, SSH, IPsec, NETCONF, JSON/REST, FTP/FTPS, PTP

The 3GPP interfaces already studied and maintained by 3GPP, UE, MEC, and Core are not in the perimeter of the O-RAN Alliance system, therefore, they are considered out of scope of this study.

2.2.1.3 Methodology

The methodology follows a structured risk assessment process based on the ISO/IEC 27005 standard described in the previous section (Section 2.1.2). It is divided into three main phases, each containing multiple detailed steps:

1. **Identification**
    a. **Identify stakeholders:** First, identify the stakeholders involved in the implementation, management, operation and maintenance of the O-RAN system. Roles and responsibilities of each stakeholder are also provided.
    b. **Define assumptions:** The list of minimum prerequisites and assumptions must be defined for the operational environment (not under the control of the O-RAN system) required to successfully operate the O-RAN system.
    c. **Identify assets:** First, locate the relevant assets the O-RAN system holds and provide details about the type (Data, component, etc.), the security properties (CIA) at rest and in transit and location.
    d. **Identify threats:** Identify the relevant threats associated with the new O-RAN components, interfaces and technologies. In addition, the threat surface and agents are given.
    e. **Identify vulnerabilities:** O-RAN systems may have weaknesses in their new O-RAN components, interfaces and technologies which need to be identified.
    f. **Define security principles:** Define security principles to be achieved to reduce risk exposure.
    g. **Elaborate and refine security principles:** Each security principle needs to be detailed and refined into requirements, recommendations and countermeasures.
    h. **Identify existing/ongoing countermeasures:** Identify all existing/ongoing O-RAN controls and consider the protection provided by these controls before applying any new ones.
2. **Risk assessment**

The value for *Risk* is defined by the following equation:

Risk = (the probability of a threat exploiting a vulnerability) x (total impact of the vulnerability being exploited)

3. **Risk treatment**
    a. Now that we know the level of risk that each threat poses, we need to decide how we'll treat them. There are four options:

i. **Modify the risk** by implementing a control to reduce the likelihood of it occurring.
ii. **Avoid the risk** by ceasing any activity that creates it. This response is appropriate if the risk is too big to manage with a security control.
iii. **Share the risk** with a third party. There are two ways: by outsourcing the security efforts to another organization or by purchasing cyber insurance to ensure the funds to respond appropriately in the event of a disaster.
iv. **Retain the risk**. This means that the organization accepts the risk and believes that the cost of treating it is greater than the damage that it would cause.

2.2.1.4 Elements related to Physical Layer

The elements related to physical Layer that were identified by the model, in the categories of assets, vulnerabilities and threats, are listed below. They will serve as transferable elements for the NATWORK PHY Threat Model.

1. **Assets**
    a. CUS Plane and M-Plane Data transported on Fronthaul Interface
    b. AAL related assets
    c. O-DU software, O-RU software, O-eNB, PNF NF equipment
    d. OFH M-Plane, including its protocol stack, OFH CUS-Plane, including its protocol stack
    e. Shared O-RU, O-RU Host, O-RU Tenant (Shared Resource Operator), O-DU Host, O-DU Tenant (Shared Resource Operator)
2. **Vulnerabilities**
    a. Failure to address overload situations (on air link)
    b. Heterogeneous security levels between O-RU and O-DU provided by different vendors
    c. Lack of authentication and access control to the Open Front Haul Ethernet L1 physical layer interface
    d. Lack of authentication that could allow an adversary to inject DL C-plane messages
    e. Lack of authentication that could allow an adversary to inject UL C-plane messages
    f. Lack of sufficient security measures in the Fronthaul due to the negative impact on the performance requirements
    g. Lack of sufficient security measures in the Fronthaul due to the negative impact on the performance requirements
    h. Lack of sufficient security measures in the Fronthaul due to the negative impact on the performance requirements
    i. Lack of authentication, and authorization protection for U-Plane data packets

j. False O-RUs

3. **Threats**
   a. An attacker penetrates O-DU and beyond through O-RU or the Fronthaul interface to access or modify sensitive information
   b. An attacker penetrates O-DU and beyond through O-RU or the Fronthaul interface to impersonate a legitimate system or user
   c. Unauthorized access to the Open Front Haul Ethernet L1 physical layer interface(s) to obtain protected information
   d. Unauthorized access to the Open Front Haul Ethernet L1 physical layer interface(s) to disrupt services
   e. An attacker attempts to intercept the Fronthaul (MITM) over the M Plane to obtain protected information
   f. An attacker attempts to intercept the Fronthaul (MITM) over the M Plane to alter m-plane data
   g. An attacker attempts to intercept the Fronthaul (MITM) over the M Plane to disrupt services
   h. DoS attack against a Master clock
   i. Impersonation of a Master clock (Spoofing) within a PTP network with a fake ANNOUNCE message
   j. A Rogue PTP Instance wanting to be a Grand Master
   k. Selective interception and removal of PTP timing packets
   l. Spoofing of DL C-plane messages
   m. Spoofing of UL C-plane messages
   n. An attacker attempts to intercept the Fronthaul (MITM) over the U-Plane to obtain user data
   o. An attacker attempts to intercept the Fronthaul (MITM) over the U-Plane to modify u-plane data
   p. An attacker attempts to intercept the Fronthaul (MITM) over the U-Plane to disrupt services
   q. Spoofing and unauthorized access of U-Plane data packets
   r. An attacker stands up a false base station attack by attacking an O-RU

2.2.1.5 Limitations

The threat model is quite comprehensive and provides great level of detail of the Physical layer related components of the O-RAN system. However, it doesn't focus on new attack vectors such as those exploiting RIS or MIMO for example. The aspect of virtualization of the physical layer and related threats are well defined and can be used as a base for NATWORK threat modelling of this category of threats.

2.2.2 ENISA Threat Landscape For 5G Networks

2.2.2.1 Description

The ENISA Threat Landscape for 5G Networks [13] provides a comprehensive assessment of cybersecurity vulnerabilities, threats, assets, and controls related to 5G infrastructure. This ENISA report is a major update of its 2019 edition, extending the coverage to include enhanced architectural components (e.g., SDN, NFV, MEC), vulnerabilities of new 5G deployment and migration paths, process-level and implementation-specific security issues and a mapping of threats to vulnerabilities and mitigations.

2.2.2.2 Scope

The threat model spans the following architectural elements of 5G [14]:

1. Core Network
2. Network Slicing
3. Radio Access Network (RAN)
4. Management and Orchestration (MANO)
5. SDN, NFV, MEC, and Physical Infrastructure
6. Security Architecture

Besides the architectural elements it also identifies threats for the common 5G use cases:

1. Enhanced Mobile Broadband (eMBB)
2. Ultra-Reliable Low-Latency Communication (URLLC)
3. Massive Machine-Type Communication (mMTC)
4. Industrial IoT (IIoT)
5. Vehicle-to-Everything (V2X)
6. Integrated Access and Backhaul (IAB)

2.2.2.3 Methodology

The **methodology** is based on ISO 27005 and adopts following steps:

1. Initial identification of relevant assets within the architecture.
2. Performing a vulnerability and a threat assessment, which evaluates the different levels of asset exposure
3. Reducing the threat surface of relevant assets by assigning security controls to the exploitable vulnerabilities

The methodology is depicted in Figure 4 ENISA Threat Modelling Methodology based on ISO 27005.

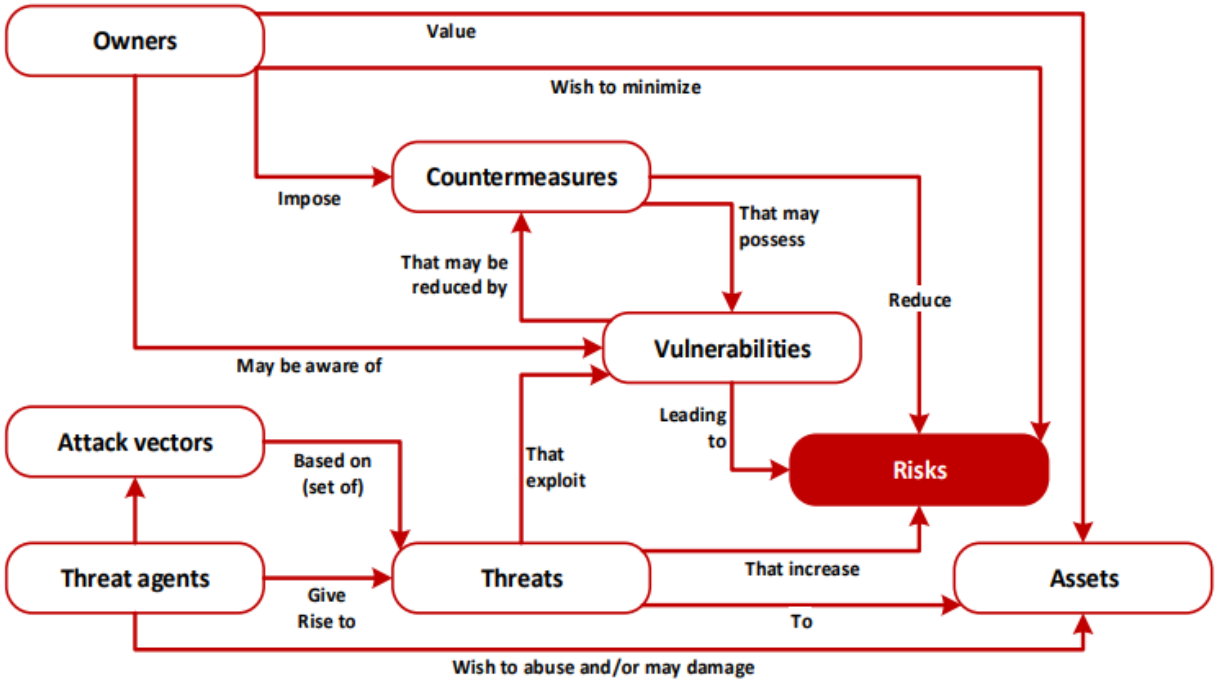

Figure 4 ENISA Threat Modelling Methodology based on ISO 27005

2.2.2.4 Elements related to Physical Layer

The elements related to Physical Layer that were identified by the model, namely the assets, the vulnerabilities and finally the threats, are listed below. They will serve as transferable elements for the NATWORK PHY Threat Model.

1. **Assets**
    a. Common Public Radio Interface (CPRI)
    b. Base Station
    c. Remote Radio Units (RRU)
2. **Vulnerabilities**
    a. **Security of Ultra-Reliable Low-Latency Communication (URLLC):** Weaknesses in the implementation of QoS may impact low-latency requirements [15]. Optimization issues of control and user plane will affect reliability and low latency of communications.
    b. **Vulnerability to Radio Jamming Attacks:** An inherent weakness of wireless cellular communications is the free frequency space that allows for intentional or unintentional interferences [16]. They can impact access of legitimate users and cause resilience issues in parts of the network.
    c. **General physical security considerations**: General physical measures need to be developed based on vulnerabilities and resulting risk-exposure that are related to the operational needs [17], supply chain of various components (delivery,

operation, implementation, maintenance) and criticality of services. Given the large number of roles involved in 5G infrastructures, the identification of physical vulnerabilities requires a holistic approach [18]. Although the document does not explicitly state so, it can be inferred that this vulnerability also applies to the equipment implementing the PHY layer, such as Base Stations or gNBs.

d. **Processes related vulnerabilities**: The report developed a set of vulnerabilities/weaknesses that arise from the absence of processes pertinent to life-cycle maintenance of systems and applications of the entire 5G infrastructure [19]. Although not explicitly listed, as in the above point, it also applies to PHY layer [19]. The report provides a comprehensive list of such vulnerabilities divided into three groups: MNO Processes, Vendor Processes and Security Processes.

3. **Threats**
    a. Threat Type: Nefarious Activity/ Abuse of assets (NAA) [20]
        i. Denial of service (DoS)
            1. Jamming the network radio
            2. Jamming device radio interface
            3. Jamming base station radio interface
        ii. Spectrum sensing
    b. Threat Type: Eavesdropping/Interception/Hijacking (EIH) [21]
        i. Interception of information
            1. Data eavesdropping via compromised small cell –
            2. Air interface eavesdropping –
            3. Device and identity tracking via rogue base station –
        ii. Eavesdropping on unencrypted message content

2.2.2.5 Limitations

The ENISA 5G Threat Landscape report, while comprehensive in scope and grounded in established standards, exhibits several key limitations that impact its practical applicability. Chief among these is its reliance on specification-based analysis rather than real-world deployment data, leading to a largely theoretical treatment of vulnerabilities and threats. The report does not incorporate empirical threat intelligence, incident records, or known attack vectors, which limits its utility for operational security teams and risk managers. Furthermore, the threat actor modelling is underdeveloped, lacking detailed adversary profiles or motivations, and the absence of vertical-specific assessments leaves a gap in evaluating context-driven risks in critical sectors like healthcare or industrial IoT. Additionally, it provides little insight to physical layer threats since it focuses on 5G as a whole. These constraints make the ENISA threat model a strong conceptual foundation but insufficient on its own for actionable decision-making focused on physical layer.

2.2.3 Additional threat models

2.2.3.1 NCCoE model

The National Cybersecurity Centre of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution.

Some aspects of securing 5G components and usage lack standards and guidance, making it more challenging for 5G network operators and users to know what needs to be done and how it can be accomplished. The NIST SPECIAL PUBLICATION 1800-33B [16], [23] addresses these challenges through an example solution and explains how a combination of 5G security features and third-party security controls can be used to implement the security capabilities organizations need to safeguard their 5G network usage. The example solution will demonstrate a 5G standalone (5G SA) network deployment that operates on and leverages a trusted and secure cloud-native hosting infrastructure and will show:

1. How cloud technologies can provide foundational security features outside the scope of the 3GPP.
2. How 5G security features can be utilized to address known security challenges found in previous generations of cellular networks such as LTE.
3. How commercial products can leverage cybersecurity standards and recommended practices for different 5G use case scenarios.

The solution will be designed around two focus areas. The **Infrastructure Security Focus Area** will concentrate on the trusted and secure cloud resources required to operate a mobile network, specifically the supporting infrastructure cybersecurity protections. The objective is to provide a trusted infrastructure to support the 5G Core Network functions, radio access network (RAN) components, and associated workloads. This focus area is included in the project to provide a trusted platform and holistic security reference architecture for a complete 5G network, as security for the underlying infrastructure is not within the scope of 3GPP specifications. On the other hand, the **5G Standalone Security Focus Area** will deploy a 5G SA network to enable the foundational configuration of the 5G Core's security features in a manner that demonstrates the

cybersecurity capabilities available in a 5G SA deployment. The deployment will include 5G New Radio base stations and a 5G Next Generation Core. The deployment will demonstrate how security capabilities can be used for continuous monitoring of 5G traffic on both signalling and data layers to detect and prevent cybersecurity attacks and threats.

In this model, risk assessment includes three components:

1. **Security category**. It is a high-level description for cataloguing the technical security capabilities considered for the proposed solution. There are two main categories with the corresponding subcategories:
    a. Infrastructure Security Category (ISC): Hardware Roots of Trust Packet Core, Hardware Roots of Trust Virtualized RAN, and Infrastructure Recommended Practice.
    b. 5G Standalone Security Category (5GSC): Subscriber Privacy, Radio Network Security, Authentication Enhancements, Interworking & Roaming Security, API Security, Network Slicing Security, Application Security, and Internet Security Protocol Recommended Practice.
2. **Security capabilities**. It describes a technical security feature which is important and relevant to commercial or private 5G networks. Each capability is associated with a security category. For example, Radio Network Security includes User Plane Integrity Protection (5GSC-2.1), and Cryptographic Algorithms Recommended Practice (5GSC-2.2).
3. **Mitigated threats and vulnerabilities**. Each security capability is intended to help mitigate certain types of threats and vulnerabilities to reduce overall risk. The model combines security with vulnerabilities and corresponding threats and briefly describes mitigation actions. For example, for Radio Network Security:
    a. 5GSC-2.1
        i. Threat/Vulnerability: user plane traffic between the device and network was not protected in earlier generations.
        ii. Mitigation: The enablement of user plane integrity protection prevents this type of threat. The support of this feature is mandatory for both the device and the network, while its use is optional and under the control of the operator.
    b. 5GSC-2
        i. Threat/Vulnerability: A network operator is limited to the cryptographic algorithms supported in the equipment deployed in its networks.
        ii. Mitigation: The implementation of both AES and SNOW3G-based algorithms and a switching mechanism to be triggered whether the configured algorithm is found to be weak.

2.2.3.1.1 Limitations

The NCCoE model exhibits some limitations for its application in the NATWORK ecosystem. The main constraint comes from its practical approach to demonstrate security over a 5G standalone (5G SA) network deployment, which restricts the threats and vulnerabilities to those that can be effectively validated on the testbed. Besides, the scope of the model does not contemplate possible 6G threats such as those based on AI, an expanded attack surface from IoT and eXtended Reality (XR), or threats from edge environments. For the physical layer, it does not offer robust countermeasures against RF spoofing and adequate anti-jamming protection solutions and does not explicitly address either adversarial ML threats (e.g., manipulating training data) or beam-level security.

2.2.3.2 ETSI Threat classification

The 3GPP, through the *3GPP TR 33.926 Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes* [18], provides a comprehensive threat analysis and identification of critical assets for 3GPP network product classes, supporting the Security Assurance Specifications (SCAS) framework used in 5G and LTE security evaluations. The key concept is the **GNP Class** (Generic Network Product Class), defined as "a class of network products that all implement a common set of 3GPP-defined functionalities for that particular network product." The technical report covers the following aspects:

1. **Threat Landscape for 3GPP Network Products**. Identifies and categorizes threats relevant to network functions such as Access and Mobility Management Function (AMF), Session Management Function (SMF), User Plane Function (UPF), Network Exposure Function (NEF), Unified Data Management (UDM).
    a. Includes both **external** and **internal** threat vectors.
2. **Critical Asset Identification**
    a. Defines what constitutes a **critical asset** in each network function.
    b. Examples include subscriber data, session and mobility state, authentication credentials, network configuration, and policies.
3. **Security Objectives**. Maps threats to **security objectives** such as confidentiality, integrity, scalability, accountability
4. **SCAS Alignment**. Supports the development of **Security Assurance Specifications (SCAS)** by providing: Threat models; Asset classification; Security requirement mapping
5. **Use in Certification**. Used by network equipment vendors and certification bodies to assess compliance with 3GPP-defined security requirements.

More specifically, regarding threats, they can be categorized using the STRIDE model (**S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, **E**levation of privilege), and are grouped into:

1. **Generic Threats (Applicable to All Network Functions).** These threats apply to all Generic Network Products (GNPs), including:
    a. Spoofing: default accounts, weak passwords, IP spoofing, malware, eavesdropping.
    b. Tampering: software tampering, log tampering, OAM traffic tampering, session tampering.
    c. Repudiation: lack of user activity trace.
    d. Information Disclosure: poor key management, insecure storage, unnecessary services, log disclosure.
    e. Denial of Service: misbehaving UEs, implementation flaws, insecure services, human error.
    f. Elevation of Privilege: over-privileged services, folder permission abuse, insecure network services.
2. **Threats Specific to Service-Based Architecture (SBA) Interfaces**
    a. JSON Parser Exploits: Execution of malicious code via JSON.
    b. Access Token Misuse: Applies to incorrect verification or replay of tokens.
    c. Client Credential Assertion Failures: Improper validation leading to spoofing or privilege escalation.
3. **Threats by Network Function Class.** Each annex in the document details threats for specific network functions. Examples include:
    a. AMF (Access and Mobility Management Function), which considers bidding down attacks on NAS security, failure to allocate new 5G-GUTI, incorrect validation of S-NSSAIs, and the use of NULL integrity protection outside emergency scenarios.
    b. UDM (Unified Data Management), which considers incorrect SUCI de-concealment, synchronization failure, and misconfigured UP security policies.
    c. AUSF (Authentication Server Function), which includes generic threats apply; no additional specific threats listed.
    d. SEPP (Security Edge Protection Proxy), which includes misuse of cryptographic material, incorrect handling of PLMN ID mismatches, and exposure of confidential IEs in N32-f messages.
    e. SMF / UPF (Session and User Plane Functions), which considers TEID and Charging ID uniqueness failures, weak or missing protection on N3/N4/N9 interfaces, and malformed GTP-U message handling.

In the specific case of the **gNB/eNB (Radio Access Network Nodes)** (Annex D), the document indicates that critical assets specific to the gNB to be protected are as follows

1. gNB Application;

2. Mobility management data: including subscriber identities (e.g. SUCI, GUTI), subscriber keys (i.e. KUPenc, KUPint, KRRCenc, KRRCint, NH), authentication parameters, APN name, data related to mobility management like UE measurements and UE's IP address;
3. User plane data;
4. The interfaces of gNB to be protected and which are within SCAS scope: N2, Xn, N3, Uu, Console interface (for local access), and OAM interface;
5. gNB Software: binary code or executable code.

Annex D also describes the threats related to control plane and user plane in the network for the gNB, which are categorized according to the STRIDE model:

1. gNB control plane data confidentiality protection (TID)
2. Control plane data integrity protection (TD)
3. User plane data confidentiality protection at gNB (TI)
4. User plane data integrity protection (TD)
5. AS algorithm selection and use (TID)
6. Bidding down on Xn-Handover (TID)
7. Key Reuse (I)
8. Security Policy Enforcement (TI)
9. State transition from inactive state to connected state (D)

2.2.3.2.1 Limitations

Though it provides a structured framework for identifying threats and critical assets across various 3GPP network product classes, the ETSI model does not include very relevant threats for the radio interface such as jamming, spoofing, or side-channel attacks. These are very relevant in 6G given the large surface attack caused by both IoT devices and additional frequency bands. Additionally, the ETSI model does not cover threat models for AI/ML-based components. The asset classification introduces another limitation, as it is relatively static and does not adapt to highly dynamic 6G environments (e.g. a UAV can be a UE or can carry a gNB).

3 NATWORK Physical Layer Threat Model

3.1 Methodology

After the review conducted in the previous sections, for NATWORK Physical Layer Threat Modelling we adapt the O-RAN methodology informed by the IEEE 3349 to better reflect the specifics of physical layer. Thus, the updated methodology is the following:

1. **Identification**
    a. **Assets:** Assets should list the NATWORK components and interfaces implementing physical layer functionalities along with their sensitivity level.
    b. **Threat Actors:** Actors threatening physical layer assets should be identified
    c. **Threats:** Threats that align with the STRIDE model and are highly relevant to PHY-layer vulnerabilities should be identified
    d. **Vulnerabilities:** Known vulnerabilities of the physical layer assets should be collected from the previously discussed threat models. Additionally emerging vulnerabilities should be identified in the relevant literature.
2. **Known Mitigation Methods:** Known mitigation methods to the above physical layer vulnerabilities should be identified.
3. **Risk Assessment:** Quantify risk with respect to physical exposure, attacker capabilities (e.g., RF equipment, physical access), and impact on NATWORK system.
4. **Risk Mitigation:** Apply relevant mitigation methods to reduce risks.

In the following sections we provide detailed analysis of each of the steps.

3.2 Assets

This section provides a brief description of what NATWORK devices and components constitute a PHY attack surface and their degree of sensitivity.

3.2.1 Assets under Spoofing and Eavesdropping

The devices that transmit or capture raw radio-frequency signals form the primary physical attack surface, because they can be fooled by forged waveforms or quietly monitored in the field. Under spoofing and eavesdropping, the **highest-sensitivity group** is made up of RF components: the Software-Defined Radio (SDR) used for V2X and other 5G/6G bands, the in-vehicle modem, and the main and auxiliary antennas that connect those radios to the air. Replay attacks or passive IQ collection against any of them can instantly undermine confidentiality, integrity, and availability. That same high tier also covers short-range radios embedded in IoT sensors, which broadcast telemetry openly, as well as programmable data-plane devices (P4 switches or SmartNICs) whose

packet mirroring or rule spoofing leaks traffic as effectively as an RF sniffer. Even the SDN/P4 fabric switches that orchestrate network slices belong in this category, because a single forged flow-table or mirror entry exposes entire slice flows.

Medium-sensitivity assets do not carry user payload directly, yet they still steer or observe the radio link in ways an attacker can exploit under specific circumstances. A Reconfigurable Intelligent Surface, for instance, can be re-tuned to favour a hidden listener. On other hand Global Navigation Satellite System (GNSS) or PTP time sources sometimes accept external signals whose legitimacy needs verification, and vehicle buses such as CAN or GNSS could be persuaded to report inaccurate speed or position. Comparable care applies to Near-RT RIC xApps, edge gateways bridging BLE/Wi-Fi to Ethernet, and cloud or edge servers hosting MEC UPFs or analytics. While scenarios like ARP/DHCP spoofing, forged MAC/IP frames, GTP-U tunnels, or timing-side channels are largely mitigable through authentication, access control, and observability, they remain design considerations. Even TPM/Keylime attestation calls for attention: ensuring quote validity and protecting the attestation channel helps keep placement decisions reliable.

At the **low-sensitivity tier** we find dashboards and monitoring tools, for example: the Green-Energy Monitor, the MMT-Operator console, Prometheus metrics and similar probes. Forged telemetry can mislead operators or leak alert content, but it will not expose raw radio frames or critical traffic. These endpoints must still be authenticated and encrypted; however, expanding them widens the attack surface far less than exposing radios, antennas, timing sources or programmable data-plane devices.

3.2.2 Assets under Jamming and Physical tampering

Regarding jamming attacks, just like the previous ones, the physical layer is the interface where those attacks take place, as this type of attack is intentional interference created by an external device with the objective of degrading the channel. Focusing on the NATWORK Use Cases (see deliverable D2.2: 6G Use Cases scenarios and requirements), the **highest-sensitivity assets** to this attack are the radio components:

1. **In UC2,** its wireless link between the gNB (notably the USRP B210 SDR) and the UE, in this case an autonomous vehicle (AV) and its sensors (GPS, LIDAR, etc.) is a critical vulnerability. Jamming can affect both the control and the operational safety of the vehicle. The RIS can also be attacked and even used to redirect the jamming to the UE or gNB.
2. **In UC3,** all IoT devices are sensitive to this, especially those with power constraints, which make it easier for the jammer to effectively interrupt their communication with the gNB, which is also a sensitive target. Even the sniffer can be attacked as it is a wireless device too.

3. **In UC4,** the New Radio (NR) equipment of the RAN gNBs, their USRPs and the UEs ones, which also include the drone used for URLLC, are all potential targets to a jamming attack with critical consequences.

Physical tampering is a completely different type of attack, as it means that an attacker has unauthorized physical access to an asset, damaging or modifying it. In contrast with the previous ones, this attack will be ineffective against wireless communications themselves but will instead affect the physical devices or wired communications. In UC1, the software components are not sensitive to physical tampering, but the servers where they are deployed are, as disrupting them could make the whole NATWORK services fail, and the VPN connection between them lets an attacker access the whole set of servers. In UC2, unauthorised access to the gNB components or the AV would compromise the whole system, and the RIS can also be physically compromised. In UC3, manipulating or damaging the sniffer would be critical for the system, and physical access to the servers can cause the system to fail too. In UC4, once again the servers will be a high sensitivity component, same as the switches, the SDRs and the UEs.

3.3 Threat Actors

Threat actors can be a broad concept, but when we talk about the physical layer, PHY-layer, of a wireless system, we are talking about those who disrupt or block legitimate communication by introducing radio signals, known as jamming signals. They aim to interfere communications using different types of attacks. For example, DoS attacks flood communications, blocking other legitimate users from using the network. Previously, we have described the different attacks, explaining the STRIDE attack compendium. We can divide the actors as follows:

1. **Cyber-criminals:** Individuals who commit cybercrimes using of hardware either as a tool or as a target or as both.
2. **Hacktivists:** Represents actors that perform cyber-attacks for political or social gain.
3. **Nation-State**: actors aggressively target public and private sector networks and gain permanent access to them to compromise, steal, modify or destroy information.

Various examples can be mentioned. For instance, in the field of warfare, we have seen countries blocking communications so that the enemy cannot be detected using satellite images. This does not involve our field of action, as we do not work via NTN. But it is worth mentioning that wireless systems go beyond 5G NR.

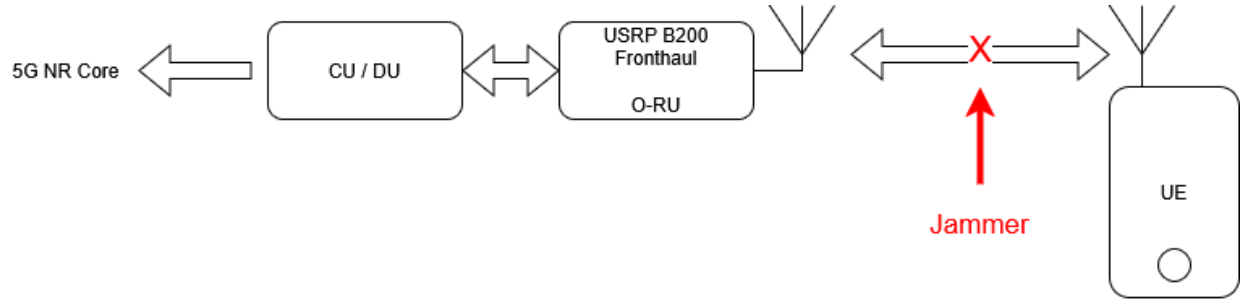

Figure 5 Jamming attack location in a wireless communication system.

To provide another example, Figure 5 above shows the threat actors in a jamming attack. As electronics are becoming more accessible to everyone, both economically and logistically, solutions such as a Universal Software Radio Peripheral (USRP) are a good starting point for attackers. In any case, hardware is becoming cheaper all the time, so even a custom PCB with a few RF components is inexpensive given the damage that could be done. In addition, software is becoming easier to build with open-source software or free tools. So, we are reaching a point where a single man can design a very complex system. To give an idea, the design of an electronic radio frequency system used to be complex, while today we have free tools that can simulate the behaviour of this system, ensuring that the radio link performs well.

Technology is evolving very rapidly. We must be prepared for many different scenarios, including attaching a jammer to a drone, for example. In this way, the attacker can get closer to the legitimate link.

3.4 Characterization of Threats

Threats that are highly relevant to PHY-layer vulnerabilities are identified in this section.

3.4.1 Jamming

Jamming attacks are a type of DoS (Denial of Service) attack on the physical layer, defined as intentional interference with a specific wireless signal. This is done by a device called jammer, which produces a high-power signal that deteriorates the received Signal to Interference and Noise Ratio (SINR) with the objective of decreasing the success of communication.

Jamming attacks are prevalent in literature and can be classified from different perspectives, as shown in the following diagram in Figure 6, presented in [19], which shows how jamming attacks can be categorize depending on the applied criteria:

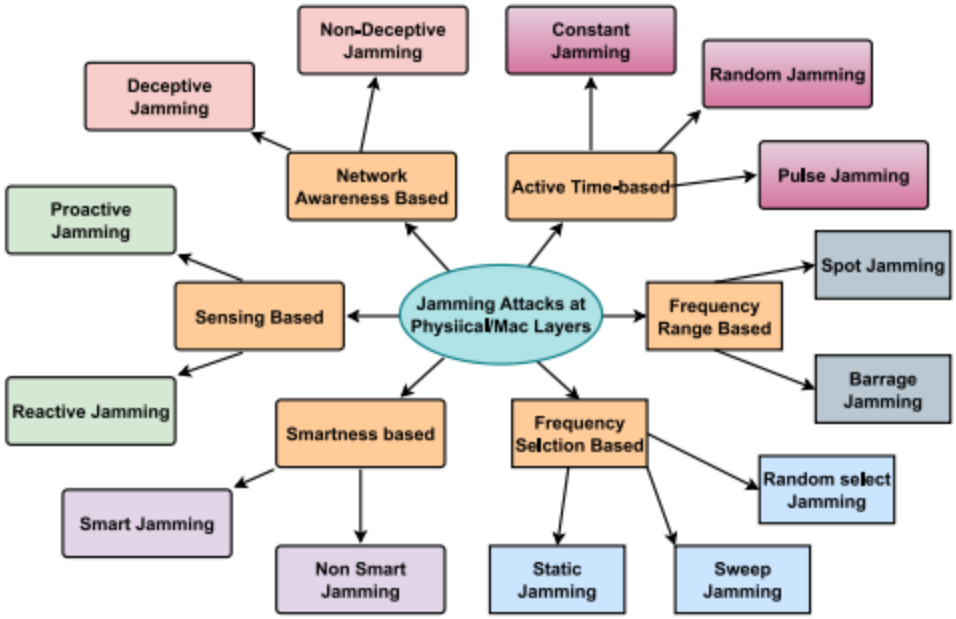

Figure 6 Types of jamming attacks

1. **Sensing-based jamming attacks**: divided into reactive and proactive jamming. The former one activates in response to the sensing of activity on the channel (minimizing detection risk and power consumption), while the last one transmits its signal without considering if there is an ongoing communication (simpler and effective with communication systems with known transmission patterns).
2. **Network-awareness jamming attacks:** deceptive and non-deceptive. Deceptive jamming uses the knowledge of the network to transmit jamming signals that imitate characteristics of the legitimate signals. On the other hand, non-deceptive jammers try to disrupt communication without trying to deceive the attacked system.
3. **Active-time-based jamming attack:** constant, random and pulse. Constant jammers maintain the interference on a frequency bandwidth continuously. Random jammers change their frequency and timing randomly. Pulse jammers transmit on periodic bursts increasing energy efficiency and reducing their detection probability.
4. **Frequency range-based jamming attack**: spot and barrage. Spot jammers transmit all their power on a single frequency at a time, while barrage jammers target several different frequencies (dividing its total power between them, making it less effective).
5. **Frequency selection-based jamming attack**: static, sweep and random select. Static jamming affects always the same frequency but is easy to detect and avoid. Sweep jammers shift their frequency to attack a range of different frequencies (the typical example is the chirp signal, which uses a tone-like signal to go over a set bandwidth, minimizing its energy consumption).

6. **Smartness-based jamming attack**: smart and non-smart attacks. Smart jammers use intelligence and adaptability to create their interference signal, in contrast with jammers that use simple and static methods.

Focusing on the 5G NR architecture, jamming can be applied to a whole set of different physical signals. As the literature has explored [20], [10], some 5G channels are more sensitive to jamming than others. Synchronization signals, like the ones present in the Signal Synchronization Block (SSB) used for downlink synchronization in 5G, are easy for an attacker to locate, are unencrypted, have a reduced frequency and time span (making them less energy demanding for the jammer) and have relatively low resistance to jamming.

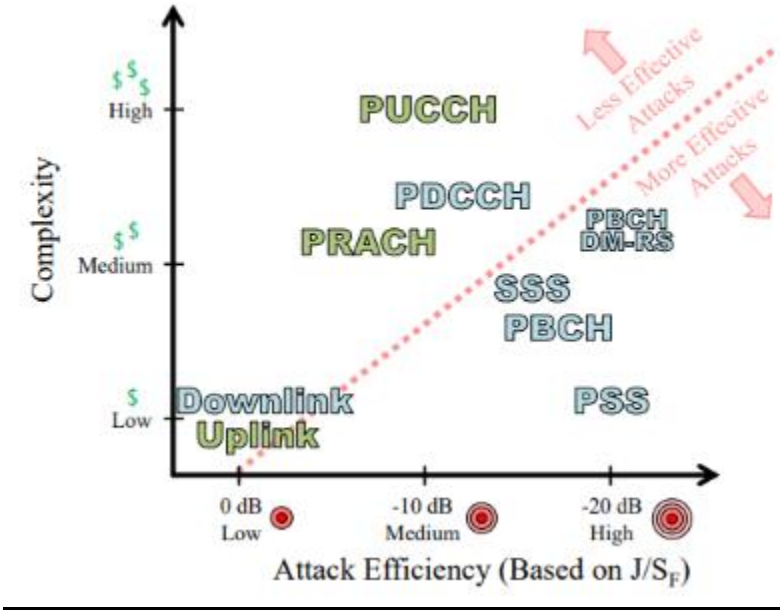

Figure 7 Ranking of the physical layer attacked signals

PBCH DM-RS is considered as the most efficient target for jamming due to being only 25% of the PBCH resources (which is part of the SSB). Outside of the PBCH, PDCCH, PRACH and PUCCH are the best targets from the jammers' perspective, having in common that they transmit control information needed to synchronise and share control information between the UE and gNB.

It is important to note that although the use of AI-based strategies is more prevalent to detect and mitigate jamming attacks, some strategies use it to improve the performance of the jammer, like using adversarial machine learning. In [28], the authors describe how it is possible to learn the transmission pattern of legitimate communication with an "exploratory attack" by observing the spectrum and using Deep Learning and they cite a previous paper which performs a jamming attack during the data transmission period. In a similar fashion and from what [28] reports, jamming can be used as an "evasion attack" during the test phase, providing incorrect input data

in the sensing phase, causing the allocation algorithm to misjudge the resource as not available (being more energy efficient than jamming the signal). If the allocation algorithm requires a training phase, the paper also explains that “causative attacks” can be done if the jammer determines the start and end of that training phase, which would cause mistakes in the classification of time-frequency RBs for example. In [29] a DRL-based (Deep Reinforcement Learning) jamming attack is presented, which adapts its policy in real time to target gNB-allocated RBs.

3.4.2 Eavesdropping

Eavesdropping is a passive threat in which an adversary or attacker intercepts transmissions to obtain control or data information without altering the signal or being detected [30]. It is classified as a fundamental radio threat among the principal 5G security concerns. In the context of 5G/6G physical-layer security, eavesdropping is also recognized in an active attack when the attacker transmits or injects signals to manipulate channel estimation [30].

In passive eavesdropping, the attacker listens to leaked energy of transmissions and may position itself near a relay to capture high-quality copies of every frame before it reaches the intended recipient. Even when payloads are encrypted, traffic-analysis attacks harvest metadata (timing, packet lengths, control-channel usage) to infer user identities or application patterns, making IoT and dense 5G scenarios somewhat more vulnerable than others [31]. In massive-MIMO deployments, highly directional beamforming pushes the secrecy capacity close to the legitimate-user capacity, so a passive eavesdropper gains little unless it is co-located within roughly half a wavelength of the user [32].

Active eavesdropping undermines core physical-layer procedures. In pilot-contamination attacks, an active eavesdropper transmits the same uplink pilot sequences as the victim UE, biasing the gNB’s channel-state-information (CSI) estimate so that downlink beamforming inadvertently steers energy toward Eve [32]. Random-pilot tests and a cooperative BS-UE handshake proposed for massive-MIMO can detect such injections with good probability at moderate SNR, restoring the secrecy advantage [32].

Beyond intercepting traffic, adversaries can abuse RF sensing itself as a side-channel. Recent mmWave, RFID and UWB-based systems reconstruct speech from sub-millimetre surface vibrations or infer keystrokes via multipath-CSI analysis, allowing through-wall surveillance and password theft without injecting packets [33].

Furthermore, legitimate nodes can harvest the same channel randomness to derive shared secrets through physical-layer key generation (PKG). Recent indoor experiments using FMCW chirps demonstrate a full PKG chain (CSI extraction, quantization, reconciliation, and SHA-256 privacy amplification) while a passive eavesdropper records the entire exchange. Results show

that the conditional min-entropy drops sharply when the attacker is within two to six wavelengths, challenging the classical λ/2 decorrelation assumption and capping the final key rate in some scenarios [34].

Adversaries are now leveraging AI-based threats to automate and scale interceptions. Deep learning and adversarial-ML models can infer CSI from sparse reference signals, classify modulation and coding schemes, reconstruct obfuscated waveforms, and automate traffic-pattern analysis, even when networks employ randomization or obfuscation countermeasures. Comprehensive reviews of adversarial ML in wireless communications highlight the unique vulnerabilities of RF data to adversarial examples and poisoning, showing how attackers can stealthily subvert deep-learning classifiers and extract sensitive information from minimal clues [38].

3.4.3 Spoofing

Spoofing refers to malicious behaviour in which an adversary impersonates a legitimate user or device aiming to compromise the core information security goals confidentiality, integrity and availability [21]; in the context of 5G and beyond 5G infrastructures, the primary actors include users seeking access to a mobile network operator's services, 5G base stations facilitating connectivity and a computationally bound adversary operating under standard security assumptions. The attack surface is thus constrained to unencrypted communication channels, *i.e.*, to certain messages in the signalling plane used to initiate authentication processes and to allocate down- and uplink resources. Exploiting any of these may result in a denial-of-service for a targeted UE or prevent UEs from establishing connections with the base station [22],[23].

For instance, the Primary and Secondary Synchronization Signals (PSS and SSS) are critical for enabling a UE to identify and synchronize with a serving cell and are broadcasted in the Synchronization Signal Blocks (SSB) [24].Author in [10] notes how the 5G NR specifications omit to define UE behaviour, when a PSS is not followed up by an SSS. Consequently, scenarios in which a UE receives spoofed SSBs lacking the SSS component could lead to connection failures, particularly if the UE implementation does not explicitly handle such cases. Furthermore, by spoofing the contents of Master Information and System Information Blocks (MIB and SIB, respectively) an adversary could provoke a UE to waste time attempting to connect to a bogus cell, effectively resulting in a DoS (*Cf*. *Figure 5* for an illustration of such a spoofing attack).

Moreover, Bitsikas and Pöpper leverage the fact that MIB and SIB messages are broadcasted in plain text and that unverified measurements reports for UEs in the handover procedures. Consequently, the handover process is susceptible to spoofing and can result in DoS, resource drain and man-in-the-middle attacks [25]. The 5G positioning process includes unauthenticated positioning reference signals (RPS) which thus, can be spoofed. According to Gao et. al's experiments, the average accuracy for positioning is less than 1 meter; using a selective PRS

spoofing attack can result in positioning errors of more than 4 meters per spoofed gNB. The consequences of this vulnerability may be detrimental. *E.g.*, ultra-reliable low latency communication (uRLLC) may extensively rely on positioning for self-driving cars where such a spoofing may provoke road accidents [25].

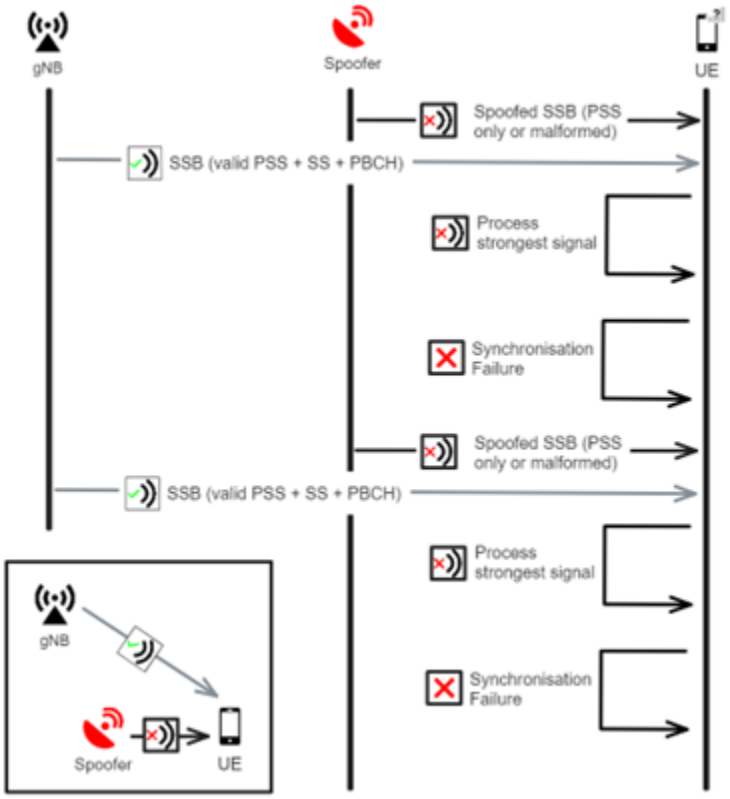

Figure 8 Spoofing Attack leveraging implicitly trusted pre-authentication messages

In a second threat model, an adversary can leverage NSO Group's Pegasus technology through what they dubbed *tactical network equipment* in a leaked product description in 2015 [26] – essentially rogue base stations. While 5G significantly enhances defence against spoofing through mutual authentication and encryption of user plane data [28], it does not protect against an insider threat, *i.e.*, this adversary controls the network operator's equipment. Amnesty International reported on several occasions where such spoofing attacks allowed nation-state sponsored adversaries to install malware on a victim's device [35],[36]. Moreover, 5G networks are anticipated to consist of an unprecedented number of connected and heterogeneous devices enabling an ever-wider range of use cases, which consequently expands the attack surface [37]. Even if the specification itself is sound, *i.e.*, its protocols do not introduce vulnerabilities, their implementation might be insecure, as demonstrated by a report published by Makkaveev. Adversaries could exploit vulnerabilities in digital signal processors to access *i.e.* microphone data and trigger a kernel panic to force a reboot of the victim device.

3.4.4 Physical tampering

The National Institute of Standards and Technology defines tampering as "*[a]n intentional but unauthorized act resulting in the modification of a system, components of a system, its intended behaviour or data*" [39]. 3GPP outlines the security features and procedures for 5G networks in the technical specification 33.501. Among these, they specify requirements towards physical security mechanisms concerning the UE and base stations to render physical tampering useless.

On the UE side, they mandate the usage of tamper resistant hardware components that hide subscription credentials. For example, even if a UE falls into the hands of an adversary, extracting the long-term keys, or the modification of the code run by the digital signal processing (DSP) component must not be possible. Furthermore, critical functions such as authentication algorithms must be executed within a secure environment and compliance to the requirements must be auditable [27]. The supply chains of modern smartphones consist of a plethora of independent and hyper-specialized manufacturers [40]. This intricate web of suppliers increases the attack surface and presents a significant challenge for implementing robust threat mitigation measures [39]. Qualcomm, for instance, produces radio frequency transceivers that provide cellular network and other connectivity to the operating systems on dedicated chips – so-called systems on a chip (SoC). To comply with TS 33.501, they designed authentication procedures for the firmware run on the SoC and the startup comprises of three main stages: Primary Boot Loader (PBL), Extended bootloader in RAM (XBL) and initialization of further functions like power management. The initial stage is secured by immutable read-only memory (ROM); *i.e.*, the PBL is directly embedded within the SoC and includes only the minimum functionality required to load, verify and run firmware. Without a valid signature of the OEM (and Qualcomm if "double signing" is required), the PBL refuses to load firmware into memory. The Secure Boot uses public key encryption, more precisely X.509 certificate chains [41]. Moreover, they implemented access-control that follows the least-privilege principle. In other words, the firmware of each component within or interacting with the SoC is only allowed to read and write data that is critical for it to function [41].

Anti-tampering mechanisms of base stations, on the other hand, need to accommodate the risks associated with physical or remote access from unauthorized personnel during the operations and maintenance processes. For starters, the setup and configurations of gNBs must be authenticated and authorized leveraging public key cryptography. All communication with other entities must follow the zero-trust principle; i.e., gNBs must authenticate entities in the 5G Core and vice versa. Furthermore, the transfer of software to gNBs e.g. to apply a patch for a vulnerability, must occur through encrypted and integrity protected communication channels. Sensitive data such as encryption key material, user plane, and control plane data must occur within a secure environment where access to the (memory) location is restricted physically [27].

While 3GPP TS 33.501 mandates a zero-trust architecture and enforces the principle of least privilege to mitigate unauthorized access, the technical safeguards can still be circumvented if, e.g. employee credentials are stolen through phishing. Even more insidious is the insider threat that can be personified by corporate spies, opportunistic, and disgruntled employees. To mitigate this threat, access to critical resources ought to be monitored and anomalies must be detected [42][43]. Finally, many employees (intentionally) violate information security policies; therefore, roughly 25% of cyber incidents result from information security policy violations [44].

3.5 Vulnerabilities

This section describes the vulnerabilities of the NATWORK PHY layer. We start by identifying well-known vulnerabilities of the physical layer assets which can be exploited by known attacks such as jamming or spoofing. Then, we move into presenting the emerging vulnerabilities, which we identified as RIS and MIMO, virtualization and AI related vulnerabilities.

3.5.1 Existing vulnerabilities in protocols and standards

Vulnerabilities in the physical layer of wireless communication systems are critical as they form the underpinning of all higher layer protocols. If communication is blocked or affected in the PHY layer, other mitigation measures become useless in upper layers. When these vulnerabilities are exploited, attackers can compromise confidentiality and integrity.

Most wireless physical layer protocols (e.g., IEEE 802.11, LTE, 5G NR) do not implement authentication mechanisms at the physical layer. This allows rogue transmitters to inject malicious signals. There are also spoofing attacks where attackers masquerade as legitimate transmitters.

In systems such as MIMO and massive MIMO (e.g., in 5G), attackers can spoof pilot signals during channel estimation, resulting in incorrect beamforming or degraded QoS. This is often referred to as pilot contamination.

Physical layer signals are broadcast by nature, making passive eavesdropping trivially easy unless higher layer encryption is applied. Directional antennas, beamforming or physical layer security (PLS) approaches are not widely adopted yet.

3.5.2 RIS and MIMO specific vulnerabilities

3.5.2.1 RIS Vulnerabilities in PHY Layer

6G wireless networks are expected to support applications with strict requirements such as autonomous driving, wireless power transfer, and extended reality. To reliably serve these applications, it is essential to minimize factors that introduce randomness into the network's quality of service. One major factor is the wireless propagation environment, which affects

performance through path loss, shadowing, and fading. The concept of programmable wireless environments (PWEs) addresses this by treating wireless propagation as a software-defined process. By dynamically controlling the propagation environment, PWEs mitigate the adverse effects of these stochastic phenomena, ensuring more stable and reliable network performance [45]. This approach transforms the wireless medium from a passive conduit into an active network participant.

The key technology enabling PWEs is Reconfigurable Intelligent Surfaces (RISs). A RIS unit offers real-time, software-defined control over the electromagnetic energy radiated by transmitters [46], thereby managing wireless link characteristics such as scattering from moving or stationary objects and significantly improving quality of service.

To convert traditional networks into PWEs, multiple RIS units must be deployed across various planar surfaces. Each RIS acts as a node in the propagation path, enabling dynamic control and enhanced resource allocation. Notably, RISes can reconstruct line-of-sight channels between base stations and users [46], create “quiet zones” to block signals in specific areas for improved physical layer security, and utilize sensing capabilities to detect and locate objects. Additionally, by ensuring that the signal's angle of arrival remains perpendicular to the trajectory of a moving user, RISes can mitigate the Doppler effect [47], which is particularly significant in vehicle-to-everything communications.

RIS technology is based on metamaterials—engineered structures made of basic units called unit cells. On a macroscopic level, a RIS is a thin, planar, rectangular tile consisting of an array of these unit cells. Each tile contains active elements, such as PIN diodes, which enable software-defined manipulation of impinging electromagnetic waves. When an EM wave strikes the RIS, it induces a current distribution that depends on the state of the active elements (the configuration). By selecting the appropriate configuration, the RIS can control the incident wave, yielding various macroscopic responses, or functionalities, such as beam steering, beam splitting, perfect absorption, modulation of phase, amplitude, or polarization, and wavefront sensing.

Computing the optimal RIS configuration for a given functionality is a complex and time-intensive optimization problem, making real-time computation impractical. Instead, this process is performed during manufacturing, where supported functionalities are matched with optimal configurations using simulation tools or prototype measurements. This procedure is known as codebook compilation. The resulting mappings are stored in a codebook database, allowing the RIS to quickly retrieve the corresponding configuration during operation.

In addition to the benefits of RIS integration, several physical-layer vulnerabilities have been identified. The most significant of them are the following:

1. **Reflection in undesired directions**: The imprecise phase tuning during manufacturing or suboptimal configuration may cause the RIS to reflect incident signals in unintended directions. Such misdirected energy can degrade performance for legitimate users and, worse, enhance the signal for a malicious receiver [48].
2. **Jamming and Interference**: The RIS units are also vulnerable to jamming. Because they are passive, an adversary can inject noise onto the RIS surface. This interference not only degrades the intended signal but may also be re-directed by the RIS, exacerbating the problem [49].
3. **Attack on RIS controller**: Another critical issue is the dependency on a dedicated controller that retrieves and applies pre-computed configuration data. This controller represents a single point of failure that is exposed to both physical and cyber-attacks. Compromising it could negate the security benefits provided by the RIS [50].
4. **Denial of Service (DoS) attack**: Since each RIS is designed to serve multiple users, its capacity is inherently limited by the number of active reflecting elements. An overload of access requests at the RIS controller can lead to a DoS attack, further compromising network reliability [51].

As concerns the reflection in undesired directions, RIS technology uses many low-cost passive elements to steer incident electromagnetic waves toward desired directions via adjustable phase shifts. In theory, such beamforming enhances signal quality, extends coverage, and improves energy efficiency. In practice, however, errors in the configuration process may result in portions of the transmitted energy being reflected toward undesired directions. This phenomenon can create interference for legitimate users and inadvertently benefit malicious receivers by providing unexpected signal paths.

The sources of this imperfection could be various. The main sources are presented below:

1. **Manufacturing and calibration errors**: During the manufacturing process, the discrete nature of the tuneable elements and tolerances in the design can lead to inaccurate phase shifts. Inadequate calibration procedures make these errors worse, so the actual phase responses don't match the expected ones.
2. **Phase noise and environmental variations**: The RIS elements are subject to phase noise and environmental variations (e.g., temperature or humidity changes) that alter the effective phase shift. Modelling these factors reveals that even small deviations can cause significant leakage into unintended spatial regions.
3. **Algorithmic limitations**: The optimization algorithms used to compute the phase configuration often assume ideal hardware. When real-world imperfections are present, the reflected beam may broaden or deviate from its intended direction, resulting in energy spillover into regions where no legitimate users are located.

Undesired reflections reduce the effective power focused on intended users, degrading link quality and overall network throughput. From a security standpoint, leaked energy may be intercepted by unauthorized parties, thereby increasing the risk of eavesdropping or even facilitating targeted jamming attacks. Such vulnerabilities challenge the fundamental promise of RIS-aided secure communications.

Additionally, a jamming attack can take place when a RIS is deployed as a jammer to reduce the Signal to Interference Noise Ratio (SINR) at the Legitimate Receiver (LR). Unlike traditional active jamming attacks that rely on their own energy to flood the victim system with strong noise signals, this RIS-enabled jammer exploited the victim system's signals by modifying their phase shifts and reflection coefficients. This RIS-based jamming attack leaves no trace, making detection and prevention more challenging and complex.

An Environment Reconfiguration Attack (ERA) is a novel jamming technique where an attacker manipulates the RIS to rapidly alter the electromagnetic propagation environment, disrupting legitimate receivers (LRs). By reflecting legitimate signals, the RIS provides the adversary with a major advantage over conventional jamming, removing the need for active jamming signal transmission. An RIS-aided manipulation attack targets the key generation rate (KGR) by having an active attacker, Eve, rapidly alter RIS phase shifts to disrupt the wireless environment. To evaluate the vulnerability of conventional key generation techniques under this attack, the authors analysed the channel frequency response coefficient.

Signal leakage attack uses Illegal Reconfigurable Intelligent Surfaces (IRISs) to increase the eavesdropping data rate. The IRIS passively enhances communication quality of illegal links and degrades the performance of Physical Layer Security (PLS) without generating an extra RF signal. For this reason, it is quite difficult to detect and prevent signal leakage. Interference attack involves the use of IRIS to transmit the interference signal that severely degrades the SINR at the LU. Similarly, it is very difficult to cancel interference signals from IRIS. Eavesdropping occurs when an attacker attempts to intercept information exchanged between communication nodes.

Regarding the attacks on RIS controller, in general [52], RIS-aided communication systems have simpler transmitter and receiver designs than traditional relay networks. However, altering an RIS's electromagnetic properties for reflection and refraction can introduce new security threats. If an attacker gains control of an RIS's microcontroller, it can be reconfigured for malicious purposes. Additionally, adversaries can manipulate signals in the time and frequency domains to disrupt or intercept legitimate user transmissions.

Specifically, [53], RIS based Pilot Contamination Attack (PCA), when an eavesdropper (Eve) injects malicious pilot signal, changes the channel estimation result, and effectively reduces the transmission performance in the downlink and this way, facilitates Eve in capturing information

via spoofing [54]. Pilot Spoofing Attack (PSA) is when an active eavesdropper launches an identical training sequence to manipulate the channel estimation outcome during the pilot training phase. In this case, RIS phase shifts are optimized in favour of Eve, making her the primary recipient of reflected signals. Unauthorized access to the RIS controller is possible due to the absence of an identification system, allowing malicious signals to be transmitted to users and potentially influencing their decision-making processes. An adversary can also exploit remote access and malware injection to compromise the RIS controller and tuneable chips, altering chip parameters that control RIS phase shifts and amplitudes.

Additionally, an attacker can manipulate electromagnetic waves, leading them to an undesired direction or creating destructive interference, by adjusting RIS controller functions. RIS enhance wireless networks but face challenges due to the high overhead required for channel estimation and phase shift optimization that could also lead to DoS. Existing studies overlook this issue in for the resource allocation aspect.

The final vulnerability in RIS-assisted networks are DoS ones that pose a significant threat to network security by exploiting the limited capacity of RIS controllers and the passive nature of RIS units. As outlined in [51], attackers can optimize RIS reflection coefficients to introduce harmful interference, severely degrading SINR and rendering legitimate communications unreliable. A key vulnerability lies in the RIS's inability to process and authenticate multiple access requests simultaneously, as its reflecting elements have a finite capacity. This limitation enables adversaries to launch an access overload attack by flooding the RIS with excessive connection requests, forcing the controller into an unstable state where it fails to optimize phase shifts effectively. The massive number of simultaneous reflection requests depletes RIS processing resources, leading to a breakdown in network coordination and communication failures for legitimate users.

Additionally, the paper emphasizes how a malicious RIS can disrupt MIMO systems through passive jamming strategies, where attackers manipulate phase shifts to maximize inter-user interference during downlink transmissions. By tuning the RIS reflection coefficients, an attacker can steer harmful signals toward specific users, intensifying symbol error rates (SER) and preventing correct data reception. The RIS remains undetectable during channel estimation phases, as it does not introduce additional power, making mitigation efforts significantly more complex. When combined with pilot contamination or spoofing, RIS-based DoS attacks become even more severe, preventing legitimate users from obtaining accurate CSI, which is critical for beamforming and signal optimization.

3.5.2.2 MIMO Vulnerabilities in PHY Layer

MIMO technology has significantly enhanced wireless communication systems by improving data rates, spectral efficiency, and overall system reliability. But despite these benefits, MIMO systems

face several challenges at the physical layer that can affect performance and network security. More specifically:

1. **Channel Estimation Errors (caused by pilot contamination & eavesdropping):** MIMO systems require accurate channel estimation for efficient beamforming and interference management.
2. **Pilot contamination:** It occurs when non-orthogonal pilot sequences are reused across cells, leading to interference and incorrect CSI estimation. Attackers can exploit these errors through pilot spoofing, where they inject fake pilot signals to manipulate CSI and direct power toward themselves, disrupting legitimate communication.
3. **Jamming Attacks:** Jamming attacks intentionally disrupt CSI estimation, beamforming, and communication reliability. Techniques include artificial noise, full-duplex, and directional jamming, all of which raise the secrecy outage probability.
4. **Doppler Shift & Mobility effect:** High mobility introduces rapid channel variations and Doppler-induced frequency shifts, causing synchronization errors, outdated CSI, and increased risk of eavesdropping in dynamic environments.
5. **Antenna Correlation:** Spatial correlation between the MIMO antennas reduces diversity and performance, weakening beamforming effectiveness while sometimes benefiting eavesdroppers with predictable channel conditions.

MIMO systems rely on accurate channel estimation to optimize signal transmission and reception. However, errors in channel estimation can significantly degrade system performance. Pilot contamination occurs when non-orthogonal pilot sequences are reused across different cells, leading to interference and inaccurate channel estimation. Survey [55] identifies non-orthogonal pilot reuse, hardware impairments, and non-reciprocal transceivers as key causes of pilot contamination in massive MIMO systems. Limited coherence time forces neighbouring cells to reuse pilot sequences, causing inter-cell interference and inaccurate CSI estimation, while hardware imperfections such as phase noise and amplifier non-linearity introduce further distortions. Additionally, transceiver mismatches in time-domain duplex (TDD) systems disrupt channel reciprocity, exacerbating pilot contamination and degrading system performance. This interference results in inaccurate channel state information (CSI), causing a degradation in system performance, including reduced spectral efficiency and compromised beamforming accuracy [56]. In multi-cell environments, pilot contamination arises because base stations inadvertently estimate channels that are influenced by users from neighbouring cells, rather than solely from their intended users. While orthogonal pilots can be assigned to users within a single cell, maintaining this orthogonality across multiple cells is not feasible. The overlapping of pilot signals from different cells destroys their orthogonality, causing interference during the training phase [57]. Many cellular networks use unity frequency reuse to maximize spectral efficiency, meaning all cells operate on the same frequencies. This increases pilot contamination because

users in different cells transmitting on the same frequency interfere with each other's pilots. Additionally, pilot contamination can be exploited by malicious users through active eavesdropping attacks, where an attacker transmits identical pilot signals to manipulate the CSI estimation, thereby improving its ability to intercept communications while degrading the intended receiver's performance [58].

Another source of channel estimation errors in MIMO systems is eavesdropping, which can be either passive or active. In passive eavesdropping, attackers simply listen to transmissions without interfering. In contrast, active eavesdropping involves injecting false signals to manipulate the channel estimation process. Common techniques include relay-based interception, pilot contamination, jamming-assisted eavesdropping, and traffic analysis, all of which exploit weaknesses in MIMO systems to gain unauthorized access to information.

Massive MIMO systems offer some protection against passive eavesdropping thanks to narrow beamforming, which focuses energy on legitimate users and reduces signal leakage. However, this protection can break down if an eavesdropper is physically close to the intended user. In such cases, the attacker benefits from similar channel conditions and may still extract sensitive data. While passive attacks are limited in scope, they remain a concern, especially in scenarios where users are closely spaced or beamforming isn't perfectly tuned [59]. Active eavesdropping poses a more serious threat. One of the most effective strategies is the pilot contamination attack is where an attacker sends deceptive pilot signals during the uplink training phase. This tricks the base station into estimating a false channel and inadvertently directing transmission power toward the eavesdropper instead of the legitimate user. Because pilot contamination already occurs naturally in multi-cell systems, these attacks are hard to detect. In some cases, attackers even combine jamming with eavesdropping, disrupting channel estimation while simultaneously listening in, further complicating detection and defence.

Attackers do not always need access to the content of messages to gather valuable information. Through traffic analysis, they can examine metadata like packet timing, transmission frequency, and signal strength to infer communication patterns. Even with encrypted data, this approach can reveal who is communicating, when communication takes place, and possibly what kind of data is being exchanged. This is particularly concerning in IoT and 5G networks, where large numbers of small, frequent packets make pattern detection easier [60]. In large-scale MIMO relaying systems, passive eavesdroppers can target the relay itself, intercepting data as it is forwarded to the final destination. These attacks are especially effective when the eavesdropper is close to the relay, allowing them to capture high-quality signals before they reach the intended recipient [61]. Also, imperfect CSI estimation at the relay weakens its ability to optimize secure transmissions, making it easier for eavesdroppers to exploit these inaccuracies and intercept data.

Furthermore, jamming attacks in MIMO systems can significantly degrade communication reliability**,** compromise security, and disrupt the accuracy of channel estimation at the physical layer. When attackers interfere during the channel estimation phase, they corrupt the estimated CSI and cause the base station to misallocate transmission resources. This attack is particularly effective in massive MIMO systems, where CSI precision is critical for beamforming and interference mitigation [62]. Additionally, artificial noise jamming, used in cooperative jamming strategies, introduces structured interference that selectively degrades eavesdroppers' reception while maintaining the quality of legitimate user signals [63]**.** Another advanced technique, full-duplex jamming, allows an adversary to simultaneously jam and eavesdrop on a signal, making detection and mitigation particularly challenging [64]**.**

The effects of jamming attacks in MIMO systems range from reduced secrecy capacity to complete communication failure. Jamming increases the secrecy outage probability, meaning that legitimate users experience develops higher error rates while eavesdroppers may still successfully decode messages [65]. In cyber-physical systems and IoT applications, jamming can be particularly disruptive as it affects real-time communications, leading to loss of control in automated processes**.** The authors of [66] provide an additional categorization of jamming techniques based on jamming signal directionality. Uniform jamming spreads noise across all directions, making it less efficient but broadly disruptive, while directional jamming focuses interference precisely toward a user, enhancing its effectiveness in impacting received SNR levels.

Moreover, the mobility of the transmitter and/or receivers and the respective Doppler shift effects introduce significant challenges to MIMO systems at the physical layer by causing rapid fluctuations in channel characteristics, thereby affecting signal quality, synchronization, and system performance. In high-mobility environments, such as satellite and vehicular MIMO communications, the channel varies quickly over time, making accurate CSI estimation difficult. This leads to channel aging, where the estimated CSI becomes outdated before it can be used effectively, resulting in degraded beamforming and spatial multiplexing performance [67]. Doppler shift, caused by relative motion between the transmitter and receiver, induces frequency offset and inter-carrier interference (ICI), which distorts the received signal and increases error rates.

Random mobility introduces fluctuations in secrecy capacity due to varying distances between transmitters, legitimate users and eavesdroppers [68], investigated under three typical random mobility models and a passive eavesdropper. The work on [69] discusses the Doppler shift as a key factor contributing to carrier frequency offset (CFO) in MIMO systems. The Doppler shift arises due to relative motion between the transmitter and receiver, leading to frequency variations that impact signal synchronization. The paper models the CFO as a combination of

oscillator mismatch and Doppler shift, where the latter is time-varying and follows a Gaussian distribution.

The work presented in [70] extends the studies on mobile receivers to incorporate mobile interferers and mobile eavesdroppers in its analytical framework for Secrecy Transmission Capacity (STC) in dynamic environments**.** Mobility induces Doppler shifts, which degrade channel estimation accuracy and cause higher synchronization errors. These effects make it more challenging for legitimate receivers to maintain robust communication, while eavesdroppers can exploit these distortions.

Finally, another important factor influencing the secrecy capacity and reliability of MIMO systems, is the correlation between the multiple antennas [71]. Antenna correlation occurs when the signal paths between antennas are not independent, typically due to closely spaced antenna elements or insufficient scattering in the propagation environment. This correlation reduces spatial diversity, limiting the ability of MIMO to exploit independent channel gains for improved performance. Study [72] analysed inter-antenna correlation in cognitive vehicular networks, highlighting that imperfect CSI further degrades security, particularly under high-mobility conditions, as antenna correlation reduces diversity gain and weakens resistance to eavesdropping.

The authors of [73] explored the impact of antenna correlation on secrecy performance in MIMO wiretap channels, where transmit antenna selection is employed at the transmitter, while the receiver and eavesdropper use maximal ratio combining. Their study found that higher correlation at the eavesdropper's antennas improves secrecy performance, whereas higher correlation at the legitimate receiver degrades it, making MIMO beamforming less effective against eavesdroppers**.** Transmit antenna selection becomes less efficient when correlation is present, as the channel diversity gain is reduced. In contrast, if the eavesdropper has high correlation, their ability to extract confidential data is weakened, showing that correlation can be both a vulnerability and a defence mechanism. Finally, study [74] shows that correlation increases as the angle spread decreases, which negatively impacts MIMO capacity and diversity gain. The findings indicate that uniform linear array systems suffer more from correlation effects than uniform circular array systems, and higher spatial correlation leads to a loss in both spatial multiplexing and diversity gains.

3.5.3 Virtualization and multi-vendor related vulnerabilities

As next-generation wireless networks adopt the O-RAN architecture with its emphasis on disaggregation, virtualization, and open interfaces, new security challenges emerge that directly impact the physical layer. This section addresses the virtualization, and multi-vendor related vulnerabilities at the physical layer, building upon insights from the O-RAN Security Threat

Modelling and Risk Assessment framework [12]. We identify the following vulnerabilities from the model as related to the physical layer:

1. **O-RAN specific vulnerabilities** -These are the security weaknesses that stem directly from the architectural principles, deployment models, and technological choices defined by the O-RAN Alliance specifications. Unlike traditional monolithic radio access networks (RANs), O-RAN promotes disaggregation, openness, and vendor diversity. While these characteristics enable greater flexibility, innovation, and cost efficiency, they inherently introduce new security concerns. Key among these is the exposure of internal network interfaces, increased dependency on standardised but often immature APIs, and the challenge of maintaining consistent security policies across multiple independently developed components. In this category, there are the following vulnerabilities related to physical layer:
    a. Unauthorized access to O-DU and RU to degrade RAN performance or execute broader network attack (Availability)
    b. Unprotected synchronization and control plane traffic on Open Fronthaul Interface (Integrity and Availability)
    c. Disable over-the-air ciphers for eavesdropping (Confidentiality)
    d. Near-RT RIC conflicts with O-gNB (Availability)
    e. Unprotected management interface (Confidentiality, Integrity, Availability)

2. **General vulnerabilities** – these refer to security risks that are not exclusive to O-RAN but arise from the widespread use of virtualization, containerization, and cloud-native technologies within the broader telecom and IT ecosystems. These vulnerabilities have been extensively studied in cloud computing and apply equally to O-RAN components deployed in virtualized environments. The physical layer vulnerabilities identified from the O-RAN Threat Model are the following:
    a. Decoupling of functions without hardware root of trust and software trust chain (Integrity)
    b. Exposure to public exploits from use of open-source code (Confidentiality, Integrity, Availability)
    c. Misconfiguration, poor isolation or insufficient access management in the O-Cloud platform (Confidentiality, Integrity, Availability)

3.5.4 AI-based Vulnerabilities

The growing adoption of AI within 5G/6G physical-layer processing not only strengthens defensive mechanisms but also opens new attack surfaces. This subsection analyses how adversaries weaponize AI for jamming, eavesdropping and spoofing, complementing the baseline threat characterization given in previous sections.

1. **Jamming** - Although NATWORK anti-jamming system (e.g., DetAction) is not especially sensitive to AI-based jamming compared with a 5G network, we are not actively countering it either. Wireless communications, as mentioned in section 4.3, can be attacked using adversarial machine learning strategies. In NATWORK's anti-jamming system, we are using a proactive frequency hopping algorithm to avoid the presence of jamming and reallocate the used frequency to one without this interference. But if another AI algorithm is used by the jammer and in an exploratory attack infers how our algorithm works, it could attack the frequencies that we are going to use next in an evasion attack (as we are not re-training the algorithm, a causative attack is not feasible in our case).
2. **Eavesdropping** - **Regarding** AI-eavesdroppers, even though our system uses physical-layer key generation (PKG) to hide data, smart attackers that use AI could still have possibilities to listen in. Studies on 5G physical-layer security show that machine-learning tools can guess the radio channel from only a few pilot signals in some scenarios, revealing who is talking and how much data is moving [22]. Other work trains AI models on encrypted Wi-Fi traffic and still works out which IoT devices are active or what they are doing [75]. Looking **to** the future, new surveys on RF sensing explain how deep learning can pick up speech, gestures or keystrokes by tracking tiny changes in radio waves [76], in 6G, some researchers warn that these smart eavesdroppers will only get better unless networks add defences such as random pilot patterns and AI-based anomaly detectors [77]. But nowadays we can regard it more as a challenge for the would-be eavesdropper than as a practical vulnerability for our NATWORK mechanisms and components.
3. **Spoofing** - Traditional spoofing depends on static identity spoofing (MAC or IP address spoofing), but AI enables more dynamic and context-dependent approaches. AI-powered spoofers can adjust in real-time by examining traffic patterns, radio signal properties, or authentication patterns to better impersonate authorized users. In the physical layer, attackers may employ generative models or deep learning methods to imitate radio frequency fingerprints, modulation patterns, or spatial-temporal signatures. In next-generation wireless networks such as 5G and future 6G networks, where physical-layer features such as beamforming are essential in device verification, AI is susceptible to abuse in constructing signals to deceive these mechanisms. For instance, AI would determine how spatial verification schemes operate and replicate the location or transmission pattern of a device. Although such attacks are currently still technically sophisticated and not yet pervasive, the application of AI makes them increasingly feasible. Without employing specialized spoofing tools to detect spoofing e.g., AI-driven anomaly detection or physical-layer identifier randomization networks can continually be made more susceptible to the threat over time. At present, these threats are generally

considered emerging rather than critical, but they represent a growing risk as AI technologies mature.

3.6 Risk and Impact Assessment

This section presents the Risk and Impact Assessment (Table 2) for the identified physical layer vulnerabilities in next-generation wireless networks, as defined within the NATWORK threat modelling framework. Building on the previous analysis of assets, threat actors, and specific vulnerabilities—including those related to jamming, spoofing, eavesdropping, physical tampering, and O-RAN virtualization risks—this section evaluates the likelihood and potential consequences of these threats in realistic deployment scenarios of NATWORK. The assessment methodology aligns with industry-recognised approaches, including ISO/IEC 27005 and the O-RAN threat model, providing a structured analysis of how vulnerabilities at the PHY layer can compromise system confidentiality, integrity, and availability. By quantifying both the probability of threat exploitation and its operational impact, this section delivers a prioritised risk landscape that informs mitigation planning and supports secure-by-design strategies across the NATWORK project.

Table 2 Risk and Impact Assessment

Risk	Likelihood (Low/Medium/High)	Impact (Low/Medium/High)	Mitigation
Unauthorized access to RIS controller	High	High	• Intelligent signal classification using ANN • Malware detection via optimization methods for chip reconfiguration
RIS reflecting signals in unintended directions	Medium	Medium	• FPGA-based controller with genetic algorithm for self-adjustment of radiation pattern • High-precision calibration during fabrication to minimize phase-shift errors

Risk	Likelihood (Low/Medium/High)	Impact (Low/Medium/High)	Mitigation
			• Real-world validation of phase-shift codebooks under various scenarios • Dynamic channel estimation with closed-loop feedback from the receiver
RIS-assisted jamming or signal manipulation RIS-based DoS via controller overload	Medium Medium	High High	• SDR-based SINR optimization • Integer Linear Programming (ILP) for dynamic RIS reconfiguration • Frequent channel randomization of RIS units for harder effective jamming alignment. Overhead-aware optimization framework to balance energy and rate efficiency
Eavesdropping using illegal RIS (IRIS)	Medium	Medium	Artificial Noise (AN)-assisted methods and cooperative jamming techniques
Pilot contamination in RIS	High	High	• Statistical methods detection for PCA to detect abnormal pilot sequences
Pilot spoofing in RIS	High	High	• Alternating Optimization algorithm and Charnes-Cooper

Risk	Likelihood (Low/Medium/High)	Impact (Low/Medium/High)	Mitigation
			transformation for PSA
Physical tampering of antennas or embedded radios	Low	Medium	Hardware-based security features and intrusion detection mechanisms
Virtualization layer compromise in multi-vendor PHY	Medium	High	• Secure boot • attestation techniques • VM/container isolation
AI-assisted adaptive jamming in PHY	Medium	Medium	• FDA-MIMO • frequency hopping • MMSE/ZF-based jamming suppression • GLRT-based detection
Pilot contamination in MIMO (multi-cell reuse)	High	High	• Adaptive pilot design and secure pilot sequences • Compressive sensing and Bayesian estimation • MMSE-based training matrix optimization • Deep learning-based pilot estimation
Pilot spoofing in MIMO	High	High	• Statistical detection methods • Secure pilot authentication • Deep neural networks for

Risk	Likelihood (Low/Medium/High)	Impact (Low/Medium/High)	Mitigation
			spoofing detection
Active eavesdropping via pilot injection	Medium	High	• Compressive sensing for sparse pilot recovery • Sparse Bayesian Learning (SBL) • ML-based anomaly detection in channel estimates
Jamming during channel estimation	Medium	High	• MMSE-JS suppression • GLRT-based detection using unused pilots
Full-duplex and directional jamming	Medium	Medium	• Frequency Diverse Array-MIMO (FDA-MIMO) • Beam nulling toward jamming sources • Frequency hopping to disrupt attacker coordination
Mobility-induced channel aging & Doppler effects	High	Medium	• AI-based beamforming and tracking • RIS for dynamic channel adaptation
Antenna correlation in MIMO system	Medium	Medium	• Metamaterial and dielectric antenna design • Hybrid precoding • Adaptive MIMO mode switching
Imperfect CSI due to	Medium	Medium	• MMSE-based transceiver design

Risk	Likelihood (Low/Medium/High)	Impact (Low/Medium/High)	Mitigation
hardware impairments			• ML-based error correction and calibration
Adversarial ML smart jamming attack	Low	Medium	• Signal injection to deceive adversarial ML algorithms
CSI profiling eavesdropper	Low	Medium	• Privacy Amplification hash reinforcement and pilot hopping breaking the model CSI estimation.
RF sensing eavesdropper	Low	Medium	• RF hardware shielding, AI anomaly monitoring or pilot hopping techniques.
An attacker penetrates and compromises the O-RAN system through the open O-RAN's Fronthaul	High	Medium	• Physical hardening
Unauthorized access to the Open Front Haul Ethernet L1 physical layer interface (cables and connections)	High	Low	• Physical hardening
An attacker stands up a rogue O-RU	High	Medium	• Physical hardening • authentication

Risk	Likelihood (Low/Medium/High)	Impact (Low/Medium/High)	Mitigation
(standalone) - a false base station			
An attacker compromises a PNF to launch attacks against VNFs/CNFs	High	Medium	• authentication
Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack	High	High	• Vulnerability handling and patch management
A successful attack could: - Compromise the deployed VNF/CNF	Medium	High	• SBOM requirements • • REQ-SEC-SYS-1 (O-RAN)

4 Key mitigation methods

Following the comprehensive risk and impact assessment, this section presents targeted countermeasures aimed at enhancing the resilience of next-generation wireless networks, with a specific focus on 5G and emerging 6G systems. The mitigation strategies are designed to reduce both the likelihood and impact of threats such as jamming, spoofing, eavesdropping, physical tampering, and vulnerabilities arising from advanced technologies like Reconfigurable Intelligent Surfaces (RIS), Massive MIMO, AI-enhanced signal processing, and O-RAN virtualization. The proposed approaches combine established best practices, such as secure signal authentication and robust hardware protections, with innovative techniques developed in response to evolving attack vectors in disaggregated, multi-vendor, and software-defined network environments. By systematically linking mitigations to the identified risks, this section provides a practical foundation for implementing secure-by-design principles and guiding future research and development efforts within NATWORK.

4.1 Existing vulnerabilities in protocols and standards

Although the vulnerabilities are significant, several countermeasures are currently being researched or deployed. One of the new techniques for achieving beamforming and directional antennas to reduce signal leakage between the base station and the users. This increases power and makes communication more resistant to jamming. Spread spectrum and frequency hopping are used to prevent jamming. By using wider spectrum areas, it is more complicated to concentrate the jamming signal, as the system cannot cover the whole spectrum for various reasons. For instance, the RF electronics are optimized for a specific range and bandwidth, i.e., the USRP B210 can operate in a bandwidth of 56 MHz

PHY-layer authentication based on radio fingerprint or channel state information. This is still a very modern approach. As we continue to develop the technology, with greater processing power, we will soon reach the point where we will be able to detect such a subtle change between one base station and another, or between one UE and another, by being able to differentiate the source of the signal.

All these mitigation techniques will be developed in the following subsections, such as beamforming using MIMO (Multiple Input Multiple Output) antenna systems.

4.2 RIS and MIMO specific vulnerabilities

4.2.1 RIS Mitigation measurements

Given the security vulnerabilities for RIS, various mitigation strategies have been proposed to counteract threats such as pilot contamination, jamming, signal leakage and unauthorized access. These methods leverage advanced detection algorithms, optimization techniques and secure frameworks to safeguard RIS-assisted communication systems. Solutions include statistical detection mechanisms, optimization-based countermeasures, AI and machine learning approaches and hardware level defences to ensure reliable and secure operation. The following section outlines key mitigation techniques compensating different RIS-based attacks, enhancing the resilience of future wireless networks.

Mitigation of RIS-PCA has been presented in [54] where a Generalized Cumulative Sum method has been applied that detects PCA and enables secure transmissions under RIS based PCA. For the case of PSA-RIS attack, work [78] suggests an alternating optimization algorithm and a Charnes-Cooper transformation procedure that addresses this PSA. To eliminate jamming originating from a RIS, in [79] a proposed solution is suggested via the use of an SDR optimization method to reduce the SINR. In [80], mitigation strategies for ERA were proposed using Integer Linear Programming to rapidly adjust the RIS configuration and counteract the attack on victim wireless communication systems. To counter RIS-based manipulation attacks, [81] proposed a path-separation-based slewing rate detection process, which removes the compromised path in the time domain and employs a flexible quantization method to maximize KGR.

For mitigation of the Signal Leakage attack, an Artificial Noise-assisted method is suggested [82] based on joint optimization to alleviate the PLS damage caused by IRIS. One possible mitigation strategy for eavesdropping is cooperative jamming [83], where the control centre actively introduces interference to disrupt the eavesdropper's ability to decode the communication.

To address unauthorized access to the RIS controller, work [84] suggests implementing an Artificial Neural Network (ANN)-based intelligent framework for signal classification and identification. To counter exploitation of remote access and malware injection to compromise the RIS controller and tunable chips, the authors in work [85], propose optimization-based mitigation methods that detect disturbances and dynamically re-tune the chip parameters. Mitigation of the electromagnetic wave manipulation to an undesired direction leading to destructive interference by an attacker is suggested in [86]. In this work an FPGA-based advanced controller with genetic algorithm optimization is suggested, allowing the system to self-adjust and maintain the desired radiation pattern.

To avoid the high-overhead of RIS channel estimation that could lead to DoS, work [87] introduces an overhead-aware framework that optimizes system rate and energy efficiency by

integrating overhead modelling into phase shifts, power, bandwidth, and feedback design. It also explores the trade-off between performance and overhead, providing a bi-objective optimization of rate and energy efficiency in RIS-assisted networks.

RIS can be applied to counter MIMO physical layer challenges, including interference and poor channel conditions induced by mobility. By dynamically adjusting the phase shifts of passive reflecting elements, RISes can manipulate wireless propagation environments, enhancing signal strength and mitigating jamming attacks. In [88], the authors focus on the challenge of channel acquisition for RIS-aided multi-user mmWave MIMO systems. They propose a novel channel estimation protocol that formulates the problem as a sparse recovery task using compressive sensing (CS) techniques, effectively reducing training overhead. Additionally, they exploit common block sparsity among users to enhance estimation accuracy. In [89], a two-stage channel estimation method is introduced, where the first stage estimates the direct MIMO channel using conventional uplink training, while the second stage employs a bilinear adaptive vector approximate message passing algorithm to estimate RIS-related channels efficiently, even under ill-conditioned scenarios. They also propose an optimization-based phase shift design to maximize the total channel gain at the receiver. RISs are also increasingly being integrated into cell-free massive MIMO systems to enhance beamforming and improve network performance. The study [90] proposes an optimization framework where RIS and base stations jointly coordinate beamforming to maximize network capacity while reducing power consumption. This cooperative approach allows for more efficient resource allocation, mitigating interference and improving spectral efficiency in distributed MIMO deployments. Meanwhile, the joint design of hybrid beamforming and RIS reflection coefficients in mmWave MIMO systems [91], introduces a penalty-based optimization algorithm to minimize power consumption while maintaining high-quality communication links. By dynamically adjusting reflection coefficients at RIS elements, the system can maintain optimal beam alignment, overcoming challenges related to path loss.

In NATWORK, we will develop a physical-layer computation procedure for RIS configuration that can be deployed across different hardware platforms, taking each device's specifications into account. We will also characterize and suppress unwanted reflections so that the RIS can serve two network roles: (1) a proactive covert mechanism that reduces signal exposure in areas with potential adversaries, and (2) a jamming mitigation mechanism that attenuates electromagnetic propagation from jammer directions to protect legitimate users.

4.2.2 MIMO mitigation measurements

In the context of MIMO physical layer security, an important mitigation method to counter the effects of pilot contamination is to use improved pilot signal techniques. The authors of [92] proposed adaptive and flexible PLS algorithms that secure both data and pilots in OFDM-based MIMO systems. The core idea is to exploit minimum-phase all-pass channel decomposition,

which enhances security without degrading legitimate user performance. This method prevents eavesdroppers from reconstructing the legitimate CSI. Similarly, methods proposed in [93] primarily focus on secure channel estimation and mitigating pilot contamination attacks by utilizing advanced techniques such as compressive sensing, Bayesian estimation, and joint data-pilot processing. Their approach involves using random or structured pilot sequences to enhance channel estimation accuracy while minimizing the risk of pilot contamination from adversarial jammers. Additionally, incorporating machine learning (ML) techniques can further optimize pilot allocation and adapt dynamically to varying channel conditions.

Minimum Mean Square Error (MMSE) methods offer advanced techniques for channel estimation and transceiver optimization in MIMO systems. The MMSE estimator is designed to minimize the mean squared error between the estimated and actual channel responses, making it more effective than traditional Least Squares (LS) or Scaled LS (SLS) methods, particularly in low-SNR environments. One approach involves using eigenvalue decomposition and Lagrange multiplier methods to derive optimal training matrices, ensuring efficient power distribution [94]. Another MMSE-based optimization strategy for multi-user MIMO systems focuses on balancing layer-wise or user-wise MSEs while minimizing total transmission power, utilizing [95]. Extending the previous, [96] focused on the impact of MMSE receivers on link-layer throughput capacity in wireless ad hoc networks. This work characterized the SINR distribution in MIMO ad hoc networks and derived an optimal active-link density for maximizing throughput capacity, also providing insights into MAC-layer protocol design.

Bayesian methods offer a powerful approach to mitigating malicious attacks on pilot signals and improving channel estimation in MIMO systems by leveraging probabilistic inference and prior knowledge of channel statistics. Unlike Least Squares (LS) or Minimum Mean Square Error, Bayesian techniques such as Sparse Bayesian Learning (SBL) and Gaussian Mixture Models (GMM) iteratively refine estimation accuracy, effectively reducing errors, combating pilot contamination, and enhancing robustness in noisy or rapidly changing environments. These methods improve interference suppression and spectral efficiency, making them valuable for massive MIMO, radar processing, and next-generation wireless networks. Specifically, [97] introduces a Bayesian framework for detecting moving targets in Gaussian clutter using FDA-MIMO radar, with the Bayesian Structured Generalized Likelihood Ratio Test (BSGLRT) and Bayesian Unstructured Generalized Likelihood Ratio Test (BUGLRT) detectors reducing dataset requirements and computational complexity. Meanwhile, [98] addresses pilot contamination in massive MIMO by estimating interference links and leveraging channel sparsity for accurate estimation without prior covariance knowledge. Additionally, [99] employs sparse Bayesian learning for high-resolution target imaging in monostatic MIMO radar, while Bayesian detection in FDA-MIMO radar enhances target detection in Gaussian clutter by mitigating interference and improving accuracy.

A popular approach that has emerged for mitigating channel estimation errors in MIMO systems is the use of Machine learning (ML) tools, particularly deep learning (DL) models. These approaches utilize neural networks to learn complex channel characteristics and improve estimation accuracy beyond traditional methods such as MMSE and LS estimation. In paper [100], the authors propose an end-to-end learning framework where a deep neural network (DNN) is trained to directly map received signals to estimated channel states. Its method employs data-driven optimization, which allows the model to adapt dynamically to channel conditions, protecting against pilot contamination. DNNs can also be used to address the challenges of channel estimation in beam space millimetre-wave (mmWave) massive MIMO systems [101]. This approach exploits the inherent sparsity of mmWave massive MIMO channels in the beam space domain, allowing for more accurate reconstruction of the channel state with fewer RF chains. Unlike conventional linear estimation methods, [102] focuses on the development of a deep learning-based two-stage channel estimation scheme for massive MIMO systems specifically designed for cases where the pilot length is smaller than the number of transmit antennas. Some ML models can also operate without extensive training requirements, significantly reducing computational complexity while achieving near-MMSE performance [103].

To mitigate the effects of jamming attacks on the physical layer, several methods are available. Detection strategies primarily rely on leveraging statistical and mathematical models to distinguish legitimate signals from jamming interference. For instance, random matrix theory-based methods [104] analyse the eigenvalue distribution of received signals to detect jamming anomalies, while subspace-based techniques exploit channel characteristics to isolate interference from authentic transmission. Meanwhile, [105] introduces a detection method that employs a generalized likelihood ratio test (GLRT) and unused pilot sequences to improve detection accuracy. For mitigation, advanced suppression techniques such as MMSE-JS (Minimum Mean Squared Error-based Jamming Suppression) [106] and ZFJS (Zero-Forcing Jamming Suppression) have been proposed in the literature. These methods utilize intentionally unused pilot signals to estimate and mitigate jamming effects, improving robustness against pilot contamination. Additionally, beamforming techniques such as FDA-MIMO (Frequency Diverse Array-MIMO) enhance interference suppression by exploiting spatial and frequency diversity, effectively nulling deceptive jammers [107], [108]. These combined approaches significantly strengthen MIMO systems against malicious jamming attacks.

Frequency-hopping techniques play an important role in mitigating jamming attacks in wireless MIMO communications by dynamically altering signal transmission frequencies to evade malicious interference. These methods employ rapid and unpredictable changes in carrier frequency to make it difficult for adversaries to attack on the correct frequency and interfere effectively. [109] introduces frequency-hopping codes to optimize radar ambiguity functions, that are proven to reduce side lobes and enhance target detection while improving resilience

against jamming. One of the problems encountered in recent technological advancements is the scarcity of spectrum resources and the interference between radar and communication systems. To mitigate this, [110] proposes a frequency-hopping MIMO (FH-MIMO) radar as a viable solution, demonstrating its ability to dynamically alter frequency channels to avoid interference and improve robustness against jamming. By embedding communication signals into radar waveforms, it discusses how FH-MIMO can provide improved spectral efficiency and better interference rejection. Recent studies have also explored novel frequency-hopping MIMO (FH-MIMO) radar-based communication frameworks, which optimize waveform selection and hopping patterns to enhance resilience against jamming [111].

Recent developments in wireless security have shown an emergence of key generation techniques at the physical layer that utilize the inherent randomness of the wireless channel. The key generation process typically follows five main steps:

1. Channel probing: This is where two communicating devices exchange channel measurements such as CSI, phase, or Angle of Arrival (AoA) to extract a shared random source.
2. Randomness extraction: Deterministic components that could be inferred by an eavesdropper are removed.
3. Quantization: This is the stage where the extracted randomness is converted into binary bits.
4. Information reconciliation: This ensures consistency between the generated keys at both ends through error correction techniques.
5. Privacy amplification: This minimizes the leaked information during key reconciliation to prevent eavesdroppers from recovering the key.

[93] provides an overview of the key generation schemes that utilize channel characteristics such as reciprocity, randomness, and spatial uniqueness to derive secure encryption keys resistant to jamming and eavesdropping. One key approach utilizes the sparsity of millimetre-wave (mmWave) MIMO channels to generate highly decorrelated keys, reducing vulnerability to eavesdropping and jamming attacks [112]. Another technique leverages beamforming and hybrid precoding to enhance security by limiting the exposure of channel information to potential attackers.

Beamforming is a signal processing technique in MIMO systems that optimizes the direction and strength of wireless transmissions by adjusting phase and amplitude across multiple antennas to improve signal quality and reduce interference in the desired directions. Traditional beamforming algorithms struggle with real-time environmental changes, leading to signal degradation, especially in high-mobility scenarios. However, AI-driven approaches, including neural networks and deep learning models, can predict and adjust beamforming patterns

dynamically, counteracting the impact of Doppler shifts. The study [113] explores the role of deep learning-based beamforming methods in enhancing signal reception accuracy, adapting to dynamic environments, and improving direction-of-arrival (DoA) estimation. Similarly, the work in [114] presents a hybrid beamforming design incorporating artificial intelligence for accurate channel estimation, ensuring high spectral efficiency while reducing power consumption. By utilizing deep learning models such as Convolutional Neural Networks (CNNs) and reinforcement learning techniques, the proposed framework intelligently selects optimal antennas and adapts beamforming parameters based on environmental changes, effectively addressing mobility-induced impairments.

A crucial part in designing MIMO systems is the antenna selection. Review [115] highlights several key factors that influence antenna selection, including channel capacity computation, multipath propagation characteristics, mutual coupling, array configuration, and element radiation properties. It emphasizes that the design of MIMO antennas should ensure low correlation between antenna elements to maximize system performance, particularly by optimizing spatial, angle, and polarization diversity. One sophisticated approach, [116], involves the use of dielectric resonator antennas, which provide high isolation and low mutual coupling by leveraging unique electromagnetic properties, as described in the MIMO dielectric resonator antenna design for 5G mm-Wave applications. Metamaterial-based MIMO antennas, such as the compact and closely spaced designs incorporating defected ground structures, are another approach that effectively reduces surface wave propagation and enhances isolation, thus improving spatial diversity and MIMO performance [117]. Other innovative approaches in the literature include an ultrawideband MIMO antenna with high isolation [118], that achieves a wide bandwidth and reduces mutual coupling through a centre-ground slot and a compact wide-band multimode antenna [119] leveraging pattern and polarization diversity, allowing multiple signals to be decorrelated without requiring large spatial separations, making it highly efficient for compact devices. Dielectric resonator antennas, as explored in [120], also contribute to improved isolation thereby improving spectral efficiency in MIMO schemes.

A complementary approach to mitigating MIMO correlation effects is using precoding, which is a signal processing technique that optimise the transmission of signals from multiple antennas to multiple receivers. It involves applying linear or non-linear transformations to the transmitted signal using CSI. According to [121], precoding techniques such as Zero-Forcing (ZF), MMSE, and hybrid analog/digital precoding are employed to counteract spatial correlation and inter-user interference in massive MIMO systems. These methods leverage CSI to optimize beamforming, enabling more effective transmission by directing signals toward desired users while suppressing interference. Particularly in mmWave systems, hybrid precoding techniques that combine analogue beamforming with digital signal processing to fine-tune the signal, so as to reduce interference and improve the achieved data rates [122].

The adaptive transmission techniques play a crucial role in mitigating antenna correlation issues in MIMO systems by dynamically adjusting transmission schemes to match varying channel conditions. The paper [123] introduces a low-complexity adaptive approach that switches between statistical beamforming, double space-time transmit diversity, and spatial multiplexing based on spatial correlation metrics to maximize capacity gains. In the same manner, [124] explores how link adaptation methods, including switching between diversity, hybrid, and multiplexing techniques, optimize spectral efficiency and mitigate performance degradation caused by antenna correlation. These strategies ensure that, depending on the spatial selectivity of the channel, the best MIMO transmission mode is selected to enhance link robustness, improve data rates, and maximize spectral efficiency in broadband wireless networks.

In the NATWORK architecture, we will develop an anti-jamming scheme that fully leverages the spatial multiplicity of the MIMO receiver array. This aims to enable precise and resilient jamming defence and deliver:

1. A DNN-based jamming identification module capable of detecting the type, DoA, phase offset, and time onset of jamming signals embedded in the received stream
2. A robust jamming mitigation mechanism that integrates techniques such as spatial correlation analysis, eigenprojection, and adaptive subspace filtering to effectively suppress a wide range of jamming types and modulation schemes

In the NATWORK architecture, we will develop an anti-jamming scheme that fully leverages the spatial multiplicity of the MIMO receiver array to enable precise and resilient jamming defence and deliver:

1. A DNN-based jamming identification module capable of detecting the type, DoA, phase offset, and time onset of jamming signals embedded in the received stream.
2. A robust jamming mitigation mechanism that integrates techniques such as spatial correlation analysis, eigenprojection, and adaptive subspace filtering to effectively suppress a wide range of jamming types and modulation schemes.

To generalize across diverse channel conditions, the system will incorporate online adaptation techniques supported by varied training datasets. Furthermore, optimizing the eigenprojection method for multi-source jamming scenarios and minimizing inference latency will be critical for real-time responsiveness. Together, these advancements will transform the current framework into a scalable, adaptive, and deployable anti-jamming defence solution.

4.3 Virtualization and multi-vendor stemming vulnerabilities

The virtualization of the physical layer in O-RAN introduces a unique set of risks due to the abstraction of hardware and reliance on shared computing infrastructure. To mitigate these risks,

the O-RAN Alliance and related cybersecurity studies have proposed a comprehensive set of strategies [12], drawn from Zero Trust Architecture (ZTA) principles and cloud-native security practices. The mitigation methods fall into several key categories:

1. Virtualization Security Controls
    a. **Hypervisor and Kernel Protection**: Implement hypervisor-based access control and intrusion detection to prevent unauthorized manipulation of virtual resources.
    b. **Isolation Mechanisms**: Enforce strict separation between VMs/CNs using security orchestration and segmentation techniques. This is crucial to prevent lateral movement and side-channel attacks (e.g., cache-timing or power-based leaks).
    c. **Boot Integrity Validation**: Secure boot mechanisms must ensure the integrity of host OS and container engines to defend against bootloader tampering and hyper jacking attacks.
    d. **VM-Level Defences**: Use virtual machine-based trusted computing, kernel protections, and isolation mechanisms as preventive layers.
2. Robust Authentication and Access Control
    a. **Role-Based and Attribute-Based Access Controls (RBAC/ABAC):** Limit access to virtualized resources using dynamic policies tailored to roles and contextual attributes.
    b. **Multi-Factor Authentication (MFA) and OAuth 2.0:** Protect administrative interfaces and APIs against privilege escalation and unauthorized access.
3. Data Security Measures
    a. **Encryption at Rest and In Transit:** Protect sensitive data and control/management plane traffic using strong encryption mechanisms like TLS 1.2+ and X.509-based.
    b. **Integrity Protection for Data in Use**: Use cryptographic validation (e.g., digital signatures) to verify data and software components during runtime
4. Monitoring and Threat Detection
    a. **Continuous Monitoring and Logging**: Capture system logs and telemetry from virtualized components for real-time threat detection and post-incident analysis.
    b. **Audit and Alerting Mechanisms**: Trigger security alerts on detection of abnormal behaviours, especially around boot processes, access attempts, and resource assignment anomalies.
5. Network and Interface Protection
    a. **API Hardening and Input Validation**: Enforce strict validation for all management and orchestration APIs to mitigate injection and manipulation attacks.

b. **Rate Limiting and Segmentation**: Implement network segmentation and DoS protection controls between O-RU/O-DU/O-Cloud components to resist volumetric and targeted flooding attacks.

6. Compliance and Lifecycle Assurance
   a. **Secure Software Development Lifecycle (SSDLC):** Incorporate vulnerability scanning, secure coding, and continuous integration pipelines into development practices.
   b. **Zero Trust Architecture (ZTA):** Adopt principles that assume breach and enforce strict identity verification and dynamic policy enforcement across all assets.

4.4 AI assisted attacks on physical layer

AI-based jamming attacks require knowledge and time to infer the pattern used by the allocation algorithm, which is the first step to attack it efficiently. In [28], a dynamic defence is designed, based on deliberately making incorrect transmissions (selected using a confidence score of the channel) that makes the AI algorithm used by the attacker fail in correctly inferring how the legitimate algorithm operates. In [29][29], interference is used by the legit transmitter in some non-allocated RBS, to make the smart jamming attack them instead of the used RBs.

To keep AI eavesdroppers out at the physical layer, we could rely on different types of defences. As a first approach, we can shuffle the pilot tones and switch our beams at sub-frame timescales, an idea already suggested in the 5G security survey for stopping channel-inference attacks. Another option could be that once a shared key is built with PKG, we pass it through a privacy-amplification hash, following the lesson from the on-the-shoulder SKG study, which showed that a spy who stands only a few wavelengths away can lower the raw entropy but still fails after the hash [34]. Another idea is to keep a safety zone around each RF component when space is tight, measures listed as hardware shielding against RF-sensing side channels in the latest survey on malicious RF sensing [33]. The 6G security roadmap notes that such moving-target and shielding ideas are the best way to frustrate smarter, AI-driven eavesdroppers [38]. With these steps, the threat remains low, turning AI eavesdropping into more of a research challenge than a real weakness for our system.

5 Conclusions

The transition towards next-generation wireless networks, including advanced 5G and future 6G systems, brings significant technological advancements, but also exposes new and complex security challenges, particularly at the physical (PHY) layer. This deliverable, D5.1, provides a comprehensive threat modelling framework for the PHY layer, addressing this critical security domain through systematic identification of vulnerabilities, threat actors, attack vectors, and risk factors. The work presented here is a key milestone for the NATWORK project, laying the groundwork for secure-by-design development of resilient, self-adaptive communication networks that align with Europe's strategic ambitions in trustworthy and sovereign 6G services.

The threat modelling methodology developed in this document is based on recognised industry standards and best practice, such as ISO/IEC 27005 for risk management, the ENISA 5G Threat Landscape, and the O-RAN Security Threat Modelling framework. However, the methodology has been adapted and expanded to reflect the unique characteristics of the evolving wireless landscape. NATWORK's approach considers the expanded threat surface resulting from virtualization, multi-vendor deployments, AI-enhanced signal processing, and emerging physical-layer technologies such as Reconfigurable Intelligent Surfaces (RIS) and Massive MIMO. The result is a comprehensive, future-oriented threat model that addresses both conventional and novel attack scenarios relevant to 5G and beyond.

The analysis presented in this deliverable demonstrates that the physical layer remains highly susceptible to diverse and evolving threats. Classical threats such as jamming, eavesdropping, spoofing, and physical tampering continue to pose significant risks to wireless networks, especially when adversaries leverage AI-driven techniques to optimise these attacks or exploit system-level vulnerabilities introduced through virtualization and multi-vendor ecosystems. Moreover, the disaggregated, open architecture promoted by initiatives like O-RAN, while fostering innovation and interoperability, inherently introduces new vulnerabilities at both the PHY layer and across the broader network stack.

A key outcome of this work is the detailed risk and impact assessment, which provides a prioritised understanding of the most pressing security risks affecting the physical layer. This assessment considers both the likelihood of threat exploitation and the severity of potential consequences, particularly in relation to the confidentiality, integrity, and availability of wireless links. The findings highlight that many physical layer attacks have cascading impacts across network functions, with the potential to undermine service reliability, compromise sensitive data, or disrupt critical applications such as autonomous systems, IoT, and smart infrastructure.

The deliverable also presents targeted mitigation strategies tailored to the identified threats. These include both established countermeasures, such as signal obfuscation, pilot authentication, and beamforming security techniques, as well as novel approaches designed to address vulnerabilities arising from AI-driven attacks, RIS misuse, and virtualization-related weaknesses. The proposed measures emphasise a proactive, adaptive, and layered security approach, aligned with NATWORK's broader vision for perennial, encryption-free self-resilience at the PHY layer.

In conclusion, the work conducted in D5.1 establishes a robust foundation for secure-by-design practices in next-generation wireless networks, with a particular focus on safeguarding the physical layer as a critical enabler of system-wide security. It contributes directly to NATWORK's Operational Objective #4 by providing actionable insights into securing wireless links against evolving threats, while also informing downstream technical developments within the project, including AI-based anti-jamming mechanisms (D5.3) and energy-efficient security processes (D5.2). Moreover, the threat model developed here will continue to evolve throughout the project lifecycle, ensuring that NATWORK remains responsive to technological advancements and emerging adversarial tactics. Ultimately, this deliverable reinforces the project's commitment to supporting Europe's leadership in secure, resilient, and trustworthy 6G communications.

References

[1] CyberPeace Institute. (2022, June) *Case Study: Viasat Attack.* https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

[2] IEEE S2CY - P3536 - Space System Cybersecurity Design Standard Working Group. (2025) https://sagroups.ieee.org/3349/

[3] Falco, G., *et al*. (2024). Minimum Requirements for Space System Cybersecurity - Ensuring Cyber Access to Space. *2024 IEEE 10th International Conference on Space Mission Challenges for Information Technology (SMC-IT)*, pp. 78-88, doi: 10.1109/SMC-IT61443.2024.00016.

[4] Yahia, O.B., *et al*. (2024) Securing Satellite Link Segment: A Secure-by-Component Design. *2024 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)*, pp. 177-182, doi: 10.1109/WiSEE61249.2024.10850060.

[5] Kang, M., Park, S., & Lee, Y. (2024). A survey on satellite communication system security. *Sensors*, 24(9), 2897. https://doi.org/10.3390/s24092897

[6] Yahia, O. B., Erdogan, E., Kurt, G. K., Altunbas, I., & Yanikomeroglu, H. Optical satellite eavesdropping. *IEEE Transactions on Vehicular Technology,* 71(9), 10126–10131. https://doi.org/10.1109/TVT.2022.3176119

[7] Marudhai, V., Prince, S., & Kumari, S. (2022). Design and simulation of physical layer security for next generation intelligent optical networks. *Wireless Personal Communications,* 127(4), 3119–3138. https://doi.org/10.1007/s11277-022-09913-6

[8] Viswanathan, A., Bailey, B., Tan, K., & Falco, G. (2024). Secure-by-component: A system-of-systems design paradigm for securing space missions. *Security for Space Systems (3S)*, 1–9. doi: 10.23919/3S60530.2024.10592289.

[9] The Aerospace Corporation (2023) *SPARTA: Space attack research and tactic analysis*. https://aerospace.org/sparta.

[10] Lichtman, M., Rao, R., Marojevic, V., Reed, J., & Jover, R. P. (2018). 5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation. In 2018 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 1–6). IEEE. https://doi.org/10.1109/ICCW.2018.8403769

[11] International Organization for Standardization (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Edition 3 (ISO/IEC 27001:2022)

[12] O-RAN Alliance (2025). O-RAN.WG11.TR.Threat-Modeling.O-R004-v05.00

[13] ENISA (2020). Threat Landscape for 5G Networks Report, December 14, 2020 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

[14] Abdel Hakeem, S.A., Hussein, H.H., Kim, H. Security Requirements and Challenges of 6G Technologies and Applications. Sensors. 2022; 22(5):1969. https://doi.org/10.3390/s22051969

[15] International Organization for Standardization (2022). Information security, cybersecurity and privacy protection — Guidance on managing information security risks, Edition 4 (ISO/IEC 27005:2022).

[16] M. Kazemian, 'Investigating the Jamming Attack on 5G NR Physical Channels', Aug. 06, 2024, *arXiv*: arXiv:2408.03028. doi: 10.48550/arXiv.2408.03028.

[17] National Institute of Standards and Technology. (2022). *5G cybersecurity: Volume B – Approach, architecture, and security characteristics* (NIST Special Publication 1800-33B). U.S. Department of Commerce. https://www.nccoe.nist.gov/sites/default/files/2022-04/nist-5G-sp1800-33b-preliminary-draft.pdf.

[18] 3rd Generation Partnership Project (3GPP). (2022). *Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes* (3GPP TR 33.926 V17.3.0). ETSI. https://www.etsi.org/deliver/etsi_tr/133900_133999/133926/17.03.00_60/tr_133926v170300p.pdf.

[19] Lohan, P., Kantarci, B., Ferrag, M. A., Tihanyi, N., & Shi, Y. (2024). From 5G to 6G networks: A survey on AI-based jamming and interference detection and mitigation. IEEE Open Journal of the Communications Society, 5, 3920–3974. https://doi.org/10.1109/OJCOMS.2024.3416808

[20] Kazemian, M. (2024). Investigating the jamming attack on 5G NR physical channels. arXiv. https://arxiv.org/abs/2408.03028

[21] Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE*, *104*(6), 1258-1270.

[22] M. Harvanek, J. Bolcek, J. Kufa, L. Polak, M. Simka and R. Marsalek, "Survey on 5G Physical Layer Security Threats and Countermeasures," *Sensors (Basel, Switzerland),* vol. 24, no. 17, 2024.

[23] N. Ludant, M. Vomvas and G. Noubir, "Unprotected 4G/5G Control Procedures at Low Layers Considered Dangerous," *arXiv preprint,* vol. 2403, no. 06717, 2024.

[24] 3GPP, 3GPP TS 38.211 Version 15.2.0 Release 15, 2018.

[25] E. Bitsikas and C. Pöpper, "Don't hand it Over: Vulnerabilities in the Handover Procedure of Cellular Telecommunications," in Annual Computer Security Applications Conferenc, 2021.

[26] NSO Group, "NSO Pegasus," 2015. [Online]. Available: https://embed.documentcloud.org/documents/4599753-NSO-Pegasus/?mode=document&embed=1. [Accessed 13 05 2025].

[27] 3GPP, *3GPP TS 33.501, V19.2.0,* 2025.

[28] Sagduyu, Y. E., Shi, Y., & Erpek, T. (2021). Adversarial deep learning for over-the-air spectrum poisoning attacks. *IEEE Transactions on Mobile Computing, 20*(2), 306–319. https://doi.org/10.1109/TMC.2019.2950398

[29] Salehi, S., Zhou, H., Elsayed, M., Bavand, M., Gaigalas, R., Ozcan, Y., & Erol-Kantarci, M. (2024). Smart jamming attack and mitigation on deep transfer reinforcement learning enabled resource allocation for network slicing. *IEEE Transactions on Machine Learning in Communications and Networking, 2*, 1492–1508. https://doi.org/10.1109/TMLCN.2024.3470760

[30] Zhou, X., Maham, B., & Hjorungnes, A. (2012). Pilot contamination for active eavesdropping. IEEE Transactions on Wireless Communications, 11(3), 903-907.

[31] Alharbi, I. A., Almalki, A. J., Alyami, M., Zou, C., & Solihin, Y. (2022). Profiling attack on wifi-based iot devices using an eavesdropping of an encrypted data frames. Adv. Sci. Technol. Eng. Syst. J, 7, 49-57.

[32] Nashat, D., & Khairy, S. (2025). Statistical-based detection of pilot contamination attack for NOMA in 5G networks. Scientific Reports, 15(1), 3726.

[33] Han, M., Yang, H., Li, W., Xu, W., Cheng, X., Mohapatra, P., & Hu, P. (2025). RF Sensing Security and Malicious Exploitation: A Comprehensive Survey. arXiv preprint arXiv:2504.10969.

[34] Mayya, A., Mitev, M., Chorti, A., & Fettweis, G. (2023, December). A SKG security challenge: Indoor SKG under an on-the-shoulder eavesdropping attack. In GLOBECOM 2023-2023 IEEE Global Communications Conference (pp. 3451-3456). IEEE.

[35] Amnesty International, "Morocco: Human Rights Defenders Targeted with NSO Group's Spyware," 10 10 2019. [Online]. Available: https://www.amnesty.org/en/latest/research/2019/10/Morocco-Human-Rights-Defenders-Targeted-with-NSO-Groups-Spyware/. [Accessed 13 05 2025].

[36] Amnesty International, "Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools," 22 06 2020. [Online]. Available: https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/. [Accessed 13 05 2025].

[37] H. N. Fakhouri, S. Alawadi, F. M. Awaysheh, I. Bani Hani, M. Alkhalaileh and F. Hamad, "A Comprehensive Study on the Role of Machine Learning in 5G Security: Challenges, Technologies, and Solutions," *Electronics,* vol. 12, no. 22, 2023.

[38] Saeed, M. M., Saeed, R. A., Hasan, M. K., Ali, E. S., Mazha, T., Shahzad, T., ... & Hamam, H. (2025). A comprehensive survey on 6G-security: physical connection and service layers. Discover Internet of Things, 5(1), 28.

[39] NIST, "tampering," [Online]. Available: https://csrc.nist.gov/glossary/term/tampering. [Accessed 13 05 2025].

[40] C. Miller, Chip War: the fight for the world's most cirtical technology, Simon and Schuster, 2022.

[41] J. Kannisto and Qualcomm Finland RFFE Oy, "Secure Boot and Image Authentication Technical Overview (v3.0)," 05 12 2024. [Online]. Available: https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/secure-boot-and-image-authentication.pdf. [Accessed 13 05 2025].

[42] M. K. S. Uddin, F. Z. Rozony and M. Kamruzzaman, "Common Cybersecurity Vulnerabilities: Software Bugs, Weak Passwords, Misconfigurations, Social Engineering," *Global Mainstream Journal of Innovation, Engineering & Emerging Technology,* vol. 3, no. 4, pp. 42-57, 2024.

[43] M. Mutlutürk, M. Wynn and B. Metin, "Phishing and the Human Factor: Insights from a Bibliometric Analysis," *Information ,* vol. 15, no. 10, 2024.

[44] Kapersky Lab, "Information security violations by staff do as much harm as hacking, Kaspersky global study shows," 22 11 2023. [Online]. Available: https://www.kaspersky.com/about/press-releases/information-security-violations-by-staff-do-as-much-harm-as-hacking-kaspersky-global-study-shows?utm_source=chatgpt.com. [Accessed 13 05 2025].

[45] Liaskos, C., Mamatas, L., Pourdamghani, A., Tsioliaridou, A., Ioannidis, S., Pitsillides, A., . . . Akyildiz, I. F. (2022). Software-defined reconfigurable intelligent surfaces: From theory to end-to-end implementation. Proceedings of the IEEE, 110, 1466–1493.

[46] Liaskos, C., Tsioliaridou, A., Pitsillides, A., Ioannidis, S., & Akyildiz, I. (2018). Using any surface to realize a new paradigm for wireless communications. *Communications of the ACM, 61*, 30–33.

[47] Basar, E. (2021). Reconfigurable intelligent surfaces for Doppler effect and multipath fading mitigation. *frontiers in Communications and Networks, 2*, 672857.

[48] Boulogeorgos, A.–A. A., Alexiou, A., & Michalas, A. (2023). On the physical layer security capabilities of reconfigurable intelligent surface empowered wireless systems. *arXiv preprint arXiv:2308.09906*.

[49] Mackensen, P., Staat, P., Roth, S., Sezgin, A., Paar, C., & Moonsamy, V. (2024). Spatial-Domain Wireless Jamming with Reconfigurable Intelligent Surfaces. *arXiv preprint arXiv:2402.13773*.

[50] Kaur, R., Bansal, B., Majhi, S., Jain, S., Huang, C., & Yuen, C. (2024). A survey on reconfigurable intelligent surface for physical layer security of next-generation wireless communications. *IEEE open journal of vehicular technology, 5*, 172–199.

[51] de Sena, A. S., Kibiłda, J., Mahmood, N. H., Gomes, A., & Latva-Aho, M. (2024). Malicious RIS versus massive MIMO: Securing multiple access against RIS-based jamming attacks. *IEEE Wireless Communications Letters, 13*, 989–993.

[52] Alakoca, H., Namdar, M., Aldirmaz-Colak, S., Basaran, M., Basgumus, A., Durak-Ata, L., & Yanikomeroglu, H. (2022). Metasurface manipulation attacks: Potential security threats of RIS-aided 6G communications. *IEEE Communications Magazine, 61*, 24–30.

[53] Naeem, F., Ali, M., Kaddoum, G., Huang, C., & Yuen, C. (2023). Security and privacy for reconfigurable intelligent surface in 6G: A review of prospective applications and challenges. IEEE Open Journal of the Communications Society, 4, 1196–1217.

[54] Huang, K.-W., & Wang, H.-M. (2020). Intelligent reflecting surface aided pilot contamination attack and its countermeasure. *IEEE Transactions on Wireless Communications, 20*, 345–359.

[55] Elijah, O., Leow, C. Y., Rahman, T. A., Nunoo, S., & Iliya, S. Z. (2015). A comprehensive survey of pilot contamination in massive MIMO—5G system. *IEEE Communications Surveys & Tutorials, 18*, 905–923.

[56] Jubin, J., Ashikhmin, A., Marzetta, T. L., & Vishwanath, S. (2011). Pilot Contamination and Precoding in Multi-Cell TDD Systems. IEEE Transactions on Wireless Communications, 10, 2640-2651. doi:10.1109/TWC.2011.060711.101155

[57] J. Zhang, B. Zhang, S. Chen, X. Mu, M. El-Hajjar and L. Hanzo, "Pilot Contamination Elimination for Large-Scale Multiple-Antenna Aided OFDM Systems," *IEEE Journal of Selected Topics in Signal Processing,* vol. 8, pp. 759-772, 2014.

[58] Zhou, X., Maham, B., & Hjørungnes, A. (2012). Pilot Contamination for Active Eavesdropping. *IEEE Transactions on Wireless Communications, 11*, 903-907.

[59] Kapetanovic, D., Zheng, G., & Rusek, F. (2015). Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. *IEEE Communications Magazine, 53(6), 21-27.*

[60] Jiao, L., Wang, N., Wang, P., Alipour-Fanid, A., Tang, J., & Zeng, K. (2019). Physical layer key generation in 5G wireless networks. *IEEE wireless communications, 26*, 48–54.

[61] Chen, X., Lei, L., Zhang, H., & Yuen, C. (2015). Large-scale MIMO relaying techniques for physical layer security: AF or DF? IEEE Transactions on Wireless Communications, 14, 5135–5146.

[62] Basciftci, Y. O., Koksal, C. E., & Ashikhmin, A. (2015). Securing Massive MIMO at the Physical Layer. IEEE Conference on Communications and Network Security (pp. 272-279). IEEE.

[63] Atallah, M., Kaddoum, G., & Kong, L. (2015). A Survey on Cooperative Jamming Applied to Physical Layer Security. IEEE.

[64] Cumanan, K., Xing, H., Xu, P., Zheng, G., Dai, X., Nallanathan, A., ... & Karagiannidis, G. K. (2016). Physical layer security jamming: Theoretical limits and practical designs in wireless networks. *IEEE Access*, *5*, 3603-3611.

[65] Rawat, D. B., White, T., Parwez, M. S., Bajracharya, C., & Song, M. (2017). Evaluating Secrecy Outage of Physical Layer Security in Large-Scale MIMO Wireless Communications for Cyber-Physical Systems. IEEE Internet of Things Journal, 4, 1987-1998.

[66] Huo , Y., Tian, Y., Ma, L., Cheng, X., & Jing, T. (2018). Jamming Strategies for Physical Layer Security. IEEE Wireless Communications, 25, 148-157.

[67] Heo, J., Sung, S., Lee, H., Hwang, I., & Hong, D. (2023). MIMO Satellite Communication Systems: A Survey From the PHY Layer Perspective. IEEE Communications Surveys & Tutorials, 25, 1543-1572.

[68] Tang, J., Dabaghchian, M., Zeng, K., & Wen, H. (2018). Impact of Mobility on Physical Layer Security Over Wireless Fading Channels. IEEE Transactions on Wireless Communications, 17, 7849-7863.

[69] Liu, Y., Zhang, P., Liu, J., Shen, Y., & Jiang, X. (2022). Physical Layer Authentication in MIMO Systems: A Carrier Frequency Offset Approach. Wireless Networks, 28, 1909-1921.

[70] Yu, K., Yu, J., & Luo, C. (2023). The Impact of Mobility on Physical Layer Security of 5G IoT Networks. IEEE/ACM Transactions on Networking, 31, 1042-1057.

[71] Peppas, K. P., Sagias, N. C., & Maras, A. (2015). Physical layer security for multiple-antenna systems: A unified approach. IEEE Transactions on Communications, 64, 314–328.

[72] Kavaiya, S., Patel, D. K., Ding, Z., Guan, Y. L., & Sun, S. (2020). Physical layer security in cognitive vehicular networks. IEEE Transactions on Communications, 69, 2557–2569.

[73] Yang, N., Suraweera, H. A., Collings, I. B., & Yuen, C. (2012). Physical layer security of TAS/MRC with antenna correlation. IEEE Transactions on Information Forensics and Security, 8, 254–259.

[74] Forenza, A., Love, D. J., & Heath, R. W. (2007). Simplified spatial correlation models for clustered MIMO channels with different array configurations. IEEE Transactions on Vehicular Technology, 56, 1924–1934.

[75] Alharbi, I. A. (2022). Profiling attack on WiFi-based IoT devices using an eavesdropping of an encrypted data frames. Advances in Science, Technology and Engineering Systems Journal, 7, 49-57.

[76] Han, M. Y. (2025). RF sensing security and malicious exploitation: A comprehensive survey.

[77] Saeed, M. M. (2025). A comprehensive survey on 6G-security: Physical connection and service layers. Discover Internet of Thing, 5(1).

[78] Yan, W., Yuan, X., He, Z.-Q., & Kuai, X. (2020). Passive beamforming and information transfer design for reconfigurable intelligent surfaces aided multiuser MIMO systems. IEEE Journal on Selected Areas in Communications, 38, 1793–1808.

[79] Lyu, B., Hoang, D. T., Gong, S., Niyato, D., & Kim, D. I. (2020). IRS-based wireless jamming attacks: When jammers can attack without power. IEEE Wireless Communications Letters, 9, 1663–1667.

[80] Staat, P., Elders-Boll, H., Heinrichs, M., Zenger, C. T., & Paar, C. (2021). Mirror mirror on the wall: wireless environment reconfiguration attacks based on fast software-controlled surfaces, CoRR, vol. abs/2107.01709. arXiv preprint arXiv:2107.01709.

[81] Hu, L., Li, G., Luo, H., & Hu, A. (2021). On the RIS manipulating attack and its countermeasures in physical-layer key generation. 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), (pp. 1–5).

[82] Wang, Y., Lu, H., Zhao, D., Deng, Y., & Nallanathan, A. (2022). Wireless communication in the presence of illegal reconfigurable intelligent surface: Signal leakage and interference attack. IEEE Wireless Communications, 29, 131–138.

[83] Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. Future Generation Computer Systems, 129, 77–89.

[84] Gurunath, R., Agarwal, M., Nandi, A., & Samanta, D. (2018). An overview: security issue in IoT network. 2018 2nd international conference on I-SMAC (IoT in social, Mobile, analytics and cloud)(I-SMAC) I-SMAC (IoT in social, Mobile, analytics and cloud)(I-SMAC), 2018 2nd international conference on, (pp. 104–107).

[85] Yang, H., Cao, X., Yang, F., Gao, J., Xu, S., Li, M., . . . Li, S. (2016). A programmable metasurface with dynamic polarization, scattering and focusing control. Scientific reports, 6, 35692.

[86] Basar, E. (2016). Index modulation techniques for 5G wireless networks. IEEE Communications Magazine, 54, 168–175.

[87] Zappone, A., Di Renzo, M., Shams, F., Qian, X., & Debbah, M. (2020). Overhead-aware design of reconfigurable intelligent surfaces in smart radio environments. IEEE Transactions on Wireless Communications, 20, 126–141.

[88] Chen, J., Liang, Y.-C., Cheng, H. V., & Yu, W. (2023). Channel estimation for reconfigurable intelligent surface aided multi-user mmWave MIMO systems. IEEE Transactions on Wireless Communications, 22, 6853–6869.

[89] Mirza, J., & Ali, B. (2021). Channel estimation method and phase shift design for reconfigurable intelligent surface assisted MIMO networks. IEEE Transactions on Cognitive Communications and Networking, 7, 441–451.

[90] Ma, X., Zhang, D., Xiao, M., Huang, C., & Chen, Z. (2023). Cooperative beamforming for RIS-aided cell-free massive MIMO networks. IEEE Transactions on Wireless Communications, 22, 7243–7258.

[91] Li, R., Guo, B., Tao, M., Liu, Y.-F., & Yu, W. (2022). Joint design of hybrid beamforming and reflection coefficients in RIS-aided mmWave MIMO systems. IEEE Transactions on Communications, 70, 2404–2416.

[92] Zegrar, S. E., Furqan, H. M., & Arslan, H. (2022). Flexible physical layer security for joint data and pilots in future wireless networks. IEEE Transactions on Communications, 70, 2635–2647.

[93] Melki, R., Noura, H. N., Mansour, M. M., & Chehab, A. (2020). Physical layer security schemes for MIMO systems: an overview. Wireless networks, 26, 2089–2111.

[94] Biguesh, M., & Gershman, A. B. (2006). Training-based MIMO channel estimation: A study of estimator tradeoffs and optimal training signals. IEEE transactions on signal processing, 54, 884–893.

[95] Shi, S., Schubert, M., & Boche, H. (2008). Downlink MMSE transceiver optimization for multiuser MIMO systems: MMSE balancing. IEEE Transactions on Signal Processing, 56, 3702–3712.

[96] Ma, J., Zhang, Y. J., Su, X., & Yao, Y. (2008). On capacity of wireless ad hoc networks with MIMO MMSE receivers. IEEE Transactions on Wireless Communications, 7, 5493–5503.

[97] Huang, B., Wang, W.-Q., Basit, A., & Gui, R. (2022). Bayesian detection in Gaussian clutter for FDA-MIMO radar. IEEE Transactions on Vehicular Technology, 71, 2655–2667.

[98] Wen, C.-K., Jin, S., Wong, K.-K., Chen, J.-C., & Ting, P. (2014). Channel estimation for massive MIMO using Gaussian-mixture Bayesian learning. IEEE Transactions on Wireless Communications, 14, 1356–1368.

[99] Mishra, A., Gupta, V., Dwivedi, S., Jagannatham, A. K., & Varshney, P. K. (2018). Sparse Bayesian learning-based target imaging and parameter estimation for monostatic MIMO radar systems. IEEE Access, 6, 68545–68559.

[100] Ma, X., & Gao, Z. (2020). Data-driven deep learning to design pilot and channel estimator for massive MIMO. IEEE Transactions on Vehicular Technology, 69, 5677–5682.

[101] He, H., Wen, C.-K., Jin, S., & Li, G. Y. (2018). Deep learning-based channel estimation for beamspace mmWave massive MIMO systems. IEEE Wireless Communications Letters, 7, 852–855.

[102] Chun, C.-J., Kang, J.-M., & Kim, I.-M. (2019). Deep learning-based channel estimation for massive MIMO systems. IEEE Wireless Communications Letters, 8, 1228–1231.

[103] Balevi, E., Doshi, A., & Andrews, J. G. (2020). Massive MIMO channel estimation with an untrained deep neural network. IEEE Transactions on Wireless Communications, 19, 2079–2090.

[104] Vinogradova, J., Björnson, E., & Larsson, E. G. (2016). Detection and mitigation of jamming attacks in massive MIMO systems using random matrix theory. 2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), (pp. 1–5).

[105] Akhlaghpasand, H., Razavizadeh, S. M., Björnson, E., & Do, T. T. (2017). Jamming detection in massive MIMO systems. IEEE Wireless Communications Letters, 7, 242–245.

[106] Akhlaghpasand, H., Björnson, E., & Razavizadeh, S. M. (2019). Jamming suppression in massive MIMO systems. IEEE Transactions on Circuits and Systems II: Express Briefs, 67, 182–186.

[107] Xu, J., Liao, G., Zhu, S., & So, H. C. (2015). Deceptive jamming suppression with frequency diverse MIMO radar. Signal Processing, 113, 9–17.

[108] Lan, L., Xu, J., Liao, G., Zhang, Y., Fioranelli, F., & So, H. C. (2020). Suppression of mainbeam deceptive jammer with FDA-MIMO radar. IEEE Transactions on Vehicular Technology, 69, 11584–11598.

[109] Chen, C.-Y., & Vaidyanathan, P. P. (2008). MIMO radar ambiguity properties and optimization using frequency-hopping waveforms. IEEE Transactions on signal processing, 56, 5926–5936.

[110] Wu, K., Zhang, J. A., Huang, X., & Guo, Y. J. (2021). Frequency-hopping MIMO radar-based communications: An overview. IEEE Aerospace and Electronic Systems Magazine, 37, 42–54.

[111] Wu, K., Zhang, J. A., Huang, X., Guo, Y. J., & Heath, R. W. (2020). Waveform design and accurate channel estimation for frequency-hopping MIMO radar-based communications. IEEE Transactions on Communications, 69, 1244–1258.

[112] Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L., & Zeng, K. (2019). Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. IEEE internet of things journal, 6, 8169–8181.

[113] Al Kassir, H., Zaharis, Z. D., Lazaridis, P. I., Kantartzis, N. V., Yioultsis, T. V., & Xenos, T. D. (2022). A review of the state of the art and future challenges of deep learning-based beamforming. IEEE Access, 10, 80869–80882.

[114] Chary, M. K., Krishna, C. V., & Krishna, D. R. (2024). Accurate channel estimation and hybrid beamforming using Artificial Intelligence for massive MIMO 5G systems. AEU-International Journal of Electronics and Communications, 173, 154971.

[115] Jensen, M. A., & Wallace, J. W. (2004). A review of antennas and propagation for MIMO wireless communications. IEEE Transactions on Antennas and propagation, 52, 2810–2824.

[116] Liu, H., Gao, S., & Loh, T. H. (2013). Compact MIMO antenna with frequency reconfigurability and adaptive radiation patterns. IEEE Antennas and Wireless Propagation Letters, 12, 269–272.

[117] Abdalla, M. A., & Ibrahim, A. A. (2013). Compact and closely spaced metamaterial MIMO antenna with high isolation for wireless applications. IEEE antennas and wireless propagation letters, 12, 1452–1455.

[118] Deng, J.-Y., Guo, L.-X., & Liu, X.-L. (2015). An ultrawideband MIMO antenna with a high isolation. IEEE antennas and wireless propagation letters, 15, 182–185.

[119] Waldschmidt, C., & Wiesbeck, W. (2004). Compact wide-band multimode antennas for MIMO and diversity. IEEE Transactions on Antennas and Propagation, 52, 1963–1969.

[120] Zhang, Y., Deng, J.-Y., Li, M.-J., Sun, D., & Guo, L.-X. (2019). A MIMO dielectric resonator antenna with improved isolation for 5G mm-wave applications. IEEE Antennas and Wireless Propagation Letters, 18, 747–751.

[121] Albreem, M. A., Al Habbash, A. H., Abu-Hudrouss, A. M., & Ikki, S. S. (2021). Overview of precoding techniques for massive MIMO. IEEE Access, 9, 60764–60801.

[122] Alkhateeb, A., Mo, J., Gonzalez-Prelcic, N., & Heath, R. W. (2014). MIMO precoding and combining solutions for millimetre-wave systems. IEEE Communications Magazine, 52, 122–131.

[123] Forenza, A., McKay, M. R., Pandharipande, A., Heath, R. W., & Collings, I. B. (2007). Adaptive MIMO transmission for exploiting the capacity of spatially correlated channels. IEEE Transactions on Vehicular Technology, 56, 619–630.

[124] Chae, C.-B., Forenza, A., Heath, R. W., McKay, M. R., & Collings, I. B. (2010). Adaptive MIMO transmission techniques for broadband wireless communication systems [Topics in Wireless Communications]. IEEE Communications Magazine, 48, 112–118.