Smart, Automated, and Reliable Security Service Platform for 6G

Deliverable D2.1
6G Threat Analysis Report

Co-funded by the European Union

ROBUST-6G project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101139068.

Date of delivery:	01/07/2024	Version:	1.0
Project reference:	101139068	Call:	HORIZON-JU-SNS-2023
Start date of project:	01/01/2024	Duration:	30 months

Document properties:

Document Number:	D2.1
Document Title:	6G Threat Analysis Report
Editor(s):	Tommy Svensson (CHA)
Authors:	Tommy Svensson (CHA), Arsenia Chorti (ENSEA), Tomas Olovsson (CHA), Betül Güvenç Paltun (EBY), Güneş Kesik (EBY), Giovanni Perin (UNIPD), Michele Rossi (UNIPD), Chamara Sandeepa (UCD), Thulitha Senevirathna (UCD), Bartlomiej Siniarski (UCD), Madhusanka Liyanage (UCD), Marco Ruta (NXW), Pietro G. Giardina (NXW)
Contractual Date of Delivery:	30/06/2024
Dissemination level:	PU
Status:	Final
Version:	1.0
File Name:	ROBUST-6G D2.1_v1.0

Revision History

Revision	**Date**	**Issued by**	**Description**
0.1	06.03.2024	ROBUST-6G WP2	Initial draft with ToC
0.2	03.04.2024	ROBUST-6G WP2	First draft with SoA
0.3	08.04.2024	ROBUST-6G WP2	First complete draft
0.4	30.05.2024	ROBUST-6G WP2	Revised version after internal review
0.5	26.06.2024	ROBUST-6G WP2	Revised version after internal review
0.6	27.06.2024	ROBUST-6G WP2	Revised version after internal review
1.0	30.06.2024	ROBUST-6G WP2	Final version

Abstract

This deliverable provides a state-of-the-art review on existing solutions for threat detection and protection, and an analysis of the characterization of security threats in 6G networks. The analysis is performed on selected key 6G technical enablers, use cases and applications with a focus on physical layer threats, for AI/ML modules, and for Application Programming Interfaces (APIs), within a common framework on threat analysis. This document will serve as basis for the design of cybersecurity capabilities within the other technical work packages in ROBUST-6G.

Keywords

6G, Threat analysis, Threat detection, Threat protection, Physical layer security, ML/AI

Disclaimer

Funded by the European Union. The views and opinions expressed are however those of the author(s) only and do not necessarily reflect the views of ROBUST-6G Consortium nor those of the European Union or Horizon Europe SNS JU. Neither the European Union nor the granting authority can be held responsible for them.

Executive Summary

6G is anticipated to play a significant role in the continuing development of modern civilization through the 2030's, as the convergence between the digital and physical worlds becomes a reality. It will assist in fulfilling far more stringent requirements than before and serving more challenging applications such as holographic telepresence and immersive communication. Joint sensing and communication, programmability, intelligent connected management and control functions, reduced energy footprint, trustworthy systems, scalability, and affordability are among the foremost characteristics of 6G.

To address the demanding and diverse needs of the anticipated use cases, 6G networks must be highly programmable, exceedingly adaptable, and efficient. Nevertheless, the additional level of efficiency, programmability and flexibility will come at the expense of increasing complexity in managing and operating 6G networks. To bring this complexity under control, a paradigm shift towards complete automation of network and service management is required. However, a significant obstacle to full automation is the protection of the network services, infrastructure and data against possible cybersecurity risks introduced by the unheard-of expansion of the 6G threat landscape.

To this end, this Deliverable D2.1 – 6G Threat Analysis Report in the ROBUST-6G project is the result of the work on assessing existing solutions and characterization of the threat landscape towards 6th Generation (6G). The deliverable reviews the current state of the art with the goal of exploring existing cyber security solutions driven by Artificial Intelligence (AI)/Machine Learning (ML) for new 6G networks. Contributions found in the literature, Standards Development Organization (SDOs), and other related European projects are evaluated to identify technical synergies and gaps that the ROBUST-6G framework will address.

This deliverable provides a state-of-the-art review on existing solutions for threat detection and protection, and an analysis of the characterization of security threats in 6G networks. The analysis is performed on selected key 6G technical enablers, use cases and applications with a focus on physical layer threats, for AI/ML modules, and for Application Programming Interfaces (APIs), within a common framework on threat analysis. This document will serve as basis for the design of cybersecurity capabilities within the other technical work packages in ROBUST-6G.

Table of Contents

1 Introduction 10
1.1 Motivation, objectives, and scope 10
1.2 Document structure 10

2 State of the Art 11
2.1 5G Threat Analysis 11
2.2 6G Threat Analysis 12
2.2.1 Network of Networks (NoN) compositional pattern 12
2.2.2 Use of a cloud continuum as base infrastructural approach 13
2.2.3 Application of radical disaggregation mechanisms 13
2.2.4 AI security 13
2.2.5 AI privacy preservation 14

3 Methodology for Threat Identification 14
3.1 The CIA model 14
3.2 Microsoft STRIDE 14
3.3 Threat, Vulnerability and Risk assessment 15
3.3.1 ETSI TVRA 16
3.3.2 HEAVENS 16
3.4 FiGHT 5G Hierarchy of Threats 16

4 Considered Key 6G Technical Enablers, Use Cases and Applications 17
4.1 Distributed Multiple-Input Multiple-Output 17
4.2 Reconfigurable Intelligent Surfaces 18
4.3 mmWaves and sub-THz 19
4.4 RF Sensing and Localization 19
4.4.1 Sensing and Localization with Communication Networks 19
4.4.2 Frequencies for Localization and Sensing 20
4.4.3 Localization and Sensing Methodologies 21
4.4.4 Signal Processing for Communications and Sensing 21
4.4.5 AI/ML for Localization and Sensing 21
4.4.6 Cooperative Sensing 22
4.4.7 Emerging Communication Technologies for Sensing and its role in 6G Systems . 22
4.4.8 Applications 22
4.5 Privacy and Security for Distributed Learning 23
4.5.1 Distributed Learning 23
4.5.2 Fully decentralized federated learning 25
4.5.3 Computational complexity and energy efficiency of defence mechanisms 25
4.5.4 Federated Learning 25
4.6 Internet of Things (IoT) 26
4.6.1 Radio Frequency Identification (RFID) for smart healthcare 26
4.6.2 Long Range (LoRA) for smart agriculture 27
4.6.3 Vehicle to everything (V2X) sidelinks 27
4.7 Application Programming Interface (API) Exposure for Beyond 5G Networks 27

5 Threat Matrix for Selected Cases 28
5.1 Distributed Multiple-Input Multiple-Output 28
5.2 Reconfigurable Intelligent Surface 29
5.3 mmWaves and sub-THz 30
5.4 Distributed Federated Learning 33
5.4.1 Analysis 1 33
5.4.2 Analysis 2 34
5.5 Internet of Things 36
5.5.1 RFIDs for Smart Healthcare 36
5.5.2 LoRA Smart Agriculture 37
5.5.3 V2X Sidelink 39
5.6 Threat Matrix for API Exposure 40

6 Conclusions 47

List of Tables

Table 3-1: Mapping between STRIDE threats and security attributes 14
Table 3-2: Comparative view of parameters to determine threat level [HEA16-D2, Table 4-3]. 15
Table 4-1: Taxonomy of common attacks in distributed learning 23
Table 4-2: Common defence mechanisms used in distributed learning 24
Table 5-1: Threat matrix on D-MIMO 28
Table 5-2: Threat matrix on RIS 29
Table 5-3: Threat matrix on mmWaves and sub-THz 31
Table 5-4: Threat matrix of common security and privacy attacks against DFL 33
Table 5-5: Threat matrix of specific security and privacy attacks against DFL 34
Table 5-6: Threat matrix on RFIDs for Smart Healthcare 36
Table 5-7: Threat matrix on LoRA Smart Agriculture 37
Table 5-8: Threat matrix on V2X Sidelink 39
Table 5-9: Potential threats to the end-to-end exposure functionality view 41
Table 5-10: Adversary types for threats to APIs 45

Acronyms and abbreviations

Term	Description
3GPP	Third Generation Partnership Project
4G	4th Generation
5G	5th Generation
5GPPP	5G infrastructure Public Private Partnership
6G	6th Generation
AFDM	Affine Frequency Division Multiplexing
AI	Artificial Intelligence
AoA	Angle of Arrival
AP	Access Point
API	Application Programming Interface
BS	Base Station
CAPIF	Common API framework
CC	Common Criteria/Control Channel
CFR	Channel Frequency Response
CIA	Confidentiality, Integrity and Availability
CIR	Channel Impulse Response
D2D	Device-to-Device

DDoS	Distributed Denial of Service
DFL	Decentralized Federated Learning
DFT-s-OFDM	Discrete Fourier Transform-spread-OFDM
DL	Distributed Learning/ DownLink
D-MIMO	Distributed Multiple-Input Multiple-Output
DP	Differential Privacy
DRL	Deep Reinforcement Learning
E2E	End-to-End
EAPI	Enriched Application Programming Interface
ESPRIT	Estimation of Signal Parameters via Rotational Invariance Techniques
ETSI	European Telecommunications Standards Institute
EU	European Union
EVITA	E-safety Vehicle Intrusion Protected Applications
FBMC	Filter-Bank MultiCarrier
fBS	false Base Stations
FL	Federated Learning
FR	Frequency Range
gNB	gNodeB
GSMA	Global System for Mobile communication Association
HCI	Human-Computer Interaction
HDBSCAN	Hierarchical Density-Based Spatial Clustering of Applications with Noise
HEAVENS	HEAling Vulnerabilities to ENhance Software
HW	HardWare
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IFFT	Inverse Fast Fourier Transform
IoT	Internet of Things
IPUPS	Inter-PLMN UP Security
ISAC	Integrated Sensing And Communication
ISG	Integrated Security Gateway
ISM	Industrial, Scientific and Medical
ISO	International Organization for Standardization
LFM	Linear Frequency Modulation
LoRA	Long Range
LOS	Line-Of-Sight
LPWAN	Low-Power, Wide-Area Network

LTE	LongTerm Evolution
MIA	Membership inference attack
MIMO	Multiple-Input Multiple-Output
MITM	Man-In-The-Middle
ML	Machine Learning
MPC	MultiParty Computation
MUSIC	MUltiple SIgnal Classification
MVDR	Minimum Variance Distortionless Response
MWC	Mobile World Congress
NaaS	Network as a Service
NAPI	New Application Programming Interface
NBI	North Bound Interface
NBIs	North Bound Interfaces
NFV	Network Functions Virtualisation
NLOS	Non-Line-Of-Sight
NoN	Network of Networks
NS	Network Service
OCDM	Orthogonal Chirp Division Multiplexing
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OWASP	Open Web Application Security Project
PHY	PHYsical (layer)
PLMN	Public Land Mobile Network
PLS	Physical Layer Security
PUF	Physically Unclonable Functions
QoD	Quality on Demand
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
RFID	Radio Frequency IDentification
RIS	Reconfigurable Intelligent Surfaces
RISA	RISA RIS Actuator
RISC	RIS controller
RISO	RIS orchestrator
RL	Reinforcement Learning
RU	Remote Unit

SBI	South Bound Interface
SDO	Standards Development Organization
SEPP	Security Edge Protection Proxy
SHAP	SHapley Additive exPlanations
SKG	Secret Key Generation
SL	SideLink
SLAM	Simultaneous Localization And Mapping
SP	Security and Privacy
SSE	Secrecy Spectral Efficiency
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
TVRA	Threat, Vulnerability and Risk Assessment
UAV	Unmanned Aerial Vehicles
UE	User Equipment
UL	UpLink
UP	User Plane
URLLC	Ultra-Reliable Low-Latency Communication
US	United States
V2X	Vehicle-to-Everything
XAI	eXplainable Artificial Intelligence

1 Introduction

6G is anticipated to play a significant role in the continuing development of modern civilization through the 2030's, as the convergence between the digital and physical worlds becomes a reality. It will assist in fulfilling far more stringent requirements than before and serving more challenging applications such as holographic telepresence and immersive communication. Joint sensing and communication, programmability, intelligent connected management and control functions, reduced energy footprint, trustworthy systems, scalability, and affordability are among the foremost characteristics of 6G.

To address the demanding and diverse needs of the anticipated use cases, 6G networks must be highly programmable, exceedingly adaptable, and efficient. Nevertheless, the additional level of efficiency, programmability and flexibility will come at the expense of increasing complexity in managing and operating 6G networks. To bring this complexity under control, a paradigm shift towards complete automation of network and service management is required. However, a significant obstacle to full automation is the protection of the network services (NS), infrastructure and data against possible cybersecurity risks introduced by the unheard-of expansion of the 6G threat landscape.

1.1 Motivation, objectives, and scope

ROBUST-6G aims to address these cybersecurity risks by introducing cutting-edge approaches for security management of 6G networks at the level of services and infrastructure and physical layer. To achieve this aim, ROBUST-6G will design and put into practice a fully automated end-to-end (E2E) smart network and service security management framework by utilizing Zero-touch network and Service Management (ZSM) and Artificial Intelligence/Machine Learning (AI/ML) techniques.

To that end, the objectives and scope of this deliverable are to provide a state-of-the-art review on existing solutions for threat detection and protection, and an analysis of the characterization of security threats in 6G networks. Focus is on access network threats, network entry phrases, eavesdropping and man-in-the-middle (MITM) attacks on the PHY, but we also identify threats on ML/AI modules and Application Programming Interfaces (APIs). The analysis is performed on selected key 6G technical enablers, use cases and applications within a common framework on threat analysis.

This document serves as basis for the design of cyber threat capabilities within the other technical work packages in ROBUST-6G and together with the use case and system requirements sections of D2.2 and D2.3 it creates the basis for the ROBUST-6G security architecture.

1.2 Document structure

The structure of deliverable D2.1 is as follows.

In Sec. 0, we provide a state-of-the-art on existing solutions for threat detection and protection in 5th Generation (5G) networks and emerging 6G networks. In Sec. 3, we give an overview of existing methodologies for threat identification, which we later use for threat identification of a set of key 6G technical enablers, use cases and applications. In Sec. 0, we introduce our considered key 6G technical enablers, use cases and applications, and in Sec. **Error! Reference source not found.** we present our threat analysis of these k ey 6G technical enablers, use cases and applications. Finally, we summarize our findings in Sec. 6.

2 State of the Art

In this section, we provide a state-of-the-art on existing solutions for threat detection and protection in 5G networks and emerging 6G networks. Contributions found in the literature, standards development organizations, and other related European projects are evaluated to identify technical synergies and gaps that the ROBUST-6G framework will address.

2.1 5G Threat Analysis

5G networks have typically been considered as part of critical infrastructures in the United States (US) and European Union (EU) and consequently a large number of international organizations have delivered reports on potential threats and mitigation measures. Below, we focus on a few indicative reports that are used as a reference by many actors.

We begin with the ENISA threat landscape “Report for 5G Networks”, issued on November 2019 [ENISA19]. This report provides an initial assessment of the threat landscape surrounding 5G networks, offering an overview of the security challenges they face. It accounts for a comprehensive 5G architecture, critical assets through an asset diagram, the evaluation of threats impacting 5G networks using a threat taxonomy (nefarious activity, such as malicious code or software, exploitation of flaws in the network architecture and of hardware/software vulnerabilities, denial of service, abuse of lawful interception, data breach, identity fraud, compromised vendors, data forging; as well as eavesdropping, disaster, accidental damage, outages, failures, and physical attacks), mapping the exposure of assets to threats, and an initial analysis of threat agent motivations. The information presented in this Threat Landscape report is sourced from publicly available data published by 5G standardization groups and organizations such as ETSI, Third Generation Partnership Project (3GPP), and 5GPPP, as well as insights from stakeholders including operators, vendors, and various national and international entities.

In addition, the "5G Security and Resilience" strategy by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) outlines a comprehensive approach to ensuring the secure and resilient deployment of 5G technology in the United States [CISA19, CISA20]. It emphasizes five strategic initiatives: developing secure policies and standards, raising awareness of supply chain risks, enhancing infrastructure security, fostering innovation in the 5G marketplace, and implementing robust risk management strategies. The strategy focuses on risk management, stakeholder engagement, and providing technical assistance, while highlighting potential vulnerabilities from legacy systems and limited vendor competition.

The FiGHT 5G Hierarchy of Threats Matrix [FiGHT] functions as a repository of adversary Tactics and Techniques, and is introduced particularly for 5G networks. It encompasses three distinct categories of techniques for the analysis of the threat surface: 1) theoretical, 2) proof of concept (PoC), and 3) observed. The bulk of the framework comprises theoretical and PoC techniques, drawing from academic research and publicly available documents. Currently, a smaller portion of FiGHT techniques are derived from real-world observations, duly documented. Modelled after the MITRE ATT&CK® framework [ATT&CK], FiGHT's tactics and techniques complement those found in ATT&CK. MITRE actively encourages contributions and feedback from interested parties within the telecommunications industry, manufacturers, and cybersecurity researchers to enhance the FiGHT Framework continuously.

The 3GPP specification report, “Study on 5G security enhancements against False Base Stations (fBS)” [33.809] is an overview of 5G system mitigations against false base stations (fBS), focusing on several key issues that might allow an impersonation attack from an illegal transmitter acting as an fBS. In particular, the following key issues are considered:

- Security of unprotected unicast messages: these messages are typically unprotected (before network entry);
- Security protection of system information: broadcasting system information, e.g., for synchronization purposes;
- Network detection of false base stations: during handovers;
- SON poisoning attempts: for self-organizing networks;
- Authentication relay attack: relay to a malicious UE connected to a fBS;
- Radio jamming: disrupt radio communications;
- Man-in-the-Middle (MITM) false gNodeB (gNB) attacks: altering messages.

In ROBUST-6G, we will look at possible solutions to these issues by leveraging physical layer authentication, resilience to MiM and jamming attacks.

The 3GPP specification report, “Study on the security of Ultra-Reliable Low-Latency Communication (URLLC) for the 5G System (5GS), (release 16)” [33.825] focuses on URLLC security, accounting for

- Retransmissions to ensure high reliability, and
- Low latency that renders standard security measures, e.g., the use of message authentication for the data plane, very hard.

In more detail, to achieve high reliability, redundant transmissions within 5G are critical. Consequently, security mechanisms applicable to supporting redundant transmission encompass all facets of communication. Addressing the low latency requirement, other essential aspects outlined in 3GPP TR 23.725, “Study on enhancement of Ultra-Reliable Low-Latency Communication (URLLC) support in the 5G Core network (5GC)” [23.725] for URLLC, such as Quality of Service (QoS) monitoring to aid URLLC service and optimization for handover procedures, are also catered to. Furthermore, additional security aspects pertaining to control plane or user plane optimizations for ensuring high reliability and reducing latency are comprehensively examined throughout the entire study and are duly reflected in the present document. In ROBUST-6G, we will look at specific aspects of fast authentication and re-authentication for URLLC.

2.2 6G Threat Analysis

The Hexa-X II project is one of the flagship projects for 6G research, and it includes security dimensions as well. It is kind of a reference guideline for us to reuse the existing know-how and build our research on top of it. For this reason, in the following we explain its state-of-the-art in terms of threat analysis.
Hexa-X II designs enablers along with the threat families they intend to address, and these enablers have been analyzed according to the principle of the 6G Delta (the direct implications of 6G technology for enhancing E2E security, privacy, and resilience evolution) as introduced by the Hexa-X project [HEX23-D13]. The structure starts with threats associated with foreseen architectural trends, following the pervasive use of AI.

Three main architectural trends conforming the security impact are given below, namely:

- Network of Networks (NoN) compositional pattern.
- Use of a cloud continuum as a base infrastructural approach.
- Application of radical disaggregation mechanisms.

2.2.1 Network of Networks (NoN) compositional pattern

The NoN scenario presents several challenges regarding the procedures required for connecting and separating network domains, as well as for ensuring optimized operations within a federated network [ZY+20]. System-level procedures need to accommodate the integration of networking solutions from various operators, with limited information exchange between integrated domains. Some federations, like those based on Device-to-Device (D2D) for Vehicle-to-Everything (V2X) communication, might be short-lived. NoN operations can be conducted peer-to-peer or hierarchically, depending on the nature of the use cases.

Ensuring the trustworthiness of NoN demands special attention to security. Security mechanisms for static multi-domain integration remain poorly defined and they should consider three basic scenarios which are outlined below:

1. Integration of fully independent networks, where each has its own security mechanisms. Dedicated proxies for control and user plane communication can secure interconnections between networks. Solutions like Security Edge Protection Proxy (SEPP) and Inter-PLMN UP Security (IPUPS) proxy can be employed. Security policy negotiations, alignment, and separate treatment of trusted and non-trusted networks are essential, especially for short-lived federations.
2. Dynamic multi-connectivity of users, akin to using 3GPP networks with "non-3GPP access networks". In this scenario, the user primarily connects to the 3GPP network, but may occasionally access other networks. The main network handles control plane messages, while other networks serve as user plane solutions, necessitating data confidentiality and integrity protection.
3. Integration of different networking solutions beyond access networks, such as transport networks for long-range interconnection or dedicated Core network slices. Mutual authentication between integrated domains is crucial in this scenario.

Mixed scenarios may combine independent networks, dynamic multi-connectivity, and diverse transport domains in the Core network. These scenarios require a combination of security considerations. While 3GPP has defined mechanisms for secure network integration [23.501], they are limited to 3GPP networks and do not extend to non-3GPP networks, even in static cases.

2.2.2 Use of a cloud continuum as base infrastructural approach

The Cloud Continuum concept [HEX23-D13] aims to integrate all infrastructure resources, including virtualized, unreliable, and constrained Far-Edge resources. However, existing approaches like the ETSI Network Functions Virtualization (NFV) Integrated Security Gateway (ISG) have limitations regarding security. These limitations include undefined business interfaces towards infrastructure providers and assumptions of a static resource pool that cannot handle dynamic and unreliable resources. The Cloud Continuum Framework [KBP23] addresses these challenges, with a key component being the Resource Layer (RL), focusing on resource operations and including resource orchestrators. The RL integrates resources from different data centers via secure South Bound Interfaces (SBIs) and exposes them to service orchestrators through North Bound Interfaces (NBIs). Security considerations include mutual authentication of attached data centers, confidential access to resources, and addressing malicious behaviors related to the RL. The framework proposes using multiple service orchestrators to create isolated resource partitions based on Network Service (NS) requirements, simplifying orchestration processes. Ensuring security for both the SBI and NBI interfaces of RL is essential for the successful implementation of the Cloud Continuum concept.

2.2.3 Application of radical disaggregation mechanisms

Disaggregation in the context of Radio Access Networks (RAN) involves breaking down complex systems into modular components, allowing for independent management and operation of hardware (HW), software (SW), and network services. While this approach offers benefits like flexibility and optimization, it also introduces new security challenges.

Disaggregation may expand the potential attack surface, making networks more vulnerable to cyberattacks. Robust authentication, authorization, secure interface management, and verification mechanisms are needed to prevent unauthorized access and data breaches. Adherence to zero-trust principles for RAN design is essential [PPR+23]. Ensuring confidentiality and integrity of data traversing through disaggregated elements is crucial, requiring encryption, integrity checking, and secure data transmission protocols. Protecting network availability against Distributed Denial of Service (DDoS) attacks originating from compromised user equipment (UE) elements is vital. Developing methods for detecting DDoS attacks at the radio interface allows for the timely implementation of mitigation measures. Innovative approaches are needed for DDoS detection, requiring the identification of new features and methodologies. These efforts enhance the ability of networks to proactively thwart attacks and maintain uninterrupted service for legitimate users. Federated Learning (FL), particularly in the realm of Deep Reinforcement Learning (DRL), has demonstrated effectiveness in various RAN optimization tasks [ATF+22]. This approach can also be applied to security operations within the network. FL security agents, positioned across different locations, collect data and transmit it to a trusted data collector before forwarding it to the inference engine. Security measures must be tailored to meet the accuracy and latency requirements of real-time applications.

Moreover, threats implied by the pervasive use of AI are divided into two sections which are given below as “AI security” and “AI privacy preservation”. AI and machine learning (ML) is expected to play a critical role in the upcoming data-driven 6G network, providing opportunities for increasing network efficiency, automating processes, and strengthening security measures against a variety of threats [ABB+20]. Ensuring the dependability, security, and privacy of AI/ML integration into the 6G framework necessitates the implementation of preventive measures against attacks on AI/ML systems. Security attacks on AI/ML attempt to disrupt or influence system functionality, posing major dangers to the functioning of 6G networks at any point of the AI/ML model lifecycle. In contrast, privacy attacks on AI/ML attempt to extract sensitive information such as training data and model parameters, demanding safeguards to ensure the confidentiality and integrity of 6G systems.

2.2.4 AI security

Studies suggest using explainable AI (XAI) and adversarial training to counter adversarial attacks [ZAM22]. In fact, standard AI/ML models often suffer from lack of transparency in decision-making, resulting in uncertain outcomes, and the replacement of black-box AI algorithms provides significant opportunities for strengthening 6G network security. In this context, XAI techniques provide explanations that improve accountability and transparency in black-box AI models, assisting in the early identification of problems with model training or data quality. By making the AI/ML system's decision-making processes more transparent, the incorporation of XAI approaches helps strengthen defensive measures and enhance trust. This kind of transparency is advisable to attaining reliable 6G communication networks.

2.2.5 AI privacy preservation

In the context of a data-driven, multi-vendor, multi-environment 6G system, each AI/ML application needs to be thoroughly investigated to identify relevant risks and implement adequate security measures. Secure multi-party computation, homomorphic encryption, differential privacy (DP), and private computing are examples of commonly used technology to deal with privacy concerns [SJL+21]. While systems such as FL and split learning prioritize privacy, they frequently require additional support from privacy-enhancing technology to address privacy concerns. However, depending primarily on privacy may expose AI/ML to security vulnerabilities by masking data or local model updates from the model trainer, hence avoiding security risk identification. To address both security and privacy (SP) concerns, it may be useful to allow the central AI/ML trainer access to some local model updates in cleartext, allowing for the detection of security attacks while maintaining training data privacy. Furthermore, potential performance and speed overheads should be considered while implementing privacy and security approaches, such as selectively using differential privacy to preserve privacy while optimizing learning speed and performance, particularly in private federated learning settings.

3 Methodology for Threat Identification

3.1 The CIA model

The CIA model with the three security attributes *Confidentiality*, *Integrity*, and *Availability*, is a classical model used to describe and identify threats against assets (software, data, hardware, and humans) in a system. This model is also a part of ISO 27001 which defines security as being CIA. The CIA model is an asset-centric (or data-centric) model, where each asset can be associated with multiple threats and with multiple security attributes. The CIA model is often seen as an academic model since it does not offer enough guidance to practitioners when identifying threats to a larger system.

3.2 Microsoft STRIDE

A more practical approach to identify threats is the method developed and used by Microsoft, the STRIDE method. It has extended the CIA attributes with *authorization*, *non-repudiation*, and *authenticity* to make it more guiding and useful when identifying threats. It also focuses on end results and threats and not on individual assets as the CIA model. Since a large complex system will have lots of components interacting with each other in complicated ways, this is a more suitable approach. It supports the creation of data-flow diagrams to see how data flows and how interactions between components occur.

The STRIDE method is easy to use also for non-security experts since it gives much better guidance than the CIA model. The method has a good track record and performs well when identifying threats and vulnerabilities in complex systems. The term STRIDE stems from the initial letters of six different threat types that should be considered when a system or function is analysed:

1. Spoofing - attackers pretend to be someone or something else.
2. Tampering - attackers change data in transit or in a data store.
3. Repudiation - attackers perform actions that cannot be traced back to them.
4. Information disclosure - attackers get access to data in transit or in a data store.
5. Denial of service - attackers interrupt a system’s legitimate operation.
6. Elevation of privilege - attackers perform actions they are not authorized to perform.

Table 3-1: Mapping between STRIDE threats and security attributes

STRIDE Threat	Security Attribute

Spoofing	Authenticity, Freshness
Tampering	Integrity*
Repudiation	Non-repudiation, Freshness
Information disclosure	Confidentiality*, Privacy
Denial of service	Availability*
Elevation of privilege	Authorization

* CIA attribute

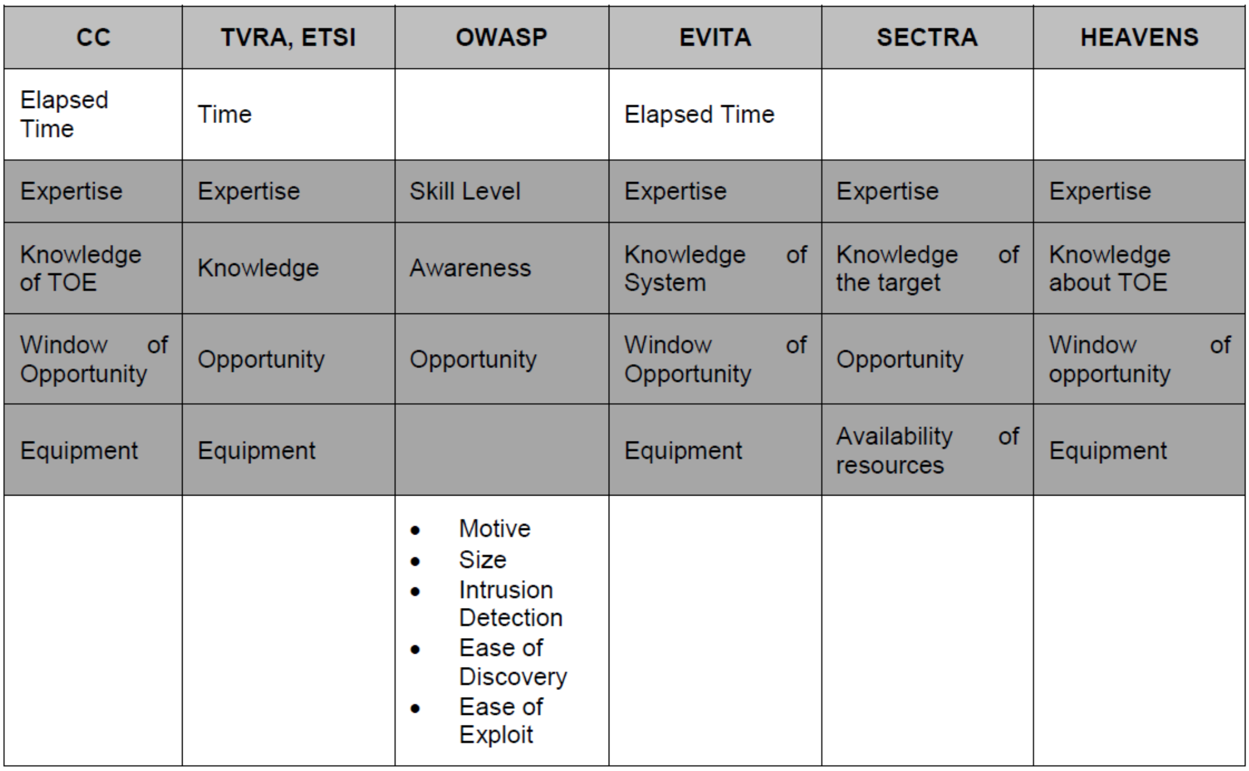
3.3 Threat, Vulnerability and Risk assessment

When threats have been identified (e.g., using STRIDE), it is necessary to follow up with a vulnerability and risk analysis. The outcome of this process will motivate and govern the choice of mitigation techniques. A threat or an attack that is extremely unlikely to happen due to its complexity, cost and limited opportunity to be performed but which would have catastrophic consequences to the system, may after the risk analysis be identified as a *critical risk* that must be addressed with all possible means.

There are different threat, vulnerability, and risk assessment (TVRA) methods available today, each with their own strengths and weaknesses, for example Common Criteria (CC), TVRA from ETSI, OWASP, E-safety Vehicle Intrusion Protected Applications (EVITA), SECTRA, and HEAling Vulnerabilities to ENhance Software (HEAVENS) [HEA16-D2]. In the end, all methods perform a risk assessment and enable one to choose mitigation techniques.

In general, whether it is ETSI TVRA, Common Criteria (CC), HEAVENS or another method being used may be a matter of taste and may not even affect the outcome of the analysis, since they all contain similar components, see Table 3-2. However, in a real setting, legal and other requirements may demand that one or more of these methods should be used.

Table 3-2: Comparative view of parameters to determine threat level [HEA16-D2, Table 4-3].



CC	TVRA, ETSI	OWASP	EVITA	SECTRA	HEAVENS
Elapsed Time	Time		Elapsed Time		
Expertise	Expertise	Skill Level	Expertise	Expertise	Expertise
Knowledge of TOE	Knowledge	Awareness	Knowledge of System	Knowledge of the target	Knowledge about TOE
Window of Opportunity	Opportunity	Opportunity	Window of Opportunity	Opportunity	Window of opportunity
Equipment	Equipment		Equipment	Availability of resources	Equipment
		• Motive • Size • Intrusion Detection • Ease of Discovery • Ease of Exploit			

3.3.1 ETSI TVRA

European Telecommunications Standards Institute (ETSI) proposes a Threat, Vulnerability, and Risk Analysis (TVRA) method which was originally developed for their standards developers to analyse security in telecommunication systems [ETSI TS 102 165-1]. In this method, the CIA model is extended with *authenticity* and *accountability*, two attributes that are also present in the STRIDE method. The TVRA method mainly describes how to identify risks to a system based on the likelihood of them to occur and the effect they may have on the system.

In short, functional security requirements are derived and assets (here hardware, software, and human) and possible vulnerabilities in these, are identified. When considering a threat to an asset, the complexity of the technology, to what extent documentation is available to the public, and the life expectancy of the asset are considered. Asset importance is then classified as low, medium, and high. Then threat agents against assets are identified, where time needed to mount the attack, expertise required, opportunity and knowledge/equipment needed is considered. Finally, risks are calculated and placed on a scale, *minor, major,* or *critical*.

The process can be summarized as:

Identify security objectives for the system → *Functional security requirements and inventory of assets* → *Threats and vulnerabilities* → *Likelihoods and impact* → *Determine risks* → *Countermeasures.*

3.3.2 HEAVENS

The HEAVENS security method [HEA16-D2] is another way to perform risk analysis and derive security requirements. The workflow is similar to that in the ETSI TVRA method, although the way threats are evaluated, and the granularity differ. HEAVENS is widely used in the automotive industry due to its flexibility and ease of use by practitioners. HEAVENS begins with STRIDE for threat identification and takes a systematic approach to derive security requirements by connecting assets, threats, security levels and security attributes. This facilitates visualization and makes an estimation of the technical impact of a particular threat on a particular asset. Similar but not identical to ETSI TVRA, it maps security objectives (safety, financial, operational, privacy and legislation) to impact level estimation during the risk assessment phase. It contains more classes than ETSI TVRA and has a more granular classification of threats to aid in defining suitable mitigation techniques.

3.4 FiGHT 5G Hierarchy of Threats

In FiGHT [FiGHT] the key categories of threats concern a high-level function of the network and are listed as follows: *reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command control, exfiltration, impact, and fraud.*

While at later stages of the project we will try to incorporate as many of these dimensions as possible, as an initial point for the development of the physical layer threat matrix we will focus on aspects related to *initial access, credential access, impact, lateral movement, and collection.* We will begin with a threat description that is typically used in cryptography to assess the strength of crypto schemes and focus on confidentiality, authentication, integrity, availability, and non-repudiation.

4 Considered Key 6G Technical Enablers, Use Cases and Applications

A full risk assessment cannot be done for a 6G system at this point in time, since all assets and the complete design are not known. A full risk assessment highly depends on the system design, the included components and their detailed functionality, their interaction with each other and how and where data is stored, information that is currently not available. Instead, below we give examples of possible threats on the PHY layer, ML/AI modules, and show how a risk analysis can be done in relation to key 6G technologies. The method adopted is based on the methods described in Ch. 3.

4.1 Distributed Multiple-Input Multiple-Output

Distributed multiple-input multiple-output (D-MIMO) has the potential to address 6G challenges at both low (cm-wave, lower mm-wave) and high (upper mm-wave and (sub-)THz) carrier frequencies. Scalable D-MIMO techniques allow for multi-user MIMO with coherent joint transmission and interference suppression capabilities and can provide robust links with a large amount of traffic. Thus, D-MIMO allows for further densification, increasing consistent area capacity, and mitigating unreliable links due to shadowing or blockage, benefiting from macro-diversity. In addition, it allows sufficient link margin despite output power limitations and high path-loss at upper mm-wave and (sub-)THz frequencies and allows for lowering effective isotropic radiated power, hence simplifying deployment [Lin22]. Moreover, D-MIMO with multi-node connectivity will allow contiguous coverage under mobility.

D-MIMO networks can be deployed in areas where capacity cannot be met by macro sites in an efficient way and used to improve performance in high-density urban areas such as public squares, stadiums, and airports. For indoor deployment scenarios, such as factories, warehouses, and offices, this technique can be used to enhance reliability and resilience aspects. It can provide reliable and resilient mobility without frequent handovers. In some scenarios, coverage from existing macro deployments may not exist. In such cases, in addition to providing data boosting, D-MIMO network also needs to provide coverage for standalone operation.

There is various research on D-MIMO in the literature covering channel estimation, flexible remote unit (RU) selection/clustering, precoding, resource allocation, power control, cf. [HYM+23] and references therein, as well as cross-tier handover. The main challenge for the widespread implementation of D-MIMO is the cost of installing many nodes in different locations that require high-speed fronthaul connections. These installations need to be easy to deploy, have a small visual impact and be flexible to scale and expand [HEX21-D22]. Thus, there seems to be important trade-offs when it comes to cost per Access Point (AP) supporting easy and massive deployment, versus security of the installations.

Security aspects of D-MIMO were briefly discussed in [HEX23-D23, Sec. 4.3.2], in which the following were identified.

- The network will have to support multi-connectivity of a user,
- The network deployment will be densified and,
- A much higher percentage of fronthaul links will be used in the network.

These three aspects will not only affect deployment scenarios, signal processing, scheduling etc., but also affect user- and control-plane security. In particular, in [HEX23-D23] it is highlighted that authentication and key agreement between the network and the user supporting the connection of a user to multiple radio units will be needed. Multi-connectivity will need an arrangement for authentication and key agreement between the network and the user, supporting connections of a user to multiple radio units, which will impact both connection management and a common encryption key to be used for the different signal paths in case of joint transmission. Furthermore, not only the higher layers but also the MAC layer will have to be secured, which might require that the network supports multiple security associations of a user.

In [HEX23-D23, Sec. 4.3.2], a summary of architectural options for D-MIMO considered for 6G deployment scenarios is provided as follows.

1. **Transport media:** The backhaul/fronthaul transport media can either be wired or wireless.
2. **Signalling**: The data transmitted over the media can further be distinguished in being digitally encoded (e.g., common public radio interface (CPRI) like), or an analogue signal modulated onto a carrier.
3. **Processing:** Processing (such as for example beamforming) in different nodes can either be performed analogue or digitally. A further distinction can be made into centralized or distributed processing.

4. **Transmission:** If multiple serving antennas serve a UE jointly, this can either happen through coherent or non-coherent transmission by the serving antennas.

An analysis of these D-MIMO architectural options from a security perspective is needed, since such an analysis might provide further important insights into the feasibility of the options for deployment in various deployment and usage scenarios, also taking security into account.

4.2 Reconfigurable Intelligent Surfaces

As defined and summarized by ETSI [ETSI-RIS], "Reconfigurable Intelligent Surfaces (RIS) corresponds to a planar surface composed of unit-cells, whose properties can be controlled dynamically to 'tune' the incident wireless signals through reflection, refraction, focusing, collimation, modulation, or absorption. RIS can be potentially deployed for both indoor and outdoor usage, including offices, airports, shopping centers, lamp posts and advertising billboards, and may take any shape or be integrated onto objects. Its characteristics may also result in low energy consumption, making RIS a sustainable technology solution. RIS can be configured to operate at any part of the radio spectrum, including frequencies from below 6 GHz to THz, and may harness tools from AI and ML to enable systems operation and optimization.

As RIS is envisaged to be a new enabling candidate wireless technology for the control of the radio signals between a transmitter and a receiver in a dynamic and goal-oriented way, turning the wireless environment into a service. This has motivated a host of potential new use cases targeting at:

i) the enhancement of various system key-performance-indicators (KPIs), and

ii) the support of new wireless technology applications and capabilities.

These include enhancements to the capacity, coverage, positioning, security, and sustainability, as well as the support of further sensing, wireless power transfer, and ambient backscattering capabilities."

The RISE-6G project [RISE-6G] has focused on innovative solutions that capitalize on the latest advances on RIS for dynamic and goal-oriented radio wave propagation control with a focus on enhanced/enabling connectivity and reliability, localization and sensing, and sustainability and security.

The impact of RIS as a new network node has been investigated in [RIS23+D26]. The different envisioned solutions where RIS devices are used can be categorized as follows.

- RIS-aided/assisted/augmented/based/boosted/empowered solutions where at least one RIS allows to obtain (appropriately defined) improved system performance metrics.
- RIS-enabled solutions where certain services/performance cannot be obtained without at least one RIS.

Defining "architecture" as a set of logical blocks that interact with each other in a network to provide users with the expected service(s)/KPIs, a logical network architecture for a RIS system has been defined in [RIS23+D26] with the following functional elements.

- RIS (device) – A RIS device can be based on the reflect-array or meta-material technology that is directly controlled by an associated RIS actuator.
- The RIS Actuator (RISA) is the element in charge of actuating the logical commands received by the RISC, i.e., of translating them into physical configurations to be applied to the RIS device.
- RIS controller (RISC) – It is the controller associated to a RISA (in the case where the RISE device is separated from the RISA) or a RIS function (in the case where the RISA is embedded into the RIS device).
- RIS orchestrator (RISO) – It is placed on a higher (hierarchical) layer, and it orchestrates multiple RISCs.

Some of the work in RISE-6G has been devoted to security, with a special focus on boosting the secrecy spectral efficiency (SSE), defined as the difference between the received spectral efficiency at the intended user and the spectral efficiency attained by the eavesdropping non-intended user.

The physical control of an RIS can be realized in various ways, all with the potential different security vulnerabilities. In [RIS23+D26] the following Control Channel (CC) taxonomy was defined.

- Implicit CC: There is no dedicated CC or signal over which explicit instructions are sent to the RISC (but the synchronization signal). As such, all decisions wrt. RIS(A) operations must be made locally by the RISC; however, these decisions can be based on other received and interpreted signals (e.g., pilot symbols, user equipment (UE) scheduling information) which implicitly (indirectly) control the behavior of the RIS.

- Explicit CC:
  - Out-of-band: Any communication channel, either wireless or wired, that does not consume resources from the primary communication channel that is influenced by the RIS; examples include: wired channel, wireless channel in a different frequency band, free-space optical, etc. This allows for simpler CC design, but at the cost of possibly lower spectral efficiency.
  - In-band: The CC employs resources overlapping RIS operational spectrum resources, so it does influence the operation of the RIS. This implies a more complex CC design, but with possibly higher spectral efficiency.

In addition, the following RIS operational modes were defined in [RIS23+D26].

- Totally Controlled RIS: RIS operations are controlled by an external entity providing the main computational processing, and informing the RISC functions through the explicit CC.
- Partially Controlled RIS: RIS operations are in part controlled by an external entity and by the RIS device itself.
- Totally Autonomous RIS: RIS operations are defined by the RISC on its own, without involving any external entity, even though an explicit CC may be present for communicating synchronization or feedback information.

4.3 mmWaves and sub-THz

A recurring theme in the development of future communication systems involves harnessing frequencies within the TeraHertz (THz) band (greater than 100 GHz) [RXK+19]. While 5G networks operate below 100 GHz and are expected to achieve peak data rates of around 20 Gbps, researchers in the THz spectrum are striving to surpass the Tbps barrier, with experimental setups already showcasing speeds in the hundreds of Gbps. In 2017, the approval of the first standard covering the THz band, IEEE 802.15.3d-2017, sparked intense research activity in the field. Operating at such high frequencies presents unique challenges, notably the exceptionally high propagation losses within the THz band. For instance, free-space path loss can reach approximately 80 dB at 300 GHz over a 1-meter distance. To mitigate these losses, high-gain antennas are essential, resulting in highly directional THz links with pencil-like radiation patterns and narrow beamwidths of a few degrees.

While this directional focus enhances privacy and security by making eavesdropping more difficult, it also necessitates precise real-time localization and tracking of users. However, this inherent challenge also presents an opportunity for PLS, as narrow beams naturally impede eavesdropping. Moreover, THz communications face specific threats, including jamming, due to the large available bandwidth, which can make the link more susceptible to interference. Despite these vulnerabilities, eavesdropping and jamming at THz frequencies are inherently more challenging due to the spatially narrow nature of THz links. However, ongoing research in the field aims to uncover and address these threats by developing tailored countermeasures and adapting existing techniques to the specific vulnerabilities of THz communications.

4.4 RF Sensing and Localization

4.4.1 Sensing and Localization with Communication Networks

Next-generation wireless networks are called to provide support for an increasing number of devices and heterogeneous applications. As part of the growing functionalities of next-generation wireless networks (including 6G), capabilities including localization of devices and sensing of the surroundings are being introduced. These services allow providing additional benefits to the users and improving the network resource management [WQW+23, SVB+22].

Localization and sensing services differ in their objective and the way the information is collected [BYK+22]. Localization means to estimate the position in space of an active wireless device, i.e., transmitting radio signals, from radio channel estimates such as the received signal power, the signal time of flight, and the angles of arrival and departure of the signal [BAB+23]. For example, a base station (BS) can estimate the distance and the relative angle of a connected user equipment (UE) from the signal received in the uplink. On the other hand, sensing refers to obtaining information about passive objects in the environment, e.g., people, furniture, cars, and road signs. In this case, the fixed and moving objects act as reflectors, diffractors, and scatters for the signals. In turn, information about the range, velocity and angular position (to name a few examples) is obtained by analyzing the way radio signals exchanged by two wireless devices are modified by the environment. Localization and sensing can be obtained through mono-static, bi-static, or multi-static systems [LCM+22]. In the first case, the system acts similarly to a radar device, where the transmitter and the receiver are co-located, and sensing parameters are extracted by the signals that are reflected to the device. Bi-static sensing is a more common setup in communication networks because it relies on the typical communication setup composed of a transmitter and a receiver that are not co-located. In multi-static sensing, multiple receivers collect the multiple signal copies generated by multi-path propagation from a transmitter device and process this data for localization and sensing.

Localization and sensing through wireless networks are made possible as wireless devices continuously estimate how the radio channel modifies the signals in their way from the transmitter to the receiver devices. The estimate is necessary to decode data properly and to apply effective data precoding before transmissions. This inherent feature of wireless devices can serve as a proxy to sense the surroundings, obtaining information about the placement of the wireless devices (localization) and the characteristics of the environment (sensing). Hence, researchers started investigating the integration of sensing functionalities within wireless communication networks [WQW+23].

The resolution and accuracy of sensing and localization depend on the frequency and on the bandwidth of the signal used for sensing purposes, as well as on the waveforms adopted. Specifically, orthogonal frequency division multiplexing (OFDM) together with orthogonal frequency division multiple access (OFDMA) is popularly adopted in communication systems to concurrently transmit multiple data symbols over orthogonal frequency sub-channels [WKG+22, WQW+23]. This transmission mode can be used to obtain an estimate of the range of targets by analyzing the different ways the signal is modified in the different subchannels. In addition to leveraging currently adopted communication waveforms for sensing purposes, researchers have been designing new waveforms that can accommodate both sensing and communication functionalities. Examples are orthogonal time frequency space (OTFS) [GKC+20, SC20, YWL+21, YWL+22], orthogonal chirp-division multiplexing (OCDM) [BZM+18, BMA+22], and affine frequency-division multiplexing (AFDM) [BKK21, BKK23, BKK24]. As another waveform design, researchers have proposed to combine OFDM with linear frequency modulation (LFM) [WQW+23]. LFM, also known as chirp, is applied in radar sensing. In OFDM-LFM, the LFM modulation is applied after the inverse Fourier transform for OFDM, i.e., the symbols are modulated onto the LFM signals. This approach allows improving the resolution of distance and velocity estimation [DJV+15]. OFDM can also be combined with phase coding and spread spectrum to improve the sensing and localization performance as summarized in [WQW+23]. Other candidate waveforms for 5G that can be useful for sensing purposes are filter-bank multicarrier (FBMC), generalized frequency-division multiplexing (GFDM), and discrete Fourier transform-spread-OFDM (DFT-s-OFDM) [WQW+23, WLH+22].

The sensing and localization accuracy in the angular dimension depends on the antenna arrays used for signal transmission and reception. The higher the number of antennas, the higher the resolution that can be achieved [LCM+22]. For localization in the angular dimension, both multiple-input multiple-output (MIMO) and analog beamforming systems can be used. Regarding the first, the channel estimates between each transmitter and receiver antenna are used to obtain the angular position of a target. In analog beamforming a beam steering process is performed to illuminate the entire environment and the target position is obtained by analyzing the signal received using the different transmission beams.

4.4.2 Frequencies for Localization and Sensing

Cellular networks historically operate on the licensed sub-7 GHz portions of the radio spectrum, ranging from 410 MHz to 7.125 GHz. This is referred to as the frequency range (FR) FR1. However, the channel bandwidth can be up to 100 MHz in FR1, and this limits the range resolution of the sensing systems to about 1.5 m [LCM+22, DBB+21]. The 3GPP has then defined an additional portion of the radio spectrum, FR2 (mmWave) that ranges from 24.25 GHz to 52.6 GHz and provides a range resolution of up to 0.375 m with a bandwidth of 400 MHz [LCM+22]. This resolution is still insufficient for some applications such as autonomous vehicles that require a precision of 0.1m in the position estimates. A possible approach to address this is to use carrier aggregation, i.e., using multiple frequency blocks for communication and, in turn, for sensing [WLY+23]. Another possibility is the use of the Terahertz portion of the radio spectrum (0.1-10 THz) [CSB+22]. Terahertz sensing provides bandwidths of up to 10 GHz improving the system resolution to 3-30 cm.

4.4.3 Localization and Sensing Methodologies

As described above, localization and sensing target two complementary tasks: while the first considers active targets, the second aims to obtain information about passive devices. However, processing methodologies to obtain the sensing parameters are common. The systems use as sensing primitive the channel estimate computed by the communication devices through training fields in the data packets. The time, frequency, and space diversity in the channel estimates allow for obtaining information about the range, velocity, and angular position of the passive or active target. In addition to estimating these quantities, the objective of sensing may be to obtain other types of information from the surroundings such as identifying the people present in the environment or recognizing the activity they are performing. In these cases, standard signal processing techniques may not suffice to address the sensing task. Hence, several AI and, in particular, ML approaches have been proposed in the literature for the different frequency bands [MCC+23, SVB+22, HSD+22l].

4.4.4 Signal Processing for Communications and Sensing

Communication systems obtain an estimate of the channel in the frequency or in the time domain. The first is referred to as the channel frequency response (CFR) and is obtained for multi-carrier systems (OFDM), while the second is indicated with channel impulse response (CIR) and is obtained for single carrier systems. The CIR provides information about the delay and complex attenuation of the multi-path components associated with the propagation environment collected at the receiver device. This information can also be obtained from the CFR by performing an Inverse Fast Fourier Transform (IFFT) over the frequency components of the OFDM modulation [WQW+23, LCM+22]. The resolution in the estimate of the multi-path component parameters depends on the bandwidth (B) of the signal available as c/2B, where c is the speed of light [LCM+22]. The range of the different targets in the environment is obtained by considering the delay of the different multi-path components associated with the targets. For localization, the LOS is usually the main source of information as it directly provides the range of the transmitting device. In case the LOS is blocked, the non-LOS (NLOS) components are used for localization [PBC+21]. Instead, for sensing, the LOS is usually irrelevant as the objective is not to localize the communication devices. In this case, the components of interest are the NLOS paths that are associated with the static and moving objects displaced in the propagation environment.

By performing a Fourier transform over the CFR estimates obtained from the signals transmitted at the same frequency and collected at different time instants, the Doppler shift associated with moving targets can be obtained [WLH+22]. The Doppler shift can be related to the movement of a transmitting device (localization) or a passive device (sensing). Hence, the velocity of the target can be estimated from this sensing parameter.

Similarly, to the estimation of the range and the Doppler in the frequency and time domain, the angle position of the target can be obtained by considering the diversity in the space domain. The multi-path signal is received at the different antennas in subsequent time instants and the relative delay among the antennas is associated with the angle of arrival (AoA) at the receiver of the signal irradiated by the transmitter. By performing a Fourier transform over the antenna dimension, the AoA and, in turn, the position of the target can be obtained [WQW+23].

The accuracy that can be achieved with the Fourier transform in the estimation of the range, velocity and Doppler depends on its granularity, i.e., the sampling rate of the system. Super-resolution approaches have been presented in the literature to improve the estimation accuracy [MBC+23]. Examples are MUSIC, ESPRIT, MVDR [WQW+23].

4.4.5 AI/ML for Localization and Sensing

AI/ML algorithms have become increasingly used for sensing and localization purposes when signal processing methods are insufficient to address the task or reach good accuracy. An overview of AI/ML's role in integrating sensing functionalities within wireless networks is presented in [DA23]. Signal processing techniques for sensing can be referred to as model-based approaches as they rely on models of *n* models of radio. AI/ML approaches are instead model-free approaches as the algorithms are data-driven and learn how to address the task from examples used during the training process [MCC+23]. The use of AI/ML for localization and sensing ranges from low-level feature extraction and pattern discovery to object detection and recognition, location tracking and prediction, environmental mapping, and cooperative localization [DBB+21]. For localization, ML is usually used to implement fingerprinting-based algorithms, that obtain an estimate of the location of the target by analyzing the characteristics of radio propagation and finding the best match with the fingerprints learned during training. For sensing, ML is extensively used in indoor environments for people monitoring, e.g., for activity recognition and person identification.

4.4.6 Cooperative Sensing

Localization and sensing can benefit from distributed sensing node cooperation [LCM+22]. This means that different devices in the environment sense the wireless channel and the information is combined to improve the accuracy and precision of the estimates. In [LCM+22], the authors identify two possibilities for the fusion of sensing data from different nodes. The first approach is to lead the sensing node to independently estimate the sensing parameters and then combine their estimates at a centralized node. A second approach consists of fusing the data at the signal level, i.e., before estimating the sensing parameters. The signals are combined at a centralized node that uses them jointly to perform sensing and localization. An example of this methodology is distributed MIMO radar. This second approach usually provides better performance as combining the estimates may lead to information loss in the process.

4.4.7 Emerging Communication Technologies for Sensing and its role in 6G Systems

Emerging communication technologies such as reconfigurable intelligent surfaces (RISs) and unmanned aerial vehicles (UAVs) are expected to benefit sensing applications [LCM+22, WWB+23]. In particular, RISs can provide a means to sense targets that are not in the line of sight (LOS) through the reconfigurable proprieties of the surfaces. UAVs can provide both strong LOS connecting the targets and sensing on-demand features as the sensing thanks to their mobility.

Sensing is one of the new key functionalities introduced by 6G systems, which is expected to be widely implemented at base stations and (eventually) terminals. This feature exhibits security and privacy concerns, as the location and movement of terminals represent sensitive information that a user may want to protect against unauthorized use. This is why it is analyzed in this deliverable.

4.4.8 Applications

Once integrated into next-generation wireless networks, localization and sensing can enable a wide range of applications. Wireless networks are omnipresent in today's digital society. Thus, the use of wireless networks for sensing allows offering users additional services to the users without the burden of installing additional hardware (*communication-assisted sensing*). Second, sensing the propagation environment provides useful information for proper communication and computing resource allocation (*sensing-assisted communications*). Given these mutual benefits, the next generations of communication networks (6G and beyond) are envisioned to jointly offer the two services, designing proper network architectures and signals to satisfy their different requirements in terms of transmission rate and bandwidth. This paradigm is referred to as *integrated communication and sensing* (ISAC) [MCC+23].
Localization and sensing enable several applications, as summarized in [LCM+22, BYK+22, DA23]. A first application consists in area imaging as radio-frequency sensing generates high-resolution, day-and-night, and weather-independent images for a multitude of applications ranging from environmental monitoring, climate change research, and security-related applications. In indoor scenarios, sensing and localization can be used for smart home applications and for people assistance through activity recognition and tracking. Sensing and localization for gesture interaction detection via wireless signals is promising for human-computer interaction (HCI) technology. Along the same lines, sensing and positioning can improve immersive telepresence for enhanced interactions. Moreover, these services enable the generation of digital twin of objects and events in the digital domain, opening a series of new possibilities, e.g., to remotely control industrial tools for manufacturing, or optimize utilities and monitoring traffic in smart cities. Localization and sensing also enable remote control of robots and UAVs. Other applications are in the field of autonomous vehicles to implement platooning, simultaneous localization, and mapping (SLAM). Environmental monitoring can also benefit from radio frequency sensing as humidity and particle concentrations can be indicated by the propagation characteristics of transmitted wireless signals.

4.5 Privacy and Security for Distributed Learning

4.5.1 Distributed Learning

Distributed Learning (DL) is a sensitive context where privacy and security can be seriously harmed in modern communication systems [MLW+23]. In this context, we define threats to security as the possibility of unauthorized or malicious access to, change of, or denial of data or models. Usually, adversaries need to be expert or have full knowledge of the target system to harm security goals such as integrity, confidentiality, and availability. Privacy is instead related to the possible disclosure of personal information.

Users threatening DL systems can be divided into two categories based on their location, i.e., a) internal malicious participants and b) external attackers. The adversarial goals of such users and the respective attack types are influenced by three factors, namely:

1. Access to information
    a. White box: the adversary has some or full information (e.g., has access to model parameters, or to part of the training dataset).
    b. Black box: the adversary has no access to the model but can feed it with some inputs and observe the outputs.
2. When the attack is performed
    a. At training stage: the adversary can access and replace the model with a "shallow" version of it or modify it.
    b. At inference stage: the adversary can observe the outputs to infer the model characteristics.
3. Whether the attack is passive or active
    a. Passive: the adversary can only observe the process without changing anything of it.
    b. Active: the adversary can act on the learning operation (e.g., poisoning).

In DL systems, through active attacks, the integrity of models and datasets is harmed, while members' privacy is usually harmed in the case of black box or inference stage attacks. A taxonomy of the possible attack methods malicious users can perform in DL systems is given in Table 4-1.

Table 4-1: Taxonomy of common attacks in distributed learning

Attack surface	*Threat – Attack method*	*Attack goal*
Integrity	Poisoning	Degrade the model quality by either injecting poisoned data into the training model, or by directly modifying the model parameters.
	Evasion	Manipulate input data to change the output category from the original one to a determined or random one (e.g., add random noise to samples to cause misclassifications).
Privacy	Model inversion	Detect correlations between unknown inputs and outputs using the information obtained observing the outputs of known inputs. The objective is to reconstruct the input for a known label. It typically works with simple linear models and is a black box attack.
	Membership inference attack (MIA)	Infer the presence of specific information in the dataset of a member observing how the model performs at inference time under that specific dataset.
	Model extraction	Infer the parameters from a trained classifier in a black box way, given that the attacker has access to predictions.
	Functionality extraction	Create an imitation model by observing input-output pairs (e.g., the observed output signal can be utilized to generate labels to train a separated model via backpropagation).

In general, to protect DL from the attacks listed above, practitioners have four ways to enhance the robustness, privacy, and security of such systems:

- **Cryptography**. Encrypting data prevents attackers from easily stealing sensitive data, making also model inference attacks more difficult.
- **Robust Aggregation** (e.g., the Krum aggregation method [BEG+17] detects outliers, likely to be poisoned or malicious clients).
- **Network Compression:** reducing the amount of information that is exchanged is beneficial for communication resources, and at the same time reduces the amount of information exposed to adversaries.
- **Differential Privacy:** add random noise to the updating parameters.

The survey in [MLW+23] identifies four levels where privacy and security can be harmed in DL systems, together with possible countermeasures. Defence mechanisms are reported in the following **Error! Reference source not found.**, specifying to what type of attacks they are effective countermeasures.

Table 4-2: Common defence mechanisms used in distributed learning

Sharing plane	*Defence mechanism*	*Description*
Data	Adversarial training	Augment training data with adversarial examples to mitigate the risk of data poisoning [DZP+20].
	Anonymization and dummy data	Remove or hide identifying features from raw data [SDL+21].
	DP on data	Add noise (Gaussian or Laplacian) [DJW13].
	Data encryption	Define access policies through encryption of data [Hur13].
Model (FL)	DP on parameters	Add noise to the model parameters [WDM+20].
	Model compression	Encoding local models before sending them to the server [GKM+21]: this makes it more difficult for a third party to retrieve the model parameters by overhearing the message.
	Model encryption	Mathematical operations applied on encrypted models result in the same operation applied to the original message [PAH+18].
	MultiParty Computation (MPC)	Participants jointly compute functions over collective data without disclosing sensitive information [BIK+17].
	Statistical Analysis	Detecting and filtering outliers (possibly malicious) based on statistical information [MCL19].
	Pretest on auxiliary dataset	Computing accuracy on all local models, reducing the impact of low-quality ones [ZCZ+20].
	Authentication	For example, using blockchain technology [CMN+19].
	Authorization	Restrict actions that agents can perform based on their trust level [XPL+07].
Knowledge	DP and secure aggregation	FederBoost [TZH+23] runs the gradient boosting decision tree (GBDT) in a decentralized manner adding DP, hence protecting the order of samples.
	MPC	Pivot [XBZ+22] enables privacy-preserving vertical decision tree training and prediction ensuring no intermediate information is disclosed.
	Encryption	SecureBoost [CFJ+21] is a lossless privacy-preserving tree-boosting system using homomorphic encryption.

Results	DP	Use of DP in distributed reinforcement learning (RL), adding noise to the rewards [YZZ+20]. This prevents leakage of information on the environment.
	MPC	Teacher-student model with several agents and a single aggregator. Joint application of DP and MPC to securely combine outputs from multiple sources [Zha18].

4.5.2 Fully decentralized federated learning

A special setting of a DL system is that of (fully) decentralized federated learning (DFL) or *serverless* FL, where devices collaborate in a peer-to-peer fashion to train a common global model, without needing a central server acting as orchestrator. This setting can be used to intrinsically enhance the security of the system, as *there is no risk that a single central node (i.e., the server) is attacked successfully*, causing significant harm to the system (from a simple DoS to a global model poisoning). Nonetheless, some aspects must be considered to guarantee a secure and effective learning process also in DFL, i.e., ensuring that all participants are trusted, and information exchange is secured. This can be achieved by:

- Authentication and access control.
- Consensus: design algorithms protecting the integrity of information exchange.
- Blockchain-assisted DL.
- Fairness and personalization of the learned model. Fairness refers to the global model being representative of the whole dataset without disfavouring a subset of participating clients. Personalization is instead the process by which a target client privately customizes the global model with further training refinement.

We underline that, while standard reinforcement learning with a central aggregator has been extensively investigated, DFL still has to be properly explored.

4.5.3 Computational complexity and energy efficiency of defence mechanisms

It is worth noting that security mechanisms often add a layer of computational complexity (or decrease the performance of the learned model). To partially mitigate their impact, we can a) use lightweight encryption methods as a trade-off with effectiveness; b) design high-efficiency secure protocols (some protocols need to increase the number of information exchanges, leading to leakage risk and reduced resource efficiency); c) perform model compression, which can help reduce the computation and communication resource usage while also increasing privacy.

The integration of the energy perspective with defence mechanisms is closely related to the increase in computation and communication resource usage that these procedures usually require. However, as security and energy efficiency are contrasting objectives, they are not usually jointly optimized. Currently, the scientific literature lack works targeting this aspect in modern 6G networks. In [SYZ+21], the authors propose a pre-computed recommendation framework suggesting the level of security (e.g., the encryption key length) based on the available energy in the device battery or a maximum energy expenditure). The scenario is relevant in the cases of smartphones, which have batteries, or base stations powered by renewables. However, this work is still preliminary, and highlights the need for finding security-energy trade-offs, but still leaves open fundamental issues such as the facts that a) we need to learn the actual relation between the specific security scheme and the energy consumption in any specific context or use case, and b) attackers may be empowered by AI and learn from previous failures improving their strategies, hence making a pre-computed strategy ineffective.

4.5.4 Federated Learning

In FL, the models that clients forward can potentially leak information on the data and its properties. Based on exploiting the model parameters shared, several attacks have been identified. Common types of attacks on FL include membership inference, which attempts to infer membership state of a client regarding the participation in the FL process, property inference that aims to detect specific properties or features in the dataset not relevant to the main task, data reconstruction attacks that attempts to recover the original dataset or part of it via techniques like reversing the gradients shared by clients. These attacks can be considered passive since they primarily launch the attack by evaluating the received model updates. However, the practicality of the attacks like inference may lie in the requirement of correctly identifying the decision boundary changes on the models with each update, which could be difficult unless the attacker has a highly accurate understanding of the model behaviours.

For this, the attackers incorporate poisoning attacks to artificially alter the decision boundary of FL models. Therefore, *poisoning is a major issue that comes as a significant threat to both the security and privacy of FL*. These attacks can then be a boosting technique for inference attacks to improve their success rate. Further, attackers also aim to compromise the utility of the models via poisoning updates. Backdoors and trigger attacks from poisoning can also affect the utility of the model for a targeted set of classes. These triggers are also used for privacy leakages, where the trigger is activated when a specific property or data in the private dataset appears in a target client. Therefore, for practically implementing decentralised FL applications in future B5G/6G networks, early detection of poisoning and elimination are essential requirements to be addressed.

Several robust algorithms that aim to mitigate poisoning attacks on FL are introduced in the research literature [SSW+24]. The following are some of the key existing techniques used for detection and elimination of potentially malicious clients:

Krum: This method considers the similarity between the participant's updates by assuming a poisoner would propose an arbitrary gradient update compared with a benign client. However, for accurate results, this method requires an estimation of the number of poisoners in the network, which is unlikely to be determined early.

FoolsGold: This technique assigns cosine similarity-based reputation scores to participants based on their historical contributions and uses these scores to weigh the influence of their updates during aggregation. It may not perform well if these reputation scores are not available. Thus, this method may not recognise poisoners that appear dynamically.

Trimmed Mean: The trimmed mean is an aggregation rule where the server identifies k; $k < n/2$ trim parameters and eliminates the largest and smallest k values while aggregating the remaining $n - 2k$ values. This means that the maximum number of malicious clients should be less than 50% of total clients.

Median: In this technique, the server considers the median value of each parameter received from clients to minimise the effect of poisoners. This also has the issue of assuming the system has less than 50% malicious clients.

FLTrust: This mechanism is also an aggregation rule which uses ReLU (Rectified Liniear Unit)-clipped cosine similarity-based trust scores to aggregate model updates. They use a root dataset, maintain a separate model in the server, and assume the root dataset is clean and generally represents the overall client models. Therefore, this method may not work if client model data deviates from the root dataset or the root dataset itself is poisoned (e.g., if taken from a third party).

FLAME: Here, the authors use a combined cosine distance and clustering with Hierarchical Density-Based Spatial Clustering of Applications with Noise (HDBSCAN) for determining poisoners. However, they assume most of the clients (>50%) are benign, which can be a limiting factor with these distance-based metrics. Furthermore, they inject noise into the model updates, which can also affect the model performance and utility.

MOAT: This work uses SHAP feature attributions for assessing poisoning in FL. SHAP (SHapley Additive exPlanations) is a method for interpreting machine learning model predictions by attributing the contribution of each feature to the final prediction based on Shapley values from cooperative game theory. However, this solution does not consider a clustering approach for poisoning detection and uses a z-score of these features and a dynamic hyperparameter ε value that is set as a threshold for anomaly detection. This value can be difficult to estimate early, and it can vary significantly depending on the nature of the dataset.

4.6 Internet of Things (IoT)

The use of physical layer security (PLS) for IoT applications emerges naturally as it can accommodate a diverse range of requirements and design aspects. To exemplify this fact, in the following we briefly overview three important IoT use cases.

4.6.1 Radio Frequency Identification (RFID) for smart healthcare

Radio Frequency Identification (RFID) stands as a widely recognized pervasive technology offering promising prospects for introducing new services and enhancing traditional ones, e.g., in a smart hospital environment where patients and staff can be tracked in real time [ASH23]. However, attention to all aspects of information security becomes imperative. Particularly, RFID passive tags face vulnerabilities to attacks due to stringent limitations on security techniques for this technology. Among the critical threats to RFID-based information systems is data tampering, involving the malicious alteration of data stored in tag memory. Various PLS solutions are suggested.

4.6.2 Long Range (LoRA) for smart agriculture

LoRa stands as an ISM-band based Low-Power, Wide-Area Network (LPWAN) communication protocol renowned for its extensive network coverage, spanning approximately 20 kilometers or more with transmitting power below 14 decibels. Its widespread adoption in academia and industry is well-documented, owing to its ability to establish independent low-power wireless connections within an external infrastructure. From a PHY point of view, LoRA uses chirp-based transmissions that lend themselves naturally for PLS as they do not require the exchange of pilot sequences. Authentication, confidentiality and availability can all be explored with PLS [XW23].

4.6.3 Vehicle to everything (V2X) sidelinks

When a mobile device operates within a cellular network, data travels in both the uplink (UL) and downlink (DL) to/from a base station. Beginning with 4th Generation (4G) LTE Advanced and continuing with 5G, standards have been developed to enable devices to directly communicate with each other, known as Sidelink (SL), either with or without the support of the traditional cellular network [AR24]. The potential of this capability becomes evident, particularly in areas where conventional cellular coverage is lacking, such as sparsely populated regions, underground environments, or situations requiring rapid connectivity for specialized applications like autonomous vehicles. However, establishing sidelinks poses various technical challenges, including search, acquisition, registration, authentication, and radio resource allocation. In this aspect, the use of physical layer security for device pairing through secret key generation (SKG) and RF fingerprinting becomes prevalent. Fusion of these approaches with sensor data, e.g., cameras and radar, can enhance the trustworthiness of the sidelink connection.

4.7 Application Programming Interface (API) Exposure for Beyond 5G Networks

Exposure of APIs are expected to play a key role in transforming networks from only a conduit of data to a “network platform”, embedding intelligence and supportive services to the applications running on top. As such, in addition to providing important enablers for new use cases in current 5G networks, they play an important part of the vision for 6G / NextG mobile networks. Example use cases demonstrated at Mobile World Congress (MWC) 2023 included Quality on demand (QoD) for cloud gaming, online training, and video calls [EXAPI]. At the same time, security of APIs is becoming recognized as a very important topic in ICT security area. For instance, in enterprise IT, the Cloud Security Alliance’s Top Threats Working Group has raised “insecure interfaces and APIs” as #2 among the top threats to cloud systems [CLD+API].

Exposing core network APIs to internal and external application functions makes the 5G network more usable, controllable, and programmable. Moreover, with the advent of 5G networks, it is natural that more vertical industries will seek to enable their communications on 5G networks, resulting in an increase in the ecosystem of third parties consuming 5G Northbound APIs. Thus, 3GPP SA6 introduced a new specification, TS 23.222 [AGPP+23], that defines a common API framework (CAPIF) that incorporates common aspects applicable to any northbound service APIs to avoid duplication and inconsistency of approach between different API specifications.

There are several efforts ongoing across organizations (e.g., GSMA, Linux foundation, 3GPP, TM forum, etc.) to enable the Network as a Service (NaaS) paradigm through externally consumable APIs. One salient effort in this direction is the CAMARA project [CMR23] which is an open-source project unveiled by the GSMA and the Linux Foundation. The CAMARA project aims to provide developers with a powerful tool to integrate and access multiple telecom services by providing an abstraction from lower-level network APIs (e.g., 3GPP northbound APIs) to higher level service APIs (i.e., CAMARA defined API’s). This paves the way to new opportunities enabling innovation, simplifying development process, and reducing time-to-market, and helps telecom operators to stay competitive in an ever-changing market.

5 Threat Matrix for Selected Cases

In this section security threats for selected key 6G technical enablers are analysed using the methodologies identified in Sec. 3.

5.1 Distributed Multiple-Input Multiple-Output

Table 5-1: Threat matrix on D-MIMO

Threats	*Attack surface*	*Vulnerable Assets*	*Threat Definition*	*Mitigation*
Spoofing	Authenticity	1. Fronthaul links 2. Backhaul links	Impersonate (spoof identity), spoof origin of UE, AP and CPU.	Robust and certified authentication protocols also on MAC layer, potentially using PLS techniques such as fingerprinting 1. user plane 2. control plane
Tampering	Integrity	1. Fronthaul traffic and backhaul 2. Infrastructure nodes	1. Packet insert, delete, modify, replay, reorder. 2. Tampering HW and SW in AP and CPU.	1. Secure protocols with encryption and signatures, potentially using PLS 2. Tampering-proof HW, secure boot, secure SW updates, device attestation. Potential framework: FiGHT methodology.
Repudiation	Non-repudiability	1. Fronthaul traffic and backhaul 2. Infrastructure nodes	Denial of responsibility of action.	PLS techniques, such as fingerprinting. ISAC for intrusion detection.
Information disclosure	Confidentiality	1. Fronthaul traffic and backhaul 2. Infrastructure nodes	1. Weakly or unprotected data traffic and storage 2. Tampering HW and SW in AP and CPU	1. Encrypted traffic. 2. Protected HW and SW. Potential framework: FiGHT methodology.

Denial of service	Availability	APs, CPUs, and cables in physical reach of attacker	1. Physical attacks on APs, CPUs and cables 2. Denial of service attacks against APs and CPUs. APs: Jamming attacks, manipulated packets	1. Multi-AP resilience. 2. Anti-jamming techniques, robust (open, certified) protocols.

5.2 Reconfigurable Intelligent Surface

Table 5-2: Threat matrix on RIS

Threats	*Attack surface*	*Threat Definition*	*PLS Schemes*	*Vulnerabilities of PLS Schemes*	*Potential mitigations*
Spoofing	Authenticity	An attacker performs a sequence of attacks to PLA tag-based schemes (in absence of RIS) inducing a specific channel at the receiver.	The RIS can be used to randomize the propagation environment and strengthen PLA tag-based schemes.	1. complex channel estimation to initiate the PLA scheme. 2. the attacker can use the RIS itself. 3. when RIS is used, SNR is lower, which also affects authentication.	1. carefully choose the RIS configurations for PLA. 2. exploit multiple RIS configurations (over time) to authenticate a message.
Tampering	Integrity	an attacker injects signals that modify in a predictable manner signals transmitted from legitimate nodes the attacker may even control a RIS for this purpose.	1. Use modulation of the RIS (controlled by the defence) to strengthen wiretap coding, SKG, and positioning RF-fingerprinting: exploit the further degrees of freedom offered by the RIS to introduce and exploit randomness 2. If the attacker controls the RIS, sensing and reconstructions of the propagation environment can be exploited at the PHY for attack detection.	1. complex channel estimation 2. lower SNRs.	1. RIS configurations choice. 2. use of time for coding. 3. hybrid RIS (with sensing capabilities) can be useful to detect attackers.

Repudiation	Non-repudiability	A node claims to not have transmitted certain messages	Spectral / spatial fingerprints to prove transmissions took place exploit RIS to sense the environment and enhance fingerprinting.	Not examined yet in the literature.	Open issue.
Information disclosure	Confidentiality	The attacker eavesdrops signals transmitted by the legitimate user	1. Wiretap coding and RIS modulation 2. transmit artificial noise against (potential attackers) without disturbing the legitimate receiver, using the beamforming properties of the RIS.	1. assumptions of the position or receiver capabilities (noise) at the receiver are typically done. 2. if the attacker controls the RIS, he can disrupt initial channel estimation and affect the beamforming of AN.	1. Use artificial noise to force a maximum SNR at (potential) attackers. 2. Authenticate and make the channel estimation phase more robust. 3. Use hybrid RIS to detect anomalous behaviour.
Denial of service	Availability	Jamming attacks in various flavours.	All PLS schemes will be affected RIS can be exploited to detect the source of attack.	DoS, very poor rates, outages.	1. Detect the attack, also using sensing capabilities of RIS 2. HRIS can also be useful in this context for their enhanced sensing capability.

5.3 mmWaves and sub-THz

Wiretap coding for THz: due to the high directivity and the short range of transmissions, wiretap coding can be used

i) when there are grounds to assume that the eavesdropper is not in the LoS between Tx and Rx and
ii) when geofencing is the required security guarantee (no leakage outside a short range).

SKG on THz: due to channel hardening and resulting low entropy in the time domain, it is expected that SKG is more favourable in the frequency domain, exploiting the very large bandwidth of THz systems. However, this needs to be confirmed by experimentation.

Authentication via positioning: cm level localization accuracy is favourable for authentication using location and RF fingerprinting.

PUFs: may be possible to use PUFs, assuming a 5 msec authentication delay based on published results.

Table 5-3: Threat matrix on mmWaves and sub-THz

Threats	*Attack surface*	*Threat Definition*	*PLS Schemes*	*Vulnerabilities of PLS Schemes*	*Potential mitigations*
Spoofing	Authenticity	An adversarial node attempts to pass as a legitimate transmitter this can be implemented by i) malicious pilot contamination for wiretap coding, ii) precoding for location-based authentication.	1. PLS-based authentication using positioning. 2. PUFs for node authentication. 3. RF fingerprinting could also be used.	**Positioning**: AoA is robust when all digital processing, but open to attacks when using hybrid analog-digital processing. **PUFs**: Weak PUFs are vulnerable to machine learning attacks. **RF fingerprinting:** the fingerprints can be reproduced if assumed known by a malicious entity.	Joint AoA and ranging with radar not examined yet in the literature. For PUFs, potential use of strong PUFs and Wiener-Ziv lossy reconciliation. No known mitigation for cloning of RF fingerprints
Tampering	Integrity	An adversarial node injects signals that modify in a predictable manner signals transmitted from legitimate nodes	1. Wiretap coding 2. SKG 3. Positioning RF-fingerprinting	Wiretap coding +++ SKG: tampering of side information transmission Positioning ++++ and / or pilot sequences	For SKG hybrid use with authenticated encryption allows provide integrity guarantees for side information without any extra overhead.
Repudiation	Non-repudiability	A node claims not to have transmitted certain messages	Spectral / spatial fingerprints to prove transmissions took place	Not examined yet in the literature.	Open issue.

Information disclosure	Confidentiality	Wiretap coding: eavesdropper along the beam direction SKG on the shoulder eavesdropping attack	1. Wiretap coding 2. SKG 3. Positioning RF-fingerprinting	1. develop site dependent secrecy maps when using wiretap coding. 2. perform offline characterization of required privacy amplification for SKG, assuming worst case scenario.	Auxiliary use of attacker fingerprinting to identify the potential presence of eavesdropper, this is yet to be examined
Denial of service	Availability	Jamming attack: there are two possible types, proactive and reactive jammers. Proactive jammers jam with random signals along presumably all dimensions of the signal space. Reactive jammers use cognitive radio type devices to jam only along the most favourable signal space dimensions	All PLS schemes will be affected resulting in DoS.	DoS, very poor rates, outages.	1. Use of jamming fingerprinting to identify attack / attacker. 2. Use of frequency hopping to avoid jamming. 3. use of energy harvesting to collect jamming power to boost useful transmissions.
Elevation of privilege	Authorization	Same as authenticity			

5.4 Distributed Federated Learning

5.4.1 Analysis 1

Table 5-4: Threat matrix of common security and privacy attacks against DFL

Threat	Attack surface	Vulnerable Assets	Attacker knowledge	Description	Potential mitigations
Poisoning	Integrity	Data and Model	White/Black box	Degrade the model quality by either injecting poisoned data into the training model or by directly modifying the model parameters.	Model/data encryption Robust aggregation methods Adversarial training Statistical Analysis Authentication
Evasion		Model		Manipulate input data to change the output category from the original one to a determined or random one (e.g., add random noise to samples to cause misclassifications).	
Model inversion	Privacy	Data	Black box	Detect correlations between unknown inputs and outputs using the information obtained observing the outputs of known inputs. The objective is to reconstruct the input for a known label.	Model/data encryption Differential privacy Dummy data Anonymization Model compression
Membership Inference Attack (MIA)		Data		Infer the presence of specific information in the dataset of a member observing how the model performs at inference time under that specific dataset.	
Model Extraction		Model		Infer the parameters from a trained classifier given that the attacker has access to predictions.	

Functionality Extraction		Model		Create an imitation model by observing input-output pairs.	

5.4.2 Analysis 2

Table 5-5: Threat matrix of specific security and privacy attacks against DFL

Threat	Security property violation	Vulnerable Assets	Attacker	Attacker knowledge	Description	Potential mitigations	Additional considerations
Data Poisoning	Integrity and Availability	Data and Model	Federated Client	Black Box	A malicious client deliberately poisons its own data to spoil the global model performance. It is a threat to the integrity of the model that also impacts its availability.	Secure aggregation method as Clipping and Zeroing can be applied to reduce the impact of the malicious updates and/or to identify the malicious actor.	In both cases it is important to be sure about who sent the malicious update. In this PK signatures can be used to address the following: in case of a malicious client the non-repudiation property allows us to avoid that the client justifies himself addressing the issue to a MITM. On the other hand, in case of a MITM, the signature will be spoiled, and we can state that the malicious update does not come from the client.
Model Updates Poisoning	Integrity and Availability	Model	MITM	Black Box	A malicious actor posed on the communication line between the clients modify a client update to spoil the global model performance. It can be implemented in two different flavours: byzantine model poisoning if the poisoning is untargeted and backdooring if the poisoning is targeted to make the model fail on a particular task.	Secure aggregation method as Clipping and Zeroing can be applied to reduce the impact of the malicious updates and/or to identify the malicious actor. Moreover, hash of the client updates can be computed and appended to the transmitted data to spot unauthorized modifications on the client update.	

Evasion Attacks	Availability	Model	Malicious Actor	White/Black box	A malicious actor that has access to the FL client manipulates the inference input to cause a misclassification.	In this case the main mitigation is Adversarial Training: add in the training phase Adversarial Samples that can be specifically engineered or can be generated adding random noise to the actual training data.	
Model Stealing	Confidentiality	Model	Model Client	Black box	A client tries to reconstruct the model by querying it with a series of input and building an input/output dataset to subsequently train a new model.	In this the addition of querying limits or a watermarking logic are two valid options. While the first one can be considered a strict policy that prevents model extraction (but also limits the availability of the model) the second does not prevent the extraction but has the goal to spot models that have been extracted.	In a Federated setting we can consider the establishment of a proprietary node that implements the watermarking logic by locally training the model on particular instances that results in a particular classification label.
Data Extraction attacks	Confidentiality	Data	Federated Client, MITM	Black Box	Include both model inversion (try to find a potential input given an output) and membership attack (distinguish whether a sample was in the training set or not). Another fashion are data reconstruction attacks exploiting GRNN (generative Regression Neural Networks) which are capable of restoring training data and their corresponding labels from the model weights.	Existing strategies are gradient compression (not only reduces the communication overhead but also reduce the resources for inference), gradient encryption (using Homomorphic Encryption), and gradient perturbation implementing differential privacy.	

FL setting attacks	Confidentiality, Integrity, Availability	FL framework, FL clients	Malicious Actor	Knowledge about the FL setting (e.g. the framework used, FQDN of FL actors, physical access to FL actors , ...)	The majority of the open-source FL frameworks available are based on the GRPC protocol (e.g., openFL and Flower). Issues regarding the protocol should be considered.	Establishment of secure connection between the nodes, mutual authentication between the nodes, hardening of the nodes using secure storages and increasing their overall reliability.	This is a broad topic because we should consider the whole stack. In this ETSI proposed a secure platform for AI that has as root of trust the use of secure hardware and on that builds the whole platform.
Data supply chain attacks	Integrity	Data	Malicious Actor	Knowledge about the data supply chain (e.g., how each node retrieves its own data and the performed operations)	A malicious actor could attack the data supply chain in each of the point. For instance, he could perform jamming of a sensor, tampering of a memory or a communication channel etc ...	This can be considered as a data poisoning that is not implemented from the federated client (in this it is a victim). The solution could be the same of classic data poisoning because there is no way to perform a data analysis on the client side.	Also, this is a broad topic because we should consider the whole data supply chain.

5.5 Internet of Things

5.5.1 RFIDs for Smart Healthcare

In smart hospitals RFID tags are used to locate and track individuals.

Table 5-6: Threat matrix on RFIDs for Smart Healthcare

Threats	Attack surface	Vulnerable Assets	Threat Definition	PLS Schemes	Vulnerabilities of PLS Schemes	Potential mitigations

Spoofing	Authenticity		Depending on the frequency of the RFID tag, different spoofing attacks are possible https://hackaday.com/2010/11/28/rfid-spoofer-with-code-and-instructions/ https://www.reddit.com/r/rfelectronics/	We could possibly combine RFID (backscatter channel) with location based or PUF authentication over the air to provide authenticity guarantees.	In location-based authentication impersonation attacks might still be possible.	Mitigations proposed for PLA.
Tampering	Integrity		A critical threat for RFID-based information systems is represented by data tampering, which corresponds to the malicious alteration of data recorded in the tag memory.	Integrity through confidentiality using a wiretap coding approach.	Assumptions regarding the channel should be realistic and pertinent to the specific environment.	On-line channel learning to evaluate secrecy capacity.
Repudiation	Non-repudiability		A node claims not to have transmitted certain messages.	Not examined yet in the literature.	Open issue.	
Information disclosure	Confidentiality		The attacker eavesdrops signals transmitted by the legitimate user.	Wiretap coding for backscatter channels.	Assumptions of the position or receiver capabilities (noise) at the receiver are typically done.	On-line channel learning to evaluate secrecy capacity.
Denial of service	Availability		Jamming attacks in various flavours.	Links compromised.	DoS, very poor rates, outages.	jammer identification and mitigation.

5.5.2 LoRA Smart Agriculture

LoRA is a chirp-based communication system. PLS results for chirp-based systems app.

Table 5-7: Threat matrix on LoRA Smart Agriculture

Threats	*Attack surface*	*Vulnerable Assets*	*Threat Definition*	*PLS Schemes*	*Vulnerabilities of PLS Schemes*	*Potential mitigations*

Spoofing	Authenticity		An adversarial node attempts to pass as a legitimate transmitter this can be implemented by i) malicious pilot contamination for wiretap coding, ii) precoding for location-based authentication.	RF fingerprinting could be used for authentication or as a second factor of authentication.	The fingerprints can be reproduced if assumed known by a malicious entity.	No known mitigation for cloning of RF fingerprints, however could be combined with PUFs or crypto based authentication.
Tampering	Integrity		Hybrid PLS and crypto schemes using message authentication codes is possible thanks to the low date rates required in LoRA.	Integrity through confidentiality using a wiretap coding approach.	Assumptions regarding the channel should be realistic and pertinent to the specific environment.	On-line channel learning to evaluate secrecy capacity.
Repudiation	Non-repudiability		A node claims not to have transmitted certain messages.	Not examined yet in the literature.	Open issue.	
Information disclosure	Confidentiality		The attacker eavesdrops signals transmitted by the legitimate user.	1.Wiretap coding for chirp-based transmissions (wideband) 2. SKFK for chirp-based systems (note that no pilot sequences are required to be exchanged).	Assumptions of the position or receiver capabilities (noise) at the receiver are typically done.	On-line channel learning to evaluate secrecy capacity
Denial of service	Availability		Jamming attacks in various flavours.	Links compromised.	DoS, very poor rates, outages.	Jammer identification and mitigation.

5.5.3 V2X Sidelink

V2X requires communication between smart vehicles and infrastructure, other smart vehicles or pedestrians. While communication with infrastructure can be handled with standard crypto, the latter two scenarios are more demanding.

In particular, sidelinks (even outside the coverage of the 5G network) need alternative ways of authentication.

In this sense, the use of SKG and PLA can be very useful for device pairing in such scenarios.

Table 5-8: Threat matrix on V2X Sidelink

Threats	*Attack surface*	*Vulnerable Assets*	*Threat Definition*	*PLS Schemes*	*Vulnerabilities of PLS Schemes*	*Potential mitigations*
Spoofing	Authenticity		Assuming the application of interest is not a strict authentication but rather a device pairing, we can leverage SKG, RF fingerprinting and highly directive transmissions through beamforming.	beamforming, SKG, RF fingerprinting.	Impersonation attacks might still be possible.	Mitigations proposed for PLA.
Tampering	Integrity		Tampering over the air of critical messages.	Integrity through confidentiality using a wiretap coding approach.	Assumptions regarding the channel should be realistic and pertinent to the specific environment.	On-line channel learning to evaluate secrecy capacity.
Repudiation	Non-repudiability		A node claims to not have transmitted certain messages.	not examined yet in the literature.	Open issue.	
Information disclosure	Confidentiality		The attacker eavesdrops signals transmitted by the legitimate user.	Wiretap coding or SKG.	Assumptions of the position or receiver capabilities (noise) at the receiver are typically done.	On-line channel learning to evaluate secrecy capacity.
Denial of service	Availability		Jamming attacks in various flavours.	Links compromised.	DoS, very poor rates, outages.	Jammer identification and mitigation.

5.6 Threat Matrix for API Exposure

Threat analysis is performed on the Quality on Demand (QoD) API example and call flows as described in [CMR+22] as a starting point. The technical scope of this study is limited to 5G network exposure.

Description of the main players in the CAMARA system below:

- Telecom operators have various capabilities across different domains (Network APIs, IT APIs, cloud APIs) that they want to expose to external consumers. They perform this exposure by means of harmonized Service APIs defined by the CAMARA project. This Service API exposure is facilitated with the help of the transformation function and the exposure gateway modules. The Exposure Gateway provides all the capabilities needed to police the interaction between telecom operators and the external entities, while the transformation function keeps a mapping between Network APIs and the service APIs and executes workflows to enforce these mappings.
- Aggregators are the entities (cloud or platform providers) that perform aggregation of Service APIs in the form of Enriched Service APIs and expose them to the capability consumers.
- Capability Consumers are the end customers consuming the Enriched Service APIs. The capability consumers may in practice be enterprise/user applications (e.g., Zoom video conferencing servers, Blacknut gaming servers, etc.). The consumers make API calls to derive functionality from the network and in turn get charged for the services obtained.

Adversaries are distinguished by the position of access to the exposure system and subdivide them into various ‘types’ based on the context and motivations of the adversary. Table 5-10 is provided to explain adversaries that are defined under Table 5-9. It is seen that attacks on the system can occur at several layers/levels of abstraction (e.g., application level, network level, user level, authentication process level etc.) thereby implying protection is needed at different touch points and at different layers. Further, the aspect of competition between operators and the presence of potentially untrusted/compromised intermediary hops between the API consumer and the network are other points of note when considering the adversary space.

Table 5-9: Potential threats to the end-to-end exposure functionality view

Adversary Type	*Vulnerable Assets\Threat Surface*	*Threat Vector*	*Security property violation/ Desired Property*	*Threats*	*Description*
Telco Insider	API exposure function (e.g., NEF, SEAL, etc.)	Information disclosure	Confidentiality	Snooping on Incoming requests/ outgoing responses to learn subscriber/other info.	Insider in the NEF, SEAL, etc.
		Denial of services	Availability	Modifying API requests/ responses (T) *DoS on a consumer by denying/dropping responses.	
		Repudiation	Non-repudiability	Clearing logs associated with API requests/responses or attacker actions.	
		Lateral Movement	Containment	Attacking the consumer/aggregator or other external element.	
Network hacker-1	Network connectivity-1 Network API	Information disclosure	Confidentiality	Snooping on Network API calls.	
		Tampering	Integrity	Modifying Network API requests to affect the telco network config, etc.	
		Tampering	Integrity	Modifying Network API responses to affect the external element/consumer.	
		Denial of services	Availability	DoS on the subscriber by denying/dropping requests/ responses.	
		Spoofing	Authenticity	Spoofing a network exposure function.	
		Spoofing	Authenticity	Spoofing a legitimate consumer/external intermediary element.	
Untrusted intermediary - Transformation function	Transformation Function	Tampering	Integrity	Tamper with the transformation mapping between the service API and the network API.	
		Information disclosure	Confidentiality	Snooping on/ learning internals of transformation mapping between the service API and the network API.	
		Tampering	Integrity	Tamper with requests/responses in transit.	

		Denial of services	Availability	Delete transformation mapping config.	
		Denial of services	Availability	Overload transformation function with unnecessary requests.	
Untrusted intermediary – Exposure Gateway	Exposure Gateway (GATE)	Tampering	Integrity	Tampering with CAPIF authentication and authorization flows.	GATE provides all the capabilities that are needed to police the interaction between the operator and the external applications, in relation to service API invocation. These capabilities include service API publication & discovery, access control (authentication & authorization of applications), auditing, accounting, and logging.
		Repudiation	Non-repudiability	Erasing logs maintained in CAPIF.	
		Elevation of privilege	Authorization	Granting unauthorized elevated privileges to certain API consumers.	
		Information disclosure	Confidentiality	Leaking credentials/keys to untrusted locations.	
		Information disclosure	Confidentiality	Snoop on east-west traffic.	
		Tampering	Integrity	Misdirecting users to the wrong/attacker-controlled AEF.	
		Denial of services	Availability	Cause Denial of Service by making the exposed API undiscoverable.	
		Lateral Movement	Containment	Move laterally to partner operator via east-west interface.	
Network hacker-5	Network connectivity-5	Tampering	Integrity	Tampering with API roaming calls between operators.	
		Information disclosure	Confidentiality	Snooping on API roaming calls.	
		Denial of services	Availability	Denial of Service on operators.	
		Spoofing	Authenticity	Spoofing a partner operator.	
Untrusted Intermediary – Aggregator	Aggregator(s)	Tampering	Integrity	Routing API traffic to the wrong destination.	
		Information disclosure	Confidentiality	Snooping on information across operators/participants/competitors.	
		Denial of services	Availability	Deny service preferentially to some parties.	

		Tampering	Integrity	Poisoning data/sources associated with enrichment functions feeding the Enriched Service API.	
		Tampering	Integrity	Tampering with responses received from the operator through Service API’s.	
Network hacker -3	Network connectivity-3, Service API	Information disclosure	Confidentiality	Snooping on Service API calls.	
		Tampering	Integrity	Modifying Service API requests to affect the telco network config, etc.	
		Tampering	Integrity	Modifying Service API responses to affect the external element/consumer.	
		Denial of services	Availability	DoS on the subscriber by denying/dropping requests/ responses.	
		Spoofing	Authenticity	Spoofing an exposure gateway.	
		Spoofing	Authenticity	Spoofing a legitimate aggregator/ external consumer.	
		Information disclosure	Confidentiality	Snooping on the Enriched API traffic (e.g., guessing what the user is doing on the UE based on QoD sessions).	
		Denial of services	Availability	Causing amplification by injecting high complexity calls repeatedly: One EAPI call can translate to many NAPI calls, this could be abused	
		Spoofing	Authenticity	Impersonating a legitimate consumer.	
		Tampering	Integrity	Tampering with Enriched API calls in transit.	
Untrusted partner	Exposure partner(s)	Information disclosure	Confidentiality	Learn confidential information about the partner operator.	
		Lateral Movement	Containment	Move laterally to the partner operator.	
		Tampering	Integrity	Inject unauthorized calls to the partner gateway.	
		Tampering	Integrity	Redirect API calls to unauthorized destination.	

		Denial of services	Availability	Cause DoS by dropping requests on east-west interface.	
Untrusted vendor		Information disclosure	Confidentiality	Learn confidential information about API requests/responses.	Supply chain attacks. The vendor can be anywhere (e.g., NEF, CAPIF, Aggregator, etc.).
		Information disclosure	Confidentiality	Learn confidential information about the operators.	
		Information disclosure	Confidentiality	Learn confidential information about the consumers/subscribers of the APIs.	
		Tampering	Integrity	Tamper with requests/responses.	
		Denial of services	Availability	Cause targeted DoS on certain API consumers.	
		Lateral Movement	Containment	Move laterally into other network elements.	
Exposure Application hacker	Application layer			Exploit vulnerabilities in the exposure application software to:	
		Tampering	Integrity	Send unauthorized requests.	
		Information disclosure Elevation of privilege	Confidentiality Authorization	Steal secrets/API keys.	
		Information disclosure	Confidentiality	Steal/learn information about the network.	
		Information disclosure	Confidentiality	Steal/learn information about other subscribers/devices.	
		Denial of services	Confidentiality	Delete important config/data relating to the app.	
		Tampering Denial of services Information disclosure	Integrity	Make unauthorized network config. changes.	
		Lateral Movement	Containment	Move laterally into the network/intermediary node.	

Table 5-10: Adversary types for threats to APIs

Adversary	*Type*	*Attacker Location*	*Example Motivation(s)*
Outsider - Consumer	API hacker	Capability consumer	Get unauthorized access to data/config. of users, make unauthorized changes.
	Competitor	Capability consumer	Tamper with a competitor's service, cause resource starvation, learn secrets, etc.
	Bot/Malicious app/ compromised device	Capability consumer	Make automated unauthorized API requests/changes on behalf of an attacker, e.g., DoS a service.
	API user with legitimate access: curious user, unintentional attacker	Capability consumer	Enumeration of users, exploration leading to unintentionally learning about subscriber data.
Untrusted Intermediary	Misbehaving/untrusted / compromised Aggregator/ aggregator user	Aggregator	Tampering requests/ responses, snooping, DoS etc. e.g., via Service API's.
	Misbehaving/untrusted / compromised Aggregator/ aggregator user	Exposure gateway	Tampering requests/responses, snooping, DoS etc.
	Misbehaving/untrusted / compromised Aggregator/ aggregator user	Transformation function	Tampering requests/responses, command transformation tampering, snooping, DoS, etc.
Network hacker-1	MITM, traffic sniffing, etc.	Hacker on interface 1 between the telco and transformation function.	E.g., Snooping on Network API calls.

Network hacker-3	MITM, traffic sniffing, etc.	Hacker on interface 3 between the exposure gateway and aggregator.	E.g., Snooping on service API calls.
Network hacker-4	MITM, traffic sniffing, etc.	Hacker on interface 4 between the aggregator and capability consumer.	E.g., Snooping on enriched service API calls.
Network hacker-5	MITM, traffic sniffing, etc.	Hacker on the East/ Westbound/ interoperability interface 5	E.g., tampering with API roaming calls between operators.
Untrusted partner	Misbehaving/untrusted / compromised Partner/ partner-user	Telco roaming partner on the east/ westbound interface.	E.g., Stealing information from the partner, etc.
Insider – from telco perspective	Misbehaving/compromised user/admin.	Within telco environment.	E.g., Snooping on incoming requests at the NEF, modifying API responses, DoS a consumer, etc.
Untrusted equipment vendor	e.g., Compromised equipment vendor of exposure node/ intermediary jump point on the way to the API consumer.	Multiple	E.g., Supply chain attack to steal data.
Exposure Application hacker	Finds vulnerabilities in the exposure application to be able to affect malicious actions.	Capability consumer	E.g., exploiting a vuln. In the exposure application logic to be able to get elevated privileges to make network changes via the API’s.

6 Conclusions

In this deliverable we have reported the work on assessing existing solutions and characterization of the threat landscape towards 6th Generation (6G).

In Sec. 2, we summarized the state-of-the-art on existing solutions for threat detection and protection 5G networks and emerging 6G networks. In particular, related to 5G, we discussed the ENISA threat landscape report for 5G networks, the FiGHT threats matrix, and 3GPP reports on security analysis related to false base stations and URLLC. Related to 6G, we reviewed the HEXA-X-II works on NoN, cloud continuum, RAN disaggregation mechanisms, AI security and privacy preservation.

In Sec. 3, we gave an overview of existing methodologies for threat identification, with focus on the CIA model, STRIDE, TVRA methods and the FiGHT method, which we subsequently used for threat identification of a set of key 6G technical enablers, use cases and applications.

In Sec. 4, we introduced our considered key 6G technical enablers, D-MIMO, RIS, mmWaves and sub-THz, RF sensing and localization, distributed learning, use cases related to IoT, and API exposure.

In Sec. 5, we presented our threat analysis of these key 6G technical enablers, use cases and applications.

These results will serve as basis for the design of cybersecurity capabilities within the other technical work packages in ROBUST-6G.

References

[23.501] 3GPP TS23.501 “System architecture for the 5G System (5GS)”, version 16.6.0 Release 16, October 2020. Online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

[23.725] 3GPP TR 23.725, “Study on enhancement of Ultra-Reliable Low-Latency Communication (URLLC) support in the 5G Core network (5GC)”, June 2019. Online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3453

[28.312] 3GPP, TS 28.312 “Intent driven management services for mobile networks” v18.1.1, Sept. 2023. Online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3554

[33.809] 3GPP TR 33.809, “Study on 5G security enhancements against False Base Stations (fBS)”, Sep 2023. Online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539

[33.825] 3GPP TR 33.825, “Study on the security of Ultra-Reliable Low-Latency Communication (URLLC) for the 5G System (5GS)”, Oct 2019. Online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3548

[36.888] 3GPP TR 36.888, “Study on provision of low-cost Machine-Type Communications (MTC) User Equipments (UEs) based on LTE (Release 12)”, June 2013. Online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2578

[ABB+20] P. Ala-Pietilä, Y. Bonnet, U. Bergmann, M. Bielikova, C. Bonefeld-Dahl, W. Bauer, and A. Van Wynsberghe, “The assessment list for trustworthy artificial intelligence (ALTAI),” European Commission 2020.

[AGPP+23] 3GPP, “TS 23.222 Common API Framework for 3GPP Northbound APIs”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDet ails.aspx?specificationId=3337, accessed on Apr 2023.

[AR24] Annu and P. Rajalakshmi, "Towards 6G V2X Sidelink: Survey of Resource Allocation—Mathematical Formulations, Challenges, and Proposed Solutions," in IEEE Open Journal of Vehicular Technology, vol. 5, pp. 344-383, 2024.

[ASH23] A. Abugabah, A. A. L. Smadi, L. Houghton,” RFID in Health care: A review of the real-world application in hospitals”, Procedia Computer Science, Volume 220, 2023, Pages 8-15.

[ATT&CK] MITRE ATT&CK® Matrix for Enterprise, Online: https://attack.mitre.org/

[ATF+22] A. Abouaomar, A. Taik, A. Filali, and S. Cherkaoui, “Federated deep reinforcement learning for open ran slicing in 6g networks,” IEEE Comm. Mag. Vol. 61, no. 2, pp. 126-132, 2022.

[BAB+23] S. Bartoletti, C. S. Álvarez-Merino, R. Barco, et al., "Positioning Methods." Positioning and Location-based Analytics in 5G and Beyond (2023): 19-50.

[BEG+17] P. Blanchard, E.M. El Mhamdi, R. Guerraoui, and J. Stainer, 2017. Machine Learning with Adversaries: Byzantine Tolerant Gradient Descent. Advances in Neural Information Processing Systems, 30.

[BIK+17] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H.B. McMahan, S. Patel, D. Ramage, A. Segal and K. Seth, 2017, October. Practical secure aggregation for privacy-preserving machine learning. In *proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1175-1191).

[BKK21] A. Bemani, N. Ksairi, and M. Kountouris, “AFDM: A full diversity next-generation waveform for high mobility communications,” in IEEE Int. Conf. Commun. Workshops (ICC Workshops), Jun. 2021, pp. 1–6.

[BKK23] A. Bemani, N. Ksairi, and M. Kountouris. "Affine frequency division multiplexing for next generation wireless communications." IEEE Transactions on Wireless Communications (2023).

[BKK24] Bemani, Ali, Nassar Ksairi, and M. Kountouris, "Integrated Sensing and Communications with Affine Frequency Division Multiplexing." arXiv preprint arXiv:2402.16468 (2024).

[BMA+22] S. Bhattacharjee, K. V. Mishra, R. Annavajjala and C. R. Murthy, "Evaluation of orthogonal chirp division multiplexing for automotive integrated sensing and communications." ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2022.

[BYK+22] A. Behravan, V. Yajnanarayana, M. Keskin, et al. "Positioning and sensing in 6G: Gaps, challenges, and opportunities." IEEE Vehicular Technology Magazine 18.1 (2022): 40-48.

[BZM+18] R. Bomfin, D. Zhang, M. Matthé, and G. Fettweis, “A theoretical framework for optimizing multicarrier systems under time and/or frequency- selective channels,” IEEE Commun. Lett., vol. 22, no. 11, pp. 2394– 2397, Nov. 2018.

[CFJ+21] K. Cheng, T. Fan, Y. Jin, Y. Liu, T. Chen, D. Papadopoulos and Q. Yang, 2021. Secureboost: A lossless federated learning framework. *IEEE Intelligent Systems*, *36*(6), pp.87-98.

[CISA20] US CISA "5G Security and Resilience", 2020. Online: https://www.cisa.gov/topics/risk-management/5g-security-and-resilience

[CISA19] CISA report "Overview of Risks Introduced by 5G Adoption in the United States", Online: https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf

[CLD+API] Cloud Security Alliance, “Top Threat #2 to Cloud Computing: Insecure Interfaces and APIs”, 2022-07-3. Online: https://cloudsecurityalliance.org/blog/2022/07/30/top-threat-2-to-cloud-computing-insecure-interfaces-and-apis.

[CMN+19] D. Calvaresi, Y. Mualla, A. Najjar, S. Galland, and M. Schumacher, “Explainable multi-agent systems through blockchain technology,” in Proc. Int. Workshop Explainable, Transparent Auto. Agents Multi-Agent Syst. (EXTRAAMAS), vol. 11763, Montreal, QC, Canada, May 2019, pp. 41–58.

[CMR+22] J. Ordonez-Lucena, F. Dsouza, (2022, August). Pathways towards network-as-a-service: the CAMARA project. In Proceedings of the ACM SIGCOMM Workshop on Network-Application Integration (pp. 53-59).

[CMR23] CAMARA, “Camara Project – Linux Foundation Project”, https://camaraproject.org.

[CSB+22] H. Chen, H. Sarieddeen, T. Ballal, H. Wymeersch, M. S. Alouini and T. Y. Al-Naffouri, "A tutorial on terahertz-band localization for 6G communication systems." IEEE Communications Surveys & Tutorials 24.3 (2022): 1780-1815.

[DA23] U. Demirhan and A. Alkhateeb. "Integrated sensing and communication for 6G: Ten key machine learning roles." IEEE Communications Magazine (2023).

[DBB+21] C. De Lima, D. Belot, R. Berkvens, et al. (2021). “Convergent communication, sensing and localization in 6G systems: An overview of technologies, opportunities and challenges,” IEEE Access, 9, 26902-26925.

[DJV+15] D. Dash, A. Jayaprakash, J. Valarmathi, and G. R. Reddy, “Generalized OFDM-LFM waveform design and analysis for multistatic airborne radar,” in Proc. IEEE Power Commun. Inf. Technol. Conf. (PCITC), 2015, pp. 924–929.

[DJW13] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, “Local privacy and statistical minimax rates,” in Proc. 51st Annu. Allerton Conf. Commun., Control, Comput. (Allerton), Oct. 2013, p. 1592.

[DZP+20] Y. Dong, Z. Deng, T. Pang, J. Zhu, and H. Su, “Adversarial distributional training for robust deep learning,” Proc. Annu. Conf. Neural Inf. Process. Syst. (NIPS), Dec. 2020, pp. 8270–8283.

[ENISA19]: ENISA, “Report for 5G Networks”, Nov. 2019. Online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

[ETSI-RIS] ETIS Reconfigurable Intelligent Surfaces, Online: https://www.etsi.org/technologies/reconfigurable-intelligent-surfaces.

[ETSI TS 102 165-1] ETSI TS 102 165-1 “CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)”, V5.2.5 (2022-01). Online: https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.05_60/ts_10216501v050205p.pdf

[EXAPI] Ericsson News, “Operators are opening up 5G networks to application developers to drive innovation”, https://www.ericsson.com/en/news/2023/2/operators-are-opening-up5g-networks-to-application-developers-to-drive-innovation, Feb 2023.

[FiGHT] MITRE FiGHT™ “5G Hierarchy of Threats”, Online: https://fight.mitre.org/

[FU98] G. D. Forney and G. Ungerboeck, “Modulation and coding for linear Gaussian channels”, IEEE Transactions on Information Theory, vol. 44, no. 6, pp. 2384-2415, October 1998.

[GKC+20] L. Gaudio, M. Kobayashi, G. Caire, and G. Colavolpe, “On the effectiveness of OTFS for joint radar parameter estimation and communication,” IEEE Trans. Wireless Commun., vol. 19, no. 9, pp. 5951–5965, Sep. 2020.

[GKM+21] V. Gandikota, D. Kane, R. K. Maity, and A. Mazumdar, “vqSGD: Vector quantized stochastic gradient descent,” in Proc. Int. Conf. Artif. Intell. Statist. (AISTATS), vol. 130, Apr. 2021, pp. 2197–2205.

[HEA16-D2] HEAVENS, “Security models”, HEAVENS, Project Deliverable D2, Mar. 2016. [Online]. Available: https://autosec.se/wp-content/uploads/2018/03/HEAVENS_D2_v2.0.pdf.

[HEX21-D22] Hexa-X, “Initial radio models and analysis towards ultra-high data rate links in 6G,” Hexa-X, Project Deliverable D2.2, Dec. 2021. [Online]. Available: https://hexa-x.eu/wp-content/uploads/2022/01/Hexa-X-D2_2.pdf

[HEX23-D13] Hexa-X Deliverable D1.3 “Targets and requirements for 6G - initial E2E architecture,” Hexa-X project, Feb. 2022, [Online]. Available: https://hexa-x.eu/wp-content/uploads/2022/03/Hexa-X_D1.3.pdf

[HSD+22l] S. Helal, H. Sarieddeen, H. Dahrouj, T. Y. Al-Naffouri, and M. S. Alouini, "Signal processing and machine learning techniques for terahertz sensing: An overview." IEEE Signal Processing Magazine 39.5 (2022): 42-62.

[Hur13] J. Hur, “Improving security and efficiency in attribute-based data sharing,” IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271–2282, Oct. 2013.

[HYM+23] O. Haliloglu, H. Yu, C. Madapatha, H. Guo, F. E. Kadan, A. Wolfgang, R. Puerta, P. Frenger and T. Svensson, “Distributed MIMO Systems for 6G”, EuCNC & 6G Summit 2023, June 6-9, Gothenburg, Sweden.

[KBP23] S. Kukliński, J. M. Batalla and J. Pieczerak, "Dynamic and Multiprovider-based Resource Infrastructure in the NFV MANO Framework," NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, Miami, FL, USA, pp. 1-4, 2023. doi: 10.1109/NOMS56928.2023.10154398.

[KKU+22] F. Klement, S. Katzenbeisser, V. Ulitzsch, J. Krämer, S. Stanczak, Z. Utkovski, I. Bjelakovic, and G. Wunder, “Open or not open: Are conventional radio access networks more secure and trustworthy than open-RAN?” 2022. [Online]. Available: https://arxiv.org/abs/2204.12227.

[LCM+22] Liu, F., Cui, Y., Masouros, C., Xu, J., Han, T. X., Eldar, Y. C., and Buzzi, S. "Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond." IEEE journal on selected areas in communications 40.6 (2022): 1728-1767.

[Lin22] X. Lin, “An overview of 5G advanced evolution in 3GPP release 18,” IEEE Commun. Stand. Mag., vol. 6, no. 3, pp. 77–83, 2022.

[Maz75] J. E. Mazo, “Faster-than-Nyquist signaling”, Bell System Technical Journal, vol. 54, no. 8, pp. 1451-1462, October 1975.

[MBC+23] F. Meneghello, A. Blanco, A. Cusano, J. Widmer, and M. Rossi, "Wi-Fi Multi-Path Parameter Estimation for Sub-7 GHz Sensing: A Comparative Study." 2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, 2023.

[MCC+23] F. Meneghello, C. Chen, C. Cordeiro and F. Restuccia, "Toward integrated sensing and communications in IEEE 802.11 bf Wi-Fi networks." IEEE Communications Magazine 61.7 (2023): 128-133.

[MCL19] L. Muñoz-González, K. T. Co and E. C. Lupu, 2019. Byzantine-robust federated machine learning through adaptive model averaging. *arXiv preprint arXiv:1909.05125*.

[MLW+23] C. Ma, J. Li, K. Wei, B. Liu, M. Ding, L. Yuan, Z. Han, and H. V. Poor, “Trusted AI in multiagent systems: An overview of privacy and security for distributed learning,” Proceedings of the IEEE, vol. 111, no. 9, pp. 1097-1132, Sept. 2023, doi: 10.1109/JPROC.2023.3306773.

[PAH+18] L. T. Phong, Y. Aono, T. Hayashi, L. Wang, and S. Moriai, “Privacy-preserving deep learning via additively homomorphic encryption,” IEEE Trans. Inf. Forensics Security, vol. 13, no. 5, pp. 1333–1345, May 2018.

[PBC+21] A. B. Pizarro, J. P. Beltrán, M. Cominelli, F. Gringoli and J. Widmer, "Accurate ubiquitous localization with off-the-shelf IEEE 802.11 ac devices." Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services. 2021.

[PPR+23] P. Porambage, J. Pinola, Y. Rumesh, C. Tao, and J. Huusko, “Xcaret: Xai based green security architecture for resilient open radio access networks in 6g,” in 2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). IEEE, pp. 699–704, 2023.

[RIS23+D26] T. Svensson, M. Crozzoli, V. Sciancalepore, M.-H. Hamon, D.-T. Phan-Huy, G. C. Alexandropoulos, K. Katsanos, B. Denis, A. Allasia, F. Saggese, P. Popovski, L. Bastianelli, F. Moglie, P. Di Lorenzo, H2020-ICT-52 RISE-6G “D2.6 RISE Network Architectures and Deployment Strategies Analysis: Final Results”, Dec. 2023.

[RISE-6G] H2020-ICT-52 “Reconfigurable Intelligent Sustainable Environments for 6GWireless Networks” (RISE-6G). Online: https://rise-6g.eu/.

[RXK+19] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, and G. C. Trichopoulos, "Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond," in IEEE Access, vol. 7, pp. 78729-78757, 2019.

[SC20] G. D. Surabhi and A. Chockalingam, “Low-complexity linear equalization for OTFS modulation,” IEEE Commun. Lett., vol. 24, no. 2, pp. 330–334, Feb. 2020.

[SDL+21] S. Shaham, M. Ding, B. Liu, S. Dang, Z. Lin, and J. Li, “Privacy preserving location data publishing: A machine learning approach,” IEEE Trans. Knowl. Data Eng., vol. 33, no. 9, pp. 3270–3283, Sep. 2021.

[SSW+24] C. Sandeepa, B. Siniarski, S. Wang, M. Liyanage, "SHERPA: Explainable Robust Algorithms for Privacy-Preserved Federated Learning in Future Networks to Defend Against Data Poisoning Attacks." 2024 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2024.

[SVB+22] A. Shastri, N. Valecha, E. Bashirov, et al. "A review of millimeter wave device-based localization and device-free sensing technologies and applications." IEEE Communications Surveys & Tutorials 24.3 (2022): 1708-1749.

[SYZ+21] S. Shen, C. Yu, K. Zhang, J. Ni and S. Ci, "Adaptive and Dynamic Security in AI-Empowered 6G: From an Energy Efficiency Perspective," IEEE Communications Standards Magazine, vol. 5, no. 3, pp. 80-88, September 2021, doi: 10.1109/MCOMSTD.101.2000090.

[TAZ+13] A. Tzanakaki, M. P. Anastasopoulos, G. S. Zervas, B. R. Rofoee, R. Nejabati and D. Simeonidou, “Virtualization of heterogeneous wireless-optical network and IT infrastructures in support of cloud and mobile cloud services”. IEEE Communications Magazine, vol. 51, no. 8, pp. 155-161, August 2013.

[TZH+23] Z. Tian, R. Zhang, X. Hou, J. Liu, and K. Ren, "FederBoost: Private Federated Learning for GBDT." *IEEE Transactions on Dependable and Secure Computing* (2023).

[WDM+20] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, T. Q. Quek and H. V. Poor, 2020. Federated learning with differential privacy: Algorithms and performance analysis. *IEEE transactions on information forensics and security*, *15*, pp.3454-3469.

[WKG+22] Q. Wang, A. Kakkavas, X. Gong, and R. A. Stirling-Gallacher, "Towards integrated sensing and communications for 6G." 2022 2nd IEEE International Symposium on Joint Communications & Sensing (JC&S). IEEE, 2022.

[WLH+22] Y. Wu, F. Lemic, C. Han and Z. Chen, "Sensing integrated DFT-spread OFDM waveform and deep learning-powered receiver design for terahertz integrated sensing and communication systems." IEEE Transactions on Communications 71.1 (2022): 595-610.

[WLY+23] Z. Wei, H. Liu, X. Yang, W. Jiang, H. Wu, X. Li and Z. Feng, "Carrier Aggregation Enabled Integrated Sensing and Communication Signal Design and Processing." IEEE Transactions on Vehicular Technology (2023).

[WQW+23] Z. Wei, H. Qu, Y. Wang, et al. "Integrated sensing and communication signals toward 5G-A and 6G: A survey." IEEE Internet of Things Journal 10.13 (2023): 11068-11092.

[WWB+23] J. Widmer, H. Wymeersch, S. Bartoletti, et al. "Enablers Toward 6G Positioning and Sensing." Positioning and Location-based Analytics in 5G and Beyond (2023): 75-97.

[XBZ+22] R. Xu, N. Baracaldo, Y. Zhou, A. Abay and A. Anwar, 2022. Privacy-preserving vertical federated learning. In *Federated Learning: A Comprehensive Overview of Methods and Applications* (pp. 417-438). Cham: Springer International Publishing.

[XPL+07] L. Xiao, A. Peet, P. Lewis, S. Dashmapatra, C. Sáez, M. Croitoru, J. Vicente, H. Gonzalez-Velez and M. L. i Ariet, 2007, July. An adaptive security model for multi-agent systems and application to a clinical trials environment. In *31st Annual international computer software and applications conference (COMPSAC 2007)* (Vol. 2, pp. 261-268). IEEE.

[XW23] J. Xu and D. Wei, "Polarization Fingerprint-Based LoRaWAN Physical Layer Authentication," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 4593-4608, 2023.

[YWL+21] W. Yuan, Z. Wei, S. Li, J. Yuan, and D. W. K. Ng, "Integrated sensing and communication-assisted orthogonal time frequency space transmission for vehicular networks." IEEE Journal of Selected Topics in Signal Processing 15.6 (2021): 1515-1528.

[YWL+22] W. Yuan, Z. Wei, S. Li, R. Schober, and G. Caire, "Orthogonal time frequency space modulation—Part III: ISAC and potential applications." IEEE Communications Letters 27.1 (2022): 14-18.

[YZZ+20] D. Ye, T. Zhu, W. Zhou, and P. S. Yu, “Differentially private malicious agent avoidance in multiagent advising learning,” IEEE Trans. Cybern., vol. 50, no. 10, pp. 4214–4227, Oct. 2020.

[ZAM22] W. Zhao, S. Alwidian, and Q. H. Mahmoud, “Adversarial Training Methods for Deep Learning: A Systematic Review.” Algorithms vol. 15, no. 8. pp. 283, 2022.

[ZCZ+20] Y. Zhao, J. Chen, J. Zhang, D. Wu, J. Teng, and S. Yu, “PDGAN: A novel poisoning defense method in federated learning using generative adversarial network,” in Proc. Int. Conf. Algorithms Architectures Parallel Process. (ICAPP), 2020, pp. 595–609.

[Zha18] J. Zhao, “Distributed deep learning under differential privacy with the teacher-student paradigm,” in Proc. 32nd AAAI Conf. Artif. Intell. (AAAI), New Orleans, LA, USA, Feb. 2018.