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

D2.2 6G Use Case Scenarios and Requirements

Lead beneficiary	TSS	**Lead author**	Vincent Lefebvre
Reviewers	Mays AL-Naday (UESSEX), Gürkan Gür (ZHAW)		
Type	R	**Dissemination**	PU
Document version	V1.0	**Due date**	31/10/2024

Co-funded by the European Union

6GSNS

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

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

UKRI UK Research and Innovation

Project information

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

Document information

Associated WP	WP2
Associated task(s)	Task T2.2
Main Author(s)	Vincent Lefebvre (TSS)
Author(s)	Merlijn Sebrechts (imec), Jorge Pose (GRAD), Julio Suárez (GRAD), J. J , Francesco Paolucci (CNIT), Rana Abu Bakar (CNIT), Abdul Khan (CNIT), Joaquín Escudero (GRAD), Péter Vörös (ELTE), Mohammed B. M. Kamel (ELTE), Maria Safianowska (ISRD), Antonios Lalas, Sarantis Kalafatidis, Konstantinos Giapantzis, Alexandros Papadopoulos, Aristeidis Papadopoulos, Giorgos Agrafiotis, Nikos Makris, Virgilios Passas, Donatos Stavropoulos, Thanasis Korakis, Anastasios Drosou (CERTH), Eryk Schiller (HESSO), Nasim Nezhadsistani (UZH), Mays AL-Naday (UESSEX), Sumeyya Birtane (UESSEX), Vinh La (MONT), Edgardo Montes de Oca (MONT), Manh Nguyen (MONT), Mark Agoustures (TSS), Wissem Soussi, Gokcan Cantali, Gürkan Gür (ZHAW)
Reviewers	Mays AL-Naday (UESSEX), Gürkan Gür (ZHAW)
Type	R — Document, report
Dissemination level	PU — Public
Due date	M10 (31/10/2024)
Submission date	31/10/2024

Document version history

Version	Date	Changes	Contributor (s)
v0.1	23/04/2024	Draft initial document for ToC validation	Vincent Lefebvre (TSS), Mark Angoustures (TSS), Maria Safianowska (ISRD), Francesco Paolucci (CNIT), Antonios Lalas (CERTH)
v0.2	23/09/2024	Draft document with initial content (upper chapters) and use case description	Vincent Lefebvre (TSS), Maria Safianowska (ISRD), Antonios Lalas (CERTH) and CERTH Team, All use case owners
v0.3	02/10/2024	Integration of all use cases	Vincent Lefebvre (TSS), Mark Angoustures (TSS), Maria Safianowska (ISRD), Antonios Lalas (CERTH) and CERTH Team, All use case owners
v0.4	07/10/2024	Reviewers-ready edition. (Fully integrated and completed)	Vincent Lefebvre (TSS), Mark Angoustures (TSS), Maria Safianowska (ISRD), Antonios Lalas (CERTH), Eryk Schiller (HES-SO)
v0.5	27/10/2024	Pre-final version	Vincent Lefebvre (TSS), Marc Angoustures (TSS), Maria Safianowska (ISRD), Antonios Lalas (CERTH)
v0.6	30/10/2024	Final review and refinements	Vincent Lefebvre (TSS), Antonios Lalas (CERTH)
v1.0	31/10/2024	Final version for submission	Antonios Lalas (CERTH)

Disclaimer

Copyright message

Table of contents

List of acronyms and abbreviations 7
List of figures 10
List of tables 12
Executive summary 14
1. Introduction 15
1.1. Purpose and structure of the document 15
1.2. Intended Audience 16
1.3. Interrelations 16
2. Emblematic 6G use cases by Standard Developing Organization (SDOs) and industry associations. 17
2.1. General 17
2.2. 6G use cases by Standardization Organizations 17
2.3. 6G associations 24
2.4. Conclusions 30
3. European research and undertaking projects 31
3.1. 6G Infrastructure Association (6G-IA) 31
3.2. Smart cities use cases review 31
3.3. 6G in agriculture (May 2024) 32
3.4. Smart Networks and Services International Cooperation Environment (SNS ICE) project 33
3.5. HEXA-X (I and II) 34
3.6. Other SNS-JU financed projects. (Stream A and B) 36
3.7. Conclusions 42
4. NATWORK's use case description methodology 43
4.1. Use case description template 43
5. Use case 1. Sustainability and Reliability of 6G Slices and Services 45
5.1. Use case 1.1 Decentralized Management and Orchestration for Intent-compliant end-to-end Service Resiliency and Continuity 45

5.2. Use case 1.2 SECaaS security 54
5.3. Use case 1.3 Green-based payload placement 62
6. Use case 2. Anti-Jamming Technologies for AVS 72
6.1. Use case 2.1 Enabling Multi-antenna for resilience 72
6.2. Use case 2.2 Empowering AI-based jamming detection and mitigation for multi path routing 84
6.3. Use case 2.3 Adaptive modulation techniques for anti-jamming autonomous recovery 90
6.4. Use case 2.4 Improving 6G security in 6G spectrum 94
7. Use case 3. IoT security 101
7.1. Use case 3.1 Anomaly detection using ML 101
7.2. Use case 3.2 AI driven penetration testing 112
7.3. Use case 3.3 Decentralized security and trust management 120
8. Use case 4. Improving Variability of Network with Continuous Security 128
8.1. Use case 4.1 Security Aware placement allocation and monitoring 128
8.2. Use case 4.2 AI aware network slicing for efficient resource utilization and monitoring 135
8.3. Use case 4.3 Software defined radio for agile payload communication 143
8.4. Use case 4.4 AI driven orchestration of micro services 151
8.5. Use case 4.5 Enabling optimized explainable MTD 166
8.6. UC 4.6. Software control flow monitoring for early DoS 176
9. NATWORK use cases KPIs 181
9.1. KPIs aggregating table 181
9.2. Completeness and orientation of NATWORK's used KPIs 183
9.3. Novel forms of KPI 184
10. Conclusions 185
References 186
Appendix 1- Milestone 2 Expert Survey Suggested Content 190

List of acronyms and abbreviations

Abbreviation	Description
3GPP	3G Partnership Project
AD	Anomaly Detection
AI	Artificial Intelligence
AI-DoS	AI optimized DoS attack agent
AI/ML	Artificial Intelligence / Machine Learning
AIAAS	AI as a Service
AIAC	AI And Communication
API	Application Programming Interface
AV	Autonomous Vehicle
BER	Bit Error Rate
BJM	Blind Jamming Mitigation
BPSK	Binary Phase- Shift Keying
CIA	Confidentiality Integrity and Availability
CNF	Containerized Network Function
CNN model	Convolutional Neural Network
CRC32	Cyclic Redundancy Check over 32 bytes sequences
CSI	Channel State information
CSI	Channel State Information
CSP	Communication Service Providers
CTI	Cyber Threat Intelligence
D-MUTRA	DLT-backed MUtual Remote Attestation
dB	Decibel
DDoS	Distributed Denial of Service
DEFM	Decision eXplainablity for MTD
DFE	Decentralized Feature Extraction
DLT	Distributed Ledger Technology (aka blockchain)
DoS	Denial of Service
DoSt	Denial of Sustainability
DPSF	Data Plane Security Function
DQN	Deep-network
DT	Digital Twin
DL/UL	Downlink/Uplink
E2E	End to end
eMBB	Enhanced Mobile Broadband
FN	False Negative
FP	False Positive
FWA	Fixed Wireless Access
gNB	Generalized Node B
gNodeB	Generalized Node B
GNSS	Global Navigation Satellite System
GPU	Graphic Processing Unit
HTC	Holographic Type Communications
ION	Intelligent Operation Network
IoT	Internet of Things
ISAC	Integrated Sensing And Communication

ISD	Intrusion Detection System
ITS	Intelligent Transportation System
JCAS	Joint communication and sensing
JrRx	Jamming-resistant Receiver
K8s	Kubernetes (i.e., a container based framework)
KDR	Key Disagreement Rate
KPI	Key Performance Indicator
LGBM	Light Gradient-Boosting Machine
LLM	Large Language Model
LLM	Large language Model
LSE	Likelihood of Successful Exploit
LSTM	Long Short-Term Memory
LSTM model	Long Short-Term Memory
LTE	Long Term Evolution
MAB	Multi Armed Bandit
MAC	Medium Access Control
MGEC	MTD Green Energy Consumption
MIMO	Multiple Input Multiple Output
MIMS	Minimal Interoperability Mechanisms
ML/DL	Machine Learning / Deep Learning
MMT	MONT's network Monitoring (i.e., commercial name)
mMTC	Massive Machine Type Communication
MTD	Moving Target Defense
MTID	Mean Time to Implement Action
MTTD	Mean Time to Detect
NCC	Network and Computing Convergence
NIC	Network Interface Component
NTRIP	Networked Transport RTCM (Radio Technical Commission for Navigation) via Internet Protocol
O-RAN	Open Radio Access Network
ONOS	Open Network Operating System
P4	Programming Protocol-Independent Packet Processors (P4)
PDR	Packet Delivery Ratio
PHY	Physical
PKG	Physical Layer Key Generation
PKG approach	Physical layer Key generation approach
PLR	Packet Loss Ratio
PRB	Physical Resource Block
PSD	Power Spectral Density
PSD	Power Spectral Density
Q-Learning	A reinforcement learning
QAM	Quadrature Amplitude Modulation
QoE	Quality of Experience
QoS	Quality of Service
QoS	Quality of Service
QPSK	Quadrature Amplitude Modulation
RAF	A deep Learning Compiler
RAM	Random Access Memory
RAN	Radio Access Network

RF	Radio Frequency
RIS	Reconfigurable Intelligent Surface
RTT	Round Trip Time
RU	Radio Unit
SCTP protocol	Stream Control Transmission Protocol
SDN	Software Defined Network
SECaaS	Security as a Service
SNR	Signal to Noise Ratio
SNS	Smart Networks and Services
SoA	State of the Art
SotA	State of the Art
SSD	Solid State Disk
SVM	Support Vector Machine
TCP	Traffic Control Protocol
TCP	Transport Control Protocol
TET	Trust Establishment Time
TIRO	Tactile Internet for Remote Operations
TN/NTN	Terrestrial Network / Non Terrestrial Network
TPM	Trusted Processing Module
UC	Use Case
UDP	User Datagram Protocol
UE	User Equipment
UE	User Equipment
UPF	User Plane Function
uRLLC	Ultra Reliable Low Latency Communication
USRPs	Universal Software Radio Peripherals
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicule to anything
VANET	Vehicle Ad-hoc Network
VM	Virtual Machine
VNF	Virtual Network Function
VPN	Virtual Private Network
VR	Virtual Reality
WAI	Wirespeed AI
WASM	Web Assembly (an interpreted language technology derived from JavaScript)
WIFI	Wireless
WMSD	Worse Case MTD service disruption
x86	Intel processor architecture
XAI	Explainable AI

List of figures

Figure 1 ITU partial use case classes requirement/degree/magnitude over five requirement classes 19
Figure 2. IMT-2030 enhanced and new capabalities for 6G 22
Figure 4 IMT's vision of novel usages brought by 6G (from 5G) 23
Figure 5. HEXA-X 6 use case families 34
Figure 6. DoSt Demonstration Diagram with FORK 46
Figure 7. CTI Solution Diagram 47
Figure 8. Use-Case UML Diagram for DoSt Attack Scenario in UC1 .1 47
Figure 9. UC1 .1 position on NATWORK's Conceptual Graph 48
Figure 10. Sequence diagram for UC 1.1 50
Figure 11. Network Convergence Lab (NCL) of UEssex 51
Figure 12.UC 1.2 SECaaS security mutual remote attestation UML 56
Figure 13. UC 1.2 position over the NATWORK's conceptual graph 58
Figure 14. UC 1.2 SECaaS security sequence diagram 60
Figure 15. UC 1.3 Green based placement presentation 62
Figure 16. UC 1.3 Modified Kubernetes layout 63
Figure 17. UC 1.3 position on NATWORK's conceptual graph 65
Figure 18 UC 1.3 CloudNativeLab main panel 66
Figure 19. CloudNativeLab architecture 66
Figure 20. UC 1.3 CloudEdgeLab architecture 67
Figure 21. UC 1.3 Initial discovery and attestation sequence diagram 68
Figure 22. UC 1.3 Trusted payload deployment sequence diagram 69
Figure 23. Use case 2.1 position on NATWORK's conceptual graph 76
Figure 24. UC 2.1 CERTH Experimental Testbed Architecture 78
Figure 25. Abstract UML diagram for UC2 .1 workflow 79
Figure 26. CERTH lab with experimental testbed 79
Figure 27: Sequence Diagram of UC2 .1 80

Figure 28: Main Activities of UC 2.1 81
Figure 29. UC 2.2 UML diagram 86
Figure 30. Use case 2.2 position on NATWORK's conceptual graph 87
Figure 31. UC2 .2 sequence diagram 88
Figure 32. UC2 .3 UML diagram 91
Figure 33. UC2 .3 position in NATWORK's conceptual graph 92
Figure 34. UC 2.3 Sequence diagram 93
Figure 35 UC 3.1 UML diagram 103
Figure 36. Use case 3.1 position on NATWORK's conceptual graph 105
Figure 37. UC 3.1 Sequence diagram 109
Figure 38. UC3 .1 Timeline (road map) 110
Figure 39. Use case 3.2 position on NATWORK's conceptual graph 113
Figure 40. UC 3.2 UML diagram 115
Figure 41. Use case 3.2 AI-DoS evaluation graph 118
Figure 42. UC #3.3 UML graph 122
Figure 43. UC 3.3 position in NATWORK's conceptual graph 123
Figure 44. UC3.3 Sequence diagram 125
Figure 45. UC 4.1 ML diagram. 129
Figure 46. Use case 4.1 osition on NATWORK's conceptual graph 131
Figure 47 UC 4.1 workflow 134
Figure 48. UC 4.2 UML Diagram 137
Figure 49. UC 4.2 position on NATWORK's conceptual graph 139
Figure 50. UC 4.2 workflow 141
Figure 51. UC 4.3 position in NATWORK's conceptual graph 146
Figure 52. UC4.3 UML diagram, (Adversary atacks of UC 2.1 upper part and UC 4.4 lower part) 147
Figure 53. UC 4.3 general sequence diagram 148
Figure 54.UC4.4 Sequence diagram 154
Figure 55. UC4.4 position in NATWORK's conceptual graph 155

Figure 56. UC 4.4 Sequence diagram 162
Figure 57. UC 4.5 UML Diagram for Possible Scenarios 168
Figure 58. UC 4.5 position on NATWORK's conceptual graph 171
Figure 59. UC 4.5 Testbed and Federation of the deep-RL Optimization for the MTD Framework 173
Figure 60. UC 4.5 Sequence Diagram with the Proposed MTD Strategy 174
Figure 61. UC 4.5 Gantt Chart for the Estimated Timeline 175
Figure 62. UC 4.6 Simple use case graph. 176
Figure 63. UC 4.6 position in NATWORK's conceptual graph 177
Figure 64. UC 4.6 Sequence diagram 179

List of tables

Table 1.ITU-T Focus Group network 2030 Use Cases and Network Requirements 18
Table 2. ITU-T Focus Group network 2030 Use Cases and Network Requirements 20
Table 3. NG Alliance use cases classes 25
Table 4. NGMN Use case functional description 27
Table 5. NATWORK's KPIs mapping with SNS project most-used KPIs 33
Table 6. HEXA-X six use case categories with their KPIs 35
Table 7. SNS financed projects Collaborative Robots use cases 37
Table 8.SNS financed projects Collaborative Robots use cases 37
Table 9. SNS financed projects Physical Awareness use cases 37
Table 10. Table 8 SNS financed projects Fully Connected World use cases 38
Table 11.SNS financed projects Trusted Environment use cases 38
Table 12.SNS financed projects Digital Twins use cases 39
Table 13. SNS project inclinations on Security, Performance and Sustainability 39
Table 14. Use case description template 43

Table 15. Relevance of UC1 .1 with NATWORK tasks 48
Table 16. KPIs for UC1 .1 49
Table 17. SECaaS security use case Functional requirements 55
Table 18. UC 1.3 relevance with NATWORK's tasks 64
Table 19. UC 1.3 used KPIs 65
Table 20. Main PHY properties of IEEE.802.11p 73
Table 21. Accuracy in jamming detection of the existing works 74
Table 22. UC 2.1 Relevance with NATWORK tasks 76
Table 23. UC 2.1 KPIs and target values 77
Table 24. UC 2.2 Requirements and challenges 85
Table 25. UC 2.3 Functional requirements 91
Table 26. UC2 .4 Functional requirement 94
Table 27. UC 2.4 Sequence diagram 95
Table 28. UC 2.4 position in NATWORK's conceptual graph 97
Table 29. UC 2.4 Sequence diagram 99
Table 30. . UC3 .3 Functional requirements 120
Table 31. UC 4.2 Functional requirement 136
Table 33. UC 4.3 relevance with NATWORK tasks 144
Table 34. Description of the use case testbed requirements 146
Table 35. UC 4.4 Functional requirements 155
Table 36. UC 4.5 Functional requirements 168
Table 37. KPIs used in UC 4.5 171
Table 38. Enumeration of NATWORK's use cases KPIs 181
Table 39. NATWORK's KPIs mapping with SNS project most-used KPIs 183

Executive summary

The deliverable D2.2 “6G Use Case Scenarios and Requirements” is aimed at providing sufficient technical elements including challenges, associated risks and timeline on 16 NATWORK’s use cases and related requirements, putting emphasis on their KPIs.

To set NATWORK in its technical context, we start with an analysis of the emblematic use cases delivered by diverse standardization institutions, industry associations and on-going SNS collaborative projects.

A specific and common use case description template is used for the 16 use cases. NATWORK quantity of use cases (i.e., 16) leads to an extended report. The document puts emphasis on NATWORK’s performance-sustainability and security-sustainability reconciliation concept and how the different use cases reflect and exemplify techniques in that direction.

The document also distinguishes novel KPIs from the initial KPIs, defined with a more accurate grasp by the contributors, 10 months after the project start.

The document concludes with the prevalence of the KPIs used by the use cases, their good coverage of most frequently used 6G KPIs and suggests an evolution to future 6G KPIs dealing in two directions concurrently (i.e., performance and sustainability).

1. Introduction

NATWORK is aligned with 6G emphasis on sustainability key values. Inspired by bio-mechanisms, NATWORK aims to regulate performance and security at sustainable resource consumption as do natural entities and immune systems. When projected to telecom networks, these bio-inspired mechanisms can be set as means to reconcile security and sustainability, security and performance, performance and sustainability. NATWORK use cases shall exemplify how these objectives can be met. Another research axis of NATWORK is to employ continuous machine learning to self-construct the ad hoc defenses when new threats occur. These principles can be applied to all layers (e.g., cloud, RAN, core, edge) which create a large exemplification range.

1.1. Purpose and structure of the document

NATWORK accounts numerous 16 use cases spread over the different layers and exemplifying the reconciliation or self-defense principles as stated above. A common high-level methodology shall be set for the description of the several categories of technical implementations, risks, timeline and verification KPIs. The methodology also reflects how each use case solves the reconciliation or self-defense concepts, using a graphical representation. The objective of the presentation is also to show the correct representativity of the different use cases over the four main reconciliation and self-defense areas.

Before these detailed and numerous use case descriptions, the document recalls the vision on 6G by the standardization and industry entities. It also looks at SNS engaged projects use cases to measure the respective weights and the intertwining of performance, security and sustainability key values looking at their most used KPIs. This work is aimed at providing the research context into which NATWORK takes place. A mapping of NATWORK's KPI and SNS project most used KPIs is produced in that sake, reflecting the specific angle on sustainability brought by NATWORK.

Last, the document aggregates all KPIs considered by the use cases and identify the ones derived from the proposal and those which have been defined by partners contributing to this document, resulting from a more accurate view of the use case associated technical work and challenges.

The remainder of this document is structured as follows:

- **Section 2** covers the emblematic use cases delivered by standardization organizations and industry associations,
- **Sections 3** covers the European SNS undertaking projects,

- **Section 4** covers the use case description methodology,
- **Section 5, 6, 7 and 8** cover the descriptions of use cases 1,2,3 and 4 broken down with sub use case descriptions, starting with use case UC 1.1 to UC4.6,
- **Section 9** covers NATWORK use case used KPIs,
- **Section 10** concludes this document, while the content of the document is discussed, reflecting on NATWORK's strategic direction and the related results of the project.

1.2. Intended Audience

The NATWORK Project's "6G Use Case Scenarios and Requirements" is devised for public use in the context of preparatory 6G Use Case Scenarios and Requirements of the NATWORK consortium, comprising members, project partners, and affiliated stakeholders. This document mainly focuses on the 6G Use Case Scenarios, KPIs, and anticipated requirements of the project, thereby serving as a referential tool throughout the project's lifespan.

1.3. Interrelations

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

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

The detailed use case analysis covered in this document is the solid initial referential for WP6 (i.e., dealing with integration and demonstration) as well as the technical WPs 3-5, which develop the technical solutions which are implied in the use cases.

2. Emblematic 6G use cases by Standard Developing Organization (SDOs) and industry associations.

2.1. General

In this section, we enumerate the 6G use cases as defined by 6G SDOs, associations-forums, and past or on-going SNS research projects. The objective is to grasp the core challenges at play to achieve the promises expected to materialize in the frame of 6G era. The chapter intends to position NATWORK's own objectives in response to the assessed requirements to meet these emblematic use cases and to better assess its novelty.

2.2. 6G use cases by Standardization Organizations

2.2.1. International Telecommunication Union (ITU)

2.2.1.1. General

ITU is a specialized agency of the United Nations, coordinating global telecommunications policies and standards. It is driven by three active groups as ITU-R dealing with the radio spectrum management and satellite orbit resources, ITU-T dealing with telecommunication standardization and normalization and ITU-D fostering global access and plan covering broader access in developing countries.

2.2.1.2. ITU-T's perspective

ITU-T itself is supporting several Focus Groups working on a large variety of topics (e.g., IA for autonomous driving, metaverse, AI for health sector, costs models for affordable services, leverage of DLT in the telecom sector). Its Focus Group on Network 2030 initiated as soon as 2018 has delivered its vision of anticipated 6G use cases at the 2030 horizon and with their impacts on the evolution and refinement of networks in that direction. The public documents relate specifically to the anticipated use cases as [1], dating from 2020, not renewed since then. A key interest of this work is the identification of the main network refinements required for the 12 different use case classes as shown below.

Table 1.ITU-T Focus Group network 2030 Use Cases and Network Requirements

Use case	Description	Requirements
Holographic Type Communications (HTC)	Transmission of 3D images through the network.	**Bandwidth**: Capacity, capacity; QoE; QoS; flexibility; and adaptable transport **Time**: Latency; synchronization; jitter; accuracy; scheduling; coordination; and geolocation accuracy **Security:** privacy; reliability; trustworthiness; resilience; traceability; and lawful intercept **AI**: Data computation; storage; modelling; collection and analytics; autonomy; and programmability ***ManyNets*:** Addressing mobility; network interface; and heterogeneous network convergence
Tactile Internet for Remote Operations (TIRO)	Real time control of remote control in fields such as Industry 4.0 or telemedicine incorporating haptic feedback in addition to vision and audio.	
Intelligent Operation Network (ION)	Use of AI to detect network impairments, pinpoint root causes of alarms and execute automatic recovery procedures	
Network and computing convergence (NCC)	Use of computing resources inside the network itself in addition to the cloud and use of computing aware orchestration capabilities, with fast routing and rerouting of traffic flows and computing tasks to the appropriate site, depending on the current conditions	
Digital Twins (DT)	Digital emulation of physical entities for improving situational awareness and a better response. Wide digital twins are considered to emulate city services.	
Space Terrestrial Integrated Networks	Integration and continuity of terrestrial and LEO satellites	
Industrial IoT with cloudification	Automatic operation and control of industrial processes to minimize human intervention	
Huge Scientific Data Applications	Support of large-scale scientific applications such as astronomical telescopes and particle accelerators	
Application-aware Data Burst Forwarding	From packet-based forwarding to burst forwarding for network efficiency enhancement.	
Emergency and disaster rescue	Improved disaster management by employing sensor, local intelligence and field communication required Intelligence to react and coordinate the evacuation of casualties.	
Socialized Internet of Things	Collaboration of IoT devices from different platforms or providers to achieve a certain task (e.g., logistics delivery) by means of establishing social relationships between them	

Use case	Description	Requirements
Connectivity and sharing of pervasively distributed AI data, models and knowledge	intelligent IoT devices taking an active role in AI processing, not just as collectors of raw data	

For simplicity, the table shows the same set of five classes of requirements analyzed for each use case (i.e., bandwidth, time synchronization, security, AI and *ManyNets).* The different use case classes engender different magnitudes over the five classes of requirements as shown in this graph considering a restricted set made of the 7 first use cases of the table. It is worth mentioning that the different classes of use cases are of very different types, being domain-specific (e.g., disaster management) or network technology driven (e.g., network and computing convergence).

Network Computing Convergence (NCC) is aligned with NATWORK's vision, fostering computing migration over the network computing continuum to reach higher sustainability to satisfy a service KPIs.

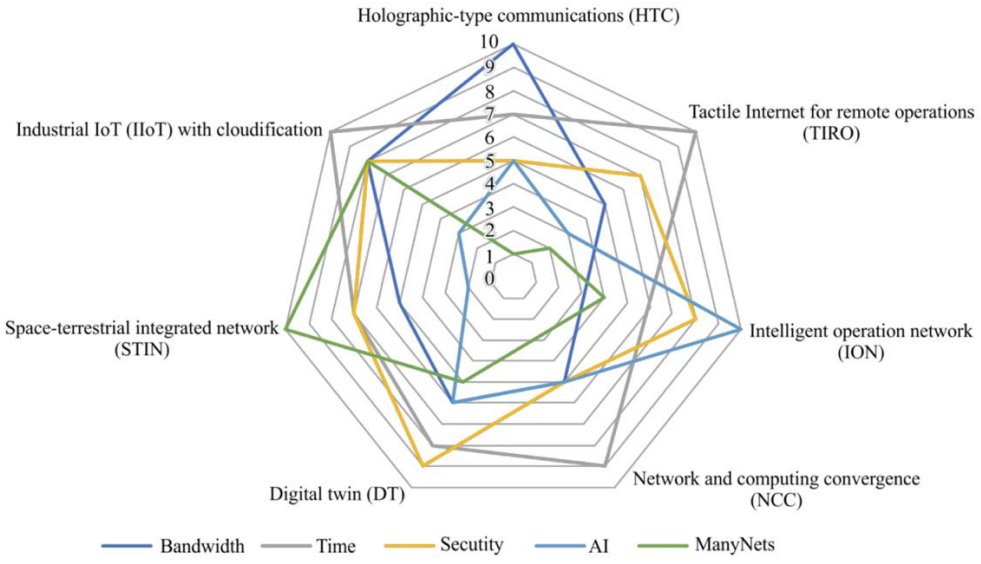


Figure 1 ITU partial use case classes requirement/degree/magnitude over five requirement classes

On the five core requirements, **NATWORK's concept and showcased use cases (as detailed in this document target the five requirements** Bandwidth (e.g., antenna optimized resilience), Time (e.g., data flow extraction telemetry for real time network adaptation), Security (e.g., attestation, MTD), AI (malware and anomaly detection, optimized payload placement) and Network and computing convergence (e.g., microservice based network functions).

2.2.1.3. ITU-R's 6G perspective

From the ITU-R has been pivotal for defining the framework for development and deployment of International Mobile Telecommunications (IMT) systems, striving for interoperability, compatibility, efficient spectrum utilization across geographical regions and regulatory frameworks. The IMT framework has evolved with labels as IMT-2000, IMT-advanced, IMT-2020 (i.e., dealing with 5G) and IMT-2030 (i.e., dealing with 6G) [2].

In[2] document, ITU has produced key high-level requirements for 6G as listed in Appendix. This table of requirements enumerates key radio-based KPIs detailed with quantified values.

Table 2. ITU-T Focus Group network 2030 Use Cases and Network Requirements

Specification/ KPI	Range
Peak Data Rate (i.e., Maximum achievable data rate under ideal conditions per device.)	Values of 50, 100, 200 Gbit/s are given as possible examples applicable for specific scenarios, while other values may also be considered.
User experience Data Rate. (i.e., Achievable data rate that is available ubiquitously7 across the coverage area to a mobile device.)	Values of 300 Mbit/s and 500 Mbit/s are given as possible examples, while other values greater than these examples may also be explored and considered accordingly.
Area Traffic capacity (i.e., al traffic throughput served per geographic area.)	The research target of area traffic capacity would be greater than that of IMT-202010. Values of 30 Mbit/s/m2 and 50 Mbit/s/m2 are given as possible examples, while other values greater than these examples may also be explored and considered accordingly.
Spectrum efficiency (I.e., average data throughput per unit of spectrum resource and per cell.)	The research target of connection density could be 106 – 108 devices/km2.
Connection density (i.e., Total number of connected and/or accessible devices per unit area.)	Values of 30 Mbit/s/m2 and 50 Mbit/s/m2 are given as possible examples, while other values greater than these examples may also be explored and considered accordingly
Mobility (i.e., Maximum speed, at which a defined QoS and seamless transfer between radio nodes which may belong to different layers and/or radio access technologies (multi-layer/multi-RAT) can be achieved.)	The research target for mobility could be 500 – 1 000 km/h.
Latency (i.e., latency over the air interface refers to the contribution by the radio network to the time from when the source sends a packet of a certain size to when the destination receives it.)	The research target of latency (over the air interface) could be 0.1 – 1 msec
Reliability (i.e., Reliability over the air interface relates to the capability of transmitting successfully a predefined amount of	The research target of reliability (over the air interface) could range from 1-10−5 to 1-10−7.

Specification/ KPI	Range
data within a predetermined time duration with a given probability.)	
Coverage (i.e., Coverage refers to the ability to provide access to communication services for users in a desired service area. In the context of this capability, coverage is defined as the cell edge distance of a single cell through link budget analysis.	No reference value is given
Positioning (i.e., positioning is the ability to calculate the approximate position of connected devices. Positioning accuracy is defined as the difference between the calculated horizontal/vertical position and the actual horizontal/vertical position of a device.)	The research target of the positioning accuracy could be 1 – 10 cm.
Sensing related capabilities (i.e., Sensing-related capabilities refer to the ability to provide functionalities in the radio interface including range/velocity/angle estimation, object detection, localization, imaging, mapping, etc. These capabilities could be measured in terms of accuracy, resolution, detection rate, false alarm rate, etc.)	No reference value is given
Applicable AI/ML-related capabilities (i.e., Applicable AI-related capabilities refer to the ability to provide certain functionalities throughout IMT-2030 to support AI enabled applications. These functionalities include distributed data processing, distributed learning, AI computing, AI model execution and AI model inference, etc.)	No reference value is given
Security and resilience (i.e., In the context of IMT-2030: – – 14) Security refers to preservation of confidentiality, integrity, and availability of information, such as user data and signaling, and protection of networks, devices and systems against cyberattacks such as hacking, distributed denial of service, man in the middle attacks, etc. Resilience refers to capabilities of the networks and systems to continue operating correctly during and after a natural or man-made disturbance, such as the loss of primary source of power, etc.)	No reference value is given
Sustainability (i.e., Sustainability, or more specifically environmental sustainability, refers to the ability of both the network and devices to minimize greenhouse gas emissions and other environmental impacts throughout their life cycle. Important factors include improving energy efficiency, minimizing energy consumption and the use of resources, for example by optimizing equipment longevity, repair, reuse and recycling. Energy efficiency is a quantifiable metric of sustainability. It refers to the quantity of information bits transmitted or received, per unit of energy consumption (in bit/Joule). Energy efficiency is expected to be improved appropriately with the capacity increase in order to minimize overall power consumption.)	No reference value is given

Specification/ KPI	Range
Interoperability (i.e., Interoperability refers to the radio interface being based on member-inclusivity and transparency, so as to enable functionality(ies) between different entities of the system.)	No reference value is given

A graphical view shows the new (i.e., non existing in 5G) and enhanced capabilities to develop for 6G.

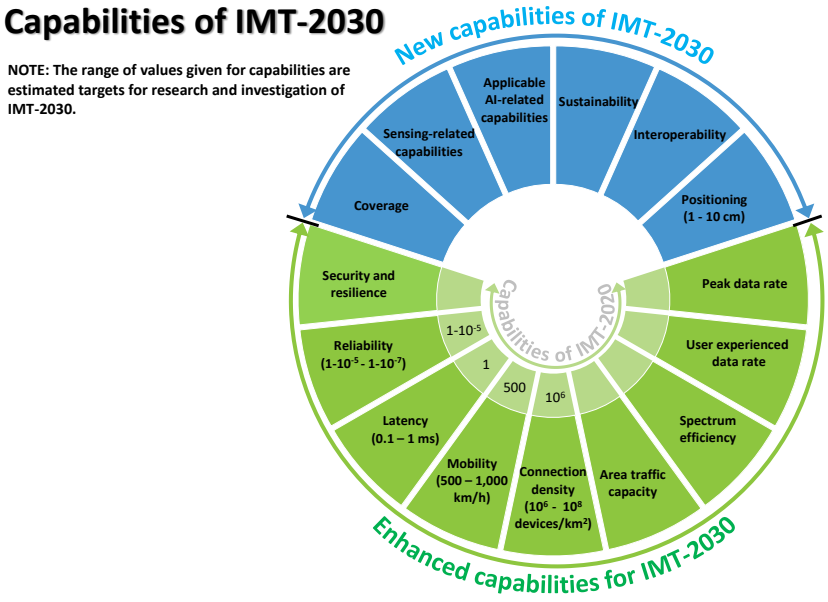


Figure 2. IMT-2030 enhanced and new capabalities for 6G

The objective of the development of IMT-2030 is to address the anticipated needs of users of mobile services in the years 2030 and beyond. This section provides relationships between IMT-2030 and existing IMT, other access systems, timelines and focus areas for further study.

Figure 2 above defines enhanced capabilities (i.e., in green) which go beyond on-going 5G development as set in [3] and the incorporation of new technology components and functionalities and/or new radio interface technology (i.e., in blue). 6G is therefore not only bringing progress on the different criteria of 5G (e.g., latency, peak data rate) but six new core values (i.e., sustainability) and technical features (i.e., positioning).

As one can consider, these enhanced and novel capabilities are covering a wide spectrum of domain-specific research areas difficult to grasp in one single project. NATWORK's concept and use cases map more than half of them (i.e., Security and resilience, reliability, Latency, Mobility, User experience data rate, Interoperability, Sustainability and Applicable AI related capabilities). More interestingly, this graph illustrates that sustainability, defined as a new capability for 2030 horizon is now stated as a must have.

2.2.1.4. Novel usage scenarios brought by IMT-2030 (versus IMT -2020)

As stated in [4], IMT–2020 design was constructed to meet three usage scenarios of enhanced Mobile Broadband (eMBB) enabling immersive communication with peak data rates up to 10 Gpbs, ultra–Reliable Low Latency Communication (uRLLC) with service latency down to 1msec and massive Machine Type Communiation (mMTC) to support 1 million devices per square kilometer. With 6G, these three core communication usages will be extended with higher performance to meet the new use cases of HD video streaming, virtual/augmented/mixed and extended reality, autonomous driving, V2X communications and intra body communication of nano machines to respectively. Moreover, three new usages of Integrated sensing and communication (ISAC), Ubiquitous connectivity and Ai and Communication (AIAC) will emerge.

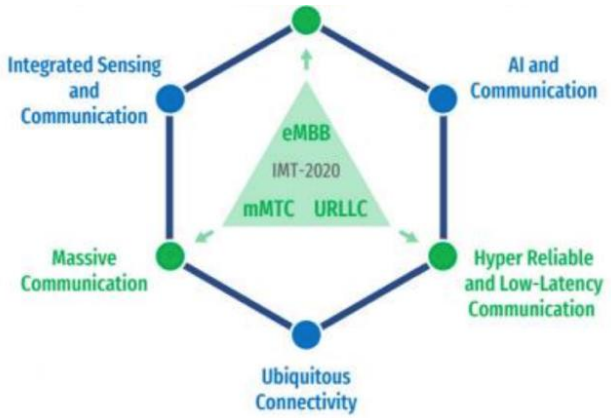


Figure 3 IMT's vision of novel usages brought by 6G (from 5G)

Sensing and Communication convergence derives from the elevation in frequency of the communication bandwidth, enabling novel forms of sensing directly derived from the radio elements (e.g., position, gesture, imaging and mapping). The malaxation of the AI and communication relates to the native leverage of AI for hyper dynamic, hyper complex fragmented resource management required to meet 6G services. Ubiquitous connectivity derives from the societal consideration to bridge the digital divide (e.g., geographical area, rural areas).

2.2.2. European Telecommunications Standards Institute (ETSI)

ETSI has a technology focused, bottom-up approach with strong technology-centered working groups (e.g., Integrated Sensing and Communications, THz communications, AI security) for specifications or for recommendations, elaborating the future in their respective domain. No working group generates a high-level definition of 6G use cases, in a perspective point of view.

2.2.3. 3G Partnership Project (3GPP)

Created in 1998 with the scope of harmonizing and conciliating 7 regional standardization agencies including ETSI working in the field of 3rd Generation of mobile communications,) 3GPP still holds today with novel missions spanning to 6G specifications. The organization is structured with domain specific specification working groups as RAN, Services and Systems, Core networks and terminals. The organization has not yet produced a use case and requirement document.

3GPP Stage-1 Workshop on IMT2030 Use Cases (May 08, 2024)

ITU-R (for Radio) defines the standards for 6G and has organized the International Mobile Telecommunication 2030 May 2024. Use cases have been developed by the many invited organization (e.g., SNS ICE, 5GAA automative association, 5GAIA Alliance for Connected Industry and Automation, B5GPC from Japan, Bharat6G from India). The vertical associations presentations put emphasis on their specific expectations, challenges notably in terms of market preparedness for 6G while 5G is not yet installed. SNS ICE ‘s vision has a broader cross-vertical vision, which is supported with the work accomplished inside HEXA-X flagship projects and other SNS calls. We propose a summary of the 6G use case presentation by SNS ICE below.

2.3. 6G associations

2.3.1. General

Our survey of association use cases includes two international 6G associations (i.e., Next G Alliance, NGMN) gathering major industry and academic stakeholders. Altogether, they form a consistent and comprehensive study material. With significant infrastructure market shares, we had added the Chinese, South Korean and Japanese national association, gathered in Asian supplier National Associations.

2.3.2. The Next G Alliance (NG Alliance)

NG Alliance is an initiative to stimulate a North American wireless technology leadership in 6G and beyond. It gathers all major industry and research institutions and governmental agencies from the US and Canada. It positions itself as embracing the full lifecycle from research, development, manufacturing, standardization and market readiness. Noticeably, IMEC, a NATWORK's partner sits in this organization as a contributing partner. NG Alliance is linked with Europe's 6G Industry Association (6G-IA) with a partnership agreement. The association is extremely productive with 20 detailed white papers focused on different research, societal or network operational topics (e.g., spectrum need, wide area cloud evolution, trust, security and resilience). From this rich library, a well-crafted and consistent document, edited in 2022 as well [5] discusses 6G applications and use cases and is considered for our analysis below.

NG ALLIANCE stores 16 identified applications and use cases in four 6G enabled categories of **Network-enabled robotics** (i.e., Coordinated Service Robots, **multi-sensory extended reality** (i.e., telepresence, immersive gaming or education), **distributed sensing and communication** (i.e., untethered wearable, public safety applications, synchronous data channels) **and personal user experiences** (i.e., hotel and shopping).

Table 3. NG Alliance use cases classes

Use case class	Use case
Network-Enabled Robotics and Autonomous systems	Online Cooperative Operation among a Group of Service Robots
	Field Robots for Hazardous Environments
Multi-Sensory Extended reality	Ultra-realistic Interactive Sport Drone Racing
	Immersive Gaming/Entertainment
	Mixed Reality Co-Design
	Mixed Reality Telepresence
	Immersive Education
	High-speed wireless connection in aerial vehicle for entertainment
Distributed Sensing and Communications	Remote data collection
	Untethered wearables and implants
	North American Digital Divide
	Public Safety
	Synchronous Data Channels
	Health care
Personalized User Experiences	Hotel experience
	Shopping experience

These 16 use cases or applications are described as potentially reachable, achievable and with statements of the relevant and associated high-level defined technical requirements. The described use cases vary in terms of representativity and societal benefits (i.e., drone racing versus health care) but are given to better illustrate the diversity of needs.

In the same vein as NGMN, the requirements are either defined generically (e.g., uRRLC, mMTC) or with relevant enabling technologies. We have extracted the most specific considered requirements for 6G use cases. They are identical to the ones stressed by MGMN in as being identical to the ones stressed by NGMN (as stated in 2.3.3.1), except for the following list of additional requirements:

- Need for security and privacy to user data
- Interworking and seamless mobility between terrestrial and NTN networks
- Very high communication service availability and DL/UL packet reliability
- Position accuracy and object-sensing accuracy - reaching centimetre levels
- High levels of localization and mapping,
- Extrême Massive Machine-Type Communications (mMTC) support
- Extreme Coverage for users in remote areas

2.3.2.1. NG Alliance's vision on security and trust

The NG Alliance has a strong consideration on security as reflected by their white paper [6], structured with chapters dealing with Security Assurance and Defence (i.e., dealing with Common Criteria's approach for vulnerability-free payloads, data provenance, privacy preserving, zero-trust architectures and the attestation means to validate these security attributes), Confidential Computing (i.e., proprietary code and data confidentiality preservation by several techniques including trusted execution environment), Secure identities and Protocols, Service Availability and Resilience and Post-Quantum cryptography.

2.3.2.2. NG Alliance and sustainability

The NG Alliance has a strong consideration on sustainability as depicted in several white papers including [7], which is a broad impact assessment of 6G, including energy expenses as well as the use of pollutants in its components and water wastes. The energy impact is split over the RAN, the core and cloud-edge domains. Sustainability is not yet considered for the security enablement as considered by NATWORK.

2.3.3. Next Generation Mobile Network Alliance (NGMN)

NGMN is a forum regrouping international mobile operators and industry, with the objective to provide impactful industry guidance to achieve ”innovative*, sustainable and affordable mobile telecommunication services for the end user*” and with a particular focus on “*Mastering the Route to Disaggregation, Green Future Networks and 6G, whilst continuing to support 5G’s full implementatio*n”. Although security is not their prime objective, their energy efficiency, network disaggregation for a more open eco-system and elevated user experience are aligned with NATWORK’s vision.

NGMN has analyzed in [8] 6G use cases in 2022 which is still a legacy and a reference since then. 50 use cases were contributed by the different participants in NGMN, then grouped in 4 different classes, and eventually produced 14 generic use cases. The use case classes and use cases identified by NGMN are shown in the following tables. The classes define the main evolutions to be considered for 6G communication. They are **enhanced Human Communication class** (i.e., XR immersive holographic communication, telepresence, multi modal communication for teleoperation, brain sensing), **enhanced machine communication class** (i.e., cobots, robot network fabric), **enabling service class** (ie 3D Hyper-Accurate Positioning, interactive mapping, digital health care, automatic detection, recognition and inspection, trusted composition of service) and **network evolution class (**Native Trusted AI (AIaaS) for the network orchestration and delivered as a service for 3rd party application layer, coverage expansion, autonomous system for Energy efficiency. NGMN 14 use cases are defined as set in table below.

Table 4. NGMN Use case functional description

Use case	Functional description
Enhanced Mobile Broadband (eMBB)	• High-Speed Internet: Ultra-fast internet access for mobile devices. • 4K/8K Streaming: High-resolution video streaming without buffering.
Enhanced Mobile Broadband (eMBB)	• Smart Cities: Integrated sensors and devices for urban management. • Environmental Monitoring: Real-time tracking of air and water quality.
Ultra-Reliable Low Latency Communications (URLLC)	• Autonomous Vehicles: Communication systems for self-driving cars. • Remote Surgery: Medical procedures performed by surgeons remotely
Fixed Wireless Access (FWA)	• Rural Broadband: High-speed internet access for remote areas. • Home Broadband: An alternative to traditional wired internet.
Industrial Automation	• Smart Manufacturing: Automated production lines with real-time monitoring. • Predictive Maintenance: Using data analytics to predict equipment failures.
Smart Grids	• Energy Management: Optimizing the distribution and consumption of electricity. • Demand Response: Adjusting power usage based on supply conditions.
Augmented Reality (AR) and Virtual Reality (VR)	• Immersive Gaming: Enhanced gaming experiences with AR/VR. • Virtual Meetings: Realistic virtual environments for remote collaboration

Use case	Functional description
Public Safety	• Emergency Services: Improved communication for first responders. • Disaster Management: Coordinated response efforts in emergencies.
Connected Health	• Telemedicine: Remote consultations and health monitoring. • Wearable Devices: Continuous health tracking through smart wearables.
Smart Homes	• Home Automation: Control of home appliances and security systems remotely. • Energy Efficiency: Optimizing energy use within the home.
Retail and Logistics	• Smart Retail: Enhanced shopping experiences with personalized services. • Supply Chain Management: Real-time tracking and management of goods.
Agriculture	• Precision Farming: Using data for efficient farming practices. • Livestock Monitoring: Tracking the health and location of livestock.
Entertainment and Media	• Live Event Streaming: Broadcasting live events in high definition. • Interactive Content: Enhanced user engagement with interactive media.
Transportation and Mobility	• Smart Traffic Management: Real-time traffic monitoring and control. • Connected Public Transport: Integration of public transport systems for efficiency.

The use cases are described with their novel functional communication services, with sets of few most required technical fulfilled needs and technologies instrumental for these envisioned use cases.

2.3.3.1. Identified core 6G requirements

We have picked up the following most stringent needs to cover the 14 use cases:

- Ultra-low latency communications uRRLC (defined without specific latency requirement).
- Extrême Massive Machine-Type Communications (mMTC) support.
- Enhanced Mobile Broadband (eMBB) for users in remote areas or disaster areas.
- Very high level of clock synchronization accuracy (precision depends on the use cases).
- Motion to Photon below 20 msec.
- Transmission of high-definition pictures or films, with a data rate of up to 4Gbps, both from urban and rural areas.
- AI-assisted decision-making
- Support for edge computing

2.3.3.2. NGMN's vision on trust

The forum has published a document on service trustworthiness in late 2023 [9].

The document enumerates the benefits of security aspects (e.g., integrity, privacy, confidentiality, reliability and service continuity) in all the considered use cases, pinpointing the main security needs. Their security requirements analysis is high-level, deriving from network

operators and users' perspectives with their focus essentially put on trust to services and data privacy. Their design consideration for 6G trustworthiness part integrates the novel concepts of decentralized trust, dynamic trust, security as a service and intelligent collaboration for optimized security services activation. The two latter points stress the need for an optimized efficiency of security enforcers activation only when required and through a cross-domain traversal optimization, **is aligned with NATWORK's vision.**

2.3.3.3. NGMN's vision on sustainability

The forum has published a document on sustainability and KPIs in [7]. This document does not explicit NATWORK's sustainable security need, which can however be considered as an implicit requirement.

2.3.4. Asian industry national associations (China, Taiwan, Korea and Japan)

We propose a rapid tour of the Asian industry associations through their last public documents.

People's Republic of China (i.e., PRC) IMT-2030 promotion group aims at forging a superior industrial leadership on 6G. The association defines the core technologies to be developed with the support of the Chinese research funds. Its white paper [10]depicts five core research directions of extended mobile broadband (eMB), massive Machine-Type Connection, ultra reliable Low Latency Communication (uRLLC), Quality Guaranteed Network Artificial Intelligence and Integrated Sensing and communication.

Taiwan Association of Information and Communication Standards white paper [11]sets up the core characteristics of 6G communications with typical values (e.g., Ultra high speed and large capacity transmission, ultra large coverage and multi dimension space, ultra precision positioning). From this initial analysis, the paper states the industrial strengths of Republic of China (i.e., ROC) in the directions of Massive MIMO, RIS antenna, JCAS/ISAC, O-RAN, Photonic network). Noticeably, security and energy-saving are two common drivers to all advanced technologies ROC is capable of. Moreover, ROC's ITRI research ministry is tightening its relationship with EU's SNS JU (i.e., 6G IA) with shared agenda and financing projects including consortium partners from both sides.

India's Telecommunications Standards Development Society or India (TSDSI), in addition to defining 6G use cases required capabilities (e.g., low latency, high bit rate, ….) as can be defined elsewhere, puts a specific emphasis on breaking the urban-rural divide with ubiquitous connectivity brought by non-terrestrial networks.

South Korea plans to take the upfront run in the 6G industry race with a first setup in 2028. Its [12]communication plan unveils the main research directions taken in the field of wireless communication with the development of extreme massive MIMS, mobile core software centric core networks, wired network, 6G integrated services (e.g., VR, urban air mobility), leveraging AI capabilities for distributing and interconnecting resources. Safety and trustworthiness, sustainability are Korean Government first ambition. Substantial investments will be specifically devoted to attaining higher performance with low power input. If the reconciliation between security and performance is not directly stated, the general research directions are aligned with NATWORK concept.

Japan's message to the 2030 white paper [13] is structured on market trends in all major industries (e.g., Agriculture, Automotive, Entertainment, Aerospace, Telecommunications, Finance, Services) to draw the line of future requirements. In other words, use cases should be pulled from industries, not pushed by the telecom infrastructure vendors.

Our tour has not identified a mention to sustainable security or sustainable performance, the key drivers of NATWORK's promises, which does not state that these novel directions are not considered in these countries, notably by members of these associations in their respective technical areas.

2.4. Conclusions

The initial work (I.e., from 2018) by SDOs and associations to qualify emblematic use cases viewed as achievable during the 6G era were all performance driven. In this initial definition work, the values of Security and Sustainability were not positioned at the same level than performance. From this step onward, three major trends had emerged and grown, the emergence of AI, the dynamicity and complexity of network services and network softwarization. In the meantime, the cyber threat landscape has grown considerably. Security is become a must-have, and it shall be powered by AI to tackle with future network complexity and dynamicity. The climate change has also become a major societal objective and 6G shall be sustainable per-se. **NATWORK's vision stands against this new expectation for more secure and more sustainable networks.** The emblematic and futuristic use cases must come with more security, reliability and energy friendliness.

3. European research and undertaking projects

3.1. 6G Infrastructure Association (6G-IA)

6G-IA is the private side of the public private joint partnerships (5G-PPP) and the Smart Networks and Services Joint Undertaking (SNS JU), hence working in close coordination with the European Commission (i.e., the public side). In fact, beyond the private sector, 6G-IA brings together a global industry community of telecoms & digital actors, such as verticals, operators, manufacturers as well as public research institutes and universities and SMEs, with the intent of being the "voice of European Industry and Research for the next networks and services". The 6G-IA carries out a wide range of activities in strategic areas including standardization, frequency spectrum, R&D projects, technology skills, collaboration with key vertical industry sectors, notably for the development of trials, and international cooperation. In its role of setting the strategic research, industry and standardization industry coordination Restricted to the association members, the association has set several types of working groups (i.e., vision, trials, pre-standardization, security, 5G/6G Connected and Automated Mobility, spectrum and WiTaR). The association also manages an inter-project steering board working group opened to SNS projects participants. The association has not published an all-in-one 6G use cases white paper but is productive in publishing vertical-oriented white papers which in fact detail several use cases of the treated domains:

- 6G SNS IA report: Smart city trials in Europe (June 2024)
- 6G SNS IA and AIOTI: Role of 6G in agriculture (May 2024)
- 6G SNS IA: Open networks and services (May 2024)
- 6G SNS IA: Open RAN and future networks development (May 2024)
- 6G SNS IA: Research priorities on microelectronics for 6G networks R&I

The two first white papers describe the requirements, challenges and expectations attributed to 6G in the domains of smart cities and smart farming. We put below our key findings in these documents.

3.2. Smart cities use cases review

The document collects all 5G-PPP phase 1 and 2 projects (i.e., which were driven and positioned on 5G networks) dealing with smart cities in a general perspective. The document explores the different use cases and their implementations, stressing lesson learnt in terms of coordination with city administration entities and extra European funding infrastructure supporting action.

This document “illustrates and points out the main requirements for new technology from cities and civil engineering point of view to enable for example the wellbeing of citizens, development of services and sustainable growth of city”. The document enumerates 14 smart cities' use cases from connected cars to water management, with a consideration to the use case dependence on three 5G-6G promises of URLLC, mMTC and eMBB. As these use cases may also require additional ancillary features and attributes (e.g., security, IoT support, slice isolation), they are notified separately. Of course, these requirements will persist with the transition from 5G to 6G and recalls the main three enablers and drivers of 5 and 6G.

3.3. 6G in agriculture (May 2024)

Agriculture captures 40% of EU budget and is driven with two prime societal goals of sustainability (i.e., self-sufficiency) and eco-friendliness in a global perspective (i.e., animal and human wellness), essentially bearing a reduced usage of pesticides and fertilizers. Global warming exacerbates the need to progress and conciliate both prime goals with shorter timelines to sustain rapid water supply contraction. On the transformation side, time-reduced and more accurate supply chains reduce carbon footprints and chemical needs. In these directions, all key promises of 6G (e.g., network density, boosted uRLLC, mMTT) will enable us to implement tomorrow’s highly demanding usages, in continuity and incremental progress from what 5G can bring today. 6G IA JU is engaging collaborative research, aligned with EU policy directions as Biodiversity Strategy and the Farm2Fork Strategy. Massive sustainable biodegradable IoTs associated with sustainable AI and networks will be the enablers for tomorrow’s agriculture in Europe. Reliable connections constitute a baseline requirement for this farming evolution.

The direct benefits attributed to the transition from 5G and 6G is discussed in [vanHilten22]. Its section 5 details the novel use cases overview (Section 5). Although 5G is understood to be only at its early stage of implementation today, its inherent limitations are noticed. By contrast, 6G enabling aspects are stated in the pilots to address the different challenges, notably stressing the energy efficiency. They are given in the table below.

Technical advances are being achieved, although it is still far from being a mature technology that will reach mass production shortly. **NATWORK’s sustainable performance** is explicitly given (as the three first bullets of this table).

Table 5. NATWORK's KPIs mapping with SNS project most-used KPIs

Area	Challenges relevant to future 6G networks
Communications and computing	▪ Energy-efficient communication networks ▪ Energy-efficient ML and AI integrated in the network ▪ Energy-efficient optimization and orchestration of support services and network virtualization functions ▪ Over-the-air computation (Air Comp) that integrates communications and computing to increase system efficiency
Sensing and communications	▪ Zero-energy devices relying solely on energy harvesting and passive communications ▪ Fulfilling sensing and communications needs with environmentally-friendly, biodegradable electronic components and devices

3.4. Smart Networks and Services International Cooperation Environment (SNS ICE) project

The project will create a collaborative environment for European and global stakeholders involved in the preparation of 6G smart networks and services. It will be the instrument to present, leverage, and position the SNS JU activities and achievements in major European and global fora. The project will work at a global level with other regions, where 6G activities are planned and ongoing. This will create an environment to promote SNS JU results and achievements, and exchange trends and ideas to achieve global consensus. Key standardization activities will be also monitored, and main roadmaps and trends will be communicated back to the SNS JU projects. The project will also establish dialogues at a European level between peer Horizon Europe Partnerships, national initiatives, research and development clusters, etc., targeting the exchange of information, plans and priorities. This will enable a better understanding of the European activities among the stakeholders involved and will potentially enable a better alignment of their plans. Additionally, SNS ICE will also be engaged in dialogues with key vertical industries through well-established associations, to identify their requirements and promote the SNS JU solutions to them. This exchange of ideas will create opportunities for tailor-cut 6G solutions and their early adoption by the vertical industries.

All these activities are expected to contribute significantly to securing Europe's leading role in the definition, provision, and exploitation of 6G solutions.

In[14], SNS ICE International and European Ecosystem use cases, depicting a European vision derived from National bodies (6G Platform Germany, Restart (Italy), Future Network services (NL)

and French Acceleration Strategy for future networks and technologies (F). The European Flagship project HEXA-X-II project and other SNS funded collaborative projects (e.g., 6G shine, 6GNTN, Fidal, Nancy, Season and trialsNet) were associated to draw the following novel use cases, arranged in six classes of Cooperative Mobile Robots, Seamless Immersive Reality, Human-centric Networks, Ubiquitous and Resilient Network, Realtime Digital Twins and Network Assisted 3D mobility. The work is remarkable in a sense that it associates to each use cases the functional requirements as well as quantified KPIs.

In the ITU's roadshow, SNS ICE presentation also integrates a very valuable sustainability study of 6G novel services, weighting the handprints (i.e., benefits) versus the footprints (i.e., costs). **This analysis can drive our work in NATWORK**, exposing also the direct benefits and savings gained against the service costs. SNS ICE study covers pros and cons of the service towards environmental, social and economic domains.

3.5. HEXA-X (I and II)

HEXA-X project is dubbed as the EU- research **flagship project**. Indeed, the project was and is still operated by a larger number of contributors (i.e., 29) from industry and academic research, delivering a deeply visionary and very accurate analysis reports and a major source of inspiration.

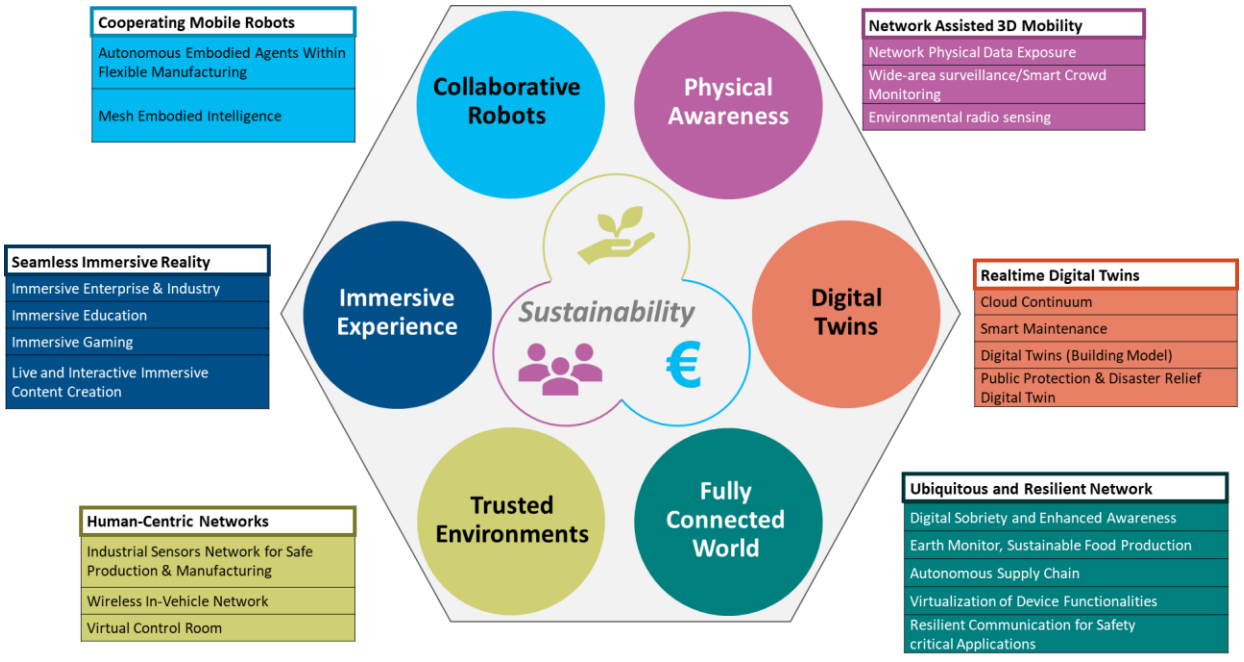


Figure 4. HEXA-X 6 use case families

HEXA-X-II [15] provides a more nurtured and valid classification of the use cases with 6 families as compared to version I. Typically, between I and II, the former use cases family aka “Enable Sustainability” has been removed and this move sounds relevant. Indeed, 6G cannot be viewed as an enabler of planet sustainability whereas conversely, sustainable 6G networks is a valid goal to take. We had made the exercise of populating the SNS project developed use cases and found the split as below (into the 6 families). The split is relatively balanced (see below). On the left column, you get the use cases.

3.5.1. HEXA-X use case families and their respective KPIs are listed below:

An abstract of this content-rich presentation is given below. SNS ICE defines six families of 6G use cases defined as below.

Table 6. HEXA-X six use case categories with their KPIs

Seamless Immersive Reality
Functional requirements: AI/ML, sensing, positioning, Privacy and Security, Continuity, low latency + synchronization
⇒ Data rate: #250 Mb/s at DL, UL for UE taking role of gateway ⇒ Area traffic capacity: 20 Mb/s/m2 ⇒ E2E latency <10 msec ⇒ Positioning <10 cm
Cooperative Mobile Robots
Functional requirements: AI/ML , sensing, positioning, local connectivity and Mobility, Dynamic topologies, low E2E latency
⇒ Data rate: <10 Mb/s (robot to robot- ⇒ Area traffic capacity < 0,1-1 Mb/s/m2 ⇒ E2E latency <0,8 msec ⇒ Reliability 99,999-99,99999 % (failure rate) ⇒ Mobility <10 Km/h ⇒ Positioning accuracy <0,1 m
Network-Assisted 3D Mobility (autonomous drone transport, assisted vehicles)
Functional requirements: AI/ML, sensing, positioning, Privacy and Security, Reliability and Continuity
⇒ Data rate: #1-10Mb/s at DL, UL for UE taking role of gateway ⇒ Area traffic capacity: 20 Mb/s/m2 ⇒ E2E latency <1-20 msec ⇒ Mobility <300 Km/h ⇒ Reliability 99,99% ⇒ Coverage 99,9% ⇒ Availability 99,99%
Digital Twins (Production plant control, overall smart cities)
Functional requirements: AI/ML, sensing, interoperability, Privacy and Security, E2E latency

⇒ Area traffic capacity: 1-10 Mb/s/m2 ⇒ E2E latency <1 msec ⇒ Reliability 99,99999 ⇒ Positioning <100 cm
Ubiquitous and resilient Network (Connectivity for remote locations, Connectivity during disasters)
Functional requirements: Flexibility, coverage/connectivity everywhere, resilience, Affordability, Continuity, Privacy and Security
⇒ Data rate: 0,1-25 DL. 2 UL Mbits/sec ⇒ Availability 98,5% ⇒ Coverage TN<10-15 Km cell radius; TN/NTN: 99,99% of human environment ⇒ E2E latency 10-100 msec ⇒ Reliability 99,9-99999
Human centric Networks (Precision healthcare, public safety during big events)
Functional requirements: AI/ML, Reliability, Positioning, sensing, Accurate Target and activity identification, Privacy and Security
⇒ Area density 1-10 Mb/s/m2 for indoor, <0,001 for outdoor ⇒ Location accuracy (depending on contexts, <0,1 to 10 m) ⇒ E2E latency 250-1000 msec ⇒ Reliability 99,9-99,999

3.6. Other SNS-JU financed projects. (Stream A and B)

3.6.1. General

SNS financed projects, already engaged in SNS 2022 & 2023 streams A and B have been analyzed with the intent of collecting their use cases and placing them into Hexa-X 6 categories. We have then sorted the use cases focused on research on security, performance and sustainability. In both cases, our intent is to assess the relative weight and importance of the categories and research topics covered by the SNS projects until now. Moreover, we have extracted the KPIs of these use cases of the SNS projects for which the use case deliverable is made public and available on their website. Except for a few specialized research projects (e.g., SUPERIOT, TERA6G) which have their own specific KPIs for assessing their use cases, the projects share the same high-level service-based KPIs (e.g., availability, latency, perceived throughput). We had counted the occurrences of each KPIs in the projects and had produced a list of most frequently used KPIs. This collection of formerly used service level KPIs took part of NATWORK's KPIs selection.

3.6.2. SNS financed project distribution over the six HEXA-X categories

The 6 categories of Hexa-X flagship project are well represented by the SNS on-going projects 59 use cases as shown in the following tables, following our assessment of the most relevant

thematic for one use case. Hexa-x Fully Connected World category appears to the most processed thematic.

Table 7. SNS financed projects Collaborative Robots use cases

Use case on IMMMERSIVE EXPERIENCE (8 use cases)	STREAM A	STREAM B
Holographic Teaching		ADROIT-6G-6G
Co watching live events		ADROIT-6G-6G
X-Reality		DETERMINISTIC
AR with perceived no latency		DESIRE-6G
XR		PREDICT-6G
Immersive Education		6G SHINE
Indoor Gaming		6G SHINE
Co-creating arts		ADROIT-6G-6G

Table 8.SNS financed projects Collaborative Robots use cases

Use case on COLLABORATIVE ROBOTS (5 use cases)	STREAM A	STREAM B
Collaborative Construction Robots		ADROIT-6G-6G
EXOskeleton		DETERMINISTIC
Factory Automation		DETERMINISTIC
Mobile Automation		DETERMINISTIC
Mobile Robot management		TIMES-6G

Table 9. SNS financed projects Physical Awareness use cases

Use case on PHYSICAL AWARENESS (6 use cases)	STREAM A	STREAM B
Smart manufacturing		PREDICT-6G
Augmented reality navigation		6G SHINE
PREDICT-6G predictive maintenance		TIMES-6G
Flexible factory		TIMES-6G
Bi-directional data stream in mobility		SUPERIOT
Consumer handled. Connectivity and positioning in remote areas		SUPERIOT

Table 10. Table 8 SNS financed projects Fully Connected World use cases

Use case on FULLY CONNECTED WORLD (23 use cases)	STREAM A	STREAM B
Maritime, Railway, Airway T-NTN continuum	STARDUST	
Residential Broadband	STARDUST	
PPDR @	STARDUST	
Global Private Network	STARDUST	
Vehicule connected	STARDUST	
Core NTN	SEASON	
Critical Operation Maintenance During Energy Constraint Disaster	6GREEN	
Energy Efficient Augmented Reality remote Assistance	6 GREEN	
Zero-Carbon client-less Virtual entreprise desktop as a service	6 GREEN	
PoC : Intelligent plane sensing assisted communication, energy efficient O-RAN and CU, Energy efficient DU, RU power amplifier blanking control	BEGREEN	
Optical Link use optimisation		FLEX-SCALE
T/NTN continuum		ETHER
Raw and DetNet exploitation		PREDICT-6G
Multi Domain Deterministic communications		PREDICT-6G
Deterministic Services for critical coms		PREDICT-6G
Dual Frequency Distributed Transceivers placed over Analog Linear Stripes		6G TANDEM
Novel THZ RIS technology (Energy efficient)		TERRAMETA
Novel THZ Transceivers for flexible, energy efficient Fiber over the air		TERA6G
AI-AI (i.e., AI-Air Interface) for Energy efficient Service KPIs reach)		CENTRIC
Network scalable trans-domain resource orchestration	ACROSS	
Novel RAN that supports scalability and security	NANCY	
Ultra reliable connectivity and high energy efficiency	NANCY	
Zero Latency and high computational capabilities at the edge	NANCY	

Table 11.SNS financed projects Trusted Environment use cases

Use case on TRUSTED ENVIRONMENT (13 use cases)	STREAM A	STREAM B
Assistant First Responder		ADROIT-6G

Use case on TRUSTED ENVIRONMENT (13 use cases)	STREAM A	STREAM B
Remote Surgery		ADROIT-6G
Rail Automation by NTN		ADROIT-6G
Maritime SAR		SUPERIOT
Powerline inspection		SUPERIOT
Secure Smart Light Rail transit		HORSE
Remote Rendering to Power XR industrial (IPR security)		HORSE
Predictive Maintenance for Airline Consortium over DLT		CONFIDENTIAL6G
Privacy-Preserving Confidential Computing platform that enables mitigation of internal threats for Telecom Cloud Providers		CONFIDENTIAL6G
Intelligent connected vehicle, missing critical services, OTA updates		CONFIDENTIAL6G
Protecting 6G Services against Cyber Threats		RIGOUROUS
Secured IoT-based Smart City extended video platform by Encryption as a Service		RIGOUROUS
Secured Utilities management		RIGOUROUS

Table 12.SNS financed projects Digital Twins use cases

Use case on DIGITAL TWINS (4 use cases)	STREAM A	STREAM B
Digital Twin for Robot		DESIRE-6G
Digital Twin		TIMES
Smart Cities		PRIVATEER
Intelligent Transport system		PRIVATEER

3.6.3. Inclination on Security, Performance and Sustainability

Our assessment of the on-going SNS projects with the lens of these three dimensions results in the following balanced distribution, given in the table below.

Table 13. SNS project inclinations on Security, Performance and Sustainability

SECURITY (25 use cases)	PERFORMANCE (18 use cases)	SUSTAINABILITY (16 use cases)
• All trusted environments use cases (per essence) (#13)	• All STARDUST (#5) • Core NTN SEASON (#1)	• 6GREEN use cases (#3) • BEGREEN use case(#1) • FLEX-SCALE (#1)

SECURITY (25 use cases)	PERFORMANCE (18 use cases)	SUSTAINABILITY (16 use cases)
• All physical awareness (as for DT, integrity of sensor data is required), (#6) • Novel RAN that supports scalability and Security by NANCY (#1) • All collaborative Cobots (#5)	• T/NTN continuum (ETHER) (#1) • RAW and DETNET application (PREDICT) (#1) • Multi domain deterministic comms (PREDICT) (#1) • Deterministic Services for Critical Coms (PREDICT) (#1) • All immersive experience (#8)	• Analog Stripes for Transceivers (TANDEM) (#1) • Novel THz RIS technology (TERRAMETA) (#1) • Novel THz Transceivers (TERA6G) (#1) • AI 4 Air Interface (CENTRIC) (#1) • Novel orchestration trans domain (ACROSS) (#1) • Ultra Reliable Connectivity and high energy efficiency (NANCY) (#1) • All Digital Twin use cases (#4)

These use cases naturally expose KPIs related to metrics of performance (e.g., bandwidth, latency, error rate, reliability, perceived and peak throughput, mobility, jitter, clock synchronicity, device density), to security (e.g., time to detect, time to mitigate) and to sustainability (e.g., spectral efficiency, RAM usage, CPU usage, energy efficiency, survival time, resilience).

The **KPIs for performance show higher usability and occurrence** counts than the ones associated with security and sustainability. All higher count KPIs are associated with Performance. They reflect the key motivations of the SNS initial phase 6G projects notably to enable novel promising use cases (e.g., holographic communication or city digital twins) which are considered as potential outcomes brought by 6G. Conversely, sustainability and security KPIs can be viewed as lower-weight objectives associated with new progress in a technical domain (e.g., RIS antenna, spectral efficiency) and security threats (e.g., DoS on core or RAN).

3.6.4. SNS projects most-used KPIs

The SNS projects most frequently used KPIs are listed below for KPIs which appear more than once. The KPIs are given by decreasing order of occurrences:

- Use case end to end **Latency** (10 counts): Application Latency is the contribution of the radio network to the time from when the source sends a packet to the time when the destination receives it (in msec).
- Use case required **Max Bandwidth** (8 counts): Maximum Bandwidth is the maximum aggregated system bandwidth.

- Use case service **reliability** (7 counts): Reliability relates to the capability of transmitting a given amount of traffic with a high success probability. within a predetermined duration with a high probability of success.
- Use case service **availability** (6 counts): Percentage value (%) of the amount of time a system is in condition to deliver services divided by the amount of time it is expected to deliver services in a specific area.
- Use case **peak throughput** (5 counts): Peak throughput is the maximum achievable throughput under ideal conditions
- Use case **device density** (4 counts): Device density is the total number of devices fulfilling a specific quality of service (QoS) per unit area (per km2)
- **Area traffic capacity** (3 counts): The total traffic throughput served per geographic area (in bps/m2). This metric measures how much traffic a network can carry per unit area. It depends on site density, bandwidth and spectrum efficiency.
- **Jitter** (3 counts): Jitter is the variation in time delay between when a signal is transmitted and when it's received over a network connection, measuring the variability in ping
- **Quality of experience** (3 counts): The Quality of Experience (QoE) is defined as “the overall acceptability of an application or service, as perceived subjectively by the end-user”, covering the complete end-to-end system effects (client, terminal, network, services infrastructure, etc.).
- **Clock Synchronicity** (2 counts): Sensor to sensor clock synchronicity (sec)
- **Block Error Rate** (2 counts): is a key performance indicator that measures the proportion of erroneously received data blocks to the total number of data blocks transmitted

Although engaged SNS projects are not equally distributed over the Hexa-X six categories, the six categories are all covered. Noticeably, the six categories focus on technical domains of different size and importance (e.g., fully connected world versus digital twin). The engaged SNS projects are dealing with Security, Performance and Sustainability. As reflected in the paragraph above, the most-used KPIs are exclusively related to performance. Conversely, security and sustainability KPIs are domain specific, hence with single or very low occurrences. In a general perspective, the engaged SNS projects relate to the first phase of SNS JU 6G research projects with the aim of demonstrating the technical practicality of the 6G extended abilities. Collectively, these projects have a good coverage over all promised 6G use cases with performance KPIs set as enablers at the first place. Last and unsurprisingly at this initial stage, KPIs are driving performance, security and sustainability independently.

3.7. Conclusions

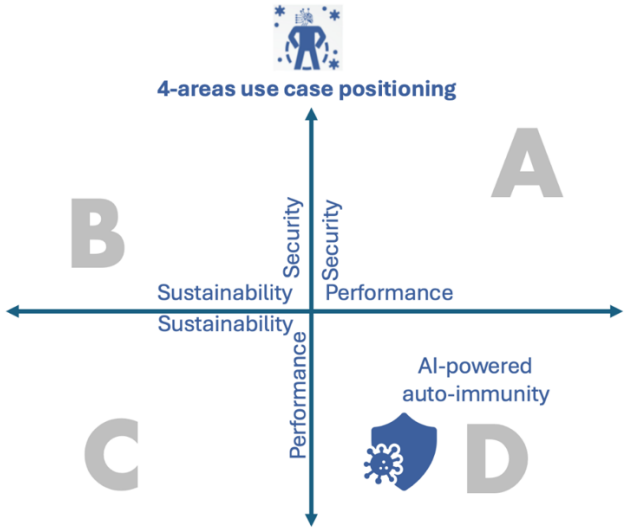
The solid financing effort of E.U on research, driven by SNS-JU is clearly engaged to fix performance, security and sustainability. These three values have similar weights on the main objectives of financed projects. Recent elements (e.g., Agriculture's AIOTI guidelines) are now stating the importance of being energy-efficient when targeting performance. This is paving the way for NATWORK's concept reconciliation performance and sustainability and security and sustainability.

4. NATWORK's use case description methodology

4.1. Use case description template

The following template has been defined collectively to grasp all technical, organizational, risks and timeline elements associated to the use case. Moreover, a graphical aid enables us to better grasp the position of the use in the NATWORK's concept.

Table 14. Use case description template

Template criteria	Information
Domain description	Functional requirements and associated challenges Enumeration of functions High level functional description (UML) Challenges taken up by the use case Use case threat model
Relevance with NATWORK	Description of **the security threat model** and associated Performance and Sustainability constraints. Placement of the use case in the 4 areas **A, B, C and D** as defined in the figure below.  The position of the use case in one or several areas reflects the objectives of the use case as set below: Use case positioned in areas A, B or C means that the use case is progressing in two dimensions of the selected area (e.g., security and performance) or that the use case progresses in one dimension without impacting on the other dimension. Use case positioned in area D means that the use demonstrates a network AI-powered self-improved immunity.
KPIs	Used KPIs to qualify the use case
Testbed requirements	Infrastructure, software and data requirements

Template criteria	Information
Sequence diagram	
Success factors	
Timeline and risks	

5. Use case 1. Sustainability and Reliability of 6G Slices and Services

5.1. Use case 1.1 Decentralized Management and Orchestration for Intent-compliant end-to-end Service Resiliency and Continuity

With the increasing number of connected devices and data-intensive applications in 6G edge-to-cloud networks, energy consumption is expected to increase substantially. Increased energy consumption and security threats have made the Sustainability and Reliability of 6G Slices and Services a crucial focus area. This use case focuses on demonstrating NATWORK's MANO service that enables communication and coordination across multiple infrastructure components and service providers in response to cascade denial of sustainability (DoSt) attacks.

This use case involves demonstrating DoSt attacks on 6G slices, along with the detection, and mitigation techniques, and Cyber Threat Intelligence (CTI) solution used in secure-by-design orchestration and management of 6G Slices. The orchestration service, incorporating optimization algorithms, will be deployed over UEssex's 6G backhaul, utilizing an edge-to-cloud computing continuum connected by a programmable network. The CTI components introduced here highlight the potential influence of vulnerability assessment on orchestration and management decisions of segments in 6G slices. All these activities are covered under Use Case (UC) 1.1.

5.1.1. General functional description

As 6G networks become more pervasive, they will require increasing amounts of energy to power the massive number of connected devices and data-intensive applications. With energy consumption being a critical factor in the sustainability and cost-effectiveness of 6G networks, this use case will explore innovative energy solutions that can support reliable connectivity and high-quality services while reducing energy costs and minimizing environmental impact. Thus, the tools that will be demonstrated in the pilot aim to optimize energy efficiency through intelligent network management and adaptive power consumption techniques.

In the first phase of the use case, a DoSt attack will be demonstrated, highlighting its impact on the 6G slices. DoSt attack detection strategies will be provided. This phase will establish our State-of-the-Art (SotA) federated orchestration solution (FORK)[16] as a baseline for secure-by-design orchestration and will also showcase the CTI solution, which will play a role in the CTI exchange between clusters and influence orchestration decisions based on the security requirements of the slices. Orchestration decisions will guide the mitigation process, ensuring that appropriate measures are taken to address vulnerabilities.

The second phase will focus on validating initial implementation of NATWORK's technologies and modules to assess the sustainability and reliability of 6G networks. The emphasis will be on the security expansion of the FORK solution, optimizations of the CTI solution, and implementation of the slice management services. The demonstration will be scaled up, with an extended evaluation of KPIs and visual representation of the results. This phase will center on improving the CTI solution and enhancing security-driven orchestration.

The DoSt attack scenario In UC 1.1 will involve generating HTTP-based oscillating demand. This will lead to continuous scaling in and out of Kubernetes containers, causing a Denial of Sustainability (DoSt) in a 6G slice. Random request generators will launch the attack, with telemetry collected through Prometheus[17] and ONOS[18] interfaces. The FORK Solution will be used as baseline to demonstrate the DoSt attack as shown in Figure 5. The demonstration will be conducted on the UEssex testbed infrastructure.

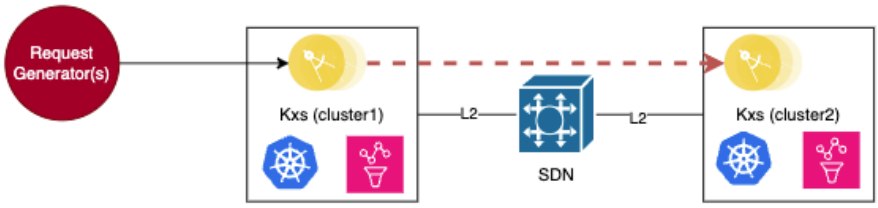


Figure 5. DoSt Demonstration Diagram with FORK

The CTI solution as shown in Figure 6 is a middleware framework designed for decentralized and adaptive CTI exchange between multiple domains. CTI solution components placed in each cluster enable threat information sharing between different domains. Vulnerability data acquired from security tools is processed and shared in real time. The data shared will play a role in influencing the orchestration and management decisions of the microservices in a cluster. The architecture is adaptive, dynamically adjusting the amount of shared information based on the vulnerability context and the security requirements of both producers and consumers. This solution brings the flexibility of controlling CTI data before it is shared and ensures CTI data does

not involve sensitive and confidential information. The CTI solution is compliant with STIX/TAXII standards for structured CTI exchange.

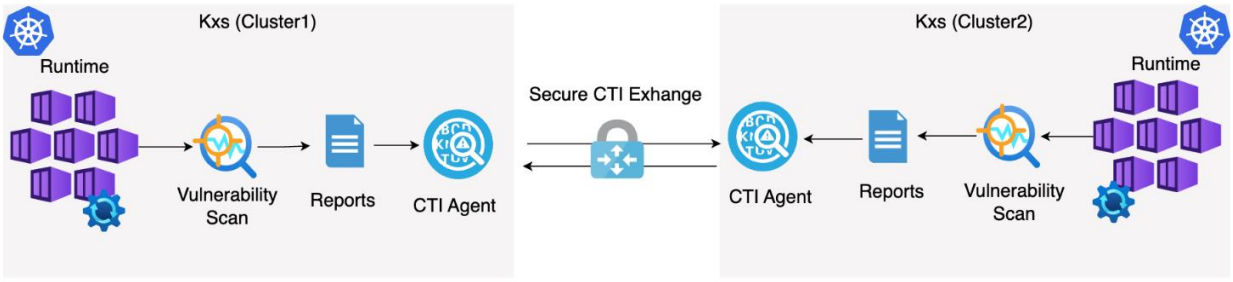


Figure 6. CTI Solution Diagram

Later in the project this framework will impact orchestration decisions by providing real-time insights into the vulnerability and security posture of clusters. It also offers a high-level overview of a cluster's trustworthiness. This allows for placing high-security applications in clusters with better hygiene scores and higher levels of trust.

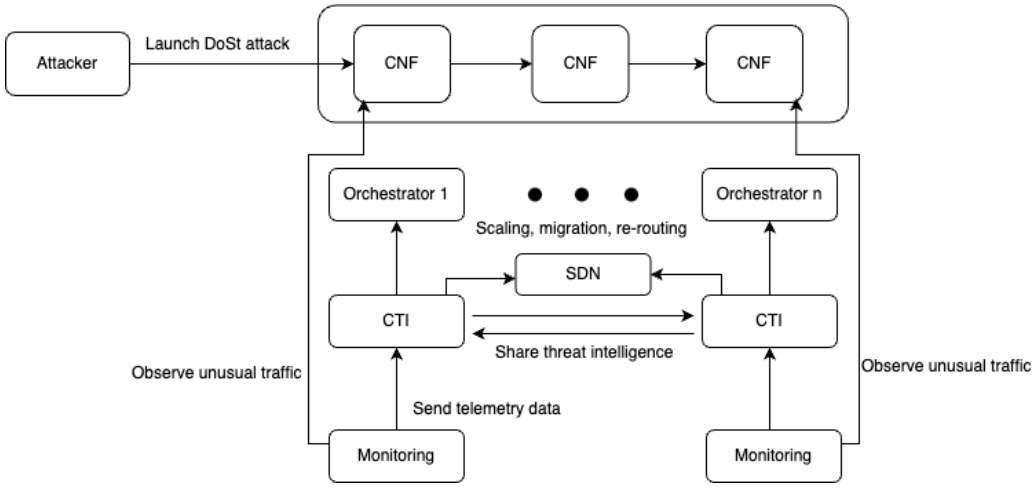


Figure 7. Use-Case UML Diagram for DoSt Attack Scenario in UC1 .1

5.1.2. Use case relevance with NATWORK

Use Case 1.1 aligns well with OO1, OO2, OO3, OO5, and OO6, as it focuses on decentralized, secure-by-design orchestration, adaptive management, and real-time CTI exchange, all aimed at enhancing the security, sustainability, and resilience of 6G networks. The

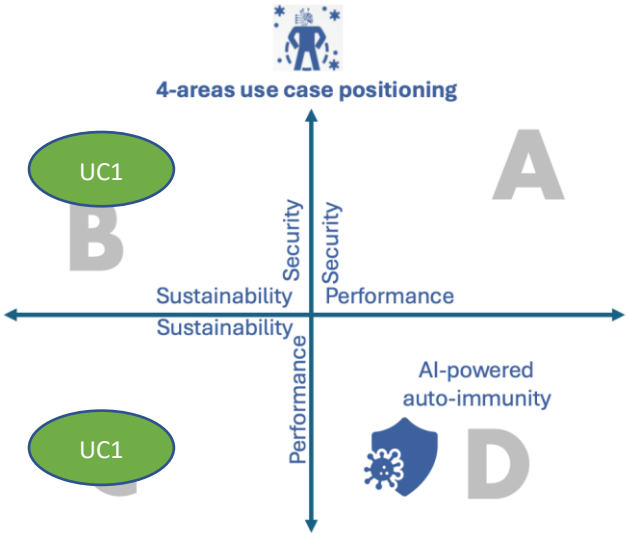


Figure 8. UC1 .1 position on NATWORK's Conceptual Graph

The use case will provide a practical demonstration of the objectives. It demonstrates real-time CTI exchange and its role in enabling secure information sharing across distributed infrastructure elements and influencing orchestration decisions. It includes security-based orchestration of 6G slices, utilizing real-time CTI to adapt to evolving threats and ensure continuity. The adaptive orchestration approach offered in the use case in response to DoSt attacks supports the goal of creating secure, resilient, and energy-efficient slices. It will provide a measurable demonstration of orchestration capabilities and security module effectiveness. The demonstration will be conducted on the UEssex infrastructure, with documentation provided for reproducibility.

The key tasks that align with UC1 .1 are summarized and highlighted in Table 15 below.

Table 15. Relevance of UC1 .1 with NATWORK tasks

NATWORK tasks	Focus Areas	Objectives	Key Activities
T2.1	Orchestration and attestation SoA	SoA analysis of security and trust establishment in the context of 6G networks	Alignment of proposed solution in respect of the SoA analysis
T2.3	End-to-End Specifications & 6G extendable Architecture design	Defining the end-to-end system requirements and technical specifications for the 6G architecture	Incorporating system requirements and technical specifications in demonstration
T3.1	Secure-by-design federated slice orchestration and management	Development of a federated solution for the secure-by-design composition and management of 6G cloud-native slices.	Showcasing development of the secure-by-design orchestration and management mechanisms

NATWORK tasks	Focus Areas	Objectives	Key Activities
T3.3	Intent-based service security and associated adaptive placement of security and services	Secure-by-design composition and configuration of cloud-native in-network security services and optimal distribution within 6G edge-to-cloud continuum to meet Net-Zero targets	Development of secure-by-design cloud-native solutions for DoSt attack detection and prevention, dissemination of CTI components for effective threat information sharing
T4.2	AIaaSecS system for software payload protection	Developing AI based Security solutions for protecting payloads in the edge-cloud	Capturing resource consumption data for vulnerability detection and intrusion detection in 6G core. AI solutions for anomaly detection
T4.3	AIaaSecS system for network management and security	Automatic identification of network changes and security threats and the corresponding action	Monitoring the network flow on the SDN side, the security of the connection and peering across services in 6G slices
T6.2	Testbed integration and Attack generation system	Setting up the testbed environment and including the relevant use case components	UEssex Testbed Lab environment setup and deploying the developed orchestration, management, security and attack generation mechanisms
T6.3	Use cases trials and demonstrations	Use case demonstration to verify NATWORK´s technologies/modules developed	Improve the network-user sustainability by innovative energy solutions that can support reliable connectivity and high-quality services, while reducing energy costs and minimizing environmental impact.

5.1.3. Definition of the use case KPIs

Use case 1.1 will consider KPIs as defined in Table 2. Based on the SoA analysis, the defined KPI values are depicted in Table 16 below. At this stage, KPI 1.1 on proposal related to end-to-end compliance with latency tolerance will be addressed in subsequent phases as the relevant components are developed. Three additional KPIs, KPI 1.5, KPI 1.6, and KPI 1.7, have been evaluated and incorporated and shown in the greyed lines.

Table 16. KPIs for UC1 .1

KPI	Title	Target value
KPI 1.1	End-to-end compliance with latency tolerance	10%

KPI	Title	Target value
KPI 1.2	Energy waste: CPU utilization under normal/attack conditions to measure energy consumption (used to estimate Energy waste percentage)	10%
A-KPI 1.5	Cluster Hygiene Scores (Number of vulnerabilities shared with score 8+/Total number of vulnerabilities)	0<x<1 (Subject to review and update)
A-KPI 1.6	Cluster CTI Exposed information Ratio (Number of vulnerability data parts revealed/Total information per CTI data)	0<x<1 (Subject to review and update)
A-KPI 1.7	Cluster CTI Hidden information Ratio (Number of vulnerability data parts hidden/Total information per CTI data)	0<x<1 (Subject to review and update)

5.1.4. Sequence diagram of use case workflow

The diagram below illustrates the sequence of actions in UC 1.1. Figure 9 focuses on the main sequence of actions of initiating DoSt attack, CTI sharing, and orchestration components. The UC workflow proceeds as follows:

Step 1. The attacker initiates a DoSt attack by sending oscillating Requests, which trigger the scaling of CNFs.
Step 2. Monitoring tools actively monitor traffic. They send the system's telemetry data to inform the CTI component.
Step 3. The CTI component, in collaboration with the Anomaly Detection (AD) systems, prepares and shares the CTI data across clusters.
Step 4. CNFs exchange threat intelligence data.
Step 5. The CTI component will notify the control plane about the anomaly.
Step 6. The orchestrator assesses the situation and determines the appropriate actions.

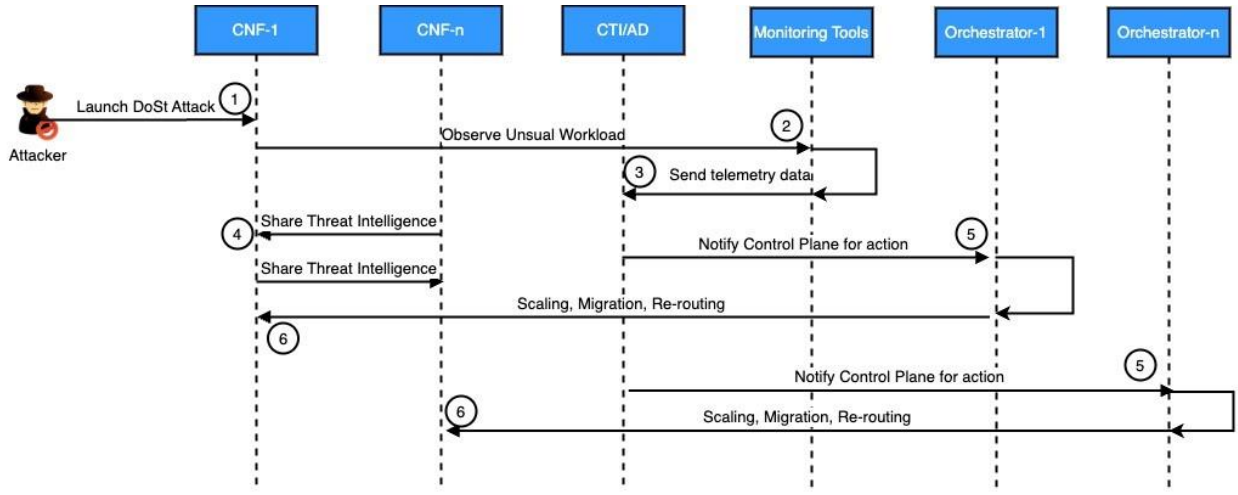


Figure 9. Sequence diagram for UC 1.1

5.1.5. Description of the use case testbed requirement

5.1.5.1. ***UEssex NCL Lab***

The tests of system components will be conducted in Network Convergence Laboratory (NCL) of UEssex. NCL, UEssex (UK), is a research data center divided into multiple variant size clusters, connected by a SDN/P4 programmable network. It mimics an edge-to-cloud continuum with offered capacities of 200+ CPUs, 200+ Terabytes storage, 180Gbs SDN and 100Gbps P4. The SDN is ONOS-controlled while the computation / storage clusters are divided between Kubernetes and OpenStack control. A snapshot of NCL is shown below in Figure 10. The use-case requires in the minimum two small virtual computing clusters, connected either directly or by SDN forwarder. This will form the initial setup, and scaling up is planned for the following phases of the use case implementation.

Figure 10. Network Convergence Lab (NCL) of UEssex

5.1.6. Timeline and Risks

5.1.6.1. Timeline

1. **Preparatory development (Months 1-12)**:

- **Activities**

  - **SoA Analysis:** Detailed SoA analysis about orchestration and management of 6G slices, work environment set up

- **FORK**: Deployment and initial run of the FORK orchestrator
- **CTI:** Deployment and initial run of the CTI solution

- **Results**
  - Have an initial implementation of FORK solution on Kubernetes, deploying cloud-native functions across domains and basic load and network tests
  - Prepared basic tools to generate oscillating requests to implement the DoSt attack
  - Initial preparation of the testbed environment

2. **Testbed preparation and integration (Months 13-24)**:

- **Activities**
  - **Integrating NATWORK solution to the demonstration:** The security-by-design FORK and CTI demonstration and integration to UC1 .1 pilot
  - **Attack mitigation:** Demonstration of the strategies developed to mitigate DoSt attacks
  - **Optimization of CTI solution:** CTI solution optimization for integrating security and orchestration components and influencing orchestration decisions
  - Updating Orchestration Solution (Newer version of FORK)
  - **Testbed scaling:** Setup the FORK and CTI components, scaling up the Testbed to medium size
  - Connection to IMEC testbed: Integration with the IMEC testbed
- **Results**
  - A running demonstrator showing attack behavior and NATWORK response
  - Scaled up testbed and attack generation service

3. **Testing, Enhancement and Finalization (Months 25-36)**:

- Scaling up the evaluation of the NATWORK solution and advancing its technology readiness
- Comprehensive demonstration of the solution's effectiveness
- Testing and showcasing system capabilities, meeting the security requirements
- System Integration, Evaluation, and Validation. The components will be integrated, followed by comprehensive evaluations and validation processes. Documentation will be prepared based on the findings and insights gathered during these assessments.

5.1.6.2. Risks

The main risks in terms of UC 1.1 are collectively presented as:

Integration of use case components:

Risk: The integration of multiple components (e.g., orchestration services, CTI modules, AI-driven optimizations) across different domains may lead to compatibility issues. Incompatible interfaces or unforeseen dependencies between the components could cause functional errors or impact the system's efficiency.

Mitigation: A modular integration approach will be adopted. Unit tests will be conducted in every stage of the implementation. Dependency will be minimized by virtue of communication through APIs.

Integration between IMEC and UEssex testbeds:

Risk: Potential incompatibility issues related to interfaces and hardware

Mitigation: Testbed integration will begin early with a clear integration plan outlining hardware and software requirements. Regular verification and coordination will take place during UC1 meetings to ensure smooth integration.

5.1.7. Summary

UC 1.1 focuses on demonstrating decentralized management and orchestration of 6G slices. It will specifically address the challenges of energy consumption and security in edge-to-cloud networks. The use case showcases the NATWORK solution by simulating Denial of Sustainability (DoSt) attacks on 6G slices and deploying detection and mitigation techniques. A key component is the Cyber Threat Intelligence (CTI) solution, which facilitates real-time CTI exchange across clusters. It will take an active role in orchestrating decisions based on vulnerability assessments. The system will leverage optimization algorithms to dynamically manage 6G slices and ensure resilience. The first phase involves deploying the FORK orchestrator and CTI solution on UEssex's 6G backhaul, while the second phase focuses on scaling, optimizing, and evaluating the solution's performance. This use case aims to validate the security, sustainability, and reliability of 6G networks, demonstrating secure-by-design orchestration and management of slices.

5.2. Use case 1.2 SECaaS security

5.2.1. Domain description

5.2.1.1. Functional requirements and challenges

Software security is a multi-facet activity, spanned over different enforcements (e.g., remote attestation) or good practices (e.g., vulnerability removal) placed at different stages. As part of UC 1.2, we describe below the techniques and their associated challenges to be developed in NATWORK and applied by TSS's SECaaS service and directed to both x86 and WASM payloads.

UC 1.2 will develop and progress the SECaaS functions to bring remote attestation, runtime integrity verification, confidentiality and execution monitoring as detailed below.

Remote Attestation (RA) is a key enabler for software security, conferring cryptographic evidence of the software origin and integrity in one measurement. RA is a verification standing at code bootstrap phase, before execution and where the impact on code performance is not critical (as the code does not execute yet). The technique lies on asymmetric encryption and hashing and is employed from core system code to user level code. The same reference cryptographic verification can be used for code at bootstrap or during its execution. The security of RA is a function of different components security level (i.e., the verifier and measurer. Centralized and bastioned verifiers are exposed to availability attacks. Distributed verifiers reside in untrusted environments and are exposed to code introspection and tampering. Measurers are located on untrusted environments, hence potentially tweaked to deliver fake measurements. Trusted Platform Modules (TPM) are solid bastioned dedicated processing units, elaborating hardware-based root of trust as well as preventing local measurement tampering attacks. However, this comes at the costs of significant workflow for the setup and deployment restriction penalties. Novel forms of distributed verification leveraging blockchain [37], [38] establish a software-based flexible root of trust, remediate to availability attacks on the verifier, abate deployment restriction imposed by TPM and reference measurement management tasks highly penalizing RA adoption. **In NATWORK, the progressed D-MUTRA blockchain-based remote attestation transforms any payload as a potential verifier or target for RA, applying a novel root of trust based on the integrity freshness (i.e., the most freshly attested entity is selected as the next RA verifier).**

To verify the code genuineness and **integrity when the code executes**, performance penalty is critical. In that sake, **novel forms of continuous and low paced measurement** processes are emerging for being always sustainable. In the domain of WASM, at the current time, no runtime code verification exists in the state of the art. **The final design of WASM bootstrap and runtime**

verification solution will be defined in NATWORK, with possible deviations from D-MUTRA (i.e., designed for x86 payloads).

Code confidentiality frustrates vulnerability search and intellectual property preservation, against opponent static and dynamic code analysis. Code encryption frustrates plainly static analysis but is not effective against dynamic analysis. **UC 1.2 will exclusively consider static analysis defence by code encryption.** Encryption can be used for anti-cloning, by provisioning the decryption key and binding it to the host.

To remediate dynamic analysis, code obfuscation or placement into Trusted Execution Environment (TEE) bring different security assurances and workflow constraints. With no ability to deliver plain assurance against reverse engineering, code obfuscation inevitably induces CPU costs in relation with the obfuscation level. In [38], the authors put emphasis on the new threats (i.e., DoS exploiting TEE hard lock on integrity verification) and associated costs (i.e., memory consumption, performance) of TEE. Last, heterogeneity is the key obstacle to TEE adoption, as penalizing fluid payload migration, one of NATWORK core principle. At the time of production of this document, technical discussions are engaged between MONT, ZHAW and TSS **to assess the positive and negative impacts caused by AMD's SEV TEE for the execution of a security function** (i.e., MMT anomaly detection network probe), in terms of memory consumption, performance and security. This work will be possibly integrated into UC 4.5 as a sub use case and related to Moving Target Defence.

Code execution monitoring relates to the collection of various metrics from the execution (e.g., CPU rate, control flow graph integrity). In UC 1.2, we will consider a newly progressed technique, based on control flow-rooted time series extraction, assessing the performance ratio during the execution of the code and precisely without impacting the performance it measures.

Table 17. SECaaS security use case Functional requirements

Functional reqs	Description	Associated challenges
Remote mutual attestation	D-MUTRA associates TSS's SECaaS and a blockchain. The SECaaS modifies the payload to append remote attestation routines and generates the reference measurement. The blockchain orchestrates the remote attestation and provisions the reference measurement to the verifier.	Support of WASM payloads, with the associated changes on the WASM interpreter, must be developed and tested. The usability of the technology, notably in the Telecom domain with the requirement of pre-installed modified WASM interpreter must be analysed.

Functional reqs	Description	Associated challenges
integrity verification	The same SECaaS and DLT coupling will be capable of lightweight continuous integrity verification, with novel types of low-paced interruptible imperceptible measurements.	The challenge and progress versus the SoA consist in setting a permanent low-paced measurement to drop performance penalty for both x86 payloads and WASM payloads. A novel spread over time hash measurement will be advanced, representing a significant progress to bring sustainable security.
Code confidentiality, anti-cloning	TSS's SECaaS enables code instruction encryption and modifies the code to insert the code decryption routine. Decryption prior execution and possibly based on platform-provisioned keys (i.e., anti-cloning).	As a substitute to WASM code obfuscation, WASM payload encryption method, which involves changes on the WASM interpreter, must be tested and its acceptability by the telecom market considered.
Code execution monitoring	Control flow time series, collecting time and frequency with the granularity of executed code blocks. Post processing for evaluation of the performance ratio	Specific KPIs of convergence (i.e., time to reach a valid measure), penalty (i.e., impact on performance) and confidence (i.e., accuracy of the measure) are conflicting. The challenge is to find a trade off for each specific payload.

5.2.1.2. Enumeration of functions

The use case sets off payload security functions which will be tentatively delivered for x86 and WASM (i.e., with consideration of technical feasibility study and associated identified risks) of:

- D-MUTRA remote and mutual attestation at bootstrap.
- D-MUTRA remote integrity verification during execution.
- Code encryption/decryption with side-on platform provisioning of keys.
- Code monitoring.

5.2.1.3. UML description

For simplicity and because software security is a multi-facet activity, we restrict our focus on our specific mutual remote attestation, which differs from the state of the art, in the sequence of actions.

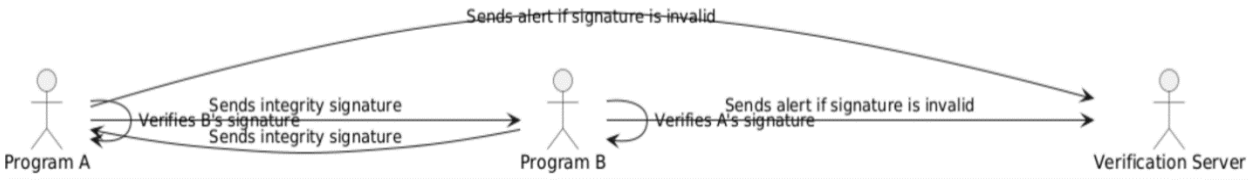


Figure 11.UC 1.2 SECaaS security mutual remote attestation UML

- Program A can measure itself and verify the measurement delivered by Program B

- Program B can measure itself and verify the measurement delivered by Program A
- Both Programs A and B transfer alerts (i.e., integrity failures) to a verification server, for figure clarity. This verification server is in fact the blockchain.

The UML brings a high-level simplified view on D-MUTRA, illustrating the mutual attestation by programs A and B. The detailed orchestration of D-MUTRA is brought in the sequence diagram which details the workflow for preparing both programs A and B by the SECaaS and for the blockchain smart contract orchestration of the remote attestations.

5.2.1.4. Challenges taken up by the use case

The challenges taken by this use cases are:

- Challenge 1. Develop platform-agnostic software security, maximizing secure payload mobility to reach concurrently higher performance and less resource consumption.
- Challenge 2. Develop software security against Confidentiality, Integrity and Availability attacks without impairing software performance.
- Challenge 3. Develop novel WASM payload security techniques against CIA attacks.

5.2.1.5. Threat Models

Several threats are tackled by the use case:

A. **Interception and replacement**. Attacker intercepts and modifies the software payload before it is loaded and launched on its targeted platform.
B. **Introspection and modification** (on the platform). Attacker introspects the running payload and modifies its memory pages during its runtime.
C. **Vulnerability search and exploit**. Attacker reverse engineers the payload, scouting for vulnerabilities for their further exploitation.
D. **Denial of service.** Attacker floods the payload with excessive workload or deprive local resources left to the payload.

5.2.2. Use case relevance with NATWORK

NATWORK's core objectives are i) reconcile performance, sustainability and security and ii) develop AI-powered self-resilience against novel threats. The use case is positioned on the first objective, with the clear ambition to take up the challenge of providing security without impairing performance and resource consumption. We had positioned the use case as straddling over both

areas A and B on the project ambition as set below. As shown by the arrows on Figure below, the use case elevates security but with the ambition to avoid creating a performance or resource excessive distortion or consumption. Hence both horizontal arrows tentatively limit the performance penalty and sustainability penalty to the lowest.

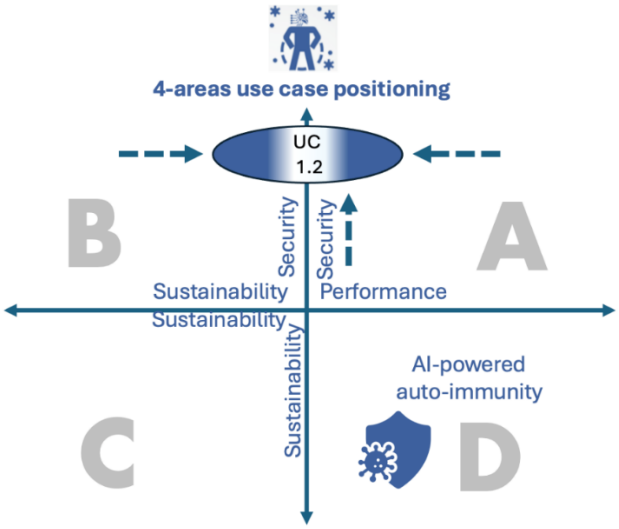


Figure 12. UC 1.2 position over the NATWORK's conceptual graph

Accurate analysis

In a general perspective and unsurprisingly for all offered security functions delivered by the SECaaS, security enhancement is always associated with a performance drop. The real operational penalty of performance drop varies according to the execution status of the software. Hence, one shall oppose the step of code bootstrapping and code execution. Remote attestation of code at bootstrap stage can be done without consideration of performance but reversely, runtime integrity verification must be done with deep consideration on the performance impact. The novel continuous security (i.e., continuous integrity verification processed during execution) relies on permanent, low paced and ultra-low resource consumption for the measurement, by scattering the measurement function through reduced operations processed over time. In practice, the use case will study the benefit of re-coding hashing function or CRC32 or a crypto proven hashing function over time with an objective of performance losses below 1% in average. This challenge goes beyond the state of the art, enabling imperceptible and continuous integrity verification. The same rule of thumb applies to software monitoring, always creating a penalty with the time series extraction over the execution. There again, the use case will be guided with the objective of providing execution insights at the lowest costs. In addition to the integrity verification, these insights will be evidence of effective execution and software normal performance ratio.

5.2.3. Definition of the use case KPIs

KPI 1.3 Respective x86 native payloads latency at start, performance degradation during runtime and overall energy waste for the aggregation of confidentiality, integrity runtime and correct execution monitoring (UC1 .2, <1sec, <10%, <10%).

This proposal stated KPI can be decomposed as follows for simplicity:

1. KPI 1.3.1, time for remote attestation cycle for x86 payloads < 1 sec
2. KPI 1.3.2, time for payload decryption for x86 payloads < 3 sec
3. KPI 1.3.3 performance degradation during runtime caused by runtime verification and performance monitoring for x86 payloads < 10 %.
4. KPI 1.3.4, overall energy waste for the aggregation of confidentiality, integrity runtime verification and correct execution monitoring for x86 payloads < 10%.

KPI 1.4 WASM security enforcement (according to our security challenge results), equivalent to x86 native implementation. We would split this KPI as below:

1. KPI 1.4.1, Feasibility study covering the four novel security functions of confidentiality preservation, authenticity, runtime integrity and monitoring: 1
2. KPI 1.4.2, Development of novel WASM security functions as the resulting of the feasibility study: 1
3. KPI 1.4.3, alignment with KPI 1.3 latency, performance degradation and energy waste: 1

WASM security will be first attained with WASM payload runtime integrity verification, a significant step taken over the state of the art. WASM payload encryption will be then tested. These two security enablement will be attained through the modification of the WASM interpreter. On that sake, the open source WASMTIME interpreter will be considered.

5.2.4. Description of the use case testbed requirement

- Infrastructure: No specific infrastructure requirements. Our development and tests will be worked out at TSS facility. The relevance and benefit of testing the solution over the NOVA ‘s infrastructure will be considered.
- security enablers:
  1. Installation of SECaaS (delivered in a container)
  2. Installation of DLT overlay (nodes delivered in a container), for D-MUTRA mutual remote attestation
  3. WASM interpreter installation
- data requirement: None

5.2.5. Sequence diagram of use case workflow

The sequence diagram delivered below reflects the x86 payload format. WASM payload format security will be developed during the project and the relevant sequence diagram could finally differ. Typically, DLT-based mutual remote attestation may not coincide with WASM payloads. TSS will further detail the outcomes of its research notably related to WASM payloads in the project deliverables.

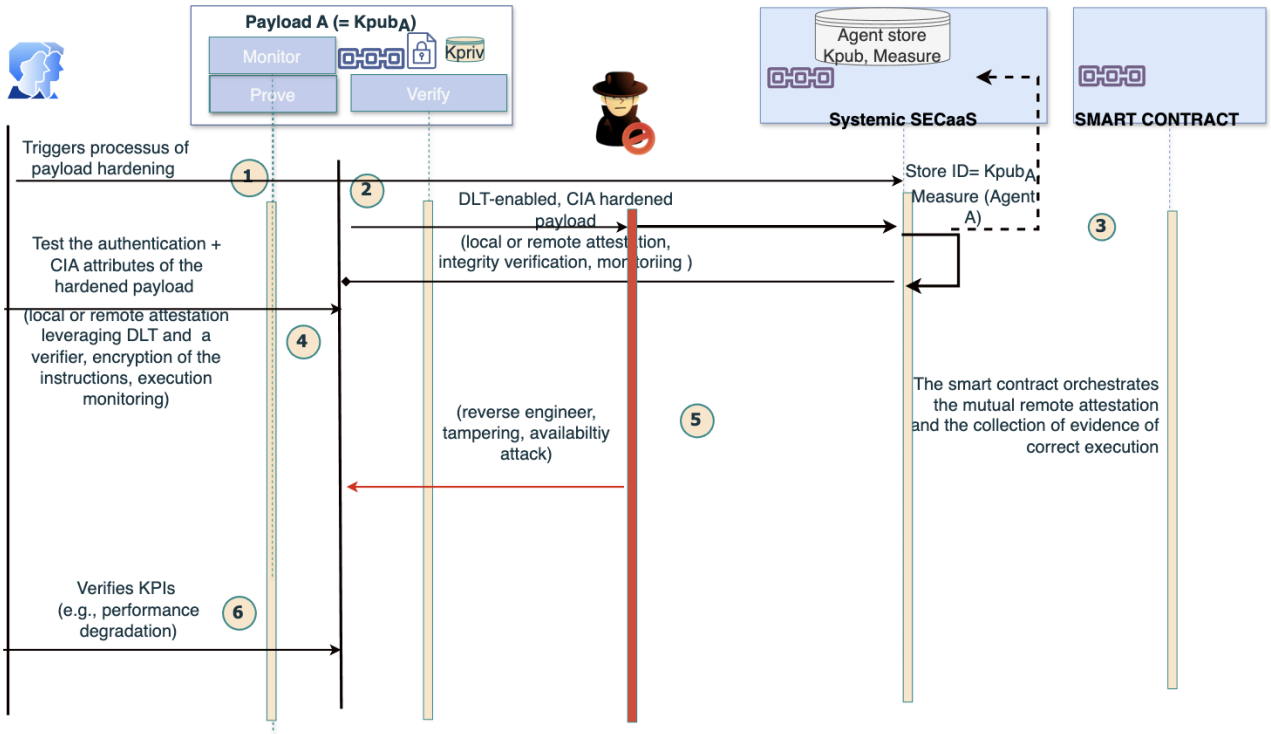


Figure 13. UC 1.2 SECaaS security sequence diagram

For clarity, the Figure 13 does not detail all operations but the main sequence of actions of payload hardening, attack on payload (and verification that the attack cannot be spawn) and KPIs verification. The use case workflow is set as follows:

Step 1. The user or a DevSecOps orchestrator instructs the SECaaS for the due hardening of a payload. Several options can be put on the SECaaS input JSON file.

Step 2. The original payload is uploaded to the SECaaS.

Step 3. The SECaaS creates a modified payload, appending the original with all needed elements to process authentication (i.e., Prove, Measure and Monitor routines, blockchain communication module, private key for signature). In addition, the SECaaS modifies the payload by encrypting

the payload instruction and appends the decryption routine). Last the SECaaS appends the runtime monitoring probes and time series extraction routine.

Step 4. The user verifies that the hardened payload satisfies the Confidentiality Integrity and Availability (CIA) attributes as set in the JSON file.

Step 5. Several attacks are spawn against the CIA hardening defenses. The verification that they cannot be worked out is produced.

Step 6. The user verifies the KPIs as defined above.

5.2.6. Timeline and risks

NATWORK progress on the SECaaS is significant and relates to bring sustainable security for running payloads, per-se a challenge and breakthrough on the state of the art. Noticeably, the novel performance-friendly integrity measurement (i.e., hash), based on a spread over time resource consumption represents a significant challenge (i.e., seamless synchronization with the measured process). Similarly, the novel security methods conferring WASM payloads with confidentiality and integrity assurances and implementing changes on the WASM interpreter bear their own risks. Last, performance monitoring with inserted probes can induce significant performance overhead, which conflicts with its goal.

5.2.7. Summary

Use case 1.2 demonstrates several new, software-based payload security functions, with the intent to bring platform and cloud-agnostic payload security. These security functions cover the CIA threat range by preserving confidentiality, integrity and by extracting payload availability evidence. These security attributes shall, as far as feasible, be available for both machine-compiled code and WASM interpreted modules. Notably for WASM modules, the use case will demonstrate significant progress versus the state of the art. The main success factors of the use case are to bring security at a very low performance impact and to support WASM. Technical risks are essentially pending on the WASM side.

5.3. Use case 1.3 Green-based payload placement

Green energy availability can vary a lot in time and geographical dimensions. Intelligent workload placement based on green energy availability is an important step towards net-zero 6G services. This requires several different innovations in multiple technologies: orchestrators need to be green-energy-aware and take this into account during scheduling and rescheduling of workloads. Underlying infrastructure must enable appropriate trust to ensure workload can safely move between datacenters without compromising privacy and Intellectual Property of workloads. Finally, there needs to be a trustworthy source of green energy information.

Within the context of the NATWORK project, UC#1.3 involves setting up a multi-location compute mesh with trusted computing-enabled hosts and verified sources of green energy information. Specifically, this will include a Kubernetes cluster spanning multiple geographic locations and using Remotely Attested Kubernetes workers to ensure the trustworthiness of the compute. Additionally, it will include an emulator of trustworthy green-energy information source. This use-case will show the technical feasibility of trustworthy net-zero payload placement while ensuring the security, integrity and confidentiality of the workloads and data.

5.3.1. General functional description

The demonstration will be conducted on the imec CloudNativeLab, CloudEdgeLab, and the UEssex testbed infrastructure. The UEssex testbed is used to simulate physically remote devices running on infrastructure outside of the control of the workload owner (imec).

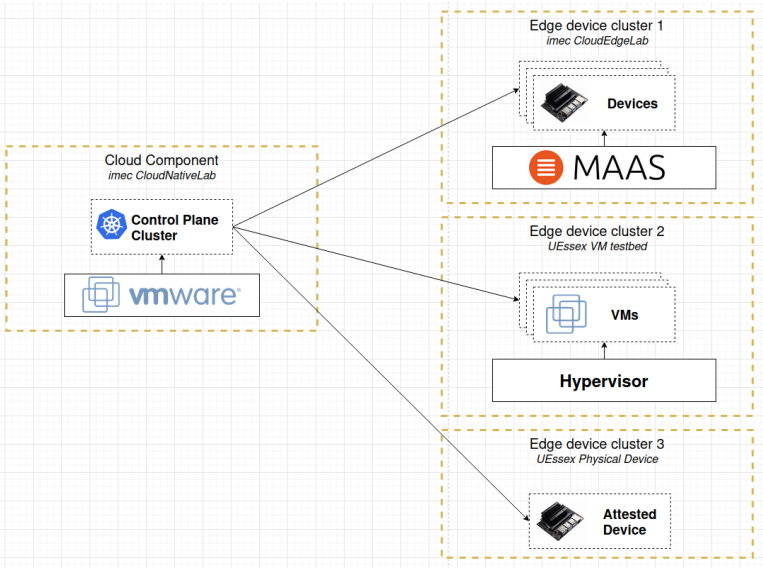


Figure 14. UC 1.3 Green based placement presentation

UC 1.3 will use modified Kubernetes scheduling algorithms that consider both the trustworthiness of workloads and the local dynamic availability of green energy, while implicitly enhancing energy efficiency through security feature optimization.
Device trust will be based on a Kubernetes-compatible device enrolment and attestation platform utilizing TPM and attested boot functionality on the remote device.

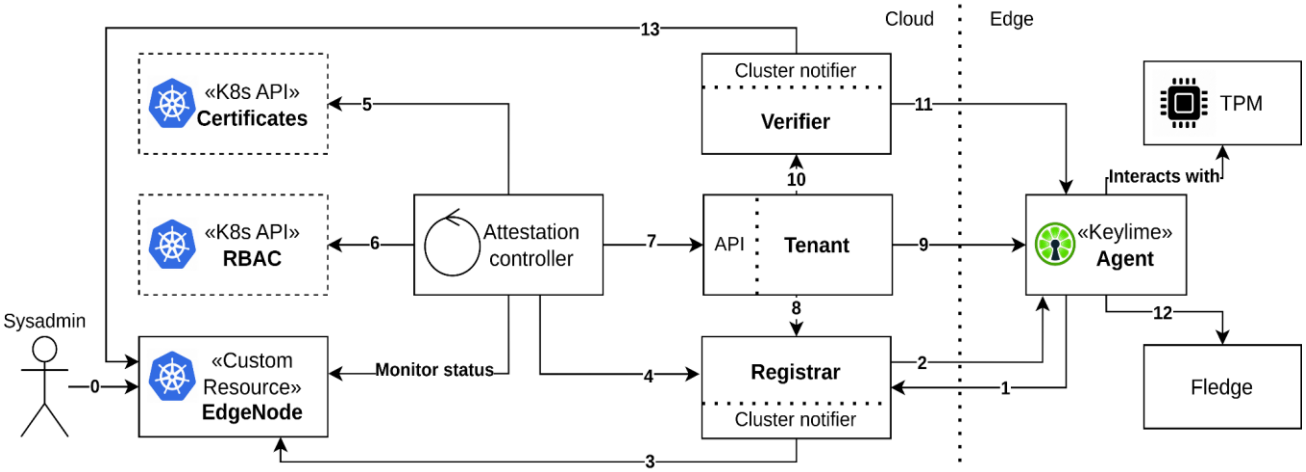


Figure 15. UC 1.3 Modified Kubernetes layout

Green energy availability information will be provided by a Green Energy Monitor agent. For this demonstration, that agent will mock this information.

5.3.2. Use case relevance with NATWORK

UC1 .3 aligns with objectives O1 and O2. Workloads in this context will refer to any service or container (including those running CNFs) that needs to be provisioned within available infrastructure. Both reactive and proactive methods, such as those based on predicted green energy availability and security features supported by nodes, will be examined. The scheduling algorithms will attempt to (re)allocate applications, considering their trust requirements, resource consumption requirements, and limitations (e.g., deadlines and budget), to available resources with a focus on those powered by renewable energy sources. Given the expected dynamic nature of green energy availability and node features, a decentralized scheduling mechanism utilizing federated learning is necessary to prevent local and global oscillation behavior. The aim of this use case is to investigate and demonstrate the applicability of novel secure workload runtimes (e.g., MicroVM/WebAssembly) in such highly dynamic execution environments. These runtimes exhibit trade-offs between security, energy efficiency, and resources, which are only partially exploited by SotA scheduling algorithms. The demonstration

will illustrate that runtime-aware scheduling can improve workload security while reducing overall energy consumption and prioritizing green energy sources. The demonstration will be conducted on the imec Virtual Wall infrastructure, with documentation provided for reproducibility. Desirable extensions for this use case include integration with decentralized orchestration from UC1 .1 and enhancements to workload security resulting from UC1 .2, and document the expansion of demonstration deployment scale to UEssex-imec digital infrastructure.

The key tasks that align with UC1 .3 are summarized and highlighted in Table below.

Table 18. UC 1.3 relevance with NATWORK's tasks

Associated tasks	Focus Areas	Objectives	Key Activities
T2.1	Orchestration and attestation State of the Art	Detailed State of the Art analysis about cloud-edge orchestration, net-zero and device attestation and Trust	Alignment of proposed solution in respect of the SoA analysis.
T3.1	Secure-by-design federated slice orchestration and management	Optimal selection and distribution of microservices/network-function and their runtime artifacts (e.g. VMs, containers, WebAssembly).	Development of the Feather orchestrator and workload placement algorithms
T4.2	AIaaSecS for software payload	Uniform device and user attestation algorithms as a base for a method to ensure the integrity of payload manipulation actions, particularly novel approaches for offline attestation.	The development of the trust-edge Attestation framework integrating with the Feather orchestrator.

As Figure 16 below shows, Use Case 1.3 encompasses a broad spectrum on the security-performance axis because it shows the platform can make this trade-off at real time by choosing to schedule workloads to use hardened security measures that have slight performance penalties. It also encompasses the spectrum of the sustainability-performance axis because it shows the platform can make this trade-off at real time by choosing from a subset of green energy-abundant datacentre locations.

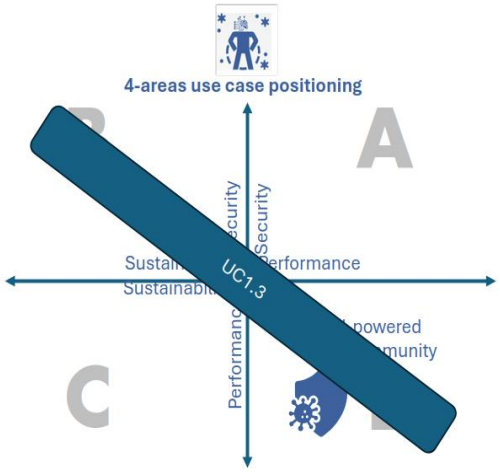


Figure 16. UC 1.3 position on NATWORK's conceptual graph

5.3.3. Definition of the use case KPIs

The following additional KPIs beyond the grant agreement have been defined.

- KPI 1.5: 100% denial of credentials of devices running non-trusted software.
- KPI 1.6: Additional latency of attestation below target value.

Based on the State-of-the-Art analysis, the defined KPI values are depicted in the table below.

Table 19. UC 1.3 used KPIs

KPI	Target value
A-KPI 1.8	100% denial
A-KPI 1.9	Additional latency at runtime: below 2% Additional latency at device deployment time: <1minute

5.3.4. Description of the use case testbed requirement

5.3.4.1. CloudNativeLab

Kubernetes testbed that allows the creation of individual Kubernetes clusters. Features:

- Login with SLICES-SC or Fed4FIRE+ credentials
- Deploy k8s cluster
- Choose #nodes #ram

- Receive VPN config
- Receive k8s credentials

CloudNativeLab WebUI available at https://practicum.cloudnativelab.ilabt.be

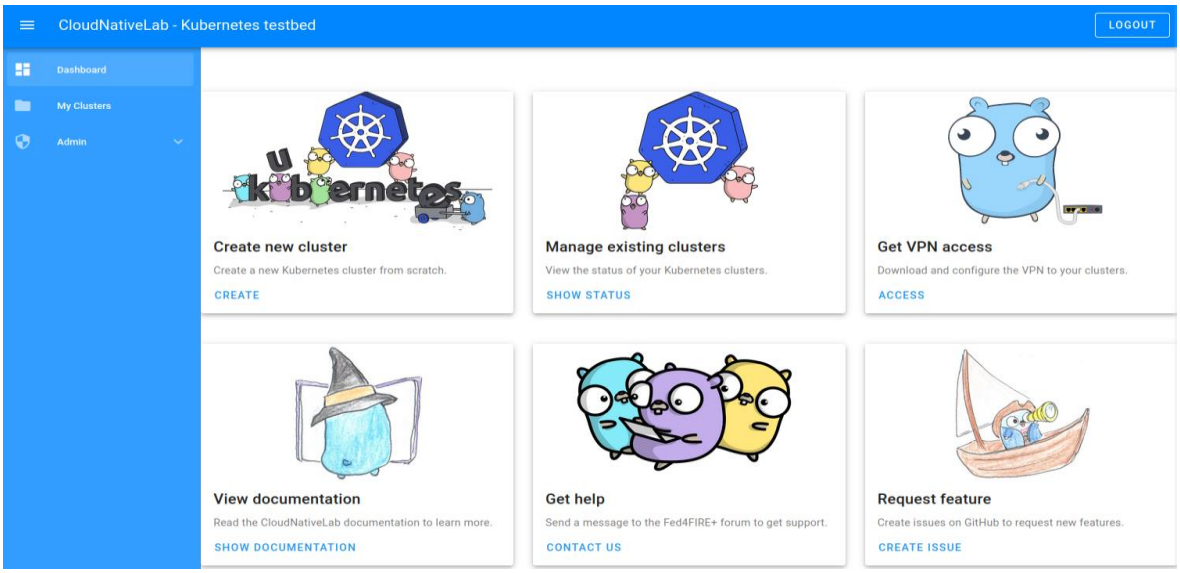


Figure 17 UC 1.3 CloudNativeLab main panel

CloudNativeLab Architecture

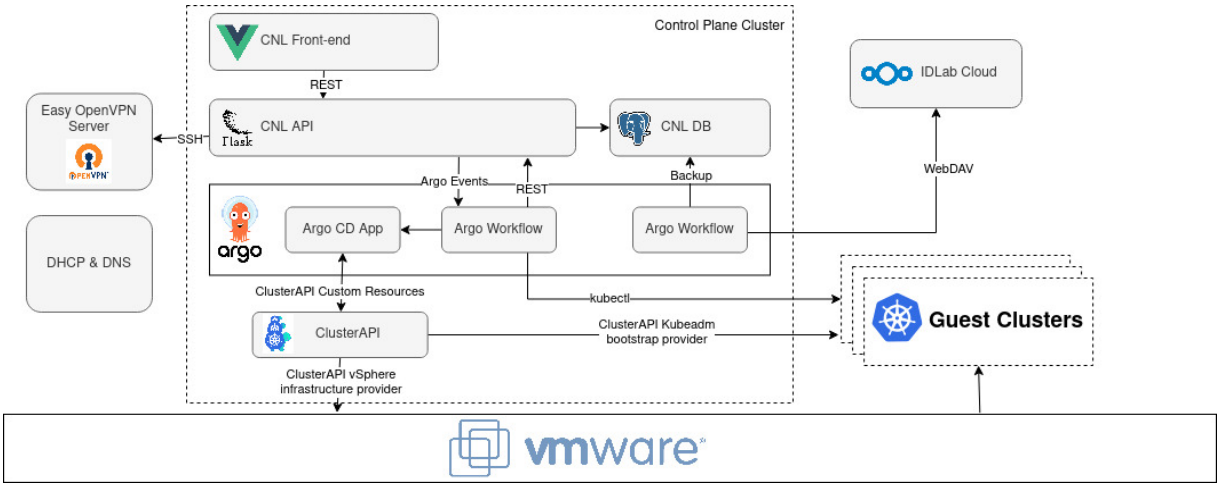


Figure 18. CloudNativeLab architecture

CloudEdgeLab

"Metal as a Service" testbed supporting the provisioning and deployment of specialized edge devices.

Features:

- Login with SLICES-SC or Fed4FIRE+ credentials
- Specialised hardware with
  - TPM
  - Arm TrustZone
  - NVIDIA GPU (Jetson)
- Remote Attestation
- Network connectivity to CloudNativeLab

CloudEdgeLab Architecture

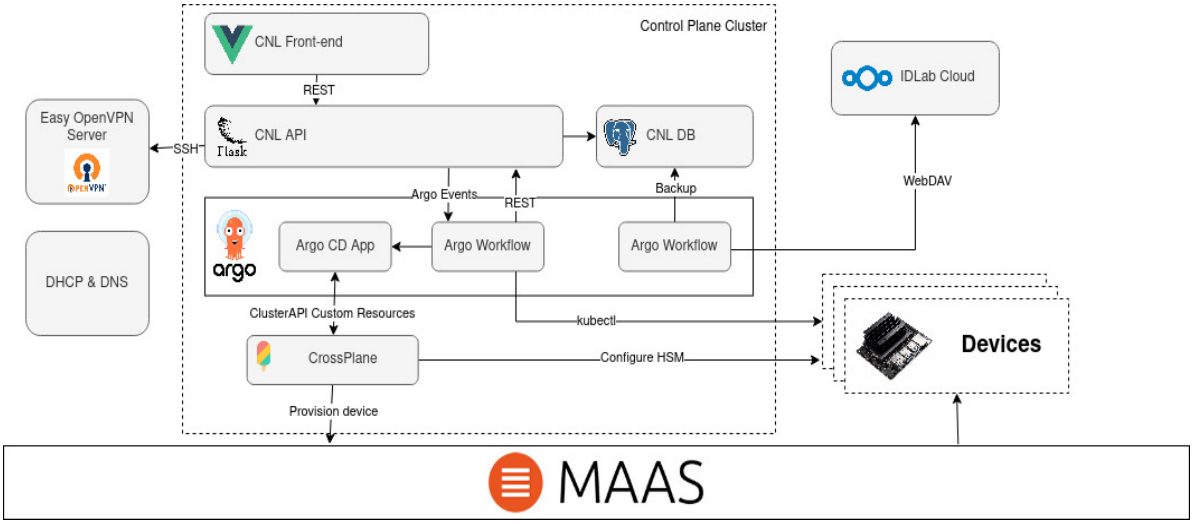


Figure 19. UC 1.3 CloudEdgeLab architecture

5.3.5. Sequence diagram of use case workflow

The first workflow shows the initial discovery, attestation, and registration of remote devices based on trust profile.

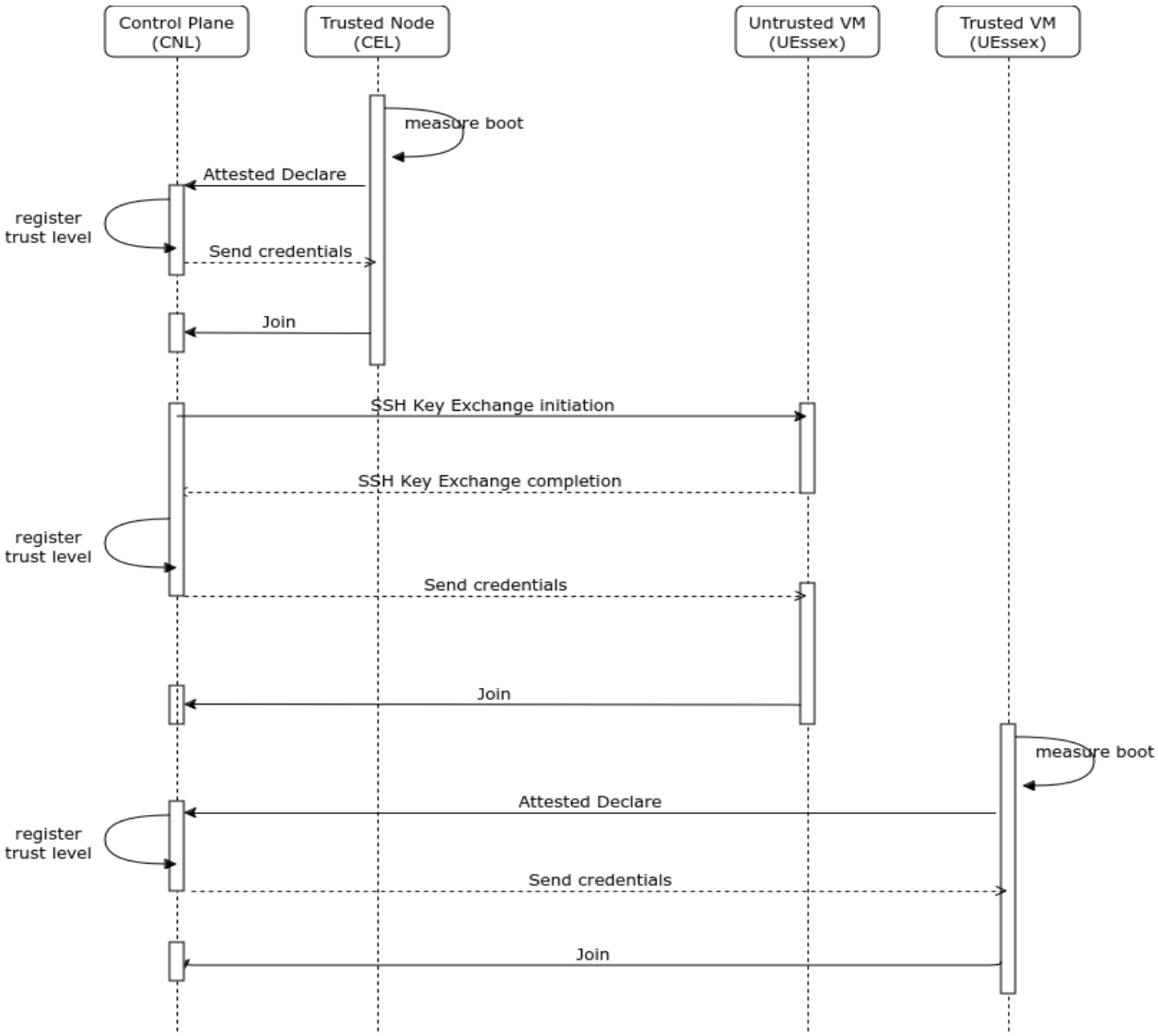


Figure 20. UC 1.3 Initial discovery and attestation sequence diagram

The second workflow shows the deployment of a trusted and untrusted workload at a time when UEssex has high green energy availability, making it a preferred compute location.

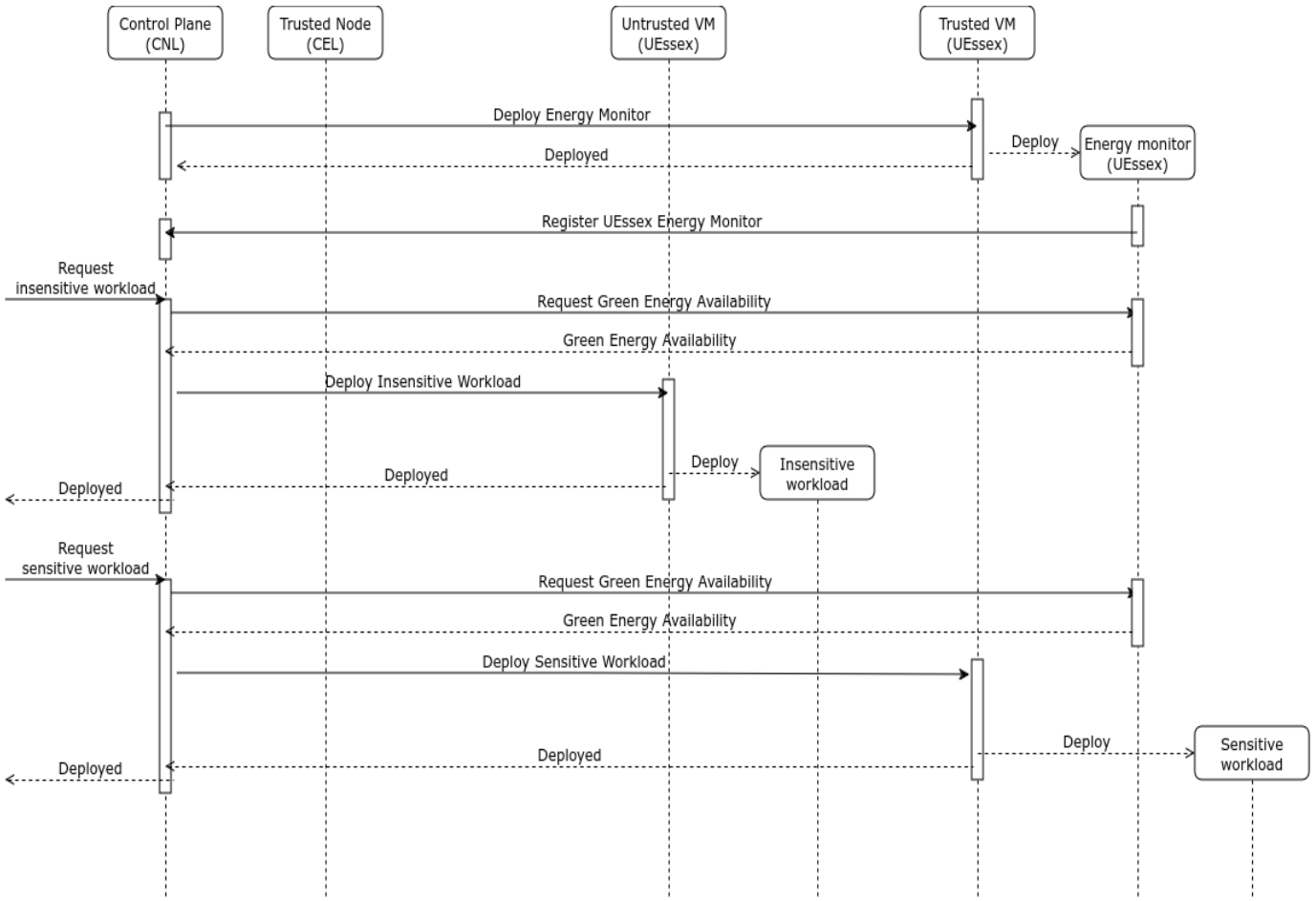


Figure 21. UC 1.3 Trusted payload deployment sequence diagram

5.3.6. Timeline and Risks

5.3.6.1. Timeline

1. **Preparatory development (Months 1-12)**:
    - **Activities**
        - **State of the Art (SoA) Analysis:** Detailed SoA analysis about cloud-edge orchestration, net-zero and device attestation and Trust
        - **Feather**: Development of the Feather orchestrator and workload placement algorithms
        - **Trust-edge**: The development of the trust-edge Attestation framework integrating with the Feather orchestrator.
    - **Results**

- Have an initial device at imec datacentre, which we attest the software and decide based on the attestation whether the device is added or not.
- Have an initial k8s cluster in imec CloudNativeLab connected to a Feather device.

2. **Testbed preparation and integration (Months 13-24)**:

   - **Activities**
     - **Feather net-zero integration:** Integration of net-zero algorithms in the proposed orchestrator.
     - **Trust-edge scheduling integration**: Integration of trust-edge attestation into k8s scheduling.
     - **CloudEdgeLab preparation**: Setup of the remote attestation-enabled hardware testbed at imec datacentre.
     - **UEssex testbed integration:** Integration with the UEssex testbed for untrusted nodes.
   - **Results**
     - A running CloudEdgeLab testbed ready to accept workloads.
     - Have a PoC cluster running with a control plane in CloudNativeLab, and devices in CloudEdgeLab, UEssex untrusted VM.

3. **Testing and enhancement (Months 25-30)**:

   - **Enhanced Solution (Month 25-30)**: The impacts of T5.3 and T5.4, as well as the transfer of the implemented methods and techniques from the simulation environment to the experimental testbed, will be executed progressively. During this phase, extensive testing and validation activities will be conducted.

4. **Final Phase (Months 31-36)**:

   - **Final System Integration and Evaluation (Month 32)**: Complete the integration of all components and perform a full-scale evaluation of the net-zero trusted workload placement.
   - **System Validation and Lessons Learned (Month 36)**: Final validation will be conducted, and the lessons learned will be documented for future iterations and deployments in real-world 6G environments.

5.3.6.2. Risks

The main risks in terms of UC 1.3 are collectively presented as:

1. **Integration of software components**:
    - **Risk**: Integration efforts between Feather and trust-edge fail because of incompatible interfaces and hardware
    - **Mitigation**: Integration between Feather and trust-edge will be cyclically tested during initial development of both solutions.
2. **Integration between imec and UEssex testbeds**:
    - **Risk**: Integration efforts into the UEssex testbeds because of incompatible interfaces and hardware
    - **Mitigation**: Integration with the UEssex testbed will start early with a clear description of testbed hardware and software requirements and will be verified and coordinated during UC1 meetings.

5.3.7. Summary

This demo shows a multi-location compute mesh capable of choosing compute locations based on green energy availability and workload trust requirements. The imec CNL will be used as the control plane of the platform, with remote devices in imec CEL, and UEssex infrastructure. This use-case will show the technical feasibility of trustworthy net-zero payload placement while ensuring the security, integrity and confidentiality of the workloads and data.

6. Use case 2. Anti-Jamming Technologies for AVS

6.1. Use case 2.1 Enabling Multi-antenna for resilience

Considering that the foreseen prevalence of Autonomous Vehicles (AV) areis expected to become prevalent in the coming decades, both for individual cars and public transportation, ensuring the security of communication between these vehicles and the outside world is of utmost importance. In addition to implementing cybersecurity measures, it is essential to develop protection mechanisms at the physical layer of the communication link. A major task is the protection of the communication links in the physical layer from interference noise sourced by jamming attacks. Within the context of NATWORK project, MIMO setup capabilities will be exploited for the detection and the mitigation of the jamming attacks. a multi-antenna setup will be employed to effectively detect jamming attacks. The detection module must be designed with exceptionally high accuracy to cover all a wide range of known types of jamming attacks. Furthermore, real-time strategies for mitigating jamming attacks need to be thoroughly investigated and developed. All these activities are covered by UC 2.1. The detection module must be robust in the type of jamming attacks, that mainly are classified based on the time duration of the interference noise and the synchronization with the legitimate transmitter operation. Furthermore, real-time strategies for mitigating jamming attacks need to be thoroughly investigated and developed. All these activities are covered by UC 2.1.

6.1.1. General functional description

Protecting Vehicle-to-Everything (V2X) networks from physical layer attacks involves addressing several critical aspects, one of which is the protocol utilized by V2X links. The primary protocol in use is currently IEEE 802.11p.

The IEEE 802.11p protocol, also known as Wireless Access in Vehicular Environments (WAVE), is an extension of the IEEE 802.11 standard, specifically designed for wireless communication in vehicular environments. It facilitates data exchange between high-speed vehicles and between vehicles and roadside infrastructure, enabling both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. The main objective of this protocol is to support applications that enhance road safety and improve traffic conditions.

Key features of IEEE 802.11p include its operation in the 5.9 GHz frequency band, which is reserved by the Intelligent Transportation Systems (ITS) and specifically spans the 5.850-5.925 GHz range. The protocol supports a maximum range of 1 km, although this range can be diminished by environmental factors and obstacles. IEEE 802.11p is designed for non-directional broadcasting, making it suitable for communication with nearby vehicles. It also boasts low latency, which is crucial for safety applications such as collision avoidance and emergency message transmission. Additionally, the protocol is optimized to handle the high relative velocities between moving vehicles. IEEE 802.11p serves as the physical (PHY) and medium access control (MAC) layer technology for Dedicated Short-Range Communications (DSRC). The main properties of the protocol PHY are illustrated in the table below. The protocol can support different modulation schemes for both reception and transmission such as Binary Phase-Shift Keying (BPSK), Quadrature Phase-Shift Keying (QPSK), 16-Quadrature Amplitude Modulation (16-QAM), 64-Quadrature Amplitude Modulation (64-QAM).

Table 20. Main PHY properties of IEEE.802.11p

Parameter	Value
Bandwidth	10MHz
OFDM subcarrier	64
Subcarrier spacing	156 KHz
OFDM symbol time	8 µs
Guard time	1.6 µs
Comb Pilot Spacing	2.2 MHz

Detection of jamming attacks in wireless communication systems has been explored through various approaches, utilizing different metrics and features. Commonly employed metrics include signal-related parameters such as signal strength, signal-to-noise ratio (SNR), and signal variance, as well as network traffic features like Packet Delivery Ratio (PDR) and Packet Loss Rate. Additionally, frequency domain features, such as spectrograms, have been used for this purpose.

In [19], the authors selected bad packet ratio, packet delivery ratio, received signal strength, and clear channel assessment as key parameters for detecting jamming attacks. These metrics were chosen because they can be easily estimated through the diagnostic mechanisms available in network interface cards across communication systems. Similarly, [20] categorizes features into three main types: Channel Metrics (e.g., Noise and Channel Busy Ratio), Performance Metrics (e.g., PDR and Maximum Inactive Time), and Signal Metrics (e.g., Minimum and Maximum Signal Strengths). This study employs Random Forests for the analysis and prediction of jamming incidents, demonstrating the effectiveness of these features in detecting attacks.

In another study[21], a range of Quality of Service (QoS) metrics, including Overall Network Throughput, Number of Packets, Application Layer Delay, TCP Round Trip Time (RTT), and TCP Re-transmissions, were measured. The authors experimented with multiple machine learning models and distinguished LSTM capability in jamming detection domain.

Furthermore, [22] investigates the use of features such as Delivery Rate (PDR), SNR Mean, SNR Variance, SNR power spectral density (PSD), and Cross-Correlation Peak. A shallow neural network with a single hidden layer containing 10 neurons has been deployed.

Lastly, [23] demonstrates a common approach involving the extraction of statistical features from signals. The authors extracted seven descriptive statistics—minimum, maximum, mean, standard deviation, and percentiles—for each window sequence, transforming it into a single feature set. After this preprocessing, different machine learning models like MPL, SVM, RAF, XGBoost, and LGBM have been tested. The accuracy levels of the current existing works in jamming detection are included in below

Table 21. Accuracy in jamming detection of the existing works

Existed Work	Jamming Detection Accuracy
[19]	97.5 %
[21]	99.5%
[22]	95-99%
[23]	99%

In terms of mitigation of jamming attack, the work in [24] presents a jamming-resilient receiver designed to protect vehicular communications from high-power constant jamming attacks. This receiver integrates two key components: a jamming-resistant synchronizer and a jamming suppressor, both leveraging MIMO principles. The solution addresses challenges in the 802.11p OFDM protocol by enabling reliable packet detection, synchronization, and channel equalization, even in the presence of jamming.

The receiver operates by identifying and synchronizing with legitimate signals, then effectively mitigating the jamming interference. It utilizes the IEEE 802.11p frame structure to estimate jamming impact and recover desired packets without needing detailed channel information from the jammer. The system's robustness was demonstrated through experiments across various vehicular scenarios, confirming its ability to maintain communication integrity under intense jamming conditions.

One common challenge in MIMO-based solutions for jamming mitigation is the need for precise Channel State Information (CSI) regarding the jammer, which is often difficult to acquire in real-

world scenarios. In response to this, the authors of [25] propose a practical anti-jamming solution that eliminates the need for any channel information, making it highly suitable for real-world wireless networks. Their approach includes a jamming-resilient synchronization algorithm and a Blind Jamming Mitigation (BJM) algorithm, which can cancel jamming signals from multiple unknown sources and equalize the channel to recover legitimate signals. They developed a multi-antenna jamming-resistant receiver (JrRx) that incorporates the BJM algorithm, and they demonstrated its effectiveness in a Wi-Fi network through experimental evaluations. Unlike previous works that focus on packet delivery rate, this study uses the post signal-to-jamming-plus-noise ratio (pSJNR) as the performance metric. The experimental results showed that as long as the receiver has more antennas than the jammers, JrRx can successfully decode signals even when jamming signals are 20 dB stronger than the transmitted signal, demonstrating its robustness against various jamming patterns.

In another study [26], the exploration of MIMO techniques as active defense mechanisms against jamming led to the development of a variation of spatial multiplexing called vSP4. This technique achieves high throughput and stable diversity gain despite interference from malicious jammers. Simulation results indicated that the vSP4 scheme significantly enhances both throughput and reliability in the presence of jamming, outperforming classic schemes such as Alamouti and Spatial Multiplexing. The performance of the proposed solution was evaluated in a Vehicular Ad-hoc Network (VANET) environment under various channel conditions using the integration of the GEMV tool in the VEINS simulator.

6.1.2. Use case relevance with NATWORK

The mapping of the UC2 .1 in respect of NATWORK's conceptual graph is represented in Figure 22.

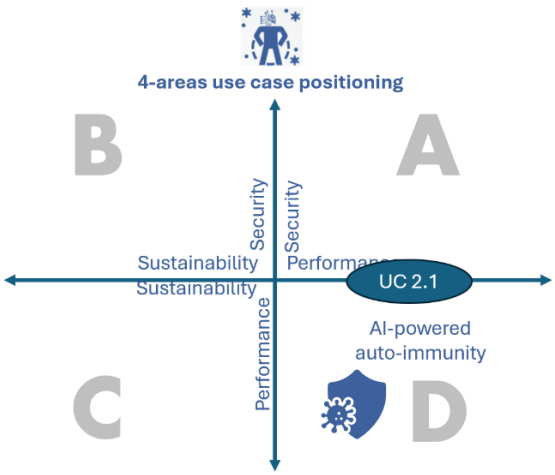


Figure 22. Use case 2.1 position on NATWORK's conceptual graph

The key tasks that align with UC2.1 are summarized and highlighted in Table 22.

Table 22. UC 2.1 Relevance with NATWORK tasks

Associated tasks	Focus Areas	Objectives	Key Activities
T5.1	Threat modelling for physical layer	Full and detailed SoA about all the possible attacks in physical layer. Categorization based on techniques and protocol.	Alignment of proposed solution for detection and mitigation in respect of the SoA analysis.
T5.3	AI-leveraged anti-jamming	Detection and mitigation of a jamming attack in mmWaves and THz bands. Utilization of beamforming techniques and adaptive modulation as a jamming protection method. Investigation of Physical Layer Key Generation (PKG) usage	Investigation of the capability of model detection to be implemented in other frequency bands. Usage of the proposed techniques for the protection of the V2X communication link.
T5.4	MIMO & RIS Surface Defense Mechanism	Usage of RIS and MIMO for enhanced communication links quality. Usage of RIS for beam-splitting, sensing and localization purposes within the communication network for further safety and protection.	Investigation of the benefits for the detection and mitigation based on MIMO and RIS capabilities.

The KPIs are the following:

- KPI2.1: Jamming attacks detected and mitigated (increase of at least 30% in the detection of attacks)
- KPI2.2 Time needed to detect and prevent a jamming attack (in the order of a few seconds, target <5s)
- KPI2.3 Time needed to recover from a jamming attack (reduction by 30% in the order of seconds)
- KPI2.4 Downtime prevented (less downtime at least 20%)
- KPI2.5 Throughput enhancement during jamming attack of at least 40%

Based on the SoA analysis, the defined KPI values are depicted in the table below.

Table 23. UC 2.1 KPIs and target values

KPI	Target value
KPI2.1 Jamming Attacks detection	99.99% in all the modulation schemes, with different SNR levels and jamming attacks type.
KPI 2.1 Jamming Attacks mitigation	Overcome existing synchronization issues.
KPI 2.2	4s
KPI 2.3	5s
KPI 2.4	Not relevant
KPI 2.5	Throughput metric will be replaced by a similar one, available in experimental testbed At least 10%

6.1.3. Description of the use case testbed requirement

In the CERTH lab, the anti-jamming system experiments use specific equipment and setups. It is illustrated in Figure 23. The core component is the SDR (Software Defined Radio), which is programmed using GNU Radio, an open-source software platform for signal processing. The SDRs are connected to USRPs (Universal Software Radio Peripherals), which serve as the hardware interface for transmitting and receiving radio signals. The USRPs provide a flexible API compatible with GNU Radio, allowing seamless integration between software and hardware.

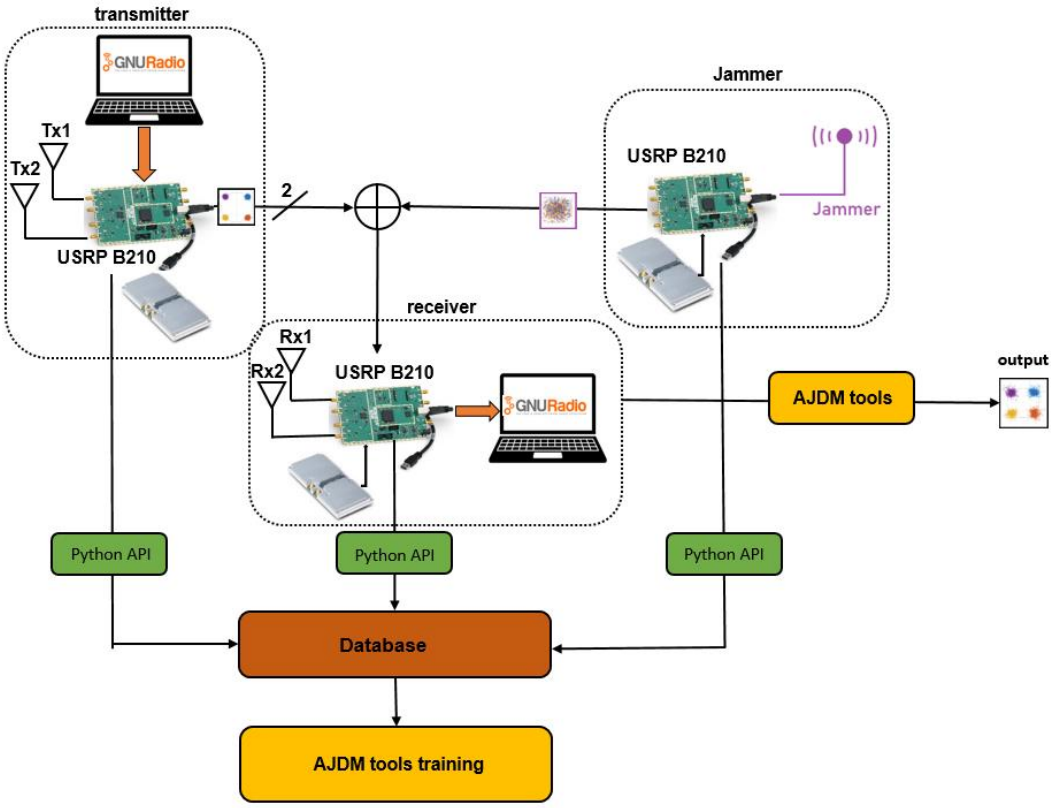


Figure 23. UC 2.1 CERTH Experimental Testbed Architecture

The lab setup consists of a transmitter, receiver, and jammer, all arranged in a controlled environment to minimize external interference. The equipment operates at 5.9 GHz, the frequency designated for the 802.11p protocol, primarily used ITS and V2X communications. The transmitter and receiver are placed 3 meters apart, while the jammer antenna is positioned between them to emit interference signals during the tests. The system uses a 10 MHz channel width for communication. The main workflow of the UC 2.1 is illustrated in the UML diagram illustrated in Figure 24.

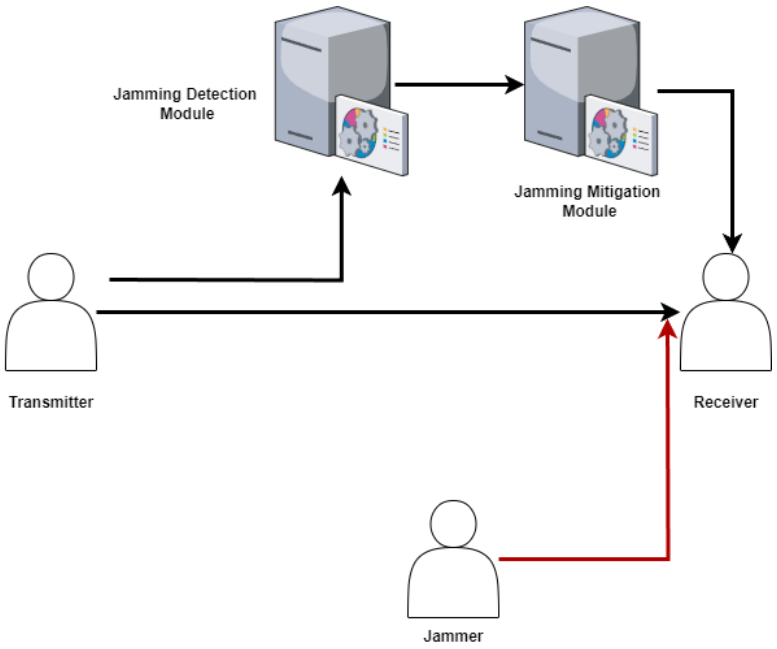


Figure 24. Abstract UML diagram for UC2 .1 workflow

All equipment is configured to allow real-time monitoring of signal quality and strength at the receiver, with the aim of evaluating the effectiveness of anti-jamming measures. The data collected from the experiments is stored in a shared database for further analysis. The testbed is illustrated in Figure 25.

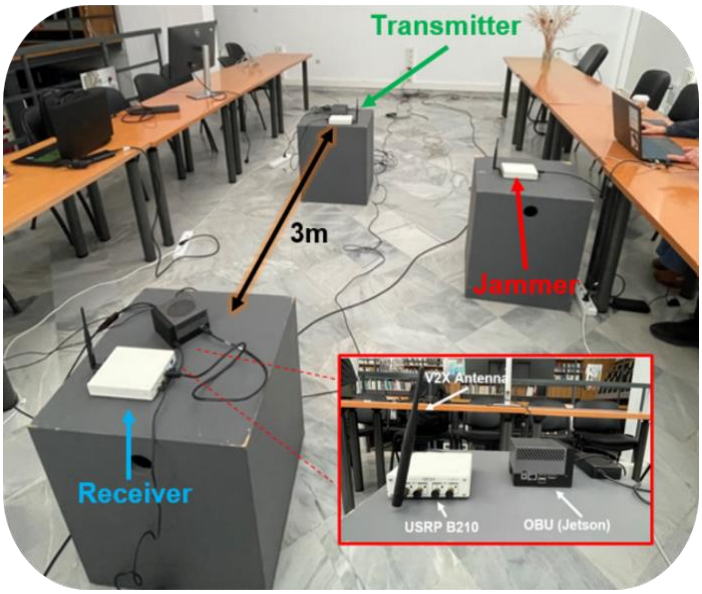


Figure 25. CERTH lab with experimental testbed

6.1.4. Sequence diagram of use case workflow

Figure 26 presents the sequence diagram for UC 2.1. As shown, it consists of three key elements: the main activities of UC, the components that initially form the jamming model and mitigation module, and the input to be integrated from the tasks outlined in the previous section.

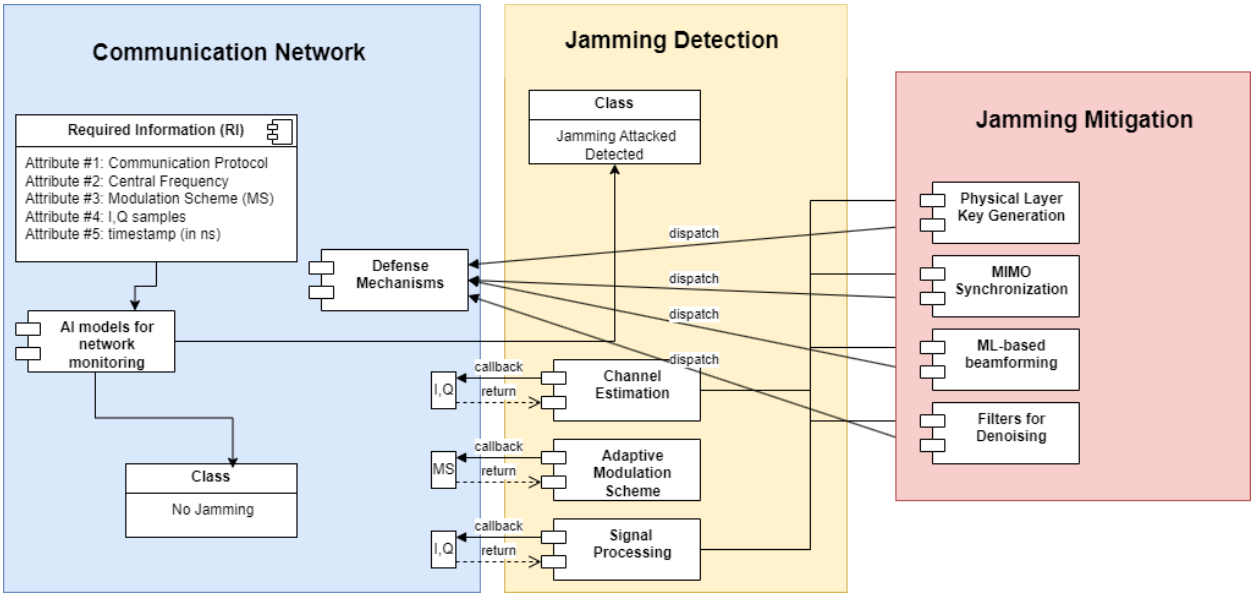


Figure 26: Sequence Diagram of UC2 .1

The jamming detection model encompasses several components in a specific time sequence: the execution and precise simulation of IEEE 802.11p on the experimental testbed, real-time processing of physical layer information (I,Q samples) from the SDRs to a central database, and the application of signal processing techniques. Additionally, it involves building and training an AI/ML model for efficient and highly accurate detection, with LSTM and CNN models being the primary candidates. Various architectures, approaches, and combinations will be explored to determine the optimal solution.

Regarding the jamming mitigation module, the initial step involves defining and implementing a MIMO setup in the experimental testbed, ensuring it meets the minimal required specifications. Signal processing techniques, such as synchronization and channel estimation, are crucial tasks but can present challenges, particularly in MIMO configurations. Following this, appropriate filters and denoising mechanisms will be developed to mitigate constant, reactive, and periodic jammers. The main activities of UC2 .1 accompanied with the required by Task inputs are illustrated in Figure 27.

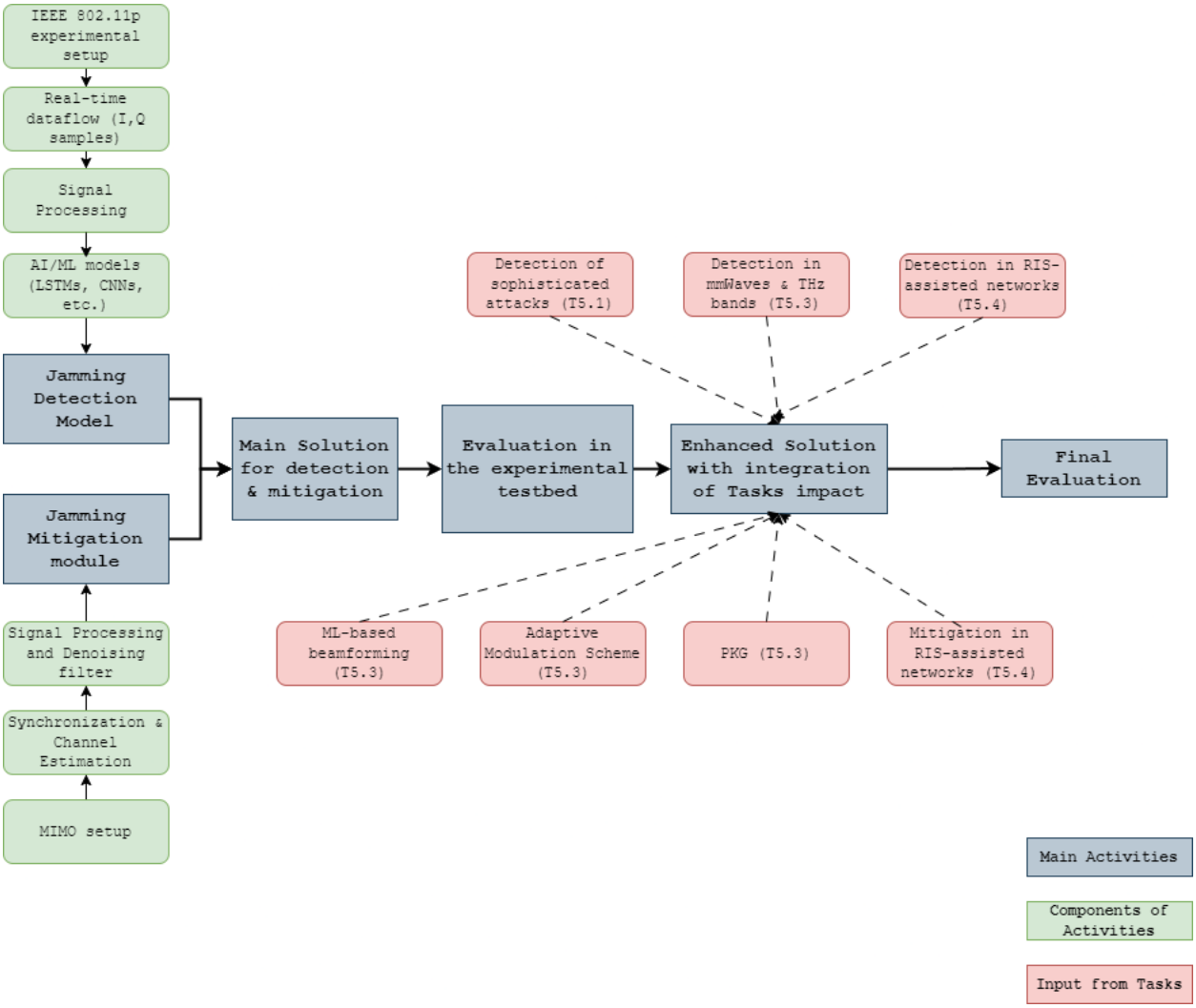


Figure 27: Main Activities of UC 2.1

Afterward, the two modules will be integrated into a unified solution, which will be evaluated using the experimental testbed. This will serve as the primary solution. Once this stage is completed, work on the enhanced solution will begin. In this phase, input from tasks T5.1, T5.3, and T5.4 will be incorporated where applicable. Key enhancements to the primary solution include extending the model to detect more sophisticated and cutting-edge jamming attacks, expanding its functionality to B5G/6G frequency bands, and enabling cooperation with RIS units. For mitigation, the system could be equipped with ML-based tools for beamforming, adaptive modulation techniques, and a PKG approach to provide a-priori protection. Additionally, the RIS-assisted network, with its advanced sensing and localization capabilities, could offer valuable insights into the jammer's characteristics.

6.1.5. Timeline and Risks

6.1.5.1. Timeliine

In UC 2.1, the jamming detection and mitigation mechanism will be systematically evaluated according to its sequence diagram. In addition to the primary activities, inputs and results from T5.1, T5.3, and T5.4 will be integrated to the extent possible, and this integration must be reflected in the UC timeline. Additionally, a collaboration with UC2.2 will be established to evaluate the proposed services and investigate jamming detection across multiple communication protocols. The specific time plan is specifically:

1. **Initial Phase (Months 4-12)**:
    - **Selecting Jamming Attacks:** The jammer will be equipped with state-of-the-art jamming techniques, including advanced methods such as frequency hopping, deceptive jamming, pulse jamming, and smart jamming strategies that adapt in real-time to the target signal's characteristics to maximize disruption efficiency.
    - **Jamming Detection Model**: The most appropriate AI/ML models for jamming detection will be evaluated to protect against selected jamming strategies. Various architectures and innovative methods will be assessed to improve accuracy and robustness with respect to different types of jamming attacks and network properties.
    - **Jamming Mitigation Mechanism**: Signal processing techniques in conjunction with AI/ML tools, will be investigated for channel estimation both with and without the presence of a jammer. Additionally, suitable denoising filters will be defined.
    - **Task T5.1:** A SoA analysis of physical layer attacks, including edge cases and potential dangers, will be conducted to ensure that the proposed solutions are aligned with the current challenges in the domain.
2. **Development Phase (Months 13-24)**:
    - **Main Solution**: The integrated main solution will be completed by month 18. This solution will serve as the foundation for incorporating contributions from relevant tasks.
    - **Evaluation of the main solution in the experimental testbed (Month 18)**
    - **Task T5.3**: Expanding the detection model to higher frequency bands will be the subsequent step after the main solution is completed. Additionally, extra protection mechanisms, including ML-based beamforming, adaptive modulation schemes, and PKG, will be examined. Following development and evaluation in a simulation environment, these mechanisms will be progressively integrated into the main solution.

- **Task T5.4:** Initially, an examination of the RIS units and their capabilities will be conducted. The specific RIS functionalities of interest will be delineated, focusing on how these functionalities can enhance detection, mitigation, and the identification of jammer properties. Additionally, a codebook for the RIS will be developed.

3. **Testing and Validation Phase (Months 25-30)**:
   - **Enhanced Solution (Month 25-30)**: The impacts of T5.3 and T5.4, as well as the transfer of the implemented methods and techniques from the simulation environment to the experimental testbed, will be executed progressively. During this phase, extensive testing and validation activities will be conducted.
4. **Final Phase (Months 31-36)**:
   - **Final System Integration and Evaluation (Month 32)**: Complete the integration of all components and perform a full-scale evaluation of the anti-jamming system performance and robustness.
   - **System Validation and Lessons Learned (Month 36)**: Final validation will be conducted, and the lessons learned will be documented for future iterations and deployments in real-world 6G environments. The feasibility of performing a final evaluation under real conditions at CERTH AV will be assessed from both technical and legal perspectives.

6.1.5.2. Risks

The main risks in terms of UC 2.1 are collectively presented as:

1. **Synchronization and Channel estimation in MIMO networks**:
   - **Risk**: Synchronization and accurate channel estimation in MIMO networks face various challenges, compounded by limitations of current experimental testbeds.
   - **Mitigation**: Advanced techniques, including sparse methods and AI, will be employed to ensure precise and timely estimations.
2. **Utilization of AI/ML tools in the real-time conditions**:
   - **Risk**: AI/ML tools can add computational delays, which need to be minimized to ensure practical utility.
   - **Mitigation**: Parallel techniques and lightweight solutions will be explored to reduce computational time.
3. **RIS Codebook procedure**:
   - **Risk**: Developing a RIS Codebook that includes all necessary functionalities is challenging and time-consuming.

- **Mitigation:** Combining physics-based knowledge with metaheuristic tools will help shorten the training period.

4. **Integration of the components**:
   - **Risk**: The diversity of proposed solutions and their complex integration could result in a highly complex system.
   - **Mitigation**: The final solution will include only essential components, designed for optimal cooperation and flexibility.

6.1.5.3. Summary

Use Case 2.1 from the NATWORK project focuses on enhancing the protection and resilience of Autonomous Vehicles (AV) against jamming attacks by employing a multi-antenna system. The primary goal is to develop and implement a detection module capable of identifying and mitigating various jamming attacks in real-time, leveraging the IEEE 802.11p protocol used for Vehicle-to-Everything (V2X) communication

The Use Case also integrates mitigation strategies, such as a jamming-resilient receiver that uses MIMO principles to maintain communication integrity. Key performance indicators (KPIs) for this use case include high detection accuracy, rapid response times, and effective throughput enhancement during attacks. The experimental setup includes Software Defined Radios (SDRs) for real-time testing and validation. The described timeline spans from initial phases of model evaluation to final integration and system validation, with careful attention to challenges like synchronization, AI/ML tool efficiency and RIS-assisted environments, as they will be investigated in the respective tasks.

6.2. Use case 2.2 Empowering AI-based jamming detection and mitigation for multi path routing

6.2.1. Domain description

In this use case we will showcase NATWORK's novel approach that combines jamming detection and selection of countermeasures into a unified process and investigate innovative AI-driven techniques that consider both phases of jamming detection as a comprehensive process, ultimately contributing to the security of 6G networks. Also, the developed algorithms will be able to demonstrate the routing of traffic through multiple paths to avoid jammed channels and ensure that the communication is not affected by jamming attacks. Finally, our machine learning-driven anomaly detection approach for pinpointing jamming attacks will be supported by an AI-

supported jamming signal identification and characterization process, reinforced by a learning-based decision-making solution for effective jamming mitigation.

6.2.1.1. Functional requirements and challenges

Table 24. UC 2.2 Requirements and challenges

Functional requirement	Description	Associated challenges
Spectrum monitoring	Spectrum must be monitored to inspect the signals present at a given frequency and extract the key features (e.g. SINR) to perform the detection of jamming signals.	Key features must be properly defined and extracted.
Jamming detection	Identification of jamming signals, as they will usually be masked by legitimate signals.	Different algorithms must be evaluated to implement a SotA solution with high enough performance
Jamming mitigation	Action/countermeasures to mitigate jamming attacks such as frequency hopping or adaptive beamforming.	Check the feasibility of different mitigation techniques in the context of a 5G-like scenario
Multi-path routing	Selection of alternative path to avoid jamming signals.	The re-scheduling or other re-route strategy must be done in a “pseudo-5G” network

6.2.1.2. Enumeration of functions

In this UC, the following functions will be implemented in our DetAction module:

- Signal key feature extraction: Before the detection phase, key features from the signal will be extracted, which will later be fed with those parameters obtained from the received signal.
- AI-based jamming detection: using ML/DL algorithms, the received signal will be classified as regular 5G traffic or under-attack traffic.
- Mitigation phase and multi-path routing: using routing the DetAction module will interact with the scheduler to avoid the jamming attack (via PRBs allocation, scheduling, beamforming or a different way to change the attacked channel).

6.2.1.3. High-level functional description (UML)

Below a high-level UML representation of the interaction of the Jammer, UE and gNB (with our DetAction algorithm) is depicted:

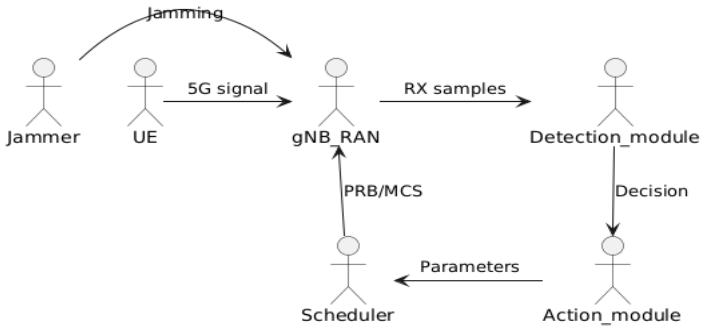


Figure 28. UC 2.2 UML diagram

As shown in the diagram:

- Both the Jammer and UE transmit their signals to the gNB, where they are received by the RAN, and after processing the received samples, they are sent to the DetAction module, which will receive them with the detection phase first.
- There, relevant metrics will be extracted to be used by the detection module in the classification of the received signal as either regular 5G or under-attack.
- With this decision, the action module will communicate with the scheduler to re-route the communication to a channel where the jamming attack is avoided.

6.2.1.4. Challenges taken up by the use case

In order to develop the DetAction module and implement it in this UC, some challenges should be overcome:

- Signal dataset development: in order to train the AI algorithms, a large enough dataset of both jamming and regular 5G signals must be obtained.
- ML/DL train and validation with 5G signals.
- 5G traffic re-routing to avoid the jamming attack, with the interaction between the DetAction module and the scheduler one of the main possible challenges.

6.2.2. Use case relevance within NATWORK

NATWORK's core objectives are i) reconcile performance, sustainability and security and ii) develop AI-powered self-resilience against novel threats. This use case is aligned with the AI-powered autoimmunity as the essential target of use case 2.2 is the detection of jamming attacks through AI-based mechanisms but, at the same, its position over the right part of the horizontal axis reflects the fact that security and performance are very relevant for the use case.

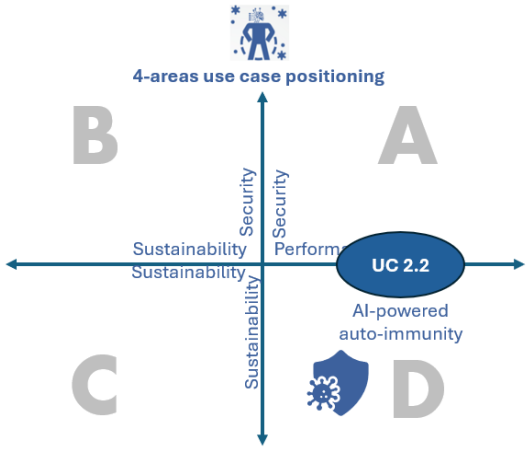


Figure 29. Use case 2.2 position on NATWORK's conceptual graph

6.2.3. Definition of use case KPIs

UC 2.2 will initially consider the following KPIs:

- KPI2.1 Jamming attacks detected and mitigated (increase of at least 30% in the detection of attacks).
- KPI2.2 Time needed to detect and prevent a jamming attack (in the order of a few seconds, target <5s).
- KPI2.4 Downtime prevented (less downtime at least 20%).
- KPI2.5 Throughput enhancement during jamming attack of at least 40%.

Additionally, the success of adaptive routing over multiple paths shows the effectiveness of the countermeasures against jamming attacks thorough the following KPI:

- A-KPI2.6 Successful establishment of connectivity to avoid jammed channels/paths (improvement of 20%).
-

6.2.4. Definition of use case testbed requirements

As the DetAction module will be implementing ML/DL algorithms over a received 5G signal and discriminate if a jamming attack is present in order to take action, some hardware and 5G libraries may be required to train and tune the implemented algorithms.

- Jamming device
- UE device
- 5G Core and gNB
- USRPs

6.2.5. Sequence diagram of use case workflow

The workflow of the two different possibilities of this UC is shown below:

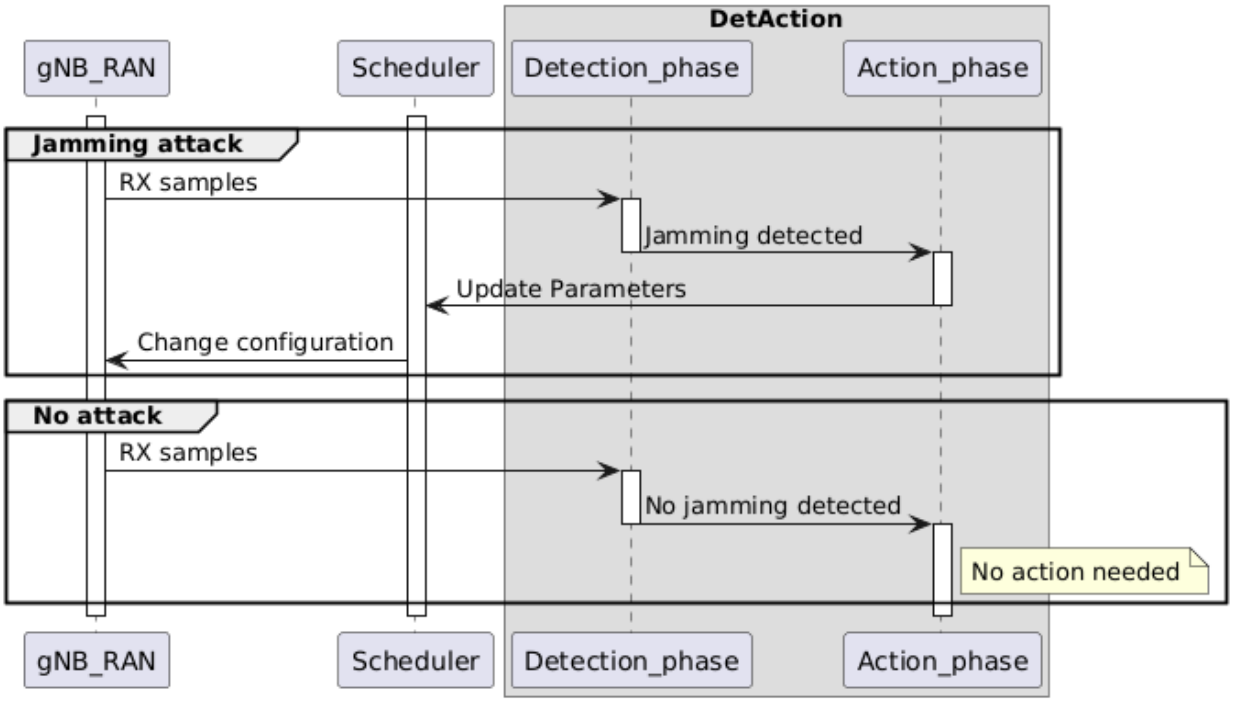


Figure 30. UC2 .2 sequence diagram

In the first scenario, a jamming attack is present on the gNB received signal:

1. The IQ samples received are sent to the detection phase,
2. AI algorithms try to detect the attack and communicate this to the action phase
3. Decision on which changes to apply to the network configuration are needed to avoid the jamming attack, and adjust the scheduler parameters accordingly
4. Finally, the updated scheduling policy (If rescheduling is applied as a countermeasure) will be implemented in the gNB RAN

In the second case, where the received signal is not being attacked:

1. The IQ samples received are sent to the detection phase,
2. AI algorithms will not detect jamming, and that will be sent to the action phase
3. The action function will not act on the scheduler, so it will continue without any notification

6.2.6. Success factors and selected KPIs

As previously mentioned, the KPIs of this UC2 .2 are the ones stated in the proposal. Particularly, KPI 2.1 and 2.5 will imply that the DetAction module can manage jamming attacks, detecting them and improving the communications under them, which aligns with the NATWORK objectives of security and performance.

6.2.7. Timeline and risks

6.2.7.1. Timeline

The timeline is undergoing definition by the different partners involved in this UC, with initial structure outlined below. Some risks associated with this UC are the hardware availability and the 5G network deployment tools (Amarisoft, SRS, etc) options for configuration, both of which might affect the different countermeasures and detection strategies at hand. As the project is at its early stages, the timeline is still a subject of discussion and organization between the different partners involved in this UC. Some risks associated with this are the hardware availability and the 5G network deployment tools (Amarisoft, SRS, etc) options for configuration, both of which might affect the different countermeasures and detection strategies at hand.

Taking those factors into account, an initial estimation of the timeline for the UC would be (over the 36 months of the project):

- Startup: 9 months (considering previous steps needed to begin with the UC design)
- Research, SotA and laboratory setup: 6 months
- Signal DB creation: 3 months (overlapping with the SotA)
- AI algorithms development and train: 8 months
- Integration and testing: 4 months
- Optimization and prototype refinement: 7 months
- Reporting: 2 months

6.2.7.2. Risks

Regarding risks, the primary challenge lies in securing the necessary materials and tools for conducting the tests. More specifically:

- Configuration of 5G scheduler
  - Risk: changing the configuration of the 5G scheduler, even in open-source tools such as OAI, may be challenging.

- Mitigation: Perform the Action functionality at lower layers.

- Utilization of dedicated SDRs
- Risk: The lab environment has limited hardware resources.
- Mitigation: Planification of SDRs resources.

- Signals database
- Risk: training the AI model requires both legitimate UE and jamming signals.
- Mitigation: planification of signals database creation and searching synergies with other NATWORK's partners.

6.3. Use case 2.3 Adaptive modulation techniques for anti-jamming autonomous recovery

6.3.1. Domain description

This use case focuses on the recovery mechanisms, which have the capability to regain lost communication caused by jamming attacks without the need for human intervention. By incorporating AI-powered adaptive modulation specifically designed for dynamic jamming environments such as the ones the AVs are operating in, machine learning-based channel estimation to enable robust modulation selection, and reinforcement learning-based modulation control, the objective is to enhance anti-jamming performance. Ultimately, this will lead to a more resilient communication system that can effectively withstand and recover from a variety of jamming attacks.

6.3.1.1. Functional requirements and challenges

Jamming mitigation: This use case will showcase the ability to mitigate the damage incurred by the jammer to the communication between end user and the network. It will incorporate AI-powered adaptive modulation specifically designed for dynamic jamming environments such as the ones the AVs operating in.

Autonomous jamming recovery: This use case also focuses on the recovery mechanisms, which can regain lost communication caused by jamming attacks without human intervention to enhance anti-jamming performance. It will employ techniques such as machine learning-based channel estimation to enable robust modulation selection, and reinforcement learning-based

modulation control. Ultimately, this will lead to a more resilient communication system that can effectively withstand and recover from a variety of jamming attacks.

The functional requirements and the associated challenges are listed below:

Table 25. UC 2.3 Functional requirements

Functional requirement	Description	Associated challenges
Jamming mitigation	Action/countermeasures to mitigate jamming attacks such as adaptive modulation techniques	If a jammer detects that the communication system is adapting its modulation, it might change its jamming technique to counteract this adaptation. Fast and frequent changes in modulation might be constrained by hardware and software capabilities of the communication system
Autonomous jamming recovery	Regain lost communication caused by jamming attacks without the need for human intervention	Balancing between robustness against jamming and maintaining an acceptable data rate.

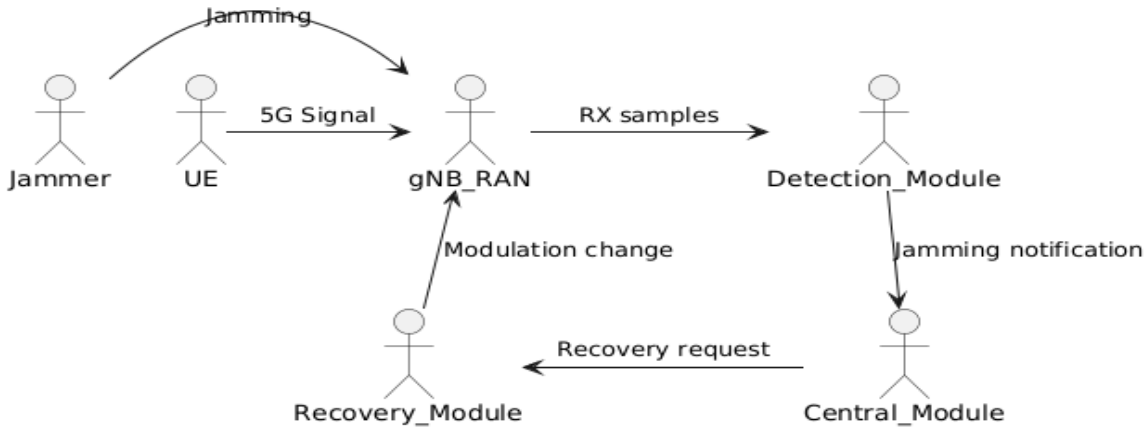


Figure 31. UC2 .3 UML diagram

6.3.2. Use case relevance within NATWORK

The use case fulfills the following NATWORK objectives:

- [OO#1]: Define a detailed extension to 6G architectures by providing E2E security
- [OO#3]: Provide Net-Zero AI-powered trustworthy and explainable management to allow for highly malleable and attack-resilient networks.

- [OO#4]: Provide Physical Layer Security that supports encryption-free, perennial self-resilience of wireless links
- [OO#5]: Deployment & experimental implementation of the security modules in relevant Use Cases
- [OO#6]: Objective 6. Evaluation, validation & verification of the security framework performance.
- [OO#7]: Formulation of KPIs, KVIs, business models, IPR procedures, and standardisation contributions for commercial viability and enhanced cybersecurity in b5G/6G networks.

Moreover, the use case can be mapped as shown below in NATWORK conceptual graph

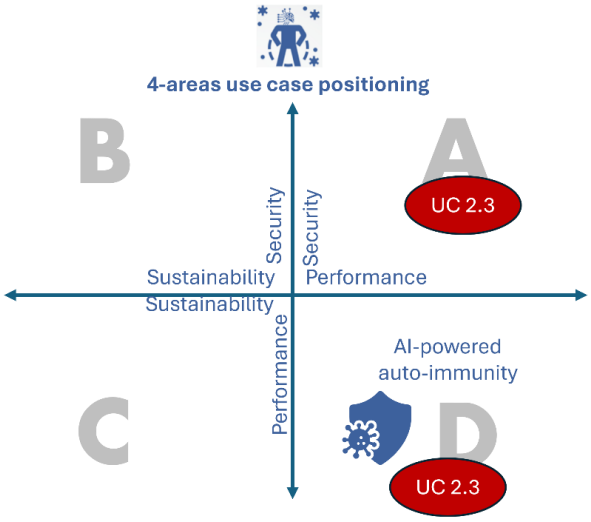


Figure 32. UC2 .3 position in NATWORK's conceptual graph

6.3.3. Definition of use case KPIs

- **KPI2.1** Jamming attacks detected and mitigated (increase of at least 30% in the detection of attacks),
- **KPI2.2** Time needed to detect and prevent a jamming attack (in the order of a few seconds, target <5s),
- **KPI2.3** Time needed to recover from a jamming attack (reduction by 30% in the order of seconds),
- **KPI2.4** Downtime prevented (less downtime at least 20%),
- **KPI2.5** Throughput enhancement during jamming attack of at least 40%

6.3.4. Definition of use case testbed requirements

Infrastructure:

- Jammer (CERTH)
- UE: AV or Smartphone (CERTH/ISRD)
- Servers (CERTH)
- RU, e.g. USRP (ISRD)
- DU, CU and RIC software
- 5G Core network software (ISRD)
- Internet connectivity (CERTH)
- Bandwidth license (CERTH)

6.3.5. Sequence diagram of use case workflow

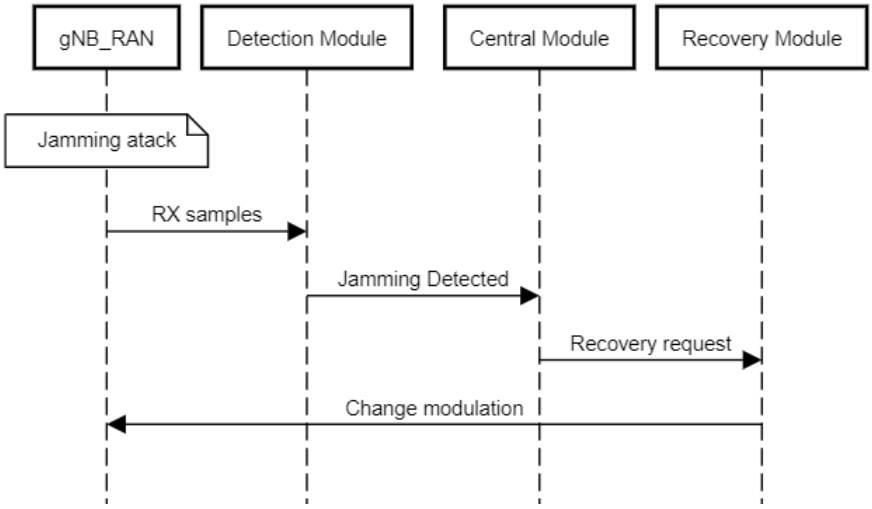


Figure 33. UC 2.3 Sequence diagram

6.3.6. Success factors and selected KPIs

The focus KPIs of this use case will be KPI2.4 Downtime prevented, and KPI2.5 Throughput enhancement during jamming attack since they are the most aligned with the objectives of NATWORK being reconciliation of security and performance. Further focus will be on the KPI2.2 Time needed to detect and prevent a jamming attack and KPI2.3 Time needed to recover from a

jamming attack as they also indirectly influence the performance of the whole system when the security measures are in place.

6.3.7. Success factors and selected KPIs

The focus KPIs of this use case will be KPI2.4 Downtime prevented, and KPI2.5 Throughput enhancement during jamming attack since they are the most aligned with the objectives of NATWORK being reconciliation of security and performance. Further focus will be on the KPI2.2 Time needed to detect and prevent a jamming attack and KPI2.3 Time needed to recover from a jamming attack as they also indirectly influence the performance of the whole system when the security measures are in place.

6.4. Use case 2.4 Improving 6G security in 6G spectrum

6.4.1. Domain description

This use case focuses on safeguarding 6G spectrum bands, particularly those in the sub-THz range, by leveraging AI-driven physical layer key generation (PKG) techniques that rely on channel reciprocity. These techniques utilize the unique characteristics of the wireless channel to generate secure keys, ensuring robust encryption that is inherently resistant to interception. AI enhances the PKG process by optimizing the generation of secure keys, taking full advantage of the unique and dynamic channel properties between devices. This approach ensures a higher level of security and protection for communications within the sub-THz frequency bands, strengthening the overall security framework of 6G networks.

6.4.1.1. Functional requirements and challenges

Table 26. UC2 .4 Functional requirement

Functional requirement	Description	Associated challenges
High-quality metrics extraction	The system must accurately extract relevant metrics from the communication channel, such as signal strength and channel state information (CSI), to serve as the basis for key generation.	Ensuring that the extracted metrics allow for the generation of a secure and sufficiently random key, balancing the need for precise data without introducing excessive computational overhead.
AI model Optimization	The AI model must process the collected metrics to optimize the key generation process, ensuring that the keys are both	Adjusting the AI model to enhance the randomness of the generated keys while optimizing the process to ensure

Functional requirement	Description	Associated challenges
	secure and resistant to discrepancies (Key Disagreement Rate - KDR).	synchronization between devices (here called Alice and Bob).
Security Evaluation	The generated keys must pass security checks, such as the NIST random test, to ensure randomness and resistance to attacks.	Testing the model against potential security threats (e.g., Eve's interception) and ensuring compliance with security standards.

6.4.1.2. High-level functional description

Below is a high-level UML representation of the interaction between the devices (Alice and Bob) and the AI module during the key generation process:

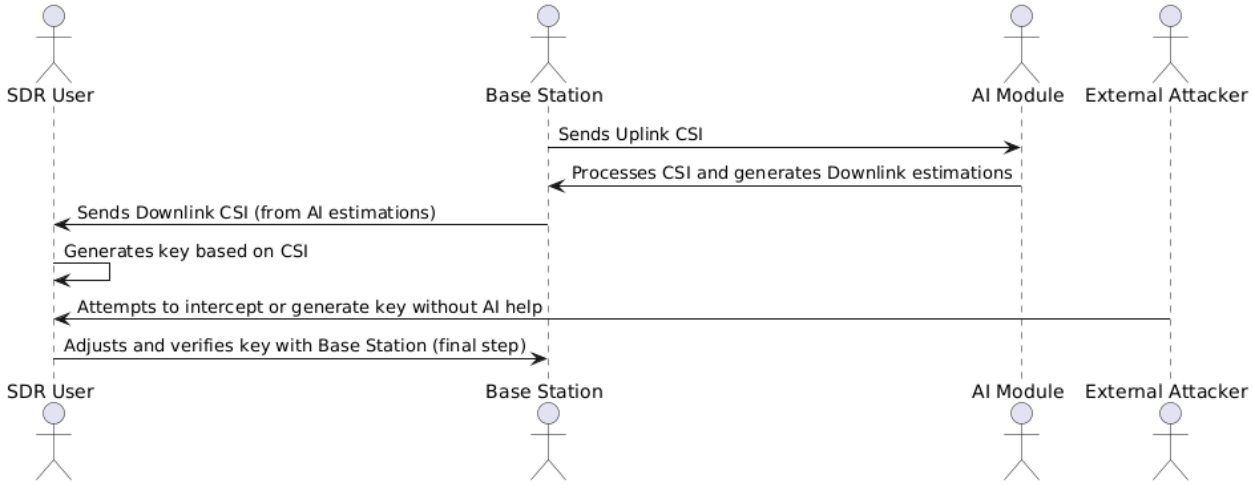


Table 27. UC 2.4 Sequence diagram

As shown in the diagram:

- The Base Station sends uplink CSI to the AI module, which processes and generates downlink CSI.
- The User receives the downlink CSI from the Base Station and generates the key based on the received data.
- The External Attacker attempts to derive the key without access to the AI's estimations.
- Finally, the Base Station and User verify and adjust the generated key for security compliance.

This workflow ensures that secure keys are generated dynamically based on the unique characteristics of the channel, optimized by AI for robustness, and the entire process is protected against external interception attempts.

6.4.1.3. Challenges taken up by the use case

In order to develop the PKG module and implement it in this UC, some challenges should be overcome:

- **Data collection of metrics**: To train and validate the AI algorithms that optimize PKG, it is necessary to gather a large and diverse dataset of relevant metrics for key generation.
- **Optimization of the AI model for key generation**: Adjusting and optimizing the AI model to improve the quality of the generated keys and reduce the Key Disagreement Rate (KDR), while maintaining a balance between accuracy and computational efficiency.
- **Testing resistance to attacks**: Evaluating the AI model's resistance to interception attempts by comparing the keys generated by the model with those potentially obtained by an external agent (Eve), ensuring the robustness of the key generation process against attacks.
- **Implementation on high frequencies testbed**: to validate the performance of the PKG mechanism in a real environment, an RF high-frequency frontend must me set. The components of this RF frontend are quite different from conventional frequency bands and the setup is itself challenging. Gradiant's sub-Thz link testbed will be used for experimentation purposes.

6.4.1.4. Use case threat model

We consider the potential threat of an external attacker attempting to extract the key generated through the PKG (Physical Key Generation) process between two users or between a base station and a user. The attacker's goal would be to compromise the system by breaking the PKG model described earlier. This model relies on the randomness and reciprocity of the channel, and any attempt to intercept or manipulate the process could undermine the security. To mitigate this, the system must validate the resilience of the key generation process, ensuring that the external attacker is unable to derive the keys from the information exchanged. Robustness against such active interception attempts is essential to maintain the integrity of the key generation system.

6.4.2. Use case relevance

NATWORK's core objectives are to reconcile performance, security and sustainability, while also developing AI-powered self-resilience against emerging threats. This use case directly contributes to these goals by focusing on improving security in 6G spectrum bands, using AI-driven physical layer key generation (PKG) techniques. The use of PKG enhances security by leveraging channel reciprocity to generate unique and secure encryption keys, providing robust protection against attacks.

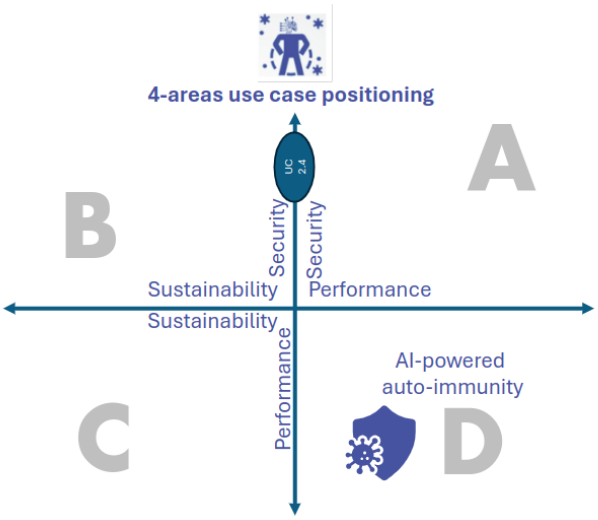


Table 28. UC 2.4 position in NATWORK's conceptual graph

6.4.3. Definition of use case KPIs

The following KPIs will be initially considered:

- A-KPI 2.7: Key Generation Length: Generation of 128-bit keys to ensure strong encryption for secure communications, providing the necessary cryptographic strength for applying AES128.
- A-KPI 2.8 NIST Random Test Compliance: The generated keys will comply with the NIST random test suite, achieving a P-value greater than 0.01 to ensure optimal randomness and security in the key generation process.
- A-KPI 2.9 Key Generation Rate (KGR): The rate of key generation will increase in proportion to the quality of the physical channel, ensuring efficient key production up to an optimal threshold, adapting dynamically to the channel conditions.

These KPIs represent the initial benchmarks for evaluating the effectiveness of the proposed security mechanisms, and further refinements may be introduced as the use case progresses.

6.4.4. Definition of use case testbed requirements

The testbed for this use case will involve the implementation of AI-driven physical layer key generation (PKG) techniques based on channel state information (CSI) obtained from the 6G sub-THz spectrum. The following hardware components will be necessary to support the testing and validation of these techniques:

- Devices (UE) capable of transmitting and receiving in sub-THz frequencies.
- USRPs to simulate the wireless channel and capture CSI data.
- Computational resources for running AI algorithms that optimize the PKG process based on CSI.
- Testbed with sub-THz frontend.

Initially, we are defining only the basic components. The specific details of the implementation will be refined as technical decisions regarding the system architecture and model's progress. Nevertheless, an estimate timeline is given in paragraph 6.4.7.

6.4.5. Sequence diagram of use case workflow

The following sequence diagram outlines the process for Physical Key Generation (PKG) between two devices. The key generation relies on the exchange of Channel State Information (CSI) between the devices and includes an optimization process using AI techniques. The workflow also evaluates the key's performance and resilience to external attacks, using standards such as the NIST randomness test to verify security compliance.

1. Device A (Alice) and Device B (Bob) begin by exchanging Channel State Information (CSI). Alice sends CSI information to Bob, who then responds with its own CSI.
2. The AI module receives the CSI data and optimizes the key generation process by analyzing the characteristics of the channel. The AI module optimizes key information and reduces key disagreements through quantization.
3. During this process, an External Attacker attempts to intercept or generate a key by analyzing the exchanged CSI. The attacker's key is compared to evaluate the system's resilience.
4. The Key Verification module (Key Validation) validates that the keys generated by both Alice and Bob are identical and resistant to any external attack attempts. The verification includes running the generated keys through the NIST randomness test to ensure the keys meet the necessary security standards.

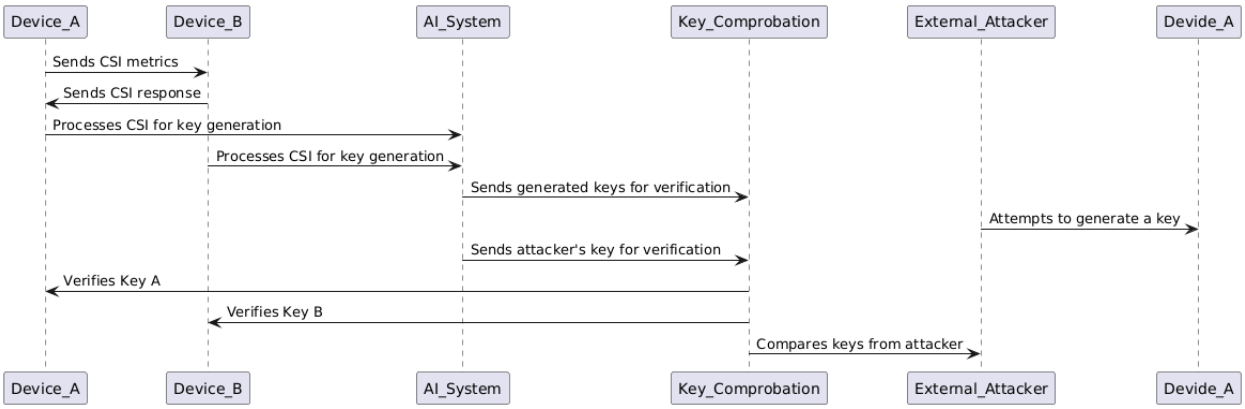


Table 29. UC 2.4 Sequence diagram

This workflow ensures that secure keys are generated dynamically based on the unique characteristics of the channel, optimized by AI for robustness, and verified for compliance with security standards.

6.4.6. Success factors and selected KPIs

The KPIs selected for this use case are focused on ensuring the security and efficiency of the physical layer key generation (PKG) process. In particular, we will evaluate:

- KPI 2.7 (Key Generation Length)
- KPI 2.8 (NIST Random Test Compliance)

-to demonstrate the robustness of the key generation mechanism, ensuring that the encryption keys are both secure and random enough to withstand potential attacks.

Additionally, KPI 2.9 (Key Generation Rate) will ensure that the system can efficiently generate keys in real-time, adapting to varying channel conditions without sacrificing security. These KPIs align with NATWORK's goals of providing enhanced security in 6G networks, while maintaining high performance in dynamic and high-frequency environments.

6.4.7. Timeline and risks

At this stage, the timeline is still flexible and subject to adjustment as the project progresses. The initial phase focuses on obtaining key channel estimations using simulation software to extract

base metrics (e.g., CSI and PSD) and validate the key generation process. Further phases will involve refining the AI and quantization processes to improve performance and security. The estimated timeline for these steps will depend on the results from early testing and the complexity of integrating optimization techniques.

- Initial Research and SoTA (until month 10)
- Development of simulation system with AI models (month 11 - month 14)
- Integration to SDRs (month 15 – month 17)
- Optimization and Performance Refinement (month 18 - month 21)
- Validation and Final Reporting (month 22 - month 25)

Regarding risks, the primary challenge lies in securing the necessary materials and tools for conducting tests. As with similar projects, the availability of hardware and testing platforms may affect the ability to meet planned milestones. More specifically:

- **Channel estimation in high bands**
  - Risk: Channel estimation from real signals can be difficult due to channel impairments such as high path loss and frequency deviation.
  - Mitigation: Perform channel estimation from synthetic signals along with channel equalization.
- **Utilization of sub-THz hardware**
  - Risk: Fragile and expensive hardware components, difficult to replace.
  - Mitigation: Adaptation to lower bands.
- **PKG system model**
  - Risk: The system is too complex to be implemented
  - Mitigation: The final PKG will include only the essential components.

7. Use case 3. IoT security

7.1. Use case 3.1 Anomaly detection using ML

7.1.1. Domain description

The rapid proliferation of IoT devices, coupled with the advent of 6G networks, introduces unprecedented opportunities for enhanced connectivity and data-driven innovation. However, this hyper-connected landscape also expands the attack surface, making IoT ecosystems particularly vulnerable to various cyber threats. UC 3.1 operates within this domain, focusing on the use of advanced Machine Learning (ML) techniques to enhance the detection and mitigation of DDoS attacks. The core premise is that traditional security measures are insufficient in the face of increasingly sophisticated and frequent attacks. Instead, there is a need for an intelligent, automated system capable of evolving alongside the threat landscape.

7.1.2. Functional requirements and challenges

The domain of IoT security in 6G networks is characterized by several key challenges that UC3 .1 seeks to address:

- **Scalability**: The sheer number of IoT devices and the volume of data they generate make it difficult to implement traditional security measures. The solution must be scalable to monitor and protect a large, distributed network without sacrificing performance.
- **Real-Time Detection and Response**: Given the speed at which DDoS attacks can incapacitate a network, the ability to detect and respond to threats in real-time is crucial. This requires efficient processing of network data and rapid execution of mitigation strategies.
- **Accuracy of Anomaly Detection**: Differentiating between benign anomalies (e.g., network congestion) and malicious activities (e.g., a DDoS attack) is challenging. High accuracy in anomaly detection is essential to minimize false positives and negatives, which can lead to either unnecessary resource consumption or undetected attacks.
- **Adaptive Security Measures**: As attackers continuously evolve their methods, static security protocols quickly become outdated. The domain demands adaptive security measures that can learn from past incidents and adjust in response to new threats.
- **Integration with Existing Systems**: The proposed security mechanisms must seamlessly integrate with existing IoT infrastructures and legacy systems without causing significant disruptions or requiring extensive overhauls.

7.1.2.1. Enumeration of functions

UC3 .1 is situated within a technological landscape that is rapidly advancing, driven by innovations in AI, ML, and network technologies. The integration of these technologies into IoT security represents a significant leap forward in the domain. Some of the key functions include:

- **AI-Driven Anomaly Detection**: In UC 3.1, we plan to build AI models, such as CNNs, to process large datasets to n order to identify patterns that may not be evident through traditional analysis, enabling more precise detection of DDoS attacks.
- **Reinforcement Learning for Dynamic Security**: Reinforcement learning algorithms enable the system to adapt its anomaly detection thresholds based on real-time network conditions. This dynamic adjustment helps maintain an optimal balance between detection sensitivity and false positive rates, enhancing overall system resilience.
- **In-Network Processing and Edge Computing**: By deploying ML models closer to the data source, UC3 .1 reduces the latency of detection and response actions. This approach is particularly well-suited to the decentralized nature of IoT networks, where rapid decision-making at the edge can prevent the spread of an attack.
- **Comprehensive Threat Mitigation**: The real-time visibility provided by the system, combined with fast mitigation capabilities, ensures that once an anomaly is detected, appropriate actions can be taken immediately to neutralize the threat, thereby protecting the integrity and availability of IoT services.

7.1.2.2. UML description

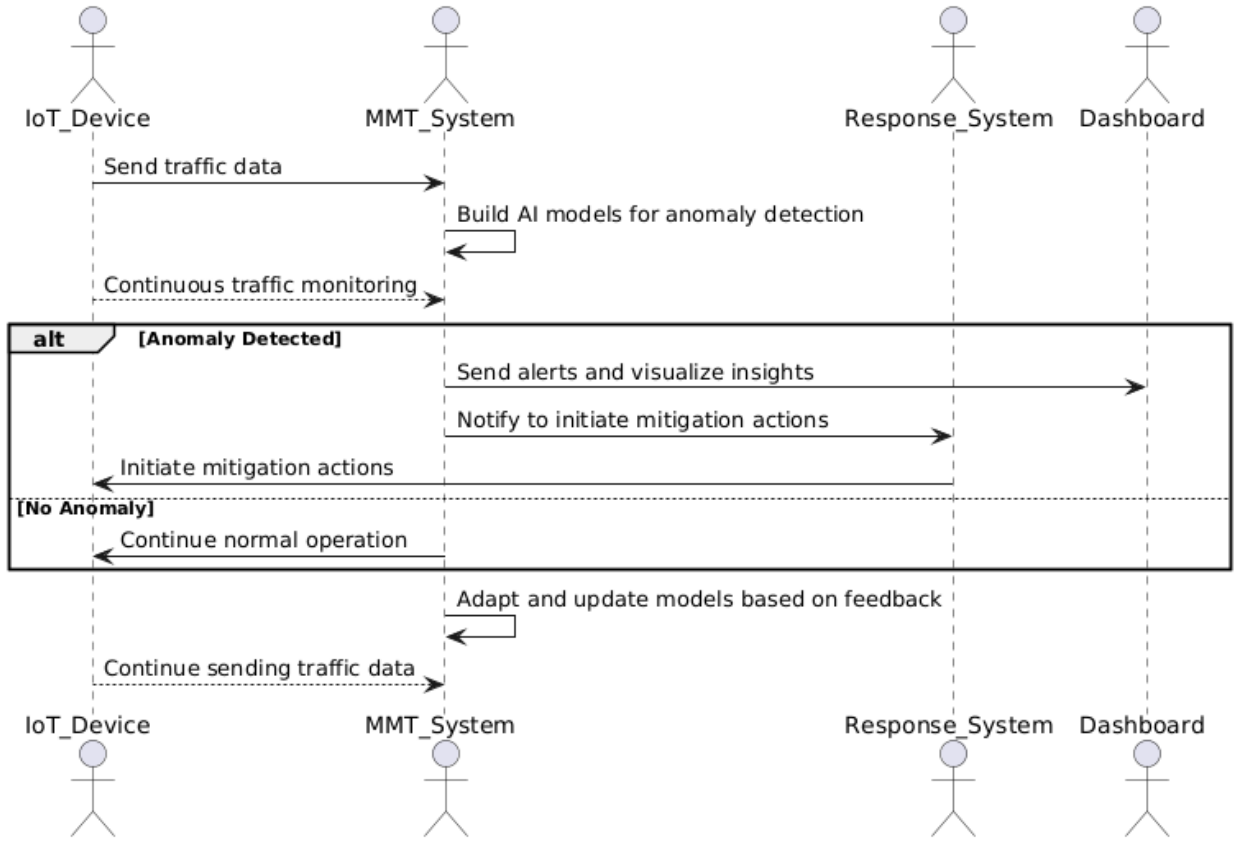


Figure 34 UC 3.1 UML diagram

The provided sequence diagram illustrates the workflow of the anomaly detection system which will be deployed in UC3.1. Here is a breakdown of the process:

- IoT devices continuously send traffic data to the MMT (MONT Monitoring Tool) system. The MMT system receives this data in real-time for further analysis.
- The MMT system uses the collected traffic data to build AI models specifically designed for detecting anomalies. These models are tuned to identify unusual patterns in the network traffic that could indicate potential threats such as Distributed Denial-of-Service (DDoS) attacks or intrusions.
- IoT devices continue to send traffic data, and the MMT system performs real-time monitoring, using the AI models to analyze this data continuously.
- If an anomaly is detected, the system takes the following actions:

- The MMT system sends alerts to a centralized Dashboard to notify operators of potential threats. The system also visualizes the relevant insights and data, allowing the security team to assess the severity of the detected anomaly.
- Simultaneously, the MMT system triggers the Response System to initiate mitigation actions. The Response System takes necessary steps, such as blocking malicious traffic or isolating compromised devices, to minimize the impact of the detected anomaly.
- If no anomaly is detected, the system continues its normal operation, ensuring uninterrupted communication between IoT devices and the MMT system.
- The MMT system continuously adapts and updates its AI models based on feedback from the system, improving its detection accuracy. This feedback loop ensures that the models evolve as the network conditions or threats change, enhancing the system's ability to identify future anomalies.
- IoT devices continue to send traffic data to the MMT system, maintaining the system's vigilance and ensuring that traffic is continuously monitored for any new potential threats.

7.1.3. Use case relevance

UC3.1 is highly relevant to the objectives of the NATWORK project, which focuses on the convergence of advanced security measures with the demands of next generation 6G networks.

- Alignment with NATWORK's Objectives: NATWORK is committed to advancing the security and resilience of IoT infrastructures within 6G networks. UC3 .1 aligns perfectly with this mission by providing a robust framework for detecting and mitigating threats, particularly Distributed Denial of Service (DDoS) attacks, which are a significant concern in large-scale IoT deployments. By focusing on automated, AI-driven anomaly detection, UC3 .1 contributes to NATWORK's broader goal of integrating cutting-edge technologies to create adaptive, scalable security solutions.
- Enhancing Security in 6G IoT Networks: As 6G networks are expected to support an unprecedented number of connected devices, ensuring the security of these devices is critical. UC3 .1 addresses this by developing machine learning models that can identify and respond to security threats in real-time, a key requirement for maintaining the integrity and availability of IoT services in such a dynamic environment. The use case also emphasizes in-network processing and edge computing, which are essential for reducing latency and enhancing the efficiency of security mechanisms in distributed IoT networks.
- Contribution to NATWORK's Innovation and Research: UC3 .1's focus on utilizing AI and machine learning for security aligns with NATWORK's emphasis on innovative research and the application of emerging technologies. The use case demonstrates how AI can be leveraged not just for anomaly detection but also for adaptive security management,

which is a critical area of innovation within the NATWORK project. The integration of Convolutional Neural Networks (CNNs) and reinforcement learning into the security framework showcases how advanced AI techniques can be effectively applied to meet the specific security needs of IoT networks in the 6G era.

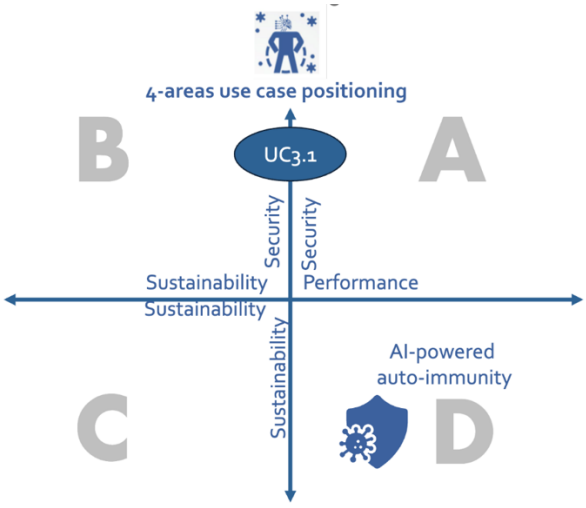


Figure 35. Use case 3.1 position on NATWORK's conceptual graph

- Support for NATWORK's Strategic Goals: One of NATWORK's strategic goals is to create a secure, resilient, and sustainable 6G ecosystem. UC3 .1 supports this goal by providing a comprehensive approach to IoT security that not only detects and mitigates threats but also adapts to the evolving threat landscape, ensuring long-term sustainability and resilience. The use case's emphasis on real-time detection and response capabilities contributes to the project's aim of ensuring that 6G networks can support mission-critical applications and services without compromising security.

- Real-World Application and Impact: UC3 .1 is designed with real-world applications in mind, particularly in scenarios where IoT devices are deployed in critical infrastructures, healthcare, smart cities, and other areas where security is paramount. This makes the use case a valuable addition to the NATWORK project, as it provides practical solutions that can be directly applied in various industries. The ability of UC3 .1 to scale and adapt to different IoT environments ensures that it can have a broad impact, helping to secure a wide range of applications that will be crucial in the 6G era.

In conclusion, UC3 .1 is not only relevant to the NATWORK project but is also integral to achieving its objectives. By advancing the state of IoT security through AI-driven anomaly detection, the use case contributes significantly to the development of a secure and resilient 6G ecosystem, which is at the heart of NATWORK's mission.

7.1.4. Definition of use case KPIs

- KPI 3.1 - Mean Time to Detect (MTTD):

In UC3 .1, the machine learning algorithms and AI-driven anomaly detection systems will be optimized to detect potential DDoS attacks and other anomalies swiftly. The goal is to achieve a mean detection time of under 5 minutes for ML-based detection rules and less than 10 milliseconds for rules not based on ML, such as those within the MONT's Monitoring Tool (MMT). This rapid detection is crucial for real-time threat mitigation in IoT networks, ensuring that attacks are identified and addressed before they can cause significant harm.

- KPI 3.2 - Number of False Positives (FP):

UC3 .1 will focus on refining its AI and ML models to minimize the occurrence of false positives to less than 1%. By achieving this low rate, the system ensures that security alerts are highly accurate, reducing unnecessary interventions and allowing security teams to focus on genuine threats. This precision is vital for maintaining the efficiency and reliability of IoT network operations.

- KPI 3.3 - Number of False Negatives (FN):

The use case aims to keep the false negative rate below 1%, ensuring that the system can effectively identify a wide range of DDoS attacks and other security threats. By minimizing the risk of undetected attacks, UC3 .1 enhances the overall security posture of IoT networks, making them more resilient against potential breaches.

- KPI 3.4 - Packet Loss Ratio (PLR):

UC3 .1's solutions will be engineered to handle IoT communication with minimal disruption, achieving a Packet Loss Ratio (PLR) of less than 0.001%, even in low-bandwidth scenarios. Maintaining such a low PLR is critical for ensuring the reliable and efficient transmission of data within IoT networks, which is essential for both normal operations and effective anomaly detection.

- KPI 3.5 - Mean Time to Resolve (MTTR):

The anomaly detection and mitigation tools developed in UC3 .1 will be designed to facilitate the rapid resolution of detected threats. The objective is to resolve any identified security issues within a mean time of under 10 minutes, thereby minimizing the impact on IoT network operations. This quick resolution time is crucial for maintaining the continuity and security of services in 6G IoT environments.

7.1.5. Definition of use case testbed requirements

This section elaborates on the various components of the testbed configuration, including network topology, security measures, and monitoring and management tools. The testbed will be developed and supported by PNET, CERTH, and MONT.

- **IoT / Wireless Sensors Network**

The testbed will include simulated and real IoT devices, sensors, and gateways. This setup is essential for emulating the diverse and complex conditions found in actual IoT deployments. Devices will be configured to generate traffic patterns that represent both normal operations and potential attack scenarios, such as Distributed Denial of Service (DDoS) attacks. The simulation environment will enable controlled testing of machine learning (ML) algorithms designed to detect and mitigate these threats in real-time.

The testbed will incorporate a multi-tier architecture, consisting of edge, fog, and cloud layers: The edge layer will include IoT gateways and edge devices that process data close to the source, minimizing latency and enabling real-time decision-making. The fog layer acts as an intermediary, providing additional processing power and storage closer to the edge, but with more computational resources than the edge layer. The cloud layer will be used for more extensive data processing, storage, and centralized management of the network. This tiered approach will allow for the evaluation of the effectiveness and efficiency of security mechanisms deployed at different levels of the network, particularly in scenarios where computational resources and network conditions vary.

- **Security Measures**

The testbed will include secure, isolated environments specifically designed for testing scenarios that involve sensitive data or potentially untrusted infrastructure providers. These environments will be segmented from the rest of the network to prevent unauthorized access and to contain any potential security incidents. This isolation is particularly important when testing security measures that involve processing confidential information or when evaluating the resilience of the system against insider threats.

In addition, the testbed will be equipped with tools and configurations necessary for conducting penetration testing and vulnerability assessments. These tools will be used to simulate attacks on the network and identify potential weaknesses in the security mechanisms. The penetration testing setup will include automated testing tools as well as manual testing procedures to ensure a comprehensive assessment of the security posture of the IoT network.

- **Monitoring and Management**

Effective monitoring and management are essential for maintaining the testbed's performance and integrity and ensuring accurate and reliable testing outcomes. A centralized dashboard (e.g., MMT-Operator) will be implemented to provide real-time monitoring of the testbed's performance. This dashboard will offer a unified interface for managing test scenarios, tracking key performance indicators (KPIs), and visualizing the results of security tests. The dashboard will enable users to monitor network traffic, detect anomalies, and observe the behavior of the ML-based intrusion detection systems in real-time. It will also facilitate the management of the testbed infrastructure, allowing for the easy deployment and scaling of test scenarios.

Furthermore, the testbed will incorporate automation frameworks to streamline the deployment and scaling of tests, the collection of results, and the resetting of the environment between tests. Automation will be critical for efficiently managing the complex and repetitive tasks involved in testing multiple scenarios and configurations. These tools will enable the rapid iteration of test scenarios, ensuring that all relevant use cases are thoroughly evaluated within a consistent and controlled environment.

7.1.6. Sequence diagram of use case workflow

This sequence diagram illustrates the workflow of our IoT use case designed for anomaly detection. The process begins with the IoT Devices, which send sensor data (such as temperature and humidity) to the IoT Gateway. The IoT Gateway then forwards the data stream to the MMT Sniffer. In more advanced network scenarios, in-operator MMT sniffers can also systematically intercept user-plane IoT traffic. Depending on the specific operator's needs, traffic interception can be configured at different stages within the network architecture, including the network edge or the core. The interception can be implemented based on bearers that encapsulate the data within GPRS Tunneling Protocol (GTP) tunnels. Software-Defined Networking (SDN) switches can be crucial in implementing this interception mechanism. These switches can be programmed to identify and handle IoT-related traffic based on predefined rules. By leveraging flow-based processing, the SDN switches can create traffic duplicates, forwarding one traffic set toward the intended destination, while simultaneously redirecting another set to the IoT MMT sniffer for monitoring. Then, the MMT Sniffer captures raw network traffic and sends it to the MMT tool for the preprocessing stage. Once the data is normalized, it is sent to the ML Anomaly Detection component, which applies machine learning and deep learning algorithms to identify any anomalies in the data. If an anomaly is detected, an alert is generated and visualized on dashboards. The alert is then logged in the Database (e.g., MongoDB), capturing details such as the timestamp, type, and severity of the anomaly. Finally, the system notifies the

Administrator/Operator of the detected anomaly, and the Administrator/Operator initiates mitigation actions. MMT continues monitoring traffic and adapts based on feedback.

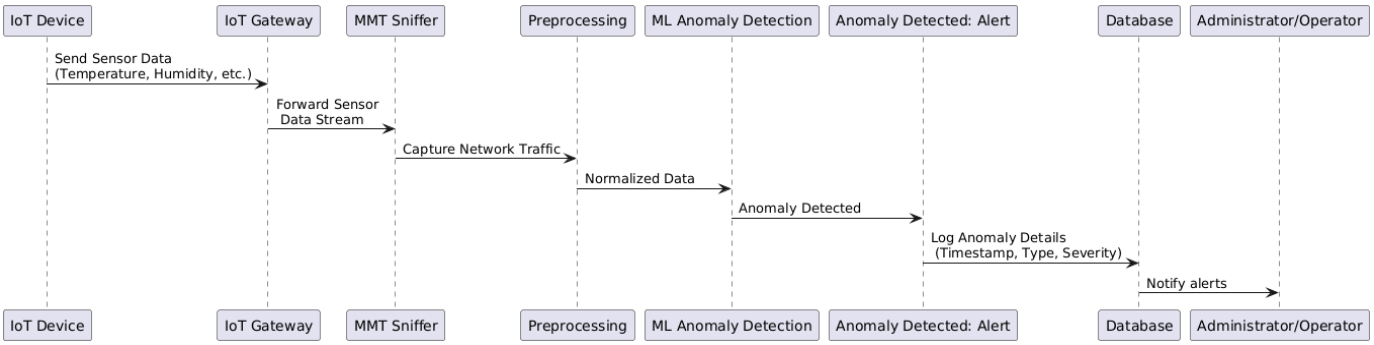


Figure 36. UC 3.1 Sequence diagram

7.1.7. Success factors and selected KPIs

Success factors for UC3 .1 will involve several key elements:

- Algorithm Efficiency: The success of UC3 .1 heavily depends on the effectiveness of the machine learning algorithms and AI-driven detection systems. These need to be fine-tuned for high accuracy, low latency, and minimal resource consumption to ensure they can detect threats swiftly and accurately without overburdening the network.
- Scalability (KPI 3.5): The ability to scale the detection systems to handle the vast amount of data generated by IoT devices in 6G networks is crucial. The solutions must perform consistently well, even as the number of connected devices grows.
- Low False Positive/Negative Rates (KPI 3.2, KPI 3.3): Achieving the targeted low rates of false positives and false negatives is essential for maintaining the reliability and effectiveness of the security systems, ensuring that real threats are detected, and false alarms are minimized.
- Rapid Response and Resolution: The ability to detect and mitigate threats quickly (as indicated by the MTTD and MTTR KPIs 3.1) is critical for minimizing the impact of security breaches and ensuring continuous network operations.
- Robust Network Performance (KPI 3.4): Maintaining low packet loss and ensuring that the security measures do not negatively affect network performance are key factors in the overall success of UC3 .1, particularly in environments with limited bandwidth.
- Integration and Adaptability: The successful integration of these solutions into existing IoT ecosystems and their adaptability to evolving threats will be vital for the long-term sustainability and relevance of the security measures developed in UC3 .1.

7.1.8. Timeline and risks

7.1.8.1. Timeline

Figure indicates the timeline of UC3.1 which spans months 9 to 36, showing key stages of the development process:

- Month 9-12: Testbed Validation and Initial Testing begins
- Month 13-08 Algorithm Development and Integration are carried out
- Month 19-24: Advanced Testing and Refinement take place
- Month 25-28: Real-world simulation and integration and conducted
- Month 19-32: Final Optimization and Documentation are completed
- Month 33-36: The project concludes with Final Review and Project Closure

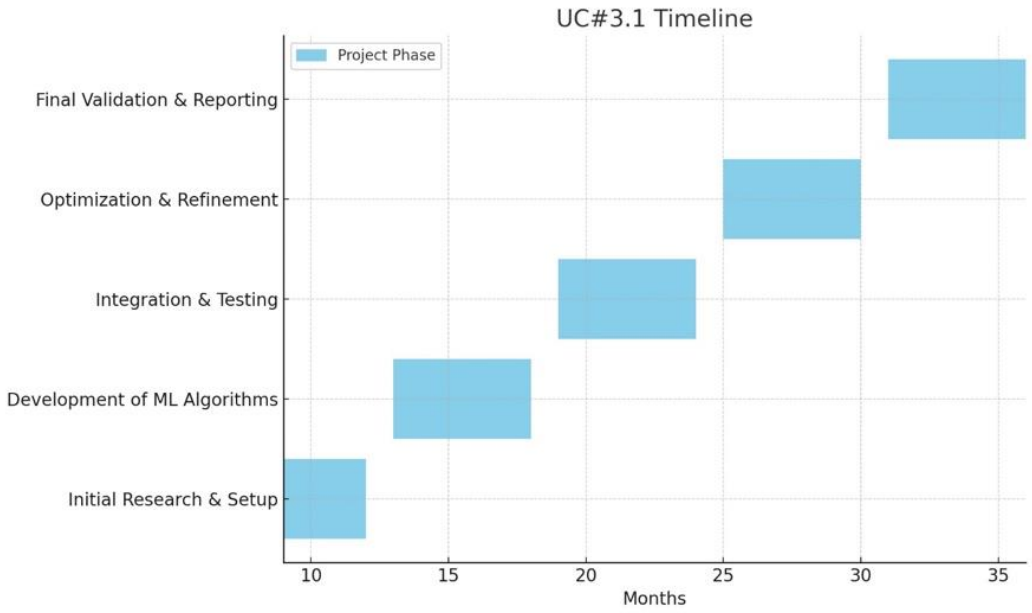


Figure 37. UC3 .1 Timeline (road map)

7.1.8.2. Risks

The potential risks for UC3.1 are as follows:

- False Positives/Negatives: Achieving a low rate of false positives and false negatives is crucial for the effectiveness of the ML models used in UC3 .1. However, fine-tuning these models to achieve high accuracy may require additional data or model adjustments, which could be time-consuming and resource intensive. To mitigate this risk, the project will utilize a diverse range of datasets, incorporating various network conditions and attack

scenarios. Continuous monitoring of performance metrics will guide the fine-tuning process, ensuring that detection accuracy improves over time. Feedback loops from real-world testing will also be integrated to refine the models further and reduce the occurrence of false positives and negatives.

- Scalability Issues: As IoT networks expand and become more complex, ensuring that detection systems can scale effectively is a significant challenge. The increasing number of devices and the volume of data can create bottlenecks in anomaly detection and response mechanisms, potentially compromising the system's effectiveness. To address this risk, scalability testing will be prioritized early in the upcoming project phases. By identifying potential bottlenecks ahead of time, the project can implement necessary adjustments to the architecture and optimize system performance. Regular scalability assessments will also be conducted as the project progresses, ensuring that the detection systems can handle the growing demands of a complex IoT network.
- Resource Constraints: Managing computational resources efficiently is critical as the AI-driven detection systems scale. Insufficient resources could lead to performance degradation, impacting the system's ability to detect and mitigate threats in real-time. Resource allocation will be optimized by carefully planning and managing the testbed infrastructure. The project will ensure that the infrastructure can support the increased computational demands, especially as the detection systems become more complex. Additionally, strategies for dynamic resource management will be implemented, allowing the system to allocate resources more effectively based on current needs.
- Real-World Testing Delays: Unforeseen issues during real-world testing could cause delays, impacting the overall project timeline and the ability to validate the system's effectiveness in practical environments. To minimize the delays, flexibility will be built into the project schedule, allowing for adjustments if unexpected issues arise. Early testing will be prioritized in the next phases of the project to identify and resolve potential problems before they escalate. This proactive approach will help keep the project on track and ensure that the system is thoroughly tested under real-world conditions.

7.2. Use case 3.2 AI driven penetration testing

7.2.1. Domain description

This use case scenario focuses on developing an advanced penetration testing tool using AI to assess network security by simulating a sophisticated phishing attack and AI-based Denial of Service (DoS) attack. The aforementioned tool will be able to generate and send phishing emails specifically targeted at 6G network administrators and operators. The primary goal is to evaluate how AI, particularly LLMs, can be leveraged to craft persuasive phishing emails that manipulate human behavior, leading to network compromise. The post-compromise technique involves a sophisticated AI-driven attack aimed at assessing the resilience of 6G infrastructure against DoS attacks. This use case primarily focuses on evaluating how AI-based attacks can degrade the QoS in 6G networks and enhancing the security of defense mechanisms.

To achieve this, LLM will be utilized to create convincing phishing content. Each phishing email will include a malicious attachment engineered to execute upon opening. This attachment will initiate a DoS attack, which is orchestrated by a separate AI algorithm employing reinforcement learning techniques to optimize the attack's effectiveness and cause maximum disruption to the network.

The purpose of the DoS attack is to evaluate the resilience of the 6G infrastructure by testing how well it can withstand and recover from a sustained disruption. It aims to assess the degree to which service quality is compromised during the DoS evaluation, such as slower performance or outages, and measure the overall impact on the end users, including how much their experience is degraded by the attack. This evaluation helps identify weaknesses and the ability of the network to maintain stability under adverse conditions. This tool will simulate real-world cyber threats, providing valuable insights into the vulnerabilities of human-operated systems and the potential of AI-driven cyber-attacks, ultimately helping to strengthen network defenses against such sophisticated threats.

7.2.2. Use case relevance to NATWORK

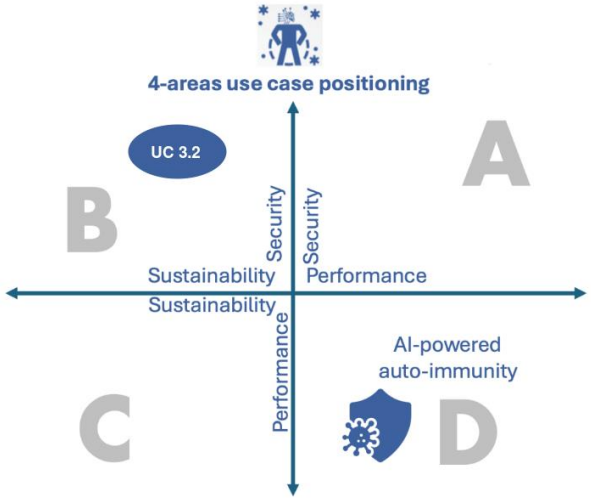


Figure 38. Use case 3.2 position on NATWORK's conceptual graph

This use case contributes to the security of NATWORK and 6G networks in several ways:

UC3.2 significantly contributes to the NATWORK project by providing a unique AI-powered penetration testing tool that goes beyond traditional solutions. Unlike other tools, it models complex DoS attack scenarios and offers deeper insights into network vulnerabilities. By combining DoS attacks with protocol-level fuzzing, it generates custom network packets tailored to the targeted 5G service. This approach identifies vulnerabilities that other tools might overlook, delivering a thorough evaluation of the network's capabilities and the communication protocols used by its services, ultimately enhancing the security of 5G and 6G networks. The main contributions follow in detail:

- **Demonstration of IoT as an Attack Vector**: By delivering the penetration testing tool from an IoT device, this approach underscores the potential risks associated with the widespread deployment of IoT devices in 5G and 6G environments. It demonstrates how compromised or malicious IoT devices can be weaponized to launch sophisticated attacks on critical network infrastructure, prompting a re-evaluation of IoT security strategies.

- **Testing Network Resilience**: The tool targets 6G network administrators, who are responsible for maintaining the integrity and security of the network. By conducting DoS attacks and deploying malicious payloads via IoT devices, this penetration testing tool helps assess the resilience of the network against attacks that may originate from less expected sources, such as IoT devices, which are often considered to be on the periphery of the network.
- **Intelligent Phishing Attacks**: For each target within the 5G and 6G network, the AI responsible for generating the phishing text will first search the internet for available information about the target. This allows the AI to create highly personalized and convincing phishing emails, increasing the likelihood of success. By gathering specific details about the target, such as professional background, interests, or recent activities, the phishing attack becomes much more effective, simulating a real-world scenario where attackers use social engineering to exploit human vulnerabilities.

7.2.2.1. Functional requirements and challenges

- To achieve the assessment of resilience to DoS attacks, the target services should include protocols such as TCP, UDP and SCTP.
- The effectiveness of AI-DoS should be compared with other DoS attack tools and the results presented.
- For the effectiveness of LLM, it would be good to have natural people to evaluate the persuasiveness of the emails it will produce.

7.2.2.2. UML description

The provided diagram illustrates the workflow of AI-DoS evaluation on 5G/6G Core. The main purpose is to discover vulnerabilities and assess resilience against attacks carried out by AI.

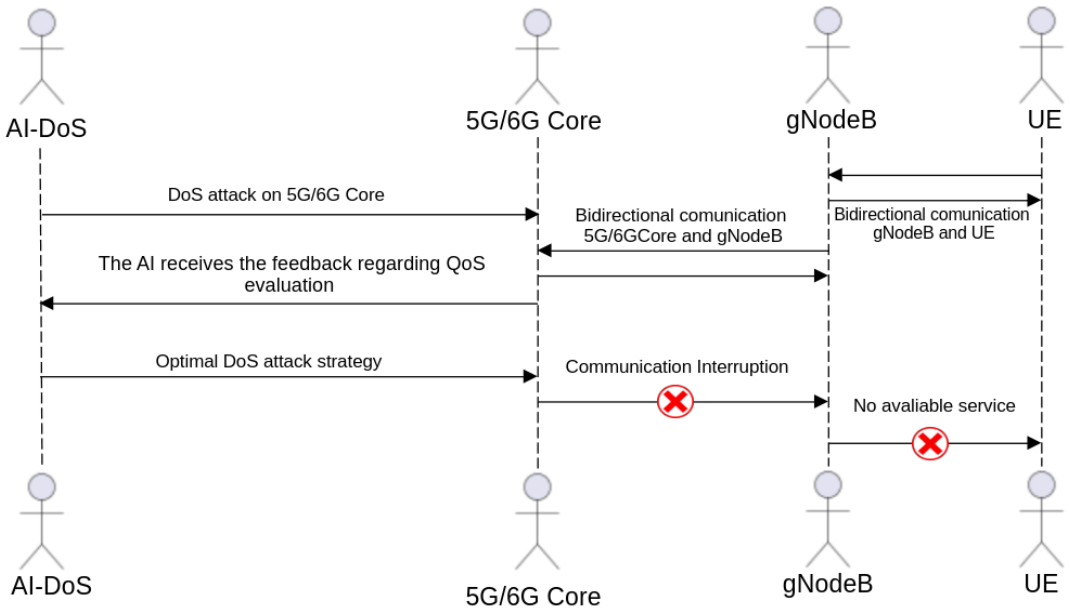


Figure 39. UC 3.2 UML diagram

Here's a breakdown of the DoS assessment process performed by AI:

- The AI-DoS initiates a DoS attack targeting the 5G/6G Core.
- The AI receives feedback regarding the QoS evaluation from the 5G/6G Core.
- Based on the feedback, the AI-DoS sends an optimal DoS attack strategy to maximize disruption.
- Normally, bidirectional communication occurs between the 5G/6G Core and gNodeB, and between gNodeB and UE.
- The DoS attack leads to a communication interruption between the 5G/6G Core and gNodeB.
- As a result, no available service is delivered to the UE.

7.2.3. Definition of use case KPIs

UC3.2 will initially consider the following KPIs:

- **A-KPI 3.6** Impact on QoS by AI-DoS evaluation tool
- **A-KPI 3.7** Comparison of results between AI-DoS and other tools used for QoS assessment, to determine which is the most effective tool.
- **A-KPI 3.8** Perform a vulnerability report regarding DoS resilience on 5G/6G components.

7.2.4. Definition of use case testbed requirements

The implementation, experimentation, and evaluation of Use Case 3.2 will be carried out on the CERTH 5G-SDN testbed, leveraging its infrastructure and tools for 5G and beyond environments. This testbed offers the required resources and services to support AI-driven microservices orchestration and the analysis of various attack scenarios. If the AI-DoS tool is deployed in an alternative testbed, it must meet the following requirements.

High-Performance PC Requirements:

- **CPU:** Multi-core processor (e.g., AMD Ryzen 7 or Intel Core i7) with high clock speeds to handle the simultaneous tasks of AI model computations and virtual machine management.
- **RAM:** At least 16 GB of RAM to manage multiple virtual machines and intensive AI tasks simultaneously.
- **Storage:** Fast SSD (at least 1TB) to provide quick access to datasets, models, logs, and to store the VM disk images.
- **Operating System:** A host OS capable of managing virtualization efficiently (e.g., Linux with KVM, or Windows with Hyper-V).

Software Configuration:

Virtualization Platform:

- **VMware Workstation, VirtualBox, Hyper-V, or KVM:** Use any of these virtualization platforms to create and manage the VMs.
- **AI Model Development Environment:**
- **Python Environment:** Set up Python with necessary libraries (TensorFlow, PyTorch) to handle LLM fine-tuning.
- **LangChain or Hugging Face:** Deploy these frameworks for fine-tuning the language models with specific data.
- **Data Management:** Incorporate data scrapers and preprocessors to fine-tune the LLM on administrator-specific data.

Virtual Machines (VMs) Setup:

- **VM 1: 6G Network Simulation**
  - **Purpose:** Simulate the 6G network infrastructure that will be targeted by the phishing attacks.

- **Configuration:** Allocate CPU cores (2-4), RAM (4-8GB), and disk space (50GB). Install a lightweight Linux distribution or Windows Server, depending on your network simulation tools.
- **Network Simulation Tools:** Use tools like **free5GC** or **Open5GS** as an alternative to create a virtual network environment that closely resembles 5G/6G technologies.

- **VM 2: Victim Environment (6G Administrators)**
  - **Purpose:** Simulate the machines used by the 6G administrators who will receive the phishing emails.
  - **Configuration:** Allocate CPU cores (2-4), RAM (4-8GB), and disk space (50GB). Install an OS similar to what the real administrators might use (e.g., Windows 10/11, Linux).
  - **Email Client and Security Tools:** Set up email clients (e.g., Outlook, Thunderbird) to receive phishing emails. Install IDS (Intrusion Detection Systems) or other security software to observe how the attack is detected or bypassed.

Network Configuration:

- **Isolated Virtual Network:**
  - Configure a virtual network within your PC using the virtualization platform to ensure that the VMs can communicate with each other and the host machine, simulating a real-world 6G environment.
  - Set up different subnets for the 6G network simulation and the administrator machines to replicate a more realistic network architecture.

Data and Workflow:

- **Phishing Email Generation:**
  - On the host PC, fine-tune the LLM using data related to the administrators. Generate targeted phishing emails designed to trick administrators into installing the malicious .exe file.
  - Deploy these phishing emails to the simulated administrator machines within the VM environment.
- **Execution and Observation:**
  - The administrator VM receives and interacts with the phishing email. If the email is successful, the .exe file containing the AI-enabled DoS attack will be executed.

- Monitor the behavior of the .exe file within the 6G network VM, observing how it impacts the network and how the IDS or other security measures respond.

7.2.5. Sequence diagram of use case workflow

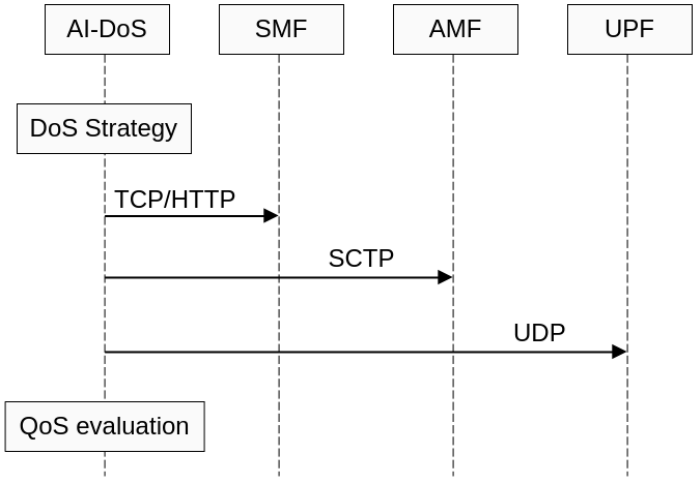


Figure 40. Use case 3.2 AI-DoS evaluation graph

The main focus is on utilizing IoT devices as vectors for AI-driven penetration testing against the sophisticated infrastructure of 5G and 6G networks. This approach highlights the potential vulnerabilities within the highly interconnected and dynamic environments that 6G networks and IoT ecosystems represent. The penetration testing tool, powered by AI, leverages the nature of IoT devices to initiate simulated attacks against 6G network administrators, providing a real-world assessment of the network's defenses.

7.2.6. Success factors and selected KPIs

1. The AI-DoS will be considered successful as long as it can effectively reduce the QoS by more than 80% in the evaluated 5G/6G service provided by CERTH
2. The impact on QoS from AI-DoS must be over 90% in comparison with other DoS evaluation tools.
3. AI-DoS will have to provide detailed information about which strategy it implemented and the impact it had on reducing the QoS.

7.2.7. Timeline and risks

7.2.7.1. Timeline

UC 3.2's timeline is broken down with five phases as shown below:

Phase 0 – Project Initiation (Months 1-2)

- Define project objectives and scope.
- Assemble the project team and allocate resources.
- Conduct preliminary research to inform development strategies.

Phase 1 – Development of AI-DoS Attack Tool (Months 3-11)

- Develop the AI-based DoS attack tool over a period of 9 months.
- Implement core functionalities and integrate AI capabilities.
- Conduct iterative testing and refinement to ensure tool effectiveness.

Phase 2 – Comparative Analysis (Months 12-16)

- Compare the results of the AI-DoS attack tool with other existing DoS attack tools over 5 months.
- Analyze performance metrics, effectiveness, and potential vulnerabilities.
- Document findings and identify areas for improvement.

Phase 3 – Creation of LLM for Phishing Email Generation (Months 17-26)

- Develop the LLM for generating phishing emails over a span of 10 months.
- Test and validate the LLM to ensure it meets desired performance standards.

Phase 4 – Integration and Testing (Months 27-30)

- Integrate the AI-DoS attack tool and the phishing email LLM into the overall security framework.
- Conduct comprehensive testing to assess interoperability and system robustness.
- Address any integration issues and optimize system performance.

Phase 5 – Final Validation and Reporting (Months 31-36)

- Perform final validation of all developed tools to ensure they meet project KPIs.
- Prepare detailed reports outlining methodologies, findings, and recommendations.

7.2.7.2. Risks

To comprehensively assess the effectiveness of the Large Language Model (LLM) in generating persuasive emails, it is essential to involve real individuals in the evaluation process.

Relying solely on automated metrics or theoretical assessments may not capture the nuanced ways in which humans perceive and respond to written communication. Expanding the evaluation framework to include human assessments can provide deeper insights and more actionable feedback.

7.2.8. Summary

This use case involves developing an AI-powered penetration testing tool to assess the security of 5G and 6G networks through advanced phishing attacks. The tool uses LLMs to craft convincing phishing emails targeting network administrators. Each email includes a malicious attachment that triggers a DoS attack, orchestrated by an AI algorithm using reinforcement learning to maximize disruption. The attack tests the resilience of the 5G and 6G infrastructure, assessing how well it withstands and recovers from disruptions, and the impact on service quality and end-user experience. This tool provides valuable insights to strengthen network defenses against AI-driven cyber threats.

7.3. Use case 3.3 Decentralized security and trust management

7.3.1. Domain description

7.3.1.1. Functional Requirements and Challenges

The growing number of devices connected to 5G/6G network raises a number of new security challenges and concerns. Use case 3.3 focuses on integrating distributed technologies to build a secure and decentralized trust and access infrastructure in 6G networks. One distributed solution is the implementation of blockchain technology, which enables secure and decentralized methods for data processing and communication. In this context, and to safeguard communication channels between IoT edge devices and to prevent unauthorized access, comprehensive end-to-end security protocols must be developed. The functional requirements and the associated challenges are listed below:

Table 30. . UC3 .3 Functional requirements

Functional requirement	Description	Associated challenges
Decentralized Trust Management	Trust relationships and security decisions lead to trust and access	Achieving secure trust and access management across the set of participating entities in the

Functional requirement	Description	Associated challenges
	control must be managed without centralized entities.	network, with possible malicious participants, without relying on a centralized managing entity.
Real-time Trust and Access Establishment	Trust and access must be controlled, established, monitored, and updated dynamically as devices and users join or leave the network	Ensuring real-time trust and access management and minimal latency for dynamic applications.
Security Data Aggregation	Aggregate the security and trust data in a secure and privacy preserving approach	protecting sensitive data and ensuring its integrity while managing distributed sources across the network.

7.3.1.2. Enumeration of Functional requirements

- **Latency**: Minimizing latency in trust verification and access control to meet the real-time demands of 6G applications.
- **Security**: Protecting the system from attacks that could exploit decentralized control mechanisms.

7.3.1.3. High Level Functional Description

The use case includes the following main functions:

- Decentralized Trust Establishment: Utilizing distributed technologies to record and verify trust relationships among devices and users.
- Security Control: Using cryptographic primitives and protocols to ensure secure data access and exchange between devices.
- Secure Aggregation: Collect the security and trust data using a secure, privacy-preserving method.
- Consensus Mechanisms: Deploying consensus algorithms to validate trust parameters and updates in the decentralized network.

7.3.1.4. UML description

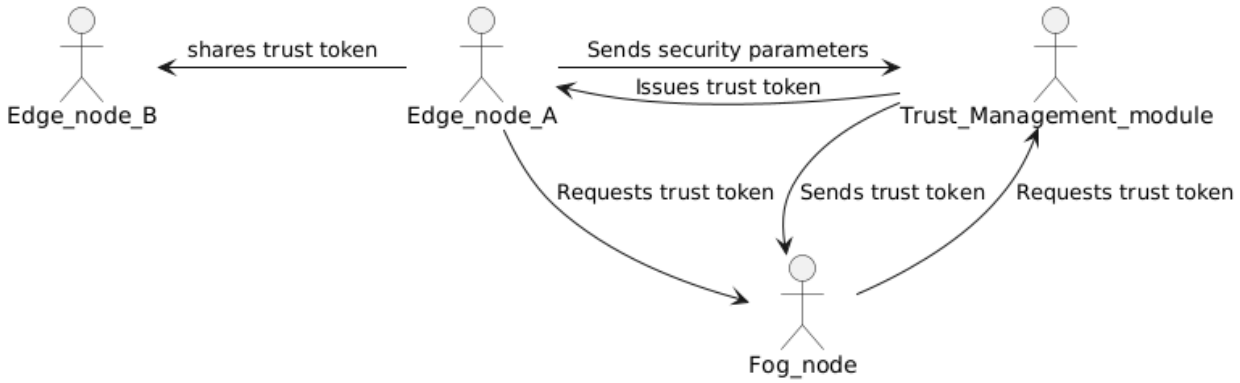


Figure 41. UC #3.3 UML graph

An edge node receives the issued trust tokens from the trust management module, based on the transmitted security parameters. The trust management module is distributed among a number of nodes to prevent a single point of failure and attack. The edge nodes can also request and receive the trust token from the fog node, in case the token has been recently cached and is not expired. A trust token is then shared with another edge node. The integrity and authenticity of the tokens are verifiable.

7.3.1.5. Challenges taken up by the use case

The challenges taken by this use cases are:

Challenge 1: Ensuring real-time trust management and minimal latency for dynamic applications.

Challenge 2: Achieving secure trust and access management across the set of participating entities in the network

Challenge 3: Protecting sensitive data, including the security and trust data, from leakage or tampering during aggregation, ensuring data integrity, and maintaining user privacy while managing distributed data sources across the network.

7.3.1.6. Use case threat model

Several threats are tackled by the use case:

Impersonation Attack: where the attacker pretends to be an authorized user or device to gain access to the network or services.

Sybil Attack: An attacker creates multiple fake identities to disrupt trust management process.

Majority Attack: An attacker gains control of more than 50% of the network to manipulate trust decisions.

Eclipse Attack: An attacker isolates a node from the network to disrupt its ability to verify trust.

7.3.2. Use case relevance to NATWORK

One of the NATWORK objectives is to fully specify a detailed 6G architecture, that is based on existing 6G architectural principles proposed by 5GPPP but is extended to provide holistic, End-to-End (E2E) security to the network. As displayed in Figure 40, use case 3.3 is positioned on the reconcile performance, sustainability and security core objective of NATWORK, with the ambition to take up the challenge of providing security. The adoption of decentralized security and trust management in 6G networks addresses the key objective of enhancing privacy and security. Centralized trust models in legacy systems are inadequate for the scale and complexity of 6G ecosystems. Use case 3.3 enables elimination of single points of failure by providing a decentralized control, therefore security risks associated with centralized entities are reduced, ensuring that a compromised node does not result in a total failure in the entire system. The use case enables real-time and autonomous trust assessment between users, devices, and applications, crucial for environments with highly dynamic connections (e.g., V2X communication, smart healthcare). The immutability of distributed technologies ensures that trust relationships and security policies are tamper-proof, enhancing the overall integrity of the system. Use case 3.3 is particularly relevant for future 6G deployments as part of NATWORK framework where data security, trustworthiness of devices, and real-time autonomous decision-making will be crucial for enabling high-assurance services.

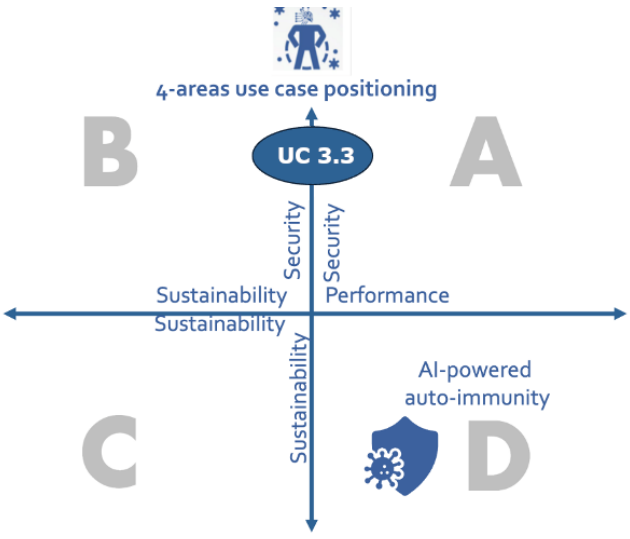


Figure 42. UC 3.3 position in NATWORK's conceptual graph

7.3.3. Definition of use case KPIs

The following KPIs are identified:

A-KPI 3.9 - Mean Time to Detect (MTTD):

The time required to detect an anomaly attack against the security and trust management system.

A-KPI 3.10– Number of False Positive (FP):
The percentage of legitimate entities incorrectly flagged as threats during security and trust management (involving injection of at least 5 different attack types)

A-KPI 3.11 – Number of False Negative (FN):
The percentage of malicious entities incorrectly flagged as benign during security and trust management (involving injection of at least 5 different attack types)

A- KPI 3.12 - Trust Establishment Time (TET):
Measures the average time required to establish trust between devices in a decentralized manner.

7.3.4. Definition of use case testbed requirements

The testbed for the use case 3.3 requires the following:

6G enabled IoT environment: Virtual machines to establish a small IoT network conditions and validate security and trust management protocols under different scenarios.

IoT Devices: Real and simulated IoT devices, sensors, and gateways replicate the diverse conditions in a real-world 6G enabled IoT environment.

Security Provers: The tools required to provide formal security verification of the proposed use case 3.3 protocol, after translating it to the relevant protocol representation.

7.3.5. Sequence diagram of use case workflow

The following figure illustrates the sequence diagram of the use case 3.3. For simplicity, the figure does not detail all operations but the main sequence of actions of the use case.

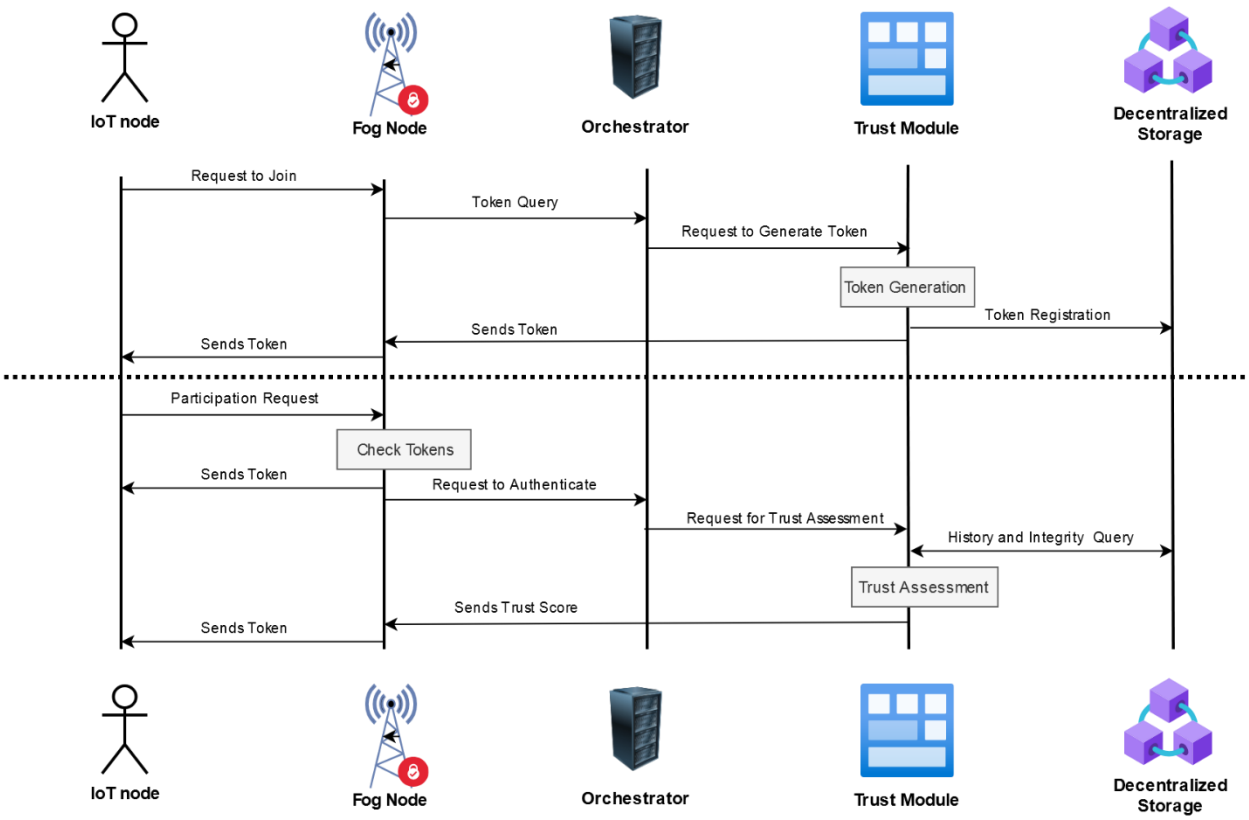


Figure 43. UC3.3 Sequence diagram

The main actors in se case 3.3 include end devices such as IoT nodes, the fog node for local data processing, the orchestrator which can be distributed among many nodes, the trust module for managing the trust and access control, and decentralized systems such as blockchain for storing and verifying trust scores. The sequence begins with the end devices requesting to join the network and being authenticated by the trust module through the orchestrator. The fog node queries the trust module through the orchestrator to check the device's historical trust score. If the score is satisfactory and the attributes are cryptographically authenticated, the end device participates in system tasks such as Federated Learning (FL) by submitting data or model updates, or by establish an end-to-end secure channel with other end devices. The orchestrator continuously monitors and assesses trustworthiness. The device's trust score is updated based on a set of criteria, then stored in the distributed system. Depending on the updated trust score and ability of prove the authenticity and integrity through cryptographic operations, the device may either continue participating or be excluded if it has been flagged as malicious. If malicious behavior is detected, the device's trust token is revoked, and it is marked untrustworthy in the system.

7.3.6. Success factors and selected KPIs

The success factors for the use case 3.3 are:

A-KPI 3.9 - Mean Time to Detect (MTTD): be at a rate of less than 10 milliseconds for rules not based on the ML.

A-KPI 3.10 – Number of False Positive (FP): be at lower than the 1% rate of FP rate.

A-KPI 3.11 – Number of False Negative (FN): be at lower than the 1% rate of FN rate.

A- KPI 3.12 Trust Establishment Time (TET): be at lower than 1s of TET.

7.3.7. Timeline and risks

The expected use case timeline is as follows:

- **Phase 0 – Initial Research (Months 1-3)**
  - Initial research into security and trust management models. This will include exploring models and identifying the possible challenges.
- **Phase 1 – Environment Development (Months 4-10)**
  - Further research and selection of platform and building blocks algorithms.
  - Develop the base architecture for decentralized security and trust management.
- **Phase 2 Implementation and Testing (Months 11-17)**
  - Simulate initial 6G conditions for testing, implement the security and trust management framework, focusing on integrating blockchain with 6G network elements.
  - Begin testing security and trust establishment consensus.
- **Phase 3 – Optimization (Months 18-29)**
  - Optimize the mechanisms for security and efficiency.
  - Simulate fault tolerance under various failure scenarios.
- **Phase 4 – Final Validation (Months 30-36)**
  - Final testing and validation with focus on refining security parameters and ensuring compliance with KPIs
  - Reporting and recommendations for deployment, focusing on risks and security.

The expected use case risks are as follows:

- **Latency Risks**: While available distributed technologies provide high security, the consensus process could introduce delays. Mitigating the latency risk and ensuring the

compliance with the defined KPIs requires precise selection and optimization of fast and lightweight consensus mechanisms.

- **Security Risks**: Despite decentralized control, threats like majority and sybil attacks could undermine security and trust. Continuous monitoring and evaluation of security models will be necessary to mitigate such risks.
- **Hardware and Infrastructure Availability**: As with any advanced use case, the availability of 6G-specific testbed infrastructure could be an issue, potentially delaying certain phases of the use case. This risk can be potentially mitigated by simulating some components of the use case.

8. Use case 4. Improving Variability of Network with Continuous Security

8.1. Use case 4.1 Security Aware placement allocation and monitoring

8.1.1. Domain description

The centralization of network data collection within controllers enables the development of powerful, centralized machine learning (ML)-based attack detection systems. However, this approach presents challenges related to scalability, link overload, and response latency due to the substantial volumes of raw telemetry data transmitted to central AI/ML servers. Moreover, it drastically affects the security of cloud and edge resources, directly exposed to traffic processed at this stage. The Security-Aware Placement Allocation and Monitoring use case (UC4#1) addresses these challenges by offloading security functions to the data plane and optimizing the placement of AI-driven security mechanisms across the network through in-line in-network solutions. This solution aims to reduce the dependency on centralized processing by enabling the deployment of lightweight AI models directly within resource-limited network equipment, close to or embedded within the data plane. This strategy minimizes data transmission overhead and enhances real-time threat detection capabilities. Current implementations of ML solutions in the data plane are still in their early stages, relying on simplified binary neural networks and experimental setups with P4-programmable software switches at lower bitrates. Traditional traffic feature extraction processes occur partially outside the data plane nodes, with AI models predominantly running in centralized or edge-based clusters. This domain seeks to advance these pioneering efforts by fully offloading wirespeed AI models for local processing, thereby improving the scalability and efficiency of security operations across the network. It encompasses the development, placement, and monitoring of AI-driven security functions that can operate efficiently within the constraints of decentralized network environments, ensuring robust, real-time protection against evolving cyber threats.

The use case will rely on the following innovations:

1) The implementation of novel data plane programmability codes capable to implement and support lightweight AI models inside network devices, with the capability to dynamically change the configuration of the model itself through SDN-based, referred to as Wirespeed AI (WAI)

2) The implementation of novel data plane programmability codes capable to extract relevant features from inspected packets and provide per-packet and aggregate values and statistics to internal or external collectors for AI training, referred to as Decentralized Feature Extraction (DFE)
3) The implementation of a security orchestrator logic capable to place, instantiate and configure in real time the deployed data plane codes in the different network devices, based on security awareness information
4) The implementation of a configurable feature telemetry for decentralized training and update of the models

8.1.2. UML diagram

The UML diagram shown in Figure 44 represents the interaction between various actors involved in the UC, a network security system, including Attacker, Data Plane Security Function, AI Engine, and Security Orchestrator.

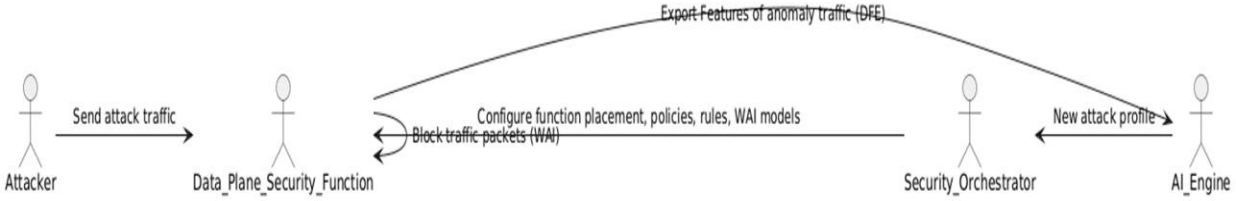


Figure 44. UC 4.1 ML diagram.

The Attacker sends attack traffic toward the Data Plane Security Function (DPSF), indicated by the arrow from the attacker to DPSF. The Data Plane Security Function detects, and blocks traffic packets based on predefined rules and mechanisms like WAI (a mechanism for traffic inspection), represented by a self-looping arrow. The Data Plane Security Function then, in parallel, exports features of the anomalous traffic it has detected to the AI Engine for further analysis. This interaction shows a collaborative process where DPSF supplies data to AI for enhanced threat identification. The AI Engine analyzes the features and detects, if present, a new attack profile, which it shares with the Security Orchestrator. This new attack profile likely contains insights and patterns about the detected anomalies. The Security Orchestrator uses this profile to adjust the security configuration by setting new function placements, policies, rules, and updating WAI models within the Data Plane Security Function, thus refining the security posture of the system. The diagram highlights an adaptive, AI-driven and offloaded approach to network security where the system learns from new attacks and dynamically updates security measures in response, including the placement of data plane functions.

8.1.3. Use case relevance

Use case #4.1's relevance stands in the innovative offloading of security functions at data plane layer, thus further securing the functions themselves together with an expected and significant performance improvement. In addition, the barrier at the data plane is expected to be faster, sustaining higher bitrates (including attacks), liberating resources for applications and functions at the CPU and GPU level.

- Alignment with NATWORK's Objectives: the use case targets NATWORK Objective 2 ("Foster secure-by-design composition and migration of novel 6G cloud-native slices"). In particular, NATWORK exploits the capabilities of programmable data planes like P4 switches and smartNICs to support in-line analytics action types implemented by the data plane of the network. Flexible reconfiguration of the data plane supports various low-level actions like via a predefined API. Existing in-network operations that are critical for the successful operation and attack detection of the 5G network will be migrated to the computing continuum– such services include the deep analysis of control and data plane network traces, allowing the identification of attacks/patterns leading to attacks. Lightweight ML models will be employed, along with high-speed switching fabrics (e.g., P4 Switches and P4 SmartNICs) enabling wire-speed detection and secure distributed computations-network in the edge to cloud continuum.
- Enhancing Security in 6G IoT Networks against threats from IoT environments: security will be enhanced by isolating the attacks at the data plane layer to create a barrier towards control and management planes, and in general isolating edge/data center resources through firewalls in the data plane and offloading-capable network equipment, such as P4 switches and smart NIC.
- Contribution to NATWORK's Innovation and Research: UC4.1 will contribute mainly to the improvement of the overall infrastructure security from a performance point of view (scalability of traffic detection thanks to programmable data planes offloading), and from a sustainability point of view, resorting to the reduction of power consumption due to the offloading of security functions inside programmable devices assumed to be already present in the network infrastructure (i.e., programmable and legacy equipment at the same throughput are demonstrated to consume similar amount of power). Therefore, the position of UC4.1 seems to be placed in area C of the NATWORK use case space, as depicted in Figure 45, in a position where at a fixed level of sustainability corresponds a higher degree of performance level. Based on the level of developed WAI at the data plane level, the UC can be also placed closed to or inside area D, since autoimmunity at the data plane is also one of the goals of the use case and the offloading technologies.

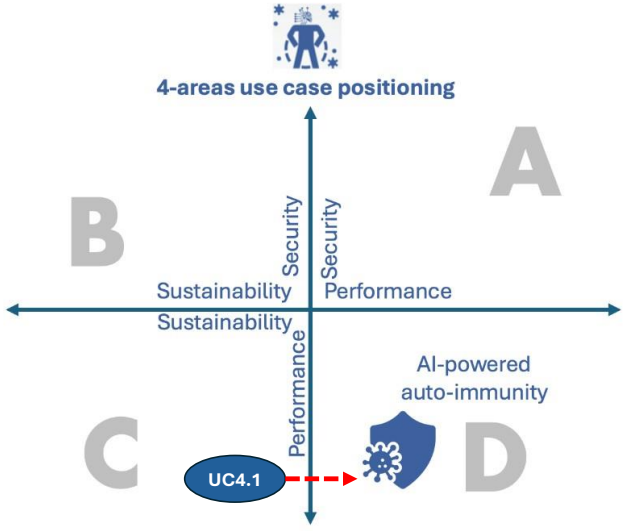


Figure 45. Use case 4.1 osition on NATWORK's conceptual graph

8.1.4. Definition of use case KPIs

The use case KPI are referred mainly to the effectiveness of data plane offloaded solutions to provide rapid, efficient, accurate and configuration-tunable detection of attacks, thanks to real time telemetry of specific features. Another class of KPI is the optimization process of place such data plane functions, assuming that not all places of the network can host such functions, providing a gain for the point of view of energy consumption thanks to the offloading to existing and already utilized hardware resources (switches, smart NIC).

About the data plane implementations performance, we identify the following KPI:

- KPI 4.1.1 DFE processing latency <50us with data plane device scalability up to 10k different flow rules.
- KPI 4.1.2 DFE computational efficiency 50% higher than existing methods (raw in-band telemetry).
- KPI 4.1.3 DFE reduces power consumption by 20% compared to standard software-based feature selection and extraction at the computational engines.
- KPI 4.1.4 WAI-based latency purely on hardware < 10 microseconds, latency on software-based WAI < 100 microseconds.
- KPI 4.1.5 50% less power consumption compared to outsourced AI systems that run on cloud or edge nodes. Our goal is to use hardware accelerations and internal resources of network devices to their fullest potential and avoid utilising dedicated AI resources like GPUs unless absolutely necessary.

8.1.5. Definition of use case testbed requirements

The use case may be evaluated and assessed in multiple testbed configurations, depending on the network segment where the functionality is deployed. For the purpose of NATWORK, the most suitable segment is the core network/metro network segment of the 6G infrastructure, considering both intra- and inter- edge data center scenarios. The motivation relies on the fact that such a solution has the potential to provide an in-line security barrier when aggregate traffic is considered between the RAN and the edge/cloud resources of the applications. In this segment, many users and many applications share heterogenous traffic packets and possible attacks to both cloud/edge resources (e.g., blades, servers, app containers) and specific UE clusters. The detection of security threats may occur at this level for both directions effectively. The main requirements for the testbed are related to the following aspects:

1) Availability of programmable data plane devices (e.g., P4/eBPF/XDP switches, programmable smart NIC with acceleration capabilities)
2) Inter- and intra- edge data center scenarios with Ethernet connectivity from 25Gb/s up to 100Gb/s
3) Availablity of telemetry collectors fed to external AI engines for online training of actual data traffic and anomaly detection of new or future attacks
4) Control and management API for SDN-oriented dynamic configuration of security functions at the data plane (e.g., deployment of function, dynamic configuration at runtime, telemetry configuration and activation)

8.1.6. Sequence diagram of use case workflow

The sequence diagram of the use case is depicted in Figure 46. In the diagram we show the main functional actors involved in the use case, placed at the different network layer. We assume three main layers according to the general Software Defined Network (SDN) architecture. In the application layer, the attackers generate trains of attack packets destined to the different attack targets. In the control/management layer, one or more Security controllers are in charge of deploy, configure and dynamically update the security functions. In addition, at the same level, central or distributed AI collectors are in charge of analyzing anomaly traffic not detected at the data plane (i.e., new attack not in the data plane function repository). Finally, in the data plane layer the main two programmable functions are deployed in different network devices. The two functions are the Wirespeed AI (WAI), the module providing in-line inference of specific attacks, with the possibility of directly blocking the packets, and the Decentralized Feature Extraction (DFE), the module in charge of selecting and extracting the packet network features and make them available at the local WAI module and at the remote collectors, upon request.

The sequence diagram illustrates a scenario that includes the deployment (placement) of the functions and runtime operations with two possible workflows due to two different attack events.

In the case of Attack 1, the selected traffic features are extracted by the DFE and passed locally to the WAI. The module is able to detect the attack since it is in the AI model enforced in the WAI function. This way the attack is blocked once directly at the data plane level, without involving any other layer.

In the case of Attack 2, the first sequences are repeated, however the attack is not covered by the AI model. In this case the attack is not blocked by the WAI in its current configuration. Local or remote triggering activates the DFE module to send feature telemetry to external AI collectors/engines (e.g., federated learning infrastructure) to enable the discovery of the attack type and, possibly, implement security countermeasures. Local triggers may be initiated by the WAI function, for example setting anomaly traffic counters. Remote triggers may occur at the security control level, whereas global anomaly detection sends probability alerts of imminent attacks or new signatures. In the latter case, the controller enables the DFE to stream real time features of the traffic selecting the most appropriate features given the assumed attack type. More than one DFE telemetry producer at the data plane can be activated, in order to detect the source of the attack or the most affected network segments, gateways or surfaces. Federated learning or inference of new attacks should come up with an update of the AI model to be submitted to the WAI module. In particular, in the case of DNN, if the model is the same and the weights are different, hitless configuration may take place thanks to WAI model update functionality. This way, by updating the model and the (optional) feature extraction function, the new attack can be effectively detected, and attack packets may be blocked or diverted to DMZ for further analysis. Several variants of the use case sequence diagram are possible and will be deeply investigated in WP3 and WP4. For example, a tentative sub-workflow running entirely in the data plane including also novel attacks may be considered provided that data plane devices are equipped with efficient AI learning stages (internal GPUs, such as in the case of the NVIDIA

Bluefield-2 with embedded GPU).

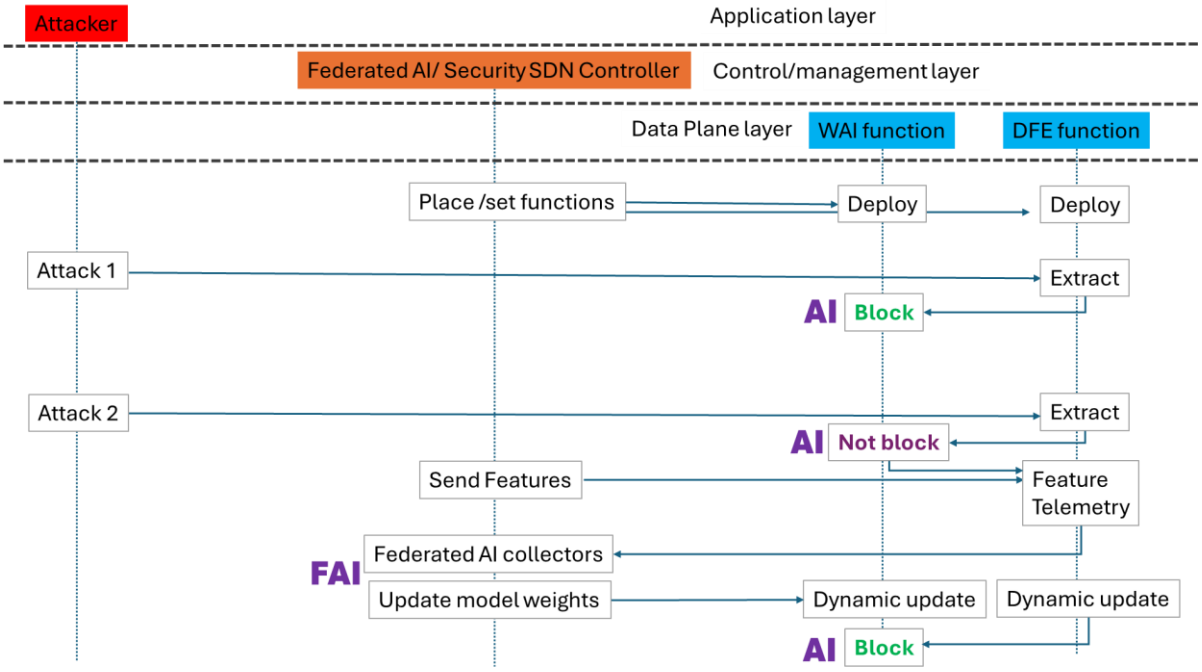


Figure 46 UC 4.1 workflow

8.1.7. Success factors and selected KPIs

- KPI 4.1.1 DFE processing latency <50us with data plane device scalability up to 10k different flow rules.
- KPI 4.1.2 DFE computational efficiency 50% higher than existing methods (raw in-band telemetry).
- KPI 4.1.3 DFE reduces power consumption by 20% compared to standard software-based feature selection and extraction at the computational engines.
- KPI 4.1.4 WAI-based latency purely on hardware < 10 microseconds, latency on software-based WAI < 100 microseconds.
- KPI 4.1.5 50% less power consumption compared to outsourced AI systems that run on
- cloud or edge nodes. Our goal is to use hardware accelerations and internal resources of network devices to their fullest potential and avoid utilising dedicated AI resources like GPUs unless absolutely necessary.

8.1.8. Timeline and risks

The primary development focus of this use case is to extend the SDN data plane programmability platform to support in-line security including inference and automatic feature telemetry

functions, with an emphasis on dynamic security function modifications to follow the traffic patterns. The integration of these technologies aims to enhance performance by enabling dynamic, programmable data flows and offloading certain processing tasks to be accelerated in the data plane, without the need to route critical traffic to CPU/GPU engines inside the edge/cloud data centers.

The detailed use case planning will adapt as work progresses in these areas, specifically targeting the acceleration of runtime processes, the AI onboarding level.

There are potential risks that key functions optimized for x86 and GPU might face limitations when adapted or rearranged within a programmable data plane platform, where there could be lack of ALU logic and memory.

8.2. Use case 4.2 AI aware network slicing for efficient resource utilization and monitoring

8.2.1. Domain description

As communication networks evolve towards 5G and beyond, the complexity and diversity of applications demanding network resources have exponentially increased. The concept of network slicing has emerged as a powerful mechanism to address these diverse requirements by creating multiple virtualized network instances over a shared physical infrastructure. Each network slice can be tailored to specific use cases, such as enhanced mobile broadband (eMBB), ultra-reliable low-latency communications (URLLC), or massive machine-type communications (mMTC), each with its own distinct resource demands and performance characteristics.

AI/ML models are traditionally run on centralized, powerful servers, which require significant computational resources and energy consumption. However, with the advent of network slicing, there is an opportunity to enhance the efficiency and scalability of AI by disaggregating large models into smaller, manageable components. This use case, AI-Aware Network Slicing, aims to distribute the components of a large AI/ML model across various network slices, enabling them to run directly in the data plane relying on less power-hungry devices.

By slicing the AI model and deploying these slices within the network infrastructure, we achieve several advantages. Firstly, the distributed nature of these components reduces the need for high-power centralized servers, thus lowering energy consumption. Secondly, it allows for more efficient use of network resources, as the AI components can be placed closer to where the data is generated, reducing latency and improving response times. Lastly, this approach allows for

more dynamic reconfigurability, as network slices can be adjusted based on real-time demands and the specific requirements of the AI model components.

The AI-aware network slicing approach represents a significant shift in how AI/ML models are deployed and managed in network environments, aligning with the goals of energy efficiency and optimized resource utilization.

8.2.1.1. Functional Requirements

The key functional requirements and their associated challenges are as follows:

Table 31. UC 4.2 Functional requirement

Functional Requirement	Description	Associated Challenges
AI model disaggregation	AI/ML models are disaggregated into slices for deployment across data plane components (switches, DPUs, NICs).	Ensuring the performance of distributed model slices while optimizing resource and energy consumption.
Dynamic slice reconfiguration	Real-time management of AI slices in response to network traffic patterns and workload changes.	Maintaining the functionality of disaggregated models under varying traffic loads without degrading performance.
Localized AI computation	AI workloads are processed at the network's edge, closer to the data source.	Minimizing latency and energy use while ensuring accurate and timely model execution.
Monitoring and verification of AI slices	Continuous real-time monitoring of AI slices to ensure correct execution and performance.	Implementing scalable monitoring mechanisms that do not introduce additional latency or overhead.

8.2.1.2. Enumeration of Functions

The use case includes the following key AI slicing functions:

- **AI model disaggregation**: Large AI models are disaggregated into smaller components, which are distributed across the network's data plane.
- **Dynamic slice reconfiguration**: The AI slices are dynamically adjusted based on network conditions and resource availability.
- **Localized AI computation**: AI processing is performed on edge devices, reducing latency and energy consumption.
- **Monitoring and verification of slices**: AI slices are continuously monitored to ensure they are functioning as expected, and any anomalies or performance degradation are detected in real-time.

8.2.1.3. UML Description

The process of AI-aware network slicing is illustrated in the sequence diagram below.

1. **AI Model Analysis and Slicing**: The large AI/ML model is analyzed and divided into smaller components based on computational requirements, data dependencies, and performance goals.
2. **Deployment of AI Slices**: The AI model slices are deployed across the network, with components placed on programmable data plane devices, edge servers, or other appropriate network elements.
3. **Real-Time Monitoring**: The performance of the AI slices is continuously monitored, to have a detailed understanding of the actual performance and resource utilization.
4. **Dynamic Reconfiguration**: In response to changes in network conditions or application demands, the AI slices are dynamically reconfigured to maintain optimal performance.
5. **Feedback Loop**: Data from the monitoring systems is fed back into the AI model, and if needed the model is resliced and redeployed to continuously improve efficiency.

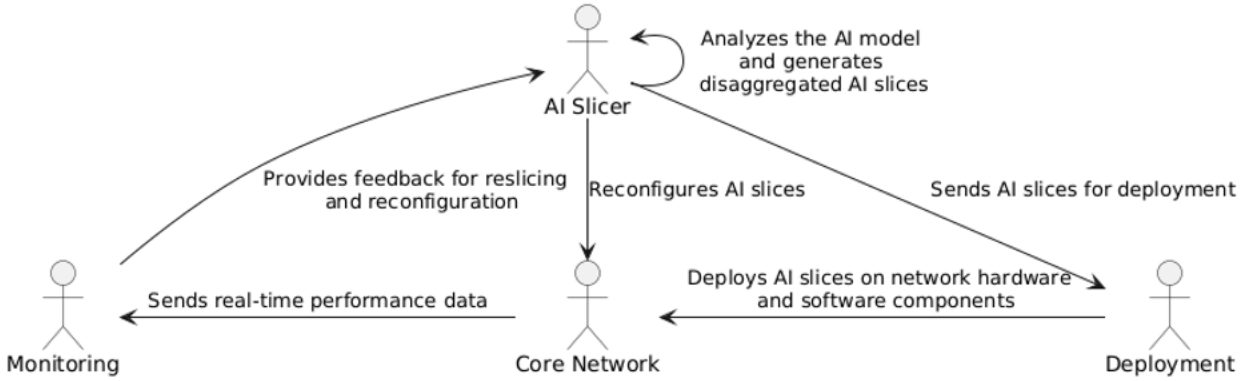


Figure 47. UC 4.2 UML Diagram

8.2.1.4. Challenges Taken Up by the Use Case

The primary challenges addressed by this use case are:

- **Challenge 1**: Developing an efficient and scalable method for disaggregating large AI models and distributing the slices across a highly dynamic and programmable network data plane.
- **Challenge 2**: Ensuring the performance of AI slices under varying network conditions, while minimizing latency and energy consumption.
- **Challenge 3**: Implementing secure, real-time monitoring mechanisms for AI slices without impacting the performance of the network or the model components.

8.2.1.5. Threat Models

Several threat models are tackled by this use case:

- **Tampering with AI slices**: Attackers may attempt to modify or replace disaggregated AI slices as they are deployed across untrusted data plane environments.
- **Reverse engineering of AI models**: The disaggregated nature of AI models may make it easier for attackers to reverse engineer model components and discover vulnerabilities.

8.2.2. Use case relevance

The relevance of this use case lies in its potential to revolutionize the deployment of AI/ML models in network environments. Traditional AI deployment models are becoming increasingly unsustainable as the complexity and size of AI models grows. The AI-aware network slicing approach addresses this by disaggregating the model, distributing the computational load across the network, and utilizing the existing infrastructure more efficiently.

This use case is particularly relevant in the context of NATWORK, where the goal is to design secure, performant, and sustainable AI solutions. AI aware network slicing enables networks to support diverse security applications with varying performance requirements. By integrating AI/ML model slicing into network slicing, operators can not only optimize the performance of AI-driven applications but also reduce the overall energy footprint of the network.

Another key advantage of this approach is its suitability for monitoring the disaggregated components of AI/ML models. By slicing and deploying AI models across the network, each individual component can be closely monitored in real-time. This allows for detailed performance tracking of each model slice, including resource consumption, latency, accuracy, and energy efficiency. Network operators can gain better insights into how each slice performs under different conditions, enabling proactive adjustments to optimize the overall AI model's performance. This distributed monitoring capability is particularly beneficial in dynamic network environments, where traffic loads and resource availability can fluctuate, providing a much-needed level of flexibility and control.

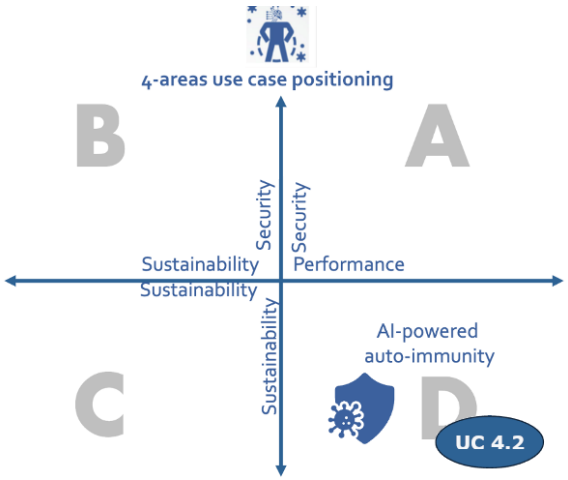


Figure 48. UC 4.2 position on NATWORK's conceptual graph

Based on the description above, the AI-aware network slicing use case can be categorized under area D, as shown in Fig. 9.2.1, as it represents a performance-driven and sustainable solution.

8.2.3. Definition of use case KPIs

The key performance indicators (KPIs) for this use case are centered around the efficiency, reconfigurability, and effectiveness of the AI model slicing and deployment process. The following KPIs will be used to evaluate the success of the AI-aware network slicing approach:

- **KPI 4.2.1: Energy Efficiency Improvement**: The AI-aware network slicing approach should reduce energy consumption significantly compared to traditional centralized AI model deployment.
- **KPI 4.2.2: Latency Reduction**: The deployment of AI slices closer to the data plane should reduce end-to-end latency.
- **KPI 4.2.3: Resource Utilization**: The network resource utilization should be optimized, with at least 50% of the AI model components running on underutilized network resources.
- **KPI 4.2.4: AI Model Accuracy Maintenance**: Despite the disaggregation, the AI model's accuracy should be maintained within 90% of the performance of the centralized model.
- **KPI 4.2.5: Dynamic Reconfiguration Time**: The time required to dynamically reconfigure AI slices to accommodate changes in network traffic should be under a few seconds.

8.2.4. Definition of use case testbed requirements

To effectively test and evaluate the AI-aware network slicing use case, a comprehensive testbed is required that reflects the diverse and dynamic nature of modern networks. The testbed should include the following components:

- **Programmable Data Plane Devices**: Devices such as programmable switches, smart NICs, and edge servers that can host AI model slices and execute them in real-time.
- **AI Model Slicing Tools**: Tools and frameworks for slicing large AI/ML models into smaller components and distributing them across the network.
- **Telemetry and Monitoring Systems**: Systems that can provide real-time feedback on the performance of the AI slices, including energy consumption, latency, and resource utilization.

8.2.5. Sequence diagram of use case workflow

The workflow for the AI-aware network slicing use case relies on several key components as shown in fig. 9.2.2.

The Network Operator initiates the process by sending a large AI model to the AI Slicer, which then disaggregates the model into smaller slices. These slices are sent to the Deployment layer for distribution across network devices like switches, DPUs, and NICs within the Core Network.

After deployment, the AI slices are configured, and Network Devices send real-time monitoring data back to the Monitoring system, which reports performance and resource usage. In the case of malicious or heavy traffic, the Core Network reports this to the AI Slicer, which might request slice adjustments or re-slicing of the model. Monitoring data continues to be sent to ensure real-time performance and fault detection, and the Monitoring system provides comprehensive reports to the Network Operator on performance and security.

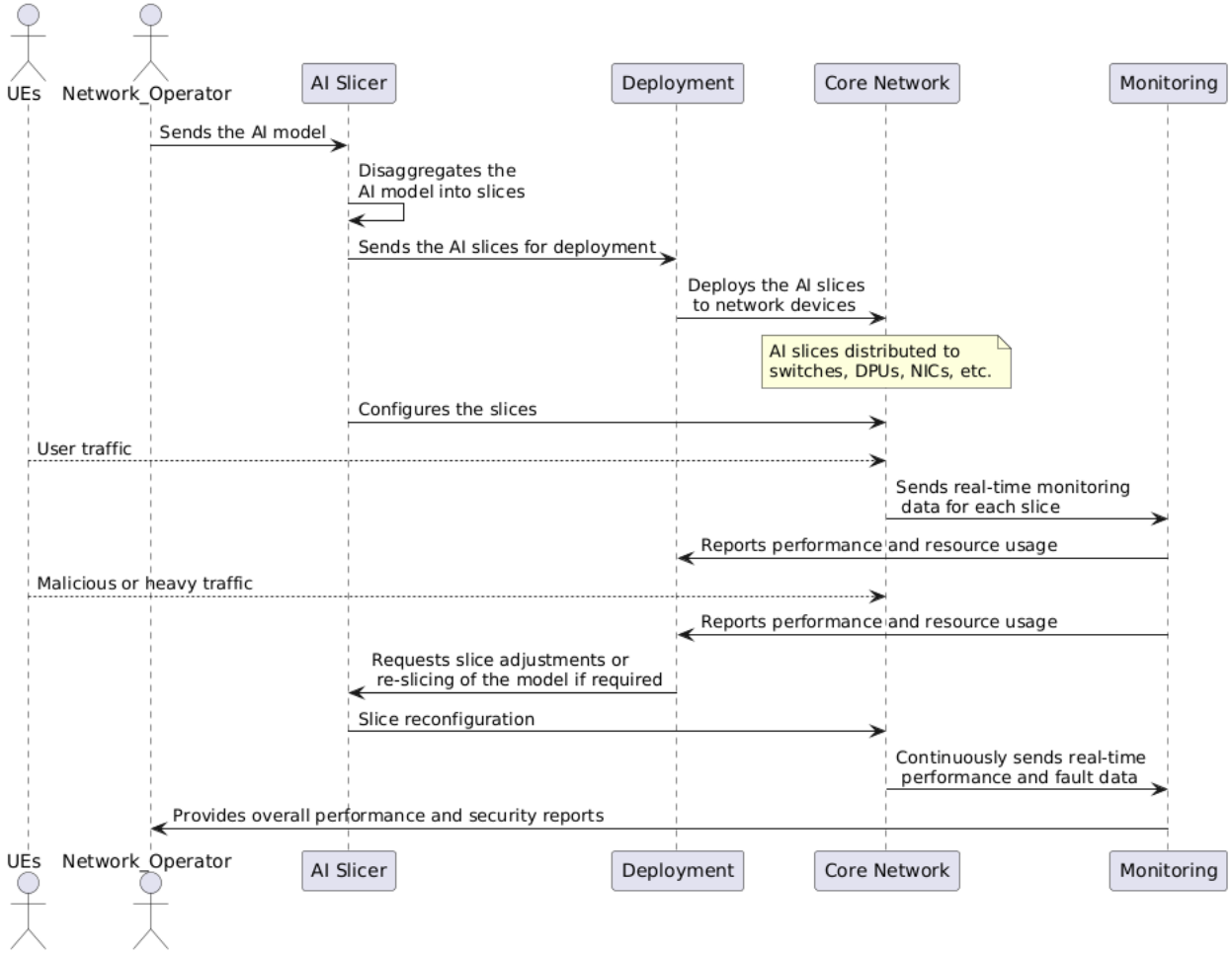


Figure 49. UC 4.2 workflow

8.2.6. Success factors and selected KPIs

The success of the AI-aware network slicing use case will be determined by its ability to achieve the defined KPIs while demonstrating the feasibility and benefits of disaggregating AI/ML models across a network. The selected KPIs include:

- **Energy Efficiency Improvement (KPI 4.2.1)**: Achieving significant energy savings by distributing AI processing across the network.
- **Latency Reduction (KPI 4.2.2)**: Reducing latency by placing AI components closer to data sources and within the data plane.
- **Resource Utilization Optimization (KPI 4.2.3)**: Efficiently using underutilized network resources to run AI components.

- **AI Model Accuracy Maintenance (KPI 4.2.4)**: Maintaining the accuracy of the AI model despite its disaggregation.
- **Dynamic Adaptation (KPI 4.2.5)**: Demonstrating the ability to adapt to changing network conditions in real time.

8.2.7. Timeline and risks

8.2.7.1. Timeline

Phase 0: Initial Research (~3 months)

The first phase will focus on conducting foundational research into AI model disaggregation and slicing. This will include exploring existing techniques for AI model partitioning and identifying the technical challenges associated with deploying AI components in the data plane.

Phase 1: Framework Development and Slicing Design (~12 months)

Following the initial research phase, this stage will focus on the development of a framework for disaggregating large AI/ML models into smaller components. A significant portion of this phase will involve designing how these model slices can be mapped to network devices and creating tools that facilitate the model slicing process. Initial lab tests on small-scale, simulated environments will be conducted to assess the feasibility and basic functionality of the model slicing approach.

Phase 2: Testbed Expansion and Early Testing (~5 months)

During this phase, the testbed will be expanded to include a wider variety of network environments and programmable devices. The AI slices will be deployed on programmable data plane elements (e.g., P4 switches), and initial performance metrics such as energy efficiency, latency, and resource utilization will be gathered.

Phase 3: Optimization and Dynamic Scaling (~6 months)

Building on the early test results, this phase will focus on optimizing the AI slicing framework, with a focus on energy efficiency, latency reduction, and dynamic reconfigurability. Real-time monitoring and feedback systems will be refined to ensure that AI components can adapt to changing network conditions and traffic patterns. Additional features, such as automated slice reconfiguration based on performance metrics, will be introduced and tested under various network loads and conditions.

Phase 4: Large-Scale Testing and Validation

In this last phase, the system will undergo large-scale testing, measuring its performance under high traffic and varying network conditions, with the aim of validating the KPIs defined earlier.

8.2.7.2. Risks:

- **Model Disaggregation Complexity:** Disaggregating a large AI/ML model without significantly impacting its accuracy or performance may prove challenging.
- **Network Infrastructure Limitations:** Programmable network devices and infrastructure may not fully support the deployment of AI slices, necessitating additional development or upgrades.
- **Latency and Performance Trade-offs:** While the goal is to reduce latency, the distributed nature of the AI components might introduce new performance bottlenecks.

8.3. Use case 4.3 Software defined radio for agile payload communication

In the NATWORK project an important aspect is utilizing software-defined radio (SDR) for agile payload communication. SDR is a flexible, reconfigurable system capable of operating across diverse frequencies and protocols. In 6G networks, SDR enables agile payload communication by dynamically assigning payloads to various frequency bands and protocols based on real-time network conditions. Machine learning-driven channel prediction forecasts future channel states and selects the optimal frequency and protocol for agile communication, thereby enhancing overall network performance. AI-powered cognitive radio further optimizes spectrum efficiency by dynamically adjusting frequency bands and protocols according to current network conditions and reduces congestion. Finally, reinforcement learning-based channel switching improves communication reliability by seamlessly transitioning to better channels when current conditions degrade. Generally, this is the approach that will be taken in this use case.

8.3.1. General functional description

Software-Defined Radio (SDR) enables flexible and reconfigurable radio communication by implementing functions in software rather than hardware. This allows SDRs to dynamically select frequency bands and protocols, ideal for use cases requiring adaptability. Machine learning-driven channel prediction [28], [29], anticipates wireless channel conditions, optimizing communication by choosing appropriate frequencies and protocols in real time. Techniques like

deep learning and reinforcement learning predict channel states based on historical and real-time data, enhancing communication reliability and efficiency.

AI-assisted cognitive radio [30]-[32] intelligently manages frequency bands, adapting to network conditions to improve spectrum efficieny and reduce congestion. Traditional systems statically assign frequencies, often leading to underutilization, whereas cognitive radio can dynamically allocate "white spaces." Reinforcement learning (RL)-based channel switching proactively selects the best available channel, crucial for environments like 5G and 6G networks where conditions rapidly change. RL algorithms [33]-[36], such as Q-learning, deep Q-networks (DQN) and multi-armed bandit (MAB), optimize switching decisions by learning from network performance, improving service quality in dynamic and high-stakes applications like vehicular networks and industrial IoT.

Conclusively, algorithms from the fields of machine learning-driven channel prediction, AI-assisted cognitive radio and Reinforcement learning will be appropriately implemented in SDR for Jammer/Adversary attack mitigation in scenarios related to UC 2.1 and UC 4.4.

8.3.2. Use case relevance with NATWORK

This section examines the relevance and relationship of UC4.3 to specific tasks of the NATWORK project. The primary tasks that correspond with UC4.3 are summarized and emphasized in Table below.

Table 32. UC 4.3 relevance with NATWORK tasks

Associated tasks	Focus Areas	Objectives	Key Activities
T4.3 AI-Enabled IDS	Develops a lightweight SDN-based AI-enabled Intrusion Detection System for cloud-based services, focusing on detecting and mitigating security threats efficiently.	- Leverage SDN's centralized data collection with AI's analytical power. - Create a resource-efficient IDS for rapid DoS attack detection and threat analysis.	- SoA ML methods for fast detection. - Thorough threat analysis and IP identification. - Use of OpenFlow protocol for energy-efficient IDS.
T4.3 AI-Enabled Mitigation Engine	Develops an AI Reinforcement learning based mechanism that takes into account multiple metrics (Resource	- Interconnect with the Monitoring tool and AI-Enabled IDS - Provide an automated real-time	- Application of SoA mitigation methods (e.g., from the SDN), development of new ones tailored for the 6G environment (such as those for sensitive network-related

Associated tasks	Focus Areas	Objectives	Key Activities
	Consumption, QoS, Mitigation Time) to select an appropriate mitigation strategy for any anomalies or attack detected.	mechanism to mitigate anomalies	containers) and incorporate frequency and protocol switching using SDR solutions. - Specify metrics for optimum mitigation measures - Research on SoA multi-objective optimization algorithm extensions for faster performance
T5.1	Threat modelling for physical layer	Full and detailed SoA about all the possible attacks in physical layer. Categorization based on techniques and protocol.	Application of the suggested techniques for adversary detection and mitigation according to current SoA methodology.
T5.3	AI-leveraged anti-jamming	Detection and mitigation of a jamming attack in mmWaves and THz bands. Utilization of beamforming techniques and adaptive modulation as a jamming protection method. Investigation of Physical Layer Key Generation (PKG) usage	Investigation of the SDR capability of band switching in case of jamming attacks.
T5.4	MIMO & RIS Surface Defense Mechanism	Usage of RIS and MIMO for enhanced communication links quality. Usage of RIS for beam-splitting, sensing and localization purposes within the communication network for further safety and protection.	Investigation of the MIMO & RIS benefits for adversary detection on the performance of band and protocol switching via SDR.

The positioning of UC 4.3 in NATWORK's conceptual graph is presented in Figure 1.

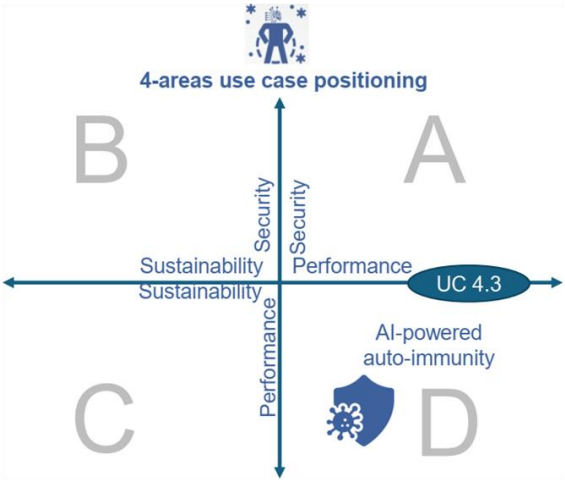


Figure 50. UC 4.3 position in NATWORK's conceptual graph

8.3.3. Description of the use case KPIs

The KPIs, relevant to this UC are the following:

- A-KPI 4.6: Jamming/adversary attacks mitigation (at least 80% accuracy in unjammed signal recovery)
- A-KPI 4.7 Time needed to mitigate a jamming/adversary attack via AI/ML frequency and protocol switching (target <5s)
- A-KPI 4.8 Time needed to recover from a jamming attack (target < 10s)
- A- KPI 4.9 Downtime reduction (less downtime at least 20%)
- A- KPI 4.10 At least 40 %, expected throughput improvement during jamming/adversary attack.

According to current SoA methods the suggested KPI values are summarized in the table:

Table 33. Description of the use case testbed requirements

KPI	Target values
A-KPI 4.6	At least 80% recovery accuracy of unjammed signal
A- KPI 4.7	10 sec
A-KPI 4.8	10 sec
A-KPI 4.9	Not relevant
A-KPI 4.10	Throughput metric defined based on the experimental testbeb

In CERTH, a lab section has been constructed that enables experiments on various anti-jamming scenarios. An important component of the experimental setup is the SDR which is programmed

via the GNU Radio open-source toolkit for signal processing. The chosen SDR units are the commercially available USRPs (Universal Software Radio Peripherals), which function as the hardware interface for radio signals transmission and reception. The equipment is calibrated for real-time monitoring of signal quality and strength at the receiver, aiming to evaluate the effectiveness of anti-jamming techniques. Data collected from the experiments is stored in a shared database for further analysis.

The capabilities of the SDR system will be extended with the use of a Daughterboard. A **Daughterboard (DoD Board)** for **Software-Defined Radio (SDR)** is an additional circuit board or module that attaches to an SDR platform (usually the mainboard). These boards typically handle tasks like **radio frequency (RF) front-end** operations, enabling the SDR to transmit and receive signals over a wider range of frequencies. It extends the SDR's frequency range to lower or higher frequency bands enabling WiFi, Cellular or even Satellite applications. It usually contains RF circuits allowing RF Signal Processing operations such as mixing, amplification or filtering. DoDs can handle transmitters, receivers and full-duplex communication allowing simultaneous transmission and reception.

Additionally, they exhibit modularity allowing swapping them depending on the application or frequency range and they are programmable to work with various communication protocols, LTE, Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15.1), Zigbee (IEEE 802.15.4) and 5G NR.

8.3.4. UML diagram

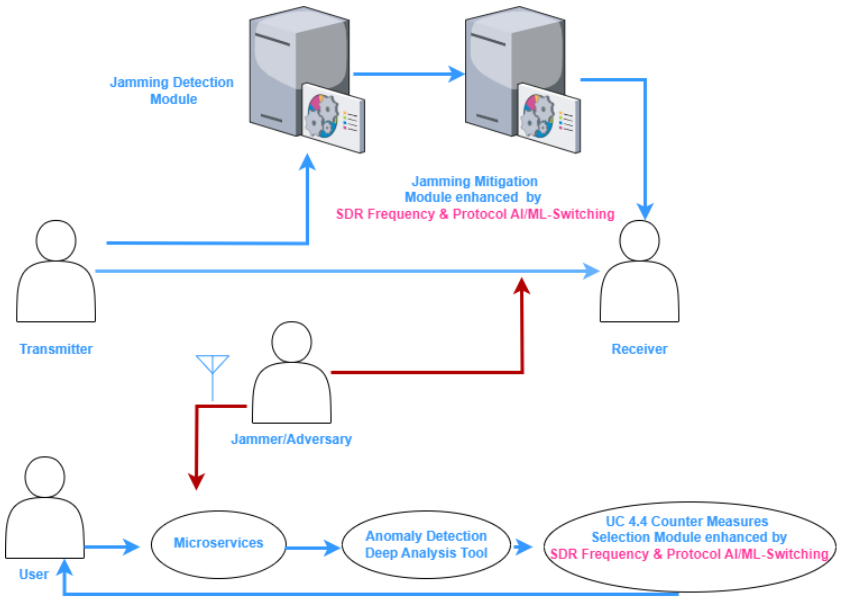


Figure 51. UC4.3 UML diagram, (Adversary atacks of UC 2.1 upper part and UC 4.4 lower part)

8.3.5. Sequence diagram of use case workflow

The sequence diagram for UC 4.3 follows:

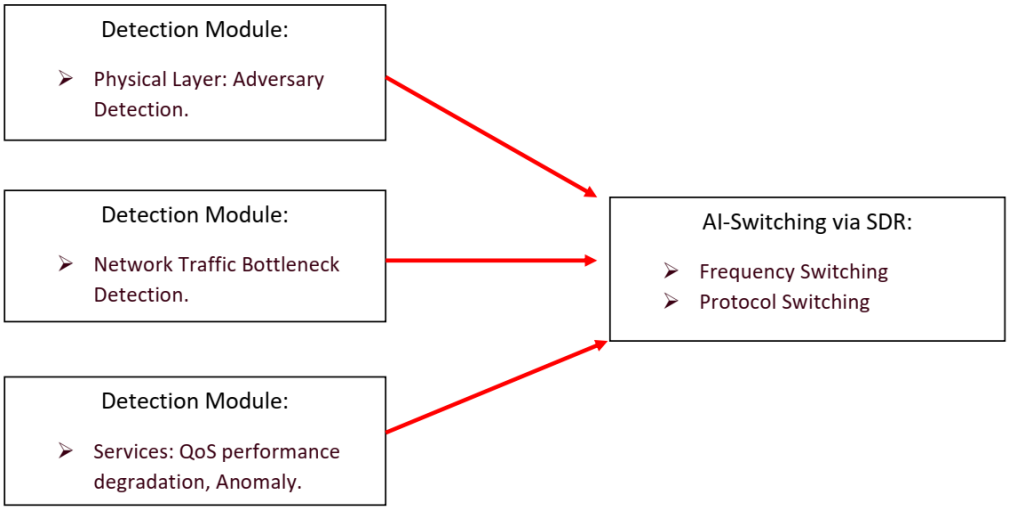


Figure 52. UC 4.3 general sequence diagram

It consists of a detection module containing three sub-modules. A Physical Layer sub-module responsible for the detection of an adversary attack i.e. Jamming, Spoofing etc. A module responsible for the network traffic bottleneck detection and a sub-module that detects a QoS performance degradation or anomaly in the Services. Existing Machine Learning methods will be used to implement the detection modules. Depending on the type of detection, appropriate generated measures (Frequency or/and Protocol switching based mainly on RL) are taken and implemented via SDR [36].

8.3.6. Timeline and risks

UC 4.3 will be considered complementary mainly to UC 2.1 and also to UC 4.4 therefore they have similar timelines and risk factors. In particular the adversary detection and mitigation mechanisms will be systematically evaluated. Alongside the main activities, inputs and outcomes from T5.1, T5.3, T5.4 and T4.3 will be incorporated as much as feasible, and this integration should be reflected in the UC timeline.

8.3.6.1. 1.1.6.1. Timeline

Initial Phase (Months 4-12):

- **Models for Jamming Detection**: AI/ML models suitable for jamming detection will be tested. Different architectures and cutting-edge approaches will be explored to enhance accuracy and robustness against various types of jamming attacks and network characteristics.
- **Jamming Mitigation Methods**: AI/ML and Signal processing techniques will be explored for channel estimation both in the presence and absence of a jammer. Furthermore, appropriate denoising filters will be identified and AI-SDR frequency or protocol switching will be implemented as an additional measure.
- **Task T5.1:** An analysis of the state-of-the-art (SoA) in physical layer attacks, including extreme cases and potential risks, will be considered for the suggested solutions to satisfy the challenges in the field.

1. **Development Phase (Months 13-24)**:
   - **Main Solution**: The integrated core solution will be finalized by month 18, serving as the basis for incorporating contributions from the relevant tasks.
   - **Evaluation of the main solution in the experimental testbed (Month 18)**
   - **Task T5.3**: Once the main solution is completed, the next step will be to extend the detection model to higher frequency bands. Additional protection mechanisms, such as ML-based beamforming, adaptive modulation schemes, PKG and SDR-based frequency and protocol switching, will also be explored. After development and evaluation in a simulation environment, these mechanisms will be gradually integrated into the core solution.
   - **Task T5.4:** An initial assessment of the RIS units and their capabilities will be carried out. Key RIS functionalities relevant to enhancing detection, mitigation, and jammer property identification will be outlined. Furthermore, a codebook for the RIS will be created.
   - **Task T4.3**: During Months 20-24, in conjunction with UC 4.4, development of AI-powered intrusion detection systems (IDS) for cloud services. This phase will explore the potential of performance improvement via SDR frequency and protocol AI/ML switching.
2. **Testing and Validation Phase (Months 25-30)**:
   - **Enhanced Solution (Month 25-30)**: The impacts of T5.3, T5.4 and T4.2 as well as the transfer of the implemented methods and techniques from the simulation environment to the experimental testbed, will be studied and analyzed. Detailed testing and validation procedures will be performed.
3. **Final Phase (Months 31-36)**:

- **Final System Integration and Evaluation (Month 32)**: Finalize the integration of all components and conduct a comprehensive evaluation of the performance and robustness of the anti-jamming system.
- **System Validation and Lessons Learned (Month 36)**: Final validation will take place, and the lessons learned will be documented for future iterations and implementations in real-world 6G environments. The feasibility of conducting a final evaluation under actual conditions at CERTH AV will be evaluated from both technical and legal standpoints.

8.3.6.2. Risks

The main risks in terms of UC 4.3 are collectively presented as:

1. **Synchronization and Channel estimation in MIMO networks**:
   - **Risk**: Synchronization and precise channel estimation in MIMO networks encounter several challenges, which are further complicated by the limitations of existing experimental testbeds.
   - **Mitigation**: Advanced techniques, such as sparse signal recovery methods and AI, will be utilized to achieve accurate and timely estimations.
2. **Utilization of AI/ML tools in the real-time conditions**:
   - **Risk**: AI/ML tools may are computationally demanding therefore their execution times must be minimized to be practically feasible.
   - **Mitigation**: Parallelization approaches and fast alternative methods will be investigated to decrease computational time.
3. **RIS Codebook procedure**:
   - **Risk**: Creating a RIS Codebook that encompasses all essential functionalities is both a difficult and computationally demanding problem.
   - **Mitigation:** Physics-based models in conjunction with metaheuristic methods will accelerate training.
4. **Integration of the components**:
   - **Risk**: The variety of the proposed solutions will probably lead to increased complexity and computation time during their integration.
   - **Mitigation**: Initially the final solution will comprise of only the essential components for optimal collaboration and flexibility. Additional efforts could be made to go beyond the essential components if research supports that such actions will offer beneficial advantages.
   -

8.3.7. Summary

- Use Case 4.3 works in tandem with UC 2.1 and UC 4.4. In UC 4.3, an intelligent ML/AI-driven protocol and frequency switching via SDR is introduced as an additional adversary-attack mitigation measure, supplementing the strategies outlined in UC 2.1 and UC 4.4.
- The mitigation approach in UC 2.1 includes Physical Key Generation, MIMO Synchronization, and ML-based Beamforming and Denoising Filtering, which can be further supported by the ML/AI frequency and protocol switching from UC 4.3, if necessary.
- Additionally, in Task 4.3 of UC 4.4, state-of-the-art (SoA) mitigation techniques for 6G networks will be applied, reinforced by the ML/AI frequency and protocol switching from UC 4.3.

8.4. Use case 4.4 AI driven orchestration of micro services

This use case focuses on the efficient management of cloud services to ensure Quality of Service (QoS) even in the presence of undetectable attacks, such as zero-day exploits. The complexity of 6G systems, due to the coexistence of multiple technologies, introduces new security threats and vulnerabilities. Therefore, it is essential to ensure the provisioning of network services even when an attacker cannot be immediately detected.

To achieve this, machine learning mechanisms based on cloud monitoring data will be employed to detect anomalous behaviors in the system that may result from malicious activities. These mechanisms include:

1. **Microservices Profiling:** Pre-process procedures to map the behavior of microservices under normal traffic and workload conditions.
2. **Real-time Anomaly Detection:** Online procedures for detecting irregular resource usage patterns indicative of potential attacks.
3. **Risk Classification:** Classification of network load based on the degree of risk targeting to the isolation malicious traffic.
4. **Automated Anomaly Mitigation:** Online procedures that try to heal, mitigate or deflect detected anomalies or attacks

Following the detection of potential threats, the system will orchestrate microservices effectively, including the implementation of network policies like load balancing, to ensure continuous provision of 6G services until the attacker is detected and mitigated.

8.4.1. Domain description

In the context of 6G networks, the AI-driven orchestration of microservices enhances network flexibility, efficiency, and adaptability. Microservices architecture, which breaks down applications into smaller, decoupled services, is particularly well-suited for dynamic 6G environments. These environments require rapid deployment and scaling of services, adaptive resource allocation, and real-time decision-making. AI integration facilitates intelligent orchestration, allowing AI algorithms to manage and optimize the deployment, scaling, and operation of microservices based on real-time data and predictive analytics.

We aim at microservices designed to have specific impacts on the resources, such as some being CPU-intensive and others being network-intensive. We assume that in the event of an attack, anomalies from attacks will be reflected on the resources allowing the system to detect unusual activities, even when the type of attack is unknown to the system.

Functional Requirements and Challenges:

- **Dynamic Resource Management:** The orchestration system must dynamically allocate resources (CPU, memory, bandwidth) across microservices, optimizing for performance, energy efficiency, and cost.
- **Real-time Adaptation:** The system must adapt to changing network conditions, user demands, and service requirements in real time, ensuring QoS consistency.
- **Scalability:** The framework should handle the deployment of microservices across a distributed 6G network infrastructure, scaling up or down as needed.
- **Resilience and Fault Tolerance:** The system must detect and mitigate failures in microservices or underlying infrastructure, ensuring service continuity.
- **Security:** The orchestration process must incorporate security measures to protect microservices from attacks and ensure data integrity and confidentiality.

8.4.1.1. High-level functional description (UML)

The UML diagram of UC4.4 represents the workflow for detecting and responding to anomalies in a microservices-based environment within the NATWORK system. The diagram breaks down the interactions among key actors in the system to illustrate the flow of monitoring data, anomaly detection, and subsequent mitigation actions.

Key Workflow Steps:

1. **User Traffic and Malicious Traffic:** The sequence begins with user traffic being processed by the system. Malicious traffic is also introduced, representing potential attacks on the microservices infrastructure.
2. **Microservices Deployment:** The microservices deployment in this sequence diagram refers to the deployment of microservices-based network functions within the 6G infrastructure, as well as other services within the broader 6G ecosystem, whether in the core network or at the edge cloud.
3. **Monitoring Broker:** The broker collects monitoring data from the SDN network, including both traffic statistics and microservices' resource consumption. This data is passed on to the next stages for deeper analysis.
4. **Statistical Analysis Tool:** The monitoring data is processed by the statistical analysis tool, which is tasked with detecting anomalies. If any irregularities are found, the system signals the deep analysis tool for further investigation.
5. **Deep Analysis Tool:** Once an anomaly is detected, the deep analysis tool performs a more granular inspection (based on AI mechanisms) to identify the nature of the threat. It retrieves details such as the type of attack, the resources affected, and attackers' IPs. This information is essential for defining the appropriate countermeasures.
6. **Countermeasure Selection:** Based on the insights from the deep analysis tool, appropriate countermeasures are proposed and established to mitigate the attack. These measures ensure the integrity and performance of the system while preventing further damage from the detected anomaly.

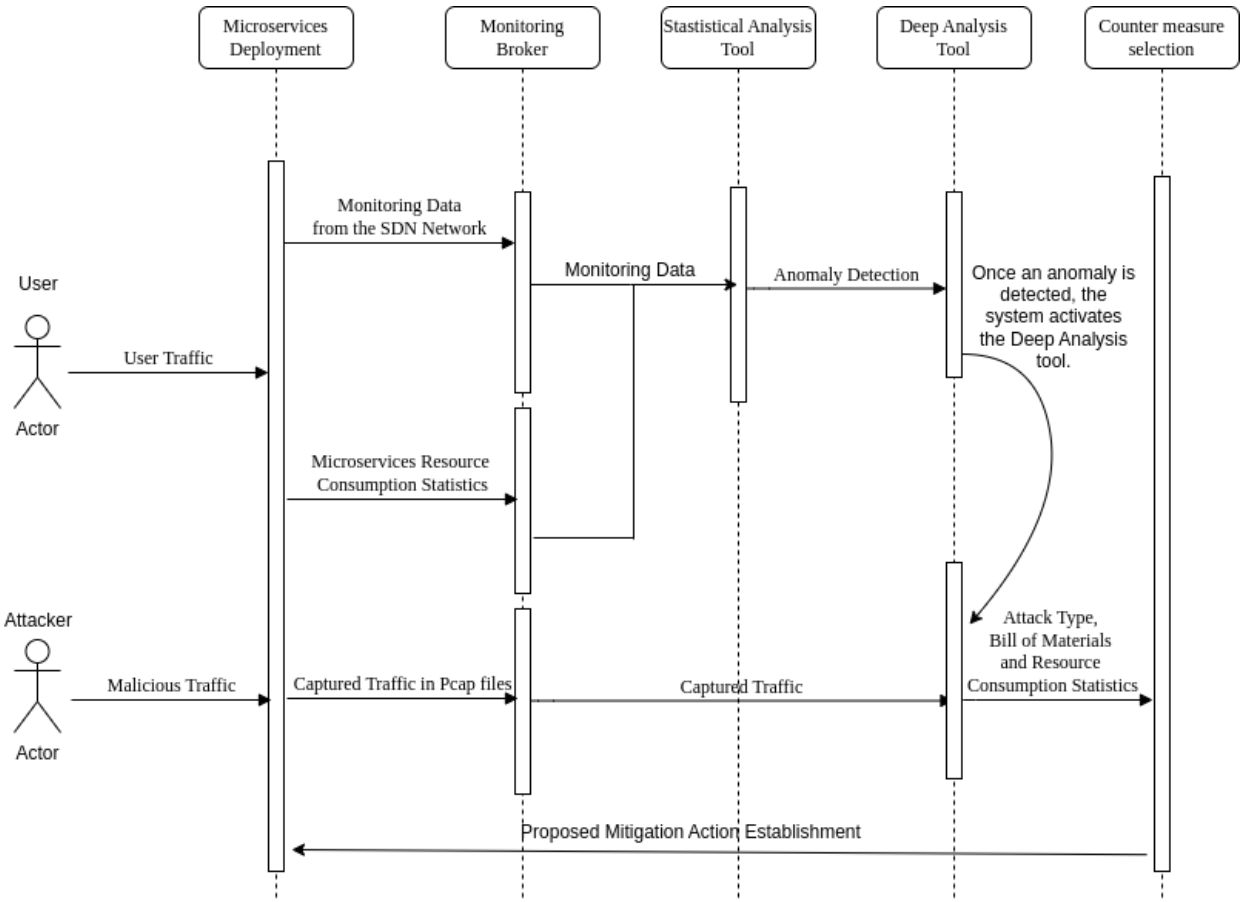


Figure 53.UC4.4 Sequence diagram

8.4.2. Use case relevance with NATWORK

Use case 4.4 is closely aligned with the core objectives of the NATWORK project by addressing the challenges of maintaining secure and efficient 6G services in dynamic environments. The use case focuses on AI-powered mechanisms to detect anomalies, allocate resources dynamically, and ensure service continuity even in the face of undetectable threats like zero-day attacks. This directly supports NATWORK's objective of delivering end-to-end security (OO#1) and developing AI-driven security frameworks (OO#2), as it provides real-time response capabilities to emerging threats while optimizing network performance and energy efficiency.

In the NATWORK conceptual graph (illustrated by the 4-areas use case positioning diagram), UC 4.4 is positioned in Area A, where security and performance converge. This positioning reflects the core goal of using security mechanisms to support performance guarantees. In distributed microservice environments, security breaches can degrade performance, leading to increased latency, service disruptions, or even complete failure. By integrating AI-driven orchestration, the

system can adaptively handle security threats in real-time, ensuring the network's performance is unaffected by potential threats.

The AI in this use case dynamically monitors and manages security parameters, ensuring that performance is guaranteed even under heavy loads or during cyber-attacks. This close link between security and performance ensures seamless service delivery across the network, aligning perfectly with NATWORK's objective of creating a secure, high-performance 6G ecosystem.

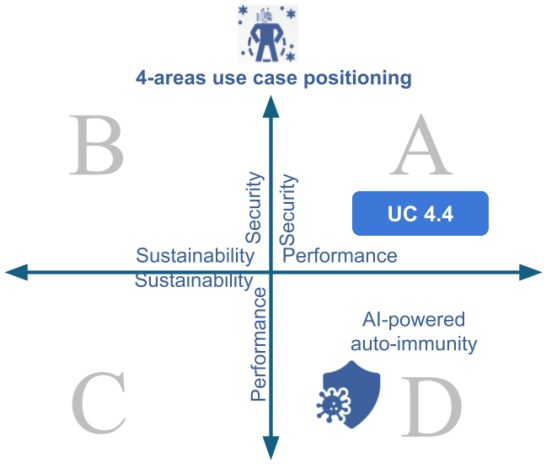


Figure 54. UC4.4 position in NATWORK's conceptual graph

In this use case, several key subsystems within the NATWORK project will be utilized to enhance network performance, security, and efficiency in 6G environments. These subsystems are investigated across different work packages and tasks within the project. Below, the tasks that will be evaluated in this context of UC4.4 are presented:

Table 34. UC 4.4 Functional requirements

Associated tasks	Focus Areas	Objectives	Key Activities
T3.3 AI-Driven Orchestration	Focuses on AI-driven orchestration, efficient resource management, and robust security measures to enhance NATWORK's AIaaSecs system in 6G environments.	- Ensure efficient cloud service management and maintain QoS in undetectable attack scenarios (zero-day). - Address security vulnerabilities in 6G	- Develop and investigate microservice profiling techniques. - Estimate compute and network resource impact. - Use anomaly detection to identify zero-day attacks.

Associated tasks	Focus Areas	Objectives	Key Activities
		systems. - Develop ML mechanisms.	- Energy-efficient microservice placement.
T3.4 Kubernetes Security	Evaluates and enhances container security within Kubernetes clusters, addressing known vulnerabilities and proposing effective remediations.	- Understand Kubernetes security services. - Identify security gaps. - Propose remediations using AI/ML techniques for enhanced security.	- Survey existing security services. - Identify security gaps in Kubernetes. - Develop remediation strategies (e.g., security policies and controls).
T4.2 Monitoring Tool	Develops a monitoring tool to track microservices' resource consumption, focusing on CPU, memory, and network statistics, under various attack scenarios.	- Implement advanced anomaly detection for identifying potential attacks. - Optimize resource monitoring for efficiency and accuracy.	- Develop a monitoring tool using Docker API. - Investigate HTTP/2-based DoS attacks. - Experiment with containerized services (Open5G, Free5G, NGINX).
T4.3 AI-Enabled IDS	Develops a lightweight SDN-based AI-enabled Intrusion Detection System for cloud-based services, focusing on detecting and mitigating security threats efficiently.	- Leverage SDN's centralized data collection with AI's analytical power. - Create a resource-efficient IDS for rapid DoS attack detection and threat analysis.	- Combine statistical ML approaches with AI for quick detection. - Provide detailed threat analysis and IP identification. - Utilize OpenFlow protocol for energy-efficient IDS.
T4.3 AI-Enabled Mitigation Engine	Develops an AI Reinforcement learning based mechanism that takes into account multiple metrics (Resource Consumption, QoS, Mitigation Time) to select an appropriate mitigation strategy for any anomalies or attack detected.	- Interconnect with the Monitoring tool and AI-Enabled IDS - Provide an automated real-time mechanism to mitigate anomalies	- Leverage existing mitigation (e.g. from the SDN) capabilities and develop new ones for the 6G context (e.g. for sensitive network related containers) - Identify the appropriate metrics for efficient mitigation choice - Extend existing SoA multi-objective optimization algorithm for faster performance

These tasks contribute to the effectiveness of the AI-driven orchestration of microservices, addressing various challenges such as resource management, security, and scalability in a 6G network environment. Each task plays a crucial role in ensuring the seamless operation and security of the network services in the face of potential threats, aligning with the broader objectives of the NATWORK project.

8.4.3. Definition of the use case KPIs

In Use Case 4.4, the primary focus is on the efficient allocation of network traffic among microservices by utilizing AI-based techniques such as load balancing and the dynamic scaling (elasticity) of microservices according to network load. The main goal is to efficiently manage the performance of the system, which is composed of various microservices, by addressing key aspects such as performance (delay, throughput), reliability (packet loss), and fault tolerance (avoiding microservice overload).

During the experiments, various attack scenarios, such as DoS attacks, will be conducted to evaluate the effectiveness of NATWORK mechanisms in several areas:

- **Maintaining Performance Under Attack Conditions**: Ensuring the system's performance remains stable even when under attack.
- **Attack Detection Time**: Measuring how quickly the system detects an ongoing attack.
- **Mitigation Time**: Evaluating the time taken to mitigate or neutralize the detected attack.

To measure the success of these objectives, the following KPIs will be used:

- **KPI 4.4: Probability of DoS Attack Detection > 80%**: The goal is to achieve a high probability of detecting DoS attacks using the AI-driven mechanisms developed within the project. In Use Case 4.4, achieving this level of detection probability is crucial for ensuring that the orchestration system can effectively respond to security threats and maintain service continuity.
- **KPI 4.5: Probability of False Detection < 10%**: This KPI targets a low rate of false positives in detecting DoS attacks. For Use Case 4.4, minimizing false detections is critical to avoid unnecessary mitigation actions that could disrupt service performance and reliability.

These KPIs provide a targeted and precise evaluation of the system's performance, reliability, and resilience, particularly in scenarios where the system is subjected to various forms of cyberattacks. By focusing on the detection and mitigation of DoS attacks, as well as maintaining

high levels of performance and minimizing false positives, these KPIs will guide the further development and refinement of the NATWORK mechanisms to ensure robust, secure, and efficient microservice orchestration in 6G networks.

In addition to the aforementioned KPIs, several performance metrics will be utilized to assess the success of the system in achieving its objectives. These metrics include:

- **Performance Under Attack**:
  - **Goal**: Maintain stable system performance even during cyberattacks like DoS.
  - **Measurable Outcome**: Performance indicators such as latency, packet loss, and throughput should stay within defined limits during stress testing (e.g., <20% degradation in throughput during DoS attacks).
- **Detection Time for Anomalies**:
  - **Goal**: Improve detection and response to security threats using AI-driven anomaly detection.
  - **Measurable Outcome**: The system should detect anomalies within **5 seconds** for minor deviations and under **3 seconds** for critical threats like DoS attacks, ensuring minimal impact on network performance.
- **Mitigation Response Time**:
  - **Goal**: Efficiently mitigate threats.
  - **Measurable Outcome**: Mitigation mechanisms should neutralize or isolate detected attacks within **2 seconds** after detection, ensuring less than **10% downtime** for affected services.
- **Microservice Scalability and Elasticity**:
  - **Goal**: Ensure smooth scaling of microservices in response to traffic loads.
  - **Measurable Outcome**: Test the system's ability to scale microservices dynamically, with scaling actions completing within **<3 seconds** and maintaining optimal CPU and memory usage across all active services.

These KPIs will provide a comprehensive evaluation of the system's performance, reliability, and resilience, particularly in scenarios where the system is subjected to various forms of cyberattacks. The results from these evaluations will inform further development and refinement of the NATWORK mechanisms to ensure robust, secure, and efficient microservice orchestration in 6G networks.

8.4.4. Description of the use case testbed requirement

The implementation, experimentation, and evaluation of Use Case 4.4 will be conducted on the CERTH 5G-SDN testbed, utilizing the infrastructure and tools designed for experimentation in 5G and beyond environments. This testbed provides the necessary resources and services to support the AI-driven orchestration of microservices and the analysis of various attack scenarios. A suite of attacks, primarily focusing on DoS attacks on different network protocols (including HTTP/2 flooding attacks), has been developed by CERTH and will be utilized in this use case.

- **SDN-based 5G Core Network**: The testbed's SDN interconnected 5G network elements will be used to manage the microservices and control the traffic flow dynamically.
- **Kubernetes API**: Kubernetes will be utilized for managing containerized microservices, enabling efficient resource allocation and scaling based on the network load.
- **Open5G and Free5G Core 5G Network Functions**: These containerized network services will be employed to manage the 5G core components and experiment with various attack scenarios, particularly focusing on network-based attacks such as HTTP/2-based DoS attacks.
- **Containerized Services**: Key containerized services that will be considered include:
    - Containers from 5G core (Open5G and Free5G)
    - NGINX server
    - Metasploitable Docker images
- **AI-Enabled Intrusion Detection System (IDS):** This tool will be used to detect and mitigate security threats in real-time, particularly focusing on identifying anomalies and unauthorized access within the microservices environment.
- **SDN-Based Microservices Resource Consumption Monitoring Tool**: This tool will monitor the CPU, memory, and network usage of microservices to detect any anomalies that could indicate a security breach or system inefficiency.
- **AI-Enabled Mitigation Engine:** This tool will mitigate security threats and anomalies in real-time focusing on the microservices environment.

These technologies and tools will be critical in evaluating the following aspects of the services provided:

- **Reliability**: Ensuring consistent service delivery and minimizing packet loss even under stress conditions.
- **Fault Tolerance**: Maintaining service continuity by effectively handling microservice failures and overloads.

- **Quality of Service (QoS)**: Maintaining optimal performance in terms of latency, throughput, and resource utilization efficiency, even in the presence of network-based attacks.

The CERTH testbed, with its comprehensive set of tools and resources, provides an ideal environment for testing and refining the AI-driven orchestration mechanisms required for resilient and efficient 6G networks.

8.4.5. Sequence diagram of use case workflow

The sequence diagram of Use Case 4.4 (AI-driven orchestration of microservices) demonstrates the workflow for orchestrating distributed microservices in an SDN-based 6G environment/ecosystem, integrated with AI-based anomaly detection and Intrusion Detection Systems (IDS). This workflow ensures continuous monitoring and adaptive responses to security threats in a distributed architecture.

Workflow Overview:

The UC 4.4. workflow overview is detailed through the description of the functionalities of the main system's components.

1. **SDN Controller**: The SDN controller is the central control point of the network and is responsible for the access control rules establishment and centralized data collection. The controller governs the overall interaction between the network nodes (servers) and the external actors, ensuring proper communication and resource allocation.
2. **SDN Network**: The SDN network serves as the communication medium between legitimate users and potential attackers. It enables the identification and control of malicious IP addresses, ensuring that the network can handle both trusted and untrusted traffic dynamically. The system has the capability to flag multiple malicious IP addresses at once, enabling swift containment of potential threats.
3. **Microservices Hosted on Distributed Servers**: Different servers are considered, each hosting a set of microservices equipped with monitoring agents. These agents are responsible for collecting key performance metrics such as CPU usage, memory consumption, and overall network resource utilization. The microservices architecture ensures that the system is modular, scalable, and capable of adapting to varying loads and network conditions.

4. **Statistical Monitoring and Anomaly Detection**: Each server continuously reports performance statistics to a central anomaly detection module. This module utilizes simple statistical models to baseline normal operations. If an anomaly is detected—such as unexpected spikes in CPU or memory usage—the system escalates the incident by activating the **AI-Enabled IDS**.
5. **AI-Enabled Intrusion Detection System (IDS)**: Upon detection of an anomaly, the system transitions to a more advanced layer of security involving the AI-Enabled IDS. The IDS uses machine learning algorithms to analyze the captured network traffic and PCAP files for any signs of malicious activity. This AI-driven component is crucial in refining the system's ability to detect sophisticated threats, allowing it to react more intelligently over time as more data is analyzed.
6. **PCAP Files**: As part of the continuous monitoring and response loop, packet capture (PCAP) files are generated and fed back into the AI-IDS. These files provide granular information about network traffic, which the IDS uses to improve the accuracy and efficiency of its anomaly detection. The feedback loop ensures that the system evolves based on real-time network behavior, minimizing false positives while enhancing threat detection capabilities.

Key Features:

- **Real-Time Monitoring**: Continuous data collection and analysis from multiple sources (servers) ensure that the system is always aware of its performance and security status.
- **AI Integration**: AI enables the system to improve its detection capabilities over time, learning from historical data and new threat patterns.
- **Scalable Microservices Architecture**: The use of microservices allows for dynamic scaling and adaptability, ensuring that the system can handle varying loads without sacrificing performance.
- **Proactive Defense**: The system's ability to identify and manage malicious IP addresses, combined with AI-driven anomaly detection, creates a proactive defense layer against network attacks.

This workflow exemplifies NATWORK's goal of developing a secure, resilient, and adaptive network environment that harmonizes performance and security in a scalable, distributed microservices framework.

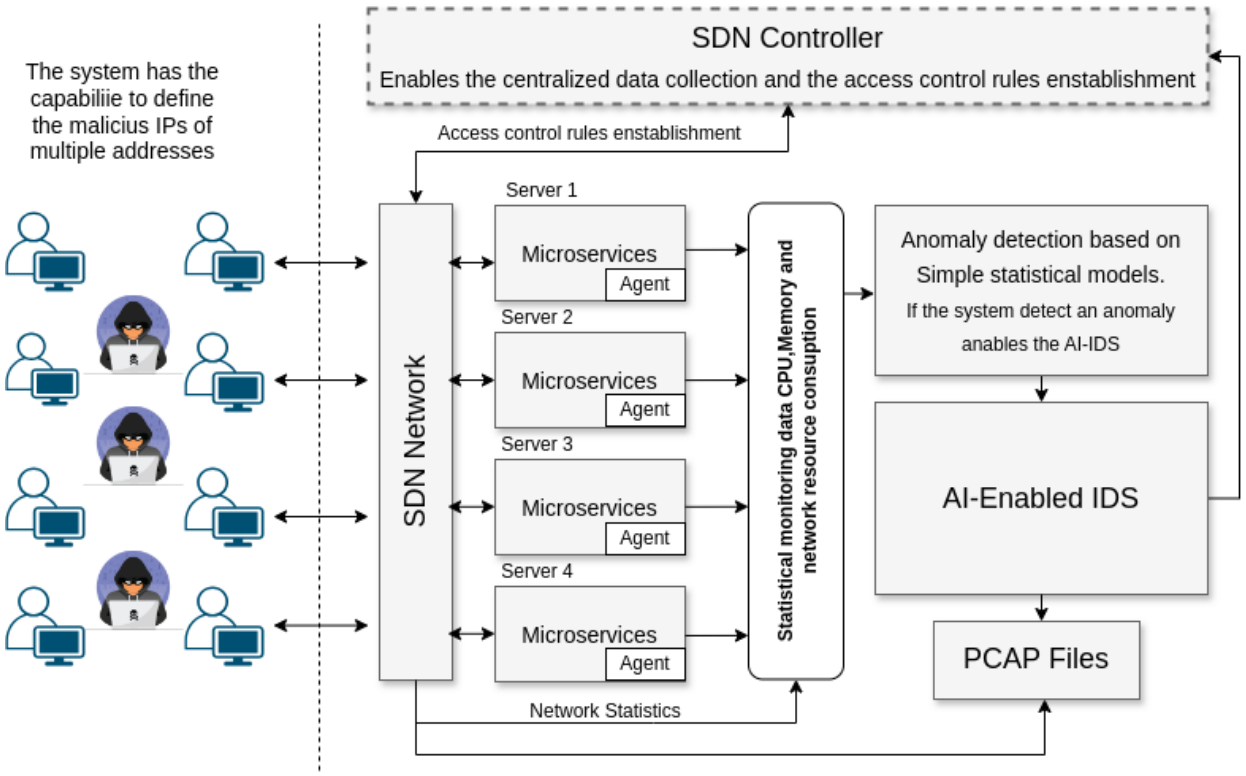


Figure 55. UC 4.4 Sequence diagram

8.4.6. Success Factors

The success of Use Case 4.4 relies on several key factors that ensure the AI-driven orchestration of microservices is both efficient and secure. The main contributions of UC4.4 in achieving NATWORK's project goals are described below:

- **Seamless AI Integration:** The integration of AI into the orchestration framework must be seamless and capable of real-time data processing and decision-making. AI's ability to detect and mitigate anomalies, including undetectable (e.g., zero-day) attacks, will be a cornerstone of success. This aligns with NATWORK's focus on AI-leveraged, self-adaptive security mechanisms that enhance network resilience and security.
- **Robust Anomaly Detection and Response:** The system's ability to detect and respond to anomalies, particularly those arising from security threats like DoS attacks, is essencial. This includes the effective use of flow data extraction and AI-based inference to detect such threats. Success will depend on achieving a high probability of detecting these attacks (**as outlined in KPI 4.4**) while maintaining a low rate of false positives (**KPI 4.5**).

- **Scalability and Elasticity:** The orchestration framework must efficiently manage the dynamic scaling of microservices in response to varying network loads, ensuring that resources are allocated optimally to maintain performance and service continuity. This scalability is key to handling the distributed nature of 6G networks and ensuring they can adapt to changing conditions without compromising on performance.
- **Resilience and Fault Tolerance:** The system must demonstrate resilience by effectively handling microservice failures or overloads and maintaining service continuity even under attack. This includes the system's ability to recover quickly from disruptions and ensure that critical services remain operational, which is vital for maintaining the overall reliability of the network.
- **Rapid Security Measures:** Implementing advanced security measures within the orchestration process is essential to protect microservices from attacks and ensure data integrity and confidentiality. The success of this use case will be directly tied to the effectiveness of these measures in preemptively detecting, mitigating, and responding to various cyber threats, as per NATWORK's objectives of improving network security.
- **Energy Efficiency:** The orchestration system must be designed to optimize energy consumption, in line with NATWORK's goal of achieving net-zero AI and energy-efficient security. Success will be measured by the system's ability to manage resources in a way that reduces power consumption while maintaining high levels of performance and security.
- **Comprehensive Testing and Validation:** The use of the CERTH 5G-SDN testbed for rigorous experimentation is critical. This environment will be essential for validating the system's capabilities under various conditions, including different attack scenarios. The success of Use Case 4.4 will be evaluated by how well the system performs in these tests, providing a solid foundation for its deployment in real-world 6G networks.
- **Continuous Improvement and Adaptability:** Finally, ongoing collaboration among project stakeholders and the ability to adapt based on feedback and experimental results will be vital. The success of the use case will depend on the system's capacity to evolve in response to new challenges, ensuring it remains robust, secure, and efficient as 6G networks develop.

8.4.7. Timeline and Risks

8.4.7.1. Timeline

In UC4.4, the AI-driven orchestration of microservices will be progressively examined through a structured timeline to ensure that all subsystems, as presented in the "Use Case Relevance with

NATWORK" section, are effectively integrated and tested. The following timeline outlines the key phases and associated tasks that will be investigated/evaluated in UC4.4.:

1. **Initial Phase (Months 4-12)**:
    - **Task T3.3**: Begin with microservice profiling under normal conditions. The initial focus will be on developing baseline profiles for microservices to understand typical behavior under standard traffic and workload conditions.
    - **Task T4.2**: Concurrently, the development of monitoring tools will start, targeting the tracking of microservices' resource consumption, which is essential for detecting any deviations indicative of potential security threats.
2. **Development Phase (Months 13-24)**:
    - **Task T4.3**: Focus on the development of AI-enabled intrusion detection systems (IDS) for cloud services. This phase will investigate the implementation of anomaly detection mechanisms, allowing for real-time identification of potential zero-day attacks.
    - **Task T3.4**: Security evaluations within Kubernetes clusters will be conducted to enhance the container security measures, ensuring the robustness of the system against known vulnerabilities.
    - **Integration with Testbed (Month 22)**: Begin integration of developed tools and mechanisms with the CERTH 5G-SDN testbed to validate the orchestration mechanisms in a controlled environment.
3. **Testing and Validation Phase (Months 25-30)**:
    - **Task T4.4**: Finalize the refinement of the orchestration framework on integration aspects, targeting real-time adaptation and scalability of microservices in response to varying network conditions and potential attack scenarios.
    - **Task T4.5**: Federated data repositories will be established to enhance the AI-driven orchestration capabilities by leveraging cross-layer AI-based attack datasets.
    - **Comprehensive Testing (Month 28)**: Extensive experimentation on the CERTH testbed will be performed, with particular emphasis on resilience, fault tolerance, and energy efficiency under different attack scenarios.
4. **Final Phase (Months 31-36)**:
    - **System Evaluation (Month 32)**: Complete the integration of all components and perform a full-scale evaluation of the orchestration system's performance and security.
    - **System Validation and Lessons Learned (Month 36)**: Final validation will take place, and lessons learned will be documented for future iterations and deployments in real-world 6G environments.

8.4.7.2. Risks

The key risks identified for UC4.4, along with their mitigation strategies, include:

1. **Technical Challenges in AI Integration**:
   - **Risk**: AI algorithms may not lead to significant improvements in operational schemes due to the complexity of real-time orchestration.
   - **Mitigation**: Iterative optimization of algorithms will be undertaken, and fallback to optimized standard services will be employed if AI-driven solutions do not perform as expected.
2. **Underperformance of Security Measures**:
   - **Risk**: The security mechanisms may fail to detect and mitigate new types of attacks, particularly zero-day exploits.
   - **Mitigation**: Continuous monitoring and iterative development of anomaly detection mechanisms will ensure the system adapts to emerging threats.
3. **Resource Constraints and Scalability Issues**:
   - **Risk**: Inadequate resources or scalability issues may arise, particularly with high computational demands from data analysis algorithms.
   - **Mitigation**: The system design will emphasize efficient resource allocation, and high-performance computing infrastructures will be utilized as necessary.
4. **Integration and Interoperability Issues**:
   - **Risk**: Difficulties may be encountered in integrating heterogeneous systems or in achieving interoperability between different microservices and orchestration tools.
   - **Mitigation**: Early and thorough integration testing, coupled with the use of standardized interfaces, will mitigate this risk.

This timeline and risk management UC4.4 aligns with the broader goals of the NATWORK project, contributing to the secure and efficient orchestration of 6G microservices.

8.4.8. Summary

Use Case 4.4 focuses on the AI-driven orchestration of microservices within 6G networks, targeting efficient resource management, robust security, and resilient service delivery. The UC integrates advanced AI and machine learning techniques to address the challenges posed by the

complexity of 6G environments, particularly in scenarios involving undetectable security threats like zero-day attacks.

Throughout the project, key subsystems from various work packages (mainly in WP3 and WP4) will be integrated and tested within the context of this use case. These subsystems include AI-driven orchestration mechanisms, Kubernetes security enhancements, and AI-enabled intrusion detection systems, all of which contribute to the overall objective of maintaining Quality of Service (QoS) under adverse conditions.

The timeline for UC4.4 is structured to ensure a gradual and systematic approach to development, testing, and integration. The project phases are designed to build on the outcomes of each task, from initial profiling and monitoring to comprehensive system validation on the CERTH 5G-SDN testbed.

Key risks have been identified, including challenges in AI integration, potential underperformance of security measures, and scalability issues. Mitigation strategies have been put in place to address these risks, ensuring that the project remains on track and achieves its objectives.

Ultimately, UC4.4 aims to contribute significantly to the NATWORK project's goals by demonstrating the effectiveness of AI-driven orchestration in enhancing the resilience, security, and efficiency of 6G networks. The successful implementation of this use case will pave the way for more robust and adaptive network management solutions in the 6G era.

8.5. Use case 4.5 Enabling optimized explainable MTD

8.5.1. Domain description

The evolution of networks towards a more distributed infrastructure, incorporating resources from the edge to the cloud, is anticipated to be a defining feature of 6G networks. The Edge-to-Cloud continuum significantly alleviates communication overhead while improving end-user Quality of Experience (QoE). However, the expansion of this infrastructure also introduces new challenges by enlarging the network's attack surface. As a result, ensuring effective management and security of services across the Edge-to-Cloud continuum becomes increasingly critical.

The security of 6G/NextG networks can be enhanced through the Moving Target Defense (MTD) strategy. MTD operates by continuously altering the network's configuration and assets, complicating efforts by attackers to exploit potential vulnerabilities. A major advantage of MTD

is its ability to disrupt attackers' intelligence-gathering processes, hindering their ability to plan attacks. By persistently changing the network configuration, MTD makes it more difficult for adversaries to identify key assets and devise effective attack strategies.

In the context of the NATWORK project, an MTD framework will be developed and deployed to proactively and reactively safeguard network functions across different network slices within a 6G network. This framework incorporates a cognitive component powered by AI/ML to optimize MTD strategies, ensuring both resource efficiency and a seamless experience from the QoE perspective. Additionally, as network functions and slices may be owned by different entities, such as virtual operators, the cognitive component's federation must be designed to improve MTD strategies collectively, without requiring the exchange of sensitive data. The MTD solution will be tested and demonstrated within UC4.5.

8.5.1.1. Functional requirements and challenges

Enforcing MTD operations can affect network performance and introduce additional operational costs and energy consumption. Therefore, a smart and dynamic approach to MTD control, following a cognitive paradigm (i.e., a closed loop of observing, orienting, planning, deciding, acting, and learning), is essential. This approach must account for security requirements, potential security benefits, overhead, and feasibility. To achieve this, we propose the utilization of Deep Reinforcement Learning (deep-RL), which holds promise for enhancing 6G network security. This is due to the nature of the optimization problem, where the optimal MTD strategy can only be learned through continuous interaction with the environment.

In addition, to increase the trustworthiness of the proposed MTD method, explainability techniques for deep-RL must be harbored, so that the produced actions by our MTD mechanism are justified. Nevertheless, explainability for RL has not been studied as much as for traditional supervised and unsupervised ML methods, due to the complex nature of the environments associated with RL. The survey study in [1] provides a novel taxonomy that analyses various works for explainability methods for RL process, which can be utilized in our work. Figure 56 graphically describes with a UML diagram UC 4.5, defining the agents and components participating in the use case.

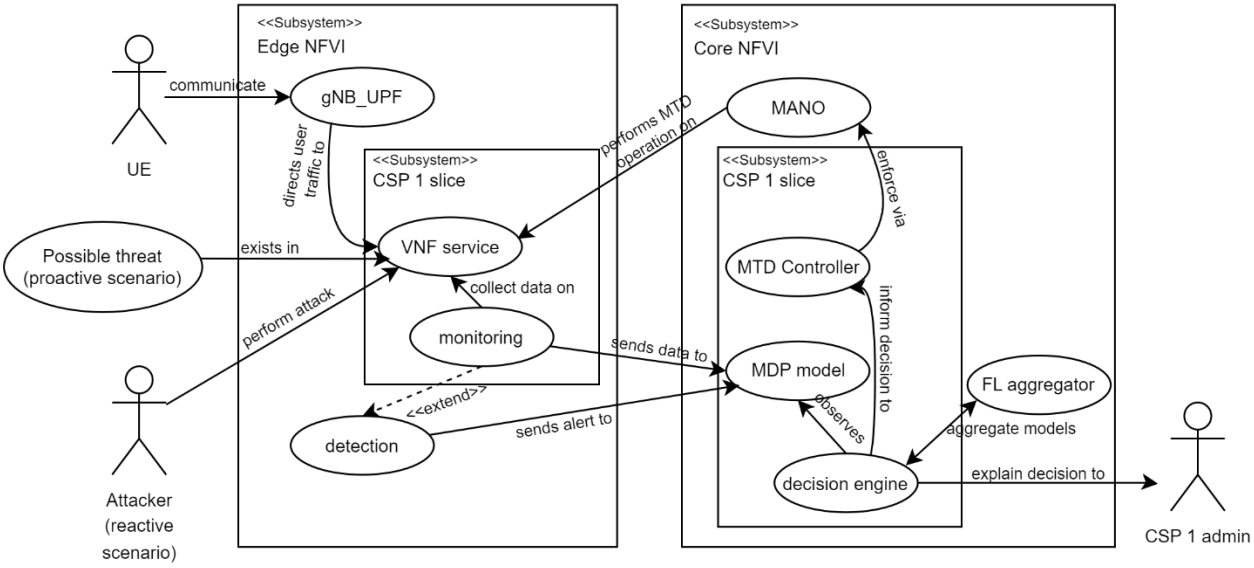


Figure 56. UC 4.5 UML Diagram for Possible Scenarios

The functional requirements and the associated challenges are listed below:

Table 35. UC 4.5 Functional requirements

Functional requirement	Description	Associated challenges
MTD framework scalability	Scaling the usage of MTD operations on a large set of network functions spanning network slices operated both on edge and core infrastructures.	6G networks will encompass ubiquitous, ultra-large-scale systems that integrate diverse technologies, systems, and devices. In a research-oriented testbed, we can only approximate the scale of a private industrial network, making it difficult to fully capture the complexities and vastness of real-world 6G deployments.
Network state assessment	Monitoring the network and present the network state in a near-real time manner with a formal model for application of MTD strategy optimization with deep-RL.	Creating a formal model of states for a complex 6G network encapsulating diverse systems and devices.
Applicability to multi-tenant 6G networks	MTD mechanism must properly operate in an environment where various CSPs are running their own MTD frameworks on a shared 6G infrastructure.	In a multi-tenant scenario, MTD actions can be performed by multiple co-located virtual CSPs. While centralized solutions are hard to implement due to the difficulty of establishing trust among different CSPs, de-centralized solutions incur challenges regarding message passing across disparate models.

Functional requirement	Description	Associated challenges
Robust and explainable learned MTD strategies	Providing transparent and robust MTD actions via explainable AI techniques for deep-RL algorithms.	Explainability techniques for RL-based algorithms are complex due to the modelling of the environment and have not been studied as much as traditional ML model explainability. Hence, coming up with a suitable explainability model is a challenging task.
Federated Learning (FL) Framework for MTD Training	Enabling federated learning for MTD decision process on different setups/environments so that the model can be constructed faster and can make better decisions.	Establishing privacy-preserving of local models during message passing phases of the federated learning. Moreover, centralized FL techniques are prone to single point-of-failure, while de-centralized methods incur additional complexity regarding P2P communication.

8.5.1.2. Enumeration of functions

The use case sets off the following security functions:

- Monitor the network state in near real-time.
- Formalize the network state data into an MDP model and optimize MTD strategies with deep-RL.
- Make deep-RL decisions explainable.
- Enforce the decisions and perform MTD operations on VNFs and CNFs (Containerized Network Functions) located in network slices both in the edge and core domains.
- Improve the deep-RL learned MTD strategy of each tenant by aggregating their respective models with a FL framework.

8.5.1.3. Challenges taken up by the use case

The challenges taken by this use cases are:

- Challenge 1: Develop an ML-based MTD mechanism for providing both pro-active and reactive security against possible threat scenarios and attacks.
- Challenge 2: Deliver MTD actions such that the benign users will not suffer from the transition/change.
- Challenge 3: Provide trustworthy and clear explanations for the MTD action decisions.
- Challenge 4: Implement a federated learning framework for multi-environment training while preserving the privacy of local models.

8.5.1.4. Threat Models

Several threats are tackled by the use case:

A. **Reconnaissance**: Attacker scans available ports and servers on the network for intelligence gathering and effective attack tailoring.
B. **Malware Infection:** Attacker infects a network function to damage or hijack its execution or introduce backdoors for stealthy intrusions.
C. **Denial of Service (DoS)**: Attacker floods the system with excessive requests to prevent benign users from getting the service.
D. **Denial of Sustainability (DoSt)**: Attacker floods the servers, which run on green energy, with excessive requests to force the system to switch to fuel-powered infrastructure.

8.5.2. Use case relevance with NATWORK

NATWORK's core objectives are i) reconcile performance, sustainability and security and ii) develop AI-powered self-resilience against novel threats.

As displayed in Figure 57, the use case is positioned on the first objective, with the clear ambition to take up the challenge of providing security without impairing performance and resource consumption. In this use-case, MTD actions will be decided based on a multi-objective task where a combination of security, performance and sustainability is considered during the decision process. Considering that the use-case is related to all the objectives, we have decided to position the use case in Region A, Region B, and Region C. Moreover, our MTD scheme relies on a deep reinforcement learning approach with continuous enhancement, allowing the model to constantly adjust itself for new threats. This nature of the MTD mechanism resembles a biological immunity system where the body constructs antibodies upon intrusions of foreign cells or germs, and re-uses these antibodies for the next encounter with such unknown organisms. Due to this analogy, we also put our use-case in Region D.

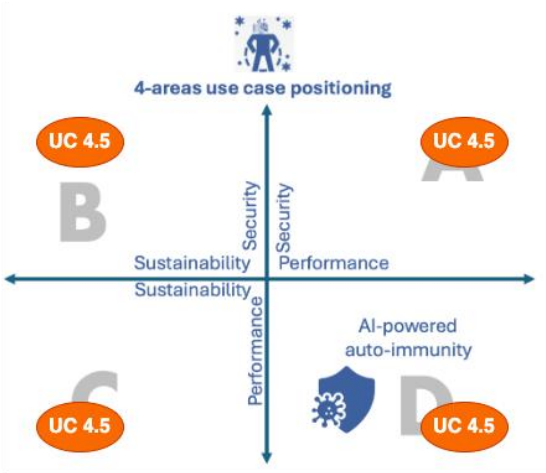


Figure 57. UC 4.5 position on NATWORK's conceptual graph

8.5.3. Definition of the use case KPIs

Use case 4.5 will initially consider the KPIs described in the following table:

Table 36. KPIs used in UC 4.5

KPI Number	Title	Unit	Target	Explanation / Reasoning / Background
A-KPI 4.11	Mean Time to implement the MTD action (MTID)	[min]	Max: MTID < 2 min (depending on the action to perform)	The time it takes for an MTD action (e.g., migrating a service) to be relayed to the action enforcer.
A-KPI 4.12	Worst-case MTD service disruption [WMSD]	[s]	WMSD < 20 s	The period during which the transferred asset is not available to the end-client/user equipment.
A-KPI 4.13	MTD action cost overhead [MACO] (worst-case)	[*percent/time*]	100% service resources in less than 2 min	A comparative value showing the overhead of MTD actions (example metrics to monitor change in CPU, RAM and storage frequency increase). The target value is the worst-case value occurring with MTD service migration.
A-KPI 4.14	MTD green energy consumption [MGEC]	[*percent*]	5-10% increase in green energy consumption	An improvement of energy footprint by dynamic placement of assets in cloud nodes powered with green-energy

KPI Number	Title	Unit	Target	Explanation / Reasoning / Background
A-KPI 4.15	Protection gain of an MTD policy a. Worst-case (P_w) b. Mean (P_m)	[percent of the Likelihood of Successful Exploits (LSE)]	a. P_w > 5% LSE decrease b. P_m > 10% LES decrease	A comparative value showing the gain in protection terms for a performed MTD action.
A-KPI 4.16	Mean decision time for MTD action (MDTA) a. proactive case b. reactive case	a. [ms] b. [s]	a. MDTA < 500 ms b. MDTA < 5 s	The mean time it takes for the optimization engine to come up with a new MTD policy.
A-KPI 4.17	Decision Explainability for MTD [DEFM]	n.d.	Human readable explanation indicating the objective of the decision	Supportive text targeting human readers to explain the decision made by the AI/ML model.

Since this use-case focuses specifically on performing smart, explainable, optimized MTD actions, we leverage MTD specific KPIs which can provide a more insightful evaluation for the developed framework.

8.5.4. Description of the use case testbed requirement

The use case takes place within a multi-cloud 5G network. While not a 6G testbed, it focuses on a configuration relevant to future networks, such as the TelcoCloud setup employing NFV and cloud-native infrastructure, virtualization of 5G core network functions, network slicing, and service distribution across the edge, adhering to the MEC standard. As depicted in Figure 8.5.4, the testbed configuration includes multiple network slices: one dedicated to the infrastructure owner's private domain and others allocated to virtual communication service providers (CSPs). The private network slice contains the owner’s VNFs, while the public network slice independently houses the VNFs of the CSPs.

This network environment operates within a MEC architecture, with network slices spanning the continuum from core nodes to edge nodes in the testbed. The Core NFVI hosts the federated learning (FL) model aggregator, which enhances the deep-RL MTD strategy for individual CSPs.

Meanwhile, the Edge NFVI accommodates the distributed User Plane Function (UPF), alongside the CSPs' private network slices, which host their VNFs and monitoring probes used by the MTD framework of each CSP.

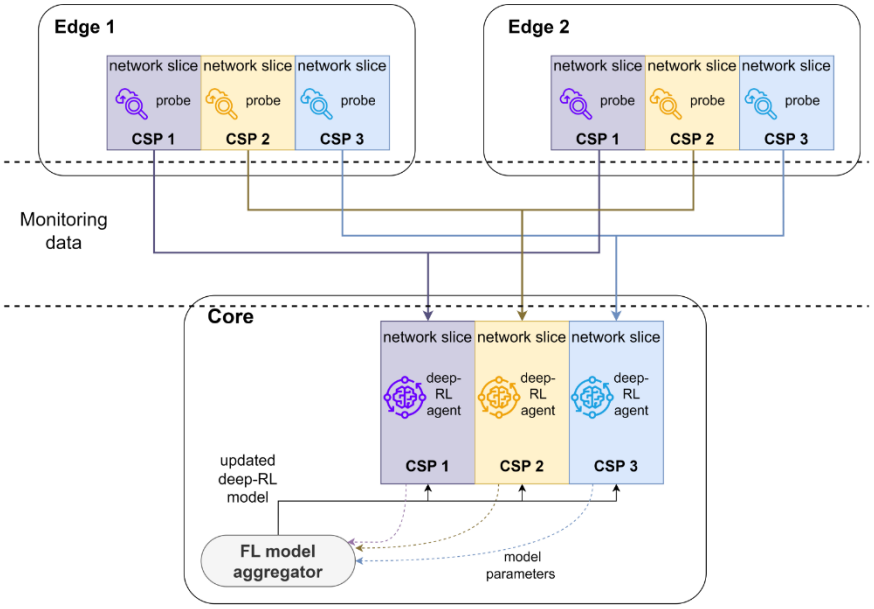


Figure 58. UC 4.5 Testbed and Federation of the deep-RL Optimization for the MTD Framework

8.5.5. Sequence diagram of use case workflow

The sequence diagram shown in Figure 59 highlights the phases of improving and enforcing the MTD strategy in both reactive and proactive security scenarios. The Federated Learning Framework, as outlined in the previous section, interacts with the decision engine to update the deep-RL model for a specific CSP by leveraging parameters from the models of other CSPs. This process runs concurrently with the decision engine transmitting its decisions to the security orchestration layer for enforcing selected MTD actions. The Decision Engine selects MTD actions either proactively, based on threat risk analysis and identified network vulnerabilities, or reactively, in response to attack or anomaly detection alerts from security agents, such as intrusion detection systems (IDS). In both cases, threat analysis and attack alerts are generated by components categorized as 'Security Data Collectors.' Additionally, the decision engine employs explainable AI (XAI) methods to provide humanly interpretable explanations of decisions for CSP administrators. Before execution, MTD actions undergo a verification step by the orchestrator (e.g., the network slice manager or NFV MANO), which assesses the feasibility of actions such as VNF reinstantiation or inter-/intra-domain migration, and enforces the validated operations.

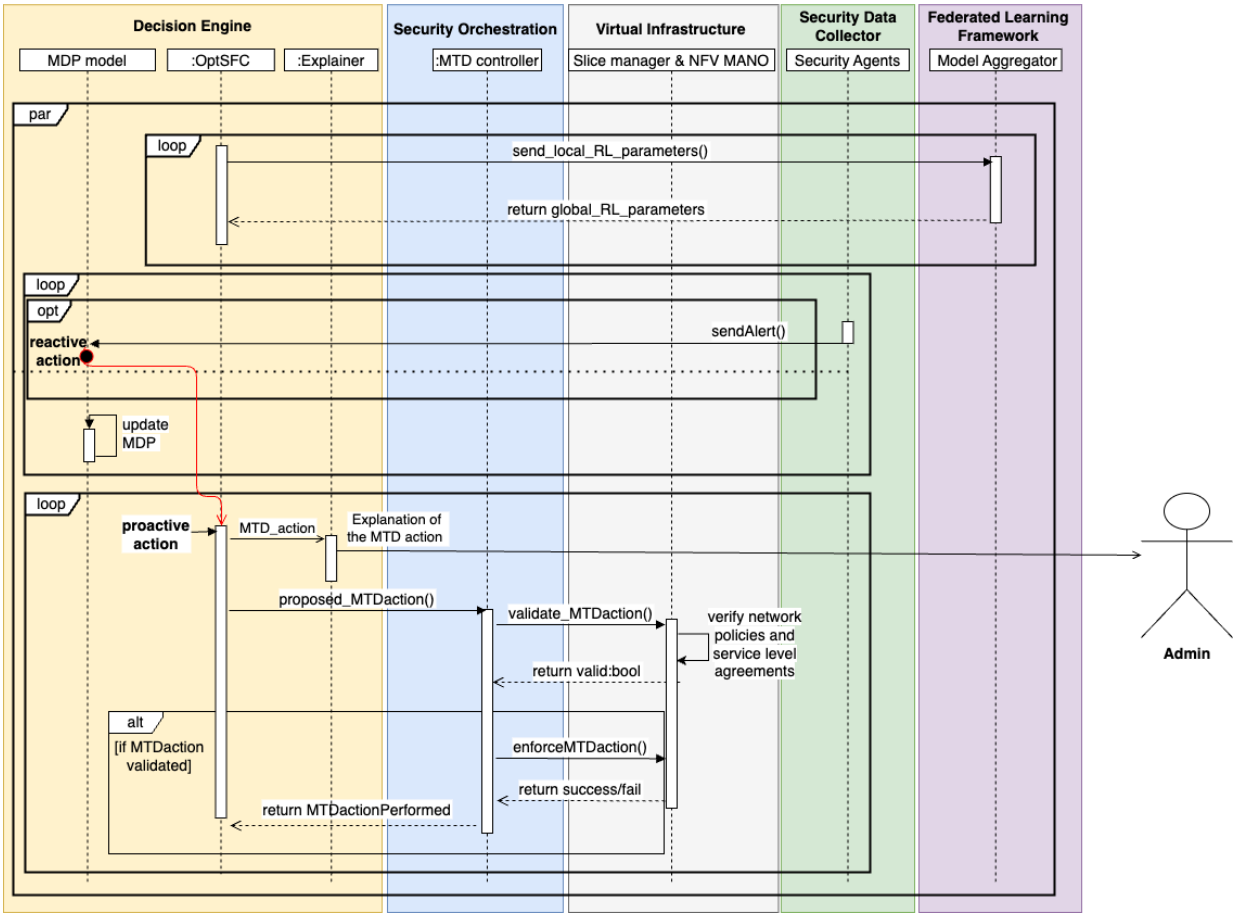


Figure 59. UC 4.5 Sequence Diagram with the Proposed MTD Strategy

8.5.6. Success factors and selected KPIs

Use case 4.5 core success is reached when achieving the following:

- The monitoring probes collect the necessary data on running VNFs, their resource consumption, and their traffic to have a near real time model of the network state.
- The Security Data Collector detects security incidents (for reactive scenarios) and threat assessment data (for proactive scenarios), alerting the MTD framework via its decision engine.
- The Decision Engine determines the optimal MTD operation in a transparent and explainable way, increasing network security while maintaining controlled QoS and consumption overheads.
- The MTD controller, in coordination with the network slice manager, enforces the MTD action on the relevant network slice components, whether VNFs or CNFs.

- The Federated Learning Framework improves the singular MTD strategy of different CSPs while maintaining the privacy of their data.
-

8.5.7. Timeline and risks

We provide an initial estimate for the foreseen timeline and tasks within the use-case, subject to further refinement in the coming months as the project progresses. In Figure 60, one can observe the tentative timeline of the use-case, where the yellow bars represent the tasks with a risk factor that brings along a high possibility of exceeding the estimated duration, and the sketched bars represent the possible delay, accounting for the unprecedented challenges we might face during our work.

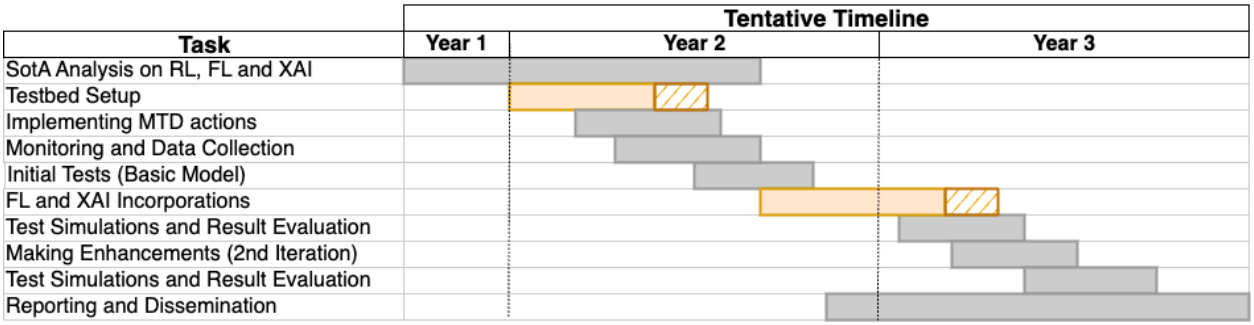


Figure 60. UC 4.5 Gantt Chart for the Estimated Timeline

We evaluate the “Testbed Setup” and “FL and XAI Incorporations” tasks as risky ones, as they mostly require collaboration with other partners, which will demand careful planning and scheduling. Note that “SotA Analysis on RL, FL and XAI” overlaps with many other tasks, indicating that it can be conducted in parallel with other tasks. We also estimate a long duration for the “Reporting and Dissemination” task, since we plan to publish results gradually as we go with the experiments, rather than finishing all the work and reporting them afterwards.

8.5.8. Summary

In conclusion, Use Case 4.5 demonstrates a robust MTD framework designed for 6G networks, leveraging AI/ML and deep-RL to optimize security strategies across a multi-entity, distributed environment while preserving data privacy through secure federated learning. The framework not only focuses on proactive and reactive protection of network slices but also ensures that decision-making processes are humanly explainable for improved robustness and accountability. By testing this framework in a multi-cloud 5G testbed, the use case validates its applicability to

future networks such as 6G, integrating advanced virtualization, network slicing, and edge-to-cloud continuum to efficiently enhance security at scale.

8.6. UC 4.6. Software control flow monitoring for early DoS

8.6.1. General description

Described as a sub use case or research topic in UC 4.1, UC 4.6 has been created. Software control flow monitoring is described in UC 1.2 as a result of the SECaaS appended probes on x86 binary payloads. In association with this work, UC 4.6 will consider how time and frequency time series, rooted on the control flow (i.e., at code block entry points) can be placed for the early detection of DoS attacks .

The threat model relevant to this UC is: **DoS attacks** when directed to service or software consist in resource exhaustion. The victim software may not be modified for that, but simply hosted by a resoure depleted platform. The attack can target the software (e.g., by flooding the input data port) or its execution environment.

The objective of this UC4.6 is: **Deliver a pre-alert of DoS attack** with the highest detection accuracy and minimal false alarms. As DoS attacks and benign host resource attritions induce the same performance loss, disambiguation in as far as it can be done, is the first objective to seek. A second objective is to qualify the content of “DoS attack” report for their usability. A ranking of the prediction (as a weather forecast could be considered.

An important aspect of UC 4.6 is to define the type of DoS attack report which can be delivered, such as:

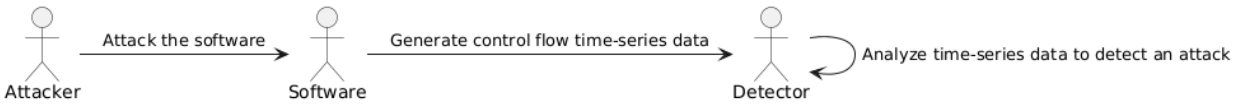


Figure 61. UC 4.6 Simple use case graph.

8.6.2. Functional requirements and challenges

8.6.2.1. Requirements

The requirements consists in generating time series on-the-fly, during payload execution and rooted in the control flow code blocks.

The time series shall therefore enable to extract on-the-fly: identification of the code block, time stamps located at the entry point. A special bufferization mechanism enables rapid storage for post processing.

A post processing utility shall be able to access to the time series timely and compute the pre-processed elements (e.g., code block time to execute, call frequency, sequence of traversed code blocks). The inference of attacks will use these pre-processing elements.

8.6.2.2. Challenges

For DoS early detection, the main challenge is to discriminate intentional DoS attacks from simple resource attrition at the host, caused by legit co-resident payload. As both causes will be revealed by the same symptoms (punctual performance drop), we will investigate if a complementary metrics or an extension of the monitored time scale can disambiguate the two types of situations. One of the considered pathway is to collet a mapping of co-resident processes on the platform. Another research activity will focus on the input data handler activity.

8.6.3. UC relevance with NATWORK

The use case is aligned with NATWORK's objective #05. *Deployment & experimental implementation of the security modules in relevant Use Cases.*

UC 4.6 positioning over NATWORK's conceptual scheme is shown below

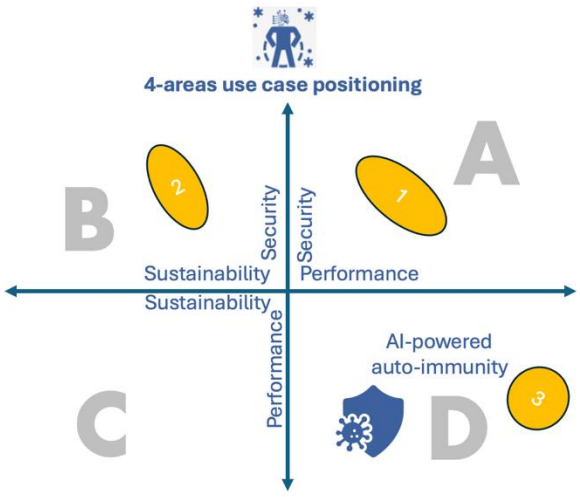


Figure 62. UC 4.6 position in NATWORK's conceptual graph

As shown above, we consider that three different areas can be mapped for UC 4.6:

Placement in Area 1 relates to the relationship between performance and security. A higher DoS attack detection rate (i.e., security) induces lower performance as both are related to the control flow monitor-related instructions (i.e., time series generation deeply rooted in the control flow graph). What is not shown however is that as soon as the cause of the DoS attack is identified and the associated remediation action is carried out (e.g., flooder's I.P address eviction), the performance will recover its original rate, before the attack took place.

Placement in Area 2 signifies that a higher security (i.e., probability of detection) elevates sustainability typically when the cause of the DoS attack and the remediation is taken.

Placement in Area 3 signifies that AI could be useful to discern DoS patterns.

8.6.4. UC 4.6 KPIs

The KPIs of the proposal are enumerated below:

- KPI 4.3 Delivery of specification PoC related to Software Control Flow Monitoring. An initial feasibility study will be produced, notably in consideration of the identified technical risks.
- KPI 4.4 Probability of detection of DoS attack inference:>80%. This KPI will be conditioned by the outcome of KPI 4.3 (i.e., initial feasibility study)
- KPI 4.5 Probability of false detection <5%. This KPI will be conditioned by the outcome of KPI 4.3 (i.e., initial feasibility study)
- Additional KPIs must be added as: A-KPI 18. False alarm rate for DoS attack detection

8.6.5. Description of the UC testbed requirement

Our first research and development will be made in TSS own infrastructure. We will first study the relevance of the two considered research pathways (i.e., focus on the victim code data handlers, focus on novel, possibly suspicious co-resident processes). The possible resulting PoC will be possibly integrated with partners over their infrastructure (e.g., MONT, NOVA, UESSEX).

8.6.6. Sequence diagram

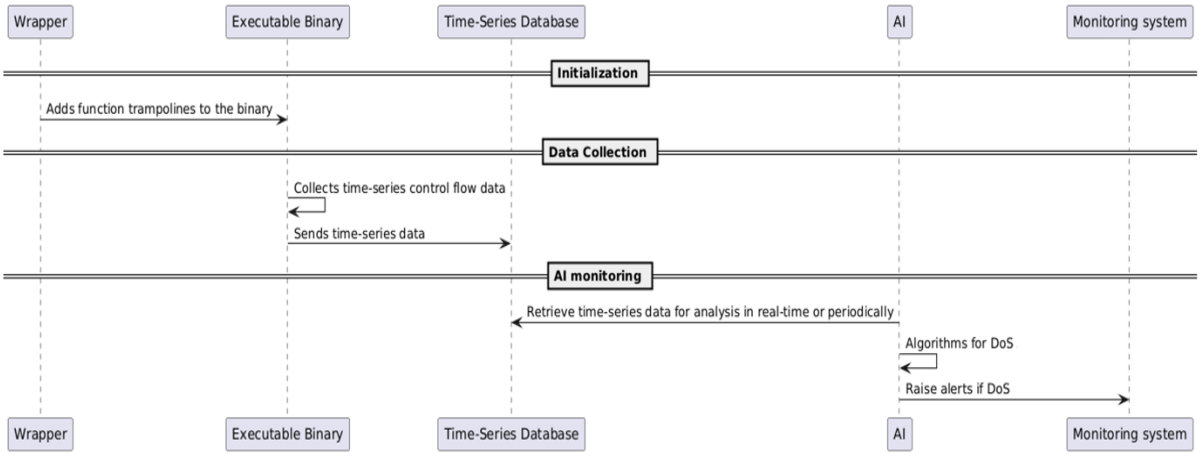


Figure 63. UC 4.6 Sequence diagram

The UC 4.6 stages are:

- Injection of trampolined routines (i.e., appended routines inserted at the block-to-block jumps or calls), at most relevant locations of the control flow graph, preventing excessive overhead. Leveraging AI for the identification of these locations is to be considered with its benefits in terms of prediction improvement, false alarm reduction, and practical applicability (i.e., quality of the training data set representative of all types of processing)
- Collection of time series by the tranpolined routines delivering time, frequency elements
- Post processing of the time series for AI inference

8.6.7. Timeline and risks

The proposal technological risk of *Control flow time and frequency metadata extraction or exploitation cannot be done,* relates to this UC 4.6. Our initial implementation on TSS testbed fully validates this risk. In practice, there is a strict requirement for being cautious and moderated when placing time series trampolines over the control flow, as they induce a significant performance penalty on the monitored software. On the other hand, at that time, there is no DoS classification method directly exploitable from these time series. Our research will have these two concurrent objectives of performance acceptable, and DoS attack accurate classification. The relevance of AI based DoS classification is also to analyzed in terms of quality of the training data notably.

UC 4.6 intends to disambiguate the origin of a software performance loss, from a DoS intentional attack or a basic resource exhaustion on the host. As stated above, disambiguation requires complementary metrics from the considered control flow time series. This core risk of UC 4.6 is the inability to complement the time series (i.e., time and frequency elements on control flow code blocks) to get an accurate DoS attack classification with novel markers, at sustainable costs. As stated in this UC 4.6's description, two research paths are considered (i.e., focus on data handlers, scouting co-resident runnning processes) but additional context metrics could be considered during our research.

The UC 4.6 timeline will be phased with NATWORK's general timelines as follows:

a. **M12**: Milestone MS 3. Delivery of the initial and on-going status on control flow time series extraction, restating the objective and problem statement.
b. **M18**: Milestone MS 4. Delivery of the pre-final research analysis report.
c. **M21**: Deliverable D3.3. Submission of the final research analysis report with associated PoC accordingly. The relevance of AI for the DoS classification will be brought at that stage
d. **M24-36**: Integration and test over NATWORK representative payload (E.G., MONT's MMT probe security service, ISRD xAPP)

8.6.8. Summary

Although originally inserted into UC 4.1, UC 4.6 is presented as a separated use case, bearing its own risk and timeline. The technical risk as stated in the proposal is still valid today and a DoS attack disambiguation method is still to be defined.

Totally aligned with NATWORK's sustainable security concept, disambiguation and DoS attack pre-alert report content must be defined to bring an additional **sustainable security** method to the market, supporting sustainable network decision-taking based on a threat ranking and at best efforts in terms of resource. Our work program is phased according to the different milestones in the project.

9. NATWORK use cases KPIs

9.1. KPIs aggregating table

The following table aggregates all KPIs used in NATWORK's 16 use cases. The upper part of the table includes the topology and syntax of the KPI labels and a color code distinguishing the proposal's KPIs and novel complementary KPIs.

Table 37. Enumeration of NATWORK's use cases KPIs

Use case	KPI
LEGEND	KPI x.y= A proposal's KPI KPI x.y.z = A proposal's KPI criteria for KPIs which include several criterias.
	A-KPI: An additional KPI (from the propoal)
UC 1.1 Decentralized MANO	KPI 1.1 End-to-end compliance with latency tolerance (UC1 .1, 10%),
	KPI 1.2 Energy waste (UC1 .1, UC1 .3, 10%),
	A-KPI 1.5 Cluster Hygiene Scores (Number of vulnerabilities shared with score 8+/Total number of vulnerabilities)
	A-KPI 1.6 Cluster CTI Exposed information Ratio (Number of vulnerability data parts revealed/Total information per CTI data)
	A-KPI 1.7 Cluster CTI Hidden information Ratio (Number of vulnerability data parts hidden/Total information per CTI data)
UC 1.2 SECaaS security	KPI 1.3.1 *Respective x86 native payloads latency at start*
	KPI 1.3.2 performance degradation during runtime
	KPI 1.3.3 overall energy waste for the aggregation onf confidentiality, integrity runtime and correct execution monitoring
	KPI 1.4 ASM security enforcement (according to our security challenge results),
UC 1.3 Green-based payload placement	A-KPI-1.8 : 100% denial of credentials of devices running non-trusted software.
	A-KPI 1.9: Additional latency of attestation below target value.
UC 2.1 Enabling multi antenna for resilience	KPI 2.1: Jamming attacks detected and mitigated (increase of at least 30% in the detection of attacks)
	KPI 2.2 Time needed to detect and prevent a jamming attack
	KPI 2.3 Time needed to recover from a jamming attack
	KPI 2.4 Downtime prevented
	KPI 2.5 Throughput enhancement during jamming attack
UC 2.2 Empowering AI based jamming detection and mitigation for multi path routing	KPI 2.1 Jamming attacks detected and mitigated
	KPI 2.2 Time needed to detect and prevent a jamming attack
	KPI 2.4 Downtime prevented
	KPI 2.5 Throughput enhancement during jamming attack
	A- KPI Successful establishment of connectivity to avoid jammed channels/paths.
UC 2.3 Adaptive modulation	Same as UC 2.2

Use case	KPI
techniques for anti jamming	
UC 2.4 Improving 6G security spectrum	A- KPI:2.7 Key Generation Length:
	A- KPI 2.8 NIST Random Test Compliance:
	A- KPI 2.9 Key Generation Rate (KGR):
UC 3.1 Anomaly detection using ML	KPI 3.1 - Mean Time to Detect (MTTD)
	KPI 3.2 - Number of False Positives (FP)
	KPI 3.3 - Number of False Negatives (FN:
	KPI 3.4 - Packet Loss Ratio (PLR)
	KPI 3..5 - Mean Time to Detect (MTTD)
UC 3.2 AI driven penetration testing	A-KPI 3.6 Impact on QoS by AI-DoS evaluation tool
	A-KPI 3.7 Comparison of results between AI-DoS and other tools used for QoS assessment, to determine which is the most effective tool.
	A-KPI 3.8 Perform a vulnerability report regarding DoS resilience on 5G/6G components.
UC 3.3 Improving variability of network with continuous security	A-KPI 3.9 Mean Time to Detect (MTTD)
	A-KPI 3.10 – False positive (FP)
	A-KPI 3.11 - False negative (FN)
	A-KPI 3.12. Trust establishment Time
UC 4.1 Security aware placement, allocation and monitoring	KPI 4.1.1 DFE processing latency
	KPI 4.1.2 DFE computational efficiency
	KPI 4.1.3 DFE impact on power consumption.
	KPI 4.1.4 WAI-based latency
	KPI 4.1.5 Power consumption
UC 4.2 AI aware network slicing for efficient resource utilization and monitoring	KPI 4.2.1 Energy Efficiency Improvement
	KPI 4.2.2 Latency Reduction
	KPI 4.2.3 Resource Utilization Optimization
	KPI 4.2.4 AI Model Accuracy Maintenance
	KPI 4.2.5 Dynamic Adaptation
UC 4.3 Software defined radio for agile payload communication	A-KPI 4.6: Jamming/adversary attacks mitigation (at least 80% accuracy in unjammed signal recovery)
	A- KPI 4.7 Time needed to prevent mitigate a jamming/adversary attack via AI/ML frequency and protocol switching
	A-KPI4.8 Time needed to recover from a jamming attack
	A- KPI 4.9 Downtime reduction
	A- KPI4.10: Throughput increase
UC 4.4 AI driven orchestration of micro-services	KPI 4.4 Probability of DoS Attack Detection
	KPI 4.5 Probability of DoS attack false detection
	A-KPI-11 Mean Time to implement the MTD action (MTID)
	A-KPI-12 Worst-case MTD service disruption [WMSD]

Use case	KPI
UC 4.5 Enabling optimized explainable MTD	A-KPI-13 MTD action cost overhead [MACO] (worst-case
	A-KPI-14 MTD green energy consumption [MGEC]
	A-KPI-15 Protection gain of an MTD policy
	A-KPI-16 Mean decision time for MTD action (MDTA)
	A-KPI-17 Decision Explainability for MTD [DEFM]
UC 4.6 Software control flow monitoring for early DoS detetion	KPI 4.3 Delivery of specification PoC related to Software Control Flow Monitoring.
	KPI 4.4 Probability of detection of DoS attack inference:>80%. This KPI will be conditioned by the outcome of KPI 4.3 (i.e., initial feasibility study)
	KPI 4.5 Probability of false detection <5%. This KPI will be conditioned by the outcome of KPI 4.3 (i.e., initial feasability study)
	A KPI 4.18. False alarm rate for DoS attack detection

9.2. Completeness and orientation of NATWORK's used KPIs

A comparison of NATWORK's used KPIs with the most used KPIs of other SNS projects most used KPIs is given below.

The following table enumerates SNS project most used KPIs and how NATWORK maps them.

Table 38. NATWORK's KPIs mapping with SNS project most-used KPIs

SNS project most used KPIs	Occurrence in NATWORK	Rationale and explaination
Latency	Several KPIs refer to latency (i.e., KPIs 1.1, 1.3.1, A-KPI from UC 1.3, KPI 4.1.1, 4.2.1)	
Reliability	Several KPIs refer to reliability directly or indirectly (i.e., KPIs 1.3, 1.4, A-KPI of UC 1.3, 3.1)	Reliability is considered as a result of security. NATWORK develops several improvements on remote attestation, a strong pillar of software security
Availability	Several KPIs refer to availability directly or indirectly (i.e., KPIs 2.4, 4.3, A-KPI of UC 4.5. MTTR KPI 3.5)	Availability is considered with DoS remediation and with moving target defence based network rearrangement
Block error rate	Packet losss ratio in KPI 3.4	
Peak Throughput	DFE KPI 4.1, 4.2	
Quality of experience	DFE KPI 4.1, 4.2	
Max Bandwith	A-KPI 4.10	
Area Traffic density	Not treated in NATWORK	KPIs relate to specific hardware-based improvements on antennas and front-end processing capacity, connected devices timing accuracy.
Jitter	Not treated in NATWORK	
Clock synchronicity	Not treated in NATWORK	

This table is however incomplete to reflect NATWORK specific focus on Energy consumption and sustainability. By essence, 6G vision and all SNS projects share sustainability as a key value, while at the current stage it does not directly translates into a specific KPI. Reversely, NATWORK heavingly focusses on energy consumption reduction with dedicated KPIs (i.e, KPI 1.2, 1.3.3, 4.2.1).

This KPIs mapping reflects the main accent given to NATWORK and its associated use cases. The use cases and are service-level oriented, ensuring that the service is performant (i.e., peak throughput and latency reduction), available (i.e., DoS detection and remediation with malware detection and moving target defense, software continuity with novel control flow monitoring), trustable by enforcement of the remote attestation and performant by reducing latency (i.e., maxifying the migration of payloads of different formats including WASM closer to users) and finally with consideration of low energy consumption.

9.3. Novel forms of KPI

All KPIs from past projects are aligned on a single axis or criteria. At the first place, they are related to performance and considered as the core element to reach novel 6G services. To reflect this view and given as an example, time synchronicity (of sensors) will enable 6G-permitted global city digital twin. This will also come with the density of traffic enabling the geographic high grained dissemination of sensors.

However, some NATWORK's KPIs embrace several dimensions of performance, energy consumption and security. KPI 1.3 and 2.2 embrace several of the three criteria and are splitted into single criteria sub KPIs (e.g., KPI 1.3.1 on performance, KPI 1.3.3 on sustainability). The splitting is made to simplify the verification of these KPIs.

A novel form of KPI may occur during the development of 6G technology. With a very high emphasis on sustainability by all parties from standardization to industry, 6G novel use case required extended performance and security, will come if sustainability is concurrently achieved. At a given time, one progress in performance will be accepted only if the impact on energy is null or decreased. This orientation may emerge new types of deeply rooted technical KPIs, embracing security or performance at a given energy consumption level (e.g., Watt/square meter). In other words, these novel KPIs will intertwin several dimensions of performance, security and sustainability.

10. Conclusions

The main objective of this document is to detail NATWORK's use cases with sufficient technical elements and risks, paving the way for the on-going use cases realization.

This document structure follows a top to bottom approach, starting with a survey of 6G emblematic use cases to the description of NATWORK's use cases.

Standardization, industry and academic research entities essentially describe the 6G main promises of 6G with the descriptions of futuristic use cases (e.g., immersive, ubiquitous and augmented reality through ultra reliable low latency ultra large bandwidth communications at the first place) while reasserting the elevated concern on security and sustainability (e.g., resource consumption), defined as complementary key values. Then our survey of SNS funded projects is given as forming a rich, multi-faceted and collective research field nurturing NATWORK's concept. From these SNS funded research projects, we extracted the most-used KPIs with the intent to position NATWORK, discerning its specific concept, notably adding sustainability as a new and specific KPI.

Simply put, NATWORK's concept is the reconciliation of network performance with security with sustainability. The main idea is that security always comes with resource consumption. Both security and resource consumption grow at the same pace and are tightly linked. This calls for developping sustainability-friendly security techniques. To progress on its tenet, NATWORK is supported by a higher number (i.e., 16) of use cases than other SNS projects (i.e., 2-5). The 16 use cases cover a large variety of technical areas such as data layer core network component, cloud native microservices, WASM software payloads, RAN, RIS antenna, security functions as malware detection, SDN based moving target defense.

These use cases are all security related and described with a common template, putting emphasis on how they grasp NATWORK's concept.

The template provides all details deemed appropriate to qualify and quantify (i.e., KPI) these 16 security-related use cases, in terms of threat models and risks. The document puts emphasis on the KPIs, identifying additional KPIs (i.e., A-KPI) complementary and coming in addition to the proposal defined KPIs. Some of these new KPIs will be further defined and elaborated during the development.

In that sake, the document gives an inclination for the formalization of 6G new KPIs, which quantify performance and security at a given energy consumption.

References

[1] ITU-T Focus Group on Network 2030 complementary use cases, available at "Network 2030- Additional representative use cases and key network requirements for Network 2030", June 2020.

[2] IMT 2030: Framework and overall objectives of the future development of IMT for 2030 and beyond, Nov 2023.

[3] IMT Vision -Framework and overall objectives of the future development of IMT for 2020 and beyond" Sept 2015, available at https://www.itu.int/rec/R-REC-M.2083-0-201509-I/en

[4] P.Nagaraj. March 2024. Researchgate. Demystifying IMT-2030 aka 6G-capabilities, Usage Scenarios, and Candidate Technologies.

[5] NG Alliance, 6G Applications and use cases, available at https://nextgalliance.org/white_papers/6g-applications-and-use-cases/, [Accessed by: October 2024]

[6] NG Alliance, 6G Trust, Security and Resilience white paper available at https://nextgalliance.org/white_papers/trust-security-and-resilience-for-6g-systems/, [Accessed by: October 2024]

[7] NG Alliance 6G sustainability KPIs and Gap Analysis, available at https://nextgalliance.org/white_papers/6g-sustainability-kpi-assessment-introduction-and-gap-analysis/, [Accessed by: October 2024]

[8] NGMN use case analysis 2022, available at https://www.ngmn.org/wp-content/uploads/220222-NGMN-6G-Use-Cases-and-Analysis-1.pdf

[9] NGMN trustworthiness analysis 2023, available at https://www.ngmn.org/wp-content/uploads/NGMN_6G_Trustworthiness.pdf

[10] China promotion Group inside IMT, “6G Usage Scenarios and Key Capabilities”, June 2021, available at chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.caict.ac.cn/english/news/202106/P020210608349616163475.pdf

[11] TAICS white paper on candidates technologies for 6G, available at https://www.taics.org.tw/eng/Publishing.aspx?PubCat_id=3 from Taiwanese Association of Information and Communication Standards. Dec 2023.

[12] Ministry of Science and ICT (MSIT), “6G Global 2023”, Available at: https://www.msit.go.kr/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=904, Nov 2023

[13] Beyond 5G Promotion Consortium (b5g.jp)” available at https://b5g.jp/en/, [Accessed by: December 2023]

[14] SNS ICE project, available at https://smart-networks.europa.eu/csa-s/#SNS-ICE, [Accessed by: October 2024]

[15] HEXA-X-II Deliverable D1.2 on 6G Use Cases, available at https://hexa-x-ii.eu/hexa-x-ii-project-releases-deliverable-d1-2-on-6g-use-cases/, [Accessed by: October 2024]

[16] Ejaz, S., & Al-Naday, M. (2024, March). FORK: A Kubernetes-compatible Federated Orchestrator of Fog-native applications over multi-domain edge-to-cloud ecosystems. In *2024 27th Conference on Innovation in Clouds, Internet and Networks (ICIN)* (pp. 57-64). IEEE.

[17] Prometheus: Monitoring system & time series database", Prometheus.io. Accessed: Sep. 30, 2024. [Online]. Available: https://prometheus.io/

[18] ONOS Project, "ONOS: Open Network Operating System", Open Networking Foundation. Accessed: Sep. 30, 2024. [Online]. Available: https://opennetworking.org/onos/

[19] Y. Arjoune, F. Salahdine, M. S. Islam, E. Ghribi and N. Kaabouch, "A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication," 2020 International Conference on Information Networking (ICOIN), Barcelona, Spain, 2020, pp. 459-464, doi: 10.1109/ICOIN48656.2020.9016462.

[20] O. Puñal, I. Aktaş, C. -J. Schnelke, G. Abidin, K. Wehrle and J. Gross, "Machine learning-based jamming detection for IEEE 802.11: Design and experimental evaluation," Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, Sydney, NSW, Australia, 2014, pp. 1-10, doi: 10.1109/WoWMoM.2014.6918964.

[21] F. T. Zahra, Y. S. Bostanci and M. Soyturk, "LSTM-Based Jamming Detection and Forecasting Model Using Transport and Application Layer Parameters in Wi-Fi Based IoT Systems," in IEEE Access, vol. 12, pp. 32944-32958, 2024, doi: 10.1109/ACCESS.2024.3371673.

[22] Enrico Testi, Luca Arcangeloni, and Andrea Giorgetti. 2023. Machine Learning-Based Jamming Detection and Classification in Wireless Networks. In Proceedings of the 2023 ACM Workshop on Wireless Security and Machine Learning (WiseML'23). Association for

Computing Machinery, New York, NY, USA, 39–44. https://doi.org/10.1145/3586209.3591395

[23] Ali, Abubakar & Singh, Govind & T. Lunardi, Willian & Bariah, Lina & Baddeley, Michael & Andreoni, Martin & Giacalone, Jean-Pierre & Muhaidat, Sami. (2022). RF Jamming Dataset: A Wireless Spectral Scan Approach for Malicious Interference Detection. 10.36227/techrxiv.21524508.v1.

[24] Pirayesh, Hossein, et al. "JammingBird: Jamming-resilient communications for vehicular ad hoc networks." *2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 2021.

[25] Zeng, Huacheng, et al. "Enabling jamming-resistant communications in wireless MIMO networks." *2017 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2017.

[26] Kosmanos, Dimitrios, et al. "MIMO techniques for jamming threat suppression in vehicular networks." *Mobile Information Systems* 2016.1 (2016): 8141204.

[27] Y. Sun, M. Peng, Y. Zhou, Y. Huang, and S. Mao, "Application of Machine Learning in Wireless Networks: Key Techniques and Open Issues," in IEEE Communication Surveys & Tutorials, v. 21, no 4, pp. 3072-3108, 2019.

[28] M. Ji, Q. Wu, P. Fan, N. Cheng, W. Chen, J. Wang and K. B. Letaief, "Graph Neural Networks and Deep Reinforcement Learning Based Resource Allocation for V2X Communications," in arXiv: 2407.06518v1

[29] K. Chowdhury and I. F. Akyildiz, "Cognitive Wireless Mesh Networks with Dynamic Spectrum Access," in IEEE Journal on Selected Areas in Communications, v. 26, no 1, pp. 168-181, 2008.

[30] T. Yucek and H. Arslan, "A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications," in IEEE Communications Surveys & Tutorials, v. 11, no 1, pp. 116-130, 2008.

[31] O. Naparstek and K. Cohen, "Deep Multi-User Reinforcement Learning for Dynamic Spectrum Access in Multichannel Wireless Networks," in GLOBECOM 2017-2017 IEEE Global Communications Conference, Singapore, pp. 1-7, 2017.

[32] C. V. Vivekanand, G. Talele, B. Jaishanthi, H. G. S. K. Maheswari and B. U. Maheswari, "Deep Reinforcement Learning for Resource Allocation in Wireless Communication System," in 2014 Ninth International Conference in Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, pp. 1-5, 2024.

[33] V. Aruna, L. Anjaneyulu, and C. Bhar, "Deep-Q Reinforcement Learning Based Resource Allocation in Wireless Communication Networks" in 2022 IEEE International Symposium on Smart Electronic Systems (iSES), Warangal India, pp. 55-72, 2022

[34] Y. Li, W. Zhang, C. X. Wang. J. Sun and Y. Liu, "Deep Reinforcement Learning for Dynamic Spectrum Sensing and Aggregation in Multi-Channel Wireless Networks," in IEEE Transactions in Cognitive Communications and Networking, v. 6, no 2, pp. 464-475, 2020.

[35] C. Chaieb, F. Abdelkefi, and W. Ajib, "Deep Reinforcement Learning for Resource allocation in Multi-Band and Hybrid OMA-NOMA Wireless Networks," in IEEE Transactions on Communications, v. 71, no 1, pp. 187-198, 2023.

[36] P. Shome, J. Modares, N. Mastronarde and A. Sprintson, "Enabling Dynamic Reconfigurability of SDRs Using SDN Principles," in Ad Hoc Networks, 8th International Conference, ADHOCNETS 2016 Ottawa, Canada, 2016.

[37] HyperLedger Avalon : available at https://lf-hyperledger.atlassian.net/wiki/spaces/avalon/overview?__hstc=120149271.c4a577029c49e44b73bd3bee6fa38565.1726617600141.1726617600142.1726617600143.1&__hssc=120149271.1.1726617600144&__hsfp=451136374

[38] S. Ankergard, E.Dushku, N.Dragoni. DTU. 2022. Proceedings of 14th International Symposium on Foundations & Practice of Security PERMANENT: Publicly Verifiable Remote Attestation for Internet of Things through Blockchain

[39] M. Lacoste, V. Lefebvre, IEEE Privacy and Security Journal. 2023. Trusted Execution Environments for Telecoms: Strengths, Weaknesses, Opportunities, and Threats

Appendix 1- Milestone 2 Expert Survey Suggested Content

Reminder:

The content which follows will form an online survey for simplicity. The form (typically Microsoft FORM) will be uploaded once the content of the questions are confirmed. This forms the initial content of the form to collect WP2's partners comments

FORM INITIAL CONTENT

Initial expert identification questions:

Identification of the profile of the responder:

- Name,
- Organization (i.e., selection inside several options such as research institute, academic, telecom operator, telecom service vendor),
- Position in the org (i.e., selection between several options such as research, operation, management, other)

Questions:

Q1: NATWORK's bio-mimicry concept is inspired by body autoimmunity system and body dynamic resource management. In essence, NATWORK fosters the development of AI-powered auto-immunity where the network discerns novel attacks and adapts its defense accordingly. Secondly, NATWORK's progresses on sustainable network performance and security (i.e., elevated network performance and security are both achieved at reasonable and sustainable costs).

Is NATWORK's concept echoing or matching with one research direction of your organization or one of your operational needs?

(Tickable Yes/No). If Y, can you provide us with a few lines description? (open space)

Q2: NATWORK's deliverable D2.2 contains 16 use cases in alignment NATWORK's concept as shown in the list below.

UC#	Thematic
UC 11	Decentralized management an orchestration
UC12	SECaaS Security
UC 13	Green based payload placement
UC 2	(given as the use case 2 owner)
UC 21	Enabling multi antenna for resilience
UC 22	Empowering AI based jamming dtection and mitigation for multi path routing
UC 23	Adaptive modulation techniques for anti jamming
UC 24	Improving 6G security in 6G spectrum
UC 31	Anomaly detection using ML
UC 32	AI driven penetration testing
UC 33	Blockchain based security and trust management
UC41	Security Aware placement allocation and monitoring
UC42	AI aware network slicing for efficient resource utilisation and monitoring
UC 43	Software defined radio for agile payload communication
UC 44	AI driven orchestration of micro services
UC 45	Enabling optimised explainable MTD
UC 4.6	Software Control Flow based DoS detection

Table A1. List of NATWORK use cases

The deliverable can be downloaded at https://natwork-project.eu/

In your opinion, do these use cases cover the different network technical domains (i.e., Radio, edge, core data and control layers, cloud).

Tickable options Y/N.

Elaborate with open writable space.

Q3: **Does Question 2 use case table contain a challenge close to the ones progressed by your organisation?**

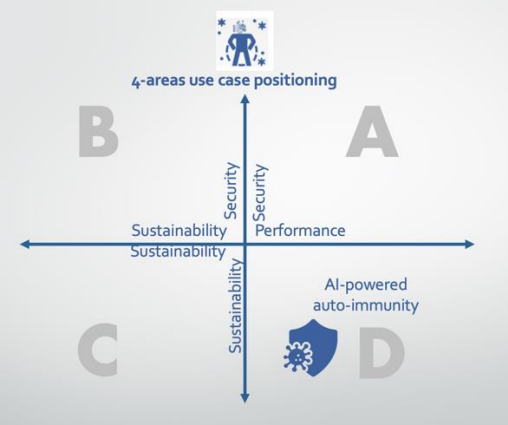
- If Y, can you elaborate (free space)
- If N, can you elaborate a 6G challenge considered as essential or supporting your action

Q4: **Which one of the four main research areas A, B, C and D of Deliverable 2.2 NATWORK's methodology representation better match the challenges faced by your organisation?**

You can tick several options:

- Area A Progressing Security at sustainable resource costs
- Area B Progressing Security while keeping performance
- Area C Progressing Performance at sustainable resource costs
- Area D Developping network AI self immunity

Free space to elaborate how your challenges are positioned in the different areas. For simplicity, the four areas of NATWORK's concept are shown in the figure below.



Q5: Deliverable D2.2 contains a list of network service level KPIs (KPIs list table 2 will be extracted from deliverable D2.2 timely).

Do you view this table as complete or reversely missing a core service level KPI?

If the answer is missing and If you wish can you elaborate?

Q6: **Beyond service level KPIs as given in Q5 table, can you indicate a domain-specific security KPI which is progressed or of importance for your organisation and corresponds to a specific security aspect (e.g., probability of malware detection) your organisation is interested by?**

If you wish can you elaborate?

Q7: **Beyond service level KPIs as given in Q5 table, can you indicate a domain-specific performance KPI which is progressed or significant by your organisation and corresponds to a domain-specific performance aspect (e.g., RIS MIMO) your organisation is interested by?**

If you wish can you elaborate?

Q8: **Beyond service level KPIs as given in Q5 table, can you indicate a domain-specific sustainablity KPI which is progressed or significant for your organisation and corresponds to a specific sustainability aspect (e.g., number of potential user connection per microwatt spent at MIMO head)?**

If you wish can you elaborate?

Q 9: **In a general perspective, do you consider Deliverable D2.2 use case description methodology as a valuable asset of the document?**

(Tickable Very Valuable, Valuable, somewhat valuable, not valuable, no idea).

If you wish can you elaborate?

Q10: **In a general perspective, do you consider Deliverable D2.2 conclusion, suggesting the elaboration of combined KPIs as a valuable outcome?**

(Tickable Very Valuable, Valuable, somewhat valuable, not valuable, no idea).

If you wish can you elaborate?
