Deliverable D5.1
Initial report on AI-driven MonB5G security and energy-efficiency techniques

Document Summary Information

Grant Agreement No	871780	**Acronym**	MonB5G
Full Title	Distributed Management of Network Slices in beyond 5G		
Start Date	01/11/2019	**Duration**	36 months
Project URL	https://www.monb5g.eu/		
Deliverable	D5.1 Initial report on AI-driven security technique		
Work Package	WP2		
Contractual due date	M17	**Actual submission date**	31/03/2021
Nature	Report	**Dissemination Level**	Public
Lead Beneficiary	EUR		
Responsible Author	Adlen Ksentini (EUR), Sabra Ben Saad (EUR)		
Contributions from	Christos Verikoukis (CTTC), Hatim Chergui (CTTC), Luis Blanco (CTTC), David Pubill (CTTC), Jordi Serra (CTTC), Sarang Kahvazadeh (CTTC), Luis Sanabria-Russo (CTTC), Tarik Taleb (AAL), Chafika Benzaid (AAL), Aiman Nait Abbou (AAL), George Tsolis (CTRX), George Guirgis (eBOS), Cao-Thanh Phan (BCOM), Mohamed Rahali (BCOM), Anestis Dalgkitsis (IQU), Luis Garrido (IQU)		

Disclaimer

Copyright message

Executive Summary

Motivated by the increased attack surface of slicing-enabled beyond 5G environments, MonB5G aims at providing a secure and trusted environment for network slice deployment and management. The distributed nature of MonB5G elements and their AI-based features are instrumental in achieving these objectives. By applying advanced data analysis and Machine Learning (ML) techniques, early and accurate identification of attacks will be possible via the automatic application of localized, self-healing mechanisms to mitigate them, taking advantage of the distribution of security management tasks and security enforcement points across the architecture.

Security functionality in MonB5G is provided by a security orchestrator (SO) entity, which examines security requirements and provides the adequate closed loops (Security as a Service - SECaaS), leveraging the slice template, the Security Service Level Agreemen (SSLA), and the threat modelling. SO instantiates and deploys SECaaS and relies on the SSLA manager to monitor and check that the security requirements of network slices are met. SECaaS is defined as a selected combination of MSs, AEs and DEs deployed on-demand to provide a Zero-touch security management of security. SECaaS features AI algorithms, at the AE, that automatically protects the running network slice by detecting anomalies and attacks and mitigates these threats with appropriate action through DE. Besides, the MonB5G system focuses on protecting AI-driven solutions run at Analytical Engine (AE) against the presence of misbehaving decentralized elements, knowing that the produced model can provide a calamitous output when trained based on corrupted data. Hence, the design of new approaches to secure AI-based training is envisioned.

Meanwhile, energy consumption reduction is another objective pursue by MonB5G. Indeed, MonB5G aims at providing all the necessary mechanisms that will allow the reduction of power consumption. Building on the MonB5G distributed network slicing architecture, where the three key components, i.e., MS, AE, and MS, will be instantiated at each technological domain, and for each network slice, several energy-aware artificial intelligence (AI) techniques are envisioned. The proposed energy optimization techniques will be envisioned for AEs and DEs. For AE, constrained federated learning (FL)-based is considered to reduce the amount of raw data exchanged between local AEs and the end-to-end AE, aiming at reducing the transmission overhead and thereby the underlying energy consumption. Regarding DE, distributed multi-agent Deep Reinforcement Learning (DRL)-based DEs are considered to perform cross-domain joint slice VNF placement and energy control. Finally, MonB5G considers a dynamic RAN offloading via a data-driven base-station (BS) switching OFF/ON.

The deliverable provides the first report of MonB5G contributions and work plan to, on one hand, secure network slicing by introducing the SO entity that provides SECaaS relying on MonB5G key components MS, AE and DE targeting zero-touch security management; on the other hand, to reduce energy consumption through ML techniques covering AE and DE components. The deliverable covers the following security aspects: the SO architecture and functions relying on the MonB5G reference architecture detailed in D2.1; AI-based security management introducing the concept of SECaas that relies and the key MonB5G elements (MS, AE and DE), a threat study on attacks on network slicing mapped to two representative use-cases, the

attack detection and mitigation using MonB5G key elements and the SO mapped to two representative use-cases. Regarding energy consumption, the deliverable provides the first contributions of the project to reduce energy consumption using optimized AI algorithms for AE and DE as well as a first approach to turn on-off Radio Access Network (RAN) components according to network slice traffics.

It is important to note that this deliverable is a merge of the deliverables D5.1 and D5.2. Accordingly, this impacted the content of the initial deliverable, as now it contains two different and separate sections, one for security covering Tasks T5.1 and T5.2 activities, and another section covering energy optimization covering the activities of T5.3. **Besides, the deliverable content is covering only 7 months of activities in WP5, hence covering mainly the initial design and description of the envisioned solutions, as the due date has been shifted from M24 to M17 per the officer's request.**

The following highlights the key achievements in this deliverable:

- A review of state of the art on security orchestrators as proposed by phases 2 and 3 projects funded under the 5GPPP program.
- A review of existing solutions that are envisioned to protect AI algorithms against attacks.
- A detailed description of the SO and SECaaS adopted in MonB5G, which rely on the MonB5G reference architecture described in D2.1.
- A detailed description of MonB5G key elements and their role to detect and mitigate attacks on network slices using AI-based algorithms targeting zero-touch security management.
- A comprehensive study of conceivable attack threats and their respective mitigation actions when used in a virtualized environment is provided, focusing on two representative use-cases covering the activities of WP5.
- A formal model for security threats, with application on the two representative use-cases.
- A first description of the MonB5G key elements MS, AE and DE functions and their interaction to detect and mitigate attacks mapped to the two representative use-cases considered in WP5. For each, component examples of envisioned algorithm and mechanism are provided.
- A comprehensive review of start of the art techniques to reduce energy consumption.
- First MonB5G energy-efficient approaches leveraging AE and DE using ML techniques, Federated Learning and Deep Reinforcement Learning, respectively.

TABLE OF CONTENTS

List of Figures

List of Tables

Abbreviations

(D)DoS	Distributed Denial-of-Service
(FL)-IDS	First Level IDS
(SL)-IDS	Second Level IDS
3GPP	3rd Generation Partnership Project
5G-GUTI	5G Global Unique Temporary Identifier
5G-PPP	5G Public Private Partnership Association
AAA	Authentication, Authorization, and Accounting
ACT	Actuation
AE	Analytics Engine
AI	Artificial Intelligence
AMF	Access and Mobility Management Function
APIs	Application Programming Interfaces
APs	multiple Access Points
AUT(H)	Authentication
BBUs	Baseband Units
BS	Base Station
CCL	Centralized Constrained Learning
CCS	Conformity Certification Services
CDF	Cumulative Distribution Function
CIA	Confidentiality, Integrity, and Availability
CLB	Centralized Load Based
CN	Core Network
CoAP	Constrained Application Protocol
CPU	Central Processing Unit
CQI	Channel Quality Indicator
C-RAN	Centralized-RAN
CSP	Constraint Satisfaction Problem
CU	Central Unit
dBm	Decibel-Milliwatts
DCI	Data Centers Interconnect
DDoS	Distributed denial of service
DDPG	Deep Deterministic Policy Gradient
DE	Decision Engine
DL	Decision Layer
DLB	Distributed Load Based
DMO	Domain Manager and Orchestrator
DNN	Deep Neural Network
DNS	Directory Name Service
DoS	Denial of service attacks
DPI	Deep Packet Inspection

DQN	Deep Q-Network
DRL	Deep Reinforcement Learning
DSO	Domain security orchestrator
DU	Distributed Unit
DVMC	Dynamic Virtual Machine Consolidation
E2E	End-to-End
ECATP	Enhanced Context- Aware Traffic Predictors
EE	Energy-Efficiency
EM	Element Manager
eMBB	enhanced Mobile BroadBand
eNodeB	evolved Node B
EPC	4G Evolved Pack Core
ETSI	European Telecommunications Standards Institute
EU	European Union
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FCAPS	Fault, Configuration, Accounting, Performance, Security
F-gNBs	Femtocell g-NodeB
FL	Federated Learning
F-SECaaS	Functional layer of SECaaS
Gbps	Gigabits Per Second
gNB	gNodeB
GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
GUTI	Globally Unique Temporary Identifier
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDDoS	Indirect Distributed Denial-of-Service
IDM	Infrastructure Domain Manager
IDMO	Inter-domain Manager and Orchestrator
IDS	Intrusion Detection System
IDSM	Inter-Domain Slice Manager
ILP	Integer Linear Programming
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IOTI	IoT Interface
InfraP	Infrastructure Provider
KPIs	Key performance indicators
LCM	Life-Cycle Management
LSTM	Long Short-Term Memory
LTE	Long-Term Evolution
LTE Cat	LTE Category protocol

LTE-M	Long-Term Evolution for Machines (MTC)
MANO	MANagement and Orchestration
MARL	Multi-Agent Reinforcement Learning
MBS	Macro Base Station
MDP	Markov Decision Process
ME	Mobile Equipment
MEC	Mobile Edge Computing
MEHW	Mobile Equipment Hardware
MIMO	Multiple-Input Multiple-Output
MITM	Man-In-The-Middle
ML	Machine Learning
MonL	Monitoring Layer
MLaaS	Management Layer as a Service
MME	Mobility Management Element
mMTC	massive Machine Type Communications
MNOs	Mobile Network Operators
MQTT	Message Queuing Telemetry Transport
MS	Monitoring System
MTC	Machine Type Communications
NAS	Non-Access Stratum
NB-IoT	Narrowband IoT
NEA	New Radio Encryption Algorithm
NFV	network functions virtualization
NFVI	NFVI Infrastructure
NFVInt	NFV Interface
NFVO	NFV Orchestrator
NG-RAN	Next Generation Radio Access technology Network
NIDS	Network Intrusion Detection Systems
NIST	National Institute of Standards and Technology
NN	Neural Network
NP-hard	Non-deterministic Polynomial-time hardness
NS	Network Slice
NS(S)MF	Network Sice (Subnet) Management Function
NSI	Network Slice Instance
NSSF	Network Slice Selection Function
NSS-SECaaS	Network Slice Subnet SECaaS
NTP	Network Time Protocol
OAI	OpenAirInterface
OFDMA	Orthogonal Frequency Division Multiple Access
oPoT	Ordered Proof of Transit
OSS	Operations Support Systems
OTT	Over-The-Top
PaaS	Platform as a service

PASTA	Process for Attack Simulation and Threat Analysis
PCF	Policy Control Function
PCRF	Policy and Charging Rules Function
PDU	Packet Data Unit
PGW	Packet Data Network Gateway
PGW-C	PDN Control Plane
PGW-U	PDN User Plane
PNF	Physical Network Function
PRBs	Physical Resource Blocks
PU	Periodic Update
PulSAR	Proactive Security Assessment and Remediation
QoS	Quality of Service
RAM	Random Access Memory
RAN	Radio Access Network
RAND	RANDom number
RBSs	Rogue Base Stations
RES	RESponse
RL	Reinforcement Learning
RMSE	Root Mean Squared Error
RNN	Recurrent Neural Network
RRC	Radio Resource Control
RRH	Remote Radio Head
RRU	Remote Radio Unit
SBA	Service Based Architecture
SBS	Small Base Stations
SCC	Security Control Class
SCNs	Small Cell Networks
SCTP	Stream Control Transmission Protocol
SDN	Software Defined Networking
SDNI	SDN Interface
SD-SEC	Software-Defined Security
SEAF	Security Anchor Function
SECaaS	SECurity as a Service
SFC	Service Function Chaining
SFF	Service Function Forwarder
SFL	Statistical Federated Learning
SFP	Service Function Paths
SGW-C	Serving Gateway Control plane function
SGW-U	Serving Gateway User plane function
SINR	Signal to Interference-plus Noise Ratio
SIP	Session Initation Protocol
SLA	Service Level Agreement
SM	Sleep Mode

SMC	Security Mode Command
SMD	Security Management Domain
SMF	Session Management Function
SML	Slice Management Layer
SMS	Short Message Service
SO	Security Orchestrator
SOC	Security Operation Center
SSLA	Security Service Level Agreement
SUCI	Subscription Concealed Identifier
SVM	Support Vector Machine
TARA	Threat Assessment and Remediation Analysis
TCP	Transmission Control Protocol
TD	Technological Domain
TDSAC	Twin-Delayed Double-Q Soft Actor-Critic
TM	Trust Manager
TOE	Target of Evaluation
TRM	Trust Reputation Manager
TRP	Transmission/Reception Point
TTP	Tools, Tactics, and Procedures
UDM	Unified Data Management
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communications
VNF	Virtual Network Functions
VSFs	Virtualized Security Functions
vSwitches	virtual Switches
WUC	Wake-Up Control
XOR	eXclusive OR
ZSM	Zero-touch network and Service Management

1. Introduction

1.1 Scope

MonB5G steps in the deployment of a novel autonomic management and orchestration mechanism framework by heavily leveraging the distribution of operations together with state-of-the-art AI-based mechanisms. The MonB5G approach focuses on the design of a hierarchical, fault-tolerant, automated, and data-driven network management system that incorporates security as well as energy efficiency as key features in order to orchestrate a high number of parallel network slices and significantly higher types of services in an adaptive and *zero-touch* way.

The deliverable provides the first report of MonB5G contributions and work plan towards Zero-touch security management and efficient energy consumption relying on AI. First, the deliverable introduces the MonB5G security architecture featuring the SO entity that provides SECaaS relying on MonB5G key components MS, AE, and DE targeting zero-touch security management. Second, it details devised ML techniques leveraging AE and DE components to reduce energy consumption.

The deliverable covers the following security aspects: the SO architecture and functions relying on the MonB5G reference architecture detailed in D2.1; AI-based security management introducing the concept of SECaas that relies and the key MonB5G elements (MS, AE, and DE), a threat study on attacks on network slicing mapped to two representative use-cases, the attack detection and mitigation using MonB5G key elements and the SO mapped to two representative use-cases. Regarding energy consumption, the deliverable provides the first contributions of the project to reduce energy consumption using optimized AI algorithms for AE and DE as well as a first approach to turn on-off RAN components according to network slice traffic prediction.

1.2 Structure

The main structure of this deliverable is summarized in the following table, linking each section with the corresponding task.

Section	Description	Task(s)	Starting Month
2	Dedicated to state of the art on security-oriented architectures in 5G, reviewing different H2020 5GPPP projects. Besides, this section reviews the security threat modelling methodology, which is needed to understand security threats in 5G and beyond networks. Finally, this section review state of the art techniques to protect ML algorithms	T5.1 & T5.2	M13
3	Presents the MonB5G envisioned security architecture for Network slicing and the AI-based components (MS/AE, DE) of MonB5G to address 5G security threats.	T5.1	M13

4	Details the MonB5G approach to detect and mitigate attacks on Network slices considering two representative use-cases.	T5.1 & T5.2	M13
5	Dedicated to energy-efficiency solutions. Besides reviewing the existing methods for energy-efficient5G and beyond networks, this section presents an initial approach of MonB5G to reduce energy consumption efficiently leveraging AE and DE with AI algorithms. In addition, it introduces first approach to turn off/on RAN relying on network slice traffic prediction.	T5.3	M13

2. Related work

2.1 Security architectures in 5G and beyond

This section presents a state of the art of security management in different EU projects targeting security orchestration in 5G networks.

2.1.1 *INSPIRE-5GPLUS*

INSPIRE-5Gplus is an ongoing project aiming at revolutionizing the security in 5G and beyond networks by implementing a fully automated end-to-end (E2E) smart network and service security management framework. To meet this goal, INSPIRE-5Gplus leverages a set of emerging trends and technologies, including Zero-touch network and Service Management (ZSM), SECurity as a Service (SECaaS), Software-Defined Security (SD-SEC), and AI/ML techniques.

The project is in the progress of implementing a fully automated, trustworthy and liability-aware security management framework for multidomain 5G and beyond networks. Figure 1 describes the conceptual architecture, where security is provided at the domain and E2E levels by the Security Management Domain (SMD) and E2E SMD, respectively. Each SMD guarantees security management within its scope using several domain components such intelligence engine and security orchestrator. While the E2E SMD spans multiple domains in order to coordinate the different domains and handle the E2E slice security management.

The term domain domain refers to the different technological domains that compose a mobile network. The set of modules in the SMD and E2E SMD operate in an intelligent closed loops fashion to enable software defined security (SD-SEC). The services provided by the different modules are connected within the domain and cross domains using domain integration fabric and cross domain integration fabric respectively.

In contrast to MonB5G that provides a full FCAPS network management, INSPIRE-5Gplus focuses only on security-related management. Regarding the security architecture, although the intersection between the security modules is similar, the approach in MonB5G is completely different. First, in terms of vertical management levels, INSPIRE-5Gplus provides security management in two vertical levels (domain and end-to-end), while MonB5G has a more sophisticated dynamic management levels that consider the particularity and the distinctive needs of slices, in addition to enhance the sub-slices isolation and their dynamic nature. Besides the static modules (domain and inter-domain), MonB5G instantiates dynamically with each slice the following three management vertical management levels: (i) Inter-Domain Slice Manager (IDSM) for slice management from end-to-end perspective; (ii) Subslice MLaaS for sub-slice management; and (iii) Embedded Element Manager (EES) embedded in all the nodes for the node internal management.

Second, INSPIRE-5Gplus introduced several components in the SMD:

- Similar to MonB5G (MS, AE, DE) closed-loop, INSPIRE-5Gplus has **security data collectors,** a **security analytics engine**, and a **security intelligence.** As the names indicate, these components are purely security-related in contrast to MonB5G that its closed-loops are more generic thus MonB5G manage multiple instances of MS, AE, and DE in a dedicated layer Monitoring Layer (MonL), Analytics layer (AL), and Decision layer (DL).

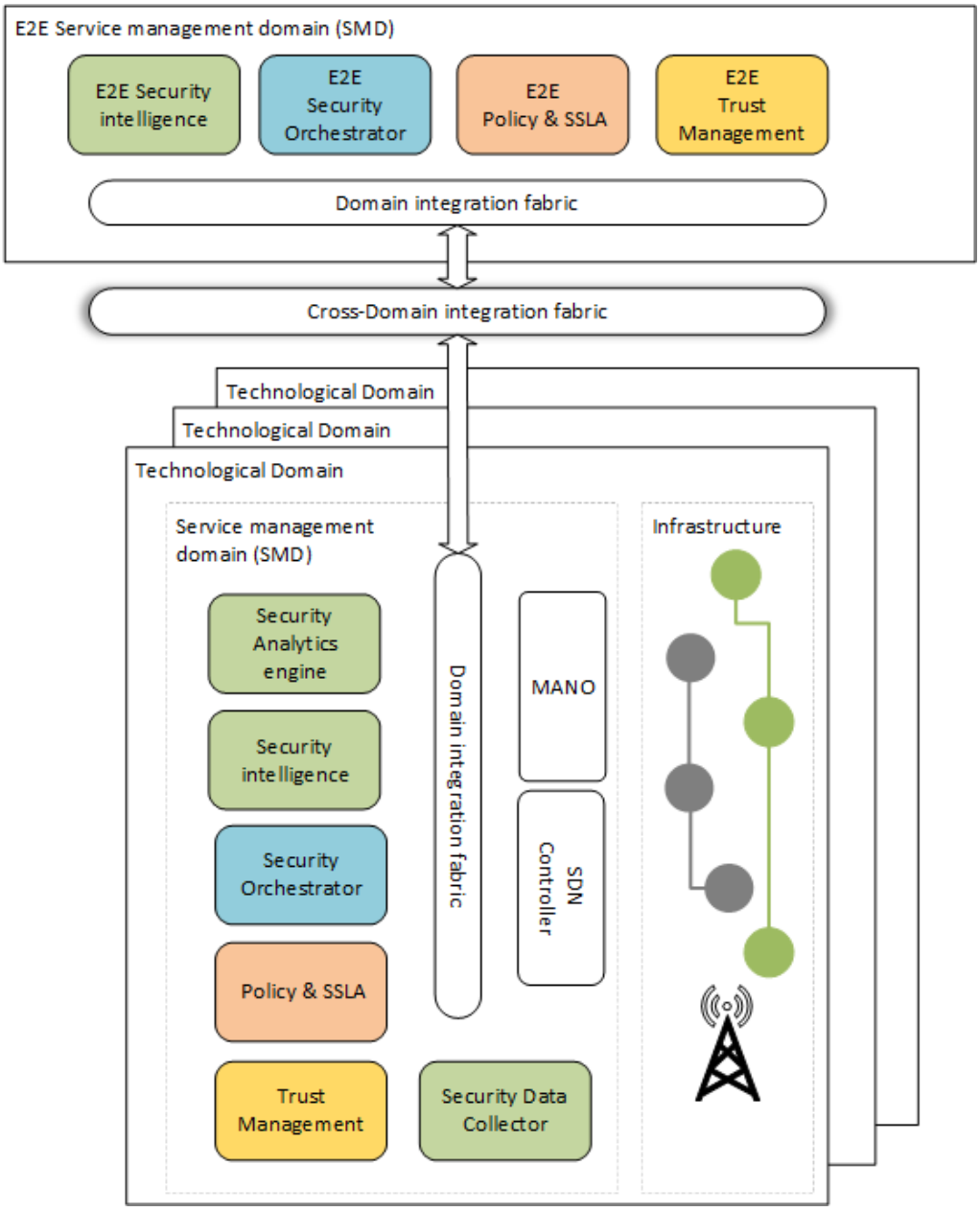

Figure 1. INSPIRE-5Gplus architecture and main components

- **Security Orchestrator (SO)** covers the security configuration enforcement in the corresponding management domain based on the decision policies. The SO intervenes between the security intelligence decision and the different Software Defined Networking (SDN) controllers, Network Functions Virtualization (NFV) MANO and the security management services through the integration fabric. Mapping to MonB5G architecture, the SO exists as a statistic component but with a different role. To clarify, the SO in MonB5G manages the security-related atomic components such as MS, AE, DE, and Actuation (ACT). In fact, the ACT can be seen as a lightweight and distributed version of the INSPIRE-5Gplus SO. Since the ACT translates and enforces the DE security policies. The roles of MonB5G's security orchestrator will be described in Section 3.1 .
- **Policy & Security Service Level Agreement (SSLA) management** negotiates the protection and security requirements level with the consumer's and provider's needs. Moreover, this component provides the monitoring specification that defines the SSLAs. The latter provide the mean to specify the security requirement and assessing their fulfilment. In MonB5G, a similar role is guaranteed by subcomponents in the security orchestrator.
- **The Trust Manager (TM)** ensures the trust in the framework involving various internal trust services, including: (i) a Trust Reputation Manager (TRM) service that assigns reputation values to monitored 5G entities; (ii) a Certification Service Conformity Certification Services (CCS) that evaluates the different 5G network components based on measured metrics that define the trustworthiness properties exposed by the components. Similarly, for trusting a slice, using a slice-related data (static and dynamic properties) and scores from a 5G slice; and (iii) an Ordered Proof of Transit (oPoT) service to trust in how data flows traverse a network [1].

In order to validate the project concepts, INSPIRE-5Gplus defined 9 test cases, among them:

- "Definition and assessment of Security and Service Level Agreements and automated remediation": In this test case, they are planning to monitor that the SSLA is ensured by monitoring Key performance indicators (KPIs) and metrics such as Data and service availability, Isolation access from other slices, and Security enforcement techniques.
- "Network attack detection over encrypted traffic in the Service Based Architecture (SBA)": As the SBA is tending to use end-to-end encryption such as DNS over the HyperText Transfer Protocol Secure (HTTPS), this use case aims to detect the type of attacks, as an example, attack against anti-malwares that can be evaded using encrypted traffic.
- "Intelligent and Secure Management of Shared Resources to Prevent the Distributed Denial-of-Service ((D)DoS)": This test case shows how to detect Indirect Distributed Denial-of-Service (IDDoS) attack in which an attacker targets a critical service slice (Indirect victim) by initiating a DDoS attack against another vulnerable slice (Direct victim) sharing the same infrastructure resources with the targeted one [2] .

INSPIRE-5Gplus introduced an architecture to secure and ensure trust in the 5G networks. Nevertheless, the current INSPIRE-5Gplus architecture appears to remain centralized in a per domain level, lacking slice-specific security management and isolation.

2.1.2 *ANASTACIA*

ANASTACIA is a framework built on top of an Internet of Things (IoT) infrastructure targeting the network security and leveraging SDN/NFV-based security enablers. It is designed to manage security policies and

defines relevant security controls to be orchestrated in Mobile Edge Computing (MEC) and Smart Building Management [3]. Figure 2 represents the reference architecture divided into the following set of planes:

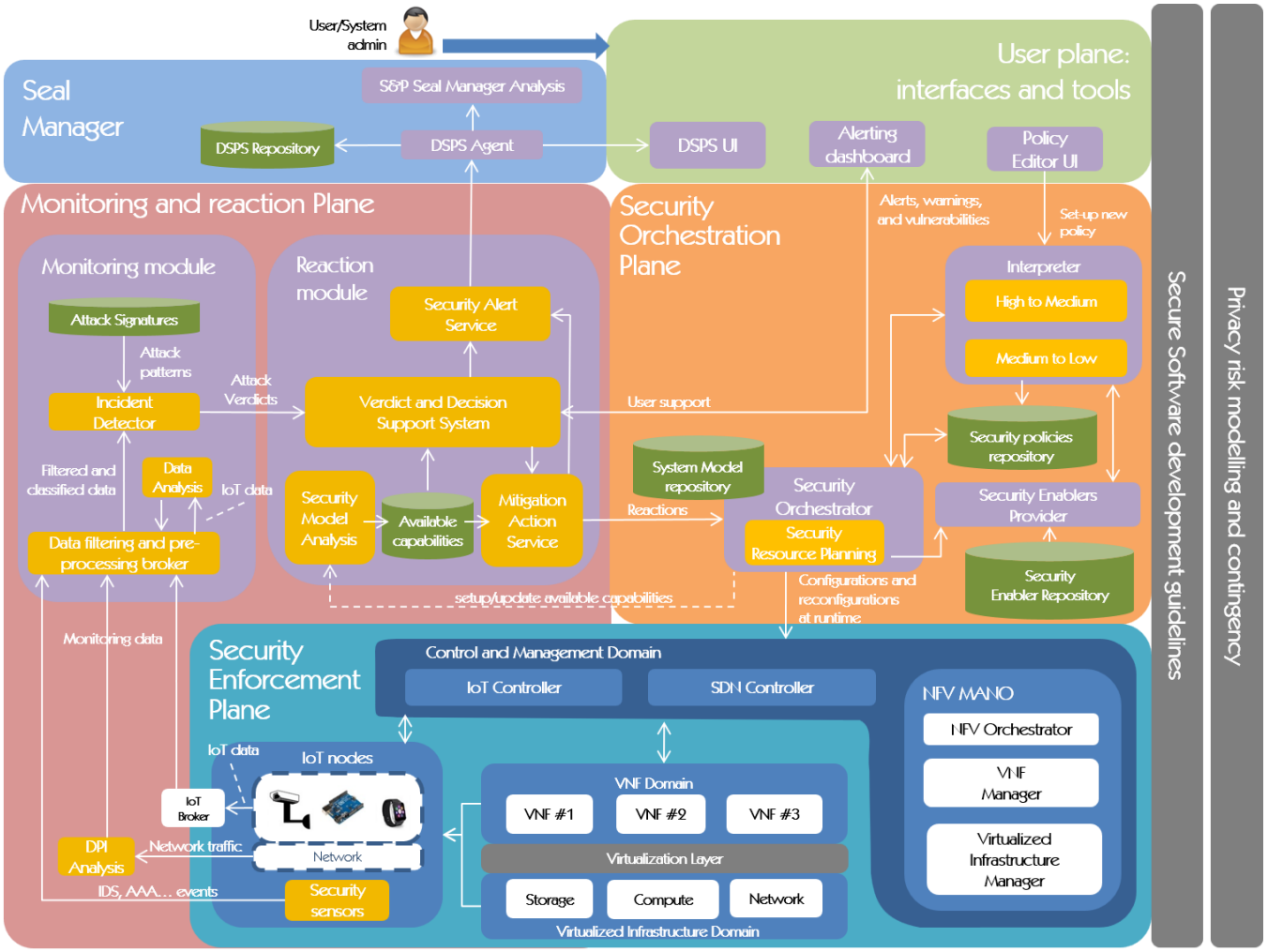

Figure 2. ANASTACIA reference architecture [3].

- **Security Enforcement Plane**: Includes Control and management domain, which is responsible for supervising and managing the resource utilization and tun-time of security enablers. This plane connects the control data plane to the security orchestration plane. Three interfaces were defined in this scope: 1) SDNI (SDN Interface) in order to improve the overall security, the security orchestrator can enforce new flow rules on the SDN controller; 2) NFVInt (NFV Intefce) for Virtual Network Functions (VNF) management, the security orchestrator also requests the NFV MANO either to instantiate new security VNF or configure an existing one; 3) IOTI (IoT Interface) through which the security orchestrator may apply security controls on the IoT infrastructure through IoT controller.
- **Security Orchestration Plane:** manages the enforcement plane resources. It incorporates a Security Orchestrator, which chooses the security enablers as an outcome of a policy refinement. A security enabler provider contains a list of security enablers able to satisfy the security policy requirements

such as authentication, authorization, confidentiality, privacy and anonymity, traffic diversion, Quality of service, data aggregation.

- **Monitoring and Reaction Plane:** Collects security-related data from the IoT platform through monitoring agents. This plane also checks the satisfaction rate of the security policies by examining threats signature, security models, and data parsing for anomalies detection. Based on the detected anomalies, reactions can be scheduled.
- **User Plane:** Incorporates a policy editor user interface that facilitates modeling security policies.
- **Seal manager domain:** provide a graphical illustration of the system status to the end-user.

In ANASTACIA, Artificial Intelligence (AI) is mainly used in the monitoring and reaction plane, more specifically at the Data analysis engine to identify compromised devices. In this scope, ANASTACIA is using an approach based on Constraint Satisfaction Problem (CSP) and declarative programming. This detection model was designed through three main steps: building an initial model, learning the best model, and finally verification of the best model. The AI-based reaction agent uses different ML algorithms such as J48, Byes Net, RandomForest, Hoeffding, Support Vector Machine (SVM), and deep learning, for detecting different attacks related to IoT behaviors and/or network patterns [4]. The tests showed the effectiveness of this model against multiple advanced attacks such as Man-in-the-middle and flooding [5].

2.1.3 5G-ENSURE

5G-Ensure is 5G-PPP phase 1 project, paving the way to the 5G networks security by designing a trustworthy security architecture that extends the existing 3rd Generation Partnership Project (3GPP) architectures, such as 3G and 4G, to fit the 5G environments and covers the concept missing such softwarization, virtualization, slice concept, and trust models involving all stakeholders. In addition to developing security enablers for the core of the 5G Reference Architecture.

5G-Ensure provides 4 basic concepts in its security architecture: domains, strata, security realms, and security control classes.

Domain: 5G-Ensure begins with dividing the 5G reference architecture into different domains. A domain in the context of the project means network entities grouped using physical or logical aspects. This concept was leveraged from TS 23.101. As shown in Figure 3, the architecture is divided into three horizontal groups of domains:

1. **Infrastructure domains:** focusing on the physical aspects of the network.
2. **Tenant domains:** logical domains running on top of the infrastructure domains.
3. **Compound domains:** defined to capture higher entities groupings. It consists of a collection of other domains determining a 5G aspect such as slice domains, core domains, etc [6].

Then, the infrastructure domains, are divided into three types, namely: (i) Universal Integrated Circuit Card (UICC) Domains (ii) Mobile Equipment Hardware (MEHW) Domains (iii) Infrastructure Provider (InfraP) Domains.

Similarly, the tenant domains is split into 10 domains such as Mobile Equipment (ME) Domains, Serving (S) Domains, etc. And the compound domains into 10 domains including slice domains, core domains as defined above.

Stratum: Is a group of protocols, data, and functions related to one aspect of the services provided by one or several domains. This concept is leveraged from TS 23.101 [7].

Security Control Class (SCC): This concept was introduced by the 5G-ensure project. It refers to a collection of security functions to protect the 5G networks. It involves (Authentication, Authorization, and Accounting (AAA), Confidentiality, Integrity, Trust ...etc.)

Security Realm: Similar to the Security Features group concept as defined in TS 33.401 [6] it captures the security requirements of strata or domains. Divided into Access Network, Application, Management, etc. security needs.

The project provides these three concepts in order to get a detailed overview of the security mechanisms required in 5G networks. The Security control classes ensure the protection of the security risk defined by the security realms. The latter captures the security concerns in one or more strata or domains. [8]

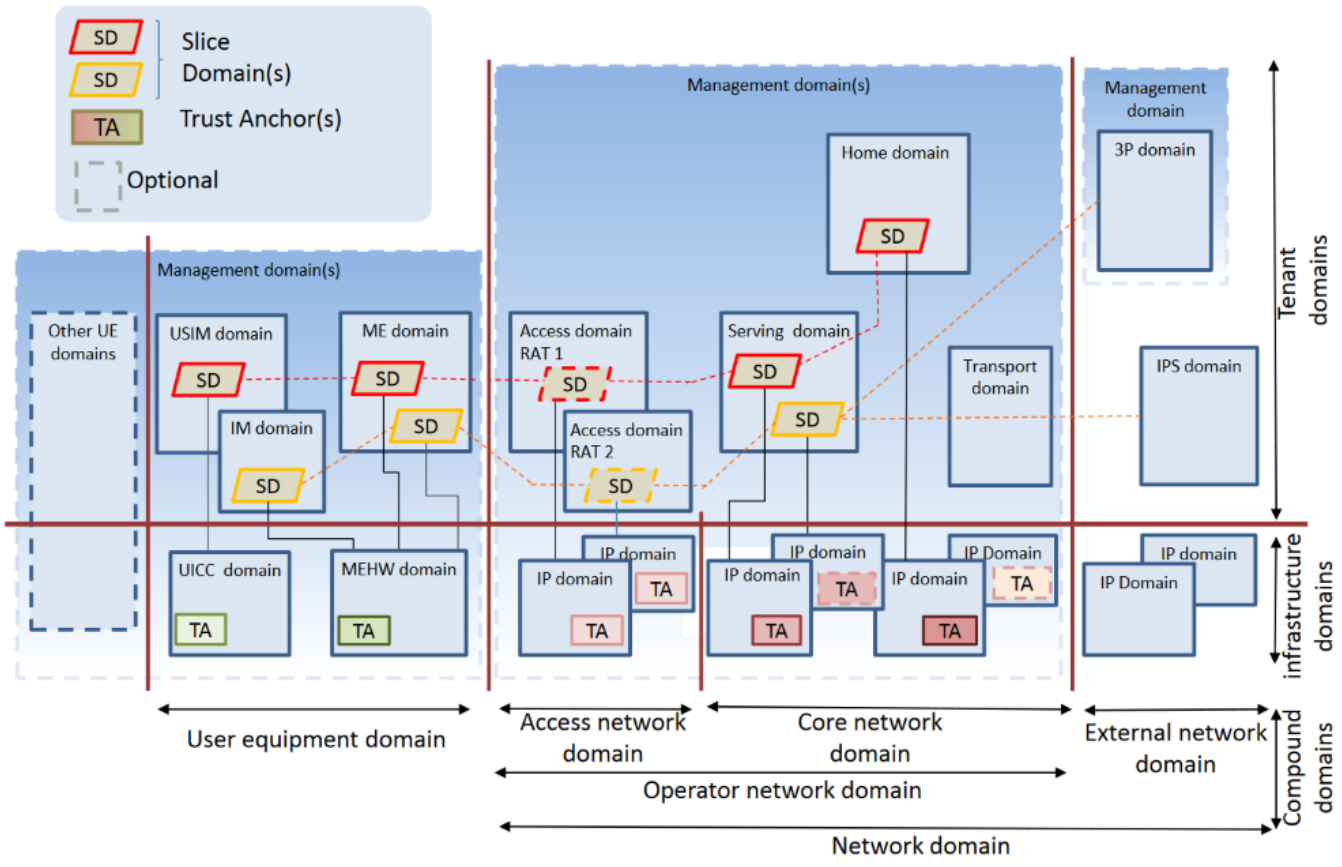

Figure 3. 5G-ensure security architecture domains

5G-Ensure defined 31 use-cases grouped into 11 thematic clusters (AAA, Privacy, Trust, Security monitoring, Security management, etc.) based on similarities. According to these use cases the project implemented a number of enablers. Table 1 shows examples.

Table 1. Expamles of 5G-ensure enablers

Category	Enablers
Authentication, Authorisation and Accounting	Internet of Things; Fine-grained authorisation
Privacy	Enhanced Identity Protection; Device Identifier Privacy; Device-based Anonymisation; Privacy Policy Analysis
Trust	Trust Builder; Trust Metric; VNF Certification; Security Indicator
Security Monitoring	Satellite Network Monitoring; PulSAR (Proactive Security Assessment and Remediation); Generic Collector Interface; System Security State Repository; Malicious Traffic Generator for 5G protocols
Network Management and Virtualisation	Access Control Mechanisms; Component-interaction Audits; Bootstrapping Trust; Micro-segmentation; Flow Control

Mapping the developed enablers onto the security architecture demonstrates its applicability. The validation of the enabler efficiency was evaluated on a testbed environment [9].

2.2 Threat modelling

Threat modeling is a risk-based approach to designing and implementing secure systems based on identifying and prioritizing threats with the purpose of developing mitigations to them [10].

2.2.1 *KEY CONCEPTS*

Key concepts and definitions from the cybersecurity domain, necessary for understanding the basics of threat modeling, include:

- **Threat:** A threat is an event or object in the environment that has the potential to harm one or more assets.
- **Vulnerability:** Vulnerabilities are exposures. A vulnerability is the result of an un-mitigated threat.
- **Risk:** A measure of damage potential, typically expressed in terms of the probability and loss expectancy associated with an event.
- **Threat Actor** or **Threat Agent**: Anything able to perform or use a use case or an abuse case.
- **Threat Vector or Attack Vector:** An interface through which an attack can traverse.
- **Attack:** Any action that supports a threat motive against a target asset by exploiting a vulnerability.
- **Attack Surface:** The set of all possible attack vectors.
- **Asset:** Any resource that has an intrinsic value. It does not have to be physical. For example:
    - Hardware
    - Credentials
    - Intellectual property

    - System availability
    - Business reputation
- **TTP**: Acronym (**T**ools, **T**actics, and **P**rocedures)
- **TOE**: Acronym (**T**arget **o**f **E**valuation)
- **Use Cases:** Expected design behavior of a system.
- **Abuse Cases:** Manipulation of use cases to achieve malicious objectives of an attacker.
- **Attack Tree:** A representation of the relationship between threats, target assets, associated vulnerabilities, correlating attack patterns, and countermeasures. Use cases serve as metadata associated with assets, and abuse cases serve as metadata for attack patterns.

2.2.2 *METHODOLOGIES*

There are numerous threat modeling methodologies of varying maturity and complexity:

- **STRIDE**, invented by Microsoft in 1999, is still applied by the Threat Modeling [11] process and respective tool of the Microsoft Security Development Lifecycle [12]. The name of the method is actually a mnemonic that is based on how threats are categorized:
    - **S**poofing identity (System Property: Authentication)
    - **T**ampering with data (System Property: Integrity)
    - **R**epudiation (System Property: Non-repudiation)
    - **I**nformation Disclosure (System Property: Confidentiality)
    - **D**enial of Service (System Property: Availability)
    - **E**levation of Privilege (System Property: Authorization)

For more details, please refer to the STRIDE cue cards by ThoughtWorks, linked from [10].

- **PASTA** (Process for Attack Simulation and Threat Analysis) [13] is a seven-stage risk-centric framework, developed in 2012, that quantifies risk that might impact a business or a system, based on context associated to the relative importance of the application to the business.
- **TARA** (Threat Assessment and Remediation Analysis) [14] is part of MITRE's portfolio and is used extensively by U.S. Department of Defense and Department of Homeland Security. It uses TTP catalogs and is also risk-centric, as it attempts to define risk mappings to threats.
- Many others: Trike, VAST, SPARTA, LINDDUN, OCTAVE, etc. Most are risk-centric model, like PASTA & TARA, while some are more focused, e.g. LINDDUN emphasizes privacy concerns.

2.2.3 *THREAT MODELING FORMAL METHOD*

In practice, there is no single correct or best methodology for threat modeling. Most of them are similar in their implementation steps, and modern security organizations tend to use a hybrid approach to threat modeling that borrows from several different methodologies.

For the purpose of the analysis per use case that follows, we will be adopting STRIDE as the threat classification model due to its simplicity and maturity.

In terms of the activities involved, the workflow is as follows (each step is elaborated further below):

1. Review system architecture and requirements
2. Identify objects in the system under assessment
3. Identify flows between those objects

4. Enumerate assets of interest
5. Enumerate threats
6. Determine exploitability and risk
7. Identify and review mitigations

Review system architecture and requirements

For each use case to be studied, the following items need to be collected and reviewed:

- System architecture diagrams in sufficient detail to determine system components and interactions, including external components & dependencies;
- Data dictionary, Data classification, and Data flow documents;
- Business requirements, Security requirements, Use cases/Abuse cases.

Identify objects in the system under assessment

This involves decomposing the target of evaluation (TOE) as follows:

- Inventory and classify all data consumed by the TOE;
- Enumerate all components the TOE consists of and determine their native security controls;
- Identify all external entities and dependencies used by the TOE;
- Inventory actors that interact with the TOE (actors do not necessarily have to be human).

Identify flows between those objects

- Identify logic flows between components and other objects identified previously;
- Inventory data sources and data sinks;
- Identify data flows between TOE components and external entities;
- Identify all trust boundaries and the methods used to enforce trust boundaries.

Enumerate assets of interest

- Enumerate all assets that must be protected to ensure the confidentiality, integrity and availability (CIA) of the TOE (assets do not necessarily have to be physical in nature);
- Include a brief description of each asset with justification for classifying the object as an asset.

Enumerate threats

Using a TTP catalog for guidance, identify and document the threats that impact TOE assets. This activity must include:

- A brief description of the threat type;
- Identifying the entry point for an attack against the targeted asset(s);
- A description of the attack pattern(s) used to carry out the threat;
- Mapping of identified threats to the associated asset(s) and threat actors.

Note on TTP catalogues: Since the inception of the seven-stage Cyber Attack Lifecycle (Kill Chain) by Lockheed Martin [15], extensive knowledge bases of adversary tactics and techniques have been introduced. MITRE

ATT&CK (https://attack.mitre.org) maintains multiple such matrices that cover preparatory techniques (PRE) and Enterprise, Cloud, Network, as well as Mobile domains. But, as more applicable for 5G and beyond networks, we will be using the recently released (updated) ENISA Threat Landscape for 5G Networks [16].

Determine exploitability and risk

- Once threats are identified, determine the plausibility of each threat as follows:
  - Conduct attack simulation (kill chain) exercises to determine whether there is realistically a path to exploitation in the context of the TOE, or…
  - Construct attack trees to model methods by which an attacker may achieve goals;
- Complete a quantitative, or at least qualitative, risk assessment for each threat.

These activities are more advanced. A threat model can be prepared without having necessarily to conduct attack simulations or construct attack trees, and risk assessment can be qualitative.

Identify and review mitigations

- For each identified threat, identify and document appropriate mitigations against the threat;
- Review mitigation controls applied. Identify and document any gaps between the existing mitigation controls and the required mitigation controls.

2.3 Protection of AI-driven solution

Despite the incontestable role that AI will play in enabling self-managing capabilities, its use introduces new threat vectors that can jeopardise the performance as well as the security of future mobile networks. Indeed, AI/ML systems can be fooled to make wrong decisions or leak confidential information [17]. Different taxonomies have been developed [18] [19] [20], classifying the attacks against AI/ML techniques into poisoning attacks, evasion attacks and model's API-based attacks. The poisoning attacks targets the training phase by tampering with data or ML algorithm. The evasion attacks aim at the inference phase by introducing small perturbations to the input samples in order to bypass the learned model. The model's API-based attacks attempt to extract the training data or the model's architecture leveraging the output of ML-as-a-Service API. The aforementioned attacks may lead to integrity, availability or privacy violation. The authors in [20] conducted an in-depth investigation of security issues that can be brought by the adoption of AI/ML techniques in 5G and beyond networks. The study identifies the potential threats vectors against AI/ML systems, while providing concrete use cases showing how the exploitation of these attacks can undermine the security of future mobile networks. The authors introduced a set of defenses to safeguard from AI threats, while pointing out their adoption challenges and advocating on which components of the ITU-T's FG-ML5G unified architecture[1] they could be enforced. Possible defense mechanisms that could be adopted to enable robust AI/ML models include input validation, adversarial training, ensemble methods and moving target defense [21] .

From standardisation perspective, the Securing Artificial Industry Specification Group (ISG SAI)[2] has been created by ETSI. The group aims to develop technical specifications to tackle threats arising from the

[1] https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx

[2] https://www.etsi.org/committee/1640-sai

deployment of AI in ICT field. Recently, the group published their first report [22], describing the challenges of securing AI-based systems, including challenges relating to data, algorithms and models in both training and testing phases. The report presents a number of different attack vectors and various real-world use cases on how these attack vectors can be leveraged.

Distributed artificial intelligence (DAI) has been leveraged in 5G and beyond networks in order to automate the management and support coordination between the different agents, in addition to reducing the costs (time, data, etc.) and also preserving privacy and confidentiality. Accordingly, MonB5G promotes the distribution of operations and autonomous management, taking advantage of the DAI such as Federated learning.

Federated learning (FL) provides a framework that keeps the training procedure on the data source side such as user devices or network slices [23]. With the aim to protect data privacy, FL aggregates only the local models' parameters in a centralized model. Nevertheless, FL rises new risk sets since the system does not have access to the raw data and gives the malicious agent full control over the training data, training procedure, and the outcome parameters. Consequently, traditional methods which protect against data poisoning (e.g. Filtering, Remove outliers, etc.) become inapplicable. It may be noted that it is difficult for an attacker to comprise all the training data since it is heavily distributed by a massive number of clients. Moreover, the attacker does not control the aggregation algorithm. FL is exposed to most of the traditional ML threats discussed earlier, a survey can be found in [24]. However, the conventional solutions remain effective in FL except for poisoning attacks that need innovative solutions thus we focus on this attack in what follow.

An overview was introduced in [25] about the mechanisms used in the centralized ML methods to detect poisoning inputs but a requirement to access the training data is needed. Studies [26] [27] examined the poisoning attacks on federated learning . In [26] the authors confirmed that the poisoning in FL is more powerful compared to the conventional techniques since FL poisoning influences the model rather than the training data. This work has introduced semantic backdoors that cause the model to misclassify inputs without perturbations (unlike adversarial examples).

V. Tolpegin et al. [27] demonstrated that data poisoning attacks such as label flipping can provoke significant drops in the model accuracy and recall, even with a small percentage of malicious participants. Moreover, the authors revealed that the adversaries can enhance the attack impact by targeting the availability in the later rounds. As a potential solution, they propose a defense strategy based on principal component analysis (PCA) to reduce update parameters dimension and cluster them at each round before the aggregation which can identify the malicious participants.

These works stated the potential threats that face the implementation of ML solutions. MonB5G is heavily based on ML and it is adopting decentralized techniques (i.e. FL) to detect network slice attacks, and also in energy-efficiency techniques. Thus the project considers the FL robustness and protection against the misbehaving decentralized elements by enhancing the existing approaches [21] [26] [27] and involving new mechanisms such as Blockchain to protect the data and the exchanged parameters in the network.

3. MonB5G Reference architecture instantiated for security management

MonB5G vision is to manage a massive number of slices using fine-grained management services tailored to 5G network slice particularities. Slices in 5G are logically isolated networks providing different services in

distinctive network requirements achieved by varying nodes, resources, localisation, etc. This heterogeneity requires specific management per slice. On the basis of these facts, in this section, we will instantiate the MonB5G reference architecture described in the D2.1 for security management.

3.1 Network slicing threats and security requirements management

In 5G network slicing, every slice is a unique composition of nodes and requirements. Hence, it has its own threat set that can be identified based on a threat model to select the slice customized security enablers. The threats depend on the service type. For instance, an IoT slice will have different threats when compared with a streaming slice. For this reason, we consider selecting security requirement for the slice dynamically before the deployment based on its template and accordingly its specific security management.

The main threat in network slicing is the weakness of isolation in terms of both resource and security. While the lack of resource isolation might lead to resource starvation, the weak security isolation facilitates attacks between the coexisting slices, for instance, a side-channel attack [28].

However, the slice spans over multiple technological domains composing the 5G network (e.g. Core Network, MEC, Tansport Network and Radio Access Network (RAN)) that are exposed to distinct threats:

- In the Core Network, the core functions are IP-based services and thus, they are target to all the IP based attacks, e.g., DDoS attacks. Furthermore, the core leverages a set of technologies such as NFV, SDN, etc., which might be immature and bring a new set of threats.
- The use of edge computing creates new cybersecurity concerns, that require dedicated security. Since the network functions hosted on the edge will not be exposed to the same physical and virtual threats as the hosted on the core. To clarify, apart from the physical threats in the user-close management, the edge might act autonomously to avoid the backhaul delay leveraging local services (i.e authentication) which rise new challenges.
- RAN threats are often related to the user authentication and authorization system, like Rogue Base Stations (RBSs) that can steal user data, tracking or redirecting the user to a malicious endpoint.

The intersection of both end-to-end slice threats and domain threats results in distinct security requirements to be delegated to the sub-slice security manager. In contrast to the end-to-end slice management that does not consider the requirements of the technological domain, or the domain centralized management that lacks strong isolation between subslices; the subslice dedicated security manager will be efficient and optimized to target the specific subslice threat related to the hosting technological domain needs and also maintains the isolation between subslice. Yet the subslice security manager can not see the other domain subslices (cross subslices management) requirements that cannot be omitted but will be centralised per domain.

3.1.1 SECURITY MANAGEMENT ARCHITECTURE AND COMPONENTS

The reference architecture of MonB5G was detailed in the D2.1. In this section, we will describe the main security management components. Figure 4 represents Monb5G architecture composed of:

i) Inter-domain management for the global networks, it also handles the first deployment request from Monb5G portal.

ii) Domains hosting slices, and a hierarchy of fine granular and higher abstractions management and orchestration layers.

To manage security enablers in MonB5G, we design security orchestrators. In general, a security orchestrator (SO) examines security requirements and provides the adequate closed loops defined by the atomic elements (MS, AE, DE, and ACT) to deliver security as a service (SECaaS). The SO leverages the slice template, the SSLA, and the threat modelling to select the required security instances.

3.1.1.1 SECURITY ORCHESTRATOR

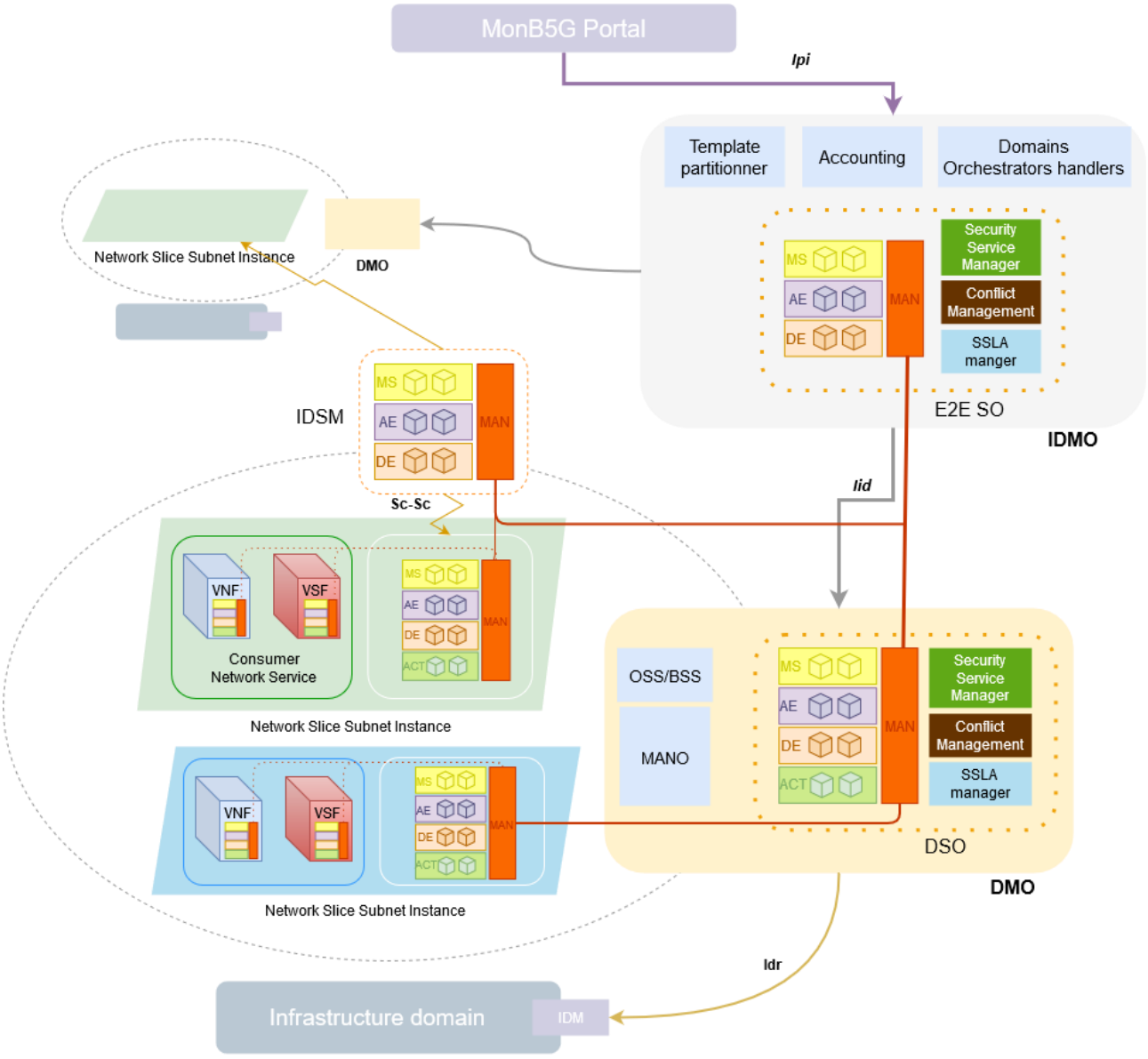

Figure 4. MonB5G Security Management architecture and components

Our architecture defines two security orchestration levels: E2E orchestrator located in IDMO level, this SO processes the E2E slice template and its SSLA. To select the IDSM security closed loops, in addition to the appropriate partitioning of security responsibilities. However, at the domain level, the local orchestrator is a part of the DMO, managing the subslices' and nodes' security closed loops and ensure the cross subslice protection of instance resource isolation.

- Security service manager: Manages the atomic security elements (MS, AE, and DE) by instantiating and deploying them in the management platforms.
- SSLA manager: Translates the SSLA requirements into security actions and KPIs while deploying a sub-slice to monitor and ensure that the tenant security requirements are met.
- Conflict manager: The different security loops are working autonomously and independently from each other thus to prevent the conflicts between the different component SO provide a module called conflict manger.

3.1.1.2 SECURITY AS A SERVICE

In MonB5G, we define the pervasive management as Management layer as a service (MLaaS). It is composed of three layers: Monitoring, Analytics, and decision layer. Each one hosts a collection of atomic elements. These modular elements are interchangeable and reusable to support FCAPS management. In this section, we will target exclusively the security management or what we call SECaaS defined as a selected combination of MSs, AEs and DEs deployed on-demand to provide a security management service.

As depicted in Figure 4, SECaaS is distributed on different management levels in the architecture categorized into two main locations: (i) Static locations to manage the whole framework slices (ii) Dynamic locations related to a single slice and its subcomponents (subslice/nodes).

SECaaS in the static levels is a part of the security orchestrators. It provides the inter-slice security management considering the cross-slice threats and providing the related actions such as migrating/quarantine slices, and the intelligence to assist and manage the dynamic SECaaS:

- E2E security orchestrator (E2E SO): As defined earlier, this component is critical before deploying the slice since its main role is to extract the slice security requirements and select the inter-Domain slice manager security services.
- Domain security orchestrator (DSO): manages a single domain's slices. The SECaaS at this level helps in managing the inter-subslices security needs and oversees the lower-level SECaaS. For instance it processes the made decisions.

SECaaS in the dynamic levels is a part of the slice management, their existence depends on the slice lifecycle and they are placed in multiple levels defined below:

- Inter-domain slice manager (IDSM): In the IDSM, SECaaS is responsible for the end-to-end slice security management. The components in this layer are selected by the E2E SO. They leverage the lower-level SECaaS to provide E2E slice security.
- Slice management layer (SML): SECaaS in this level manage the security in the domain slice (subslice). It is one of the crucial PaaS since it provides the executive layer (ACT layer) that executes the security decision policies coming from the same level or higher levels. The execution of the security combines the translation of the high-level policy into a low-level configuration then enforcing the configuration

in the existing Virtualized Security Functions (VSFs) or requesting the deployment of a new VSF (Security enabler).

- Node: Lightweight SECaaS related to a specific node (VNF) ensuring the protection of the inner application and the exposed protocols. It can be deployed in the creation of the VNF image or at the instantiation phase where it can be either running inside the VNF or hosted into a separate VNF the essential point is that this management loop is limited to a single VNF scope.

***SECaaS components*:**

The SECaaS is a combination of the atomic elements defined below:

- Monitoring system (MS): collects real-time security-relevant data, provides information to the AE, and pre-processes the collected data. For instance, an MS might collect the traffic from a specific interface and pre-process it by extracting the flows and features needed by an AE attack detector.
- Analytics engine (AE): based on AI algorithms, it processes the monitored data in order to extract high-level security information and events. For example, it could analyse the feature extracted from the traffic flows to detect DDoS traffic. Analysing the collected KPIs, network flows and resource status will help diagnostic the node and the network to detect or predict attacks and security issues.
- Decision engine (DE): This is the mastermind that can tell the system what to do as a reaction or prevention to protect the network against security threats. The decision can configure an existing security enabler in the slice or deploy a new one. In the previous example, the DE might decide to block the traffic in an existing FW or deploy a new FW. These decisions are described in an abstract model rather than vendor-specific. The DEs are atomic elements that have a specific autonomic security function that needs to be carefully selected based on the potential threats existing in the slices, VNFs, etc. In other words a single DE cannot be generic to detect all potential threats neither the ability to provide all the possible decision; however each DE has different characteristics for the set of security events that can manage and their related decisions depending on this the SO choose the best DE.
- ACT: The ACT component is responsible for the final phase in the autonomous loop. It is in charge of enforcing security decisions, first by performing a translation from the high-level decision into vendor-specific configuration according to the targeted enablers. Then, executing the decision steps that can be updating the configuration of an existing VNF/VSF or deploying a new one through MANO.
- Manager (MAN): playing the role of a channel between the three layers hosting the previous components in addition to wrapping these layers and expose interfaces to the external entities such SO, Higher SECaaS, etc.

3.1.1.3 INFRASTRAUCTURE SECURITY MANAGEMENT

MonB5G assumes that the infrastructure needs a programmable management, for this reason it provides Infrastructure Domain Manager (IDM) that manages the infrastructure by requesting management functions from the DMO to cooperate in the security management. These security management functions manage the resources and support cross-slice attacks the detection such as resource starvation. In addition to trust operations for instance boot trust.

3.1.1.4 ARCHITECTURE INTERFACES

We introduce bellow the main interfaces and reference point used by the security components:

- Iid: Os-Ma-Nfvo-like interface, used by the IDMO to manage slices LCM implemented by DMO. It can be seen as MANO Os-Ma-Nfvo extended interface. It may provide LCM abstractions and provides to IDMO data and management capabilities of the DMO. Including communication between the E2E Security Orchestrator and domain orchestrators
- Idr: DMO-IDM permit to the DMO allocating, updating or deallocating resources. This interface is also used to exchange between DMO and IDM security related information about the infrastructure, for example, free and used resources changes by specific VNF instances.
- So-Os: The reference point between the SO and the OSS is used by the OSS to delegate the management of the security goals of network slice to the SO.
- Sc-MB5G: The reference point between the security mangers and the MonB5G sublayer components is used to interact with MonB5G components to create closed loops for security management.
- Sc-Sc: This reference point is used for the control communications between two security services. The E2E security service has a global view over the activities of slice subnet security platforms and manages the E2E security requirements. In turn, the slice subnet security service controls the functional security platforms to ensure that each slice subnet instance is well protected.
- Sc-Ma: The reference point between the security platform and the MANO particularly interactions with NFVO to manage and monitor NFVs. It is related to the reference point Sc-Or as defined in ETSI GS NFV-IFA 033.
- Sc-Vnf: The reference point between the security platform and the consumer NFV object. The functional security platform offers VSFs such as firewall, Intrusion Detection System (IDS), access management as protection measures to improve the security of the slice subnet instance.

3.2 AI-driven security through MS/AE/DE

As stated earlier, MonB5G advocates for LCM procedures mainly based on ML and AI and relies on three distinct entities that collaborate, namely, Monitoring System (MS), Analytic Engine (AE), and Decision Engine (DE). The combination of the three elements allows enforcing the concept of zero-touch management (ZSM) using ML. MS and AE are used to monitor the system functioning and detect security threats, while DE will consider actions to mitigate threats and avoid that the system fails. In the context of network slicing, ZSM is highly needed to mitigate the high complexity to manage network slices, as several components of different technological domains (VNF, Physical Network Function (PNF), MANO, NFVI, RAN, CN, etc.) are involved; this increases the number of threats that may come from several sources. MonB5G mitigates this complexity with the usage of MS/AE/DE. MS is deployed to monitor key KPIs from different domains, AE correlates and analyses the monitored data to detect threats, and DE considers and enforces multi-domain decisions.

In this section, we recall each entity's functioning and its role in the AI-driven security solution provided by MonB5G. More details on the three MonB5G key entities are available in D2.1.

3.2.1 MONITORING SYSTEM (MS)

The role of MS in MonB5G is to collect critical information on the functioning of a system and provides this information, after, for example, aggregation or normalization, to AE, which in turn uses this information to

detect and react to Network Slice (NS) Life-Cycle Management (LCM) events, such as performance degradation, performance optimization, and security threats.

MS interacts with different entities that orchestrate and manage the end-to-end NS, i.e., different DMOs. Besides, MS interacts with slice-specific VNF and applications, as well as shared VNF and PNF among network slices.

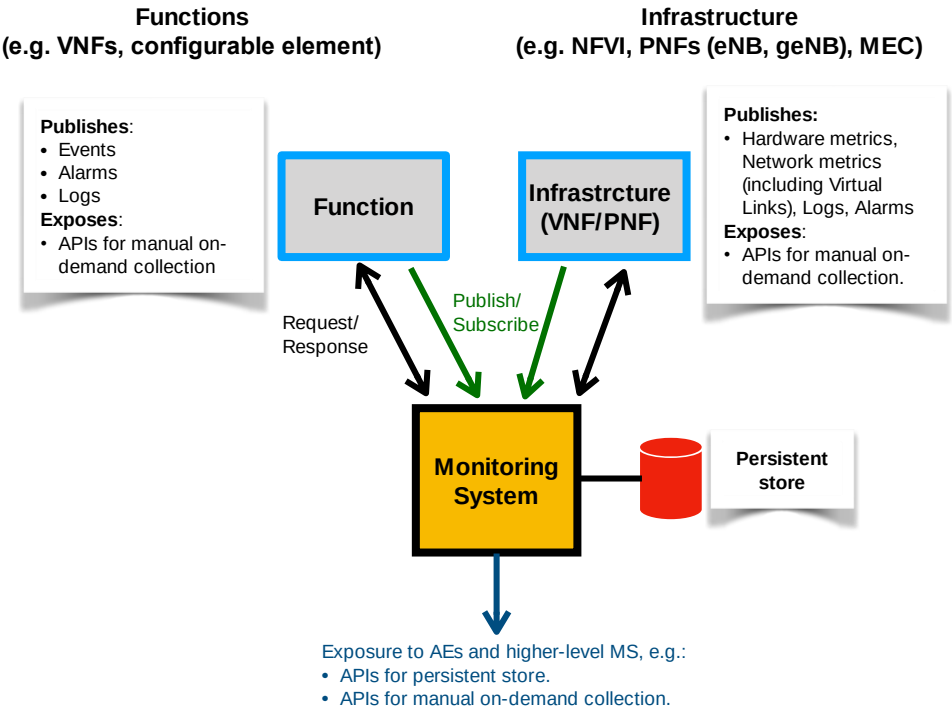

Figure 5. MS interaction

As depicted in Figure 5, we distinguish between information that monitors the state of the infrastructure shared by the running slices and the information that monitors the VNF of tenants and applications state.

For the infrastructure monitoring, MS has to interact with DMO(s) to collect information on:

- NFVI: such as computing platforms and hardware;
- PNF running network functions on dedicated hardware: such as eNB/geNB, router, and UPF;
- VNFs running common virtualized network functions: such as Core Network (CN) functions or Directory Name Service (DNS).

Regarding Function monitoring, MS has to interact with the VNFs or applications of the tenants. Since there is no standard way to enforce such interaction, MonB5G may dictate design guidelines that would allow MS to request and collect metrics from VNFs or applications. In this case, MS may collect all information considered as service-level metrics, such as Events, Alarms, Logs.

The principal consumer of MS information is AE, which is in charge of triggering the monitoring of needed information from MS. The latter starts the monitoring process by connecting to the appropriate source, i.e., infrastructure and Function. Accordingly, MS exposes two types of Application Programming Interfaces (API): control API and data collection API. Control API may be used by AE to request metrics to monitor, the periodicity, the duration, etc. While the data collection API is the interface from which data are provided to AE as requested through the control API. The control API also indicates how data are provided, i.e., publish/subscribe, request/response, the data format, etc.

Particularly, in the context of security, MS is envisioned to monitor metrics on the computing and network resource consumption of VNFs and PNFs to detect overconsumption of resources, which may indicate abnormal functioning of the VNF or PNF. Besides, MS should be able to monitor service-level KPI of VNF or PNF, such as the attach and detach requests of UEs at the Mobility Management Element (MME), which can be used to detect DDoS attacks.

3.2.2 *ANALYTICAL ENGINE (AE)*

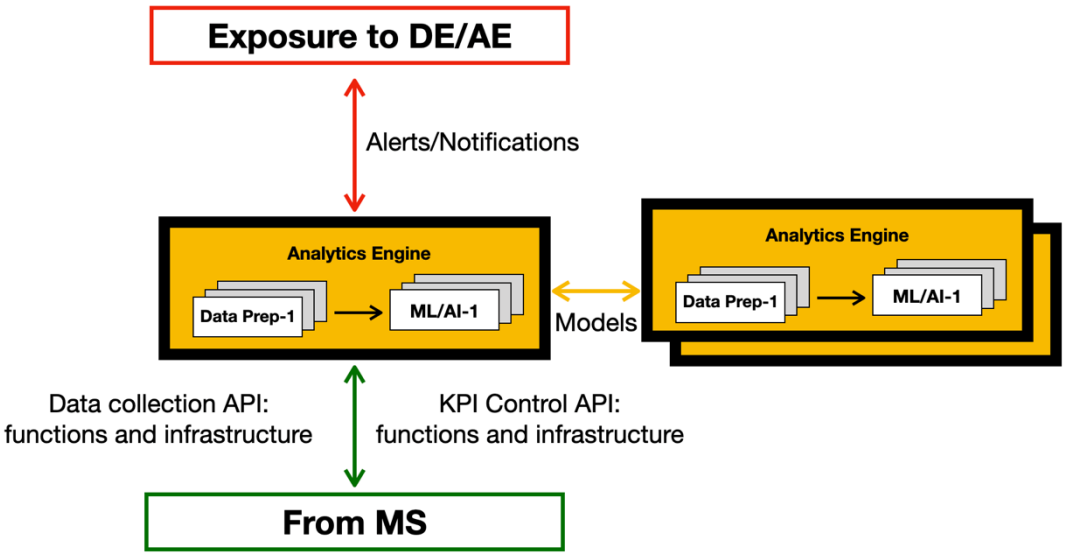

Figure 6. AE interactions

As opposed to MS, AE does not store but processes data gathered from the same or lower-level MS or AE and exposes the result to any requester (i.e., Decision Engine or other AE) in an on-demand or periodic fashion. AE to AE communication is possible, mainly to build a learning model using federated learning techniques. Figure 6 illustrates the interaction between AE and MS and between AE and DE.

Generally, the main functions of AE are: (i) identify performance degradation of a network slice; (ii) optimize the performance of a network slice or the DMO resources; (iii) react to security threats. To this aim, AE subscribes for data types to which it is interested in using the control API exposed by the MS. The data type will be determined according to the logic of the LCM application execution. Then, AE starts receiving the stream of data or use a request/response mechanism, depending on the purpose of the analysis. AE may adapt the monitoring data rate or stop the request and request for other related monitoring information.

AE is able to complete an inference task locally, extract features, and to analyse these features and send alerts and notifications to DE. AE may collaborate with other AE to build distributed learning (based on federated learning) model to realize the analysis and notify the DE accordingly.

In the case of AI-oriented security, AE has a crucial role. AE collects data from several MS, covering a wide range of information coming from different domains. The collected data is correlated and interpreted by AE, using ML algorithms. An example of AE relying on ML is anomaly detection using neuronal networks or a classifier.

3.2.3 *DECISION ENGINE (DE)*

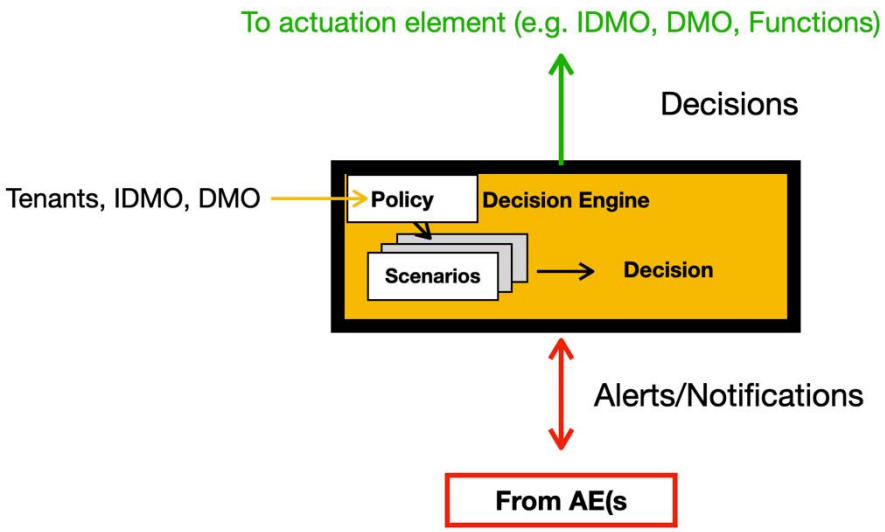

Figure 7. DE interactions

As depicted in Figure 7. DE interactions, DE is the decision making element of the MonB5G architecture. It analyses alerts and notifications from AE(s) and considers a decision to take. The decisions are either derived using a local ML algorithm, based mainly on Reinforcement Learning (RL), or a predefined policy enforced by the Tenant or DMO through Intent, or a combination of both.

DE may collect notification from several AEs, which may interact with MS monitoring different TDs to consider a global decision on the end-to-end NS. Global decisions are mainly considered at the IDMO level.

DE interacts with actuation elements (function, DMO, or IDMO) to enforce the considered decisions. For local decision, DE interacts with DMO and function; while for global decisions, the DE has to interact with IDMO.

4. MonB5G AI-driven security techniques: Attack identification and mitigation

4.1 In-Slice attack mitigation: case of MME/AMF

4.1.1 INTRODUCTION

Through this scenario, we will demonstrate the robustness of MonB5G for identifying, detecting, and then mitigating the in-slice attacks. The main objective is to define and implement the following MonB5G security features: security orchestration through the combination of MS/AE/DE, attack detection, and mitigation involving one or two DMO (RAN and CN).

For this scenario, we consider a subset of UEs that have been attached to a specific Network Slice Instance (NSI) and generate malicious traffic towards the infrastructure services, trying to exploit management interfaces. A typical example is compromised Machine Type Communications (MTC) devices generating a massive number of network attachment requests corresponding to DDoS attacks on the Core Network element, namely MME/AMF. This generates events both at the RAN and the core network level, where separate monitoring (MS) components are deployed. At the same time, decision (DE) and analytics engines (AE) are deployed at the management plan. These attacks need to be quickly identified, and the system should ensure that it has not incorrectly classified normal network traffic as malicious (i.e., false positive). Moreover, the decision engine should apply the appropriate policy to mitigate them.

Before detailing the function and the logics of the three MonB5G entities (i.e., MS, AE, and DE), we give an overview on existing DDoS attacks and solutions focusing on mobile networks.

4.1.2 STATE OF THE ART ON EXISTING ATTACK AND SOLUTIONS

The isolation offered by Network Slicing offers performance enhancements to the applications, but is also essential for security. While slicing should ensure isolation, where such that attacks (e.g., data leakage, breach, DDoS) remain contained and do not propagate to the network. Yet slices also have many inherent vulnerabilities, in the slice selection and isolation mechanisms.

This sub-section will investigate the state-of-the-art threats affecting specifically in-slice attacks. First, through a broader look, utilising the core information security triad; confidentiality, integrity, and availability (CIA). Second, by examining threats to specific function assets.

Network Slicing Threats vs. CIA Triad [29]

1. **Traffic Monitoring**
   When an attacker can monitor traffic (north or southbound), they could also understand the slice configuration, thus breaching confidentiality. Furthermore, if the attacker can capture a token or impersonate an element, this could escalate to a breach of authorization or authentication.
2. **Traffic Injection**
   When an attacker can inject traffic into northbound or southbound interfaces, effectively exposing them through breach/disruption of the NFV orchestrator, as well as the corresponding subset of elements controlled by the network slice management system. Thus, causing breach of integrity or availability with varying breadths.
3. **Side-channel Attacks**
   If any given slice does not properly allow access to other slices' data/control plane, it could allow side channel attacks through shared resources. These attacks are time-based, and infer the data from slices by introducing combinations of data from the cache, until one is processed faster than the others. This causes breach of confidentiality of varying severity, but also availability and integrity

where a neighbour slice could introduce jitter in a time-constrained service within a shared resource with other slices.

4. **Resource Hijacking**
   Slices having shared resource quotas can be abused by an attacker disrupting a single slice service, then re-shaping its usage to consume resources via the most expensive functions. Thus the network slice will be forced to take more resources form the shared pool and thus compromise availability.
5. **End-devices Breach**
   Some end devices are vulnerable due to a poor design and are thus susceptible to contamination by malware, hardware tampering or sensor errors. These compromised devices could allow inter-slice communication unintentionally, and thus cause a breach of confidentiality, and can provide unauthorized access to a slice.

4.1.2.1 MOBILITY MANAGEMENT ELEMENT (MME) AND ACCESS AND MOBILITY MANAGEMENT FUNCTION (AMF) SECURITY

ACCESS AND MOBILITY MANAGEMENT FUNCTION (AMF)

The Access and Mobility Function (AMF) in a 5G core network is a control plane function with main responsibilities of:

i. Registration Management
ii. Reachability Management
iii. Connection Management
iv. Mobility Management

Thus, AMF receives all connection and related information from the User Equipment (UE), and handles its connection and mobility tasks. Therefore, it presents specific vulnerabilities to the ecosystem, the following sub-section will investigate into more details threats that are specific to corresponding AMF assets.

According to ETSI's Security Assurance Specification [30], the identified assets will be classified into one of the following six categories:

1. **Spoofing identity**
   Identity spoofing is accessing and then using another user's authentication credentials (username and password) illegally.
2. **Tampering with data**
   Data tampering involves the malicious alteration of data. This includes unauthorized changes made to persistent data, as well as the changes in data as it flows between two computers over an open network, such as the Internet.
3. **Repudiation**
   Repudiation is a threat when a malicious user performs an illegal operation in a system that lacks the ability to trace the illegal operations. Non-repudiation refers to the ability of a system to counter repudiation actions.
4. **Information disclosure**

Information disclosure involves the exposure of sensitive information to individuals who should not have access to it. For example, an intruder is able to read data in transit between two computers.

5. **Denial of service**
   Denial of service (DoS) attacks deny service to valid users. For example, making a Web server temporarily unavailable.
6. **Elevation of privilege**
   Where an unprivileged user gains *privileged* access, and thus has sufficient access to disrupt the system.

AMF Assets and their corresponding threats according to 3GPP Technical Specifications [31] are presented in the flowing table:

Table 2. AMF Assets and their corresponding threats according to 3GPP Technical Specifications

Threat name	Threat Description	Threat Category	Threatened Asset
Resynchronization	If a RANDom number (used for authentication), and AUT(H) Authentication are not included when synchronization fails, the resynchronization procedure does not work correctly. This can result in a wasting of system resources and denial for a legitimate user to access the system.	Denial of Service	Sufficient Processing Capacity
Failed Integrity check of Initial Registration message	If integrity check of attach message fails, then the user identity cannot be verified. This can result in a wasting of system resources and denial for a legitimate user to access the system.	Denial of Service	Sufficient Processing Capacity
RES verification failure	Threat Description: If a malicious UE initiates a registration request using a Subscription Concealed Identifier (SUCI) and this request is followed by primary authentication in which an incorrect RESponse is sent to the network, then the RES verification will fail. In this case, if the RES verification failure is not properly handled e.g., AMF or Security Anchor Function (SEAF) does not reject the registration request directly, or initiates a new authentication procedure with the UE, this would result in the wasting of system resources.	Denial of Service	Sufficient Processing Capacity
Bidding Down	If Security Mode Command (SMC) does not include the complete initial Non-Access Stratum (NAS) message if either requested by the AMF or the UE sent the initial NAS	Tampering of Data, Information Disclosure	User account data and credentials

	message unprotected, the UE can force the system to lower the security level by using weaker security algorithms or turning security off, making the system easily attacked and/or compromised.		
NAS integrity selection and use	If NAS does not use the highest priority algorithm, NAS layer risks will be exposed and/or modified or be open to denial of service.	Tampering of data, Information Disclosure, Denial of Service	Sufficient Processing Capacity, Control plane signal
NAS NULL integrity protection	If NAS NULL integrity protection is used outside of emergency call scenarios, an attacker can initiate unauthenticated non-emergency calls.	Elevation of Privilege	Sufficient Processing Capac
NAS confidentiality protection	If security-mode complete message is not confidentiality protected, the AMF cannot confirm that the SMC is executed correctly. This can result in waste of system resources and deny a legitimate user access to the system.	Tampering of Data, Information Disclosure, Denial of Service	Sufficient Processing Capacity
Bidding down on Xn-Handover	If AMF cannot verify that the 5G security capabilities received from source g-NodeB (gNB) via the target gNB are the same as the UE security capabilities that the AMF has stored, the source gNB may force the system to accept a weaker security algorithm than should be allowed, thus forcing the system into lower-security level making the system easily attacked and/or compromised.	Tampering of Data, Information Disclosure	User account data and credentials
NAS integrity protection algorithm selection in AMF change	If the highest priority NAS integrity protection is not selected by the new AMF within AMF change, the new AMF could then use a weaker algorithm forcing the system into a lowered security level making thee system easily attacked and/or compromised.	Tampering of Data, Information Disclosure	User account data and credential
Threats related to release of non-emergency bearer	If authentication fails in the AMF and the non-emergency bearer is not released, the UE can continue receiving unauthorized call, wasting valuable system resources.	Denial of Service	Sufficient Processing Capacity
Invalid or unacceptable UE security capabilities	A flawed AMF implementation accepting insecure or invalid UE security capabilities may put User Plane and Control Plane traffic at risk, without the operator being aware. If	Tampering of Data, Information Disclosure	User account data and credentials, Mobility

	NULL ciphering algorithm and/or NULL integrity protection algorithm of the UE security capabilities is accepted by the AMF, all the subsequent NAS, Radio Resource Control (RRC), and user plane messages will not be confidentiality and/or integrity protected. The attacker can easily intercept or tamper control plane data and the user plane data. This can result in information disclosure as well as tampering of data.		Management data
Failure to allocate new 5G-GUTI	If a new 5G-Global Unique Temporary Identifier (GUTI) is not allocated by AMF in certain registration scenarios (i.e. receiving request messages of type: "initial registration", "mobility registration update", Service Request message sent by the UE in response to a Paging message), an attacker could keep on tracking the user using the old 5G-GUTI after these registration procedures.	Information Disclosure	Mobility Management data

MOBILITY MANAGEMENT ENTITY (MME)

Mobility Management Entity is a key control node of the 4G Evolved Pack Core (EPC), as defined by standards and has the following responsibilities:

- Mobility management: Provides the necessary session management for subscriber mobility within the network, as well as support for mobility/handovers between networks. It tracks the current location of all subscribers including the states of their user device, in order to allow calls, Short Message Service (SMS), and other mobile services to be delivered to them.
- Authentication and security: Support user access authentication with Home Subscriber Server (HSS) and Internet Protocol (IP) packet filtering functionality and prevent unwanted access and fraud attempts towards the network.

Current vulnerability as per National Institute of Standards and Technology (NIST) [32] is the insufficient input validation of the Stream Control Transmission Protocol (SCTP) traffic, which poses a threat as a remote attacker can create a DoS condition on an evolved Node B (eNodeB) that is connected to the compromised device. An attacker could further exploit this vulnerability by leveraging a man-in-the-middle position between the eNodeB and the MME and then sending a crafted SCTP message to the MME. If successful, this exploit would in turn cause the MME to stop sending SCTP messages to the eNodeB, triggering a DoS condition.

4.1.2.2 SOLUTIONS AND MITIGATIONS FOR MME AND AMF SECURITY

Distributed Denial of Service (DDoS) attacks are the most commonly used "cyber-weapons" for disrupting the proper functioning of victims, and are usually launched using a huge number of distributed, remotely, and

controlled devices organized into botnets. The objective is to target computing resources, including computer systems, network devices, servers, and web applications, by sending huge traffic to overwhelm these systems and cause a temporary interrupt or a suspension of their services. The main well-known DDoS attacks are DNS request flood, Internet Control Message Protocol (ICMP) request flood, Session Initiation Protocol (SIP) request flood, User Datagram Protocol (UDP) flood, Hypertext Transfer Protocol (HTTP) flood, Transmission Control Protocol (TCP) SYN flood.

It is well established that 5G organizes the supported applications into three network slice types. The first type is the eMBB (enhanced Mobile BroadBand) slice, which is basically an extension of the 4G mobile broadband service seeking higher bandwidth and data rate. The second is the URLLC (Ultra-Reliable Low Latency Communications), which provides low-latency and reliable communication. The third type is the mMTC (massive Machine Type Communications), which supports massive IoT devices with narrow bandwidth requirements.

Services belonging to mMTC rely on interconnected things and devices, which communicate automatically without any human intervention. Due to the massive number of deployed devices per mMTC service, DDoS attacks are more and more using mMTC devices [33] and now considered as one of the main sources of the propagation of DDoS attacks. Indeed, the massive number of connected devices (more than a million per km^2) makes it easier for attackers to launch high traffic using multiple botnets. Accordingly, the mobile core's attack surface is significantly larger than it used to be, and the proposed approaches to security are no longer adequate. Previously, DDoS targeted hosts on the internet, but, nowadays, they have started attacking Core Network components of 4G and 5G.

Classically, DDoS attacks are mitigated, especially in the phase of anomaly detection, using ML algorithms: such as Naive Bayes, Neural networks, Support Vector Machine, Decision Tree, K-Nearest Neighbor. In [34], a system called DeepDefense based on Deep Learning has been introduced. DeepDefense filters network traffic using rules and stores detected attacks in a database. DeepDefense filters each packet of real network traffic and classifies it either as a DDoS attack or a legitimate one. DeepDefense reacts to a DDoS attack by dropping packets tagged as DDoS. Another solution, namely Anti-DDoS Technique, has been proposed in [35]. It relies on self-learning Bloom Filter, which is a data structure designed to identify whether an element is present in a set rapidly. It has been used to identify DDoS attacks using (1) the advantage of ML to detect attacks; (2) the threat mitigation based on Bloom filters. Authors in [36] suggest implementing Bloom filter in the routers to block the packets with similar information, such as destination ports and addresses.

All the previous solutions are limited by centralized data collectors and actors to identify and mitigate the DDoS attacks. However, in real situations, the DDoS is a distributed threat as attackers launch distributed botnets from different network locations. A cooperative attack detection based on a hierarchical RL was proposed in [37] to identify the network attacks. The attack detection is performed using a distributed detection system executed at different 5G key network components, such as base stations. The advantage of using RL is the ability to detect new misbehaviour and attacks, as RL is an online learning algorithm.

The work introduced in [37] proposes to deploy distributed IDS (Intrusion Detection System) agents to monitor and protect wireless communication of 5G networks. The IDS agents are of two types: First Level (FL)-IDS and Second Level (SL)-IDS. The FL-IDS is deployed at each access point and uses a one-class SVM algorithm for anomaly detection. If an anomaly is detected, FL-IDS forwards an alert to SL-IDS for further verification, including the identity (id) of the suspected user equipment (UE) as well as the related suspected features such as packets sending rate and duration of the communication. If SL-IDS detects an attack, it

forwards a report to the Security Operation Center (SOC) for further investigation. The report sent by SL-IDS includes the infected target's identity, such as user equipment, base station, or servers of Centralized-RAN. SoC relies on a set of techniques to detect and predict the new attack patterns, where a human (a security expert) is involved in the decision making to reduce the false-positive rate. Although this solution uses a distributed monitor, it is partially automated as a security center with human intervention is needed.

In [38], a novel solution is proposed to mitigate DoS/DDoS attacks using smart contracts and AI in 5G. The proposed solution offers an embedded AI module into smart contracts. The latter was used to ensure the efficiency and trustworthiness of AI training and its execution, hence eliminating the possibility for any other parties to insert backdoors into the AI module. The proposed solution can limit DoS/DDoS attacks by amplifying the cost and forcing rational users not to launch DoS/DDoS attacks, which can avoid them before they occur. Also, a distributed infrastructure of the blockchain was used to prevent attackers from evading smart contracts auditing.

Usually, mMTC traffic is of two types. The first one is the periodic update (PU) type, associated with low-rate non-real-time devices activity, which regularly transmits data to a central entity. The second type is Event-driven. In this type, MTC devices transmit data following an event triggered either by the device itself or by a remote server. To achieve DDoS attacks when mMTC slices are running, attackers aim to take control of an important number of devices connected, using event-driven-based traffic, with a long sleep period [39]. A detection algorithm was proposed in [39] using the Markov chain recurrence properties to identify DDoS attacks relaying on mMTC devices. Indeed, the recurrence time of mMTC devices is either in ON or the OFF state. ON state means that a device is in a transmission mode, while OFF state corresponds to the mode of sleep (or idle). When a DDoS attack is happening, it forces the mMTC devices to send extra signalling traffic; hence the recurrence time of the active state (ON) will increase. At the same time, the idle state will experience a decreased recurrence time during the attack. In order to identify the DDoS attacks, the number of visits related to the active Markov state is continuously monitored and compared to a given threshold chosen and accommodated according to the characteristic parameters of the 3GPP MTC traffic model [40].

4.1.3 FORMAL METHOD THREAT MODELING

In this section we summarize the outcome of applying the threat modeling methodology of section 2.2.3 for the use case of interest.

4.1.3.1 SYSTEM OVERVIEW

The diagram of Figure 8 provides a high-level overview of the system and target of evaluation (TOE). For simplicity, we have only included components of 4G or 5G networks that directly or indirectly participate to the attack scenario, as well as components of MonB5G involved with the attack mitigation solution.

The diagram also discriminates between:

- components that may be affected (assets, in yellow);
- components not on the security critical path (in blue);
- MonBG entities introduced for detection and response (in green); and
- entities external to, or not in control of, the TOE (in grey).

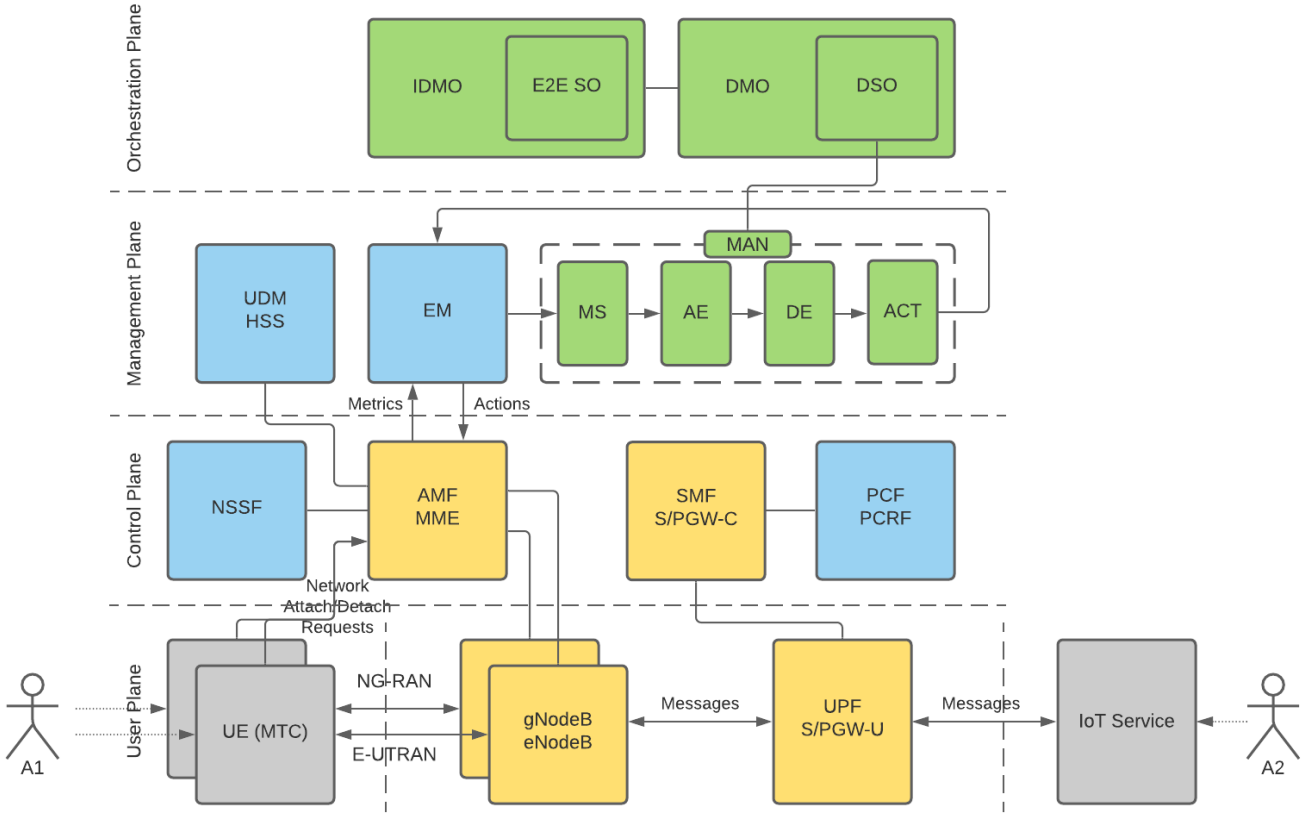

Figure 8. System Diagram of mMTC Use Case

4.1.3.2 SCOPE

Aligned with the use case of interest, the threat model herein mainly focuses on threats against the Availability properties of the TOE. To avoid repetition, the following are not included in the scope of the presented threat model:

- General threats against network slicing, outlined in section 4.1.2 and the literature referenced therein
- Threats against AMF and MME, already covered earlier in sections 4.1.2.1 and 4.1.2.2 of this deliverable

4.1.3.3 COMPONENTS

Table 3 details the different network and MonB5G components.

Table 3. Components

ID	Classification	Layer	Description
UE (MTC)	External	User Plane	User Equipment, devices with a mobile terminal attached to the 4G or 5G network, in this case of MTC/IoT variety
gNodeB/eNodeB	Asset	User Plane	4G/LTE or 5G base stations

UPF / S/PGW-U	Asset	User Plane	5G User Plane Function node on the data path, or the equivalent for 4G/LTE (Serving Gateway User plane function (SGW-U) & Packet Data Network Gateway (PGW-U))
IoT Service	External	Internet	Internet Service that remotely controls and receives messages from MTC/IoT devices
NSSF	Component	Control Plane	Network Slice Selection Function (NSSF), leveraged by AMF to select the network slice instance(s) that the devices attach to
AMF / MME	Asset	Control Plane	5G Access and Mobility Management Function, or the equivalent 4G/LTE Mobility Management Entity
SMF / S/PGW/C	Asset	Control Plane	5G Session Management Function (SMF), or the equivalent for 4G/LTE (Serving Gateway Control plane function (SGW-C) & PGW-C)
PCF / PCRF	Component	Control Plane	5G Policy Control Function (PCF), or the equivalent for 4G/LTE Policy and Charging Rules Function (PCRF)
UDM / HSS	Component	Management Plane	5G Unified Data Management function (UDM), specifically the subset that maps to the 4G/LTE Home Subscriber Server database
EM	Component	Management Plane	Element Manager for AMF / MME
MAN	MonB5G	Management Plane	Manager for the MonB5G MS / AE / DE / ACT components
MS	MonB5G	Management Plane	An instantiation of the MonB5G Monitoring System component
AE	MonB5G	Management Plane	An instantiation of the MonB5G Analytics Engine component
DE	MonB5G	Management Plane	An instantiation of the MonB5G Decision Engine component
ACT	MonB5G	Management Plane	An instantiation of the MonB5G Actuation component
DMO / DSO	MonB5G	Orchestration	Domain Security Orchestrator component of MonB5G Domain Manager and Orchestrator
IDMO / E2E SO	MonB5G	Orchestration	E2E Security Orchestrator component of MonB5G Inter-domain Manager and Orchestrator

4.1.3.4 ASSETS

Table 4 includes the vulnerabilities per component.

Table 4. Assets

ID	Component	Layer	Vulnerabilities
C1	AMF / MME	Control Plane	To conserve battery power, MTC devices will frequently detach and re-attach to the mobile network. Relevant requests by base stations are handled by the AMF / MME, which can be overwhelmed by the high request rate, when large numbers of devices perform this in synchrony.
C2	gNodeB / eNodeB	User Plane	Base stations are vulnerable to performance (throughput/latency) degradation, when large numbers of mobile terminals excessively utilize resources. Proportional-fair sharing algorithms have their limits in addressing this. In the case of mMTC, these limits do not relate to high per-UE throughput demands, but to an enormous number of terminals that compete for base station frequency or time-domain resources, causing them to fail in achieving low latency in message transmissions.
C3	UPF / S/PGW-U	User Plane	Compared to base stations, these entities on the data path between the mobile network and the Internet are considered less vulnerable to resource utilization pressure, at least when it has to do with MTC devices that typically have low throughput needs. However, given that they have to handle the aggregation of messages from potentially millions of devices, in a distributed denial of service scenario they will have to scale to handle huge spikes in packets per second rates.
C4	SMF / S/PGW/C	Control Plane	Reflecting on the potential resource pressure on the corresponding data plane components, the control plane counterparts have been included as a TOE asset. However, they are less vulnerable to availability threats in MTC case, since they are involved only on a per session basis, not on a per packet basis, as the above.

4.1.3.5 ACTORS

Table 5 displays the different actors and their role.

Table 5. Actors

ID	Role
A1	The actor identifies a security flaw of the UE (MTC) hardware/firmware/software, or manages to inject such a firmware/software vulnerability, by participating to the software supply chain and exploiting the regular updates these devices tend to receive. The actor then exploits the security flaw to establish a command & control channel that manipulate the network communication behaviour of these devices.
A2	The actor identifies a security flaw in the IoT Service that remotely manages the UE (MTC) devices. The actor then exploits this security flaw to gain control of the network communication patterns of these devices, for example by controlling the message triggering frequency and synchronization between them.

4.1.3.6 ENTRY POINTS

Table 6 shows the entry point of the system.

Table 6. Entry points

ID	Components	Protocol	Description
E1	UE (MTC) - gNodeB/eNodeB	Next Generation Radio Access technology Network (NG-RAN)/ E-UTRAN (LTE Category protocol (LTE Cat), Long-Term Evolution for Machines (MTC) (LTE-M), Narrowband IoT (NB-IoT), …)	Network attachment and message transmission interface between the UE (MTC) and the system
E2	UPF/PGW-U - IoT Service	IP / Application Layer (HTTP, Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), …)	Connection-less or connection-oriented IP-based E2E transport between UE (MTC) and IoT Service

4.1.3.7 BOUNDARIES

The diagram of Figure 8 depicts some of the security and trust boundaries of the system. If we exclude the boundaries that correspond to the entry points above, there are additional boundaries, such as between: i) the (user plane, control plane, etc.) layers of the system, ii) the instances of the components provisioned for different network slices and iii) the (RAN, Edge, CN, etc.) technological domains that a network slice spans. Given the broad range of these boundaries and the differences in implementation between 4G & 5G ("legacy" vs service-based architecture), we will not be extensively listing and analysing them in this threat model.

4.1.3.8 THREATS AND MITIGATIONS

Table 7 summarizes the threats and litigation of mMTC use case.

Table 7. Threats and Mitigations of mMTC Use Case

ID	Attacker	Entry Point	Asset	Type	Threat	Likeli-hood	Impact	Risk	Mitigation
T1	A1, A2	E1, E2	C1	Denial of Service	An attacker exploits security flaws of UE (MTC) devices or IoT Service to cause excessive distributed and synchronized network attach and detach requests that degrade the performance and affect the availability of AMF / MME.	M	H	H	See section 4.1.4

T2	A1, A2	E1, E2	C2	Denial of Service	In a scenario similar to the above, base stations can be led to resource starvation, deteriorating their latency and affecting their ability to serve other mobile terminals.	M	M	M	Indirectly by the same mitigation as T1
T3	A1, A2	E1, E2	C3	Denial of Service	In a scenario similar to the above, when it is distributed to a large number of devices, disproportionate capacity of assets can be occupied by having to process enormous packets/s rates from devices.	L	L	L	Indirectly by the same mitigation as T1
T4	A1, A2	E1, E2	C4	Denial of Service	In a scenario similar to the above, when it is distributed to a large number of devices, the number of concurrent packet data sessions assets will have to handle will spike.	L	L	L	Indirectly by the same mitigation as T1

4.1.4 MITIGATION USING MONB5G AI-DRIVEN SECURITY TECHNIQUES

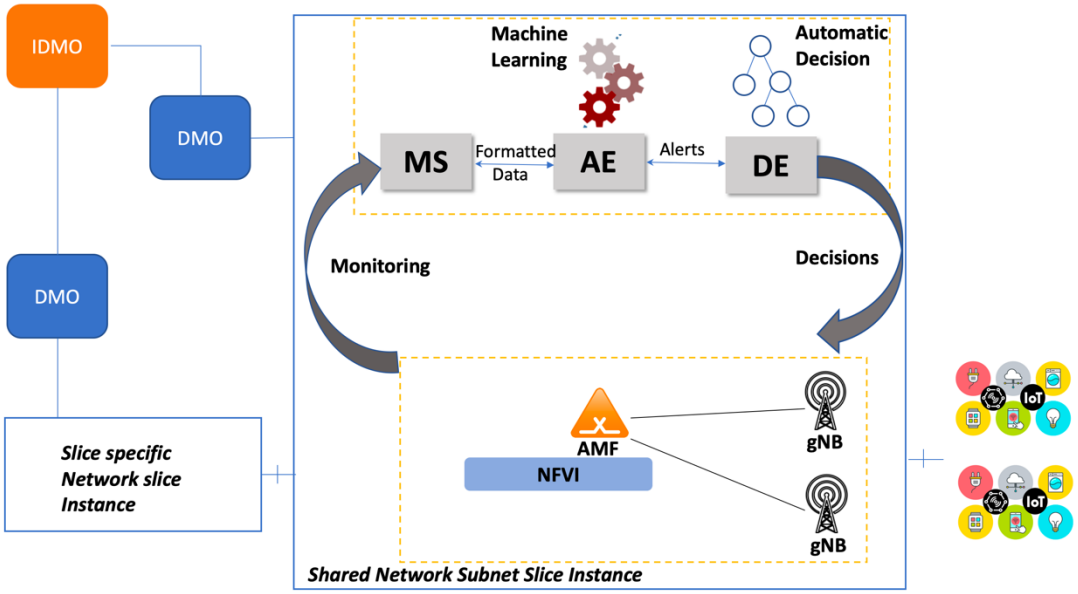

Figure 9. In-Slice attacks detection using MonB5G system

Figure 9 illustrates a simplified view of the envisioned system architecture representing the MonB5G elements and their interaction with the network components running a mMTC network slice. In this scenario, we assume a mMTC network slice deploying a high number of devices connected through different eNB/gNB.

The mMTC network slice is composed of a dedicated network slice instance running the network slice owner applications and a shared network slice subnet instance managed by the infrastructure owner. The shared network subnet instance is composed of eNB/gNB and the core network running on top of a virtualized infrastructure. The eNB/gNBs are considered as shared PNF, while the core network elements are VNFs shared among the run network slices. MS/AE/DE role is to detect in-slice DDoS attacks and mitigate these attacks. According to the security architecture shown in Figure 4, MS/AE/DE correspond to the SECaaS, but they are permanent and not instantiated on demand. They are configured and handled by the infrastructure manager. They ensure zero touch management for the shared network instance. After each enforced decision, SECaaS informs the DMO. The DMO in this case covers the CN and RAN domain or only the CN domain that is run as VNF. In both cases, it is owned, managed, and controlled by the infrastructure owner.

It is important to recall that the MS role is to monitor the key elements to detect the attack, AE includes ML models to detect an attack, and DE mitigates the attacks and enforces decisions. Now we will detail the role of each element in the system.

MS:

In the case of the considered scenario, we assume that the MTC devices are controlled by an attacker that launches DDoS attacks on the MME/AMF element of the core network. As the objective is to overload the MME/AMF, an attacker should continuously generate a high number of attach and detach requests. Indeed, the MME/AMF needs to handle each request separately. Each request will generate several control plane messages; if the number of requests is very high, the MME/AMF may be overloaded, and the provided service is disturbed. Therefore, the number of attach and detach requests should be continuously monitored and collected by the MS. These metrics are considered service-level metrics and need to be extracted from the MME/AMF. Usually, a service-level metric should be provided by the managed element (here MME/AMF) through the Element Manager (EM). To do so, the EM exposes an API, to request the metric via HTTP request/response, or subscribe to the event if a communication bus is used.

AE:

In order to detect attacks in a mMTC network slice it is important to understand how the MTC devices communicate and generate traffic. MTC devices are generating traffic using a specific pattern according to the type of used application. We can distinguish between three cases:

1. Event-based, where the MTC devices connect if an event happen (like fire-detection, earthquake, etc.). They connect (attach to the network) and send a small amount of traffic (few packets);
2. Trigger-based, where a remote server trigger a connection to the device to gather data (measure of temperature, or humidity, etc.);
3. Periodic, where the MTC devices connect periodically to send data (temperature, humidity, etc.).

While type two and three can be easily predicted using information from the slice owner, type 1 is very difficult to predict. 3GPP in [41] introduces two traffic models to characterize type 3, namely based on Beta distribution (3,4) and Uniform distribution (0,1).

- Model 1: Uniform distribution over a duration T in which MTC devices access the network uniformly over a period of time, i.e., in a non-synchronized manner. This model does not take account of the correlation between the transmissions of the devices.
- Model 2: Beta distribution over T in which a large amount of MTC devices access the network in a

highly synchronized manner. This model generates correlated traffic in a specific time interval.

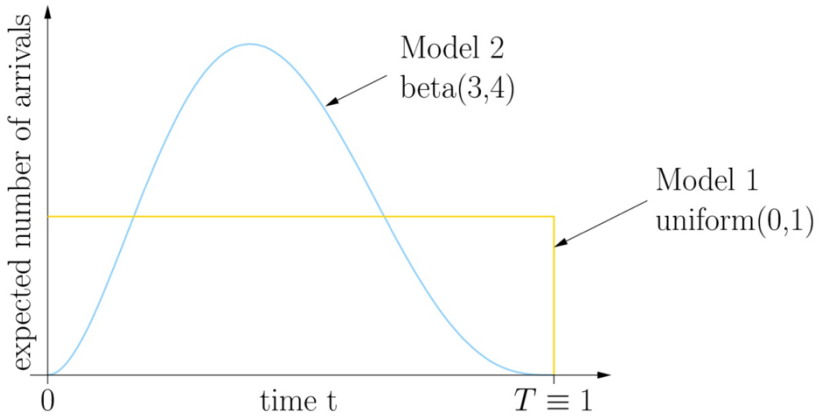

Figure 10. MTC traffic model [42]

Table 8. Parameters of the 3GPP model

Characteristics	Model 1	Model 2
Number of device N	1000, 3000, 5000, 10000, 30000	
Distribution *f(t)* over *[0,1]*	unifrom	beta(3,4)
Period *T*	60s	10s

Figure 10 and Table 8 illustrate and detail the 3GPP traffic model, respectively.

Knowing that the MTC traffic is well specified, different options can be considered when defining the attack detection algorithm to be run by AE. Obviously, using a trained Neuronal Network is one of the solutions. The Neural Network (NN) (Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), or an association of both) can be trained using the normal traffic generated by MTC devices belonging to mMTC slice. Either by using synthetic data generated using one of the models specified by 3GPP or real-traces. Then, the trained algorithm can run as an IDS by analyzing the attach requests monitored by MS and classifying the traffic as normal or abnormal. If the traffic is abnormal, AE notifies DE by including the International Mobile Subscriber Identity (IMSI) or GUTI suspected as belonging to the attacks.

DE:

The DE algorithm considers the alerts sent by the AE to mitigate the attacks. Before applying the appropriate decision, the DE algorithm may apply filters such as Kalman Filter to reduce the probability of false positives. Regarding the decision enforcement, DE can request the MME/AMF to detach the concerned IMSI or GUTI involved in the DDoS attacks and communicated by the AE. It should be noted that the GUTI is assigned by the MME/AMF to a UE at the first attach to avoid sending the IMSI each time a UE initiates an attach request.

In addition, the MME may ban the concerned IMSI (and GUTI) in the HSS database. In order to enforce these decisions, DE communicates with MME/AMF by using the API exposed by EM of the latter.

Involved technologies:

Table 9 summarizes the different that can be used to validate the components described in this use-case scenario.

Table 9. Technological tools

Element	Technology
MME/AMF	OpenAirInterface (OAI)
Traffic generator	Magma OAI
EM MME/AMF	To be implemented on OAI
MS/AE/DE	To be implemented

Validation of the MonB5G:

In order to validate the effectiveness of using the MonB5G system to detect in-slice attacks in the case of mMTC, we will collect KPI. They cover two categories. The first one includes KPIs related to the performance of the system to detect quickly in-slice DDoS attacks and mitigate the attacks. Here we can mention the following KPI:

- The time taken from the start of the attack/anomaly until its detection by the MonB5G system. This KPI will be compared to a vanilla solution that might be relying on existing IDS, such Snort
- The time taken from the start of the attack/anomaly until it detections. This KPI will be compared to a vanilla solution that might be relying on existing IDS, such Snort.

The second category covers the KPIs concerning the ML algorithm used by AE. We can mention:

- False positive rate in attack classification (percentage of false classification of events as attacks). The MonB5G system will be compared to a vanilla solution based on IDS, such as Snort.
- Learning robustness that covers precision, recall (true positive rate), fall-out (false positive rate), Area Under Curve values above/below specific thresholds. Again the MonB5G system will be compared to a vanilla solution based on IDS.

4.2 Traffic steering and Security VNF instantiation

4.2.1 INTRODUCTION

To protect network slices against cyber security attacks, it is highly important to follow useful guidelines for managing the security life cycle from international bodies such as ENISA or NIST or another government security agency. These guidelines lead to a convergent approach to building cyber security capabilities, which is divided in several stages: Preparation, Reaction, Improvement. The initial phase, the Preparation focuses on capturing the customer's security needs and understanding the network slice structure to identify the

assets to be protected. It then assesses the vulnerabilities, threats and risks associated with these assets and prepares and implements appropriate protection measures. The Reaction phase starts with a cyber security incident that is occurring or has occurred, the containment must be then carried out to limit the spread of the attack and its impact, following by the eradication of the cause of the incident. The recovery of the system to normal functioning completes this second stage. In the last stage, the Improvement, deeper investigation is conducted to identify emerging vulnerabilities, threats and risks, lessons learned from the incident response contribute to improving the defence in place.

Thanks to the security intelligence collected, future network slices will be better prepared with a higher level of protection. Security operations in all three phases may require directing dynamically suspicious traffic through existing security controls or update the network slice with supplementary VNFs providing the missing security features. For instance, threat intelligence has identified an emerging vulnerability for a device that requires the deployment of a new security function to detect if the device is under attack. Another case is when an indicator has been raised to signal an unusual traffic is being sent by a server, the incident response needs then to redirect the flow to an inspection function to confirm it is actually an incident. Dynamic traffic steering is a major feature of SFC framework [43] thanks to the concepts of Service Function Forwarder (SFF) which allows the application of a sequence of network functions to a particular traffic.

During the preparation phase, the SO are not deploying security controls to prevent all the threats as some of them have low occurrence likelihood or their potential impact are limited. SO relies instead on the Reaction to mitigate the residual risks and instantiate dynamically the needed security enablers.

The NFV-MANO is complement to the SFC, as it manages the lifecycle of VNFs including the security enablers that compose the service function paths (SFP). Indeed, through the interfaces offered by the NFV orchestrator, virtualized security functions (VSF) are deployed on demand, their capacity adjusted according to the actual load. In addition, the NFV orchestrator places optimally VSF instances in the infrastructure according to the criteria, and it terminate them when no longer needed to save costs.

Through scenario aLTEr attack, which will be described in the next section, we will show the interactions between the components of MonB5G, the SFC and the NFV MANO how the security life cycle is realized.

4.2.2 STATE OF THE ART ON EXISTING ATTACK AND SOLUTIONS

4.2.2.1 VNF INSTANTIATION

VNF Instantiation is the process of deploying an instance of a VNF through an NFV platform, and having it ready for handling traffic. The instantiation process includes two steps; provisioning the needed virtual resources, and configuring the templates bundled in the same VNF.

VNFs may have inherent software or system vulnerabilities, or malware designed to perform attacks, therefore they could either be the source or the target of a threat or attack. Attacks from within VNF are possible due to software vulnerability flaws, where a malicious attacker could exploit a flaw (using snort[1] for example) to bypass firewall restrictions or take advantage of a buffer overflow to execute a malicious code.

[1] https://www.snort.org/

Furthermore, VNFs have virtualization vulnerabilities, according to ENISA's threat Landscape [44]:

1. Network Virtualisation Bypassing
   The improper configuration along with bad network slicing implementation can result in loss of data which can harm both confidentiality and privacy. As the networks are shared between different users, it should be assured that only legitimate traffic enters or leaves a network slice. Unless traffic is isolated, slice trespassing will happen.

2. Abuse on data Centers Interconnect (DCI) protocol
   Whatever system relies on virtualisation is usually deployed within data centers, thus inheriting their threats and vulnerabilities. This threat refers to the lack of authentication and encryption. Under those circumstances, potential attackers can create spoofed traffic in a way that it makes possible traversing DCI links or creating a DoS attack of DCI connections.

3. Virtualised Host Abuse
   In a virtualised environment, physical resources are shared between the different applications and their users running on virtualised host. Thus there is a vulnerability that some of those users want to overcome the boundaries and the limitations of their virtualised space, invading the neighbouring spaces, scavenging information. This threat permits cross-inspection of various tenant's data flow, neighbouring attacks which allow the mapping of topology, thus serving as the initial step for DoS attack.
4. Abuse of Cloud Computational Resources
   In NFV networks, as the compute nodes are outside of the core, it requires the operators to loosen the security rules between the controller and the compute nodes. This slackening of the security can open up the whole environment to a malicious attacker and thus compromise it, leading to data loss, breaches, and loss of service.

Additionally, ETSI's GS [45] suggests that VNFs' lack management authentication is a prime vulnerability, and that is should be addressed. The report includes the specifications and the requirements for the aforementioned problem. Management authentication is essential for any real-world deployment and affects every phase of the VNF lifecycle. The existence of an authentication API that can allow only authorised users to get access and manage to operate the VNF, will mitigate this vulnerability.

As evident that most of VNF related vulnerabilities lead to DoS disruption, we refer to a detailed survey [46] of SDN-based DDoS attack detection and mitigation solutions aggregated DDoS (flooding) attacks into the three categories by the authors:

i. Reflection-based Attacks

These are reflection-based volumetric attacks where the attacker overwhelms the target network by injecting a large number of ICMP packets. Two infamous examples of this type of attacks are the Smurf[1] and Fraggle[2] attacks.

ii. Protocol Exploitation Attacks

Where attackers can exploit the synchronize (SYN) protocol and send large UDP packets to consume more bandwidth. Examples are the SYN flooding and UDP fragmentation attacks.

iii. Amplification-based Attacks

Where attackers are able to generate large volume of DNS and Network Time Protocol (NTP) requests to jam their servers, rendering the target and surrounding infrastructure inaccessible to regular traffic.

4.2.2.2 SOLUTIONS AND MITIGATIONS

A recent report [47] describes a novel mitigation experiment that was performed under the **EU H2020 SoftFIRE project**[3]. The solution designed is called **BotsOnFire**, and within its report the authors specify the implementation of two Virtual Network Functions (VNF) and an SDN application, and their testing as SDN/NFV applications.

Their 3-tier solution is described as follows:

I. Botnet detection:

A Snort Deep Packet Inspection (DPI) VNF is deployed for detecting botnets at low level. Snort is one of the most widely used Network Intrusion Detection Systems (NIDS) for misuse detection, which is 5G compliant due to its ability to analyze GPRS Tunneling Protocol (GTP) packets natively without having to de-capsulate them first.

II. Botnet mitigation.

A Honeynet[4] VNF is created for emulating malicious behaviors of compromised user equipment (UE). The Honeynet is a security component chosen to the isolate bots in the compromised UEs by emulating their behavior, thus preventing real bots from executing attacks. This mechanism has been because honeynets can be used to continuously analyze how botnets evolve over time and advise the monitoring and detection modules to adapt their internal processes to the changes observed.

III. Enabling detection and mitigation procedures in SDN

An SDN application (called FlowT) has also been implemented to enable security functions of the Snort and Honeynet VNFs. Effectively mirroring suspicious flows to the Snort VNF for inspection and diverting network flows exchanged between bots and the server for botnet emulation by the Honeynet VNF. FlowT enables

[1] https://www.sciencedirect.com/topics/computer-science/smurf-attack

[2] https://www.radware.com/security/ddos-knowledge-center/ddospedia/fraggle-attack/

[3] https://www.softfire.eu/

[4] https://www.honeynet.org/

both features selectively applying network flow mirroring and diversion rules to the virtual switches (vSwitches) being managed by the SDN Controller.

4.2.3 FORMAL METHOD THREAT MODELING

In this section we summarize the outcome of applying the threat modeling methodology of section 2.2.3 for the use case of interest.

4.2.3.1 SYSTEM OVERVIEW

The diagram of Figure 11 provides a high-level overview of the system and target of evaluation (TOE). For simplicity, we have only included components of the network that directly or indirectly participate to the attack scenario, as well as components of MonB5G involved with the attack mitigation solution.

The diagram also discriminates between:

- Components that may be affected (assets, in yellow);
- Components not on the security critical path (in blue);
- MonBG entities introduced for detection and response (in green); and
- Entities external to, or not in control of, the TOE (in grey).

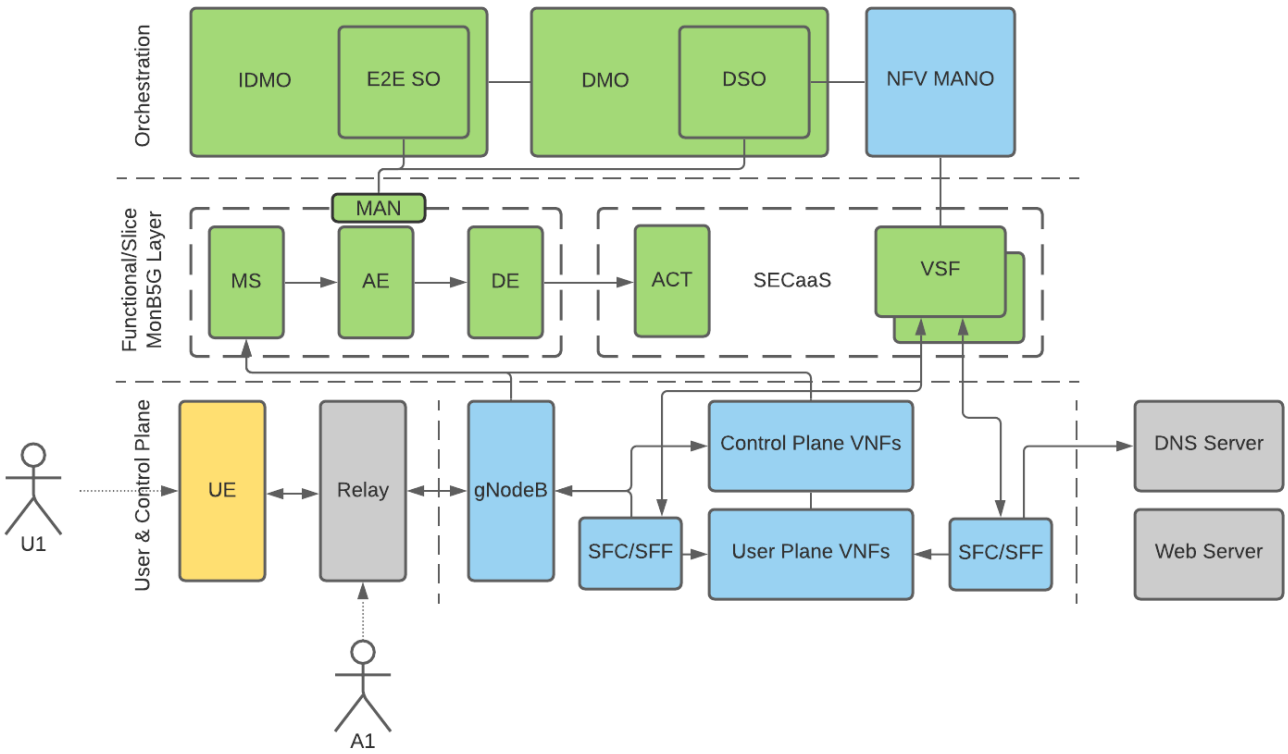

Figure 11. System Diagram of aLTEr Use Case

4.2.3.2 SCOPE

Aligned with the use case of interest, the threat model herein mainly focuses on threats against the confidentiality properties of the UE.

4.2.3.3 COMPONENTS

Table 10 details the different network and MonB5G components.

Table 10. Components

ID	Classification	Layer	Description
UE	Asset	User Plane	User Equipment with a mobile terminal attached to the network
Relay	External	User Plane	Unlawfully intercepts and tampers with data communications
gNodeB	Component	User Plane	Network base station
SFC/SFF	Component	User Plane	Service Function Classifier and Forwarder, offloads processing of data flows to a chain of network functions
User Plane VNFs	Component	User Plane	Virtual Network Functions on the data path
Control Plane VNFs	Component	Control Plane	Virtual Network Functions on the control plane
DNS Server	External	Internet	Domain Name Server under control of A1
Web Server	External	Internet	Web Server under control of A1
MAN	MonB5G	Functional / Slice Layer	Manager for the MonB5G MS / AE / DE / ACT components
MS	MonB5G	Functional / Slice Layer	Instantiations of the MonB5G Monitoring System component
AE	MonB5G	Functional / Slice Layer	Instantiations of the MonB5G Analytics Engine component
DE	MonB5G	Functional / Slice Layer	Instantiations of the MonB5G Decision Engine component
ACT	MonB5G	Functional / Slice Layer	Instantiations of the MonB5G Actuation component
SECaaS / VSF	MonB5G	Functional / Slice Layer	Virtual Security Function instantiated by MonB5G SECaaS
NFV / MANO	Component	Orchestration	Management and Orchestration stack that orchestrates VNFs
DMO / DSO	MonB5G	Orchestration	Domain Security Orchestrator component of MonB5G Domain Manager and Orchestrator
IDMO / E2E SO	MonB5G	Orchestration	E2E Security Orchestrator component of MonB5G Inter-domain Manager and Orchestrator

4.2.3.4 ASSETS

Table 11 includes the vulnerabilities per component.

Table 11. Assets

ID	Component	Layer	Vulnerabilities
C1	UE	User Plane	Communications between UE and base stations are wireless and take place over public frequency bands. These communications can be intercepted and relayed by an appliance that masquerades as a base station. Even though the E-UTRAN protocols have reasonable provisions for encrypting these communications and UE enforces them, standard data integrity checks at the Packet Data Unit (PDU) and IP level aim at detecting packet transmission errors, rather than protecting from tampering.

4.2.3.5 ACTORS

Table 12 displays the different actors and their role.

Table 12. Actors

ID	Role
U1	The actor (victim) normally uses a device (smartphone, tablet, laptop equipped with a mobile terminal) to connect to Internet web sites and services via the operator's mobile network.
A1	The actor (attacker) deploys a Relay that intercepts and relays transmissions between U1's device and the operator's mobile network. The Relay also has functions to tamper with these transmissions at layer 2. Finally, the actor has control of a DNS Server and optionally a Web Server on the Internet.

4.2.3.6 ENTRY POINTS

Table 13 shows the entry point of the system.

Table 13. Entry points

ID	Components	Protocol	Description
E1	UE - gNodeB	E-UTRAN	Network attachment and packet data communications interface between the UE and the system

4.2.3.7 BOUNDARIES

The diagram of Figure 11 depicts some of the security and trust boundaries of the system. If we exclude the boundary that corresponds to the entry point above, there are additional boundaries, such as between: i) the (user plane, control plane, etc.) layers of the system, ii) the instances of the components provisioned for different network slices and iii) the (RAN, Edge, CN, etc.) technological domains that a network slice crosses. Given the broad range of these boundaries and the variety of implementations, we will not be extensively listing and analysing them in this threat model.

4.2.3.8 THREATS AND MITIGATIONS

Table 14 summarizes the threats and litigation of aLTEr use case.

Table 14. Threats and Mitigations of aLTEr Use Case

ID	Attacker	Entry Point	Asset	Type	Threat	Likeli-hood	Impact	Risk	Mitigation
T1	A1	E1	C1	Tampering of Data, Spoofing of IP	A1 deploys Relay on E1 that intercepts communications of U1's device (C1). The Relay identifies DNS requests and replaces encrypted PDU with one that has as destination IP the address of a DNS Server in control of A1.	L	L	L	See section 4.2.4
T2	A1	E1	C1	Information Disclosure	The DNS Server in control of A1 receives DNS requests from U1's device (C1). This reveals which Internet web sites and services U1 visits, violating U1's privacy. A1 can manipulate DNS responses for specific sites to redirect them to a Web Server under their control, to steal credentials or other sensitive information.	L	H	M	Indirectly by the same mitigation as T1

4.2.4 MITIGATION USING MONB5G AI-DRIVEN SECURITY TECHNIQUES

The techniques and complexity of cyber-attacks are constantly evolving and diversifying. In this context, AI can be a great help for security systems to anticipate, detect and stop threats. ML techniques can collect and explore continuously a huge amount of data to learn the updated reports about the security threats in a very short time.

The major limitation of a traditional security system based on expert rules is that it requires a good understanding of the attacker's behaviour and the used techniques and then deploy the needed action to stop it. Meanwhile, the attacks become so fast and the techniques are evolving and can bring great damage in a very short period of time before setting up a defence system. The second limitation of traditional systems is that they cannot be easily scaled with large systems. Future networks will be characterized by a high number of hosted devices which brings additional vulnerabilities that cannot be handled with a traditional approach.

Future security systems should have the capacity to learn faster the attacker's behaviour and take good mitigation actions. The AI techniques can learn from past human decisions to take future actions faster with less error risk. They can also extract more interesting features and non-linear correlations from the collected data that cannot be observable by humans. A technique like deep learning allows going deeper into knowledge to identify the threads from their first signs.

The AI model can assist the security system in different tasks. For example, the first and the most important step is the fast identification of the attack. Classification models based on outlier detection techniques can

be useful to detect new attacks or suspicious behaviours that are not already registered in the database. Time series analysis models offers also multiple efficient techniques to detect the attack patterns in the traffic and stop the suspicious flows. AI techniques can be also useful to make global actions on the network infrastructure to enhance security criteria like isolation to reduce risks, or resilience in the event of an incident by duplication the critical VNFs. This can be seen as an optimization problem, where the objective is to maximize these criteria (isolation, resilience, availability…) with the minimum cost. This task can be very complex, especially when multiple constraints should be considered. Reinforcement Learning techniques showed great potential in solving such problems. The idea is to have an agent that learns to take the appropriate action on the network environment that maximizes the global reward.

- The use case we intend to use to evaluate the effectiveness of the network detection and response system using MonB5G AI security the attack aLTEr [48]. The aLTEr attack is a man-in-the-middle (MITM) attack type and is carried out between the user equipment (UE) and the gNB. It consists of breaking the layer two of the user radio bearer, exploiting the user data integrity protection can be missing as a vulnerability to carry out the attack. In 5G System, it is agreed that the use of user plane protection (Integrity Protection and/or encryption) is optional and it depends on the operator policy as these procedures lead to a higher latency and power consumption. As shown in Figure 12 , the attack comprises two stages, the User Redirection and the DNS Spoofing stages. In the first stage, the attacker in the MITM position on radio bearer intercepts the DNS look up message in the user plane, and replaces the original DNS server IP address by its own instead, the message will be then redirected to the rogue name server. Thus, the attacker has an opportunity to spoof the IP address DNS entries for a target application server by replacing them with the IP address of a server under his control. To conduct the attack, the adversary conducts the following modus operandi:
- Taking advantage of the encryption algorithm is malleable to modify a cipher-text into another ciphertext which will be decrypted as another plaintext. In fact, data confidentiality is based on the use of the ciphering algorithm New radio Encryption Algorithm (NEA) to encrypt plaintext by applying an XOR operation of the plaintext block and the keystream block.
- Recognizing a DNS packet by its small size
- Knowing the original DNS server IP address which is usually well defined by the network operator
- Preserving IP packet checksum

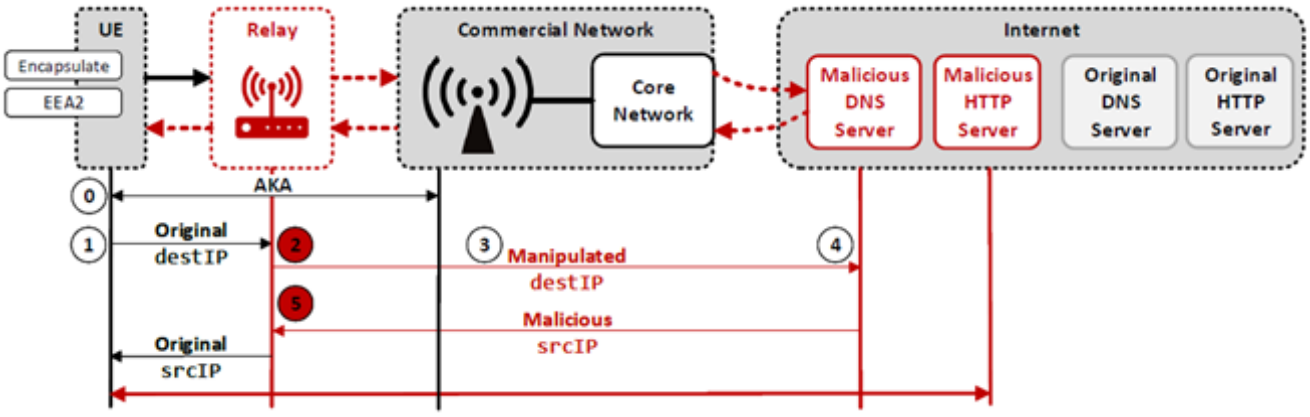

Figure 12. Overview of the DNS redirection attack [48]

The impact of this attack if succeeded is severe as exchanged data and activities are disclosed to the adversary.

This attack cannot be detected at the gNB if the option integrity protection is not enabled, however understanding the techniques used by the adversary to accomplish this attack, we propose a defence solution based on the MonB5G security framework to prevent the attacker from succeeding his planned actions.

Since the attack is invisible at the radio level, we will build a defensive system in the cloud domain to detect and respond to it. At the initial stage, the security orchestrator in the cloud domain captures the security needs from the user and the operator and it dedicates security platform SECaaS if it doesn't exist for the protection of network slice subnets, and one per network slice subnet instance to offer security controls for its VNFs and virtual links.

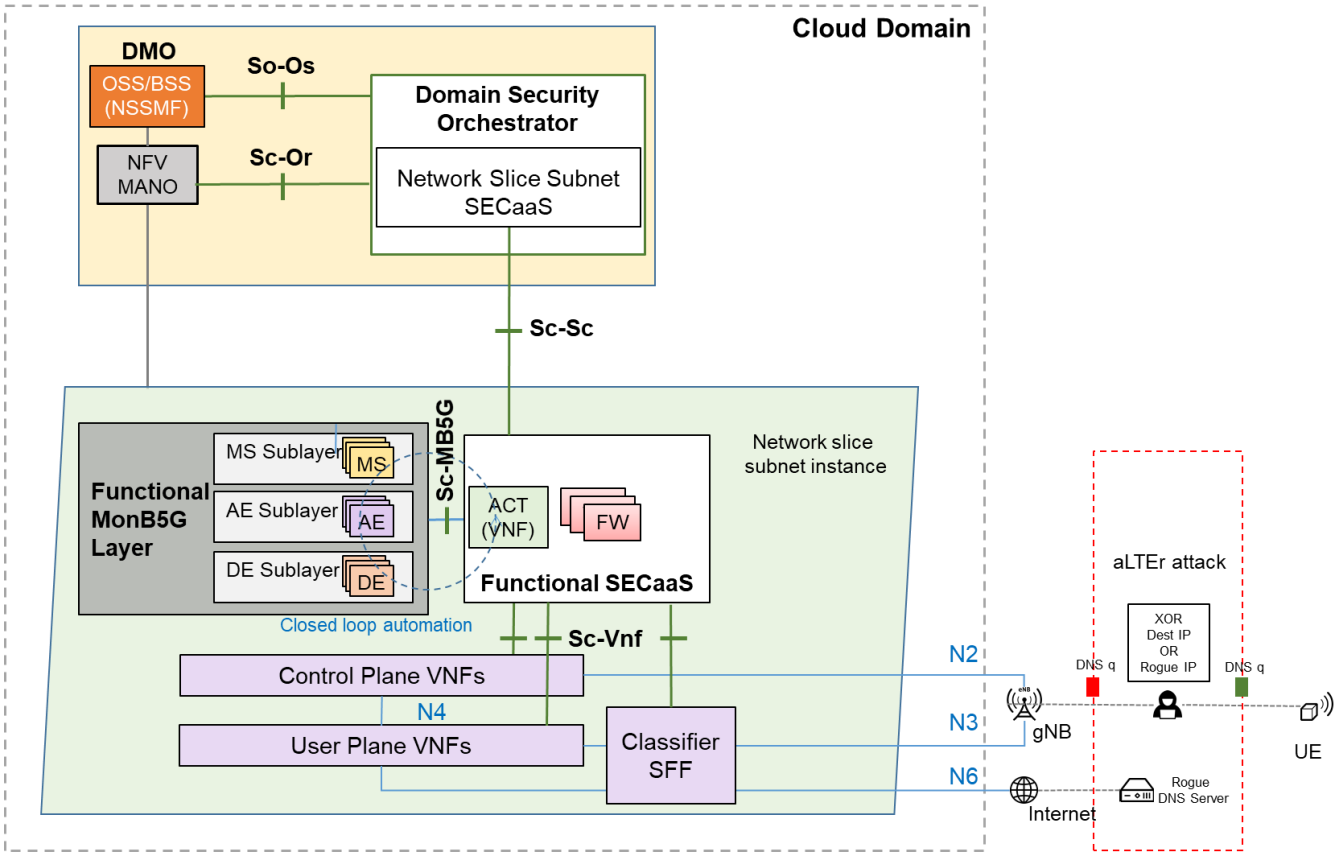

Figure 13. Overview of the MonB5G security framework leveraging MonB5G sublayers to defend a network slice against the aLTEr attack. The network slice subnet SECaaS (NSS-SECaaS) provides security services to the management of network slice subnet instances, while the functional SECaaS (F-SECaaS) dedicates it services to the security for the constituent NFV constructs internal to the network slice instance.

As depicted in Figure 13, the domain security orchestrator leverages on-demand security services (SECaaS) to protect the network slice in all aspects of its lifecycle, from the design phase to the termination of the network slice. The SECaaS at the slice management layer (NS(S)-SECaaS) helps the Network Slice (Subnet)

Management Function (NS(S)MF) collect the security objectives derived from the customer's requirements, the provider's internal policies, and the understanding of the service and network structures. The NSS SECaaS satisfies these objectives by specifying the protection solution to be deployed together with the network slice instance, and the measures of the solution are offered as services by a security platform dedicated to the functional layer, called F-SECaaS.

The F-SECaaS ignores the meaning of network slice, its purpose is to ensure the safeguards of NFV constructs by providing the appropriate security controls. The F-SECaaS uses MonB5G sublayer components such as:

- The MS to perform the network security monitoring that quietly and unobtrusively collects intra-slice IP network traffic, and it interprets them in network protocol transaction logs suitable for analysis
- Based on the network high level logs received from the MS, the AE uses AI/ML to detect anomalies in network protocol transactions. If a sign of an incident is found by the detection meaning a security incident will occur in the future, or it is occurring or it has occurred, an alert is raised to trigger a response. Narrow down to our attack use case, a DNS request with an unusual DNS server is an indicator
- Intrusion detection systems may produce false positives or incorrect indicators which need to be validated. Using the knowledge base of attack tactical and techniques, the DE can conduct hypothesis-driven investigation to confirm the occurrence of the incident. The unusual destination DNS server can be a result of either a legitimate private DNS server configured in the UE or an attempt to redirect the DNS request sent by the user. To obtain the desired IP address of DNS server when the ciphered text is decrypted after the gNB, the attacker needs to know the original DNS server address to modify. This address is usually disclosed by the network operator via the primary and secondary DNS parameters. An approach to confirm the attack is the DE generates an action plan which silently replaces the DNS server address for the user by a hidden value. The user connection needs to be restarted to renew the IP settings, and the DE starts to wait for receiving subsequent DNS requests from the user. If the DE is triggered again for that UE, it means the aLTEr attack incident is then confirmed because the DNS server IP address matches with the XOR result of the hidden and the disclosed addresses. The response plan to this attack consists of enabling the integrity protection by requesting the SMF to provide user plane security policy for a PDU session to the gNB during the PDU session establishment procedure [49]. Otherwise, the hypothesis result invalidates the alert as the user is using a private DNS, the SFC classifier is updated to steer the private DNS away from the detection to avoid any future false positive alerts. And finally, the DE plan includes the rolls back of the network settings for the user.
- The NS-SECaaS instantiates DE responsible for hypothesis-based investigation to validate aLTEr attack after the alert has been raised. Actually, each attack has its own modus operandi, therefore it is more appropriate to deploy dynamically the investigation VNF and its policies to adapt to the threat. This response function is created on the event the F-SECaaS has escalated when it was not capable to handle the alert.

As for the NSS-SECaaS, it is responsible for supervising network slice instances, it collects security reports and events raised by network slice instances, it analyses them to sort out the security issues that can be solved locally. As a response, it updates a network slice instance with additional security enablers as well as it controls the life cycle of its VNFs. Finally, the NSS-SECaaS disseminates the knowledge learned from one network slice instance to all other instances to improve proactively their protection. The NSS-SECaaS leverages the following MonB5G sublayer components:

- The MS to collect security reports from each network slice instances and status and LCM information of their constituent NFV objects (network services, VNF, connectivity, …)
- The AE to analyse the collected information to identify emerging vulnerabilities and threats or learn lessons from the incidents that have been addressed. Applied to the aLTEr attack use case, the hypothesis-based threat hunting VNF needs to be deployed in extension to perform investigation as this attack has not been foreseen at the network slice preparation stage.
- The DE to plan actions to improve the defence in place in the network slice instance. In addition, the DE may plan to share lessons learned from one network slice instance and extrapolate the security configuration changes to all network slices. According to the level of sensitivity and criticality of a device, the DE plan the activation of the integrity protection of the UP prevent the aLTEr attack.
- The ACT executes the DE output action plan, such as creating security VNFs to be inserted into from a network service using the interface SecurityVnf Mgmt.001 of the reference point point Sc-Or defined in [50].

Through this use case, we highlight the use of the MonB5G components in the security framework and the roles they play in the cyber security incident response. They actually contribute to the process of preventing the attack from achieving its purpose. The openness of the MonB5G framework to external systems is illustrated via the various options of the response plan which includes actions towards entities, such as a) customer VNF and b) security VNF to update their configuration, c) the SFC controller to steer user traffic and also d) the NFV orchestrator to instantiate a security VNF. Finally, the use of SECaaS offer makes it possible the distribution, the delegation-escalation and the adaptability to demands of security services.

5. MonB5G Energy-Efficiency Techniques

In this section, we present MonB5G preliminary works on energy-efficiency. By leveraging MonB5G distributed network slicing architecture, where the three administrative elements, I.e., the monitoring system (MS), analytic engine (AE) and decision engine (DE), are instantiated at each technological domain and for each slice, several energy-aware artificial intelligence (AI) and design techniques are proposed by MonB5G to achieve energy-efficiency vision in MS, AE and DE. Specifically, distributed multi-agent Deep Reinforcement Learning (DRL)-based **DE**s are considered to perform cross-domain joint slice VNF placement and energy control by incorporating the energy cost into the DE multi-objective reward function. Moreover, to reduce the transmission overhead and thereby the underlying energy consumption, a constrained federated learning (FL)-based **AE** is introduced which makes the analysis and prediction task more energy-efficient by dramatically reducing the amount of raw data exchanged between local AEs and the end-to-end AE, and resulting in more scalability to support a massive number of concurrent slices. Based on slice traffic analysis, MonB5G considers also a dynamic RAN offloading via a data-driven base-station (BS) switching OFF/ON. Finally, the **MS** has been designed in such a way to minimize the measurement load by adding an internal memory called common online memory store (COMS).

This section starts by reviewing the main works on energy-efficiency in the context of 5G networks, including network slicing. It then delves into MonB5G contributions that cover all the three technological domains, namely, RAN, Edge, and Cloud and the three administrative elements, i.e., MS, AE and DE.

5.1 Energy-Efficiency in 5G Networks: A Review

Energy-efficiency (EE) is a major key performance indicator for the sustainability of beyond 5G networks. In this regard, network resource management algorithms should achieve the best Quality of Service (QoS) with minimum energy consumption. This involves node-level and network-level strategies that require network architectures with more flexibility/programmability in resource placement and allocation.

First, there are multiple approaches to achieve EE at the RAN domain [51]. In the 5G, the strategies for BS ON-OFF switching, an approach already used for previous generations of communication systems (LTE) [52] [53] [54] [55], are still very relevant. This technique consists on turning off BS depending on how the traffic across the BS varies for EE [56] [57] [58] [59], which is proven to be an NP-Hard problem [[52] , [60], [61]]. To add to this difficulty, the technological enhancements of 5G networks require ON/OFF switching strategies to be re-adapted for the new communication technologies [56]. For example, in the 5G RU/CU/DU functional split, 5G users are connected to RUs and processing is done by centralized units (CUs). On-Off switching of RUs/DUs is very similar to more traditional ON-OFF switching used for previous communication technologies. But given that the RU/DUss are already designed as low-power transmitters in 5G achieving a 10x reduction based on this technique is not viable. Because of this, it is also appealing to look to RU-DU-CU ON-OFF Switching. It is possible to turn off CUs if they are underutilized, but then the associated RUs/DUs are left without service. In order to prevent users from losing QoS, RUs need to be associated with new CUs dynamically, which results into a more complex scheduling and user association problem. In addition, given that 5G BSs can use several frequency band layers, the propagation and obstacle loss is more critical, and makes the association of users to neighboring BSs a more difficult problem. In this regard, a distributed Q-learning algorithm has been introduced [62], which chooses how deep a BS can sleep according to the best switch-off sleep mode (SM) level policy that maximizes the trade-off between energy savings and system delay. Moreover, as cell load impacts its energy-efficiency, a multi-agent online reinforcement learning-based traffic offloading algorithm has been introduced [63], which benefits from the awareness about other macro-cells offloading strategies to improve the quality of the selected traffic offloading action without explicit information exchange. This yields 14% improvement in network energy-efficiency. In the same direction, a joint energy-aware Deep Q-network (DQN) traffic offloading and demand forecasting strategy has been presented [64], which leverages an open dataset from a major telecom operator to train BSs' control model leading to 5% energy-efficiency gain compared to native Q-learning. Since 5G networks intrinsically endure a large energy waste resulting from the high redundancy of lightly loaded, always-on, small-cell base stations, a game theoretic approach to design a distributed energy efficient bandwidth sharing mechanism for small-cell networks has been proposed [65]. It invokes a reinforcement learning approach to intelligently and dynamically learn good strategies for user-equipment association and orthogonal frequency division multiple access (OFDMA) scheduling to strike a balance between energy efficiency and user throughput. Moreover, Feng et. al. [57] propose a solution to maximize the EE of massive Multiple-Input Multiple-Output (MIMO) systems in heterogenous networks. Their system considers a macrocell which is a two-tier heterogenous network that consists of macro base station (MBS) with a massive MIMO and some small base stations (SBSs). They demonstrate the optimality of their Integer Linear Programming (ILP) solution, for which they relax the constraints of the problem formulation by allowing the association of users to BSs to be a continuous variable in the domain [0,1] instead of a binary variable. They apply a similar approach to the variable that defines the ON-FF state of a SBS, defining it as a continuous variable in the same domain. In addition to this, they decompose the problem in two sub-problems in order to find the optimal solution, for which they develop two solutions: one centralized and the other distributed. Interestingly, they find that the throughput achieved

with a BS On-Off switching strategy drops, highlighting a trade-off between this metric and EE [51], [56]. Celebi et. al. [58] propose a traffic load definition for dense small cell networks (SCNs) involving randomly distributed SBSs and user equipments (UEs). In their model, it is possible for a UE to be within the coverage of multiple SBSs. They provide a centralized (CLB, centralized Load Based On/Off switching) and another distributed (DLB, distributed Load Based On/Off switching) solution to establish a compromise between EE and network throughput. They compare these solutions with a more complex one called Wake-Up Control (WUC) in which a MBS has the ability to wake up any sleeping SBS. In CLB, the SBSs are turned off when they present the minimum instantaneous load value as a response to each SBS that had just woken after a specific time period. The DLB operates in a very similar way to the CLB, with the difference between them is that DLB does not rely on a central controller to decide candidate SBSs to turn off, but rather use the most recently woken-up SBS to become the decision maker, and choose candidates for the next SBS that will be turned off. The WUC approach is different in this respect, since the MBS controller can decide to wake up any sleeping SBS at any time, without requiring specific time windows for this. This allows to service outstanding requests a bit faster, instead of letting them wait for the specific time window. Their results demonstrate that the blocking probability of all approaches decreases as more SBSs are turned on (higher on ratio) and as the tolerable delay gets larger. WUC performs better than CLB/DLB when the on ratio is below 0.5, but they become very similar after that point. Similarly, the throughput of CLB/DLB and WUC converge very closely to each other for non-sleeping SBS fractions larger than 30%. However, WUC yields less EE even though it has larger average throughput.

On the other hand, in the context of a cooperative multi-operator 5G network based on virtualized radio access and core, a sleep-mode and spectrum-sharing strategy to minimize the gNB power consumption has been presented [66]. The proposed dynamic inter-operator spectrum–sharing formulation is cognizant of inter-RAN traffic volume to motivate mobile network operators (MNOs) to cooperate to achieve energy efficiency in their RANs. In this intent, an inter-operator joint optimization problem is formulated to obtain power efficient intra- and inter-RAN beamforming vectors for supplementary energy gains and improved UE signal reception. On the other hand, by leveraging network function virtualization (NFV) technology, an energy-efficient dynamic network functions placement has been proposed [67]. It leverages ILP to adapt the joint locations of DU/CU and MEC to the actual distribution of network processing and transport resources. This enables to aggregate DUs/CUs into fewer cloud servers, resulting thereby in 20% energy saving.

Moreover, many works focus on solving the cross-domain energy-efficiency optimization problem with single agent reinforcement learning. Most notably, in [68] the authors propose a novel zero-touch framework, based on a continuous model-free deep reinforcement learning method to minimize energy consumption and virtual network function instantiation cost. They present an Actor-Critic-based algorithm called, twin-delayed double-Q soft Actor-Critic (TDSAC) and elaborate on how such system can solve dynamic control and optimization problems in network slicing. Similarly, in [69], Li et al. propose a Deep Deterministic Policy Gradient (DDPG) based algorithm, aiming to obtain the optimal power control scheme. They evaluate the proposed framework with multiple comparisons with the other well-known algorithms, such as Deep Q-learning. The showcased numerical results imply that the proposed framework was able to significantly minimize energy consumption.

Recently, to accommodate the performance of reinforcement learning algorithms in the great scale of the edge-cloud systems of the next-generation networks, a lot of attention has been brought to multi-agent reinforcement learning algorithms. In recent bibliography, Shah et al in [70], employ Multi-Agent Reinforcement Learning (MARL) to solve the Service Function Chaining (SFC) placement problem for Internet

of Things (IoT) connected devices. The presented system enables IoT devices to access processing power from the Network Function Virtualization (NFV) enabled network by sending requests and gaining access through SFCs that are deployed in the network. Their proposed solution is based on multiple DQN agents that map the SFCs to the substrate network and it is considered a resource allocation method. Regarding energy efficiency, in [71] the authors tackle the problem with Dynamic Virtual Machine Consolidation (DVMC). They propose a distributed multi-agent reinforcement learning framework that is able to select the most adequate power mode and frequency of each host during runtime. According to the presented results, their algorithm was able to reduce data centre energy consumption by up to 15% compared to similar works such as [72].

5.2 MonB5G Energy-Efficiency

5.2.1 DECENTRALIZED ENERGY-EFFICIENT DE CONTROL

To leverage MonB5G distributed network slicing architecture, we have developed a multi-agent reinforcement learning framework that can perform intra-slice SFC placement across multiple domains to jointly minimize user latency and maximize throughput. We are modifying and extending our proposed framework to include cross-domain energy-efficiency maximization as defined in [68].

As depicted in Figure 14, we consider a network composed of multiple geographical domains, each with its own subnetwork. Each local network is composed of switches, server hosts, and links. All network entities have a limited number of resources and their utilization implies running costs. A maximum number of VNFs can be deployed on the domain servers with limited processing capability calculated by million operations per time slot per central processing unit (CPU). Domains can be classified as edge or cloud. Edge domains are considered to have multiple transmission/reception points (TRPs) of the Centralized-RAN (C-RAN) CU-DU split-based network, giving connected terminals access to the network through a beamforming solution. We split the network into two graphs of different levels. The substrate network graph and the domain level graph.

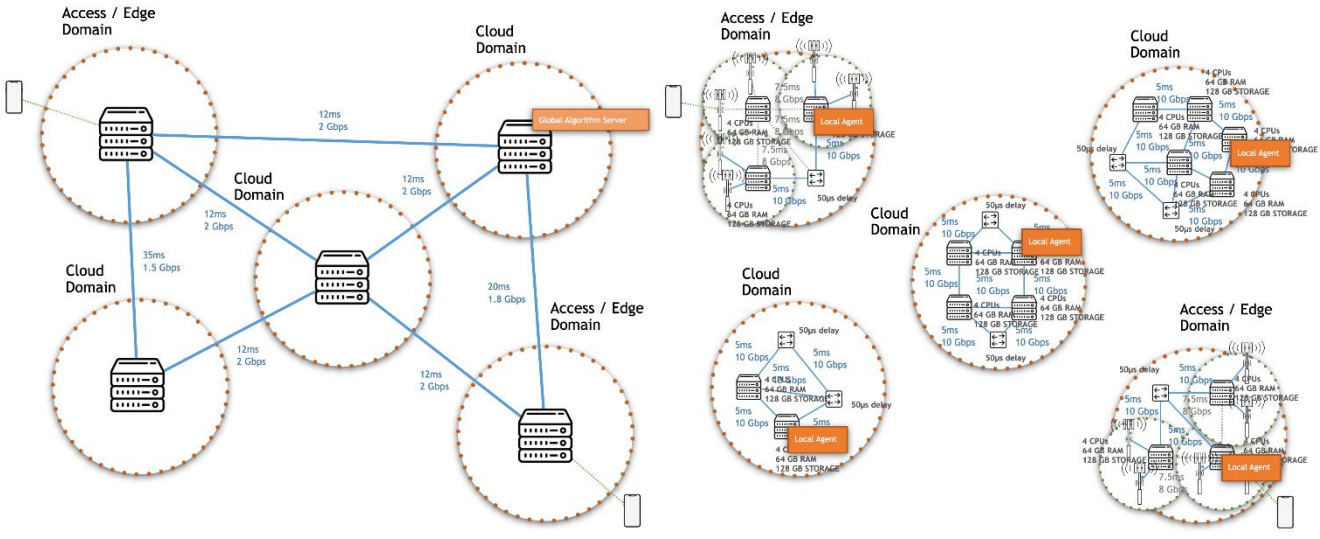

Figure 14. Substrate network and local domain network graphs.

The distributed energy efficiency management framework is made of multiple reinforcement learning agents located in every domain as shown in Figure 15. A globally accessible VNF enables messaging capabilities between the local domain agents and is used for calculating and distributing the global reward. This architecture enables scalability of both the problem and action spaces of the defined Markov Decision Process (MDP) problem. The problem objective is to achieve lower total costs under strict user QoS, predefined thresholds, latency, and computing resource constraints. We define the distributed MDP problem as below:

- **Local domain agent state space:** The state space provides input data about possible network configurations for an agent via the interaction with the environment. At the domain level, the local agent state is defined as the CPU, RAM, and storage utilization values of all local servers, the intradomain link bandwidth utilization and latency values, each user's data rate and the maximum allowed latency SLA, the number of local arrival requests for each slice corresponding to each SFC and the domain energy status.
- **Local domain action space:** The action space is defined as the decision of the local agent. We define it as a discrete value action that defines the server to which every VNF of the SCFs must be migrated to ensure higher throughput and energy efficiency, but also lower latency at the same time.
- **Shared Reward:** The reward is feedback on how the performed action affected the environment. We define a shared reward as the average of all local rewards to enable cooperation [73]. The reward can be expressed with the following equations:

Equation 1 Cross-domain reward

$$R = \sum_{r=0}^{D} r_d$$

where *D* is the number of domains,

Equation 2 Domain reward

$$r_d = \frac{t_s + e_d}{l_s}$$

where *ts* is the offered service throughput, and *ls* is the service latency, given that each user has access to one service.

Equation 3 Local return

$$e_d^{(t)} = \frac{1}{\frac{1}{M^{(t)}}\left(\mathcal{E}_{\text{Net}}^{(t)}\right)} + \sum_{m=1}^{M} \varepsilon_m^{(t)}$$

as defined in [68].

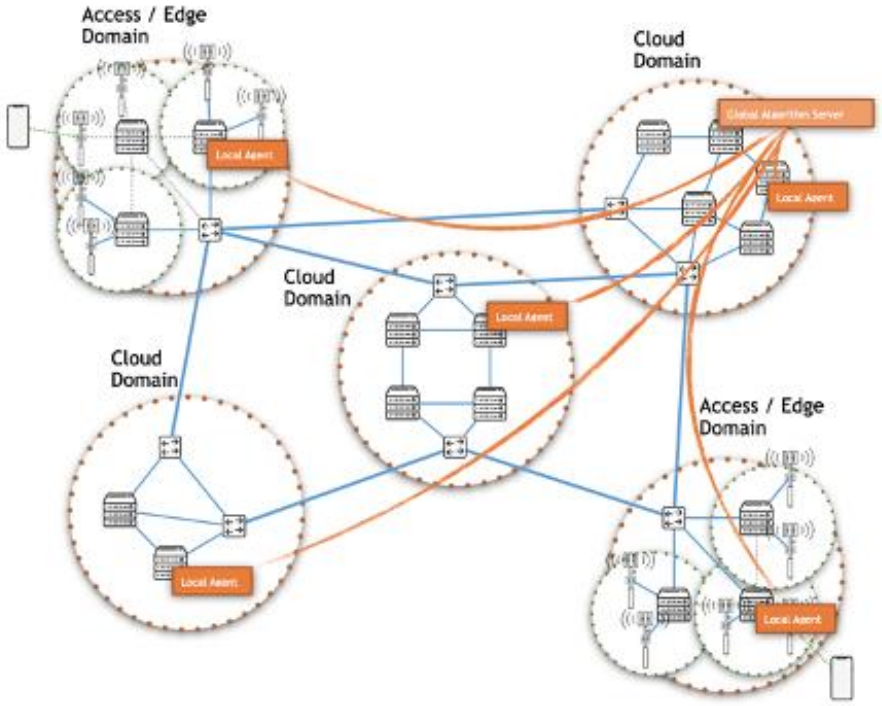

Figure 15. Location of learning agents and domains.

5.2.2 *ENERGY-EFFICIENCY AT RAN*

Our contribution in comparison to the BS ON-OFF switching strategies reviewed above relies on time-series prediction of the traffic-load [56] at the network slice level using enhanced context- aware traffic predictors (ECATP). Whereas the work in [59] implements different design heuristics for their algorithm according to domain knowledge in wireless communications, our predictors are designed using Deep Neural Networks with enhanced loss functions for training that inject knowledge regarding the resource allocation problems for traffic load management in 5G networks.

Many research works have used prediction in some form to drive ON-OFF Switching strategies [61], [74], [75], [76]. In [61], Jang et. al. have implemented ON-OFF Base switching using LSTM-based networks with Root Mean Squared Error (RMSE) loss functions considering the user position, without considering network slicing. In contrast, our proposal does the ON-OFF switching based solely on the traffic prediction at the slice level. Park et. al. , [74] use a Markov-based prediction scheme to predict the UEs traffic load in the hot region, and then drive the ON-OFF Switching of RRH (remote radio heads) based on the traffic prediction and other traffic related metrics. Our prediction approach is radically different in all cases, since ECATP allows to use different Deep Neural Network (DNN) architectures, and considers different issues related to resource allocation in 5G networks. Huang et. al. [76] propose a solution that predicts the UEs traffic load in hot regions of traffic as the tidal effect using a Markov-based scheme, and this prediction is used to drive a load balancing-based cell association algorithm to optimize UE-BS associations and an ON-OFF strategy for the F-gNBs (Femtocell g-NodeB). Their prediction procedure is totally different from ours, since they are using an MDP process for it

and predicting other aspects of UE behavior in order to calculate the traffic load of the network. On the other hand, Mohamed et. al. [75] used a mechanism to predict the time in which a BS should be turned on based on the measurement of the pilot signal of the SBS and the times it has been turned on in the past, instead of the traffic load.

In the approach we are proposing, we intend to use the traffic prediction to re-route the traffic of a SBS to another SBS [61], or directly to the MBS, assuming the costs of re-routing do not result in service level agreement (SLA) violations or even higher energy costs. As previously explained, our prediction is based on our ECATP framework, that has context-aware predictors and uses different DNN architectures depending on their prediction performance to optimize the usability of the prediction values. If our predictions determine that it is feasible to turn off a BS without re-routing traffic, then the BS will be turned off for the time-window in which such low-traffic conditions occurs.

We base the development of this approach on a model of a communication infrastructure that consists on a MBS with a number of associated SBSs, similar to Feng et. al. [57], which yields a two- tier RAN architecture common in telecommunication network deployments [75]. The prediction is done at network slice granularity, which gives a layer of flexibility in how resources are allocated to handle the traffic load. Based on the predicted traffic at different time windows, the SBSs will be turned off when their traffic is below a certain threshold that allows its traffic to be re-routed without compromising the QoS of other slices. Likewise, the SBS will be turned on with some time in advance when the traffic predicted at a future time window increases accordingly, in order to prevent service degradation due to switching delays [75].

5.2.3 *ENERGY-EFFICIENCY AE AT EDGE*

To ensure energy-efficiency at the edge, dynamic resource allocation for network slicing can leverage advanced federated learning (FL) techniques. In this subsection, a new class termed *Statistical Federated Learning (SFL)* for energy-efficient analytic engine (AE) is presented, which can learn resource provisioning models over a data distribution in an offline fashion while respecting some preset local SLA constraints defined in terms of long-term statistics over an observation window. The focus here is on resource cumulative distribution function (CDF)-based SLA---that is also dataset-dependent and nonconvex non-differentiable---and the corresponding SFL local optimization task is formulated using the proxy-Lagrangian framework and solve it via a non-zero sum two-player game strategy. Numerical results show that the proposed decentralized AE resource provisioning approach enables SLA enforcement while significantly reducing the communication overhead and energy consumption compared to a centralized setup at the expense of a short delay.

As depicted in Figure 16, we consider a beyond 5G edge-RAN architecture under the central unit (CU)/distributed unit (DU) functional split, wherein each transmission/reception point (TRP) is co-located with its DU which is connected to the corresponding CU by a fronthaul link. In this respect, each CU k ($k = 1,...,K$) runs as a virtual network function (VNF) on top of a **commodity hardware located at the edge cloud** and performs slice-level RAN key performance indicators data collection via a monitoring system (MS) as well as implements AI-enabled slice resource analytics through the so-called analytics engine (AE). For each CU k and slice n ($n = 1,…,N$), MS (k, n) has a local dataset $D_{k,n}$ of size $d_{k,n}$ that is generally small and non-exhaustive. Therefore, the corresponding local AE participates in a federated learning task—to accurately train its resource analysis model—and is thereby connected to **an end-to-end AE located at the core cloud** that plays the role of model aggregator without having access to the raw mini-datasets.

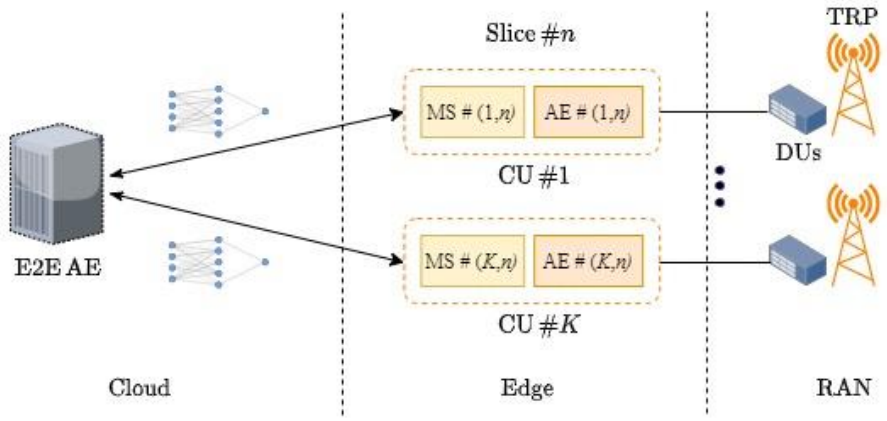

Figure 16. Network architecture with decentralized MS/AE at the edge cloud

As summarized in Table 15, the collected datasets correspond to encoded measurement data from a live LTE-advanced network with 3200 TRPs. It includes, as input features, the hourly traffics of the main over-the-top (OTT) applications, channel quality indicator (CQI), and MIMO full-rank usage. The supervised output KPI might be either the number of occupied downlink (DL) physical resource blocks (PRBs), or the CPU load or the number of RRC connected users. Once the slices are defined, the traffic of the underlying OTTs is summed to yield the traffic per slice.

Table 15. Mini-datasets features

Metrics		Description
Features	**OTT Traffics per TRP**	Includes the hourly traffic for the top OTTs: Apple, Facebook, Facebook Messages, Facebook Video, Instagram, NetFlix, HTTPS, QUIC, Whatsapp, and Youtube
	CQI	Channel quality indicator reflecting the average quality of the radio link of the TRP
	MIMO Full-Rank	Usage of MIMO full-rank spatial multiplexing in %
Output	**DLPRB**	Number of occupied downlink physical resource blocks
	CPU Load	CPU resource consumption in %
	RRC Connected Users	Number of RRC users' licenses consumed per eNB

According to the SLA established between slice *n* tenant and the physical operator, any assigned resource to the tenant should not exceed a range $[\alpha_n, \beta_n]$ with a probability higher than an agreed threshold γ_n. This translates into learning the resource allocation model under empirical cumulative density function

constraints, which amounts to solving the following local optimization task at FL round *t (t = 0,...,T -1)*,

$$\min_{\mathbf{W}_{k,n}^{(t)}} \frac{1}{D_{k,n}} \sum_{i=1}^{D_{k,n}} \ell\left(y_{k,n}^{(i)}, \hat{y}_{k,n}^{(i)}\left(\mathbf{W}_{k,n}^{(t)}, \mathbf{x}_{k,n}\right)\right),$$

$$\text{s.t. } F_{\mathbf{x}_{k,n}\sim\mathcal{D}_{k,n}}(\alpha_n) = \frac{1}{D_{k,n}} \sum_{i=1}^{D_{k,n}} \mathbb{1}\left(\hat{y}_{k,n}^{(i)} < \alpha_n\right) \leq \gamma_n,$$

Empirical CDF

$$\tilde{F}_{\mathbf{x}_{k,n}\sim\mathcal{D}_{k,n}}(\beta_n) = \frac{1}{D_{k,n}} \sum_{i-1}^{D_{k,n}} \mathbb{1}\left(\hat{y}_{k,n}^{(i)} > \beta_n\right) \leq \gamma_n,$$

where $\ell(.)$ is the squared error loss function, 1(.) stands for the indicator function.

The local SFL optimization can be solved using a proxy-Lagrangian approach that consists of forming two Lagrangians. The first, L_1, is containing the loss function and a smooth approximation of the SLA constraints called proxy constraints, where the indicators are replaced with smooth sigmoid functions. The second Lagrangian, L_2, is composed of the original SLA constraints. The joint optimization of the two Lagrangians turns out to be a non-zero-sum two-player game wherein the first player wishes to minimize L_1 and the second player aims at maximizing L_2. This process ends up reaching a nearly-optimal nearly-feasible solution to the original constrained problem. The obtained weights are then sent back to the central server (e.g., the central AE) to perform averaging. This process is summarized in Algorithm 1.

Algorithm 1: Federated learning with local proxy-Lagrangian two-player game for slice n.

Input: R_λ, η_λ, T, L.
OSS server initializes $\mathbf{W}_n^{(0)}$ with random Gaussian weights and broadcasts it to local AEs.
for $t = 0, \ldots, T-1$ **do**
  parallel for $k = 1, \ldots, K$ **do**
  Initialize $M =$ `num_constraints` and $\mathbf{W}_{k,n,0} = W_n^{(t)}$
  Initialize $\mathbf{A}^{(0)} \in \mathbb{R}^{(M+1)\times(M+1)}$ with $\mathbf{A}_{m',m}^{(0)} = 1/(M+1)$
  for $l = 0, \ldots, L-1$ **do**
    Let $\lambda^{(l)}$ be the top eigenvector of $A^{(l)}$
    `# Oracle optimization`
    Let $\mathbf{W}_{k,n,l} = \mathcal{O}_\delta\left(\mathcal{L}_{\mathbf{W}_{k,n,l}}(\cdot, \lambda^{(l)})\right)$
    Let $\Delta_\lambda^{(l)}$ be a gradient of $\mathcal{L}_\lambda(\mathbf{W}_{k,n,l}, \lambda^{(l)})$ w.r.t. λ
    `# Exponentiated gradient ascent`
    Update $\tilde{\mathbf{A}}^{(l+1)} = \mathbf{A}^{(l)} \odot \cdot \exp\left\{\eta_\lambda \Delta_\lambda^{(l)}(\lambda^{(l)})\right\}$
    `# Colunm-wise normalization`
    $\mathbf{A}_m^{(l+1)} = \tilde{\mathbf{A}}_m^{(l+1)} / \left\|\mathbf{A}_m^{(l+1)}\right\|_1$, $m = 1, \ldots, M+1$
  end
  return $\mathbf{W}_{k,n}^{(t)} = \mathbf{W}_{k,n,L-1}$
  Each local AE (k, n) sends $\mathbf{W}_{k,n}^{(t)}$ to the OSS server.
  end parallel for
  return $\mathbf{W}_n^{(t+1)} = \sum_{k=1}^K \frac{D_{k,n}}{D_n} \mathbf{W}_{k,n}^{(t)}$
  and broadcasts the value to all local AEs.
end

Algorithm 1. Federated learnig with local proxy-Lagranging two-plyer game for slice n.

To evaluate the energy-efficiency of the proposed SFL, we intent to conduct extensive experiments where we consider an additional baseline, namely, a centralized constrained learning (CCL) model that is trained on the full dataset composed of the aggregation of the K=200 mini-datasets. The training will be done using batches of the same size as the local datasets, i.e., 1000 samples. This means that a communication round in the federated setup is equivalent to 100 epochs over a batch in the centralized one. Based on the overhead analysis and datasets sizes, the energy consumption will be calculated as follows:

- **Local Computation energy:** Let f = 2 GHz be the computation capacity at each CU, which is measured by the number of CPU cycles per second and $C = 10^4$ (cycles/sample) is the number of CPU cycles required for computing one sample data at each CU, and $\mu=10^{-28}$ is the is the effective switched capacitance that depends on the chip architecture. For the centralized setup we assume the same CPU type as well. The local computation energy at each CU is given by [77],

$$E_k = \kappa C d_k f^2$$

- **Transmission energy:** We consider R = 1 Gbps transport channels between CUs and the central OSS server with transmit optical power of p =-2 dBm [78] . Therefore, the transmission energy is given by,

$$E_{\text{trans},k} = p\frac{d_k}{R}$$

The final results of the presented concepts will be provided in the next deliverable.

5.2.4 DE CROSS-DOMAIN CLOUD AND RAN ENERGY-EFFICIENCY

To tackle the joint energy-efficiency at the cloud and RAN domains, the decision engine (DE) is built upon a continuous model-free DRL scheme that aims to minimize energy consumption and virtual network function (VNF) instantiation cost for each slice. The design is based on a novel Actor-Critic-based to stabilize learning termed *TDSAC.* The TDSAC enables the local DE to accumulate the knowledge learned in the past to minimize future network slicing costs.

The whole energy consumption in cloud and RAN domains involves CPU, VNF deployment, and radio optimal beamforming transmission, and is given by

$$\mathcal{E}_{Net}^{(t)} = \underbrace{\sum_{z=1}^{Z} \iota P_z^3 + \sum_{x=1}^{X} \psi_x}_{\text{baseband}} + \underbrace{\sum_{n=1}^{N}\sum_{m=1}^{M} \mathbf{v}_m^H \mathbf{G}_n^H \mathbf{G}_n \mathbf{v}_m}_{\text{transmission}}$$

where, the objective is to minimize the overall network cost with respect to the incurred computing resources and energy consumption under some QoS constraints at each decision time step and thereby the continuous model-free DRL optimization is given by,

$$\begin{aligned} \min \quad & \frac{1}{M^{(t)}}(\mathcal{E}_{Net}^{(t)}) \\ \text{subject to} \quad & p_m \leq \mathcal{P}_{max}, \quad m \in M, \\ & SINR_m \geq SINR_{th,l}, \quad m \in M, l \in L, \\ & \Delta_m \leq \Delta_{th,l}, \quad m \in M, l \in L. \end{aligned}$$

This problem can be formulated from a MDP perspective, where the objective is to achieve lower total costs under user QoS, predefined thresholds, and computing resource constraints. This reflects the correlation between energy consumption and CPU usage, where beamforming power for each user affects SINR that in turn influences computing resource consumption.

Actor-Critic methods are a combination of policy optimization and Q-Learning. Unlike the DDPG [79] and TD3 [80], the TDSAC benefits from stochastic policy gradient to stabilize the learning and improve time efficiency while mitigating very high sample complexity and meticulous hyperparameter tuning: i) The (clipped) double Q-learning technique parameterizes critic networks and critic. Unlike the TD3 in TDSAC, the next state-actions used in the target come from the current policy instead of a target policy. ii) The target in Q-learning depends on the model's prediction so cannot be considered as a true target. To address this problem, we use another target network instead of using Q-network to calculate the target. iii) In TDSAC, the delayed strategy updates the policy, temperature, and target networks less frequently than the value network to estimate the value with a lower variance to have a better policy. iv) Experience replay enables RL to reuse and memorize past experiences to solve the catastrophic interference problem. In our method, we store experiences to train deep Q-Network and sample random many batches from the experience replay (buffer/queue) as training data. The proposed DE approach is summarized in Algorithm 2.

Algorithm 2: TDSAC-based Network slicing

Initialize actor network ϕ and critic networks θ_1, θ_2
Initialize (copy parameters) target networks θ_1', θ_2'
Initialize learning rate $\ell_\alpha, \ell_Q, \ell_\pi$
Initialize replay buffer β
Import custom gym NS environment ('smartech–v2')
while $t <$ max_*timesteps* **do**
  if $t <$ *start_timesteps* **then**
    a = env.action_space.sample()
  else
    Select action $a \sim \pi_\phi(a|s)$
  end
  next_state, reward, done, _ = env.step(a)
  store the new transition (s_t, a_t, r_t, s_{t+1}) *into* β
  if $t \geq$ *start_timesteps* **then**
    sample batch of transitions $(s_{t_B}, a_{t_B}, r_{t_B}, s_{t_B+1})$
    $\theta_i \longleftarrow \theta_i - \ell_Q \nabla_{\theta_i} J_Q(\theta_i)$, *i=1,2* *#Update soft Q-function*
    if $t \mod freq$ **then**
      $\phi \longleftarrow \phi + \ell_\pi \nabla_\phi J_\pi(\phi)$ *#Update policy weights*
      $\alpha \longleftarrow \alpha - \ell_\alpha \nabla_\alpha J(\alpha)$ *#Adjust temperature*
      $\theta_i' \longleftarrow \tau\theta_i + (1-\tau)\theta_i'$ *i=1,2* *#Update target network*
    end
  end
  if *done* **then**
    obs, done = env.reset(), False
  end
  t=t+1
end

Algorithm 2. TDSAC-based Network slicing

We use PyTorch [81] interfaced with an OpenAI Gym-based [82] developed B5G simulator as the most famous simulation environment in the DRL community and evaluate our method against other State-of-the-Art DRL approaches, namely, TD3, DDPG, and SAC [83] with a minor change to keep all algorithms consistent. To guarantee a trade-off between CPU resource usage and energy consumption a cross-layer and correlated DE cost function is considered.

5.2.5 *OPTIMIZED MS*

MonB5G MS design considers an internal memory called COMS as depicted in Figure 17. It is added in order to avoid implementing hard synchronization constraints among the MS, DE, AE whenever information needs to be exchanged. In this way, the DE and AE can be more flexible in terms of the length of their processing without compromising the granularity at which the MS can sample monitoring data from the controlled systems. So, it is the MS (depending on its capabilities and amount of information as well as the granularity set from an External User Interface (EUI)) that somehow defines how fast the data is sampled. Also the stored data includes predictions and decisions of AE and DE, respectively. This strategy enables a maximum of data reutilization and minimizes the measurement load.

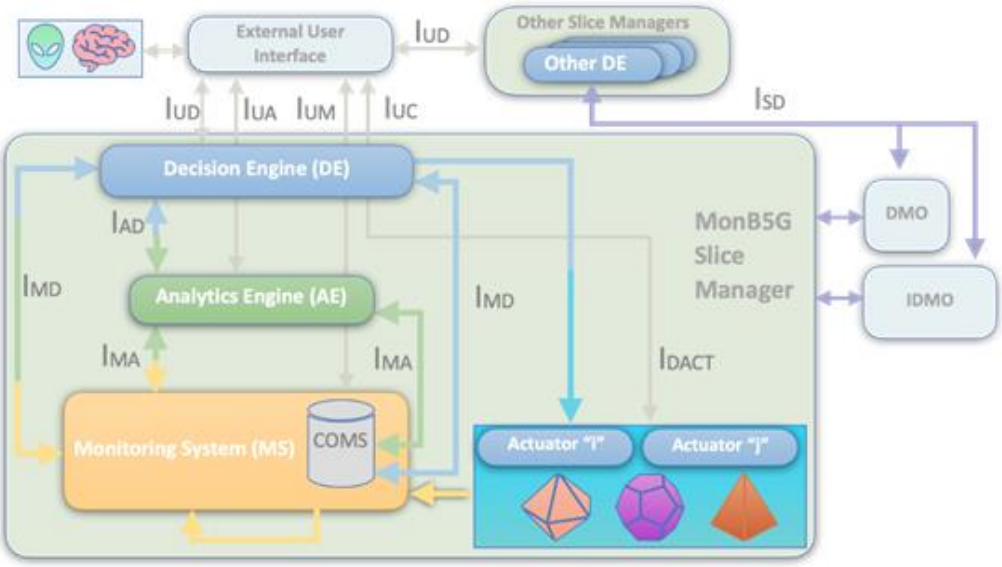

Figure 17. MonB5G MS with COMS

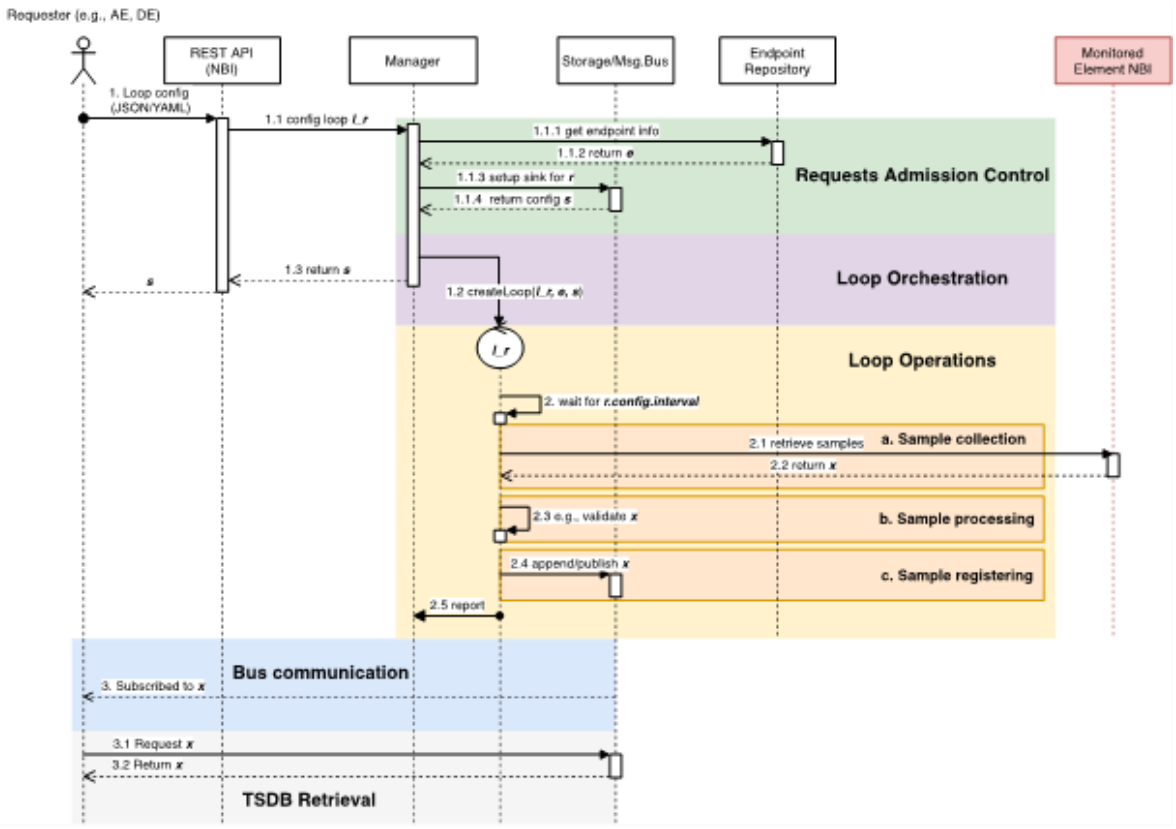

Figure 18. MS Request and metrics retrieval from Monitored Element

As described thoroughly in D3.1 and showcased in Figure 18 , the MS measurement is also based upon the concept of dynamic Sampling Loops that provides a high degree of flexibility in the monitoring and reduces the resulting energy consumption. Advanced results will be provided in the final deliverable D5.2.

6. Conclusions and next steps (EUR)

In this deliverable, we summarized the activities conducted by the consortium on security management of network slices and energy efficiency. Although only seven months left from the beginning of the activities, many achievements have been made. First, we refined the security architecture derived from the reference architecture devised in WP2 to achieve Zero-touch security management. In addition, two representative use-cases of security attacks on network slices have been identified and detailed in order to illustrate how MonB5G AI-based components are used to identify attacks and mitigate them. Finally, the deliverable introduced the initial contribution on energy-efficiency in the context of 5G and beyond networks.

As a perspective, we will continue refining the security architecture of MonB5G by relying on the outputs of the two considered examples, which will be defined further, particularly the AE/DE components and the Slice Orchestrator (SO). For the latter, a more dynamic role will be further explored and exploited to ensure a full distributed security management process.

Finally, we will consolidate and evaluate the proposed energy-efficient mechanisms.

7. References

[1] INSPIRE-5Gplus, "White Paper: Intelligent Security Architecture for 5G and Beyond Networks," November 2020.

[2] INSPIRE5Gplus, "D5.1: 5G Security Test Cases," 2020.

[3] Zarca, Alejandro Molina et al, "Security management architecture for NFV/SDN-aware IoT systems," IEEE Internet of Things Journal 6.5 (2019): 8005-8020.

[4] Bagaa, Miloud et al, "A machine learning security framework for IoT systems," IEEE Access 8 (2020): 114066-114077.

[5] D.Rivera et al., "Final monitoring components services implementation report,".*Montimage, CNR, ATOS, AALTO, UTRC, Anastacia H2020 Eur. Project Deliverable D 4 (2019).*

[6] TS 33.401, "Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture".

[7] TS 23.101, "General Universal Mobile Telecommunications System (UMTS) architecture (Release 13)," 3GPP, 1999.

[8] 5GPPP Architecture Working Group, "View on 5G Architecture".

[9] 5G-ensure, "Deliverable D2.1 Use Cases," 5G-Ensure, 2016.

[10] Jim Gumbley, "A Guide to Threat Modelling for Developers".*Article on MartinFowler.com, May 2020, https://martinfowler.com/articles/agile-threat-modelling.html.*

[11] Microsoft SDL, "Threat Modeling".*https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling.*

[12] Microsoft Security Development Lifecycle (SDL), "https://www.microsoft.com/en us/securityengineering/sdl/".

[13] Marco Morana, Tony UcedaVelez, "PASTA Process for Attack Simulation and Threat Analysis (PASTA) Risk-centric Threat Modeling," September 2019, http://securesoftware.blogspot.com/2012/09/rebooting-software-security.html.

[14] Jackson E. Wynn, "Threat Assessment and Remediation Analysis (TARA)," August 2020, https://www.mitre.org/publications/technical-papers/TARA-collection.

[15] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, https://www.lockheedmartin.com/content/dam/lockheed-ma.

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

[17] T.Taleb and C. Benzaid , "ZSM Security: Threat Surface and Best Practices," *IEEE Network Magazine,* vol. 34, no. 3, pp. 124 - 133, Jun 2020.

[18] M. Barreno, B. Nelson, R. Sears, A. D. Joseph and J. Tygar, "Can Machine Learning Be Secure?," *Proc. of ASIACC06,* pp. 16-25, 2006.

[19] NISTIR 8269, "A Taxonomy and Terminology of Adversarial Machine Learning," Oct. 2019.

[20] T.Taleb and C. Bemzaid , "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?," *IEEE Network Magazine,* vol. 34, no. 6, pp. 140 - 147, Nov. 2020.

[21] C. Benzaid, T.Taleb, M.Z. Farooqi, "Trust in 5G and Beyond Network.," *IEEE Network Magazine,* p. (to appear).

[22] ETSI , "ETSI GR SAI 004 v1.1.1.Securing Artificial Intelligence (SAI); Problem Statement," Dec. 2020.

[23] Brik Bouziane and Ksentini Adlen, "On Predicting Service-oriented Network Slices Performances in 5G: A Federated Learning Approach," *2020 IEEE 45th Conference on Local Computer Networks (LCN),* pp. 164 - 171, 2020.

[24] Lyu, Lingjuan and Yu, Han and Yang, Qiang, "Threats to federated learning: A survey," *arXiv preprint arXiv:2003.02133,* 2020.

[25] Baracaldo, Nathalie and Chen, Bryant and Ludwig, Heiko and Safavi, Jaehoon Amir, "Mitigating poisoning attacks on machine learning models: A data provenance based approach," *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security,* pp. 103--110, 2017.

[26] Bagdasaryan, Eugene and Veit, Andreas and Hua, Yiqing and Estrin, Deborah and Shmatikov, Vitaly, "How to backdoor federated learning," *International Conference on Artificial Intelligence and Statistics,* pp. 2938--2948, 2020.

[27] Tolpegin, Vale and Truex, Stacey and Gursoy, Mehmet Emre and Liu, Ling, "Data poisoning attacks against federated learning systems," *European Symposium on Research in Computer Security,* pp. 480--501, 2020.

[28] The evolution of security in 5g, "A slice of mobile threats," 5GAmericas, Tech. Rep, 2019.

[29] S. E. C. M. e. a. Cunha VA, "Network slicing security: Challenges and directions," Internet Technology Letters, vol. 2, no. 125, 2019.

[30] ETSI, "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes (33.926),," ETSI, 2016.

[31] 3GPP, "Security architecture and procedures for 5G System," 3GPP, 2019.

[32] NIST, "National Vulnerability Database," 26 1 2020. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-16026. [Accessed 4 2 2021].

[33] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray and Y. Jin, "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice," *Journal of Hardware and Systems Security,* 2018.

[34] X. Yuan, C. Li and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," in *IEEE International Conference on Smart Computing (SMARTCOMP)*, Hong Kong, 2017.

[35] C. Y. Tseung, K. P. Chow and X. Zhang, "Extended abstract: Anti-DDoS technique using self-learning bloom filter," in *IEEE International Conference on Intelligence and Security Informatics (ISI)*, Beijing, 2017.

[36] e. a. E. Y. K. Chan, "Intrusion Detection Routers: Design, Implementation and Evaluation Using an Experimental Testbed," *IEEE Journal on Selected Areas in Communications,* vol. 24, no. 10, pp. 1889-1900, 2006.

[37] H. Sedjelmaci, "Attacks Detection Approach Based on a Reinforcement Learning Process to Secure 5G Wireless Network," in *IEEE International Conference on Communications Workshops (ICC Workshops)*, Dublin, 2020.

[38] L. Fang, B. Zhao, Y. Li, Z. Liu, C. Ge and W. Meng, "Countermeasure Based on Smart Contracts and AI against DoS/DDoS Attack in 5G Circumstances," *IEEE Network,* vol. 34, no. 6, pp. 54-61, 2020.

[39] R. Ettiane, A. Chaoub and R. Elkouch, "Robust Detection of Signaling DDoS Threats for more Secure Machine Type Communications in Next Generation Mobile Networks," in *IEEE Mediterranean Electrotechnical Conference (MELECON)*, 2018.

[40] "3gpp ts 22.368 v11.5.0: Service requirements for machine-type communications," 3GPP, 2012.

[41] 3GPP, "Study on RAN improvements for machine-type communications,," Tech. Rep., TR 37.868, 2012..

[42] 3GPP, "Study on RAN Improvements for Machine-type com- munications. Technical report, TR 37.868,," 2012..

[43] R. J. M. S. a. A. E. Deval Bhamare, "A survey," *Journal of Network and Computer Applications,* 2016.

[44] ENISA, "Sectoral/Thematic Threat Analysis," ENISA, 2020.

[45] ETSI, "Group Specifications: Network Functions Virtualisation (NFV) Release 3," ETSI, 2017.

[46] N. Z. Bawany, J. A. Shamsi and K. Salah, "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions," *Arabian Journal for Science and Engineering,* vol. 42, pp. 425-441, 2017.

[47] M. G. Pérez, A. H. Celdrán, P. G. Giardina, G. Bernini, P. Simone, F. J. G. Clemente, G. M. Pérez, G. Festa and P. a. Fabio, "Mitigation of cyber threats: Protection mechanisms in federated SDN/NFV," *Concurrency and Computation Practice and Experience,* 2019.

[48] K. K. T. H. a. C. P. David Rupprecht, "Breaking LTE on Layer Two," in *Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2019.

[49] T. 23.502, "Procedures for the 5G System (5GS)," 3GPP, 2020.

[50] NFV-IFA033, “Sc-Or, Sc-Vnfm, Sc-Vi reference points - Interface and Information Model Specification,” ETSI, 2020.

[51] Y. R. Li, M. Chen, J. Xu, L. Tian and K. Huang, “Power saving techniques for 5g and beyond,” IEEE Access, vol. 8, pp. 108675–108690, 2020.

[52] Wei-Te Wong, Ya-Ju Yu and Ai-Chun Pang, “Decentralized energy-efficient base station op- eration for green cellular networks,” in 2012 IEEE Global Communications Conference (GLOBE- COM), pp. 5194–5200, 2012.

[53] A. Bousia, E. Kartsakli, L. Alonso and C. Verikoukis, “Dynamic energy efficient distance- aware base station switch on/off scheme for lte-advanced,” in 2012 IEEE Global Communica- tions Conference (GLOBECOM), pp. 1532–1537, 2012.

[54] W. Tomaselli, D. Sabella, V. Palestini, V. Bernasconi and V. Squizzato, “Energy efficiency per- formances of selective switch off algorithm in lte mobile networks,” in 2013 IEEE 24th An- nual International Symposium on Personal, Indoor, and Mobile Radio.

[55] S. Xu, Y. Li, Y. Gao, Y. Liu and H. Gacanin, “Opportunistic coexistence of lte and wifi for future 5g system: Experimental performance evaluation and analysis,” IEEE Access, vol. 6, pp. 8725–8741, 2018.

[56] M. Feng, S. Mao and T. Jiang, “Base station on-off switching in 5g wireless networks: Ap- proaches and challenges,” IEEE Wireless Communications, vol. 24, no. 4, pp. 46–54, 2017.

[57] M.Feng, S.Mao and T.Jiang, “Boost:Basestationon-offswitchingstrategyforenergyefficient massive mimo hetnets,” in IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, pp. 1–9, 2016.

[58] H. Çelebi, Y. Yapıcı, İ. Güvenç and H. Schulzrinne,, “Load-basedon/offschedulingforenergy- efficient delay-tolerant 5g networks,” IEEE Transactions on Green Communications and Network- ing, vol. 3, no. 4, pp. 955–970, 2019.

[59] F. Elsherif, E. K. P. Chong and J. Kim, “Energy-efficient base station control framework for 5g cellular networks based on markov decision process,” IEEE Transactions on Vehicular Technol- ogy, vol. 68, no. 9, pp. 9267–9279, 2019.

[60] J. J. Q. Yu and V. O. K. Li, “Base station switching problem for green cellular networks with social spider algorithm,” in 2014 IEEE Congress on Evolutionary Computation (CEC), pp. 2338– 2344, 2014.

[61] G. Jang, N. Kim, T. Ha, C. Lee and S. Cho, “Base station switching and sleep mode optimiza- tion with lstm-based user prediction,” IEEE Access, vol. 8, pp. 222711–222723, 2020.

[62] A. El-Amine, M. Iturralde, H. A. Haj Hassan and L. Nuaymi, “A Distributed Q-Learning Approach for Adaptive Sleep Modes in 5G Networks,” 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 2019, pp. 1-6.

[63] I. AlQerm and B. Shihada, "Energy Efficient Traffic Offloading in Multi-Tier Heterogeneous 5G Networks Using Intuitive Online Reinforcement Learning," in IEEE Transactions on Green Communications and Networking, vol. 3, no. 3, pp. 691-702, Sept. 2019.

[64] C.-W. Huang and P.-C. Chen, "Mobile Traffic Offloading with Forecasting using Deep Reinforcement Learning," [Online]. Available: https://arxiv.org/abs/1911.07452 (Accessed: 15 Apr. 2020).

[65] Y. Wang, X. Dai, J. M. Wang and B. Bensaou, "A Reinforcement Learning Approach to Energy Efficiency and QoS in 5G Wireless Networks," in IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1413-1423, June 2019.

[66] J. Opadere, Q. Liu, T. Han and N. Ansari, "Energy-Efficient Virtual Radio Access Networks for Multi-Operators Cooperative Cellular Networks," in IEEE Transactions on Green Communications and Networking, vol. 3, no. 3, pp. 603-614, Sept. 2019.

[67] Y. Xiao, J. Zhang and Y. Ji, "Energy efficient Placement of Baseband Functions and Mobile Edge Computing in 5G Networks," 2018 Asia Communications and Photonics Conference (ACP), Hangzhou, 2018, pp. 1-3.

[68] "Actor-Critic-Based Learning for Zero-touch Joint Resource and Energy Control in Network Slicing".

[69] "Deep Deterministic Policy Gradient Based Dynamic Power Control for Self-Powered Ultra-Dense Networks".

[70] "Multi-Agent Deep Reinforcement Learning Based Virtual Resource Allocation Through Network Function Virtualization in Internet of Things".

[71] MAGNETIC, "Multi-Agent Machine Learning-Based Approach for Energy Efficient Dynamic Consolidation in Data Centers".

[72] "An Advanced Reinforcement Learning Approach for Energy-Aware Virtual Machine Consolidation in Cloud Data Centers".

[73] "REWARD DESIGN IN COOPERATIVE MULTI-AGENT REINFORCEMENT LEARNING FOR PACKET ROUTING".

[74] H. Park and Y. Lim, "Energy-effective power control algorithm with mobility prediction for 5g heterogeneous cloud radio access network," Sensors (Basel), vol. 6, pp. 8725–8741, 2018.

[75] A. Mohamed, O. Onireti, M. Imran, H. Pervaiz, P. Xiao and R. Tafazolli, "Predictive base sta- tion activation in futuristic energy-efficient control/data separated ran," in 2017 IEEE Globecom Workshops (GC Wkshps), pp. 1–7, 2017.

[76] X. Huang, S. Tang, Q. Zheng, D. Zhang and Q. Chen, "Dynamic femtocell gnb on/off strate- gies and seamless dual connectivity in 5g heterogeneous cellular networks," IEEE Access, vol. 6, pp. 21359–21368, 2018.

[77] Y. Mao, J. Zhang and K. B. Letaief, "Dynamic computation offloading for mobile-edge computing with energy harvesting devices," IEEE J. Sel. Areas Commun., vol. 34, no. 12, pp. 3590–3605, Dec. 2016.

[78] “https://community.fs.com/blog/understanding-the-tx-rx-optical-power-on-the-transceiver.html”.

[79] T.P. Lillicrap et al, “Continuous control with deep reinforcement learning,” in ICLR,2016.

[80] S. Fujimoto et al, “Addressing function approximation error in actor-critic methods,” in ICML,2018.

[81] T. Haarnoja et al, “Soft actor-critic: Off-policy maximum entropy deep reinforcement learning with a stochastic actor,” in ICML,2018.

[82] “https://pytorch.org/”.

[83] “https://gym.openai.com/”.