NATWORK

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

D2.1 SoA analysis & benchmark assessment

Lead beneficiary	UESSEX	**Lead author**	UESSEX
Reviewers	TSS, NOVA, CERTH		
Type	R	**Dissemination**	P
Document version	V1.0	**Due date**	30/06/2024

Co-funded by
the European Union

6GSNS

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

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

UK Research
and Innovation

Project information

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

Document information

Associated WP	WP2
Associated task(s)	T2.1
Main Author(s)	UESSEX
Author(s)	Mays AL-Naday (UESSEX), Vinh La (MONT), Edgardo Montes (MONT), Merlijn Sebrechts (IMEC), Francesco Paolucci (CNIT), Rana Abu Bakar (CNIT), Abdul Khan (CNIT), Bruno Volckaert (IMEC), Jaime Fúster (NEC), Roberto González (NEC), Péter Vörös (ELTE), Mohammed B. M. Kamel (ELTE), Károly Kecskeméti (ELTE), Joaquín Escudero (GRAD), J. Pose (GRAD), Nasim Nezhadsistani (UZH), Eryk Schiller (UZH), Antonios Lalas, Anastasios Drosou, Virgilios Passas, Sarantis Kalafatidis, Konstantinos Giapantzis, Nikolaos Makris, Ilias Syrigos, Georgios Agrafiotis (CERTH), Maria Safianowska (ISRD), Md Munjure Mowla (ISRD), Vincent Lefebvre (TSS)
Reviewers	Angelos Lampropoulos (NOVA), Vincent Lefebvre (TSS), Sarantis Kalafatidis (CERTH), Antonios Lalas (CERTH)
Type	R — Document, report
Dissemination level	P - Public
Due date	M6 (30/06/2024)
Submission date	30/06/2024

Co-funded by the European Union

Document version history

Version	Date	Changes	Contributor (s)
v0.1	01/03/2024	ToC added and assignments agreed (kick-off)	Mays AL-Naday (UESSEX)
v0.2	04/06/2024	Complete first version without introduction and summary sections	Mays AL-Naday (UESSEX), Virgilios Passas, Nikolaos Makris, Ilias Syrigos, Georgios Agrafiotis (CERTH), Vincent Lefebvre (TSS), Vinh La (MONT), Edgardo Montes (MONT), Merlijn Sebrechts, Bruno Volckaert (IMEC), Francesco Paolucci, Rana Abu Bakar, Abdul Khan (CNIT), Jaime Fuster, Roberto González (NEC), Mohammed B. M. Kamel, Péter Vörös, Károly Kecskeméti (ELTE), Joaquín Escudero (GRAD), Maria Safianowska, Md Munjure Mowla (ISRD), J. Pose (GRAD), Nasim Nezhadsistani (UZH), Eryk Schiller (UZH)
v0.3	11/06/2024	Complete executive summary, introduction, challenges and conclusions	Mays AL-Naday (UESSEX), Antonios Lalas, Anastasios Drosou, Sarantis Kalafatidis, Virgilios Passas, Konstantinos Giapantzis, (CERTH)
v0.4	12/06/2024	Complete draft, ready for review, track changes ON	Mays AL-Naday (UESSEX)
v0.45	13 /06/2024	Complete draft with integrated change requests from reviewers.	Mays AL-Naday (UESSEX), Angelos Lampropoulos (NOVA), Vincent Lefebvre (TSS)
v0.5	20/06/2024	Review complete and feedback to co-authors	Mays AL-Naday (UESSEX), Angelos Lampropoulos (NOVA), Vincent Lefebvre (TSS), Sarantis Kalafatidis (CERTH)
v0.6	26/06/2024	Pre-final version for production	Mays AL-Naday (UESSEX)
v0.7	27/06/2024	Final version delivered to COO	Mays AL-Naday (UESSEX)
v0.9	29/06/2024	Final review and refinements	Antonios Lalas (CERTH)
v1.0	30/06/2024	Final version for submission	Antonios Lalas (CERTH)

Disclaimer

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or 6G-SNS. Neither the European Union nor the granting authority can be held responsible for them. The European Commission is not responsible for any use that may be made of the information it contains.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the NATWORK consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the NATWORK Consortium nor any of its members, their officers, employees, or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the NATWORK Consortium nor any of its members, their officers, employees, or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

Content

List of acronyms and abbreviations 9

List of Figures 14

Executive summary 15

1. Introduction 16

1.1. Purpose and structure of the document 17

1.2. Indented Audience 18

1.3. Interrelations 18

2. Radio Access Network (RAN) 20

2.1. O-RAN open architecture and associated risks 20

2.2. Jamming in RAN 21

2.3. User access, security and mobility threats 22

2.3.1. DoS and DDoS Attacks 22

2.3.2. eSIM Security 23

2.3.3. Mobility-based Attacks 26

2.3.4. Radio Attacks 27

2.3.5. DDoS in RAN 29

3. Data-plane 30

3.1. Data plane threats 30

3.2. GTP-U, SIP protocol and IoT protocol-based threats 31

4. Orchestration and management plane 33

4.1. Orchestration and management challenges 33

4.2. ML based orchestration threats 34

4.2.1. Machine Learning Security Challenges 35

4.2.2. AI-based Attacks 37

4.2.3. Net-Zero Projects 38

5. Clouds: edge-to-core 39

5.1. Network core threats 39

5.2. Edge runtime Management and workload isolation 41
5.3. Edge-clouds threats 42
6. Data & Privacy 44
6.1. Data privacy regulation landscape and challenges 44
7. Affected network service KPIs 47
7.1. Performance 47
7.2. Security 49
7.3. Reliability 53
7.4. Energy 54
7.5. Cost 56
8. Solutions and Technologies 58
8.1. Security-by-Design 58
8.1.1. Workload isolation 59
8.2. Trust management 63
8.2.1. Trust between actors 63
8.2.2. Trust of systems and assets 65
8.2.3. E2E trust assessment 68
8.3. Attack detection & Protection 68
8.3.1. RAN Jamming detection and protection 68
8.3.2. Multi layer DDoS detection and protection 70
8.3.3. Edge/MEC attacks detection and protection 74
8.3.4. Smart orchestration by Moving Target Defence 75
8.4. Machine Learning Frameworks for CTI Analysis 76
8.5. Service accurate monitoring and traceability 80
9. Roadmap summary 83
9.1. Priority challenges 83
9.1.1. Scalability and Performance 83
9.1.2. Security and Privacy 84
9.1.3. Energy Efficiency and Sustainability 84

10. Conclusions 86

References 87

List of acronyms and abbreviations

Abbreviation	Description
3GPP	3rd Generation Partnership Project
ABI	Application Binary Interface
AI	Artificial Intelligence
ANN	Artificial Neural Networks
AOT	Ahead Of Time
APT	Advanced Persistent Threats
AS	Autonomous System
ASNs	Autonomous System Numbers
BS	Base Station
BCI	Brain-computer interactions
C2C	Command and Control
CapEx	Capital Expenditures
CCPA	California Consumer Privacy Act
CDH	Computational Diffie-Hellman
CDN	Content Delivery Network
CNF	Cloud-native Network Function
CNFs	Containerized Network Funtions
CNN	Convolutional Neural Networks
CPU	Central Processing Unit
CTC	Cyber Threat Coalition
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service
DiD	Defence in Depth
DLT	Distributed Ledger Technologies
DNS	Domain Name System
DOM	Document Object Model
DoS	Denial of Service
DoSt	Denial of Sustainability
DPI	Deep Packet Inspection
DRL	Deep Reinforcement Learning
DSM	Distributed Slice Mobility
DT	Decision Tree
EBC	Extreme Bandwidth Communication
EDoS	Economic Denial of Sustainability
ENISA	European Union Agency for Cybersecurity
ESC	Environmental Sensing Capability
eSIM	Embedded Subscriber Identity Module

ETSI	European Telecommunications Standards Institute
eUICC	Embedded Universal Integrated Circuit Card
EIH	Eavesdropping/Interception/Hijacking
FDD	Frequency Division Duplex
FGSM	Fast-Gradient Sign Method
FLOPS	Floating-Point Operations per Second
FNN	Feedforward Neural Network
GAN	Generative Adversarial Networks
GDPR	General Data Protections Regulation
GHG	Greenhouse Gases
GPUs	Graphics Processing Units
GRU	Gradient Recurrent Unit
GTP	GPRS Tunneling Protocol
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technologies
IDL	Interface Description Language
IDS	Intrusion Detection Systems
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IoC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
ISD-Ps	Issuer Security Domain-Profiles
JIT	Just In Time
KNN	K nearest neighbor
KPIs	Key Performance Indicators
KVM	Kernel-based Virtual Machine
LDAP	Lightweight Directory Access Protocol
LLMs	Large Language Models
LoR	Logistic Regression
LR	Linear Regression
LSTM	Long Short Term Memory
LTE	Long Term Evolution
MAC	Medium Access Control
MANO	Management and Orchestration
Mbps	Megabits per second
MEC	Multi-Access Edge Computing
MFA	Multi-factor Authentication

MIMO	Multiple-Input Multiple-Output
MitM	Man-in-the-middle
ML	Machine Learning
mMIMO	Massive Multiple-Input Multiple-Output
mMTC	massive Machine-Type Communications
mmWave	milimeter Wave
MNO	Mobile Network Operator
MSSQL	Microsoft Structured Query Language Server
MTD	Moving Target Defence
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
MU-MIMO	Multi-User MIMO
MQTT	MQ Telemetry Transport
NB	Naive Bayes
NetBIOS	Network Basic Input / Output System
NFV	Network Function Virtualisation
NN	Neural Network
Non-RT RIC	Non Real-Time RAN Intelligent Controller
NR	New Radio
NS	Name Server
NT	Network Tomography
NTP	Network Time Protocol
NAA	Nefarious Activity/Abuse of Assets
OCI	Open Container Interface
O-RAN	Open Radio Access Network
ODL	Open Daylight
ONAP	Open Network Automation Platform
ONF	Open Networking Foundation
ONOS	Open Network Operating System
OpEx	Operational Expenditures
OS	Operating System
OSM	Open Source MANO
OSS	Operation Support Systems
OTA	Over The Air
SBC	Single-Board computers
SBoM	Software Bill of Materials
SFC	Service Function Chaining
SMF	Session Management Function
SM-SR	Subscription Manager-Secure Routing
SotA	State of the Art
SSDP	Simple Service Discovery Protocol

TPM	Trusted Platform Module
PBCH	Physical Broadcast Channel
PCA	Pilot Contamination Attack
PDCCH	Physical Downlink Control Channel
PDCP	Packet Data Convergence Protocol
PDSCH	Physical Downlink Shared Channel
PDR	Packet Delivery Ratio
PER	Packet Error Rate
PFCP	Packet Forwarding Control Protocol
PHA	Potentially Harmful Applications
PHY	Physical Layer
PLA	Physical layer authentication
PLS	Physical layer security
PPCP	Packet Data Convergence Protocol
PRACH	Physical Random Access Channel
PRB	Physical Resource Block
PSS	Primary Synchronization Signal
PUCCH	Physical Uplink Control Channel
PUSCH	Physical Uplink Shared Channel
PUP	Potentially Unwanted Program
RAN	Radio Access Network
RDF	Resource Description Framework
RF	Random Forest
RLC	Radio Link Control
RNN	Recurrent Neural Network
RoT	Root of Trust
RSS	Received Signal Strength
SDN	Software Defined Network
SDO	Standard Development Organization
SEEM	Secrecy Energy Efficiency Maximization
SIP	Session Initiation Protocol
SKG	Secret Key Generation
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSS	Secondary Synchronization Signal
STIX	Structured Threat Information Expression
SVM	Support Vector Machine
TDD	Time Division Duplex
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TFS	Technical Framework Specification

Co-funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI
UK Research and Innovation

TLS	Transport Layer Security
TPUs	Tensor Processing Units
TTPs	Trusted Third Parties
UCO	Unified Cybersecurity Ontology
UDP	User Datagram Protocol
UE	User Equipment
UPF	User Plane Function
UPIP	User Plane Integrity Protection
URLLC	Ultra-reliable low-latency communication
VIM	Virtual Infrastructure Manager
VM	Virtual Machine
VMI	Virtual Machine Introspection
VoLTE	Voice over Long-Term Evolution
WAMR	WebAssembly Micro Runtime
WASI	WebAssembly System Interface
WIT	WebAssembly Interface Type
Wasm	WebAssembly
XAI	Explainable Artificial Intelligence
OTA	Over-the-Air
EIS	Embedded Universal Integrated Circuit Card Information Set
SM-DP	Subscription Manager Data Preparation
SM-SR	Subscription Manager-Secure Routing
ZSM	Zero touch network and Service Management
ZTA	Zero Trust Architecture

List of Figures

Figure 1 Simplified schematic overview of application-level containers. 61

Executive summary

6G is emerging as the next generation of mobile networks, integrating tactile and mission-critical application domains with significant impact on daily lives. To enable a sustainable 6G ecosystem, with reliable operation of its services and confidence in maintaining service level agreements, there is a critical need to tackle the cybersecurity challenges emerging with 6G propositions. Some of such challenges are inherited from 5G as they have not been fully addressed, while others are novel with the adoption of new enablers. The latter is particularly true with the adoption of AI, introducing new risks to AI security as well as data privacy. The mission of the NATWORK project is to develop a flexible and adaptive cybersecurity framework of solutions that are sustainable and adaptive to 6G threats and cascade attacks against 6G infrastructure and/or its services.

To be able to develop such efficient and adaptive cybersecurity solutions that meet 6G expectations, there is need first to analyse the foreseen security challenges associated with emerging propositions of the 6G architecture and its requirements; and review the landscape of threats and attacks already perceived in 5G and how they can evolve in 6G. Particularly, taking into account the infrastructure complexity and expectation of frictionless provision of services and seamless management over multiple autonomous 6G systems. It is further required to review state-of-the-art cybersecurity solutions, adopted in various domains relevant to 6G and assess their adoption in 6G to counter expected threats.

This document comprehensively reviews state-of-the-art in cybersecurity of 5G and 6G networks, services and relevant technologies. It analyses the challenges associated with various components in 6G, from the radio access to the core network and from edge to core clouds. The document provides a detailed analysis of AI application for cybersecurity in 5G/6G and the security of AI when adopted in network operations. It further reviews challenges and threats to data privacy when sharing for AI training. Complementarily, the document reviews the affected threat mitigations KPIs by different types of attacks along with state-of-the-art cybersecurity solutions adopted in the various relevant domains. The above are used to set the priority challenges of the NATWORK project and guide the research and innovation efforts in cybersecurity solutions, within the technical work packages in the rest of the project timeline.

1. Introduction

6G is emerging as the next generation in mobile networks and services. The architectural design is still in the making with several European and international efforts defining the requirements, functions, components, capacities and enablers. The main differentiators of 6G are: the expansion towards Terahertz wireless radio communications; connecting vulnerable end-devices at a much larger scale; the integration of AI in network operations from the edge to the core and on multiple planes (management, control, data); and, frictionless cloudification of network and user services over multiple clouds [Ziegler2020, Alwis2021, Porambage2021, Bhat2021, Jiang2021, Quy2023]. Added to that, 6G end-to-end requirements are expected to have a new level of stringency. They specify ultra-reliable low-latency communications (URLLC), ultra-fast recovery and resiliency, energy efficiency and sustainability and privacy preservation and security by design [Nguyen2020, Nguyen2021, Porambage2021, Quy2023].

The prospects above introduce several cybersecurity challenges and threats of attacks, some of which are novel (such as AI trustworthiness and dependency on datasets), requiring scalable, adaptive and efficient solutions. For a start, the adoption of AI in network management and control requires establishing confidence and 'trust' in the logic of decisions, made by the machine learning models (ML) used in AI services. The field of explainable AI (XAI) is working building confidence, through explainability of decisions. But this is still primitive in maturity, when considering AI integration in mission and time critical operational environments. Added to that, the dependency of AI on datasets introduces novel cybersecurity threats in manipulating data to influence AI decisions. On the other hand, AI has an emerging use in launching targeted and intelligent attacks circumventing existing access control, detection and protection solutions. Such threats and attacks have not been addressed in current state-of-the-art, nor their impact on stakeholders in 6G ecosystems. There is a need to analyse AI-related challenges, vulnerabilities and threats to develop suitable counter measures.

ENISA provides a comprehensive risk modelling of the 5G ecosystem [ENI2024], categorized according to the following threat taxonomy: Nefarious Activity/Abuse of Assets (NAA), Eavesdropping/Interception/Hijacking (EIH), Physical Attacks (PA), Unintentional Damages (UD), Failures or Malfunctions (FM), Outages (OUT), Disasters (DIS), and Legal (LEG). The threat taxonomy is matched with vulnerabilities according to the STRIDE method, which includes Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege in various places of the 5G system. Finally, a detailed list of vulnerabilities is provided for various components, including the Core Network (CN), network slicing, Radio Access Network (RAN), Software-Defined Networks (SDN), Multi-Access Edge Computing (MEC), physical infrastructure, implementation options, Mobile Network Operator (MNO) processes, vendor processes, and security assurance processes.

Orthogonally, there is a new scale of complexity in service and resource management in 6G, with emerging need for cooperation and coordination across autonomous cloud and network systems. This comes with 6G adoption of the cloud-native paradigm and the target of frictionless service provisions over multiple clouds, extending from the edge to the core and including the new radio access. This means a typical 6G service will likely be managed by multiple entities, such as a cloud orchestrator(s) and SDN controller(s). These entities will need to coordinate their threat intelligence sharing and decision-making processes, not only to protect against cascade attacks but more so to provide security-by-design orchestration.

The importance of availability, particularly for URLLC services, cannot be overstated. However, the increased complexity and interconnectivity of 6G networks also broaden the attack surface for malicious actors. From Distributed Denial of Service (DoS/DDoS) attacks to Economic Denial of Sustainability (EDoS/DoSt) attacks and sophisticated energy harvesting manipulations and routing attacks, the potential for disruption is vast and varied. Furthermore, physical layer attacks, malware, ransomware, and mobility-based attacks pose significant risks not only to network functionality but also to energy efficiency, crucial for achieving net-zero energy goals. To address these multifaceted challenges in 6G ecosystems, comprehensive security frameworks, innovative mitigation strategies, and collaborative efforts among industry stakeholders are essential [Scalise2024].

An overarching target in any cybersecurity solutions that address 6G challenges is that they must be sustainable; in cost, energy consumption and the induced CO2 footprint. At the current stage there is no clarity on the energy requirements to meet 6G expectations, nor a mature understanding of the potential energy threats to 6G, abusing resource-intensive services. To be able to design sustainable cybersecurity solutions, there is a need to analyse the current state of the art of solutions and their environmental, as well as socio-economic cost in 6G systems. There is further need to analyse emerging threats of energy exhaustion in 6G to be able to device suitable detection and protection from energy-related attacks that renders a 6G deployment and/or service unsustainable.

1.1. Purpose and structure of the document

This document provides a comprehensive state of the art review of the cybersecurity challenges foreseen in the road toward 6G adoption, summarizing the potential threats and attacks and existing technologies and solutions to tackle them, with a special consideration on sustainability.

The document comprehensively covers 6G components and is structured with sections focused on the radio access, the data plane, the orchestration and management plane and the edge-to-core cloud. These sections cover the associated risks brought by network function virtualization

(NFV), the payload security, runtime (virtualization) security, AI security and AI-for-security in 6G as well as data privacy. The latter is covered with a separate section as being a key user and E.U concern notably for the adoption of novel 6G user centric services. Moreover, the document analyses the affected mitigation solutions KPIs by different threats and their impact in a 6G ecosystem. The wide coverage of state-of-the-art literature and solutions is then utilized to summarise the priority challenges for the NATWORK project and guide the upcoming research and innovation to address them.

The remainder of this document is structured as follows:

- **Section 2** covers the security and sustainability challenges on the RAN,
- **Sections 3, 4 and 5** cover the same challenges on the Data plane, the orchestration and management plane and edge to core clouds, respectively,
- **Section 6** covers the challenges and threats on Data and privacy,
- **Section 7** addresses the affected network KPIs.
- **Section 8** covers state-of-the-art security solutions and technologies at play to mitigate identified 5G/6G threats.
- **Section 9** brings NATWORK’s road map summary, and
- **Section 10** draws the document conclusions.

1.2. Intended Audience

The NATWORK Project’s SoA analysis & benchmark assessment is devised for public use in the context of preparatory SoA analysis & benchmark assessment of the NATWORK consortium, comprising members, project partners, and affiliated stakeholders. This document mainly focuses on the SoA analysis & benchmark assessment methodologies, challenges, and anticipated benchmarks of the project, thereby serving as a referential tool throughout the project's lifespan.

1.3. Interrelations

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

NATWORK is categorized as a "Research Innovation Action - RIA" project and is methodically segmented into 7 WPs, further subdivided into tasks. With partners contributing to multiple activities across various WPs, the structure ensures clarity in responsibilities and optimizes communication amongst the consortium's partners, boards, and committees. The interrelation framework within NATWORK offers smooth operation and collaborative innovation across the consortium, ensuring the interconnection of the diverse expertise from the various entities (i.e., Research Institutes, Universities, SMEs, and Large industries) enabling scientific, technological, and security advancements in the realm of 6G. The SoA analysis & benchmark assessment, addresses all SoA activities of the NATWORK project workplan to provide the initial guidelines for the development purposes of the technical WPs, such as WP3, WP4, and WP5, as well partially WP6.

2. Radio Access Network (RAN)

2.1. O-RAN open architecture and associated risks

Several reports have been published that analyse the security challenges of the RAN networks, especially considering the openness aspect, which is gaining prominence in the 6G developments. [BSI2022] identifies the following security risks: O-RAN development process not following security/privacy by design/default, lack of specification & optionality introduces considerable risks, rights & roles concept not sufficiently defined, and selection of security protocols does not always follow best security practices. [CISA2022] identifies the following concerning factors: changing threat surface due to network disaggregation, security considerations related to open-source software and security concerns not unique to Open RAN, e.g., cloud risks, secure virtualization/containerization, and Distributed Denial of Service (DDoS) attacks. [IFRI2022] emphasizes the following challenges: increased risk of misconfiguration and vulnerabilities in low-quality components, larger attack surface, potentially greater reliance on unreliable (e.g., open-source) components & vendors, and risk of increased dependency on foreign suppliers. [NTT2021] further amplifies these concerns, listing: security issues of open-source software and off-the-shelf technologies, increased threat surface due to exposed interfaces, security issues related to added RAN functions, higher probability of physical attacks, cloud security issues, and process vulnerabilities. Also, [NIS2022] adds the following to the list: expanded threat surface, increased complexity for network fault management, deficiencies in technical specifications, increased dependency on infrastructure providers, impacts on network security and performance due to mix-and-match, and security risks due to resource sharing.

The most recent report on Open RAN security challenges is a study [Quad2023] which develops a categorization of security risks for Open RAN networks, reviews existing expert reports, and considers how to set conditions in a neutral and non-biased manner. Based on the developed methodology, a total of 1338 unique security threats have been identified. It then performs comparative study of Open RAN and traditional vertically integrated networks. In addition, it provides a resulting overall risk rating and highest risk components of Open RAN. Finally, based on the analysis, the report identifies the following major security challenges of Open RAN:

- Increased RAN attack surface;
- AI/ML related risks;
- Cloud related risks;
- Unreliable vendors and open-source software related risks;
- Stakeholder management and process challenges.

2.2. Jamming in RAN

Despite over forty years of evolution, cellular networks remain susceptible to jamming attacks. This vulnerability primarily stems from the absence of practical and efficient anti-jamming techniques at the wireless PHY/MAC layer, necessary for securing radio packet transmissions amidst jamming signals. The vulnerability also accentuates the critical need for an in-depth understanding of jamming attacks and for more research efforts on the design of efficient anti jamming techniques.

In a recent survey [Priyadarshani2024] the authors investigated prevalent jamming attacks and the corresponding countermeasures in EBC technologies such as millimeter wave, terahertz, free-space optical, and visible light communications. They classified the jamming attacks such as proactive, reactive, and advanced jammers. There are several jamming mitigation techniques such as regulated transmit power, spread spectrum techniques, spatial diversity, jamming filtering, adaptive coding and modulation, RIS, game theory, and AI/ML. Author [Pirayesh2022] conducted a comprehensive analysis of existing anti-jamming strategies in wireless networks, covering techniques such as power control, spectrum spreading, frequency hopping, MIMO-based jamming mitigation, and jamming-aware protocols. They also provided a literature review on jamming attacks and countermeasures within emerging wireless technologies, including mmWave communications and learning-based wireless systems.

An overview of jamming attacks and their mitigation techniques on 5G communications was presented where the author analysed the vulnerability of 5G NR to jamming, spoofing, and sniffing by looking at individual physical channels and signals [Lichtman2018]. Arjoune et al. presented state-of-the-art detection and mitigation techniques [Arjoune2020] and discussed their suitability to defeat smart jammers in 5G wireless networks. The study highlighted that while 5G New Radio (NR) enhances network resilience against jamming through dynamic resource allocation, it remains susceptible to sophisticated jamming attacks. This underscores the necessity for advanced research into robust anti-jamming strategies for 5G systems. In these papers, mostly the authors studied the different vulnerabilities of the NR physical layer to jamming attacks. Similar to LTE, it was shown that the NR physical channels and signals could be targeted by network-specific jamming attacks. In particular, the authors studied jamming attacks on PSS, SSS, PBCH, PDCCH/PUCCH, PDSCH/PUSCH, PRACH, and reference signals. In order to carry out jamming attacks on NR synchronization signals, the jammer must possess detailed knowledge of the system configurations, including the subcarrier spacing and the offset-ref-low-scs-ref-PRB parameter, which are crucial for pinpointing the position of the PSS/SSS within the frame. Sheikhi et al. [Sheikhi2020] compared how power-optimized jamming attacks affect the spectral efficiency of FDD and TDD massive MIMO systems. Utilizing the channel reciprocity in TDD mode, the jammer manipulates the estimated uplink channels to refine its jamming strategy for the downlink. In FDD mode, the jammer leverages the second-order statistics of the channels to craft the jamming signal.

Recently, the PHY-layer vulnerability of 5G cellular networks has been investigated for learning-based applications. Sagduyu et al. [Sagduyu2021] introduced an adversarial attack designed to deceive the deep learning model utilized for dynamic spectrum allocation in 5G networks. This scheme involves the deliberate transmission of well-designed jamming signals during the sensing or data transmission phases, with the objective of manipulating the input to the Environmental Sensing Capability (ESC) classifier within the 5G system. Kim et al. [Kim2021] developed a malicious attack on learning-based beam pattern prediction in 5G mmWave networks. Their scheme involves introducing perturbations to the neural network input, disrupting the classification of beam patterns by legitimate 5G users. Furthermore, they devised perturbations to compel the neural network to select suboptimal beam patterns.

Shi et al. [Shi2021] explored the susceptibility of learning-based network slicing in 5G networks. Their approach involves a power-constrained jammer constructing a reinforcement learning model to monitor channels and disrupt Physical Resource Blocks (PRBs) to maximize the disruption of network slicing requests. Simulations revealed that while machine learning promises enhanced reliability and efficiency for 5G networks, it is significantly vulnerable to adversarial attacks, posing a threat to 5G performance degradation. It is worth mentioning that these Jamming attacks on cellular networks often necessitate precise timing synchronization to effectively disrupt specific control signals. Given that synchronization signals are broadcast periodically, malicious attackers can readily obtain the necessary timing information. Consequently, these targeted jamming attacks represent a significant threat to cellular networks.

2.3. User access, security and mobility threats

2.3.1. DoS and DDoS Attacks

Access availability is paramount for ensuring uninterrupted communication and service delivery in 6G networks. DDoS attacks exploit vulnerabilities in network infrastructure, causing outages and disrupting connectivity for users. These attacks often target critical resources such as servers, routers, and bandwidth, crippling the network's ability to handle legitimate traffic. As 6G networks are expected to support a myriad of applications, including URLLC services, ensuring high availability becomes even more critical to meet stringent performance requirements. DDoS attacks hinder accessibility by saturating network links and degrading the quality of service for legitimate users. The excessive traffic can lead to increased power consumption as infrastructure components work harder to process and mitigate the bogus requests [Naser2023]. This can have profound implications for applications that rely on real-time data transmission, such as autonomous vehicles and remote healthcare systems. Ensuring equitable access to network resources while mitigating the impact of malicious attacks requires a comprehensive security framework that proactively identifies and mitigates potential threats. The acceptability of a 6G network hinges on its perceived reliability, security, and resilience. DDoS attacks undermine acceptability by disrupting services and eroding user trust in the network infrastructure. Moreover, the proliferation of interconnected devices and the Internet of Things exacerbates the attack surface, increasing the likelihood of successful infiltration by malicious actors [Chen2024].

To enhance acceptability, network operators must invest in robust security measures, conduct regular risk assessments, and collaborate with stakeholders to address emerging threats effectively. Affordability encompasses the economic viability of accessing and utilizing network services. DDoS attacks can incur significant financial losses due to downtime, mitigation costs, and reputational damage. For businesses and organizations, the affordability of 6G network services depends on the ability to mitigate these risks while maintaining cost-effective operations. Investing in scalable security solutions, leveraging artificial intelligence and machine learning for anomaly detection, and adopting resilient network architectures can help mitigate the financial impact of DDoS attacks and ensure the long-term affordability of 6G networks. To address the threat of DDoS attacks in 6G networks, a multi-faceted approach to security is necessary. This includes deploying intrusion detection and prevention systems (IDPS), implementing traffic filtering mechanisms, and leveraging DDoS mitigation techniques. Additionally, fostering collaboration among industry stakeholders, government agencies, and cybersecurity experts is essential for sharing threat intelligence and best practices. By proactively identifying vulnerabilities and implementing robust security measures, the 6G ecosystem can mitigate the risk of DoS/DDoS attacks and ensure the resilience and integrity of communication networks [Musa2024, Scalise2024].

2.3.2. eSIM Security

Embedded Subscriber Identity Module (eSIM)-based identities and provisioning offer opportunities for innovation and growth in IoT ecosystems. For instance, eSIMs can enable new business models and revenue streams for service providers, such as pay-on-use subscriptions and dynamic network selections. They also facilitate adopting new IoT applications, including connected vehicles and smart homes or cities [Krish2024]. A European Union Agency for Cybersecurity (ENISA) study examines the security challenges of eSIM technology, highlighting issues like bloated and locked profile attacks, memory exhaustion, undersized memory exploits, and eSIM swapping [Bafo2023]. These vulnerabilities can allow attackers to disrupt services or steal confidential data. While there have been few recorded cybersecurity incidents, the widespread deployment of IoT devices and increased use of eSIMs could lead to more cyber events. Key challenges in IoT implementations include the time-consuming and costly provisioning and administration of devices. Secure provisioning of services, which involves granting access to data, applications, and updates, is crucial but traditionally requires human intervention, increasing the risk of errors and attacks. eSIMs present an alternative to these issues. Another major challenge is the need for a common standard for eSIM technology, leading to potential interoperability problems between different devices and networks. Ensuring reliable Over-the-Air (OTA) management requires robust security protocols and infrastructures, which can be difficult to implement in remote or challenging environments.

Risk 1: eSIM Swapping: Attackers can perform eSIM swapping by obtaining personal data and claiming device damage to gain access to the subscriber's account on the Mobile Network Operator (MNO)'s portal. They initiate an eSIM swap and scan the displayed QR code to activate the profile. This can lead to profile deactivation, loss of connectivity, unauthorized access, and potential espionage. Tools like Simjacker exploit SIM toolkit instructions to manipulate profiles and intercept subscriber credentials.

Risk 2: Memory Exhaustion: Memory exhaustion attacks deplete the Embedded Universal Integrated Circuit Card (eUICC)'s memory resources, preventing it from providing the related services. By exploiting the remote provisioning procedure's error handling, attackers can fill the eUICC's memory with empty Issuer Security Domain-Profiles (ISD-Ps), leading to orphaned profiles. This can result in financial loss for MNOs and make device recovery impossible. The attack is complex to trace as it leaves no evidence besides lost messages.

Risk 3: Under sizing Memory: A malicious Subscription Manager-Secure Routing (SM-SR) component can prevent profile installations by manipulating the 'remaining Memory' field in the Embedded Universal Integrated Circuit Card Information Set (EIS) file to zero. This stops new profile uploads and can remain undetected, especially in devices with multiple profiles. The attack disrupts MNO and Subscription Manager Data Preparation (SM-DP) operations and hampers service provisioning.

Risk 4: Inflated Profile: An inflated profile attack, initiated by a compromised SM-DP or malicious MNO, exhausts the eUICC's available memory by creating a profile that fits the memory size. This prevents other operators from storing profiles on the eUICC. The attack can be detected only if the profile leaves sufficient memory for new profiles.

Risk 5: Locking Profile A malicious MNO: a device can be locked to a specific network by installing a profile with a modified POL1 (data describing the Policy Control Functions in a profile) file that includes the 'Can not Be Disabled' rule. This action turns off other profiles and prevents MNOs from deleting the compromised profile, effectively locking the eUICC to a particular network. This tactic can be used for cyberwarfare, supply chain attacks, or competitive blocking.

Risk 6: Protocol Attacks: Attackers persuade users to install malicious applications or compromised apps containing malicious code. These apps can access sensitive information, such as phone numbers and messages, especially on rooted devices. Attackers can launch 'man-in-the-middle' attacks and traffic eavesdropping by acquiring security files as plaintexts. The lack of user security awareness facilitates these attacks.

Risk 7: Attacks on MNOs and the eSIM Supply Chain: Attackers target MNOs and other entities in the eSIM supply chain, including software developers and product manufacturers. By accessing secure source codes and infecting legitimate apps, they can spread malware and leak information. Such attacks erode trust in the provisioning delivery supply chain and disrupt operations.

Risk 8: SIM Data Extraction: This attack involves extracting sensitive data stored on the eSIM, such as authentication keys, user profiles, and other personal information. Attackers might use physical attacks, side-channel attacks, or software exploits to gain access to the data stored on the eSIM. Extracted data can be used for various malicious purposes, including cloning the eSIM to impersonate the user, accessing the user's network services, or selling the information on the black market. It compromises user privacy and can lead to significant financial and reputational damage.

Several measures can be implemented to counter the risks associated with eSIM technology. For eSIM swapping, enhanced authentication methods such as Multi-Factor Authentication (MFA) should be used to secure account access and profile changes. Monitoring systems can detect unusual activities, such as multiple swap requests, and alert users and administrators. Ensuring that QR codes for profile activation are secured and accessible only through authenticated sessions can also help prevent unauthorized access.

To address memory exhaustion attacks, request throttling can limit the number of provisioning requests within a specific timeframe, preventing resource exhaustion. For undersized memory attacks, integrity checks on EIS can detect and prevent manipulation. Inflated profile attacks can be mitigated by implementing strict validation checks for profile sizes before installation and setting policies to limit the maximum memory a single profile can occupy. Monitoring memory usage and profile installations can help detect and respond to potential inflation attacks. For locking profile risks, implementing policies to prevent modifications to POL1, developing mechanisms to revoke or disable compromised profiles, and ensuring prompt notification and recovery processes are essential.

To counter protocol attacks, users should be encouraged to download apps only from trusted sources and keep their devices updated with security patches. App permissions should be limited, especially those requiring sensitive information or root access. Promoting security awareness among users helps them recognize and avoid malicious applications while implementing root detection mechanisms prevents apps from running on rooted devices.

To protect against attacks on MNOs and the eSIM supply chain, conducting thorough security assessments, regular audits, and compliance checks are necessary. Countermeasures against SIM data extraction will ensure that the remote provisioning of eSIM profiles is conducted over secure channels, which is crucial for maintaining security. This involves using strong encryption and authentication mechanisms to protect the data transmitted between the mobile network operator (MNO) and the eSIM. Secure provisioning prevents unauthorized access during profile download and installation, ensuring that only legitimate profiles are added to the eSIM. Using eSIMs with tamper-resistant hardware is essential for enhancing physical security. Tamper-resistant eSIMs are designed to resist physical attacks and make data extraction significantly more difficult. These hardware components are equipped with protective measures such as secure memory, cryptographic modules, and physical shielding. These features prevent attackers from accessing sensitive information stored on the eSIM through physical manipulation or hardware-based exploits. By integrating tamper-resistant hardware, manufacturers can ensure higher security, protecting the eSIM from physical breaches and enhancing overall data protection.

2.3.3. Mobility-based Attacks

Mobility-based attacks in 6G networks pose significant challenges, particularly given the intricate interplay between high mobility and the need for seamless, secure connectivity. These attacks, such as location spoofing, handover disruptions, routing manipulations, relay attacks, sybil attacks, man-in-the-middle (MitM) attacks and timing attacks, exploit vulnerabilities that arise from the constant movement of devices. For instance, attackers can manipulate handover protocols to force frequent transitions between cells, leading to increased signalling overhead and inefficient use of network resources. Similarly, false routing information can disrupt the optimal flow of data, causing increased retransmissions and higher energy consumption as the network struggles to maintain connectivity [Liu2021].

From the perspective of achieving net-zero energy consumption, mobility-based attacks can have a particularly detrimental impact. Efficient energy use is a cornerstone of net-zero initiatives, and the additional processing and communication overhead caused by such attacks directly contradict these goals. For example, excessive handovers triggered by handover attacks or the need to reroute data multiple times due to routing attacks can lead to increased energy expenditure in both network infrastructure and mobile devices. This heightened energy usage not only raises operational costs but also escalates the carbon footprint of the network. Addressing these security vulnerabilities is thus essential not only for maintaining robust and reliable connectivity but also for ensuring that the sustainability targets of 6G networks are met [Saeed2023, Naser2023].

2.3.4. Radio Attacks

Although 5G is supposed to be 90% more efficient than 4G in terms of energy consumption per unit of traffic W/Mbps [Williams2022], the total increase in traffic due to enhanced capabilities that 5G New Radio provides is somehow debated, with Ericsson suggesting that is possible to quadruple the data traffic without increasing network energy consumption with the modernization of infrastructure and its management with the help of AI, the use of energy saving software and optimizing 5G network performance [Ericsson2020]. However, as mentioned in [Williams2022], the methods and data used to these estimations are not publicly available, so conclusions are difficult to draw from them. However, these predictions are made based on a normal behaviour of the network, which can be disrupted by several attacks. Focusing first on the physical layer, some of the most prominent ones are jamming, eavesdropping and pilot contamination attacks.

2.3.4.1. Jamming

Jamming is a Denegation of Service attack type, defined as the generation of interference with the objective of preventing legitimate communications in any wireless network. There are several types of jamming strategies, mostly focused on using the less possible power to effectively disrupt communications, as the generation of interference with enough strength is very supply demanding. Some of them are [Pirayesh2022]:

- Constant jamming: the simplest one, radiating a signal in all available bandwidth without interruption.
- Random jamming: instead of always being active, this jamming turns on and off at random time periods, saving power proportional to the amount of time that it is turned off.
- Periodic jamming: similar to the previous one, but it switches between attacking and sleep periodically instead of randomly (which makes it easier to detect but, in some scenarios, more effective due to some communications in 5G and other networks are periodic too).
- Reactive jamming: more complex than the previous ones, it sniffs the link and only attacks when detects that a legitimate communication is taking place (the disadvantage is that it may have a delay in its attack).

In general, for a jamming attack to be more effective and efficient, it needs more information and understanding of the network behaviour. In particular, some 5G sequences such as PSS and PBCH are some of the less complex and effective jamming spots to prevent users from accessing network as shown in [Lichtman2018], which compares different 5G signals in terms of their complexity and power efficiency as a measure between the average received jammer power and the signal power, over one 5G frame).

The effects of jamming in network energy consumption are harmful in general. Detection and countermeasures usually involve additional processing which will lead to an increase in energy consumption. Furthermore, there is a concept known as "energy harvesting" from a jamming attack, as shown for example in [Al-Hraishawi2023] which interestingly proposes a scheme that enables multiple legitimate users to harvest energy from surrounding multiple jamming attacks in a 5G and beyond mMIMO scenario, where there exists a trade-off between the amount of energy obtained and the achievable sum rate, increasing the transmitted power or the overall system performance [Al-Hraishawi2021] (previous study on a non-multiple users scenario). Other applications of that harvested energy are shown in [Belmega2017], used to generate a secret key (SKG) and in [Rezgui2019], where the legitimate user can neutralize the jammer attack by tuning the transmit power and the energy harvesting duration.

2.3.4.2. Other radio attacks

Eavesdropping is a type of attack against users' privacy, in which the attacker tries to obtain the data exchanged between gNodeB and UE in 5G. At its core, it is a passive attack, which makes it undetectable, but it can only obtain unencrypted data (although it is possible to extract statistical information about the communications even with encrypted messages). In 5G networks, that is the case of broadcast messages (like the SSB for example) and the first messages with the UE when it starts the synchronization procedure to access the network. As a passive attack it does not impact directly in the energy consumption; however, popular countermeasures as the injection of artificial noise [JindanXu2020] effectively demands large amounts of power usage, as the scheme requires to use beamforming to send the data signal correctly to their legitimate receiver and also needs to radiate artificial noise (like a jamming attack against possible eavesdroppers) over the rest of the transmission directions. In [Chen2020], energy efficiency is considered using a constraint on the total transmitted power on their algorithm (namely, Secrecy Energy Efficiency Maximization (SEEM)).

On 6G scenarios, [Mitev2023] explains the use of secret key generation (SKG) applying the channel between Alice and Bob and the importance of focusing on short coding block length scenarios (as secrecy capacity [Wyner1975] increases with block length, but this is a constraint in realistic scenarios). This paper also mentions and explains the use of hybrid crypto systems in combination with the SKG, which let optimize the problem imposing new constraints, such as channel capacity or power (which could be interesting to achieve net-zero scenarios). In [Li2020], the authors propose a Physical Layer Security (PLS) scheme combined with an edge caching scenario (storing contents requested by users on edge servers) with two hops (if a BS does not have the content in cache, it requests this from another BS to send it to the user) optimizing the secure transmission probability, which is broken apart into connection probability and confidentiality probability, optimizing the redundancy rate jointly with the caching probability.

With more knowledge of the network, attackers can use legitimate signals to try to impersonate a node. The so called **pilot contamination attacks** (PCA) are based on using pilot signals (some of them can be replicated, computing the sequence and locating it in time and frequency following the 3GPP standard for 5G for example) which can lead to DoS due to mistakes in the channel estimation or help to eavesdrop signals when that channel estimation is used in the beamforming, which would be made using the deceptive pilot. Other advanced attack is the spoofing, which is also the use of legitimate signals, usually to perform a man-in-the-middle attack and obtain sensible information. In [Mitev2023], the SKG scheme is also discussed under an active attack with a countermeasure consisting of transmitting randomized probe signals instead of deterministic pilots [Mitev2019]. Another approach against PCA is the use of deep learning algorithms, such as generative adversarial networks (GANs) as in [Yadav2024], to discriminate pilot contamination signals from the legitimate ones. Finally, **physical layer authentication** (PLA), where physical characteristics of the device or channel are used to identify it, which can lead to discover attacks as usually all spoofing signals come from the same source and direction [Nguyen2020] or the hardware-specific characteristics of a device can be compared with a reference template [Jian2020]. As shown in [Senigagliesi2020], deep learning models can outperform conventional statistical methods for PLA.

Other types of attacks are more focused on the authentication process. The work of [Shaik2019] highlights that the device capabilities are exchanged in LTE and 5G without protection or verification, which leads to some attacks like identification ones (discovering software or hardware characteristics), bidding down attacks (hijack a legitimate user to use a network with lower data rates, like LTE or even 3G/2G) and finally, particularly delicate against the net-zero objective, a battery draining attack against NB-IoT devices to breakdown their power saving capabilities. This type of attack has also been identified as a risk in satellite communications [Zhang2023], preventing the satellite from entering a hibernating and making it overuse of its battery, and is mentioned as a critical vulnerability. Although the literature about energy drain attacks in B5G and 6G scenarios is limited, the work of [Moussaoui2022] mentions the 5G vulnerability to these battery-drain attacks as a subtype of MitM attack and set it as a security requirement for the incoming network. On a specific use case scenario [Hakeem2022], the battery drain attack is also mentioned as a hazard in the case of wireless brain-computer interactions (BCI) using 6G network, with this being particularly relevant as it may pose a threat to the user own health.

2.3.5. DDoS in RAN

The DDoS attacks are becoming more prevalent in recent years, with a 10x increase between 2005 to 2022 [Hummel2022] and already in 2019 there were estimated 23 million DDoS weapons worldwide ready to attack [Bacon2019]. This makes the DDoS attacks some of the most damaging cybersecurity threats. In 5G it becomes even more dangerous compared to previous cellular generations, due to the fact possibility of millions of IoT devices being able to connect to the network in an mMTC paradigm, thus making them also a possible target of hackers to create botnets which can be used for DDoS attacks. The report [BPI2019] cited DDoS as the most significant security concern of the 5G industry.

The components of the 5G communication system, including User Equipment (UEs), access networks, and core networks, are susceptible to security breaches [Khan2022]. In a network slicing scenario, where access and core network functions (such as the User Plane Function (UPF)) are virtualized on shared physical resources, the attack surface expands. For instance, a UE infected with malware could inundate a virtualized UPF function with DoS traffic. In more severe instances, multiple compromised UEs could form a botnet to launch DDoS attacks against a UPF, leveraging a network of interconnected UEs. Such attacks have the potential to impact the performance of unaffected UEs utilizing the same or different slices that share the targeted UPF. Many data sets including CICDoS [Jazi2017], CICIDS2017, CSECICIDS2018 [Sharafaldin2018], and CIC-DDoS2019 [Sharafaldin2019] are available for DoS/DDoS attacks. Author et al. delve into user plane DDoS attacks leveraging the IP protocol stack to generate excessive traffic [Abdelrazek2024]. A thesis paper showed a simplified implementation of DDoS attack on 5G and analysed its performance [Shorna2021].

3. Data-plane

3.1. Data plane threats

The deployment of 5G networks introduces new vulnerabilities and threats, particularly in the user plane and through the data plane devices of Software Defined Networking (SDN). In the 5G/6G core segment of the network, the attacks and the vulnerabilities conceived in the data plane are similar to those affecting a standard SDN/NFV environment. Interception and eavesdropping involve unauthorized access to data as it travels between the UE and the network core. Despite the enhanced encryption protocols in 5G, weaknesses in these protocols or their implementation can still be exploited. For instance, vulnerabilities in the encryption key management or flaws in the software can be targeted by attackers to intercept sensitive communications. Such breaches can lead to the exposure of confidential information, including personal data, financial transactions, and sensitive communications. This not only violates user privacy but can also have broader implications for data security across networks [Ahmad2019] [Li2021].

Compared to the attack using the signalling protocol on the control plane, the protocol-based attack on the user/data plane of the 5G/6G core network has not attracted much attention so far. Only a few DoS and message tampering attacks, using the SIP protocol to connect to the IMS server built within carriers to provide VoLTE services in the 4G network, have been announced.

Co-funded by the European Union 6GSNS Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI UK Research and Innovation

However, because various IoT services and voice services are provided in the 5G network, it is expected that DDoS attacks using protocol messages on the user plane will become a major issue. Potential network-based attacks on the user plane have been classified into three types: GTP-U protocol-based attack, SIP protocol-based attack and IoT protocol-based attack.

3.2. GTP-U, SIP protocol and IoT protocol-based threats

The GTP-U protocol is a tunnelling protocol that operates in the user plane by connecting with the GTP-C of the control plane. A typical attack based on the GTP-U protocol is a DoS attack that overloads the 5G core equipment through the GTP-in-GTP attack. There is a possibility that an attacker may obtain network and subscriber information, including the tunnel endpoint identifier, by exploiting the vulnerabilities of the GTP protocol. It is also possible to induce a DDoS attack on networks with messages exploiting GTP through IoT botnets [Pineda2023].

The SIP protocol is a voice signal control protocol used to provide VoIP over LTE services. Research by the authors in [Ko2016] has shown that attackers can conduct protocol-based attacks, such as DoS attacks and call hijacking, by exploiting SIP messages. Various messages, such as INVITE, which is a call control message of the SIP protocol, can be used for these attacks.

In the 5G mobile network, the data traffic of IoT devices, in addition to the data traffic generated by existing smartphones/UE, is expected to increase [Li2021]. For IoT-based DDoS attacks, various types of DDoS are possible on the network protocol stack. These include attacks on IoT application protocols (e.g., MQTT, SOAP) and traditional IP attacks (e.g., SYN flood, UDP flood, DNS flood, HTTP flood). The main targets of these IoT DDoS attacks are the 5G network infrastructure (RAN, core equipment, network slice, memory of physically shared platform, etc.), the Internet service application servers connected via 5G network infrastructure, and the devices connected to the 5G network. These latter IoT DDoS attacks can deplete interconnected network infrastructure resources, potentially resulting in a large-scale service failure.

Last, on IoT protocols, the most considered type of attacks (i.e., DDoS), several ways can be used to affect the operation of core networks resorting to the data plane, including proper inter-slice operation. The work in [Sathi2021] proposes a new targeted attack, the Distributed Slice Mobility (DSM) attack, aimed at the network slices of 5G networks. This attack exploits user-initiated inter-slice mobility and results in performance and economic harm to the control plane functions and the targeted network slice. The detection of DSM attack is challenging since it originates from legitimate traffic. The work also outlines defence strategies to mitigate performance damage from the DSM attack but acknowledges the difficulty in devising practical solutions to prevent economic damage. A relevant threat analysis was carried on by the work in [Amponis2022], focusing on attacks impacting the UPF functionality. In particular, authors focus on the PFCP protocol running in the 3GPP N4 interface, between the Session Management Function (SMF) and the User Plane Function (UPF). Attacks performed using this protocol can disassociate UE from the data net, exhaust the UPF resources to handle legitimate connection requests, perform eavesdropping attack. The authors evaluate the adoption of these attacks in a 5G-enabled drone swarm scenario targeting the attack to specific swarms. The same authors extend the scope of the attacks targeting the UPF also including the handover functionalities in the work in [Amponis2023], in which the authors release datasets related to malicious GTP traffic in the data plane. A final aspect concerns the security countermeasures adopted to enhance the UPF protection. Authors in [Je2022] discuss the evolution of User Plane (UP) security, highlighting the introduction of full-rate UP integrity protection (UPIP) in Release 16 of the 3rd Generation Partnership Project (3GPP) standards to enhance security. However, implementing full-rate UPIP requires increased computational resources, particularly in the Packet Data Convergence Protocol (PDCP) layer. To address this challenge, the authors propose a new concept called Selective UP Security at the PDCP layer. This approach identifies packets where application layer security (e.g., Transport Layer Security - TLS) has already been applied and applies additional PDCP layer security only to non-encrypted portions, reducing processing overhead significantly.

4. Orchestration and management plane

4.1. Orchestration and management challenges

Metropolitan 6G core networks are foreseen to be enabled by a connected set of autonomous systems, consisting of multiple heterogeneous programmable transport networks and clouds [Ziegler2020, Alwis2021, Porambage2021, Bhat2021, Quy2023]. These require end-to-end decentralised management and orchestration, foreseen to be backed by intelligent decision support through AI services [Siriwardhana2021, Alwis2021, Bhat2021, Parra-Ullauri2024]. This is to enable frictionless provision of 6G network slices, distributed and connected over multiple heterogenous Autonomous Systems (ASes). Providing such end-to-end orchestration requires addressing a range of existing and emerging security challenges, to secure the 6G infrastructure and more so to provide security level agreements to 6G slices. The higher degree of decentralisation and multi heterogeneous domain interaction in 6G means that detecting malicious behaviour and acting on requires larger and more frequent sharing of threat intelligence information across domains.

Energy efficiency is another critical factor to enabling sustainable operation of 6G services and the underlying infrastructure. Tackling energy-exhausting threats in 6G is a non-trivial challenge. Since cloudification emerged in 5G, attacks against cloud infrastructure have increased. Particularly, (Distributed) Denial of Service (DoS/DDoS) and more recently the evolved Denial of Sustainability (DoSt) - a.k.a Economic Denial of Sustainability (EDoS) - variant [Monge2019, Dennis2021, Catillo2023]. Both forms of attacks exploit the cloud capacity to absorb growth in workload by scaling up virtual resources, and the primitive decision support from threat shielding systems, to the orchestration counterparts. The additional challenge with DoSt attacks is the difficulty in detecting them. Unlike DoS/DDoS attacks, DoSt do not disable their target service. Instead, they increase the load/demand level to a threshold below the capacity limit, thus continually exhausting service resources and causing them to scale up beyond the budget limit of the service provider [Porambage2021, PorambageGur2021]. For cloudified services, this translates into higher operational costs for the service provider, incurred by the additional cloud cost to absorb the attack, rendering the service unsustainable to operate [Monge2019, Dennis2021, Lalropuia2021, Catillo2023]. The impact of DoSt can be particularly high for resources intensive services, such as AI and Distributed Ledger Technologies (DLTs), as a slight increase in demand could result in a significant increase in resource utilisation. Added to that, the novel ways in which such services can be abused - for example through 'convergence prevention', makes attack tracing and identification hard [PorambageGur2021].

Aside from the cloud, the focal point of cybersecurity in 5G has been around protecting the management overlays. In SDN and NFV realms, attacks against SDN controllers and NFV MANOs have been the main challenges [Porambage2021, Siriwardhana2021, ShenFeng2023]. These have been largely driven by vulnerabilities in APIs exposed between the middleware elements (controller, MANO components) and data-plane elements. The vulnerability of APIs poses critical security challenge. Because the management and orchestration plane of modern Beyond 5G and future 6G telecommunication networks is reliant on APIs given its design to be automated in near real-time, a process standardized as Zero touch network and Service Management (ZSM) by the European Telecommunications Standards Institute (ETSI) [Ortiz2020], follows a cyclic closed-loop approach of "monitoring", "analysing", "detecting", "deciding", and "enforcing". ETSI is also the main Standard Development Organization (SDO) behind the Network Function Virtualization (NFV) standard, initiating the movement of telecommunication networks (5G and future 6G network) towards virtualizing its assets and enabling the software-based orchestration of network functions (NFs) and network slices. The ETSI NFV defined additional components for the security orchestration in the NFV architecture such as the OSS security manager (OSSM), NFV Security Manager (SM) and Security Agents (SA)[NFV-SEC024], enabling the integration of new automated optimized security orchestration that leverages AI/ML.

Complementary, the stringent requirements for 6G QoS, require ultra-fast responsiveness and reliability from cybersecurity services, in addition to being energy efficient. These, namely energy efficiency, responsiveness and reliability may well be some of the biggest challenges to be addressed for 6G cybersecurity services [Porambage2021, ShenFeng2023, SalahdineHan2023, Parra-Ullauri2024].

To enable cloudified and sustainable 6G networks at scale, it is critical to develop scalable cybersecurity solutions that: a) feed threat intelligence of D/DoS and DoSt to orchestration middleware layers; b) develop novel anomaly detection solutions for emerging services (e.g. AI and DLT); and c) extend said middleware with logic and intelligence to make orchestration decisions (e.g. service placement, migration, routing, mapping) based on the security 'hardness' of infrastructure and the pattern of demand offered to 6G services. Moreover, the trajectory of requirements stringency, strongly suggests increased reliance on proactive decision-making based on continual learning and predictions to achieve the high responsiveness needed to meet said requirements.

4.2. ML based orchestration threats

As the telecommunications industry progresses towards the deployment of 6G networks, numerous security challenges related to data and machine learning (ML) are emerging. The anticipated capabilities of 6G, such as ultra-low latency, massive connectivity, and enhanced data rates, will heavily rely on advanced ML algorithms for efficient operation and management. However, the integration of ML in 6G also introduces new vulnerabilities and threats. This section explores the current state of research and identifies the key security challenges in this domain.

4.2.1. Machine Learning Security Challenges

4.2.1.1. Model Security

The integration of machine learning (ML) in 6G technologies introduces several security challenges that need to be addressed to ensure robust and secure networks. Protecting ML models from various attacks is vital for maintaining the reliability of 6G networks:

- Model Inversion Attacks: Attackers can reconstruct input data from the outputs of ML models, posing a threat to data privacy. Techniques like secure multi-party computation and homomorphic encryption are being explored to protect against such attacks [HussainR2020].
- Adversarial Attacks: One of the primary security concerns is the susceptibility of ML models to adversarial attacks. These attacks involve subtly manipulating input data to deceive the ML model into making incorrect predictions or classifications. For example, adversarial attacks like the Fast-Gradient Sign Method (FGSM) can significantly increase the mean square error of ML models used for tasks such as mmWave beam prediction, rendering them ineffective under attack [HussainR2020].
- Reinforcement Learning attacks: In this type of attack, a malicious user utilizes Reinforcement Learning algorithms to autonomously learn and execute strategies that disrupt 5G and 6G components [SANCUS]. In these attacks, an RL agent is trained to identify and exploit vulnerabilities within a network by executing various attack scenarios. Through a process of trial and error, the agent optimizes its actions to maximize disruption, such as overwhelming network resources or manipulating traffic patterns to cause service outages. This method allows for adaptive and intelligent attacks that can dynamically adjust based on the network's defences and configurations, making them particularly challenging to detect and mitigate.
- Model Integrity and Data Poisoning: Ensuring the integrity of ML models and training data is crucial. Data poisoning attacks can corrupt training datasets, leading to compromised models that make erroneous decisions. This is particularly dangerous in critical applications like autonomous driving or healthcare, where accurate predictions are vital [Zhang2020][Zhou2021][Ramirez2022].
- Privacy Concerns: ML models often require large amounts of data, which can include sensitive personal information. Protecting this data from unauthorized access and ensuring compliance with data protection regulations is essential. Techniques like federated learning, which allows models to be trained on decentralized data, can help mitigate these privacy concerns [Zhang2020].
- Model Stealing and Evasion: Attackers can also attempt to steal ML models or evade them. Model stealing involves reverse-engineering a deployed model to understand its parameters and functionality, potentially leading to intellectual property theft. Evasion

attacks aim to make the ML model miss certain patterns, such as not detecting a specific type of network intrusion [Truong2021].

- Explainability and Trustworthiness: Ensuring that ML models are explainable, and their decisions are transparent, is important for building trust. Explainable AI techniques can help provide insights into how decisions are made, which is crucial for human security experts to verify and validate the models' outputs [Truong2021].
- Adaptive Security Mechanisms: The dynamic nature of 6G networks necessitates adaptive security mechanisms that can respond to evolving threats in real-time. ML models themselves must be capable of adapting to new types of attacks and continuously improving their defense mechanisms through techniques such as adversarial training and reinforcement learning [Truong2021].

4.2.1.2. Trustworthiness and Explainability

Machine learning (ML) trustworthiness and explainability are critical challenges in the context of 6G technologies. As 6G networks integrate more advanced and ubiquitous ML and AI technologies, ensuring these systems are both trustworthy and explainable becomes paramount for the security, reliability, and user acceptance of the network. The primary challenges are outlined in [Brik2023, Wang2022] and include the following:

- Security and Privacy: The deployment of ML models in 6G networks introduces significant security and privacy concerns. Models can be susceptible to adversarial attacks, where inputs are subtly altered to mislead the model, causing incorrect predictions without being detected. Additionally, data privacy is a critical issue, especially with the vast amount of personal and sensitive information processed by 6G networks. Ensuring the integrity and confidentiality of this data is crucial for maintaining trust in ML applications.
- Bias and Fairness: ML models can inherit biases present in the training data, leading to unfair and discriminatory outcomes. In a diverse and globally connected 6G environment, biased ML decisions can have widespread negative impacts. Ensuring fairness involves rigorous auditing of training datasets and implementing bias mitigation techniques throughout the model development process.
- Robustness: ML models need to be robust to variations and uncertainties in data. In the dynamic and heterogeneous 6G environment, models must perform reliably across different contexts and conditions. Robustness testing and the development of models that can generalize well to new, unseen data are essential for trustworthiness.
- Complexity of Models: As ML models, particularly deep learning models, become more complex, understanding how they make decisions becomes increasingly difficult. This lack of transparency can hinder the ability of users and operators to trust and effectively manage these models. Techniques for explainability, such as interpretable

models, feature importance scoring, and model-agnostic explanation methods, are necessary to make these complex models more understandable.

- Regulatory Compliance: With stringent regulations around data protection and algorithmic transparency, particularly in regions like the EU with GDPR, there is a pressing need for ML models to be explainable. Regulatory bodies require explanations for automated decisions, especially those impacting consumers' lives, such as in healthcare or finance, which are services likely to be integrated with 6G technologies.
- Human-AI Interaction: For effective deployment of ML in 6G, there must be a synergy between human operators and AI systems. Explainability plays a key role in fostering this interaction by allowing operators to understand, trust, and effectively intervene in AI-driven processes. This is crucial for maintaining control over critical network operations and ensuring that AI systems augment rather than undermine human decision-making.

Ongoing research focuses on developing frameworks and tools to enhance both trustworthiness and explainability in ML models used in 6G networks. For example, the SIX-Trust framework introduces layers of trust (Sustainable Trust, Infrastructure Trust, and Xenogenesis Trust) to build a holistic trust model for 6G networks. Additionally, explainable AI (XAI) techniques are being integrated into the design of 6G networks to provide transparency and accountability in AI-driven processes.

4.2.2. AI-based Attacks

Considering the advancements in AI, particularly in the use of adversarial neural networks for DoS attacks on 5G and beyond networks, it is crucial to prioritize the development of defence mechanisms. AI systems' capability to execute sophisticated and coordinated attacks across various protocols underscores the vulnerability of modern infrastructures to AI-based threats [Zolotukhin2022].

The research by [Sagduyu2021] examines the vulnerabilities of 5G networks to adversarial machine learning attacks. It focuses on disrupting spectrum sharing and spoofing physical layer authentication in network slicing using Deep Learning classifiers and Generative Adversarial Networks (GANs). The authors propose defence strategies to increase adversarial uncertainty during model training, emphasizing the need for robust defences in the 5G context. The paper also explores the use of Reinforcement Learning to optimize 5G network operations, underscoring the vital role of advanced machine learning techniques in enhancing 5G security and efficiency.

[Hu2018] developed a novel GAN-based framework called GANFuzz to enhance the security and robustness of industrial network protocols through advanced fuzz testing techniques. This framework utilizes Deep Learning to automatically learn and generate test cases that simulate realistic network traffic, enabling more effective identification of vulnerabilities and errors in industrial network protocol implementations. This approach marks a significant departure from traditional methods, offering a more efficient and automated way to test and secure critical industrial systems.

4.2.3. Net-Zero Projects

Two telecommunications giants, Vodafone UK [Baldock] and Ericsson [Ericsson] are spearheading ambitious projects aimed at combatting climate change through technological innovation. Vodafone UK emphasizes the transformative potential of 5G Standalone (SA) technology in reducing energy consumption and carbon emissions across various industries. By leveraging 5G SA-enabled solutions such as IoT, drones, and smart grids, Vodafone UK envisions substantial advancements in renewable energy production, particularly in wind farms, and the optimization of traditional sectors like agriculture. Their proposed merger with Three UK signals a commitment to accelerating the rollout of 5G SA networks nationwide, vital for maximizing the impact of these initiatives and driving the UK's transition to Net Zero.

Meanwhile, Ericsson's commitment to sustainability extends beyond its operations to encompass its entire value chain. With a clear understanding of ICT's potential to mitigate climate change, Ericsson sets ambitious targets to achieve Net Zero emissions by 2040. Through a systematic approach involving emission reduction in both its supply chain and portfolio, as well as the neutralization of remaining emissions through approved carbon removal credits, Ericsson aims to lead the way in corporate climate action. Their dedication to aligning advocacy activities with the Paris Agreement's goals underscores a holistic approach to sustainability, positioning Ericsson as a key player in the global effort to limit global warming and create a more sustainable future.

5. Clouds: edge-to-core

5.1. Network core threats

The advent of 5G and upcoming 6G technologies promises to transform connectivity, offering speeds multiple times faster than current LTE networks. This leap will significantly boost the number of Internet of Things (IoT) devices linked to these networks, fostering an intricately connected ecosystem. This ecosystem will be capable of supporting massive Machine Type Communications (mMTC), enabling a multitude of IoT devices to access and operate over the network effortlessly.

Despite these advancements, substantial security challenges remain. A significant number of IoT devices suffer from inadequate security measures, making them susceptible to malicious attacks. If these devices are compromised, they can be used to launch widespread distributed denial-of-service (DDoS) attacks, which are a significant problem currently [Global Research and Analysis Team2024] and have the potential to worsen in the future, severely disrupting 5G network operations. Establishing comprehensive security standards for IoT devices is particularly difficult due to the diversity of devices spanning various sectors—ranging from smart manufacturing and urban sensors to surveillance systems—each with distinct uses and supply chains.

Securing lower-end IoT devices poses an even greater challenge because these devices often use weak passwords and outdated security protocols, rendering them vulnerable to tampering. Such vulnerabilities make these devices easy targets for unauthorized access and man-in-the-middle attacks, potentially leading to the exposure of sensitive subscriber data, such as International Mobile Subscriber Identity (IMSI). Cybercriminals can exploit these security gaps, using malware to co-opt IoT devices into large-scale botnets, which they can remotely control to execute coordinated attacks.

The evolution of 5G/6G networks has transitioned from relying on hardware to utilizing software-based infrastructure. This new infrastructure leverages communication servers, network devices, and network slicing services through SDN (Software-Defined Networking) and NFV (Network Functions Virtualization) technologies. By employing these technologies, it is possible to partition a single physical network into multiple virtual networks, thereby offering tailored network slicing services for applications. Instead of using specialized hardware, network functions can be implemented on general-purpose x86 servers as virtual machines. Although virtualization technology, which underpins 5G/6G equipment and service implementation, offers benefits like resource efficiency, flexibility, and availability by sharing physical network and hardware server resources (such as CPU and memory), it also presents vulnerabilities. These vulnerabilities include susceptibility to load attacks on shared hardware resources, unauthorized access to network slices and shared resources, malicious software distribution through shared resources, and configuration errors in virtualization management software.

SDN technology separates the network control plane (SDN controller) from the data plane (SDN switch), which was traditionally processed in hardware. This separation introduces potential security risks, such as traffic bypass attacks that exploit vulnerabilities in the control protocol between SDN controllers and switches, unauthorized access between switches and controllers, and resource depletion in SDN systems due to DoS attacks. For instance, a saturation attack could overwhelm the SDN switch flow table by targeting SDN controllers. Similarly, NFV technology, when implemented on general-purpose servers, is prone to security issues unless there is stringent control over hypervisor security, malicious VM migrations, changes or authentication of applications running on virtualized network functions, and authorization of networking functions. Without adequate mechanisms for application authentication and authorization, malicious third-party applications could potentially extract network information from SDN controllers [Ahmad2018, Chica2020, Maleh2023, Farooq2023].

Network slicing, a new feature in 5G networks, logically separates traffic for service while utilizing the same physical network. If these slices are not properly isolated, attacks from one slice could impact others. For example, an attacker could execute a network slicing resource depletion attack by overloading a specific service's network slice, thereby affecting other slices or triggering specific applications. Additionally, without proper encryption of network slices, attackers might intercept or alter data from other slices [Cunha2019, Olimid2020].

The softwarization of networks, given the aforementioned characteristics, may also provide new opportunities for Advanced Persistent Threats (APTs). These threats involve resourceful attackers establishing a long-term presence within a system to carry out malicious activities over an extended period. APTs have been an emerging issue for some time now [Global Research and Analysis Team 2024], and with the growing reliance on cyber systems, their persistence is likely. Consequently, researching APT models, exploring potential solutions, and formulating open questions for further investigation is imperative [A. Alshamrani2019, Salim2023].

Orchestration today encompasses various methods for managing the application lifecycle, particularly within cloud environments. Modern service and network management platforms are structured in multiple layers, which allows for individual management and maintenance of each layer. These layers are typically operated by different administrative entities; for example, a cloud infrastructure provider manages the underlying servers using virtual infrastructure manager (VIM) software (such as [Kubernetes2023] or [OpenStack2023]), while connectivity between these servers may be handled through a programmable fabric controlled by an SDN controller (like ONOS [1_ONF2023], ODL [1_TheLinuxFoundation2023], or ETSI TFS [1_ETSI2024]). Additionally, a local NFV Management and Orchestration platform (such as ETSI OSM

[2_ETSI2024] or ONAP [2_TheLinuxFoundation2023]) might oversee several VIMs and SDN controllers at each site, while an overlay operation support system (OSS) supervises multiple, possibly geographically dispersed, MANO platforms across different network domains. On top of these systems, application-level orchestrators aim to achieve optimal service deployments based on high-level user-defined orchestration policies. This complex software stack allows for seemingly seamless integration between various layers, thanks to significant efforts by the industrial and research communities to standardize APIs through global standardization bodies (like ETSI [ETSI2023] and IETF [IETF2023]) and technology consortia (such as ONF [2_ONF2023] and the Linux Foundation [3_TheLinuxFoundation2023]).

Despite significant advancements, several critical issues remain unresolved, necessitating drastic solutions for sustainable service orchestration in the future. Firstly, the partial detachment of orchestration layers makes end-to-end orchestration nearly impossible. Each layer has a limited view of the entire system, providing orchestration APIs for a restricted set of resources and only leveraging local events. While this isolation simplifies orchestration, it complicates achieving a comprehensive end-to-end orchestration. Secondly, the current single-objective orchestration model is inadequate. Each layer's control loops are centred around a single goal (e.g., performance), failing to meet the diverse and often conflicting requirements of modern overlay services. Future orchestration must handle multiple objectives and dynamically prioritize them based on business needs. Thirdly, future orchestrators need to incorporate AI to determine the necessary changes, contrasting with today's MANO systems (e.g., OSM) that only manage feasible changes. Optimizing for both rapidly changing system conditions and external market factors is challenging but well-suited for AI. Finally, the scalability of end-to-end orchestrators will face significant challenges in the 6G era. Future platforms must manage the ad-hoc behaviour of 6G devices forming spatiotemporal IoT swarms and swiftly respond to numerous events. These demands will strain the current centralized orchestration frameworks. Despite advancements in frameworks like ONF's Aether, OSM, and ONAP, no system currently addresses all these challenges.

5.2. Edge runtime Management and workload isolation

Due to the resource constraints and the unique security environment of edge computing, edge runtimes require designs that foster performance security and sustainability. Several edge-oriented Kubernetes-based platforms are currently available, for example KubeEdge[1] and Eclipse ioFog [Cilic2023]. KubeEdge has a memory overhead of only 70 MiB for its worker nodes, although its edge architecture requires custom components and is not compatible with other Kubernetes nodes by default. ioFog[2], another popular orchestration platform for the edge, has a

[1] https://kubeedge.io/

[2] https://iofog.org/

memory footprint of only 100 MiB on worker nodes, which is fairly low in comparison with other Kubernetes distributions. However, while these frameworks are aimed at edge computing, they are limited to container workloads.

Some studies [Mavridis2021] use KubeVirt[3] to deploy and evaluate (micro)VM alternatives on Kubernetes clusters. However, while KubeVirt enables the deployment of virtualized workloads, it also requires extensive intervention in a Kubernetes cluster to work (e.g. custom resources, daemonsets). Unlike KubeVirt, Feather [Goethals2024] is aimed specifically at creating a multi-runtime agent for edge computing, without the need to modify an existing Kubernetes cluster in any way.

FLEDGE [Goethals2020] is a Kubernetes-compatible edge agent based on Virtual Kubelets[4], and designed for minimal resource overhead, using only around 50MiB of memory. A Virtual Kubelet is essentially a proxy which poses as an actual kubelet to the Kubernetes API but allows any sort of underlying provider to interpret and execute the received commands. Feather aims to extend the State of the Art by allowing the OCI-compliant side-by-side orchestration of various types of workload images (e.g. containers, microVMs) on edge devices, without architectural or operational changes to an existing Kubernetes cluster or its control plane nodes.

Due to limited device resources, State-of-the-Art (SotA) edge computing platforms and solutions focus primarily on containers to isolate workloads, even in multi-stakeholder scenarios. Kubernetes-derived systems such as KubeEdge and FLEDGE [Goethals2020] use containers exclusively, as does ioFog [Cilic2023]. More recently, Feather [Goethals2024] has expanded edge workload isolation to OSv unikernels.

5.3. Edge-clouds threats

DoSt (a.k.a EDoS) is a special form of attacks, targeting cloud systems and by virtue their extension towards the edge. Such attacks aim to strain the resources allocated to service, but not to the point of causing a Denial of service (DoS), thereby causing a scale-out of resources that increases operational costs. This form of attacks is increasingly being addressed in the literature, with examples including the work of [Ficco2019, Xu2020, Dinh2020, Dinh2021, Dennis2021, Ta2022, Kashi2022]. Typically, this form of attack has been targeting cloudified services, as it causes a scale up of infrastructure resources to absorb the attack, effectively causing unsustainable operation of the target service and its provider (namely a cloud user/customer). The work of [Dinh2020, Dinh2021, Ta2022] investigates DoSt in SDN-enabled cloud systems. They argue that DoSt attacks are an alternate version of classic DDoS attacks, with modified intensity to remain below the threshold of typical anomaly detection filters. In that sense, DoSt may

[3] https://kubevirt.io/

[4] https://github.com/virtual-kubelet/virtual-kubelet

include TCP SYN and HTTP flood attacks, Slowloris and Low and Slow attacks. The work of [Dennis2021] similarly outlines three main classes of EDoS attacks targeting: specific cloudified services (e.g. through HTTP-based intrusion), cloud/network infrastructure (CPU, storage, bandwidth [Dinh2020]) and those targeting network connections (e.g. TCP, UDP flooding attacks). Notably, attacks can be launched against not only cloud resources allocated to a service, such as CPU and storage, but against the SDN infrastructure (bandwidth on links and flow tables). More so, DoSt/EDoS can further target the cloud service provider and the corresponding infrastructure. For example, the work of [Ficco2019] investigates how EDoS can be launched against cloud service providers with the aim of causing excessive energy consumption that render the OPEX of cloud infrastructure unsustainable. The work of [Xu2020, Kashi2022] investigates a variant of EDoS attacks named Yo-Yo, in which a threat actor would induce oscillating periods of high and low demand; causing continued scale-out/scale-in. While this form of attacks results in the typical effect of increasing the OPEX of cloud customers to unsustainable levels, it further has the side effect of inducing higher orchestration and resource management overhead on the cloud provider, beyond sustainability levels of the provider themselves.

6. Data & Privacy

6.1. Data privacy regulation landscape and challenges

Data privacy involves safeguarding sensitive information from unauthorized access, use, or disclosure, allowing individuals to control their personal data [Chua2021]. The rise of digital technologies and the rapid increase in data volume have made protecting data in digital environments more crucial [Saraswat2022]. With the emergence of cloud computing, the Internet of Things (IoT), and big data analytics, data has become more accessible and interconnected. This enhanced accessibility has exposed organizations to numerous cyber threats and vulnerabilities. Cyberattacks on sensitive data have grown more sophisticated, presenting significant challenges to organizations across different sectors [Djenna2021]. Additionally, regulatory frameworks like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have increased the legal responsibilities of organizations regarding data protection and privacy [Hartzog2020]. Consequently, there is a pressing need for organizations to implement strong data privacy and security measures, such as encryption, access controls, data anonymization, and threat intelligence, to mitigate risks and comply with regulatory requirements [Villegas2023].

Key points to consider of privacy and data protection in the context of 6G networks, which are anticipated to be a significant advancement over current 5G technology are presented below:

1. **Vast Data Handling:** 6G networks will facilitate the handling and transmission of enormous amounts of data from a diverse array of sources. These sources include:
    - IoT Devices: Internet of Things devices such as smart home appliances, wearable technology, and industrial sensors.
    - Autonomous Vehicles: Self-driving cars and drones that require real-time data processing and communication.
    - Smart Cities: Urban environments equipped with interconnected systems for traffic management, utilities, public services, and surveillance.
2. **Privacy Concerns:** The sheer volume and variety of data being processed in 6G networks raise significant privacy concerns:
    - Personal Data: Sensitive information related to individuals' health, habits, location, and behaviour may be collected and transmitted.
    - Anonymization Challenges: Ensuring data is anonymized to protect individual identities can be difficult, especially when multiple data sources are combined.
    - Consent Management: Ensuring users are fully aware of what data is being collected and how it is used is crucial. Obtaining and managing user consent effectively is a key challenge.

3. **Data Protection:** Protecting data in 6G networks involves several layers of security measures:
    - Encryption: Encrypting data during transmission and storage to prevent unauthorized access.
    - Authentication: Ensuring that devices and users accessing the network are legitimate and authorized.
    - Access Controls: Implementing strict access controls to limit who can view or manipulate data.
4. **Potential for Data Breaches:** With more data being transmitted, the potential for data breaches increases. Key considerations include:
    - Advanced Threats: Cybercriminals may use more sophisticated techniques to breach 6G networks.
    - Attack Surfaces: With more devices and interconnected systems, the potential entry points for cyber-attacks increase.
    - Incident Response: Rapid and effective response mechanisms are necessary to mitigate the impact of any data breaches that occur.
5. **Data Misuse:** Beyond breaches, there is also the risk of data being misused by authorized entities:
    - Surveillance: Increased data collection can lead to privacy infringements through excessive surveillance.
    - Profiling: Data can be used to create detailed profiles of individuals, which can then be exploited for commercial or political purposes.
    - Ethical Considerations: The ethical use of data must be considered, ensuring that it is not used in ways that harm individuals or society.
6. **Regulatory Compliance:** Ensuring compliance with data protection regulations will be critical:
    - Global Regulations: Different regions have varying regulations, such as GDPR in Europe, CCPA in California, and others globally.
    - Data Sovereignty: Data may need to be stored and processed within certain geographical boundaries to comply with local laws.
    - Continuous Updates: Regulations may evolve, requiring networks to continuously update their compliance measures.

The introduction of new regulations (e.g. GDPR, EU Right to be Forgotten etc.) has led to the development of privacy preservation techniques such as radio fingerprinting at the physical layer [Zhang2023], data and communication anonymization at the connection layer, and differential privacy, homomorphic encryption, data masking, or secure multi-party computing at the service layer. However, ensuring privacy protection in 6G networks is more critical for several reasons.

Firstly, 6G is expected to support key applications like wearable devices that handle highly sensitive user data. While these applications can enhance human lives by reducing fatal accidents, improving sleep quality, and aiding in the rehabilitation of people with disabilities, they also risk the illegal collection and misuse of physical and medical data used by interconnected control systems [Niksirat2024]. Although these threats are not new, 6G will intensify them. Moreover, the strategy of migrating many core components and applications to the cloud in 6G is flawed. This "cloudification" increases the risk of unauthorized access and exposure of customer data, including the potential for illegal disclosure by unauthorized employees. Lastly, securing personal data becomes more challenging with the advent of supercomputing and intelligent agents. The expected rise in AI-enabled smart applications with 6G will connect humans and objects, allowing AI to extract more contextual information about individuals and their environments [Timan2021]. While this can provide consumers with personalized services like recommendations for attractions, films, and routes, it also raises significant privacy concerns. Furthermore, as 6G networks emerge, the intersection of machine learning (ML) and privacy presents both challenges and opportunities. There are two aspects in this alliance: privacy invasion and protection through ML. On one hand, there are malicious actors that can exploit ML models to breach privacy and on the other hand, a secure ML structure (pre-emptive privacy considerations during the design), or the correct application of ML, can protect privacy in 6G networks [Sun2020].

7. Affected network service KPIs

This section states the network service KPIs, notably aligned with NATWORK's Performance, Security and Sustainability key values.

7.1. Performance

- **Round Trip Time Latency:** measures the time it takes for a packet to travel from its source to its destination, and the time taken to receive the reception confirmation. This parameter informs not only about the data transfer delay but also about the processing time of the channel (including all hops and network nodes).
    - **How it is affected:** The observation of the results of the impact on latency shows a general, exaggerated increase in latency during the DDoS attacks. [Djuitcheu2023]
- **One-way latency (Network Function)**: measures the time it takes for a packet to travel across the network function, supposing there is a 1:1 relationship with the input-output function with respect to the considered packet.
    - **How it is affected**: depending on the load of the system (OS, guest system, containerized environment) and the number of operations needed for the packet, the one-way latency may vary in an unpredictable way. In case of attacks, CPUs are overloaded bringing to network function disruptions or very high latency values.
- **Jitter**: informs about the variation in the reception delays of packets at the destination. This parameter informs about network saturation or congestion.
    - **How it is affected:** Jitter exhibits high and irregular fluctuations, signifying the disruptive nature of DDoS attacks on maintaining consistent communication quality. [Djuitcheu2023]
- **Packet loss:** measures the rate of received packets for a given period compared to the number of packets sent. This parameter informs about the quality of reception of the recipient and the quality of the transmission medium to properly route packets on the network.
    - **How it is affected:** Substantial rise in packet loss percentages during attack scenarios, leading to increased floodings and the saturation of the gateway have been observed. [Djuitcheu2023]

- **Bitrate/ Throughput:** is the number of bits transmitted or processed per unit of time. Understanding this parameter can help characterize a service or a communication, because its abrupt and irregular growth can indicate improper network activity.
  - **How it is affected:** It is affected in a twofold manner during DDoS attack. On one hand a fall in bit rate caused by network congestion or exhaustion of network resources leading to a drop in the overall bit rate of the network can be observed. On the other hand, observing the growth of the network's bit rate on the gateway side, a spike is observed owing to the system being flooded with a massive amount of data arriving at the gateway, pushing it to process more packets than necessary. [Djuitcheu2023]
- **Spectral Efficiency:** The amount of data transmitted over a given bandwidth in a specific time period. Higher spectral efficiency ensures that the network makes the most efficient use of available spectrum resources.
  - **How it is affected:** Jamming reduces the signal-to-noise ratio (SNR), causing increased errors in data transmission. This leads to retransmissions, lower data rates, and inefficient use of spectrum resources. Whilst, by consuming excessive bandwidth and causing network congestion, DoS attacks can prevent efficient spectrum utilization and degrade overall network performance [ITU2023].
- **Bandwidth Utilization:** The percentage of the network's total available bandwidth that is currently being used. Higher utilization indicates efficient use of available resources, but excessive utilization can lead to congestion and performance degradation.
  - **How it is affected:** Bandwidth utilization is influenced by the volume of data traffic, the efficiency of data transmission protocols, and the network's ability to manage and prioritize different types of traffic. Implementing traffic management techniques such as load balancing, dynamic bandwidth allocation, and quality of service (QoS) policies can optimize bandwidth utilization.
- **Throughput of LLM (Tokens/second)**: The number of tokens generated per second. It's a critical performance metric, particularly for real-time applications. This metric depends on model size, hardware capabilities, and optimization techniques.
  - **How it is affected:** i) Model Size (parameters) and Complexity (model architecture), ii) Hardware capabilities (AI-specific chips and parallelism), iii) Optimization Techniques (quantization, pruning).

7.2. Security

In the context of 6G, security is a paramount concern due to the increased sophistication of cyber-attacks and the need to protect sensitive data across a highly complex and interconnected ecosystem. According to [Nguyen2021, Tataria2021], some key performance indicators (KPIs) related to security in 6G networks are as follows:

- **Threat Detection Rate:** The percentage of security threats successfully identified by the system out of the total number of threats. High threat detection rates are essential to pre-emptively counteract potential security breaches.
    - **How it is affected:** 6G networks will connect a vast number of devices, ranging from IoT devices to autonomous vehicles, significantly increasing the attack surface. With more entry points for potential attacks, it becomes more challenging to maintain a high TDR. The diversity of connected devices necessitates more sophisticated detection mechanisms capable of handling a wide range of threat vectors.
- **Threat Detection time:** The mean time to detect a security threat considering the data collection time, data transition time, and the analysis/inference time leading to detecting the threat.
    - **How it is affected:** The distributed nature and cloud-to-edge continuum of 6G can affect the duration of data gathering and data aggregation needed for large-scale monitoring, possibly increasing threat detection time. On the other hand, shifting the decision-making process to the edge can expedite the detection of localized threats targeting the specific network entry point.
- **Response Time to Security Incidents**: The average time taken to detect, analyse, and respond to security incidents. Rapid response times minimize the impact of security incidents on network performance and user data.
    - **How it is affected:** The ultra-low latency, high bandwidth, and massive scale of 6G networks pose unique challenges to security incident response. With threats evolving rapidly and attacks becoming more distributed, security teams must employ real-time detection and response mechanisms, leveraging advanced technologies such as AI-driven threat detection and automated mitigation. Compliance with privacy regulations adds an additional layer of complexity, necessitating proactive measures such as regular security assessments and employee training to ensure effective incident response in 6G networks.

- **False Positive Rate**: The rate at which legitimate activities are incorrectly flagged as malicious. Lower false positive rates improve operational efficiency by reducing the workload on security teams and avoiding unnecessary disruptions, but it is equally important to strike a balance to prevent the oversight of genuine threats.
    - **How it is affected:** Network monitoring tools can identify false alerts for network scans and the algorithms for attack detection (core, RAN) can be too sensitive. Security systems that monitor user activities may generate a false positive in user behaviour when an individual's actions are flagged as abnormal or potentially malicious.
- **False Negative Rate**: The rate at which actual security threats go undetected. A false negative is more damaging than a false positive because it lets a problem go undetected, creating a false sense of security. Minimizing false negatives ensures that real threats are identified and addressed promptly.
    - **How it is affected:** Detection limitations may come from different sources such as non-identified newly emerging threats, zero-day attacks and sophisticated attacks. The attack detection algorithms may also underperform and lead to false classification of suspicious behaviour as normal.
- **Data Breach Rate**: The frequency of successful unauthorized data access incidents. A low data breach rate indicates strong data protection measures and high overall security.
    - **How it is affected:** The ultra-low latency and high bandwidth increase the speed and volume of data transmission, potentially accelerating the spread of breaches. The massive scale and complexity of 6G networks expand the attack surface, making it harder to detect and prevent breaches. Advanced and evolving threats, such as AI-driven attacks and IoT exploitation, further heighten the risk of breaches. Additionally, the distributed nature of attacks and the need for real-time threat detection and response mechanisms make it challenging to effectively mitigate breaches.
- **Encryption Coverage**: The percentage of data that is encrypted both at rest and in transit. Comprehensive encryption coverage is crucial for protecting data privacy and integrity.
    - **How it is affected:** The vast scale and increased number of interconnected devices expand the encryption requirements, making comprehensive coverage more difficult to achieve. High-speed data transmission and ultra-low latency demand efficient encryption methods that do not compromise performance. Advanced threats and AI-driven attacks may exploit weaknesses in encryption algorithms,

necessitating continuous updates and advancements in cryptographic techniques. Additionally, the diverse range of devices, including IoT and edge computing, requires consistent and robust encryption protocols to protect data across the entire network.

- **Authentication Success Rate**: The percentage of legitimate user authentication attempts that are successful. High authentication success rates ensure secure access while maintaining user convenience.
    - **How it is affected:** The massive increase in connected devices, including IoT and edge computing, complicates the authentication process, potentially leading to higher failure rates. The ultra-low latency and high-speed requirements necessitate efficient and rapid authentication mechanisms, which must balance security with performance. Advanced and evolving threats, such as AI-driven spoofing and sophisticated identity theft, can undermine authentication methods, reducing their effectiveness.
- **Patch Management Efficiency**: The average time taken to deploy security patches across the network. Efficient patch management reduces vulnerability windows and protects the network from known exploits.
    - **How it is affected:** The sheer scale and complexity of interconnected devices, including IoT and edge computing, make it difficult to ensure timely and comprehensive patch deployment across the network. High-speed data transmission and ultra-low latency demands require that patches be applied without disrupting service, which can be technically challenging. The rapid evolution of threats, including AI-driven attacks, necessitates frequent updates, straining patch management processes.
- **Access Control Violation Rate**: The frequency of unauthorized access attempts that are detected and blocked by the system. A low violation rate indicates robust access control mechanisms, essential for maintaining network security.
    - **How it is affected:** The massive increase in connected devices and the complexity of network environments make it harder to enforce consistent access control policies. Ultra-low latency and high-speed requirements necessitate efficient access control mechanisms that can operate seamlessly without slowing down the network. Advanced threats, such as AI-driven attacks and sophisticated unauthorized access techniques, can exploit weaknesses in access control systems, increasing violation rates.

- **Service Availability During Attacks**: The percentage of time that services remain available and operational during security attacks. High service availability ensures continuous operation and minimizes the impact of attacks on users.
    - **How it is affected:** The ultra-low latency and high-speed requirements mean that even minor disruptions can have a substantial impact on services. The vast number of interconnected devices increases the attack surface, making it easier for attackers to launch distributed denial-of-service (DDoS) attacks that can overwhelm network resources. Advanced threats, such as AI-driven attacks, can quickly adapt and target vulnerabilities, complicating defence efforts.
- **User Privacy Compliance**: The extent to which the network complies with relevant privacy regulations and standards (e.g., GDPR, CCPA). Ensuring compliance with privacy regulations protects user data and avoids legal repercussions.
    - **How it is affected:** The vast amount of data generated by interconnected devices in 6G ecosystems necessitates robust data protection measures. Compliance is challenged by the complexity of monitoring and securing data flows across diverse and distributed systems. Moreover, sophisticated attacks can exploit vulnerabilities in data handling processes, potentially leading to breaches that violate privacy regulations and standards. Additionally, the diverse range of devices and the need for seamless interoperability can lead to inconsistencies in privacy protection across different parts of the network. Compliance with privacy regulations in such a dynamic and complex environment necessitates continuous monitoring, regular audits, and the implementation of adaptive privacy-preserving technologies.
- **Security Audit Frequency and Success Rate**: The regularity and outcomes of security audits conducted to assess network vulnerabilities and compliance. Frequent and successful security audits help identify and mitigate potential security risks proactively.
    - **How it is affected:** The vast amount of data generated by a massive number of interconnected devices makes it difficult to ensure comprehensive privacy protection. High-speed data transmission and ultra-low latency require advanced encryption and real-time data processing, complicating the implementation of privacy measures. Sophisticated threats, including AI-driven attacks, can target and exploit personal data, increasing the risk of privacy breaches.
- **Intrinsic Security of AI:** Measures the inherent security capabilities built into an AI system to protect against threats, vulnerabilities, and unauthorized access. Higher values indicate stronger intrinsic security.

- **How it is affected:** Intrinsic security of AI is influenced by several factors, including the robustness of the algorithms used, the quality of training data, and the security measures integrated during the development process. Implementing secure coding practices, employing robust authentication and encryption techniques, and ensuring rigorous validation and testing of AI models can enhance intrinsic security.

These KPIs are essential for maintaining a robust security posture in 6G networks, ensuring that they can effectively counteract emerging threats while protecting user data and maintaining regulatory compliance.

7.3. Reliability

- **Network Availability:** The percentage of time the network is operational and available for use. High availability ensures continuous service for critical applications [ITU2023].
  - **How it is affected:** 6G will support massive connectivity for IoT devices, many of which have limited processing capabilities and may not support advanced security features. The heterogeneity and resource constraints of IoT devices can complicate network management, leading to potential vulnerabilities and points of failure. Ensuring high availability will require scalable and efficient management solutions capable of handling a large number of diverse devices.
- **Connection Density:** The number of connected devices per unit area. It ensures the network can handle a high number of simultaneously connected devices, especially in dense environments [ITU2023].
  - **How it is affected:** device connectivity may be affected by several factors. Authentication failure and DoS attack (in both the RAN and core parts of the network) may provoke this lack of connectivity. Low energy efficiency in both devices and network access components (e.g., gNB) may also cause a reduction in the connectivity capacity of the network.
- **Service Recovery Time:** The time it takes to restore service after a failure or disruption. Minimizing service recovery time is crucial for maintaining continuous service in critical applications [ITU2023].
- **Mean Time Between Failures (MTBF):** The average time between system failures. A higher MTBF indicates a more reliable network infrastructure [ITU2023].

- **Mean Time to Repair (MTTR):** The average time required to repair a failed component or system. Lower MTTR helps in quickly restoring services and maintaining reliability [ITU2023].
- **Packet Loss Rate:** Proportion of packets lost during transmission, indicating network reliability.
- **Redundancy:** Measures the extent to which additional resources, or pathways are incorporated into a network to ensure continued operation in the event of a failure. Higher values indicate greater ability to maintain service continuity and reliability.
    - **How it is affected:** Redundancy is influenced by the design and architecture of the network, including the inclusion of backup systems, duplicate communication paths, and failover mechanisms. The use of fault-tolerant hardware and software, along with automated recovery processes, further contributes to the network's ability to withstand failures.

7.4. Energy

- **Network Energy Consumption:** The total energy consumed by all network components, including base stations, core network elements, and edge devices. Monitoring network energy consumption helps in identifying energy-saving opportunities across the network.
    - **How it is affected:** 6G networks will connect a diverse array of devices, including high-mobility devices like drones and autonomous vehicles. Maintaining connectivity and performance for highly mobile and heterogeneous devices requires adaptive and dynamic network management, which can be energy-intensive. Mobility-induced handovers and the need to provide consistent service levels across various environments further increase energy demands.
- **Energy Consumption per User Equipment (UE):** The average energy consumed by user devices during communication. Lower energy consumption per UE leads to longer battery life and reduced energy demand from user devices.
    - **How it is affected:** Compromised end devices join ranks of botnets performing DDoS attacks or crypto mining which drains the devices’ batteries [Bobrovnikova2020]. The target device of DDoS attack also experiences elevated energy usage due to processing additional packets.
- **Energy Consumption per packet:** Measures the energy required to transmit a single network packet. Lower values indicate higher energy efficiency.

  - **How it is affected:** This metric is influenced by the type of network hardware used, the efficiency of the transmission protocols, and the overall network architecture. By optimizing the deployment of network functions and choosing energy-efficient hardware, the energy consumption per packet can be reduced. Additionally, improvements in software algorithms that manage packet routing and transmission can further enhance energy efficiency.

- **Energy Consumption per Bit (J/bit):** Measures the energy required to transmit one bit of data. Lower values indicate higher energy efficiency.

  - **How it is affected:** The energy consumption per bit is affected by factors such as the efficiency of data encoding and transmission technologies, the quality of the network infrastructure, and the effectiveness of energy-saving protocols. Utilizing advanced data compression techniques, energy-efficient transceivers, and optimizing signal processing can significantly reduce the energy required per bit. Additionally, reducing interference and improving signal quality can also lower the energy consumption for data transmission.

- **Carbon Footprint:** The total amount of greenhouse gases (GHG) emitted due to network operations, usually measured in CO2 equivalents (CO2e). Reducing the carbon footprint is crucial for achieving sustainability goals in 6G networks.

  - **How it is affected:** Devices exploited during DDoS or illicit crypto mining increase the carbon footprint

- **Energy efficiency of LLMs (tokens/kWh):** The number of tokens generated per unit of energy on Large language models (LLMs). It is influenced by multiple factors including model architecture, hardware utilization, and optimization techniques.

  - **How it is affected:** i) Model Architecture: The design of the neural network significantly impacts its energy consumption, ii) Hardware Utilization: The type of hardware used for training and inference plays crucial role, iii) Optimization Techniques: Techniques like model pruning and quantization can reduce the energy footprint of LLMs.

- **Energy Footprint of ML (FLOPS):** Measures the Floating-Point Operations per Second (FLOPS) that a ML model is using and based on this metric we are able to estimate the energy consumption of the ML tasks [Henderson2020]

  - **How it is affected:** i) Model Complexity: The number of parameters in a model significantly impacts its FLOPS. Moreover, different architectures have varying computational efficiencies, ii) Hardware: Graphics Processing Units (GPUs) AND

Tensor Processing Units (TPUs) are optimized for parallel processing, making them more efficient for ML tasks compared to CPUs. Furthermore, newer AI-specific chips are designed to maximize performance per watt, thus improving the energy efficiency of ML operations.

7.5. Cost

- **Revenue:** total income generated by a company
  - **How it is affected:** Server downtime due to DDoS attacks, security breaches and other incidents directly translates to the loss of revenue for the companies. In 2020, 25 percent of respondents worldwide reported the average hourly downtime cost of their servers as being between 301,000 and 400,000 U.S. dollars. [Alsop2019]
- **Employee productivity:** employees' performance in fulfilling their tasks
  - **How it is affected:** Employee's efficiency is impacted by a degraded or a completely down business application or service. Cost per hour of employee downtime should thus be factored into total costs of security breach [Sansone].
- **Remediation costs:** costs of mitigating the impact of an attack or security breach
  - **How it is affected:** To remedy the attack, companies incur additional costs such as overtime, outside consultants, and compensations to customers [Sansone].
- **Market share:** percentage of a total revenue in a market on which a company operates
  - **How it is affected:** Customers dissatisfied due to downtime and security breaches might choose the competitors instead, causing the company to lose market share [Sansone].
- **Ransom costs:** payment demanded by an attacker to unlock a computer or access to data
  - **How it is affected:** Attackers threaten an organisation by holding their files hostage and requiring a ransom fee [Sansone].
- **Total Cost of Ownership (TCO):** Overall cost to own and operate the network, including capital expenditures (CapEx) and operational expenditures (OpEx).
  - **How it is affected:** TCO is influenced by factors such as the initial investment in network infrastructure, ongoing maintenance costs, energy consumption, and the efficiency of network management. Advances in technology that reduce energy

usage and improve operational efficiency can lower the TCO. Additionally, the scalability and upgradeability of the network infrastructure play a significant role in managing long-term costs.

- **Cost per Bit Transmitted:** Financial cost associated with transmitting a single bit of data.
  - **How it is affected:** This metric is impacted by the efficiency of the network's data transmission protocols, the energy consumption of the transmission process, and the overall utilization of network resources. Enhancements in compression technologies, improvements in energy efficiency, and optimization of data routing can reduce the cost per bit transmitted.
- **Cost per Device:** Average cost to connect and maintain a single device within the network.
  - **How it is affected:** The cost per device is influenced by the price of the hardware, installation costs, maintenance requirements, and the network's ability to support a high density of devices efficiently. Technological advancements that enable easier installation, remote management, and reduced maintenance needs can decrease the cost per device.

8. Solutions and Technologies

8.1. Security-by-Design

Security by design is an approach that integrates security from the initial conception and design stages of a system or application up to its implementation and testing stages [Sequeiros2021]. The goal of this strategy is to anticipate and mitigate potential threats and vulnerabilities at various levels of the system. This is achieved through methodologies such as threat modelling during conception, authorization and access management during design, secure coding during implementation, and security testing and audits during the maintenance phase.

A fundamental principle of the security by design approach is Defence in Depth (DiD), which advocates for a layered defensive system to enhance the resilience and security of systems and networks [Kuipers2006]. DiD ensures that if one layer of defence is compromised or fails, additional layers will help mitigate the impact of the attack and prevent further compromise. A practical example of this principle is multi-factor authentication (MFA), which extends authentication beyond just a secure password by requiring additional verification steps.

One way to implement DiD security using 6G orchestration is through Moving Target Defense (MTD) strategies. As further detailed in Section 9.3.4, MTD can leverage the virtualization of network functions in isolated and portable workloads (e.g., VMs, microVMs, and containers) to dynamically migrate them across the 6G infrastructure. This continuous movement disrupts attacker targeting strategies and renders their gathered intelligence obsolete.

In 6G network orchestration and management, while MTD uses strategic placement and movement of network resources to improve security, equally important are also improving service performance, operational cost efficiency, and energy consumption efficiency. These objectives often conflict, potentially favouring one goal on the detriment of another. For example, relocating a VNF from a remote Virtual Infrastructure Manager (VIM) to an edge node's VIM can optimize communication but may be predictable to attackers, thus limiting the security gain. Conversely, random placement enhances security by reducing predictability but can negatively impact network performance and the QoS of the relocated service. Therefore, developing a cognitive decision system is essential to determine the optimal MTD strategy, addressing this multi-objective decision problem [Soussi2023].

The virtualization and the types of virtualized workloads leveraged by MTD is described in the following Section 8.1.1.

8.1.1. Workload isolation

Virtualization has blurred the traditional boundaries between hardware, software, and networking components in ICT systems, paving the way for the microservices paradigm. This paradigm shift has transformed how software is developed, deployed, and managed within modern cloud-based networking infrastructures. By isolating and encapsulating workloads within isolated or semi-isolated environments, virtualization enhances the modularity, portability, replicability, distribution, and autonomous orchestration of microservices-based ICT systems. In microservices architecture, availability and fault tolerance are primarily achieved through application replication and load balancing, which distribute requests across multiple replicas to ensure continuous and reliable service.

Live migration, another feature enabled by workload encapsulation, maintains the resilience and availability benefits of having replicas across distributed nodes without the resource overhead associated with multiple copies. This method ensures that the number of copies remains constant, optimizing resource use.

Additionally, live migration is employed to regulate and reduce energy consumption, particularly in cloud datacenters, through "consolidation" methods. These methods involve live migrating active workloads to a minimal number of hosts, allowing other datacenter nodes to enter hibernation, thus conserving energy [Hermenier2006]. Security is also enhanced through both isolation and portability. Portability, for instance, facilitates the implementation of MTD operations such as evasion techniques [Soussi2021]. The following subsections describe the characteristics of state-of-the-art virtualization technologies, specifically VMs, microVMs, containers and system interfaces such as WASI.

8.1.1.1. MicroVMs

There are several technologies that enable the creation of microVMs, among which unikernels are a varied group with excellent security and performance features [Kuenzer2021, Abeni2023]. Unikernels are a type of library operating system in which a program, along with only the required system libraries and system calls, is compiled into a single kernel space executable embedded in a VM image, thus minimizing image size and attack surface. Furthermore, they can be roughly classified into two types: POSIX-compatible ones that focus on existing software, and those based on non-POSIX system interfaces which sacrifice compatibility for smaller images and lower resource requirements. OSv [Kivity2014] in particular is a POSIX-compatible unikernel platform with wide compatibility for existing programs and programming language runtimes. Although microVMs generally support a wide variety of hypervisors for their execution, QEMU with KVM (Kernel-based Virtual Machine) acceleration is a widely supported option. Different classes of virtualization technologies, including gVisor and Firecracker, have been compared and benchmarked [Goethals2022], and their performance examined at the kernel level [Anjali2020].

8.1.1.2. Containerization

Containers represent partially isolated workloads that, in contrast to VMs, do not run a full OS kernel of their own but operates with the OS kernel of the host machine. This reduces container image size and memory overhead on the host during its life cycle, and makes it faster to spin-up (because VMs have to initiate a full OS), reduces backups duration and storage (because of reduced images size), and generally makes it faster to manipulate (i.e., to replicate, to snapshot, to migrate, and to restore). On the other hand, VMs have more technological maturity and knowledge base, as it came long before the usage of containers, and provides a higher isolation of the workload independent of the host's OS (but not the host's hypervisor), making VMs arguably more portable than containers, which mainly depend on the OS kernel being Linux.

Containers can be of two types, application containers (e.g., Docker), and system containers (e.g., LXC). The latter provides an improved semi-isolated environment with an OS of its own, but still reliant on the host's OS kernel for functionalities like device management and system configuration, maintaining containers' lightweight properties.

Another significant difference lies in how applications are implemented using VMs compared to containers. For instance, 5G/6G vendors developing virtual network functions (VNFs), following the ETSI NFV standard, typically consolidate all necessary components into a single VM. This results in a single sizeable monolithic application. In contrast, for cloud-native network functions (CNFs) using containers the microservices development approach is adopted. This involves implementing multiple smaller services in portable and relatively independent containers, easier to transfer and manage by automated orchestrators (such as Kubernetes).

The primary methods for isolating containers rely on three key Linux features known as namespaces, control groups (Cgroups), and rootfs [Kumaran2017]. The reduced isolation exposes the risk of container escaping vulnerabilities and system privilege escalation [Souppaya2019]. Recent examples of such exploited vulnerabilities include CVE-2019-5736, CVE-2022-0185, and CVE-2022-0811.

Containers can be classified into two types, i.e., operating system-level containers and application-level containers. Both types run within an isolated environment within the host and share the underlying kernel of the host. By sharing the underlying kernel of the host operating systems, containers are more lightweight compared to VMs, with boot times of only a couple of seconds, and almost native host performance. Operating system level containers run an entire operating system, whereas application-level containers run an application or service, bundled with a minimal set of dependencies required by that application [Kumaran2017].

Figure 1 depicts a simplified overview that illustrates how application-level containers are organized on a host. Note the container runtime in between the host operating system and the containers. A container runtime is the counterpart of a VM hypervisor and is responsible for running and managing containers. Container runtimes can be divided into two groups, i.e., low-level and high-level container runtimes. A low-level container runtime mainly focuses on running a container, while a high-level container runtime has more advanced functionality, such as, managing container lifecycles and images, providing certain application programming interfaces, etc.

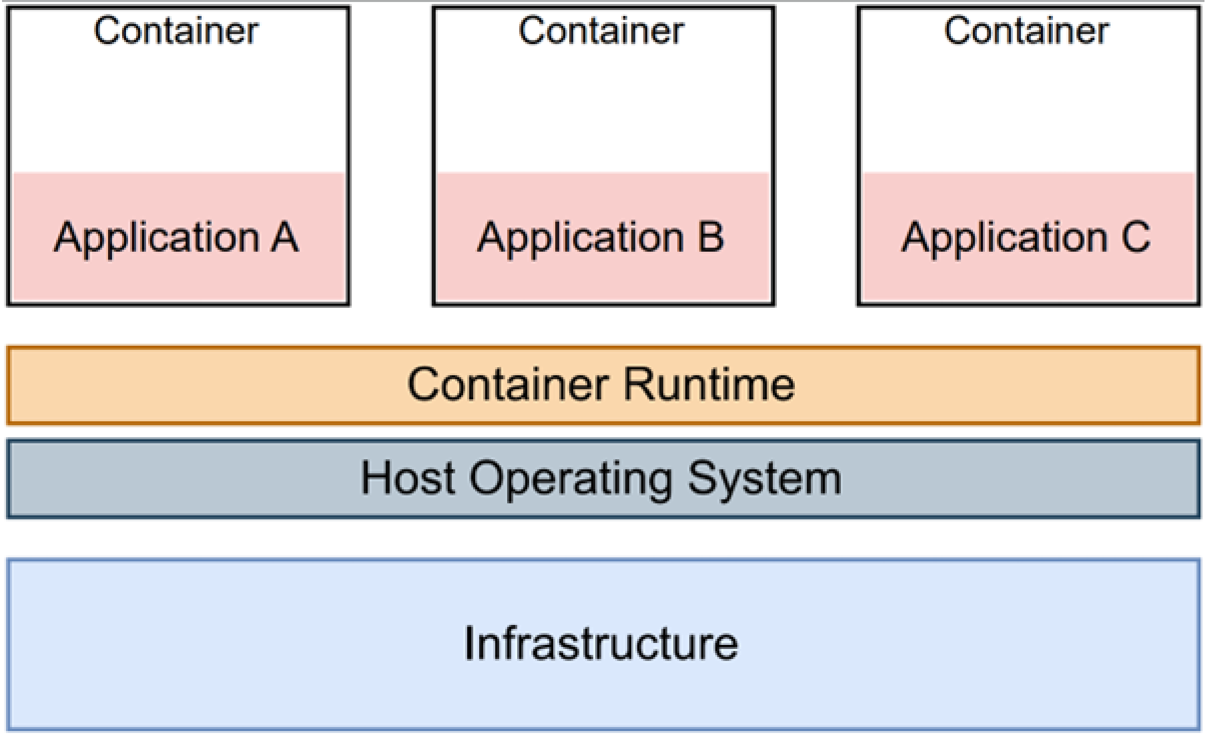

Figure 1 Simplified schematic overview of application-level containers.

8.1.1.3. WebAssembly

As a more secured and performant variant of Javascript, WebAssembly (Wasm) fosters payload migratability, in perfect alignment with NATWORK project. Wasm is a binary instruction format for a stack-based VM. Wasm was originally developed for improving the performance of Web applications in Web browsers and allowing fully featured complex applications to securely run in the browser. Wasm is designed as a portable compilation target for a wide variety of programming languages [Haas2017].

Since Wasm was originally developed to run untrusted code, i.e., code provided by unknown websites, security is one of the main focuses. Just like JavaScript code runs inside a secure sandbox inside the browser’s runtime to prevent malicious code to access system files or resources, Wasm is also sandboxed. Wasm binary code is executed by a Wasm VM (i.e., Wasm runtime) by either using Just In Time (JIT) compilation to compile the binary code to native machine code at runtime, or by running native machine code which was transpiled from Wasm binary code beforehand using Ahead Of Time (AOT) compilation. Although the name implies it, Wasm is not merely limited to the Web. Several runtimes enable the execution of Wasm binaries on a myriad of platforms via a system interface that enables direct OS communication, called WASI (WebAssembly System Interface) [Spies2021].

To employ Wasm outside the browser as a replacement for traditional application containerization, access to OS functionality is provided by the WASI Application Programming Interface (API). WASI is a fast, secure and security focused system interface for the Wasm platform and consists of a modular collection of API proposals defined with the Wasm Interface Type (WIT) Interface Description Language (IDL). WASI provides a secure and portable way to access several system resources, such as files, networking, Document Object Model (DOM) manipulations, peripheral devices, etc [Clark2019]. The Bytecode Alliance [5], an industry partnership focussing on developing Wasm outside the browser by collaborating on standardization proposals and implementation, maintains two Wasm runtimes: Wasmtime[6] and WAMR[7].

Wasmtime [Clark2022] can be considered as a general-purpose runtime, focussing on server-side and non-web embeddings with components. It has full component model support and first-class support for eight programming languages, and community support for an additional two. On the other hand, WebAssembly Micro Runtime (WAMR) [BytecodeAlliance2019] is specifically designed to be as lightweight as possible, targeting embedded devices and the edge. This translates itself into the provided features and the supported guest languages. Support for the component model is planned for the end of 2024, and it only has robust support for C and C++. Due to this, Wasmtime is currently the de-facto Wasm runtime to run Wasm outside of the browser.

WasmEdge[8] is a Wasm runtime that is not maintained by the Bytecode Alliance, but is a Cloud Native Computing Foundation Sandbox project, maintained by The Linux Foundation. WasmEdge mainly focuses on bringing Wasm to the Edge by enabling cloud-native, serverless, and decentralized applications to run on edge devices, such as low powered IoT Single Board Computers (SBC). The WebAssembly Component Model is an architecture for building interoperable Wasm libraries, applications and environments. It builds on top of the core WebAssembly specification by introducing a standardized way of specifying modules. These components express their interfaces and dependencies via WIT and the canonical Application Binary Interface (ABI). The canonical ABI defined by the component model defines the binary representation of the WIT type definitions. Unlike core Wasm modules, components may not

[5] https://bytecodealliance.org/
[6] https://wasmtime.dev/
[7] https://bytecodealliance.github.io/wamr.dev/
[8] https://wasmedge.org/

Co-funded by the European Union 6GSNS Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI UK Research and Innovation

export Wasm memory, reinforcing Wasm sandboxing and facilitating interoperation between languages with different memory assumptions.

8.2. Trust management

Trust management is the process of establishing, maintaining, and evaluating trust relationships to ensure secure and reliable interactions between individuals, organizations, or entities. When dealing with trust management, one has to bear in mind that trust relations naturally appear on different levels and with different characteristics. There is administrative trust in form of agreements, written in conventional contracts (i.e. analogue paper contracts), and signed by trusted and authorized humans of each participating party and there is the technical level of trust which based on the conventional contracts applies the administrative trust between the technical components. Below we present the current State of the Art for trust management systems between actors, systems (assets) also providing some information considering Trust assessment.

8.2.1. Trust between actors

Trust among different stakeholders is fundamental to the integrity and functionality of many systems like digital communications, financial transactions, business operations etc. Establishing trust ensures that parties can reliably interact, exchange information, and perform transactions with confidence in each other's authenticity and intentions.

8.2.1.1. Reputation based systems

Reputation-based systems evaluate the trustworthiness of entities based on their past behaviour or interactions, assigning reputation scores to influence decision-making processes and promote trust within a community. Based on architecture, only two ways of implementation exist, distributed (decentralized) or centralized.

Centralized systems rely on a central node to collect, aggregate and manage reputation data. Sites like e.g. Amazon are classic examples of centralized reputation systems, where a central server manages and processes all data [Resnick2002]. This is effective in environments where trust is high. A system with unlinkable user behaviour was proposed in [Garms2019], shifting the reputation values, from items to users, in order to be more realistic and secure. Distributed or decentralized systems distribute reputation management among all nodes participating. Many approaches exist, such as the EigenTrust algorithm [Kamvar2003], which calculates global trust values based on the transitive trust of peers, significantly improving trust in peer-to-peer networks and reducing the effect of cooperating malicious nodes. A more complex system is PeerTrust [Xiong2004], which calculates multiple parameters, including the number of transaction and credibility of feedback sources, among others and is context aware. Another paper proposed DRBTS [Srinivasan2006], where sensor nodes depend on trusted beacon nodes, using a simple majority principle for providing location information. Simulations demonstrate the scheme's robustness in dense networks, its adaptability to various security requirements, and its minimal overhead compared to similar approaches. Blockchain based solutions also exist [Mrabet2023], in order to create immutable and transparent reputation systems, where secure multiparty computation ensures confidentiality of feedback.

8.2.1.2. Trusted third-party

Trusted third parties (TTPs) are entities that facilitate trust between parties in digital transactions by verifying identities and credentials. The concept of TTPs has evolved from the need for intermediary entities that can vouch for the trustworthiness of participants in a digital ecosystem, resulting in many different types.

A TTP-based scheme was introduced [Rizvi2014], that enables cloud customers to encrypt data using symmetric key algorithms, with the TTP handling key management and heavy computations to ensure data confidentiality while reducing client-side computational burden. A novel TTP-based e-service was proposed, using blockchain technology and cryptographic methods to securely manage and store sensitive electronic documents, with an independent company acting as the TTP [Bazydło2024]. TTP-mtOTP [Trahan2022] is a protocol for transferring multiple RFID-tagged items from an old owner to a new owner using a trusted third party (TTP) to ensure privacy and security. The TTP authorizes the transfer, authenticates the new owner, and the protocol is shown to be resistant to multiple security attacks while being compared favourably against other TTP-based OT protocols in terms of privacy, security, computation, and communication. There, also, exists a TTP-based signcryption scheme [Ullah2020] using symmetric session key exchange protocols to protect against man-in-the-middle and Denial-of-Service attacks in cloud computing. This scheme offloads encryption and decryption from the TTP, providing enhanced security features such as data integrity, confidentiality, authenticity, non-repudiation, forward secrecy, unforgeability, and un-traceability, and demonstrates superior performance in flexibility, reliability, and efficiency compared to existing schemes. A contract signing protocol introduces a TTP as an offline arbitrator that intervenes during disputes, ensuring fairness and security in the contract signing process [Wang2018]. It utilizes an identity-based confirmation signature scheme, which is secure against existential forgery under the CDH assumption and offers a flexible construction that avoids the impracticality of classical public-key techniques for identity-based signatures from bilinear pairings.

8.2.1.3. Use of Certificates

Certificates are digital documents used to establish the identity and credentials of entities (individuals, organizations, or devices) involved in electronic transactions and communications. They are a critical component of Public Key Infrastructure (PKI) systems, ensuring secure data exchange over the internet by enabling authentication, data integrity, and encryption. An experimental protocol for publicly logging Transport Layer Security (TLS) certificates exists, enabling auditing of certificate authority (CA) activity and identification of suspect certificates [Laurie2013]. The protocol aims to increase transparency by allowing anyone to audit both CA activity and the certificate logs themselves. It often works in conjunction with public key pinning, where a new HTTP header is introduced, enabling web host operators to instruct user agents to "pin" cryptographic identities for a defined period [Evans2015]. This pinning requires hosts to present certificates matching pinned fingerprints, thereby mitigating man-in-the-middle attacks by limiting trusted authorities and reducing reliance on potentially compromised Certification Authorities. A novel solution for certificate revocation was offered [Naor2000], utilizing authenticated dictionaries to represent revocation lists for efficient verification and updates. It improves scalability, communication costs, and robustness compared to traditional methods, with compatibility with X.500 certificates. Also, a certificate-based encryption (CBE) was introduced [Gentry2003], as a means to simplify Public Key Infrastructure (PKI) by enabling implicit certification, eliminating third-party queries on certificate status. Additionally, its incremental CBE scheme significantly reduces CA's computation and bandwidth requirements without employing hash chains or trees typical in previous PKI proposals. Another paper defines certificate-based signatures [Kang2004], aligning with Gentry's encryption scheme, and presents two specific schemes with security proofs under a GDH group assumption. This approach may aid in constructing an efficient PKI integrating Gentry's CBE scheme and provides a delegation-by-certificate proxy signature scheme with proven security.

8.2.2. Trust of systems and assets

As networks get more diverse, the need for verification on components and assets becomes increasingly more important. In this context, assets include hardware and software components but not data.

8.2.2.1. Zero trust architectures

Among the most notable design approaches for trusting digital assets and systems is zero trust architectures (ZTAs). This approach focuses on establishing authentication and trust relationships for each asset rather than implicitly trusting an asset based on its location (for example an asset located on an internal company network). At each core, ZTA has a policy engine which is responsible for verifying components according to a set of rules. A summary of methodologies can be seen here [Stafford2020, He2022, Syed2022, Buck2021]. These are generally divided into user to machine verification, where proposed solutions include certificates, organization issued identities and biometrics among others, and machine to machine verification where techniques can also include measurements on standard device usage and machine learning assisted authentication.

8.2.2.2. Remote attestation

Another innovative approach deals with verification of remote systems and applications running on them is remote attestation. Current literature presents several approaches based on the target platform application. Clemens et al [Clemens2018] present a framework for resource constraint IoT devices where the required metrics are taken on the device during runtime, while the rest of the functionalities are offloaded to a node with more available resources. Another example of IoT remote attestation [Gonzalez-Gomez2024] leverages performance metrics modules available to a device and a pre-trained device specific machine learning classifier to predict if the device is behaving normally or not. Other examples focus on cloud computing solutions. One such example is seen here [Hassan2020] where a QoS metric is used to assess whether a cloud provider abides by the agreed upon SLAs and user requirements. Thijman et al [Thijsman2024] present another scenario where cloud-edge trust is required, but edge devices may be accessible to the attacker. To mitigate this threat, devices are enrolled as Kubernetes worker nodes and are classified into Kubernetes clusters, which provide metrics on device behaviour. Other approaches to remote attestation include utilizing trusted platforms modules and are split into singular attestation, where one device is evaluated, and swarm attestation, where a network of devices is being collectively evaluated. An overview of those techniques can be found here [Banks2021].

8.2.2.3. Local & Remote Attestation

Local & Remote attestation considers the trust of the software stack based on hardware root of trust and remote verifying parties. Figuring out what to measure remains a major challenge. Bravi et al. [Bravi2023] present a trust monitor that takes input from multiple attestation technologies to manage trust in heterogeneous infrastructures, allowing multiple technologies to work together in protecting the entire device (firmware, kernel, runtime). Research on automated policy decisions based on attestation inputs remains underdeveloped. Thijsman et al. [Thijsman2024] present a platform to enroll physically vulnerable edge devices in a cluster after remote attestation. They provide a link between attestation events on the device and its cluster permissions. The binary nature of these measurements, either pass or fail, is identified as an open challenge. To meet required security-SLAs a more flexible system is required, capable of dynamically adjusting trust levels based on SBoMs or other reference sources.

This heterogeneity is a cause for concern and an active part of the research field. Attestation relies on a strong root of trust for measurement, using a TPM as this RoT has proven beneficial due to its rigorous standardization benefiting homogeneity in an otherwise heterogeneous field. Problems arise however when identifying the anchor for this RoT, which often relies on proprietary CPU implementations such as Intel TXT leading to a plethora of TPM based solutions without a clear anchor for the RoT. Efforts to bypass this have resulted in (partial) TPM implementations based on trusted execution technologies (Song2022, Narayanan2023), while these solutions do not take away the use of proprietary solutions such as ARM TrustZone or Intel SGX they do provide more clarity on the anchor for a RoT.

Finally, decentralized attestation is an active topic of research. In edge or IoT networks, devices might not always have access to a centralized trust server or might not want to rely on such a single point of failure. Devices might also want to extend their trust to another party's trust domain and prove themselves there. Blockchain and smart contracts are often used to provide trust in such situations [Zhang2024].

Complementary, few trust-based solutions have been proposed to mitigate DoSt/EDoS attacks, including EDoS shields and self-verifying Proof-of-Work (sPoW) [Ta2022]. The former is a filtering approach that allows cloud nodes to accept/reject incoming requests based on trust in the source; whereas the latter is an integrity verification mechanism that requires a source of demand to solve a PoW to verify their identity.

8.2.2.4. Natwork's considered Platform-agnostic payload trust leveraging blockchain

Trust on deployed payloads will be improved by considering platform-agnostic blockchain remote attestation by SECaaS, as a continuity of work processed in [DESIRE-6G D3.1]. This work fosters a simplified mutual attestation scheme where any SECaaS-processed software nodes can mutually be verified, then verify other nodes, breaking all forms of hardware based or kernel-based dependences and drastically simplifying the reference measurement provisioning of classical remote attestation. During Natwork, this work will expand the support to three types of covered payloads of the project (i.e., machine compiled payloads, containerized payloads and WASM). In that vein, the project will cover different sorts of claims including static claims (e.g., memory footprint of the payloads, reflecting authenticity at bootstrapping stage or runtime integrity preservation during execution) and novel claims such as proof of execution or performance rating as initiated in [DESIRE-6G D4.1] by control flow monitoring when an instrumentation is made possible, typically through a SECaaS payload rewriting or processing. Last, the project will consider up to date progresses made by processor vendors and Linux working groups and associations to reach platform-agnosticity with trusted execution environments.

Complementary, few trust-based solutions have been proposed to mitigate DoSt/EDoS attacks, including EDoS shields and self-verifying Proof-of-Work (sPoW) [Ta2022]. The former is a filtering approach that allows cloud nodes to accept/reject incoming requests based on trust in the source; whereas the latter is an integrity verification mechanism that requires a source of demand to solve a PoW to verify their identity.

8.2.3. E2E trust assessment

Understanding, classifying, measuring and assessing the levels of trust have been some of the fundamental research challenges in trust management [Jøsang2005], uncertainty reasoning [Jøsang2016], computing [Marsh1994], information security [Grandison2003, Jensen2014], and security risk analysis [Lund2010]. Trust fusion from different sources and discounting of a re-commented evaluation based on confidence in the entity conducting the evaluation have always been two focal points in trust management and recommendation networks. Trust fusion has been formalized in Subjective Logic (SL) and used for in a variety of applications including multi-source and biometric information fusion [Vishi2017]. In recent years, the semantics initially attributed to fusion operators in SL, have been the subject of criticism [Dezert2014] and subsequent improvement [Jøsang2017, Heijden2018] after better clarifying the relationship of SL to Dirichlet distributions and Dempster-Shafer belief functions [Jøsang2007]. Bayesian distributions and networks have been studied for trust level evaluation and recommendation networks [Nguyen2018], for managing uncertainty in relation to trust [Ivanovska2015] and for trust fusion [Rafailidis2019]. Recent work [Ivanovska2018] has brought together Bayesian networks with subjective trust networks [Jøsang2016] into subjective networks that extend subjective trust networks with the ability to reason not only over uncertainty but also about previously unknown relationships. There is a growing research interest in using trust management and uncertainty reasoning for highly distributed and/or federated environments and 5/6G related verticals including misbehaviour detection [Dietzel2014, Heijden2019, Kamel2020, Müller2021].

8.3. Attack detection & Protection

8.3.1. RAN Jamming detection and protection

In recent years, several research efforts have been performed to investigate the different anti-jamming techniques in wireless communication, especially in the RAN domain. These includes massive MIMO techniques, spectrum spreading techniques, alternative eNodeB, dynamic resource allocation, jamming detection mechanisms, and coding techniques.

The interference cancellation efficacy of MIMO communications improves significantly with the increase in the number of antennas, a characteristic of massive MIMO technology. However, due to its high power demands and the extensive space required to house a large array of antennas, massive MIMO is typically implemented in cellular base stations (eNodeB). As a result, massive MIMO techniques are utilized to counteract jamming attacks in cellular uplink transmissions. Vinogradova et al. [Vinogradova2016] suggested projecting the received signal onto the estimated signal subspace as a method to nullify jamming signals. The principal challenge with this technique lies in accurately identifying the user's signal subspace.

Researchers [Do2017] developed a jamming-resilient receiver for massive MIMO systems to handle constant broadband jamming in cellular network uplink transmissions. Their approach involves reserving some pilot signals within a frame, which are then used to estimate the jammer's channel. Concurrently, legitimate users estimate their desired channels amidst the jamming. Leveraging the law of large numbers, thanks to the multitude of antennas on the base station (BS), this method allows for the creation of a linear spatial filter at the BS. This filter mitigates the jamming signal and helps recover the legitimate signal. Akhlaghpasand et al. [Akhlaghpasand2017] introduced a method to detect jammers in massive MIMO systems using unused pilots during the training phase, applying a generalized likelihood ratio test on these pilots in uplink transmissions to evaluate the method's accuracy and study how the number of unused pilots and antennas at the base station affects performance.

Besides MIMO-based jamming mitigation, rerouting traffic via an alternative eNodeB offers another strategy [Makarevitch2006] for dealing with jamming attacks in cellular networks. If the currently serving eNodeB is compromised by jamming and becomes non-functional, users can switch to a different eNodeB if one is available. Coding and scrambling methods are also employed to safeguard wireless communications from jamming attacks in cellular networks. Jover et al. [Jover 2014] concentrated on enhancing the security of the physical channels in LTE networks, specifically the PBCH, PUCCH, and PDCCH. Arjoune et al. [Arjoune2020] analyzed the effectiveness of current machine learning techniques for detecting jamming in 5G communications, specifically assessing the performance of neural networks, support vector machines (SVM), and random forest algorithms. They created a database for this purpose using metrics such as packet error rate, packet delivery ratio, and received signal strength. They used different machine learning algorithms using PER, RSS, and PDR features for the constant jamming attack application scenario. Sadeghi et al. developed an algorithm to create physical adversarial perturbations targeting an end-to-end auto-encoder wireless system. They demonstrated that these designed adversarial attacks are more disruptive than traditional noise-like constant jamming attacks. Zhong et al. introduced two learning-based adversarial attacks aimed at diminishing a legitimate user's channel access performance. Within their framework, the user employs a dynamic channel access mechanism facilitated by an actor-critic deep reinforcement learning (DRL) model. The attacker transmits a jamming signal to a single channel during each time slot, thereby decreasing the accuracy of the user's channel selection. Zhu et al. explored jamming attacks on mmWave MU-MIMO systems and proposed a hybrid beamforming strategy that enables users to reclaim their signals despite jamming. Specifically, they designed analog beamforming vectors to nullify jamming at each user and digital beamforming vectors to eliminate inter-user interference. Xiao et al. investigated the resilience of mmWave massive MIMO systems against smart jamming attacks, proposing a learning-based power allocation strategy for massive-antenna base stations. They assessed how the number of transmit antennas influences the network's achievable sum rate.

Moreover, Reconfigurable Intelligent Surfaces (RIS) [Naeem2023] represent a state-of-the-art technology that facilitates the control and manipulation of electromagnetic waves via a planar surface comprising multiple, reconfigurable unit cells. Key attributes of RISs include the ability to manipulate electromagnetic waves in a controlled and precise manner, their high degree of flexibility and compatibility with existing communication systems, and their relatively low cost. RISs offer extensive functional versatility, as they can be configured to provide a range of capabilities, including signal enhancement, noise reduction, beam steering, absorption, and anomalous reflection. RIS has emerged as a significant physical layer security module [Bae2024]. By directing signals in specific directions and blocking them beyond designated boundaries and frequency bands, RIS can bolster the security of communication systems. In addition to enhancing communication security, AI techniques can be utilized to optimise the RIS configuration to maximise its security capabilities.

[Zou2023] adopted the RIS deployed on an unmanned aerial vehicle (UAV) to enhance information transmission while defending against both jamming and eavesdropping attacks. Furthermore, an innovative deep reinforcement learning (DRL) approach is proposed with the purpose of optimizing the power allocation of the base station (BS) and the discrete phase shifts of the RIS. [Cao2022] developed alos the relax-and-retract based joint transmit and reflecting beamforming to enhance the received signal of the legitimate device and mitigate anti-jamming signal of the jammer. Simulation results verified that the developed scheme can enhance the anti-jamming performance of multiple RISs (multi-RIS) assisted aerial-ground system with lower complexity compared with existing methods.

8.3.2. Multi layer DDoS detection and protection

Recently, the frequency and intensity of DDoS attacks have increased significantly. Due to that, researchers have been actively developing solutions to counter such volumetric attacks [Zhao2024]. The protection against DDoS attack can be realized through approaches such as implementing cryptographic measures that prevent attackers from being able to issue the attack. Additionally, by studying the normal patterns of the traffic, the abnormal traffic including the DDoS attack can be detected and prevented. Ma et al. [Ma2022] proposed a model to protect against DDoS attacks in 6G by assessing the trustworthiness of devices. This proposal combines spatial and temporal trust values to effectively represent the usual behaviour patterns of the devices and, as a result, distinguish between attack traffic based on previous communication behaviours. A signature-based approach to detect DDoS attacks in 6G networks proposed by Nazar et al. [Nazar2023]. In order to detect malicious behaviour of nodes, an anomaly detection system has been proposed that uses attack signatures to detect and mitigate the DDoS attack.

Chen et al. [Chen2024] proposed a defence architecture to prevent the DDoS attack. Their proposal targets specific field of V2X, through 6G.

Utilizing AI based approaches, specifically ML techniques become one of the main methods in detecting DDoS attacks in 6G [Ma2022]. SDN/NFV enabled networks may utilize AI techniques for intrusion detection and prevention [Abdulqadder2020]. Compared to traditional approaches, AI based approaches efficiently protect against various security attacks, including DDoS. Due to their accuracy and fast rate of processing, machine learning techniques have shown to be effective in detecting DDoS attacks in SDN systems [Santos2020]. Kianpisheh and Tarik [Kianpisheh2024] proposed a federated learning-based approach to prevent several security attacks in 6G, focusing on DDoS detection as a use-case. In their proposed model, deep reinforcement model has been adopted to solve the trade-off between the DDoS attack detection and response time.

Machine Learning (ML)-based DDoS detection methods can be categorized into three primary groups [Najafimehr2023], namely supervised, unsupervised, and hybrid, each with multiple subcategories. A comprehensive taxonomy of ML-based DDoS detection methods is presented. Idhammad [Idhammad2018] et al. proposed a hybrid learning approach for DDoS detection consisting of three steps: entropy computation, co-clustering, and classification. First, the average entropy of four features, including Source packet count, Destination packet count, Source byte count, and Destination byte count, is computed for an online traffic time window.

Author et al. presented a novel DoS/DDoS attack dataset collected from a simulated 5G network slicing test bed. Finally, they showed a deep-learning-based bidirectional LSTM (Long Short Term Memory) model, namely, SliceSecure can detect DoS/DDoS attacks with an accuracy of 99.99% on the newly created data sets for 5G network slices. They generated a new dataset for benign traffic and DoS/DDoS attacks traffic with the simulated 5G network slices and made it publicly available. They simulated a 5G network slice testbed using Free5GC [Free5GC] and UERANSIM [UERANSIM] and showed the impact of DoS/DDoS attacks on performances of 5G network slices.

Author [Bousalem2022] et al. introduced a 5G prototype that utilizes Machine Learning (ML) for attack detection and mitigation within sliced networks. Built on OpenAirInterface, the prototype facilitates the on-demand creation of network slices and the dynamic allocation of physical resources, guided by user behaviour and inputs from a northbound Software Defined Network (SDN) application. The focus is on Distributed Denial of Service (DDoS) attacks targeting the 5G Core Network, executed by one or more malicious users. With the implementation of a specially developed ML module, it has been demonstrated that the prototype can detect these attacks, and then autonomously establish a sinkhole-type slice with limited physical resources to isolate the malicious users.

Author [Hussain2020] et al. proposed a methodology to convert the network traffic data into image form and trained a state-of-the-art CNN model using ResNet. The problem is addressed by Author [Alanazi2022] et al. through the proposal of a deep learning (DL)-based ensemble solution for efficient detection of DDoS attacks in SDN. Four hybrid models are presented, employing three ensemble techniques and various DL architectures, such as convolutional neural networks, long short-term memory networks, and gated recurrent units, with the aim of enhancing SDN traffic classification. Experimentation was carried out on the benchmark flow-based dataset CICIDS2017. The most common DDoS attacks are SYN, TCP, ICMP, UDP, HTTP, and DNS flood [Seifousadati2021].

Various machine learning (ML) and deep learning (DL) models have been employed for network attack detection [Sharafaldin2019]. Decision tree (DT), logistic regression (LoR), linear regression (LR), Naive Bayes (NB), support vector machine (SVM), K nearest neighbor (KNN), random forest (RF), XGBoost, AdaBoosting, ResNet, artificial neural networks (ANNs), and convolutional neural networks (CNNs) have been applied using the CICDDoS2019 dataset to detect DDoS attacks. Additionally, the CICIDS2017 dataset, KDD datasets, CAIDA 2007 dataset, IoT NI, BoT IoT, MQTT, MQTTset, IoT-23, IoT-DS2, and UNSWNB15 datasets have been utilized for DDoS attack detection. The CICDDoS2019 dataset is well-known for evaluating the performance of ML and DL models for DDoS attacks, containing real-time DDoS attacks from network traffic. It encompasses a wide range of DDoS attacks, including 'DNS', 'SNMP', 'NTP', 'WebDDoS', 'MSSQL', 'UDP', 'LDAP', 'NetBIOS', 'SSDP', 'PortScan', 'UDP-Lag', and 'SYN'. Researchers often utilize this dataset to identify optimal features and models for DDoS attack detection, aiming to minimize execution time. In a recent survey, Author [Ali2023] et al. conducted a systematic review for using ML/DL approaches to identify DDoS attacks in SDN networks.

In recent studies, the enhanced processing capabilities and programmability of modern network switches have been leveraged to develop innovative paradigms in Intrusion Detection Systems (IDS) and Deep Packet Inspection (DPI).

Author [Ramzan2023] et al. investigated the Distributed Denial of Service Attack Detection in Network. This study adopts deep learning models including recurrent neural network (RNN), long short-term memory (LSTM), and gradient recurrent unit (GRU) to detect DDoS attacks on the most recent dataset, CICDDoS2019, and a comparative analysis is conducted with the CICIDS2017 dataset.

Author [Alahmadi2023] et al. conducted a recent survey mentioning DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models. DDoS attacks are one of the major risks to the security of IoT networks. In this attack, the attacker uses numerous compromised nodes to overwhelm the target by producing significant network traffic that consumes the target's resources. This eventually destroys the infrastructure, interrupts services, and prevents authorized users from accessing associated services. DDoS attacks employ two diverse types of techniques: reflection and amplification techniques.

Author [Alzhrani2023] et al. applied two Deep Learning algorithms Convolutional Neural Network (CNN) and Feed Forward Neural Network (FNN) in a dataset specifically designed for IoT devices within 5G networks. They provided a detailed description of the dataset used in the study, the network infrastructure, and the Deep Learning algorithms used for DDoS detection. Author [Talpur2024] et al. introduced an innovative approach by integrating evolutionary optimization algorithms and machine learning techniques. This study proposes XGB-GA Optimization, RF-GA Optimization, and SVMGA Optimization methods, employing Evolutionary Algorithms (EAs) Optimization with Tree-based Pipelines Optimization Tool (TPOT)-Genetic Programming. Datasets pertaining to DDoS attacks were utilized to train machine learning models based on XGB, RF, and SVM algorithms, and 10-fold cross-validation was employed.

Recently, Author et al. [Xavier2023] demonstrated a Machine Learning-based Early Attack Detection system utilizing the Open RAN Intelligent Controller. This approach leverages the OpenRAN framework to gather measurements from the air interface for attack detection and dynamically manage the operation of the Radio Access Network (RAN). A Machine Learning model was designed to classify various types of DoS attacks with high accuracy using the air interface measurements collected by the near-real-time RIC, specifically focusing on physical and MAC layer measurements.

An attacker penetrates the Non Real-Time RAN Intelligent Controller (Non-RT RIC) [O-RAN2021] to cause a DoS or degrade the performance. Open RAN systems can employ machine learning algorithms that are trained to protect the network from DDoS attacks with very high accuracy. For example, a plethora of ML based mechanisms for DDoS detection can be found in the literature [Doshi2018]. Five classification methods, including K-nearest neighbors (KNN), Decision Tree (DT), Random Forest (RF), Support Vector Machine with linear kernel (L-SVM), and Neural Network (NN) have been studied for intrusion detection. The authors found that all five methods were able to detect DDoS attacks with a high level of accuracy. However, the authors considered only three types of DDoS attacks. A total of 13 different DDoS attacks were considered [Sharafaldin2019].

O-RAN security report [Quad2023] defined the 14 requirements and 6 controls for the RAN Intelligent Controllers and associated RAN Apps which primarily relate to authentication and authorization, the protection of information exchanged between these components, and the ability to recover from DDoS attacks.

A promising new approach has emerged with the integration of programmable network devices into these efforts. In one such solution, [Yoo2024] enhance the classic SYN cookie method used to mitigate SYN flooding attacks by introducing a split-proxy design. In this design, a server agent tracks established connections while a switch agent handles the heavy lifting of managing traffic and calculating SYN cookie hashes. This approach maintains the line-rate speed of programmable switches and overcomes the limitations and vulnerabilities associated with small memory sizes. In another approach, Zhang et al. [Zhang2020] developed a framework called Poseidon, which includes a policy language enabling system administrators to easily articulate and deploy defense policies across their networks in an automated and distributed manner. This solution offers both versatility and ease of use, as it protects against various types of volumetric attacks, including SYN floods, DNS amplification, and UDP floods. Importantly, users do not need to understand the specific details of how the generated application is allocated across available resources.

Author [Djuitcheu2023] et al. investigated the role of policy and regulation in enhancing the security and resilience of 5G systems against DDoS attacks, highlighting the need for incorporating DDoS attack resilience into policy and regulatory frameworks, collaborating with regulatory bodies to define security standards and compliance requirements, and fostering information sharing and coordination among 5G stakeholders.

Author et al. delve into user plane DDoS attacks leveraging the IP protocol stack to generate excessive traffic [Abdelrazek2024]. They introduce a novel detection method situated within the Radio Access Network (RAN). This method analyses the patterns of radio protocols and their functionalities to identify user plane DDoS attacks initiated from User Equipment (UEs). Crucially, the method does not depend on directly scrutinizing user plane packets such as IP packets. Instead, it utilizes the attributes of 3GPP radio protocols (such as MAC, RLC, PDCP) to identify IP DDoS attacks nearer to their source. This early detection capability aids in preventing DDoS traffic from spreading to the transport network.

For DoSt/EDoS, various machine learning approaches have been proposed to detect this form of attacks in cloud networks (including SDN-enabled clouds). The work of [Dinh2020, Din2021] proposes a LSTM-based machine learning detection system that analyses historical time-series data of CPU, storage and bandwidth utilisation to identify abnormal workload and traffic flow patterns. The work of [Ta2022] adopts a ML approach analyses the features of SDN flows and score them to steer attention towards abnormal traffic, suspected of being part of a EDoS attack.

8.3.3. Edge/MEC attacks detection and protection

Compared to previous technologies, 6G depends on the intelligence on the edge. Therefore, MEC that aim to bring the power of cloud computing to the edge of the network is considered as a promising technology and a potential enabler for 6G. However, because of the distributed nature of 6G networks, MEC in 6G is vulnerable to various security attacks, including physical attacks [Ranaweera2021]. Due to that, in late 2014 ETSI has initiated MEC Standarization [ETSI2014] to update various issues and providing a standardized MEC architecture [HU2015].

Many researchers utilized AI based technologies to secure the MEC by proposing attack detection models. The communication layer can be monitored by security functions in MEC, such as a machine learning model that analyses the traffic and detects the malicious behaviour. In this case, MEC functions as an intrusion detection system that detects the possible attacks. Additionally, MEC may detect the bogus models provided by malicious nodes [Mukherjee2020]. Authors in [Gopalakrishnan2020] proposed a model that utilizes deep learning to predict the traffic and detect the cyber attacks in MEC with an accuracy of detection that reaches 97.65% of the attacks. Cheng et al. [Cheng2022] proposed an AI based model to detect and mitigate the security attacks in MEC. Their proposed model is able to detect the malicious traffic by collecting and analysing the traffic in 5G networks. Additionally, the model detects the bogue base station by exploiting the signal strength in three phases of data collection, train and detection. Authors in [Liu2021] proposed a GRU based neural network model to detect the malicious traffic and possible threats in the HTTP traffic.

Some researchers focused on a single important attack in their proposed model. As a very common attack, DDoS attack detection in MEC was addressed by the researchers. Huang et al. [Huang2024] proposed a combined model of container-based task isolation with lightweight online anomaly detection that detects the DDoS attack in MEC. During the detection of an attack, the proposed model provides a scheduling method that optimises the edge resource allocation and the service quality for benign users in the network. Kabdjou and Shinomiya [Kabdjou2024] proposed an architecture that utilises the cyber deception metrics to detect the HTTP DDoS attacks in MEC. The architecture introduces proactive measures that actively mislead and redirect potential attackers. Also, the deception tactics effectively mitigate advanced threats, diverting assailants away from critical assets and into fabricated environments.

8.3.4. Smart orchestration by Moving Target Defence

In the design of cybersecurity solutions, the defending party consistently encounters the challenge that the offensive party typically enjoys an indefinite amount of time to observe the behavior of the target network. Each security solution aimed at countering previously encountered attacks inevitably introduces patterns that may potentially be leveraged by adversaries for recognition, evasion, or even weaponization.

One emerging strategy addressing this dilemma is Moving Target Defense (MTD). MTD is defined by NIST as: ``The concept of controlling change across multiple system dimensions in order to increase uncertainty and apparent complexity for attackers, reduce their window of opportunity, and increase the costs of their probing and attack efforts" [NIST01]. At its core, MTD operates on the principle of dynamically altering the network's surfaces, rather than solely focusing on thwarting known attack vectors. By continuously shifting these surfaces, MTD disrupts adversaries' efforts to map out the system effectively. Furthermore, a notable advantage of the

MTD approach lies in its capacity to swiftly adapt configurations, such that even if an adversary identifies a vulnerability within a specific setup, the system will have transitioned to a different configuration by the time exploitation is attempted. Deviating a bit from the base concept, MTD can also be used to focus on well-known attacks that lack sophistication, e.g., DDoS attacks [Chai2020].

In [Tan2023] The authors categorize MTD strategies based on temporal and spatial dimensions, offering a comprehensive overview of the intersection between MTD and game-theoretic decision-making processes in the network. In another recent paper [Żal2024], the authors present a new variation of the often-discussed address mutation technique. Their main contribution is their focus on the preservation of Quality of Service (QoS). In their suggested solution the programmable network devices keep track of the network flows and mutate the addresses without need for reinitialization.

Jafarian et. al. [Jafarian2023] present a novel iteration of the address mutation technique, extending to such a degree that it warrants adoption of the authors' terminology, referred to as host mutation. The authors propose a comprehensive solution that not only alters the IP addresses of hosts but also encompasses modifications to MAC addresses, domain name responses to rDNS queries, and fingerprints. Yoon et. Al. [Yoon2021] leverage SDN capabilities to implement IP address shuffling and use multi-agent deep-RL to train and obtain efficient MTD shuffling policies in in-vehicle edge networks.

The Microsoft Defender Research Team is also promoting security research in the direction of MTD and automated defense optimization with their open-source research platform "CyberBattleSim" [Microsoft2021], using deep-RL to optimize defensive strategies based on network simulations of medium-sized traditional and enterprise networks.

As previously mentioned in Section 8.1.1, MTD operations can also involve the migration of the 6G network functions as they operate in portable workloads such as VMs, microVMs, and containers. For instance, Soussi et. Al. [Soussi2023] present MERLINS, a framework migrating stateless VNFs (running in VMs) in a 5G testbed and showcasing both proactive defense, against malware and backdoor infections, as well as reactive defense, mitigating binary tampering attacks. Notably, MERLINS considers the problem of balancing the security benefits of such migrations with the operational costs and impact on availability/QoS. They address this by formulating the problem as a multi-objective optimization task solved using deep-RL.

8.4. Machine Learning Frameworks for CTI Analysis

The analysis of Cyber Threat Intelligence (CTI) and Indicator of Compromise (IoC) clearly shows the use of legitimate services such as CDN, Cloud Services, Instant Messaging, File Sharing Systems for the propagation of malicious files or malicious links related to the C2C architecture

(Command and Control) or malware infection. Among those services, we can find AWS, Dropbox, Google Docs, Discord. This presents a difficulty in countering the problem with traditional blocking methods. In this scenario, different works have attempted to characterise the main problem, the quality of the SIEM dataset, the methodology for analysing and detecting URLs, infrastructure organization of malware, and trends. In this section, we list previous efforts to define methodologies and propose an active solution for all challenges related to this topic using Machine Learning.

Network entities and organizations have implemented countermeasures to prevent attacks by blocking content that has been previously identified as malicious or suspicious by other entities that have suffered such attacks. However, the lack of standardization in how they should report their incidents limits the ability of other entities to leverage these previous experiences. To resolve this limitation, different organizations have standardized the sharing of Cyber Threat Intelligence information using the STIX (Structured Threat Information Expression) format over the past few years. The STIX format represents incidents as entity-relationship graphs connecting significant attack components for a specific threat. Initiatives like Hail to TAXII or OpenCTI make this type of forensic information publicly available in the STIX format. However, only some private initiatives, such as the Cyber Threat Alliance, use this information to improve cybersecurity solutions.

STIX datasets have already been used in various ways. A notable trend among CTI is grouping different sources provided in textual reports or lists of indicators of compromise into a Semantic Entity Database. For example, [Syed2016] proposes a Unified Cybersecurity Ontology (UCO). Then, several works rely on similar concepts (i.e., ontologies) to recover knowledge graphs by feeding external CTI sources (including STIX providers) and applying semantic queries. The STIX knowledge graphs are often used as search engines from which assumptions can be derived that help and improve the work of a human expert. In [Kim2018], an external STIX dataset is used to derive a new database schema and extract well-defined security rules in standardized formats like YARA and Snort. Finally, [Ekelhart2021] builds graphs using UCO to extract entities from application logs. Therefore, STIX-based graphs are prominently used as databases for user-defined queries. However, these works depend on the construction of ontologies based on a structured database and integrating it with an external knowledge source. This implies an additional phase of ontology building and entity recovery, often obtained through the analysis of plain text sources.

8.4.1.1. Threat Intelligence Sharing

[Bouwman2020] examines the value of commercial threat intelligence, finding little overlap between providers and open feeds. Paid services exhibit delayed and limited coverage, which raises concerns about their timeliness. Interviews reveal that clients prioritize workflow optimization over threat detection, informally evaluating threat intelligence rather than through quantitative metrics.

[Bouwman2022] focuses on the COVID-19 Cyber Threat Coalition (CTC), a voluntary security information sharing community with over 4,000 members. The study examines two questions: whether large-scale collaboration improves coverage and whether freely available threat data enhances defender capabilities. The findings reveal that while the CTC largely adds existing industry sources, its blocklist deviated from COVID-19-related domains to generic abuse due to strict quality control measures. However, within the COVID-19 data, the CTC demonstrated added value by including a significant proportion of unknown domains for existing abuse detection systems. The article derives three lessons for future threat intelligence sharing initiatives based on this unique experiment.

[Almashor2022] focuses on analyzing a set of URL data derived from SIEM threat intelligence platforms, proposing to group them into attack campaigns that can be characterized and share similarities. One of the findings is that there are many malicious URLs that remain active and functional even after being marked as malicious.

Cloud Security

[Rakotondravony2017] focuses on classifying attacks in Infrastructure as a Service (IaaS) cloud environments, particularly those involving Virtual Machines (VMs), using mechanisms based on Virtual Machine Introspection (VMI). The classification methodology considers the source, target, and direction of attacks, allowing cloud actors to deploy VMI-based monitoring architectures.

DNS Security

[Alowaisheq2020] discovers the security risk posed by obsolete Name Server (NS) records in active domains, particularly those residing within the domain zone. The authors demonstrate the practical exploitation of this type of obsolete NS record, leading to a silent domain takeover. Through an exhaustive analysis of high-profile domains, DNS hosting providers, and public resolver operators, they identify numerous susceptible domains and vulnerable parts, including government entities, payment services, Amazon Route 53, and CloudFlare. The document also delves into mitigation techniques for affected parties, providing a comprehensive understanding of this new security risk.

Network Analysis

Regarding network analysis, [Luckie2020] presents a system that learns regular expressions to extract Autonomous System Numbers (ASNs) from hostnames of router interfaces, incorporating topological restrictions and PeeringDB data. By modifying an existing method, it improves the accuracy of ASN extraction, increasing agreement with inferred ASNs from 87.4% to 97.1% and reducing error rates. This work expands the possibilities for router ownership inference based on evidence.

Malware Analysis

In the field of malware analysis, [Yao2023] investigates the abuse of web applications by malware as a substitute for attacker-controlled servers. It was found that delays in collaboration between incident responders and web application providers facilitated the proliferation of this malware. The authors developed Marsea, an automated malware analysis pipeline, which identified 893 instances of malware involved with web applications across 97 families, highlighting a 226% increase since 2020.

[Ife2019] presents a longitudinal measurement of the malware delivery ecosystem on the web. Through an analysis based on data, the authors examine network infrastructures and files downloaded at different periods of time (one day, one month, one year). They identify two distinct ecosystems: a larger network responsible for delivering Potentially Unwanted Programs (PUP) and separate networks that deliver malware. Although they are mostly disjointed, there is a crossover between the two ecosystems. The study reveals skewed proportions (17:2) of PUP to malware in the wild, observes periodic activity in the malicious network, and highlights the potential for improving dismantling techniques for researchers and law enforcement.

[Ife2021] is an advancement over their previous work in [Ife2019]. Using the same type of dataset, it examines the response of malware delivery operations to attempts at dismantling. The findings indicate the prevalence of distributed delivery architectures, the importance of identifying key "superbinaries," and the predictable and unpredictable behaviors exhibited by malware operations after dismantling. The study suggests the need to improve security hygiene, coordination between service providers, and the development of threat monitoring techniques to effectively interrupt malware operations.

[Labreche2022] focuses on the attacked side of the malware delivery ecosystem through the configuration of isolated virtual machines that act as infected victims of various droppers. The work centers on the analysis over time of the behavior of droppers and the malicious load downloaded, trying to find correlations between victim characteristics and the choice of malicious software left by each downloader.

[Popescu2015] explores proactive identification of malicious URLs, crucial in light of the strong dependence of malware on the internet for its propagation. The authors discuss practical considerations, emphasizing automatic learning and unsupervised learning techniques for efficient detection in memory. They evaluate a dataset of 6 million URLs collected over 48 weeks, tracing the evolution of detection rates and false positives. Based on this analysis, they obtain insights into the current landscape of malware and attack vectors on the internet.

[Roy2021] proposes a detailed analysis of malicious URLs hosted on Twitter, highlighting the problem of blocking such resources when they point to legal file-sharing platforms, Google Forms, and Microsoft's corresponding form service, as well as WordPress web hosting domains, Google Cloud Storage API, etc. The study highlights Twitter's poor countermeasures in terms of timeliness and coverage.

[Zhu2020] evaluates the use of Virus Total file labeling and the difficulty in correlating and aggregating files that belong to the same malware family but are labeled differently, incompletely, or incorrectly by AV services and files. It examines the dynamics of labeling motors on VirusTotal. By reviewing 115 academic articles, the authors categorize and validate common labeling methods used by researchers. They collect daily snapshots of VirusTotal labels for over 14,000 files from 65 engines and demonstrate the benefits of aggregating labels based on thresholds to stabilize file labels. The study reveals that certain "trusted" motors may have inferior performance, motor groups are correlated, and some motors produce false positives. The article concludes with suggestions for improving data annotation practices using VirusTotal.

[Shen2021] provides some interesting ideas for representing metrics regarding the popularity of the domain, geographical distribution, categorization, etc. By focusing on Potentially Harmful Applications (PHA) in Android, it provides a useful list of related works on the analysis of malware distribution and characterization of domains that could be useful for our work.

8.5. Service accurate monitoring and traceability

Monitoring is a key aspect for managing complex cloud-native infrastructures and enhancing operational efficiency. For 5G networks, end-to-end real-time monitoring is a paramount factor. This involves gathering infrastructure metrics (such as compute, storage, and network) as well as domain-specific metrics for components like gNBs or MEC services. As we transition towards 6G, the need for sophisticated monitoring and traceability solutions will only intensify, driven by the increased complexity and performance requirements of 6G networks.

In 6G networks, monitoring will continue to support the **lifecycle management of services** and facilitate **intelligent reconfiguration and alerting** for stakeholders, including infrastructure owners, operators, slice owners, and service/application developers [Taleb2022]. It will enable real-time tracking of service performance and resource utilization, allowing for proactive management and optimization of network resources. Effective monitoring will also support dynamic service orchestration and automated healing processes, ensuring high availability and reliability of services. With the help of AI and machine learning, 6G networks will benefit from intelligent monitoring systems that can detect anomalies, predict potential issues, and automatically trigger reconfigurations to maintain optimal performance. These systems will provide real-time alerts to stakeholders, enabling them to take immediate corrective actions and minimize service disruptions. **Multi-tenant networks**, which support network slices, will require the monitoring of key performance indicators (KPIs) across different technological domains managed by various entities. For example, a network operator focuses on the KPIs of components running the network slice (e.g., RAN, cloud/edge, routers), while a slice owner may consider high-level KPIs (e.g., end-to-end delay) for SLA validation.

One advanced version of monitoring in 6G will be telemetry. Telemetry provides detailed statistics about a given traffic flow based on metadata extracted from a set or all the packets belonging to that flow. Instead of relying on cloud-based virtualized solutions, **leveraging programmable data planes** (e.g., using P4) will be crucial. Data plane programmability can be exploited for monitoring and telemetry in the core network segment. For instance, the work by Paolucci et al. [Paolucci2021] proposed a UPF offloaded implementation inside a programmable switch, including the telemetry of desired flows to a data analytics collector. This functionality, offloaded in a programmable switch, enables the operator to perform a detailed analysis of traffic statistics, including UPF latency performance, thus indicating possible performance degradation due to excessive load, congestion, or attack events. Additionally, network attacks using different protocols as drivers can be profiled using the programmable data plane. Musumeci et al. [Musumeci2020] used programmable postcard telemetry of specific metadata features (e.g., the rate of TCP SYN packets) to feed AI engines in near real time, showing a drastic improvement in AI-based attack detection in terms of processing latency compared to standard SDN controller detection, reducing the detection time from several seconds to a few hundred microseconds.

Beyond network programmability solutions for monitoring and telemetry, **application-level tools** will play a vital role in 6G. Open-source tools like Prometheus and Grafana will continue to be pivotal for advanced monitoring solutions. Barrachina et al. [Barrachina2022] proposed a framework that employs over-the-air transmissions and focuses on deploying Open5GS and Prometheus-based monitoring as containerized network functions (CNFs) within a Kubernetes cluster. This setup, spanning a multi-tier network with a multi-access edge computing (MEC) host, demonstrated the effectiveness of an end-to-end monitoring system through Grafana dashboards. These dashboards provided insights into both infrastructure resources and radio metrics for scenarios such as user plane function (UPF) re-selection and user mobility.

Network tomography (NT) is an emerging monitoring approach that will be increasingly relevant in 6G. NT estimates network performance based on measurements from a limited subset of network elements, presenting several benefits over traditional monitoring techniques but is susceptible to identifiability issues. Kakkavas et al. [Kakkavas2021] demonstrated how NT could address current monitoring challenges by complementing and working together with Software-Defined Networking (SDN). NT leverages SDN capabilities such as the centralized view of the entire network, direct flow-level measurements, and controllable routing to yield accurate estimations with low overhead. This work explored the range of applications for NT-based solutions in 5G networks and beyond, including virtual and vehicular networks.

Monitoring the performance of network slices in 6G will pose challenges due to the significant network overhead associated with direct measurements. To address this issue, the work in network tomography suggests estimating slices' delays in the network by finding the minimal combination of end-to-end simple monitoring paths necessary to minimize estimation error. A new genetic algorithm is introduced to identify the optimal monitoring paths required for network tomography while minimizing their number. The evaluation results indicate the effectiveness of both fixed mutation and adaptive mutation approaches, with the adaptive mutation approach outperforming the fixed method by exploring new solutions and avoiding local minima, leading to faster convergence and better results in estimating network slice delays.

In summary, as we move towards 6G, the integration of advanced monitoring and traceability techniques will be crucial for ensuring operational efficiency, security, and performance. By leveraging programmable data planes, advanced telemetry, application-level tools, and emerging techniques like network tomography, 6G networks will be better equipped to handle the complex demands of future communication systems.

9. Roadmap summary

The NATWORK project roadmap identifies key areas that are critical to achieving success in building a robust, scalable, and future-proof 6G network infrastructures, targeting to meet the evolving demands of next-generation networks. The key areas that are critical to the success of NATWORK project are the following:

- Scalability and Performance;
- Security and Privacy;
- Energy Efficiency and Sustainability.

In the sub-section below, a description of these key areas as well as key actions towards the success of NATWORK project on these areas are illustrated.

9.1. Priority challenges

The following key areas have been identified as critical to the success of NATWORK roadmap:

9.1.1. Scalability and Performance

The exponential growth in data traffic, driven by applications such as video streaming, IoT devices, and virtual reality, necessitates networks that can scale effectively without compromising performance. Achieving high bandwidth and low latency, while accommodating a large number of interconnected devices, remains a paramount challenge. This requires advancements in both hardware and software to ensure that networks can handle the increased load and provide consistent performance.

Key Actions:

- **Foster software payload migrability** with no-latency bootstrap for execution at the best location and closer to the users.

- **Develop Dynamic Architectures**: Create network architectures that can automatically scale in response to demand fluctuations, ensuring that performance remains robust during peak usage times.

- **Enhance Traffic Management:** Strengthen network resource allocation and traffic management strategies utilizing AI-enabled techniques for load balancing and elasticity among microservices. The target is to ensure efficient management of growing data flows, enabling rapid and reliable data transmission across the network infrastructure.

- **Design of 6G Network Functions:** Design and develop adaptive and resilient 6G network functions capable of maintaining high performance under diverse and changing network conditions.

9.1.2. Security and Privacy

As networks expand and integrate more devices, the threat landscape also grows, making security and privacy a top priority. A significant challenge is to ensure that data remains secure and user privacy is maintained in a pervasive network environment. This includes safeguarding against cyber-attacks, data breaches, and unauthorized access while balancing the need for transparency and data sharing.

Key Actions:

- **Implement Advanced Security Measures:** Use robust encryption and authentication to safeguard data and ensure only authorized access.
- **Deploy AI-Based Security Solutions:** Utilize artificial intelligence for real-time detection and mitigation of security threats, enhancing the network's ability to respond to cyber-attacks.
- **Establish Data Governance Policies:** Develop comprehensive frameworks and policies for data governance and privacy compliance to protect user information and maintain regulatory standards.
- **Develop platform-agnostic security** for higher payload migrability.
- **Develop continuous security** during execution notably by accurate service and payload monitoring.
- **Develop Physical Layer Security modules** based on novel RIS and AI-based MIMO technologies

9.1.3. Energy Efficiency and Sustainability

The increasing number of network devices and the growing volume of data traffic contribute significantly to energy consumption and environmental impact. Developing energy-efficient technologies and promoting sustainable practices within the networking infrastructure are critical challenges. This includes optimizing power usage across all network components and integrating renewable energy sources where feasible.

Key Actions:

- **Innovate in Energy-Efficient Technologies:** Develop network equipment and technologies that consume less power while maintaining high performance, reducing the overall energy footprint.
- **Integrate Renewable Energy Sources:** Promote the adoption of renewable energy in network operations to lower carbon emissions and support environmental sustainability.
- **Implement Sustainable Practices:** Establish best practices for energy management in data centers and network maintenance to ensure sustainable and eco-friendly operations.
- **Develop on-demand security** to reduce the carbon impact of security.

10. Conclusions

To develop a sustainable 6G ecosystem, there is a need to develop sustainable cybersecurity solutions that can provide efficient protection and resiliency against 6G threats and attacks, given the bespoke characteristics of 6G. To be able to develop such solutions, it is first required to analyse the landscape of cybersecurity challenges in 6G, reviewing potential threats and attacks and their impact on relevant KPIs and summarizing state-of-the-art cybersecurity solutions and how they can be leveraged in tackling such threats. This document has reviewed state-of-the-art literate in 5G and 6G cybersecurity. It provided a comprehensive review of the challenges on road towards 6G, from the radio access to the core programable transport network and from edge to core clouds. The document summarised the application of AI in network security as well as the security of AI, the dependency on datasets and the challenges in data sharing such as privacy. Orthogonally, the document reviewed state-of-the-art cybersecurity solutions and enabling technologies, including security-by-design principles, intrusion detection and protection systems, payload hardening technologies and emerging AAA systems. The comprehensive review is then utilised to summarise the priority challenges to be tackled in the lifetime of the NATWORK project. Insights developed in this report will be leveraged in guiding the research and innovation in work packages: WP3 that focuses on composition of secure complex 6G services; WP4 developing AI as a Security Service; and, WP5 addressing self-resilience of 6G wireless devices. Insights will further guide the use-cases development and evaluation in work package WP6.

References

[1_ETSI2024] ETSI Software Development Group for TeraFlowSDN, Available: https://tfs.etsi.org/

[1_ONF2023] ONF, “Open Network Operating System (ONOS)”, 2023, Available: https://opennetworking.org/onos/

[1_TheLinuxFoundation2023] The Linux Foundation, “OpenDaylight (ODL)”, 2023, Available: https://www.opendaylight.org/

[2_ETSI2024] ETSI, “Open Source NFV Management and Orchestration (MANO) software stack”, https://osm.etsi.org/

[2_ONF2023] Open Networking Foundation (ONF), 2023, Available: https://opennetworking.org/

[2_TheLinuxFoundation2023] The Linux Foundation, “Open Network Automation Platform (ONAP)”, 2023, Available: https://www.onap.org/

[3_TheLinuxFoundation2023] The Linux Foundation, 2023, Available: https://www.linuxfoundation.org/

[A. Alshamrani2019] Alshamrani, A., S. Myneni, A. Chowdhary, and D. Huang. "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities." IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1851-1877, Second quarter 2019, doi: 10.1109/COMST.2019.2891891.

[Abdelrazek2024] Abdelrazek, L., Fuladi, R., Kövér, J., Karaçay, L., & Gülen, U. (2024). Detecting IP DDoS Attacks Using 3GPP Radio Protocols. IEEE Access, 12, 24776-24790.

[Abdulqadder2020] Abdulqadder, I.H., Shijie Z., Deqing Z., Israa T., and Syed M.. "Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms." Computer Networks 179 (2020): 107364.

[Abeni2023] Abeni, L. (2023). Real-time unikernels: A first look. In Lecture Notes in Computer Science, pages 121–133. Springer Nature Switzerland.

[Ahmad2018] Ahmad, Ijaz, et al. "Overview of 5G security challenges and solutions." IEEE Communications Standards Magazine 2.1 (2018): 36-43.

[Ahmad2019] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov and M. Ylianttila, "Security for 5G and Beyond," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3682-3722, Fourthquarter 2019, doi: 10.1109/COMST.2019.2916180.

[Akhlaghpasand2017] H. Akhlaghpasand, S. M. Razavizadeh, E. Bjornson, and T. T. Do, ¨ "Jamming detection in massive MIMO systems," IEEE Wireless Communications Letters, vol. 7, no. 2, pp. 242–245, 2017.

[Alabdulmohsin2016] Ibrahim Alabdulmohsin, YuFei Han, Yun Shen, and Xiangliang Zhang. 2016. Content-agnostic malware detection in heterogeneous malicious distribution graph. In Proceedings of the 25th ACM International on Conference on Information and Knowledge Management. 2395–2400.

[Alahmadi 2023] Alahmadi AA, Aljabri M, Alhaidari F, Alharthi DJ, Rayani GE, Marghalani LA, Alotaibi OB, Bajandouh SA. DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions. Electronics. 2023; 12(14):3103. https://doi.org/10.3390/electronics12143103

[Alanazi 2022] Alanazi, F.; Jambi, K.; Eassa, F.; Khemakhem, M.; Basuhail, A.; Alsubhi, K. Ensemble Deep Learning Models for Mitigating DDoS Attack in Software-Defined Network. Intell. Autom. Soft Comput. 2022, 33, 2.

[Alanazi2022] Alanazi, F.; Jambi, K.; Eassa, F.; Khemakhem, M.; Basuhail, A.; Alsubhi, K. Ensemble Deep Learning Models for Mitigating DDoS Attack in Software-Defined Network. Intell. Autom. Soft Comput. 2022, 33, 2.

[Al-Hraishawi2021] H. Al-Hraishawi, S. Chatzinotas and B. Ottersten, "Exploiting Jamming Attacks for Energy Harvesting in Massive MIMO Systems," in ICC 2021 IEEE International Conference on Communications, Montreal, QC, Canada, 2021, pp. 1-6, doi: 10.1109/ICC42927.2021.9500422.

[Al-Hraishawi2023] H. Al-Hraishawi, O. Abdullah, S. Chatzinotas and B. Ottersten, "Energy Harvesting From Jamming Attacks in Multi-User Massive MIMO Networks," in IEEE Transactions on Green Communications and Networking, vol. 7, no. 3, pp. 1181-1191, Sept. 2023, doi: 10.1109/TGCN.2023.3280036.

[Ali 2023] Ali, T.E.; Chong, Y.-W.; Manickam, S. Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review. Appl. Sci. 2023, 13, 3183. https://doi.org/10.3390/app13053183

[Ali2023] Ali, T.E.; Chong, Y.-W.; Manickam, S. Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review. Appl. Sci. 2023, 13, 3183. https://doi.org/10.3390/app13053183

[aligungr] aligungr/UERANSIM", https://github.com/aligungr/UERANSIM/

[Almashor2022] Mahathir Almashor, Ejaz Ahmed, Benjamin Pick, Sharif Abuadbba, Jason Xue, Raj Gaire, Shuo Wang, Seyit Camtepe, and Surya Nepal. 2022. Unraveling Threat Intelligence Through the Lens of Malicious URL Campaigns. arXiv preprint arXiv:2208.12449 (2022).

[Alowaisheq2020] Eihal Alowaisheq, Siyuan Tang, Zhihao Wang,Fatemah Alharbi, Xiaojing Liao, and XiaoFeng Wang. 2020. Zombie Awakening: Stealthy Hijacking of Active Domains through DNS Hosting Referral. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (Virtual Event, USA) (CCS '20). Association for Computing Machinery, New York, NY, USA, 1307–1322. https://doi.org/10.1145/3372297.3417864

[Alsop2019] Thomas Alsop, Global enterprise server hourly downtime cost 2019, Statista, May 18, 2022, Online: https://www.statista.com/statistics/753938/worldwide-enterprise-server-hourly-downtime-cost/ (Accessed: May 2024)

[Alwis2021] C. D. Alwis, A. Kalla, Q.V. Pham, P. Kumar, K. Dev, W.J. Hwang, M. Liyanage, "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research," in IEEE Open Journal of the Communications Society, Volume 2, pp. 836-886, 2021, doi: 10.1109/OJCOMS.2021.3071496.

[Alzhrani2023] Alzhrani, R. M., & Alliheedi, M. A. (2023). 5G Networks and IoT Devices: Mitigating DDoS Attacks with Deep Learning Techniques. arXiv preprint arXiv:2311.06938.

[Amponis2022] Amponis, G., Radoglou-Grammatikis, P., Lagkas, T. et al., Threatening the 5G core via PFCP DoS attacks: the case of blocking UAV communications. J Wireless Com Network 2022, 124 (2022). https://doi.org/10.1186/s13638-022-02204-5.

[Amponis2023] George Amponis, Panagiotis Radoglou-Grammatikis, Thomas Lagkas, Savas Ouzounidis, Maria Zevgara, Ioannis Moscholios, Sotirios Goudos, Panagiotis Sarigiannidis, "Generating full-stack 5G security datasets: IP-layer and core network persistent PDU session attacks", AEU - International Journal of Electronics and Communications, Volume 171, 2023, 154913, ISSN 1434-8411, https://doi.org/10.1016/j.aeue.2023.154913.

[Anjali2020] Anjali, Caraza-Harter, T., and Swift, M. M. (2020). Blending containers and virtual machines. In Proceedings of the 16th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments. ACM.

[Arjoune2020] Y. Arjoune and S. Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2020, pp. 1010-1015, doi: 10.1109/CCWC47524.2020.9031175.

[Arjoune2020] Y. Arjoune, F. Salahdine, M. S. Islam, E. Ghribi, and N. Kaabouch, "A novel jamming attacks detection approach based on machine learning for wireless communication," in

Proceedings of IEEE International Conference on Information Networking (ICOIN), pp. 459–464, 2020.

[Bacon2019] Bacon M., DDoS attacks among top 5G security concerns, TechTarget, 13 May 2019, Online: https://www.techtarget.com/searchsecurity/feature/DDoS-attacks-among-top-5G-security-concerns. Accessed May 2024.

[Bae2024] J. Bae, W. Khalid, A. Lee, H. Lee, S. Noh, H. Yu, "Overview of RIS-enabled secure transmission in 6G wireless networks," in Digital Communications and Networks, 2024, https://doi.org/10.1016/j.dcan.2024.02.005

[Bafo23] Georgia Bafoutsou, Maria Papaphilippou, Evangelos Kantas, Marnix Dekker, Embedded Sim Ecosystem, Security Risks and Measures, ENISA, 2023. Source: https://www.enisa.europa.eu/publications/embedded-sim-ecosystem-security-risks-and-measures. Last-accessed: Mai 23, 2024.

[Baldock] H. Baldock, “How 5G standalone can help our shift to Net Zero,” Totaltele.com. [Online]. Available: https://totaltele.com/how-5g-standalone-can-help-our-shift-to-net-zero/. Accessed: 22-May-2024.

[Banks2021] BANKS, Alexander Sprogø; KISIEL, Marek; KORSHOLM, Philip. Remote attestation: A literature review. arXiv preprint arXiv:2105.02466, 2021.

[Barrachina2022] S. Barrachina-Muñoz, M. Payaró and J. Mangues-Bafalluy, "Cloud-native 5G experimental platform with over-the-air transmissions and end-to-end monitoring," 2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Porto, Portugal, 2022

[Bazydło2024] Bazydło, Grzegorz, Kamil Kozdrój, Remigiusz Wiśniewski, and Aniruddha Bhattacharjya. 2024. "Trusted Third Party Application in Durable Medium e-Service" Applied Sciences 14, no. 1: 191. https://doi.org/10.3390/app14010191

[Belmega2017]: E. V. Belmega and A. Chorti, "Protecting secret key generation systems against jamming: Energy harvesting and channel hopping approaches", in IEEE Trans. Inf. Forensics Security, vol. 12, no. 11, pp. 2611-2626, 2017.

[Bhat2021] J. R. Bhat and S. A. Alqahtani, "6G Ecosystem: Current Status and Future Perspective," in IEEE Access, vol. 9, pp. 43134-43167, 2021, doi: 10.1109/ACCESS.2021.3054833.

[Bobrovnikova2020] Bobrovnikova, K., Lysenko, S., Gaj, P., Martynyuk, V., & Denysiuk, D. (2020). Technique for IoT cyberattacks detection based on DNS traffic analysis. W T. Hovorushchenko, O. Savenko, P. Popov, & S. Lysenko (Red.), Proceedings of the 1st International Workshop on

Intelligent Information Technologies and Systems of Information Security (IntelITSIS) : Khmelnytskyi, Ukraine, 10-12 June 2020 [online] (T. 2623, s. 208–218). CEUR-WS.

[Bousalem 2022] Badre Bousalem, Vinicius F Silva, Rami Langar, Sylvain Cherrier. Deep Learning-based Approach for DDoS Attacks Detection and Mitigation in 5G and Beyond Mobile Networks. 8th International Conference on Network Softwarization (NetSoft 2022), Jun 2022, Milan, Italy. pp.228-230, ff10.1109/NetSoft54395.2022.9844053ff.

[Bousalem2022] Badre Bousalem, Vinicius F Silva, Rami Langar, Sylvain Cherrier. Deep Learning-based Approach for DDoS Attacks Detection and Mitigation in 5G and Beyond Mobile Networks. 8th International Conference on Network Softwarization (NetSoft 2022), Jun 2022, Milan, Italy. pp.228-230, ff10.1109/NetSoft54395.2022.9844053ff.

[Bouwman2020] Xander Bouwman, Harm Griffioen, Jelle Egbers, Christian Doerr, Bram Klievink, and Michel van Eeten. 2020. A different cup of TI? The added value of commercial threat intelligence. In 29th USENIX Security Symposium (USENIX Security 20). USENIX Association, 433–450. https://www.usenix.org/conference/ usenixsecurity20/presentation/bouwman

[Bouwman2022] Xander Bouwman, Victor Le Pochat, Pawel Foremski, Tom Van Goethem, Carlos H. Ganan, Giovane C. M. Moura, Samaneh Tajalizadehkhoob, Wouter Joosen, and Michel van Eeten. 2022. Helping hands: Measuring the impact of a large threat intelligence sharing community. In 31st USENIX Security Symposium (USENIX Security 22). USENIX Association, Boston, MA, 1149–1165. https://www.usenix.org/conference/usenixsecurity22/presentation/bouwman

[BPI2019] BPI Network, Opportunities And Challenges In A 5g Connected Economy, May2019

[Bravi2023] ≤E. Bravi, D. G. Berbecaru, and A. Lioy, “A Flexible Trust Manager for Remote Attestation in Heterogeneous Critical Infrastructures,” in 2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Dec. 2023, pp. 91–98. doi: 10.1109/CloudCom59040.2023.00027.

[Brik2023] Brik, B., Chergui, H., Zanzi, L., Devoti, F., Ksentini, A., Siddiqui, M. S., ... & Verikoukis, C. (2023). A survey on explainable AI for 6G O-RAN: Architecture, use cases, challenges and research directions. arXiv preprint arXiv:2307.00319.

[BSI2022] BSI, "Open RAN Risk Analysis (5GRANR)," 2022.

[Buck2021] BUCK, Christoph, et al. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Computers & Security, 2021, 110: 102436.

[BytecodeAlliance2019] B. Alliance, “Webssembly Micro Runtime” https://bytecodealliance.github.io/wamr.dev/

[Cao2022] Y. Cao and W. Cheng, "Multiple Reconfigurable Intelligent Surfaces Assisted Anti-jamming for Aerial-ground Communication," ICC 2022 - IEEE International Conference on Communications, Seoul, Korea, Republic of, 2022, pp. 698-703, doi: 10.1109/ICC45855.2022.9838834.

[Catillo2023] M. Catillo, U. Villano, and M. Rak, "A survey on auto-scaling: how to exploit cloud elasticity," International Journal of Grid and Utility Computing, Volume 14, No. 1, pp 37-50, March 2023, https://doi.org/10.1504/IJGUC.2023.129702.

[Chai2020] X. Chai, Y. Wang, C. Yan, Y. Zhao, W. Chen, and X. Wang, "DQ-MOTAG: Deep reinforcement learning-based moving target defense against DDoS attacks," in 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC). IEEE, Aug 2020.

[Chen2020]: P. Chen, J. Ouyang, W. -P. Zhu, M. Lin, A. E. Shafie and N. Al-Dhahir, "Artificial-Noise-Aided Energy-Efficient Secure Beamforming for Multi-Eavesdroppers in Cognitive Radio Networks," in IEEE Systems Journal, vol. 14, no. 3, pp. 3801-3812, Sept. 2020, doi: 10.1109/JSYST.2020.2967470.

[Chen2024] X. Chen, W. Feng, Y. Chen, N. Ge and Y. He, "Access-Side DDoS Defense for Space-Air-Ground Integrated 6G V2X Networks," in IEEE Open Journal of the Communications Society, vol. 5, pp. 2847-2868, 2024.

[Chen2024] X. Chen, W. Feng, Y. Chen, N. Ge, and Y. He, "Access-side DDoS defense for space-air-ground integrated 6G V2X networks," IEEE Open J. Commun. Soc., vol. 5, pp. 2847–2868, 2024.

[Cheng2022] Cheng, S. M., Hong, B. K., & Hung, C. F. (2022). Attack detection and mitigation in MEC-enabled 5G networks for AIoT. IEEE Internet of Things Magazine, 5(3), 76-81.

[Chica2020] Chica, Juan Camilo Correa, Jenny Cuatindioy Imbachi, and Juan Felipe Botero Vega. "Security in SDN: A comprehensive survey." Journal of Network and Computer Applications 159 (2020): 102595.

[Chua2021] H.N. Chua, J.S. Ooi, & A. Herbland. (2021). The effects of different personal data categories on information privacy concern and disclosure. Computers & Security, 110, 102453.

[Cilic2023] Cilic´, I., Krivic´, P., Zˇ arko, I. P., and Kusek, M. (2023). Performance evaluation of container orchestration tools in edge computing environments. Sensors, 23(8):4008.

[CISA2022] CISA, "Open Radio Access Network Security Considerations," 2022.

[Clark2019] L. Clark, "Standardizing WASI: A system interface to run WebAssembly outside the web," Mozilla Hacks – the Web developer blog, Mar 2019, accessed: May 27, 2024. [Online].

Available: https://hacks.mozilla.org/2019/03/standardizing-wasi-a-webassembly-system-interface/

[Clark2022] L. Clark, “Wasmtime reaches 1.0: Fast, safe and production ready!” https://bytecodealliance.org/articles/wasmtime-1-0-fast-safe-and-production-ready, 2022.

[Clemens2018] CLEMENS, John; PAL, Raj; SHERRELL, Branden. Runtime state verification on resource-constrained platforms. In: MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM). IEEE, 2018. p. 1-6.

[Cunha2019] Cunha, Vitor A., et al. "Network slicing security: Challenges and directions." Internet Technology Letters 2.5 (2019): e125.

[Dennis2021] J.B. Dennis, M.S. Priya, “A Profile-Based Novel Framework for Detecting EDoS Attacks in the Cloud Environment,” Wireless Personal Communications, Volume 117, pp 3487–3503 (2021). https://doi.org/10.1007/s11277-021-08280-y

[DESIRE-6G D3.1]. DESIRE-6G SNS project deliverable available at https://zenodo.org/records/10356033

[DESIRE-6G D4.1]. DESIRE-6G SNS project deliverable available at https://zenodo.org/records/https://zenodo.org/records/10356108

[Dhammad2018] Dhammad M, Afdel K, Belouch M. Semi-supervised machine learning approach for DDoS detection. Appl Intell. 2018;48(10):3193-3208

[Dinh2020] P. T. Dinh and M. Park, "Dynamic Economic-Denial-of-Sustainability (EDoS) Detection in SDN-based Cloud," 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), Paris, France, 2020, pp. 62-69, doi: 10.1109/FMEC49853.2020.9144972.

[Dinh2021] P. T. Dinh and M. Park, "Economic Denial of Sustainability (EDoS) Detection using GANs in SDN-based Cloud," 2020 IEEE Eighth International Conference on Communications and Electronics (ICCE), Phu Quoc Island, Vietnam, 2021, pp. 135-140, doi: 10.1109/ICCE48956.2021.9352082.

[Djenna2021] A. Djenna, S. Harous, & D.E. Saidouni (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10), 4580.

[Djuitcheu 2023] Djuitcheu, H., Shah, T., Matthias, T., & Schotten, H. D. (2023). DDoS impact assessment on 5G system performance. Authorea Preprints.

[Djuitcheu2023] Djuitcheu, H., Shah, T., Matthias, T., & Schotten, H. D. (2023). DDoS impact assessment on 5G system performance. Authorea Preprints.

[Do2017] T. T. Do, E. Bjornson, E. G. Larsson, and S. M. Razavizadeh, ¨ “Jamming-resistant receivers for the massive MIMO uplink,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, pp. 210–223, 2017.

[Doshi2018] R. Doshi, N. Apthorpe, N. Feamster, Machine learning DDoS detection for consumer internet of things devices, in: 2018 IEEE Security and Privacy Workshops (SPW), IEEE, 2018, pp. 29–35.

[EC2021] European Commission, "The EU Toolbox for 5G security," 2021.

[Ekelhart2021] Kurniawan, K., Ekelhart, A., & Kiesling, E. 2021. An ATT&CK-KG for Linking Cybersecurity Attacks to Adversary Tactics and Techniques. http://ceur-ws.org/Vol-2980/paper363.pdf

[ENI2024] ENISA: Threat Landscape for 5G Networks Report. Dec 2020. Available-online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks. Last-accessed: Jun 2, 2024.

[Ericsson] Ericsson.com. [Online]. Available: https://www.ericsson.com/en/about-us/sustainability-and-corporate-responsibility/environment/climate-action. Accessed: 22-May-2024.

[Ericsson2020] Ercisson. Breaking the energy curve. An innovative approach to reducing mobile network energy use. White paper. https://www.ericsson.com/495d5c/assets/local/about-ericsson/sustainability-and-corporate-responsibility/documents/2020/breaking-the-energy-curve-report.pdf

[Eshete2014] Birhanu Eshete and V. N. Venkatakrishnan. 2014. WebWinnow: Leveraging Exploit Kit Workflows to Detect Malicious Urls. In Proceedings of the 4th ACM Conference on Data and Application Security and Privacy (San Antonio, Texas, USA) (CODASPY ’14). Association for Computing Machinery, New York, NY, USA, 305–312. https://doi.org/10.1145/2557547.2557575

[ETSI2014] ETSI, (2014). Multi-access edge computing (MEC). Available online: https://www.etsi.org/technologies/multi-access-edge-computing, last access: 30 May 2024

[ETSI2023] European Telecommunications Standards Institute (ETSI), 2023, Available: https://www.etsi.org/

[Evans2015] C. Evans, C. Palmer and R. Sleevi, Public key pinning extension for HTTP, Fremont, CA, USA, pp. 1-28, Apr. 2015, [online] Available: https://www.rfc-editor.org/rfc/rfc7469.txt.

[Farooq2023] Farooq, Muhammad Shoaib, Shamyla Riaz, and Atif Alvi. "Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review." Electronics 12.14 (2023): 3077.

[Ficco2019] M. Ficco, “Could emerging fraudulent energy consumption attacks make the cloud infrastructure costs unsustainable?,” Information Sciences, Volume 476, 2019, Pages 474-490, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2018.05.029.

[Free5GC] “free5GC.” https://www.free5gc.org/

[Garms2019] Garms, L., Quaglia, E.A. (2019). A New Approach to Modelling Centralised Reputation Systems. In: Buchmann, J., Nitaj, A., Rachidi, T. (eds) Progress in Cryptology – AFRICACRYPT 2019. AFRICACRYPT 2019. Lecture Notes in Computer Science(), vol 11627. Springer, Cham. pp. 429–447 https://doi.org/10.1007/978-3-030-23696-0_22

[Gentry2003] Gentry, C. (2003). Certificate-Based Encryption and the Certificate Revocation Problem. In: Biham, E. (eds) Advances in Cryptology — EUROCRYPT 2003. EUROCRYPT 2003. Lecture Notes in Computer Science, vol 2656. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-39200-9_17

[Global Research and Analysis Team2024] Global Research and Analysis Team (GReAT). "APT Trends Report Q1 2024." Securelist, https://securelist.com/apt-trends-report-q1-2024/112473/.

[Goethals2020] Goethals, T., Turck, F. D., and Volckaert, B. (2020). Extending kubernetes clusters to low-resource edge devices using virtual kubelets. IEEE Transactions on Cloud Computing.

[Goethals2022] Goethals, T., Sebrechts, M., Al-Naday, M., Volckaert, B., and Turck, F. D. (2022). A functional and performance benchmark of lightweight virtualization platforms for edge computing. In 2022 IEEE International Conference on Edge Computing and Communications (EDGE). IEEE.

[Goethals2024] Goethals, T.; De Clercq, M.; Sebrechts, M.; De Turck, F. and Volckaert, B. (2024). Feather: Lightweight Container Alternatives for Deploying Workloads in the Edge. In Proceedings of the 14th International Conference on Cloud Computing and Services Science – CLOSER

[Gonzalez-Gomez2024] GONZALEZ-GOMEZ, Jeferson, et al. LightFAt: Mitigating Control-flow Explosion via Lightweight PMU-based Control-flow Attestation. arXiv preprint arXiv:2404.02608, 2024.

[Gopalakrishnan2020] Gopalakrishnan, T., Ruby, D., Al-Turjman, F., Gupta, D., Pustokhina, I. V., Pustokhin, D. A., & Shankar, K. (2020). Deep learning enabled data offloading with cyber attack detection model in mobile edge computing systems. IEEE Access, 8, 185938-185949.

[Hakeem2022]: Abdel Hakeem SA, Hussein HH, Kim H, “Security Requirements and Challenges of 6G Technologies and Applications,” in Sensors, vol. 22, no.5, pp. 1969., 2022. https://doi.org/10.3390/s22051969.

[Hartzog2020] W. Hartzog, & N. Richards (2020). Privacy's constitutional moment and the limits of data protection. BCL Rev., 61, 1687.

[Hassan2020] HASSAN, Hala, et al. Enhanced QoS-based model for trust assessment in cloud computing environment. IEEE Access, 2020, 8: 43752-43763.

[He2022] HE, Yuanhang, et al. A survey on zero trust architecture: Challenges and future trends. Wireless Communications and Mobile Computing, 2022, 2022.

[Henderson2020] P. Henderson, J. Hu, J. Romoff, E. Brunskill, D. Jurafsky, and J. Pineau. (2020). Towards the systematic reporting of the energy and carbon footprints of machine learning. J. Mach. Learn. Res. 21, 1, Article 248

[Hermenier2006] F. Hermenier, N. Loriant, and J.-M. Menaud, “Power management in grid computing with xen,” in International Symposium on Parallel and Distributed Processing and Applications, pp. 407–416, Springer, 2006.

[HU2015] Hu, Y. C., Patel, M., Sabella, D., Sprecher, N., & Young, V. (2015). Mobile edge computing—A key technology towards 5G. ETSI white paper, 11(11), 1-16.

[Hu2018] Hu, Z., Shi, J., Huang, Y., Xiong, J., & Bu, X. (2018, May). GANFuzz: a GAN-based industrial network protocol fuzzing framework. In Proceedings of the 15th ACM International Conference on Computing Frontiers (pp. 138-145).

[Huang2024] Huang, H., Meng, T., Guo, J., Wei, X., & Jia, W. (2024). SecEG: A Secure and Efficient Strategy against DDoS Attacks in Mobile Edge Computing. ACM Transactions on Sensor Networks, 20(3), 1-21.

[Huh2022] Siwon Huh, Seonghwan Cho, Jinho Choi, Seungwon Shin, and Hojoon Lee. 2022. A Comprehensive Analysis of Today’s Malware and Its Distribution Network: Common Adversary Strategies and Implications. IEEE Access 10 (2022), 49566–49584.

[Hummel2022] Hummel, R. et al., 5th Anniversary DDoS Threat Intelligence Report: Unveiling The New Threat Landscape, NETSCOUT 2022

[Hussain 2020] Hussain, F.; Abbas, S.G.; Husnain, M.; Fayyaz, U.U.; Shahzad, F.; Shah, G.A. IoT DoS and DDoS attack detection using ResNet. In Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 5–7 November 2020; pp. 1–6

[Hussain2020] Hussain, F.; Abbas, S.G.; Husnain, M.; Fayyaz, U.U.; Shahzad, F.; Shah, G.A. IoT DoS and DDoS attack detection using ResNet. In Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 5–7 November 2020; pp. 1–6

Co-funded by the European Union

Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

UK Research and Innovation

[HussainR2020] Hussain, R., & You, I. (2020). Security Concerns on Machine Learning Solutions for 6G Networks in mmWave Beam Prediction. arXiv preprint arXiv:2005.08683.

[Idhammad2018] Idhammad M, Afdel K, Belouch M. Semi-supervised machine learning approach for DDoS detection.Appl Intell. 2018;48(10):3193-3208

[IETF2023] Internet Engineering Task Force (IETF), 2023, Available: https://www.ietf.org/

[Ife2019] Colin C Ife, Yun Shen, Steven J Murdoch, and Gianluca Stringhini. 2019. Waves of malice: A longitudinal measurement of the malicious file delivery ecosystem on the web. In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security. 168–180.

[Ife2021] Colin C Ife, Yun Shen, Steven J Murdoch, and Gianluca Stringhini. 2021. Marked for disruption: tracing the evolution of malware delivery operations targeted for takedown. In 24th International Symposium on Research in Attacks, Intrusions and Defenses. 340–353.

[IFRI2022] IFRI, ""Open" Telecom Networks (Open RAN)," 2022.

[Invernizzi2014] Luca Invernizzi, Stanislav Miskovic, Rub´en Torres, Christopher Kru¨gel, Sabyasachi Saha, Giovanni Vigna, Sung-Ju Lee, and Marco Mellia. 2014. Nazca: Detecting Malware Distribution in Large-Scale Networks. In Network and Distributed System Security Symposium.

[ITU2023] International Telecommunication Union, Recommendation ITU-R M.2160-0 (11/2023). M Series: Mobile, radiodetermination, amateur and related satellite services. Framework and overall objectives of the future development of IMT for 2030 and beyond.

[Jafarian2023] Jafarian, J.H., Niakanlahiji, A. "MultiRHM: Defeating multi-staged enterprise intrusion attacks through multi-dimensional and multi-parameter host identity anonymization." Computers & Security, Volume 124, Page 102958. 2023.

[Jafarian2023] Jafarian, Jafar Haadi, and Amirreza Niakanlahiji. "MultiRHM: Defeating multi-staged enterprise intrusion attacks through multi-dimensional and multi-parameter host identity anonymization." Computers & Security 124 (2023): 102958.

[Jazi2017] Hossein Hadian Jazi, Hugo Gonzalez, Natalia Stakhanova, and Ali A. Ghorbani. "Detecting HTTP-based Application Layer DoS attacks on Web Servers in the presence of sampling." Computer Networks, 2017.

[Je2022] D. Je et al., "Selective User Plane (UP) Security for Throughput Enhancement in Mobile Communication," 2022 IEEE Globecom Workshops (GC Wkshps), Rio de Janeiro, Brazil, 2022, pp. 1194-1199, doi:10.1109/GCWkshps56602.2022.10008490.

[Jian2020]: T. Jian et al., "Deep learning for RF fingerprinting: A massive experimental study", in IEEE Internet Things Mag., vol. 3, no. 1, pp. 50-57, 2020.

[Jiang2021] W. Jiang, B. Han, M. A. Habibi and H. D. Schotten, "The Road Towards 6G: A Comprehensive Survey," in IEEE Open Journal of the Communications Society, vol. 2, pp. 334-366, 2021, doi: 10.1109/OJCOMS.2021.3057679.

[JindanXu2020] J. Xu, W. Xu, D. W. K. Ng and A. L. Swindlehurst, "Secure Communication for Spatially Sparse Millimeter-Wave Massive MIMO Channels via Hybrid Precoding," in IEEE Transactions on Communications, vol. 68, no. 2, pp. 887-901, Feb. 2020, doi: 10.1109/TCOMM.2019.2954517.

[Jover2014] R. P. Jover, J. Lackey, and A. Raghavan, "Enhancing the security of LTE networks against jamming attacks," EURASIP Journal on Information Security, vol. 2014, no. 1, p. 7, 2014

[Kabdjou2024] Kabdjou, J., & Shinomiya, N. (2024). Improving Quality of Service and HTTPS DDoS Detection in MEC Environment with a Cyber Deception-Based Architecture. IEEE Access.

[Kakkavas2021] G. Kakkavas, A. Stamou, V. Karyotis and S. Papavassiliou, "Network Tomography for Efficient Monitoring in SDN-Enabled 5G Networks and Beyond: Challenges and Opportunities," in IEEE Communications Magazine, vol. 59, no. 3, pp. 70-76, March 2021.

[Kamvar2003] Kamvar, Sepandar D., Mario T. Schlosser and Hector Garcia-Molina. "The Eigentrust algorithm for reputation management in P2P networks." The Web Conference (2003).

[Kang2014] Kang, B.G., Park, J.H., Hahn, S.G. (2004). A Certificate-Based Signature Scheme. In: Okamoto, T. (eds) Topics in Cryptology – CT-RSA 2004. CT-RSA 2004. Lecture Notes in Computer Science, vol 2964. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24660-2_8

[Kashi2022] M. M. Kashi, A. Yazidi and H. Haugerud, "Mitigating Yo-Yo attacks on cloud auto-scaling," 2022 14th IFIP Wireless and Mobile Networking Conference (WMNC), Sousse, Tunisia, 2022, pp. 46-53, doi: 10.23919/WMNC56391.2022.9954300.

[Khan2022] Khan, M. S., Farzaneh, B., Shahriar, N., Saha, N., & Boutaba, R. (2022, October). SliceSecure: Impact and Detection of DoS/DDoS Attacks on 5G Network Slices. In 2022 IEEE Future Networks World Forum (FNWF) (pp. 639-642). IEEE.

[Kianpisheh2024] S. Kianpisheh and T. Taleb, "Collaborative Federated Learning for 6G With a Deep Reinforcement Learning Based Controlling Mechanism: A DDoS Attack Detection Scenario," in IEEE Transactions on Network and Service Management, early access.

[Kim2018] Eunsoo Kim, Kuyju Kim, Dongsoon Shin, Beomjin Jin, and Hyoungshick Kim. 2018. CyTIME: Cyber Threat Intelligence ManagEment framework for automatically generating security rules. In Proceedings of the 13th International Conference on Future Internet Technologies (CFI

2018). Association for Computing Machinery, New York, NY, USA, Article 7, 1–5. https://doi.org/10.1145/3226052.3226056

[Kim2019] Dohoon Kim. 2019. Potential Risk Analysis Method for Malware Distribution Networks. IEEE Access 7 (2019), 185157–185167. https://doi.org/10.1109/ACCESS.2019.2960552

[Kim2021] B. Kim, Y. E. Sagduyu, T. Erpek, and S. Ulukus, "Adversarial attacks on deep learning based mmWave beam prediction in 5G and beyond," in Proceedings of IEEE Statistical Signal Processing Workshop (SSP), pp. 590–594, 2021.

[Kivity2014] Kivity, A., Laor, D., Costa, G., Enberg, P., Har'El, N., Marti, D., and Zolotarov, V. (2014). OSv—Optimizing the operating system for virtual machines. In 2014 usenix annual technical conference (usenix atc 14), pages 61–72.

[Ko2016] E. Ko, S. Park, S. Kim, K. Son and H. Kim, "SIP amplification attack analysis and detection in VoLTE service network," 2016 International Conference on Information Networking (ICOIN), Kota Kinabalu, Malaysia, 2016, pp. 334-336.

[Krish2024] P. Krishnan, K. Jain, S. R. Poojara, S. N. Srirama, T. Pandey, R. Buyya, "eSIM and blockchain integrated secure zero-touch provisioning for autonomous cellular-IoTs in 5G networks," in Computer Communications, vol. 216, pp. 324-345, 2024.

[Kubernetes2023] Kubernetes: Production-Grade Container Orchestration", 2023, Available: https://kubernetes.io/

[Kuenzer2021] Kuenzer, S., Badoiu, V.-A., Lefeuvre, H., Santhanam, S., Jung, A., Gain, G., Soldani, C., Lupu, C., Teodorescu, S¸ ., Raducanu, C., Banu, C., Mathy, L., Deaconescu, R., Raiciu, C., and Huici, F. (2021). Unikraft. In Proceedings of the Sixteenth European Conference on Computer Systems. ACM.

[Kuipers2006] Kuipers D, Fabro M. Control systems cyber security: Defense in depth strategies. Idaho National Lab.(INL), Idaho Falls, ID (United States); 2006 May 1.

[Kumaran2017] S. Kumaran S., Practical LXC and LXD. Apress, 2017.

[Kwon2015] Bum Jun Kwon, Jayanta Mondal, Jiyong Jang, Leyla Bilge, and Tudor Dumitra¸s. 2015. The dropper effect: Insights into malware distribution with downloader graph analytics. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. 1118–1129.

[Labreche2022] Fran¸cois Labr`eche, Enrico Mariconti, and Gianluca Stringhini. 2022. Shedding Light on the Targeted Victim Profiles of Malicious Downloaders. In Proceedings of the 17th International Conference on Availability, Reliability and Security. 1–10.

[Lalropuia2021] K.C. Lalropuia, V. Khaitan (nee Gupta), “Availability and reliability analysis of cloud computing under economic denial of sustainability (EDoS) attack: a semi-Markov approach,” Cluster Computing, 24, 2177–2191 (2021). https://doi.org/10.1007/s10586-021-03257-9

[Laurie2013] B. Laurie, A. Langley and E. Kasper, Certificate transparency, Fremont, CA, USA, pp. 1-27, Jun. 2013, [online] Available: https://www.rfc-editor.org/rfc/rfc6962.txt

[Li2020]: S. Li, W. Sun, H. Zhang and Y. Zhang, "Physical Layer Security for Edge Caching in 6G Networks," in GLOBECOM 2020, 2020 IEEE Global Communications Conference, Taipei, Taiwan, 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9322524

[Li2021] Y. Li, Y. Yu, W. Susilo, Z. Hong and M. Guizani, "Security and Privacy for Edge Intelligence in 5G and Beyond Networks: Challenges and Solutions," in IEEE Wireless Communications, vol. 28, no. 2, pp. 63-69, April 2021, doi: 10.1109/MWC.001.2000318

[Lichtman2018] M. Lichtman, R. Rao, V. Marojevic, J. Reed, and R. P. Jover, “5G NR jamming, spoofing, and sniffing: threat assessment and mitigation,” in Proceedings of IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–6, 2018.

[Lichtman2018]: M. Lichtman, R. Rao, V. Marojevic, J. Reed and R. P. Jover, "5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation," 2018 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, USA, 2018, pp. 1-6, doi: 10.1109/ICCW.2018.8403769.

[Liu2021] Liu, X., Zhang, W., Zhou, X., & Zhou, Q. (2021). MECGuard: GRU enhanced attack detection in Mobile Edge Computing environment. Computer Communications, 172, 1-9.

[Liu2021] Q. Liu, S. Sun, B. Rong, and M. Kadoch, “Intelligent reflective surface based 6G communications for sustainable energy infrastructure,” IEEE Wirel. Commun., vol. 28, no. 6, pp. 49–55, 2021.

[Luckie2020] Matthew Luckie, Alexander Marder, Marianne Fletcher, Bradley Huffaker, and K. Claffy. 2020. Learning to Extract and Use ASNs in Hostnames. In Proceedings of the ACM Internet Measurement Conference (Virtual Event, USA) (IMC ’20). Association for Computing Machinery, New York, NY, USA, 386–392. https://doi.org/10.1145/3419394.3423639

[Ma2022] Ma, Y., Xu C., Wei F., and Ning G. "DDoS detection for 6G Internet of Things: Spatial-temporal trust model and new architecture." China Communications 19, no. 5 (2022): 141-149.

[Makarevitch2006] B. Makarevitch, “Jamming resistant architecture for WiMAX mesh network,” in Proceedings of IEEE Military Communications conference (MILCOM), pp. 1–6, 2006.

[Maleh2023] Maleh, Yassine, et al. "A comprehensive survey on SDN security: threats, mitigations, and future directions." Journal of Reliable Intelligent Environments 9.2 (2023): 201-239.

[Mavridis2021] Mavridis, I. and Karatza, H. (2021). Orchestrated sandboxed containers, unikernels, and virtual machines for isolation-enhanced multitenant workloads and serverless computing in cloud. Concurrency and Computation: Practice and Experience, 35(11).

[Microsoft2021] Microsoft Defender Research Team, "Cyberbattlesim," https://github.com/microsoft/cyberbattlesim, 2021, created by Christian Seifert, Michael Betser, William Blum, James Bono, Kate Farris, Emily Goren, Justin Grana, Kristian Holsheimer, Brandon Marken, Joshua Neil, Nicole Nichols, Jugal Parikh.

[Mitev2019]: M. Mitev, A. Chorti, E. V. Belmega and M. Reed, "Man-in-the-middle and denial of service attacks in wireless secret key generation", Proc. IEEE Glob. Commun. Conf., pp. 1-6, 2019.

[Mitev2023]: M. Mitev, A. Chorti, H. V. Poor and G. P. Fettweis, "What Physical Layer Security Can Do for 6G Security," in IEEE Open Journal of Vehicular Technology, vol. 4, pp. 375-388, 2023, doi: 10.1109/OJVT.2023.3245071.

[Monge2019] M. A. S. Monge, J. M. Vidal, G. M. Pérez, "Detection of economic denial of sustainability (EDoS) threats in self-organizing networks, Computer Communications," Volume 145, 2019, pp 284-308, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2019.07.002.

[Moussaoui2022]: M. Moussaoui, E. Bertin and N. Crespi, "5G shortcomings and Beyond-5G/6G requirements," in 2022 1st International Conference on 6G Networking (6GNet), Paris, France, 2022, pp. 1-8, doi: 10.1109/6GNet54646.2022.9830439.

[Mrabet2023] Mrabet, Khalid, Faissal El Bouanani, and Hussain Ben-Azza. 2023. "Dynamic Decentralized Reputation System from Blockchain and Secure Multiparty Computation" Journal of Sensor and Actuator Networks 12, no. 1: 14. https://doi.org/10.3390/jsan12010014

[Mukherjee2020] Mukherjee, M., Matam, R., Mavromoustakis, C. X., Jiang, H., Mastorakis, G., & Guo, M. (2020). Intelligent edge computing: Security and privacy challenges. IEEE Communications Magazine, 58(9), 26-31.

[Musa2024] N. S. Musa, N. M. Mirza, S. H. Rafique, A. M. Abdallah, and T. Murugan, "Machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks—current research solutions," IEEE Access, vol. 12, pp. 17982–18011, 2024.

[Musumeci2020] Musumeci, F., Ionata, V., Paolucci, F., Cugini, F., & Tornatore, M. (2020). Machine-learning-assisted DDoS attack detection with P4 language. ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 1-6.

[Naeem2023] F. Naeem, M. Ali, G. Kaddoum, C. Huang and C. Yuen, "Security and Privacy for Reconfigurable Intelligent Surface in 6G: A Review of Prospective Applications and Challenges," in IEEE Open Journal of the Communications Society, vol. 4, pp. 1196-1217, 2023

[Najafimehr 2023] Najafimehr M, Zarifzadeh S, Mostafavi S. DDoS attacks and machine-learning-based detection methods: A survey and taxonomy. Engineering Reports. 2023; 5(12):e12697. doi: 10.1002/eng2.12697

[Najafimehr2023] Najafimehr M, Zarifzadeh S, Mostafavi S. DDoS attacks and machine-learning-based detection methods: A survey and taxonomy. Engineering Reports. 2023; 5(12):e12697. doi: 10.1002/eng2.12697

[Naor2000] M. Naor and K. Nissim, "Certificate revocation and certificate update," in IEEE Journal on Selected Areas in Communications, vol. 18, no. 4, pp. 561-570, April 2000, doi: 10.1109/49.839932.

[Narayanan2023] V. Narayanan et al., “Remote attestation of confidential VMs using ephemeral vTPMs,” in Proceedings of the 39th Annual Computer Security Applications Conference, in ACSAC ’23. New York, NY, USA: Association for Computing Machinery, Dec. 2023, pp. 732–743. doi: 10.1145/3627106.3627112.

[Naser2023] S. Naser, L. Bariah, S. Muhaidat, and E. Basar, “Zero-energy devices empowered 6G networks: Opportunities, key technologies, and challenges,” IEEE Internet Things M., vol. 6, no. 3, pp. 44–50, 2023.

[Nazar2023] Nazar, M. J., Alhudhaif, A., Qureshi, K. N., Iqbal, S., & Jeon, G. . Signature and flow statistics based anomaly detection system in software-defined networking for 6G internet of things network. International Journal of System Assurance Engineering and Management, 1-11 (2023).

[NFV-SEC024] ETSI NFV SEC, Document n. GS NFV-SEC 024, " Network Functions Virtualisation (NFV) Security; Security Management Specification " V 0.0.8 with status: Early draft - with comment: Agreed in NFVSEC_24, 2023.

[Nguyen2020]: V. L. Nguyen, P. C. Lin and R. H. Hwang, "Enhancing misbehavior detection in 5G vehicle-to-vehicle communications", in IEEE Trans. Veh. Technol., vol. 69, no. 9, pp. 9417-9430, Sep. 2020.

[Nguyen2021] V. -L. Nguyen, P. -C. Lin, B. -C. Cheng, R. -H. Hwang and Y. -D. Lin, "Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges," in IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2384-2428, Fourthquarter 2021, doi: 10.1109/COMST.2021.3108618.

[Niksirat2024] K. S. Niksirat, L. Velykoivanenko, N. Zufferey, M. Cherubini, K. Huguenin, and M. Humbert. (2024). Wearable Activity Trackers: A Survey on Utility, Privacy, and Security. ACM Comput. Surv. 56, 7, Article 183

[NIS2022] NIS Group, "Report on the cybersecurity of Open RAN," 2022.

[NIST01] NIST, “NIST Vocabulary.” https://csrc.nist.gov/glossary/term/moving_target_defense.

[NTT2021] NTT Docomo, "5G Open RAN Ecosystem Whitepaper," 2021.

[Olimid2020] Olimid, Ruxandra F., and Gianfranco Nencioni. "5G network slicing: A security overview." IEEE Access 8 (2020): 99999-100009.

[Openstack2023] OpenStack: Open Source Cloud Computing Infrastructure”, 2023, Available: https://www.openstack.org/

[Oprea2023] Oprea, A., & Vassilev, A. (2023). Adversarial machine learning: A taxonomy and terminology of attacks and mitigations (No. NIST Artificial Intelligence (AI) 100-2 E2023 (Withdrawn)). National Institute of Standards and Technology.

[O-RAN2021] O. R. P. C. O-Ran Alliance, Open-RAN Security in 5G (2021). doi: https://www.openranpolicy.org/wp-content/uploads/2021/04/Open-RAN-Security-in-5G-4.29.21.pdf

[Ortiz2020] J. Ortiz, R. Sanchez-Iborra, J. B. Bernabe, A. Skarmeta, C. Benzaid, T. Taleb, P. Alemany, R. Mu˜noz, R. Vilalta, C. Gaber, J.-P. Wary, D. Ayed, P. Bisson, M. Christopoulou, G. Xilouris, E. M. de Oca, G. G˙ur, G. Santinelli, V. Lefebvre, A. Pastor, and D. Lopez, “INSPIRE-5Gplus: Intelligent security and pervasive trust for 5G and beyond networks,” in Proceedings of the 15th International Conference on Availability, Reliability and Security, ser. ARES ’20. New York, NY, USA: Association for Computing Machinery, 2020.

[Paolucci2021] F. Paolucci et al., "User Plane Function Offloading in P4 switches for enhanced 5G Mobile Edge Computing," 2021 17th International Conference on the Design of Reliable Communication Networks (DRCN), Milano, Italy, 2021, pp. 1-3, doi: 10.1109/DRCN51631.2021.9477338.

[Parra-Ullauri2024] J. M. Parra-Ullauri, X. Zhang, A. Bravalheri, S. Moazzeni, Y Wu, R. Nejabati, D. Simeonidou, "Federated Analytics for 6G Networks: Applications, Challenges, and

Opportunities," in IEEE Network, Volume 38, no. 2, pp. 9-17, March 2024, doi: 10.1109/MNET.2024.3355218.

[Pineda2023] D. Pineda, R. Harrilal-Parchment, K. Akkaya and A. Perez-Pons, "SDN-based GTP-U Traffic Analysis for 5G Networks," NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, Miami, FL, USA, 2023, pp. 1-4, doi: 10.1109/NOMS56928.2023.10154440.

[Pirayesh 2022] H. Pirayesh and H. Zeng, “Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey,” in IEEE Commun. Surv. Tut., vol. 24, no. 2, pp. 767–809, 2022.

[Pirayesh2022]: H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 767-809, Secondquarter 2022, doi: 10.1109/COMST.2022.3159185.

[Popescu2015] Adrian Stefan Popescu, Dumitru Bogdan Prelipcean, and Dragos Teodor Gavrilut. 2015. A Study on Techniques for Proactively Identifying Malicious URLs. In 2015 17th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC). 204–211. https://doi.org/10.1109/SYNASC.2015.40

[Porambage2021] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, "The Roadmap to 6G Security and Privacy," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1094-1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.

[PorambageGur2021] P. Porambage, G. Gür, D. P. Moya Osorio, M. Livanage and M. Ylianttila, "6G Security Challenges and Potential Solutions," 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 2021, pp. 622-627, doi: 10.1109/EuCNC/6GSummit51104.2021.9482609.

[Priyadarshani2024] Priyadarshani, Richa, Ki-Hong Park, Yalcin Ata, and Mohamed-Slim Alouini. "Jamming Intrusions in Extreme Bandwidth Communication: A Comprehensive Overview." arXiv preprint arXiv:2403.19868 (2024).

[Quad2023] National Telecommunications and Information Administration, United States Department of Commerce, Quad Critical and Emerging Technology Working Group, Open RAN Security Report, May 2023

[Quy2023] V. K. Quy, A. Chehri, N. M. Quy, N. D. Han and N. T. Ban, "Innovative Trends in the 6G Era: A Comprehensive Survey of Architecture, Applications, Technologies, and Challenges," in IEEE Access, vol. 11, pp. 39824-39844, 2023, doi: 10.1109/ACCESS.2023.3269297.

[Rakotondravony2017] No¨elle Rakotondravony, Benjamin Taubmann, Waseem Mandarawi, Eva Weish¨aupl, Peng Xu, Bojan Kolosnjaji, Mykolai Protsenko, Hermann De Meer, and Hans P Reiser. 2017. Classifying malware attacks in IaaS cloud environments. Journal of Cloud Computing 6, 1 (2017), 1–12.

[Ramirez2022] Ramirez, M. A., Kim, S. K., Hamadi, H. A., Damiani, E., Byon, Y. J., Kim, T. Y., ... & Yeun, C. Y. (2022). Poisoning attacks and defenses on artificial intelligence: A survey. arXiv preprint arXiv:2202.10276.

[Ramzan2023] Ramzan, M.; Shoaib, M.; Altaf, A.; Arshad, S.; Iqbal, F.; Castilla, Á.K.; Ashraf, I. Distributed Denial of Service Attack Detection in Network Traffic Using Deep Learning Algorithm. Sensors 2023, 23, 8642. https://doi.org/10.3390/s23208642

[Ranaweera2021] Ranaweera, P., Jurcut, A. D., & Liyanage, M.. Survey on multi-access edge computing security and privacy. IEEE Communications Surveys & Tutorials, 23(2), 1078-1124. (2021)

[Resnick2002] Resnick, P. and Zeckhauser, R. (2002), "Trust among strangers in internet transactions: Empirical analysis of eBay' s reputation system", Baye, M.R. (Ed.) The Economics of the Internet and E-commerce (Advances in Applied Microeconomics, Vol. 11), Emerald Group Publishing Limited, Leeds, pp. 127-157. https://doi.org/10.1016/S0278-0984(02)11030-3

[Rezgui2019]: G. Rezgui, E. V. Belmega and A. Chorti, "Mitigating jamming attacks using energy harvesting", in IEEE Wireless Commun. Lett., vol. 8, no. 1, pp. 297-300, Feb. 2019.

[Rizvi2014] Syed Rizvi, Katie Cover, Christopher Gates, A Trusted Third-party (TTP) based Encryption Scheme for Ensuring Data Confidentiality in Cloud Environment, Procedia Computer Science, Volume 36, 2014, Pages 381-386, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2014.09.009.

[Roy2021] Sayak Saha Roy, Unique Karanjit, and Shirin Nilizadeh. 2021. What remains uncaught?: Characterizing sparsely detected malicious urls on twitter.

[Sadeghi2019] M. Sadeghi and E. G. Larsson, “Physical adversarial attacks against end-to-end autoencoder communication systems,” IEEE Communications Letters, vol. 23, no. 5, pp. 847–850, 2019.

[Saeed2023] M. M. Saeed, R. A. Saeed, M. Abdelhaq, R. Alsaqour, M. K. Hasan, and R. A. Mokhtar, “Anomaly detection in 6G networks using machine learning methods,” Electronics (Basel), vol. 12, no. 15, p. 3300, 2023.

[Sagduyu2021] Sagduyu, Y. E., Erpek, T., & Shi, Y. (2021). Adversarial machine learning for 5G communications security. Game Theory and Machine Learning for Cyber Security, 270-288.

[Sagduyu2021] Y. E. Sagduyu, T. Erpek, and Y. Shi, “Adversarial machine learning for 5G communications security,” arXiv preprint arXiv:2101.02656, 2021

[SalahdineHan2023] F. Salahdine, T. Han, N. Zhang, “5G, 6G, and Beyond: Recent advances and future challenges,” Annals of Telecommunications, Volume 78, pp 525–549 (2023). https://doi.org/10.1007/s12243-022-00938-3

[Salameh2022] Salameh, Ahmed I., and Mohamed El Tarhuni. 2022. "From 5G to 6G—Challenges, Technologies, and Applications" Future Internet 14, no. 4: 117. https://doi.org/10.3390/fi14040117

[Salim2023] Salim, Duraid, Manmeet Mahinderjit Singh, and Pantea Keikhosrokiani. "A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model." Heliyon, vol. 9, 2023, e17156. 10.1016/j.heliyon.2023.e17156.

[SANCUS] SANCUS Project [Online]. Available: https://sancus-project.eu/. Accessed: 20-June-2024.

[Sansone] Isabella Sansone, The Damaging Impacts of DDoS Attacks, Online: https://www.corero.com/the-damaging-impacts-of-ddos-attacks/. Accessed: May 2024

[Santos2020] Santos, R., Danilo S., Walter S., Admilson R., and Edward M.. "Machine learning algorithms to detect DDoS attacks in SDN." Concurrency and Computation: Practice and Experience 32, no. 16 (2020): e5402.

[Saraswat2022] A.K. Saraswat, & V. Meel (2022). Protecting Data in the 21st Century: Challenges, Strategies and Future Prospects. Information Technology in Industry, 10(2), 26-35.

[Sathi2021] V. N. Sathi and C. S. R. Murthy, "Distributed Slice Mobility Attack: A Novel Targeted Attack Against Network Slices of 5G Networks," in IEEE Networking Letters, vol. 3, no. 1, pp. 5-9, March 2021, doi: 10.1109/LNET.2020.3044642.

[Scalise2024] P. Scalise, M. Boeding, M. Hempel, H. Sharif, J. Delloiacovo, and J. Reed, “A systematic survey on 5G and 6G security considerations, challenges, trends, and research areas,” Future Internet, vol. 16, no. 3, p. 67, 2024.

[Seifousadati 2021] Seifousadati, A.; Ghasemshirazi, S.; Fathian, M. A Machine Learning approach for DDoS detection on IoT devices. arXiv 2021, arXiv:2110.14911.

[Seifousadati2021] Seifousadati, A.; Ghasemshirazi, S.; Fathian, M. A Machine Learning approach for DDoS detection on IoT devices. arXiv 2021, arXiv:2110.14911.

[Senigagliesi2020]: L. Senigagliesi, M. Baldi and E. Gambi, "Comparison of statistical and machine learning techniques for physical layer authentication", in IEEE Trans. Inf. Forensics Security, vol. 16, pp. 1506-1521, Oct. 2020.

[Sequeiros2021] João B. F. Sequeiros, Francisco T. Chimuco, Musa G. Samaila, Mário M. Freire, and Pedro R. M. Inácio. 2020. Attack and System Modeling Applied to IoT, Cloud, and Mobile Ecosystems: Embedding Security by Design. ACM Comput. Surv. 53, 2, Article 25 (March 2021).

[Shaik2019]: A. Shaik, R. Borgaonkar, S. Park, J.-P. Seifert, "New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities," in Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, pp. 221-231, doi: 10.1145/3317549.3319728.

[Sharafaldin 2019] I. Sharafaldin, A. H. Lashkari, S. Hakak, A. A. Ghorbani, Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy, in: 2019 International Carnahan Conference on Security Technology (ICCST), IEEE, 2019, pp. 1–8.

[Sharafaldin2018] Iman Sharafaldin et al. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization:. In Proceedings of the 4th International Conference on Information Systems Security and Privacy, pages 108–116, 2018.

[Sharafaldin2019] Iman Sharafaldin et al. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. In 2019 International Carnahan Conference on Security Technology (ICCST), pages 1–8, October 2019.

[Sheikhi2020] A. Sheikhi, S. M. Razavizadeh, and I. Lee, "A comparison of TDD and FDD massive MIMO systems against smart jamming," IEEE Access, vol. 8, pp. 72068–72077, 2020.

[Shen2019] Yun Shen and Gianluca Stringhini. 2019. ATTACK2VEC: Leveraging Temporal Word Embeddings to Understand the Evolution of Cyberattacks. In 28th USENIX Security Symposium (USENIX Security 19). USENIX Association, Santa Clara, CA, 905–921. https://www.usenix.org/conference/usenixsecurity19/presentation/shen

[Shen2021] Yun Shen and Gianluca Stringhini. 2021. ANDRUSPEX: leveraging graph representation learning to predict harmful app installations on mobile devices. In 2021 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 562–577.

[ShenFeng2023] L. Shen, K. Feng, and L. Hanzo, "Five Facets of 6G: Research Challenges and Opportunities," ACM Computing Surveys, Volume 55, Issue 11, Article 235 (November 2023), 39 pages. https://doi.org/10.1145/3571072

[Shi2021] Y. Shi, Y. E. Sagduyu, T. Erpek, and M. C. Gursoy, "How to attack and defend 5G radio access network slicing with reinforcement learning," arXiv preprint arXiv:2101.05768, 2021.

Co-funded by the European Union

[Shorna2021] Shorna, Sabira Khanam, "Performance Analysis of 5G DDoS Attack Using Machine Learning" (2021). Electronic Theses and Dissertations. 2201. https://digitalcommons.memphis.edu/etd/2201

[Siriwardhana2021] Y. Siriwardhana, P. Porambage, M. Liyanage and M. Ylianttila, "AI and 6G Security: Opportunities and Challenges," 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 2021, pp. 616-621, doi: 10.1109/EuCNC/6GSummit51104.2021.9482503.

[Song2022] L. Song, Y. Ding, P. Dong, Y. Guo, and C. Wang, "TZ-IMA: Supporting Integrity Measurement for Applications with ARM TrustZone," in Information and Communications Security, C. Alcaraz, L. Chen, S. Li, and P. Samarati, Eds., Cham: Springer International Publishing, 2022, pp. 342–358. doi: 10.1007/978-3-031-15777-6_19.

[Souppaya2019] M. Souppaya, J. Morello, and K. Scarfone, "NIST Special Publication 800- 190 Application Container Security Guide," 2017. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-190

[Soussi2021] W. Soussi, M. Christopoulou, G. Xilouris and G. Gür, "Moving Target Defense as a Proactive Defense Element for Beyond 5G," in IEEE Communications Standards Magazine, vol. 5, no. 3, pp. 72-79, September 2021.

[Soussi2023] W. Soussi, M. Christopoulou, G. Gür and B. Stiller, "MERLINS – Moving Target Defense Enhanced with Deep-RL for NFV In-Depth Security," 2023 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Dresden, Germany, 2023.

[Spies2021] B. Spies and M. Mock, "An Evaluation of WebAssembly in Non-Web Environments," 2021 XLVII Latin American Computing Conference (CLEI), Cartago, Costa Rica, 2021, pp. 1-10, doi: 10.1109/CLEI53233.2021.9640153.

[Srinivasan2006] A. Srinivasan, J. Teitelbaum and J. Wu, "DRBTS: Distributed Reputation-based Beacon Trust System," 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, Indianapolis, IN, USA, 2006, pp. 277-283, doi: 10.1109/DASC.2006.28.

[Stafford2020] STAFFORD, V. A. Zero trust architecture. NIST special publication, 2020, 800: 207.

[Sun2020] Y. Sun, J. Liu, J. Wang, Y. Cao and N. Kato (2020). "When Machine Learning Meets Privacy in 6G: A Survey," in IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2694-2724, Fourthquarter 2020.

[Syed2016] Z. Syed, Ankur Padia, Tim Finin, Lisa Mathews and Anupam Joshi. 2016. UCO: A Unified Cybersecurity Ontology. In The Workshops of the Thirtieth AAAI Conference on Artificial Intelligence. Artificial Intelligence for Cyber Security: Technical Report WS-16-03.

[Syed2022] SYED, Naeem Firdous, et al. Zero trust architecture (zta): A comprehensive survey. IEEE Access, 2022, 10: 57143-57179.

[Ta2022] Q. V. Ta and M. Park, "Economic Denial of Sustainability (EDoS) attack detection by attention on flow-based in Software Defined Network (SDN)," 2022 International Conference on Information Networking (ICOIN), Jeju-si, Korea, Republic of, 2022, pp. 183-185, doi: 10.1109/ICOIN53446.2022.9687229.

[Taleb2022] Taleb, T., Benzaed, C., Lopez, M.B., Mikhaylov, K., Tarkoma, S., Kostakos, P., Mahmood, N.H., Pirinen, P., Matinmikko-Blue, M., Latva-aho, M., & Pouttu, A. (2022). 6G System architecture: A service of services vision. ITU Journal on Future and Evolving Technologies.

[Talpur2024] Talpur F, Korejo IA, Chandio AA, Ghulam A, Talpur MSH. ML-Based Detection of DDoS Attacks Using Evolutionary Algorithms Optimization. Sensors. 2024; 24(5):1672. https://doi.org/10.3390/s24051672

[Tan2023] Tan, J., Jin, H., Zhang, H., Zhang, Y., Chang, D., Liu, X., Zhang, H. "A survey: When moving target defense meets game theory." Computer Science Review, 48, 100544. 2023.

[Tataria2021] H. Tataria, M. Shafi, A. F. Molisch, M. Dohler, H. Sjöland and F. Tufvesson, "6G Wireless Systems: Vision, Requirements, Challenges, Insights, and Opportunities," in Proceedings of the IEEE, vol. 109, no. 7, pp. 1166-1199, July 2021, doi: 10.1109/JPROC.2021.3061701.

[Thijsman2024] J. Thijsman, M. Sebrechts, F. De Turck, and B. Volckaert, “Trusting the Cloud-Native Edge: Remotely Attested Kubernetes Workers.” arXiv, May 16, 2024. doi: 10.48550/arXiv.2405.10131.

[Thijsman2024] THIJSMAN, Jordi, et al. Trusting the Cloud-Native Edge: Remotely Attested Kubernetes Workers. arXiv preprint arXiv:2405.10131, 2024.

[Timan2021] Timan, T., & Mann, Z. (2021). Data protection in the era of artificial intelligence: trends, existing solutions and recommendations for privacy-preserving technologies. In The elements of big data value: Foundations of the research and innovation ecosystem (pp. 153-175). Cham: Springer International Publishing.

[Trahan2022] J. L. Trahan and V. Cherneva, "TTP-mtOTP: Trusted Third Party, Ownership Transfer Protocol for Multiple RFID Tags," 2022 IEEE International Conference on RFID (RFID), Las Vegas, NV, USA, 2022, pp. 35-40, doi: 10.1109/RFID54732.2022.9795963.

[Truong2021] Truong, H. T., Pham, C., Pham, T. X., & Nguyen, N. (2021). Security for AI in 6G Communications. Journal of Communications and Networks, 23(4), 279-287.

[Ullah2020] Ullah, S., Li, XY. & Lan, Z. A novel trusted third party based signcryption scheme. Multimed Tools Appl 79, 22749–22769 (2020). https://doi.org/10.1007/s11042-020-09027-w

[VanLiebergen2022] Kevin van Liebergen, Juan Caballero, Platon Kotzias, and Chris Gates. 2022. A Deep Dive into VirusTotal: Characterizing and Clustering a Massive File Feed. arXiv:2210.15973 [cs.CR]

[Villegas2023] Villegas-Ch, W., & García-Ortiz, J. (2023). Toward a Comprehensive Framework for Ensuring Security and Privacy in Artificial Intelligence. Electronics, 12(18), 3786.

[Vinogradova2016] J. Vinogradova, E. Bjornson, and E. G. Larsson, “Detection and ¨ mitigation of jamming attacks in massive MIMO systems using random matrix theory,” in Proceedings of IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), pp. 1–5, 2016.

[Wang2013] Gang Wang, Jack W. Stokes, Cormac Herley, and David Felstead. 2013. Detecting malicious landing pages in Malware Distribution Networks. In 2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). 1–11. https://doi.org/10.1109/DSN.2013.6575316

[Wang2018] C. -H. Wang, "An Identity-Based Fair Contract Signing Protocol Constructed by the Confirmation Signature," 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan, 2018, pp. 1-6, doi: 10.1109/DESEC.2018.8625116

[Wang2020] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, W. Zhou, “Security and privacy in 6G networks: New areas and new challenges, Digital Communications and Networks,” vol 6, issue 3, 2020, pp. 281-291, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2020.07.003.

[Wang2022] Wang, Y., Kang, X., Li, T., Wang, H., Chu, C. K., & Lei, Z. (2022). SIX-Trust for 6G: Towards a secure and trustworthy 6G network. arXiv preprint arXiv:2210.17291.

[Williams2022]: L. Williams, B. K. Sovacool, T. J. Foxon, “The energy use implications of 5G: Reviewing whole network operational energy, embodied energy, and indirect effects,” in Renewable and Sustainable Energy Reviews, vol. 157, p. 112033, 2022.

[Wyner1975] A. D. Wyner, “The wire ‐ tap channel,” in Bell Systems Technical Journal, , vol. 54, no 8, pp. 1355-1387, 1975.

[Xavier2023] Xavier, B. M., Dzaferagic, M., Collins, D., Comarela, G., Martinello, M., & Ruffini, M. (2023, May). Machine learning-based early attack detection using open RAN intelligent controller. In ICC 2023-IEEE International Conference on Communications (pp. 1856-1861). IEEE.

[Xiao2018] Z. Xiao, B. Gao, S. Liu, and L. Xiao, “Learning based power control for mmWave massive MIMO against jamming,” in 2018 IEEE Global Communications Conference (GLOBECOM), pp. 1–6, IEEE, 2018.

[Xiong2004] Li Xiong, & Ling Liu. (2004). PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities. IEEE Transactions on Knowledge and Data Engineering, 16(07), 843–857. doi:10.1109/tkde.2004.1318566

[Xu2020] X. Xu, J. Li, H. Yu, L. Luo, X. Wei, G. Sun, " Towards Yo-Yo attack mitigation in cloud auto-scaling mechanism," Digital Communications and Networks, Volume 6, Issue 3, 2020, Pages 369-376, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2019.07.002.

[Yadav2024] J. D. Yadav, V. K. Dwivedi,, S. Chaturvedi, "Enhancing 6G network security: GANs for pilot contamination attack detection in massive MIMO systems," in AEU-International Journal of Electronics and Communications, 175, p. 155075, 2024

[Yao2018] Zijun Yao, Yifan Sun, Weicong Ding, Nikhil Rao, and Hui Xiong. 2018. Dynamic word embeddings for evolving semantic discovery. In Proceedings of the eleventh acm international conference on web search and data mining. 673–681.

[Yao2023] Mingxuan Yao, Jonathan Fuller, Ranjita Pai Sridhar, Saumya Agarwal, Amit K. Sikder, and Brendan Saltaformaggio. 2023. Hiding in Plain Sight: An Empirical Study of Web Application Abuse in Malware. In USENIX Security Symposium.

[Yoo2024] Yoo, Sophia, Xiaoqi Chen, and Jennifer Rexford. "SmartCookie: Blocking large-scale SYN floods with a split-proxy defense on programmable data planes." In USENIX Security, August 2024.

[Yoon2021] S. Yoon, J.-H. Cho, D. S. Kim, T. J. Moore, F. Free-Nelson, and H. Lim, "DESOLATER: Deep Reinforcement Learning-Based Resource Allocation and Moving Target Defense Deployment Framework," IEEE Access, vol. 9, pp. 70 700–70 714, 2021.

[Zal2024] Żal, M., Michalski, M., Zwierzykowski, P. "Implementation of a Lossless Moving Target Defense Mechanism." Electronics, Volume 13, Issue 5, Article Number 918. 2024.

[Żal2024] Żal, M.; Michalski, M.; Zwierzykowski, P. Implementation of a Lossless Moving Target Defense Mechanism. Electronics 2024, 13, 918. https://doi.org/10.3390/electronics13050918.

[Zhang2020] Zhang, J., Li, C., & Zhang, J. (2020). Physical Layer Security for 5G and Beyond. IEEE Wireless Communications, 27(6), 120-126.

[Zhang2020] Zhang, M., Li, G., Wang, S., Liu, C., Chen, A., Hu, H., Gu, G., Li, Q., Xu, M., and Wu, J. "Poseidon: Mitigating Volumetric DDoS Attacks with Programmable Switches." Proceedings 2020 Network and Distributed System Security Symposium, 2020.

[Zhang2023] J. Zhang, G. Shen, W. Saad and K. Chowdhury, "Radio Frequency Fingerprint Identification for Device Authentication in the Internet of Things," in IEEE Communications Magazine, vol. 61, no. 10, pp. 110-115, October 2023

[Zhang2023] Y. Zhang et al., "Energy Drain Attack in Satellite Internet Constellations," 2023 IEEE/ACM 31st International Symposium on Quality of Service (IWQoS), Orlando, FL, USA, 2023, pp. 1-10, doi: 10.1109/IWQoS57198.2023.10188709

[Zhang2024] X. Zhang, K. Qin, S. Qu, T. Wang, C. Zhang, and D. Gu, “Teamwork Makes TEE Work: Open and Resilient Remote Attestation on Decentralized Trust.” arXiv, Feb. 13, 2024. doi: 10.48550/arXiv.2402.08908.

[Zhao2024] Zhao, Z., Zhaoxuan L., Zhihao Z., Jiongchi Y., Zhuoxue S., Xiaofei X., Fan Z., and Rui Z.. "DDoS family: A novel perspective for massive types of DDoS attacks." Computers & Security 138 (2024): 103663.

[Zhong2020] C. Zhong, F. Wang, M. C. Gursoy, and S. Velipasalar, “Adversarial jamming attacks on deep reinforcement learning based dynamic multichannel access,” in 2020 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6, IEEE, 2020.

[Zhou2021] Zhou, X., Xu, M., Wu, Y., & Zheng, N. (2021). Deep Model Poisoning Attack on Federated Learning. Future Internet 2021, 13, 73.

[Zhu2019] J. Zhu, Z. Wang, Q. Li, H. Chen, and N. Ansari, “Mitigating intended jamming in mmWave MIMO by hybrid beamforming,” IEEE Wireless Communications Letters, vol. 8, no. 6, pp. 1617–1620, 2019.

[Zhu2020] Shuofei Zhu, Jianjun Shi, Limin Yang, Boqin Qin, Ziyi Zhang, Linhai Song, and Gang Wang. 2020. Measuring and Modeling the Label Dynamics of Online {Anti-Malware} Engines. In 29th USENIX Security Symposium (USENIX Security 20). 2361–2378.

[Ziegler2020] V. Ziegler, H. Viswanathan, H. Flinck, M. Hoffmann, V. Räisänen and K. Hätönen, "6G Architecture to Connect the Worlds," in IEEE Access, vol. 8, pp. 173508-173520, 2020, doi: 10.1109/ACCESS.2020.3025032.

[Zolotukhin2022] Zolotukhin, M., Zhang, D., Hämäläinen, T., & Miraghaei, P. (2022). On attacking future 5g networks with adversarial examples: Survey. Network, 3(1), 39-90.

[Zou2023] C. Zou, C. Li, Y. Li, X. Yan, "RIS-Assisted Robust Beamforming for UAV Anti-Jamming and Eavesdropping Communications: A Deep Reinforcement Learning Approach," Electronics 2023, 12, 4490. https://doi.org/10.3390/electronics12214490