ROBUST-6G: Smart, Automated, and Reliable Security Service Platform for 6G

Conference Paper · July 2024

CITATIONS
0

READS
41

19 authors, including:

Bartlomiej Siniarski
University College Dublin
20 PUBLICATIONS **45** CITATIONS
SEE PROFILE

Chamara Sandeepa
University College Dublin
19 PUBLICATIONS **68** CITATIONS
SEE PROFILE

Madhusanka Liyanage
University College Dublin
335 PUBLICATIONS **10,720** CITATIONS
SEE PROFILE

ROBUST-6G: Smart, Automated, and Reliable Security Service Platform for 6G

Bartlomiej Siniarski*, Chamara Sandeepa*, Shen Wang *, Madhusanka Liyanage *,
Cem Ayyildiz†, Veli Can Yildirim†, Hakan Alakoca‡, Fatma Güneş Kesik‡ Betül Güvenç Paltun‡,
Giovanni Perin§, Michele Rossi§, Stefano Tomasin§, Arsenia Chorti¶, Pietro G. Giardina‖,
Alberto García Pérez**, José María Jorquera Valero **, Tommy Svensson††, Nikolaos Pappas‡‡, Marios Kountouris[x]
*University College Dublin, Ireland †GOHM, Muğla, Turkey ‡Ericsson Research, Turkey
§ University of Padova, Italy¶ENSEA, CNRS, France, ‖Nextworks, Italy **University of Murcia, Spain
††Chalmers University of Technology, Sweden ‡‡Linköping University, Sweden [x] EURECOM, France
Email: *bartlomiej.siniarski@ucd.ie , *abeysinghe.sandeepa@ucdconnect.ie, *{shen.wang,madhusanka}@ucd.ie,
†{ca,veli.yildirim}@gohm.com.tr, ‡{hakan.alakoca,gunes.kesik,betul.guvenc.paltun}@ericsson.com,
§ {giovanni.perin.1, michele.rossi, stefano.tomasin}@unipd.it ¶arsenia.chorti@ensea.fr, ‖p.giardina@nextworks.it,
**{alberto.garciap, josemaria.jorquera}@um.es ††tommy.svensson@chalmers.se,
‡‡nikolaos.pappas@liu.se, [x]marios.kountouris@eurecom.fr

***Abstract*—In the progressive development towards 6G, the ROBUST-6G initiative aims to provide fundamental contributions to developing data-driven, AI/ML-based security solutions to meet the new concerns posed by the dynamic nature of forthcoming 6G services and networks in the future cyber-physical continuum. This aim has to be accompanied by the transversal objective of protecting AI/ML systems from security attacks and ensuring the privacy of individuals whose data are used in AI-empowered systems. ROBUST-6G will essentially investigate the security and robustness of distributed intelligence, enhancing privacy and providing transparency by leveraging explainable AI/ML (XAI). Another objective of ROBUST-6G is to promote green and sustainable AI/ML methodologies to achieve energy efficiency in 6G network design. The vision of ROBUST-6G is to optimize the computation requirements and minimize the consumed energy while providing the necessary performance for AI/ML-driven security functionalities; this will enable sustainable solutions across society while suppressing any adverse effects. This paper aims to initiate the discussion and to highlight the key goals and milestones of ROBUST-6G, which are important for investigation towards a trustworthy and secure vision for future 6G networks.**

I. Introduction

Sixth Generation (6G) networks will play a prominent role in developing civilization toward the 2030s as the convergence between digital and physical worlds becomes a reality. Specifically, recent trends, such as network densification, high rates, and massive antennas, are expected to be further enhanced and coupled with new services, generating a real digital revolution [1]–[3], and enabling challenging applications including holographic telepresence, immersive communications, and physical sensing via radio waves, to name a few. Pervasive in-network Artificial Intelligence (AI) and Machine Learning (ML) will be instrumental in offering such new functionalities via network edge processing and optimizing 6G network functions via data-driven approaches.

This paper presents ROBUST-6G, a project funded by the European Union (EU) through the HORIZON SNS-JU 2023 initiative. Its primary purpose is to develop a holistic end-to-end 6G security architecture with inherent AI functionalities for heterogeneous network environments. Specifically, the project aims (i) to develop methodologies ensuring that AI-driven security functionalities are robust, energy efficient, explainable, effective (in terms of performance), and privacy-preserving; (ii) to design and implement zero-touch automation, security, and resource management for trusted and certified services among multiple stakeholders in distributed dynamic scenarios; (iii) to develop AI/ML-enabled techniques to detect and mitigate physical layer attacks on networks and user devices, and to propose novel physical layer security for demanding scenarios (requiring low latency, low energy consumption, and low complexity), using 6G radio technologies.

Within the same call, the EU also funded SAFE-6G, a project leveraging AI techniques to coordinate user-centric safety, security, privacy, resilience, and reliability functions of 6G networks, with a specific focus on the (far) edge. Related to ROBUST-6G, in the recent past, the EU projects RIGOUROUS and HEXA-X-II were funded. The latter is the European flagship project targeting 6G networks and services in a holistic way, expanding from research to system analysis and early validation/proof of concept. RIGOUROUS instead identifies and addresses the major cybersecurity, trust, and privacy risks related to 6G and ML-centric edge computing infrastructures. Similarly, ROBUST-6G is devoted to designing and developing secure, sustainable, and trustworthy 6G services through the use of AI/ML. Compared to them, it is focused on the security and energy sustainability of a fully automated smart network, aligned with the Zero-touch network and Service Management (ZSM) architecture and solutions, and encompassing physical layer security.

II. ROBUST-6G ARCHITECTURE

ROBUST-6G, as a cutting-edge 6G-oriented project, paves the path of forthcoming telecommunication networks, ensuring security and privacy-preserving. In this vein, those features are its cornerstones to define a high-level architecture that covers a broad spectrum of requirements in a heterogeneous and multi-stakeholder environment foreseen for 6G, as the one illustrated in Figure 1. Such high-level architecture has a dual mission since it enables consumers, such as verticals, to maintain their secure expectations aligned with their business requirements, and telecommunication companies, such as Communication Service Providers (CSP), to provide network services for advanced wireless connectivity to different verticals, as well as the architecture needed to communicate. In order to facilitate the communication between verticals and CSP, ROBUST-6G envisions creating a framework called Unified Exposure Framework aligned with CAMARA principles [4], which exposes security and management services to the different service providers with a certain level of abstraction.

With the accelerated digitization in verticals, the 5G/6G networks are expected to provide new value-added services ever-present with extreme connectivity in sectors such as manufacturing and automation. In addition, CSPs are also expected to provide network capabilities with innovative services that enable business automation. Verticals can access services via the abstractions provided by our framework. The framework also provides APIs that can be used by the verticals' applications (proprietary or third parties), even for specific requirements. Depending on the network and requirement model, these applications may be deployed over a public or on-premises edge/cloud infrastructure.

Figure 2 represents the details of the internal functionality under the Unified Exposure Framework, generating the ROBUST-6G functional architecture. The Data Management Module oversees the collection of infrastructure, network, and service data, comprising Data Fabric for data processing and exposure, and Data Governance for defining access policies. It identifies assets to be protected and assesses associated risks, ensuring controlled and secure data access. To guarantee the fulfilment of the Trustworthy and Sustainable AI pillars [5], ROBUST-6G aims to safeguard the privacy, as well as ensure robustness, transparency, explainability, reliability, fairness, and sustainability of the AI, among others. It consists of (1) a distributed federated learning (FL) service, which performs incident detection/prediction/response, (2) Trustworthy and Sustainable AI-driven Security Functions to ensure trust in AI functionality, and (3) AI Life-Cycle Management to enable mechanisms such as training, scaling, and deployment.

Zero-Touch Security Management Module relies on closed loops to provide rapid responses to detected or expected incidents. The Data Management Module sends security information about infrastructure, networks, and services to the closed loops. Within these loops, Decision Agents are powered by the Trustworthy and Sustainable AI-driven Security Functions component described previously, but Decision Agents might request that the controlled solution be reconfigured. Each reconfiguration request has a priority in the queue of the Security Orchestrator that performs the activation by the Robust Control and Provisioning Engine (RCPE) and the actuators. The RCPE notifies all control loops that system reconfiguration is in progress, as it assumes the role of managing closed loops (coexistence of multiple closed loops). In addition, it allows external entities to interact with the loops. Actuators impose the reconfiguration of parameters and provide details on the completion of the procedure. Once all actuators involved in the ongoing reconfiguration are completed, all control loops are notified, and the new reconfiguration is saved in a historical database for possible rollbacks and stability according to the target KPIs. Finally, the Security Administration Console allows humans to know why AI agents made their decisions thanks to the XAI capability and enables them to intervene in decisions manually.

The Physical Layer Security Module detects and mitigates physical layer threats autonomously with local AI capabilities. Within this module, RAN equipment can make rapid decisions independently without interacting with the upper network layer. Life cycle management and updates of local AI functions are controlled by the Distributed AI-driven Security Module. Inferences from the physical layer security module are communicated to the Data Management Module via monitoring data. It also manages Radio frequency (RF) fingerprinting migration and predicts changes in low-power devices' communication security.

III. TRUSTWORTHY AND SUSTAINABLE AI/ML FOR 6G SECURITY

ROBUST-6G identifies several key areas where the trustworthiness and sustainability of AI are essential for 6G.

A. Privacy Preservation Techniques for Peer-To-Peer (P2P) Collaborative FL Platforms

FL is a decentralized machine learning approach enhancing privacy by training models locally on devices, avoiding the need to transmit personal data to a third party. Despite its advantages, FL faces privacy threats, including membership inference, property inference, and model inversion attacks, stemming from overfitting, model complexity, and lack of privacy-focused architectures. With the involvement of peers in a P2P environment, these threats are amplified due to enhanced communication and ease of entry. Therefore, ROBUST-6G aims to address them by developing privacy-preserving techniques.

B. Distributed Federated Learning (DFL) Intrusion Detection

DFL offers a decentralized approach to avoid single-point failures in FL systems, using P2P connections for model training and synchronization. However, such systems are susceptible to Byzantine attacks where malicious nodes compromise model accuracy. ROBUST-6G plans to implement DFL-based intrusion detection to identify and mitigate malicious activities, ensuring the robustness of collaborative model training.

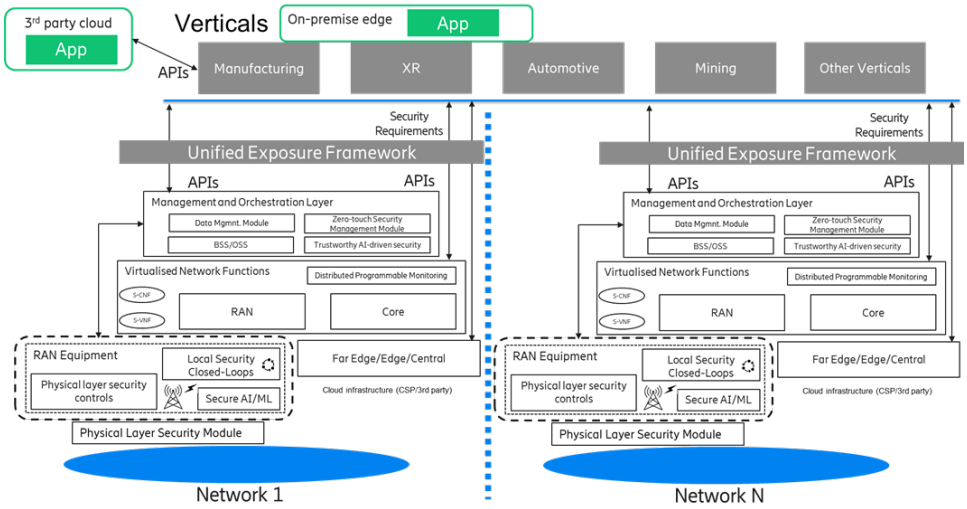


Fig. 1: ROBUST-6G High Level Architecture

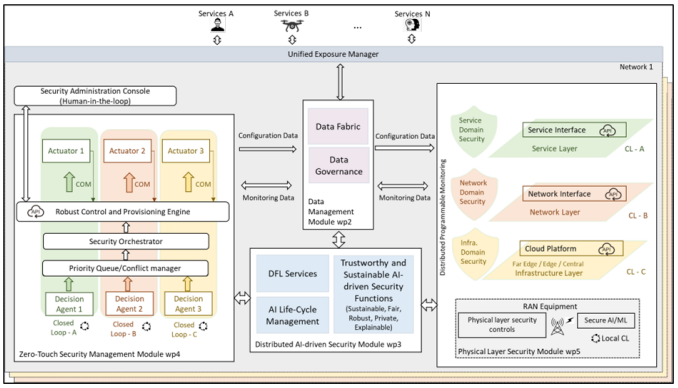


Fig. 2: Functional architecture of ROBUST-6G

C. Detection of Security Threats in FL Systems

Edge AI in 6G can face vulnerabilities to poisoning attacks that degrade model accuracy. These attacks can be data or model-based, with various strategies for execution. To counteract these, ROBUST-6G proposes using clustering, aggregation rules, reference datasets, and differential privacy, although these methods have limitations. The project will leverage Explainable AI (XAI) to enhance the detection of poisoning threats by interpreting influential instances in a privacy-preserving manner. This approach aims to improve the trustworthiness and security of FL in the ROBUST-6G.

D. Scalable and Sustainable AI

Recent research directions have focused on scalability and energy efficiency in FL, often separately and seldom incorporating security considerations. Energy-efficient learning over mesh networks, offering better scalability and security due to their topology, remains largely unexplored. ROBUST-6G aims to address the gaps by optimizing FL and decentralized learning for energy efficiency, scalability, and security, designing efficient client selection algorithms, and integrating efficient hardware and software. It will develop a distributed learning simulator to test model aggregation algorithms and evaluate them using key performance indicators (KPIs), with the best solutions implemented in a realistic testbed.

E. Adversarial ML

State-of-the-art AI-driven adversarial attack methods such as Fast Gradient Sign Method (FGSM), Projected Gradient Descent (PGD), and Universal Adversarial Perturbations (UAP), along with black-box approaches like Zeroth Order Optimization (ZOO), highlight the transferability and potential impact of adversarial data. To counteract these threats, defense mechanisms like adversarial training, input normalization, and adversarial regularization have been proposed. ROBUST-6G will focus on enhancing the robustness of ML models against such attacks using XAI to improve detection and defenses. This involves developing a controlled environment for simulating ZSM architecture, evaluating attacks and defenses through designated KPIs, and formulating comprehensive defenses.

F. Fair and explainable AI methodologies for threat detection and prediction

XAI supplements traditional threat detection by providing insights into model decision-making, also addressing security concerns, such as poisoning and evasion attacks. The project aims to utilize XAI for developing fair and understandable detection and prediction systems, focusing on centralized ML models. It seeks to overcome challenges like the instability of post-hoc XAI methods, the accuracy-explainability trade-off, and minimizing potential algorithmic biases, thus ensuring fair and explainable threat detection within the ZSM architecture.

G. Trustworthiness Evaluation Framework

Trustworthy AI, emphasizing fairness, explainability, robustness, and accountability, is crucial for reliable cyberattack detection. However, a unified framework to evaluate AI trustworthiness comprehensively, especially in fully distributed AI environments, is lacking. ROBUST-6G will develop a framework to assess ML/DL model trustworthiness in decentralized 6G networks, incorporating security, robustness, and fairness.

H. Closed loop automation: management and coordination

The concept of closed-loop automation, essential for ZSM, involves stages like observation, decision-making, and actuation. Managing multiple closed loops in complex 6G environments remains a challenge. The project targets the development of an advanced mechanism for Zero-Touch management of security workflows in 6G systems, leveraging AI/ML and trusted FL, as shown in Figure 3. It aims to orchestrate security functions effectively, ensuring optimal corrective actions in a multi-loop environment, supported by a programmable monitoring platform for pervasive data collection.

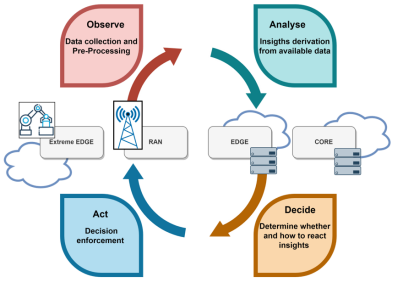


Fig. 3: Observe, Analyze, Decide, Act loop

IV. Zero-touch management for secure 6G

A. AI-driven predictive cybersecurity algorithms

Predictive cybersecurity uses advanced technologies like machine learning, AI, and behavioral analytics to foresee and prevent cyber-attacks. While not being applied in the evolution of 5G, it holds promise for the upcoming 6G era by offering capabilities for threat detection and risk assessment. Emerging technologies such as deep learning, reinforcement learning, and graph-based anomaly detection are enhancing its effectiveness. Despite its strengths in scalability, efficiency, and adaptability, predictive cybersecurity faces challenges like data quality dependency, the potential for false positives, and algorithmic bias. To strike a balance, in ROBUST-6G, we propose a new methodology to design new AI-driven algorithmic models that will combine advanced processes like data analytics, machine learning, and domain expertise to enable predictive cybersecurity decision-making, considering support to multi-tenancy environments. Particularly, our algorithms are structured according to the ETSI ZSM standard reference architecture for zero-touch management and closed-loop automation and will integrate seven main cross-correlated processes, i.e., data collection, data pre-processing, feature selection, model selection, data analytics, model training and evaluation, and intelligence services of both management and end-to-end service management domains.

B. AI/ML-driven security orchestration

ROBUST-6G will provide an orchestration service at the E2E and at the domain level in ZSM specific to security. This Security Orchestrator (SO) oversees the different security enablers to enforce the security requirements, formalized in Security Service Level Agreements (SSLAs) and the security policies and drives the security management by interacting with the control plane, the orchestration and management plane, and security management services. SSLAs and Policy Management are intended to introduce the business and security requirements as established by humans into a fully automated environment, therefore driving the behavior of the system. SSLAs establish a contract between operators to ensure a certain level of security that subjugates the system. Furthermore, Security Policies provide the abstraction and the formalism to enforce such SSLAs or other security restrictions generated either via AI techniques or by human imposition. The security orchestration process will be fed with the evolving system model, which is derived from the structural information coming from the network administrators, the monitors that inspect the deployment for any changes, the trust indicators, as well as the insights and evolved plans inferred by the AI-based Decision Engine.

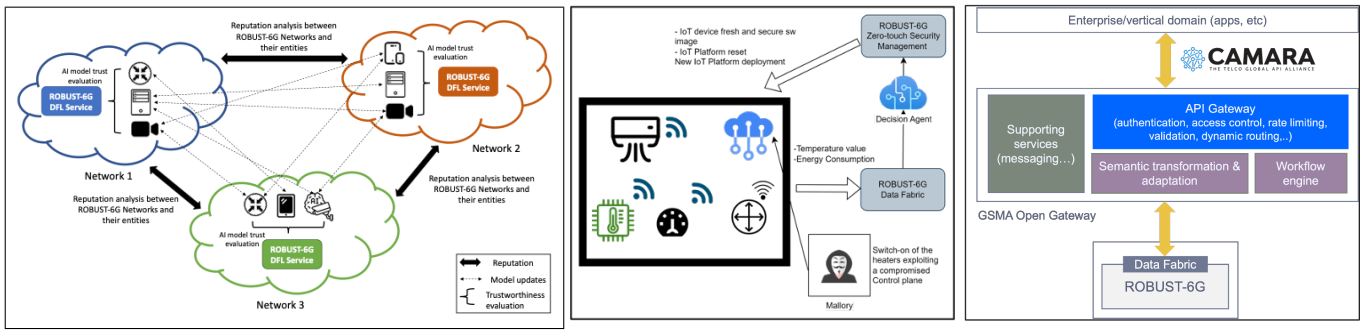
V. AI/ML enabled physical layer security

While we have witnessed important improvements in 5G security protocols compared to LTE, there remain key unresolved issues, in particular with respect to latency/power-constrained devices and massive connectivity regimes. Reconsidering the design of security protocols bottom up, starting at the physical layer, is not only feasible in 6G but also serves as an effective approach to addressing security challenges in emerging applications such as massive machine type communications (mMTC), ultra-reliable low latency communications (URLLC), and autonomous cyberphysical systems. The proposed roadmap in ROBUST-6G to incorporate PLS into future wireless security protocols builds on recent advances regarding AI/ML pre-processing to facilitate channel engineering and extrapolate channel features pertinent to PLS. Principal key elements of 6G radio environment for the secure communications is illustrated in Figure 5

A. AI/ML fingerprint-driven detection and mitigation of physical layer attacks for trustworthy and resilient 6G radio

As the next generation of communication environments becomes more heterogeneous, dynamic, and susceptible to a variety of security threats, addressing security concerns is crucial in ensuring the resilience of 6G networks [6], [7]. Detection, identification, and mitigation are key security challenges, such as network entry attacks, authentication attacks, and jamming attacks. Addressing related threats utilizing ML techniques at the physical layer, is a promising approach [8].

ROBUST-6G involves developing ML-based solutions for detecting and classifying attacks, including jamming and synchronization attacks on distributed Multiple-Input Multiple-Output (dMIMO), e.g., RF fingerprinting to classify attackers and device authentication. Edge AI and localized processing also aid in rapid decision-making for low-power devices, thereby reducing the reliance on frequent communication over the network. The PLS module of the ROBUST-6G security architecture can provide the orchestrator with comprehensive



(a) Use case 1 (b) Use case 2 (c) Use case 3

Fig. 4: Overview of the use cases and their key workflows and interactions among multiple components

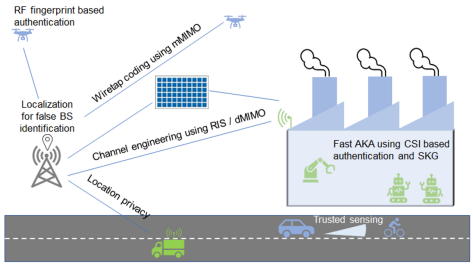


Fig. 5: Trustworthiness of the 6G radio environments and physical layer security applications

insights across network layers via a comprehensive trust evaluation via trustworthy AI, anomaly and threat detection.

B. Enhancing 6G radio trust and resilience with PLS

Several challenges lie within developing security controls for 6G radio, considering heterogeneous network topologies, stringent latency requirements, minimal footprint, and quantum-resistance [7]. As currently post-quantum cryptographic algorithms are complex for low-end IoT devices, PLS can close the gap [9], with respect to confidentiality and authentication [10]. As part of ROBUST-6G, pencil-sharp beamforming is employed in ultra-massive MIMO systems, particularly in the mmWave and THz bands as a practical setting for wiretap coding. Furthermore, dMIMO and Reconfigurable Intelligent Surfaces (RIS)-enabled channel engineering in the backhaul and fronthaul are considered. Secrecy maps are developed using worst-case estimators, such as conditional min-entropy leakage estimation. Furthermore, we explore new approaches for determining adversarial nodes, including false base stations, based on location/RF fingerprinting.

C. Privacy, sensing integrity, and PHY anomaly detection 6G

The trustworthiness of the 6G radio access network is enhanced through novel sensing capabilities, encompassing high-precision positioning and radar ranging. Positioning information is used as a second soft authentication factor in semantic and context-enabled PLS [8]. As recent protocols use the angle of arrival (AoA) as a feature to counter Sybil cyberattacks [11], positioning integrity (such as AoA) and multi-sensor fusion across a variety of modalities is explored. There are still challenges associated with learning robust and generalizable ML/DL models for 6G positioning and the goal of our project is to develop resilient and adaptable ML/DL models to bridge this gap. 6G positioning privacy has also become a big concern, prompting a wide range of approaches, including k-anonymity, cryptography-based mechanisms, and positioning obfuscation. We explore new obfuscation techniques, such as reinforcement learning, and explore positioning privacy at the signal level by examining channel charting. Ultimately, we aim for the development of a PHY anomaly detector integrating sensing, RF fingerprinting, and positioning capabilities.

VI. Implementation

This section elaborates on the implementation framework for the ROBUST-6G project, illustrating the interplay between orchestrated use cases and the dedicated testbeds.

1) Use case 1: AI Model Trustworthiness Evaluation in 6G Distributed Scenarios

This use case, presented in Figure 4a, focuses on evaluating the trustworthiness of decentralized ML/DL models, examining aspects such as model robustness, sustainability, explainability, fairness, security in communications, and infrastructure trustworthiness, including physical and sensing layers. Mitigation strategies against potential attacks using Physical Layer Security (PLS) are also considered.

Scenario 1: Decentralized Federated Learning

Aims to design a decentralized federated learning framework suitable for 6G's distributed networks, moving away from centralized approaches. This framework assesses AI model trustworthiness across essential trust pillars (e.g., accountability, fairness) and federated learning aspects like privacy. It also explores enhancing local model performance by evaluating updates based on the sending entity's reputation.

Scenario 2: Physical and Sensing Layer Trust Introduces trustworthiness measures from the infrastructure, focusing on the physical and sensing layers' integrity, security, and resilience. It considers probabilistic trust measures, leveraging data from onboard sensors, RF signatures, and more, to ensure comprehensive security across layers.

2) Use case 2: Automatic Threat Detection and Mitigation in 6G-Enabled IoT Environments

This use case explores complex scenarios in 6G's extreme edge IoT environments, leveraging the ROBUST-6G platform

TABLE I: Key Performance Values and Indicators for the ROBUST-6G Project

Category	KVI Name	Description
Scientific and Technological	Publication and Dissemination Index	Number of open-access publications, datasets, posters, talks, and academic theses to evaluate the project's scientific outreach.
	Framework Adoption Rate	Adoption of the European consensus framework for 6G by international bodies.
	AI Acceptance Level	Integration of AI concepts across various platforms and services.
	Ethical Compliance Rate	Alignment with GDPR and other European ethical standards.
Economic and Societal	Digital Service Adoption	Uptake of digital services enabled by the project, reflecting improvements in accessibility, affordability, and availability.
	Business Integration Index	Involvement of new actors and formation of strategic alliances in the B2B and B2C sectors.
	Job Creation and Growth Rate	Creation of high-quality jobs and growth of the ICT sector as a result of the project.
	Skills Development Rate	Number of MS and PhD graduates trained in 6G technologies for workforce development.
ROBUST-6G Specific	Security Solution Deployment Rate	Frequency and scope of implementing new security enablers developed within ROBUST-6G into marketable products.
	Standardization Influence	Impact on 6G standardization efforts, especially the development of 6G KPIs within key documents like the ITU IMT 2030 vision document.
High Societal Impact	Emergency Response Confidence Level	Trust in digital systems for critical missions to evaluate the project's contribution to secure and trustworthy emergency systems.
	Healthcare Cost Savings and Trust	Savings per patient and trust levels in autonomous e-health components.
	Cobot Integration Efficiency	Reduction in travel/commuting time and improvements in rural job market accessibility due to autonomous cobots.
	Agricultural Productivity Gains	Time savings in agricultural activities through federated learning and AI threat detection.

for Zero-touch Security management, Data Fabric, and AI/ML for threat detection, decision-making, and mitigation.

Scenario 1: Economic Harm via Device Violation

Targets unauthorized control of IoT devices, like HVAC systems, for economic damage. AI decision agents analyze IoT data to detect anomalies, distinguishing between cyberattacks and system failures, leading to corrective actions like software updates or blacklisting attacker IPs. Overview of this scenario is presented in Figure 4b.

Scenario 2: Cryptojacking Attack on IoT Devices

Involves attackers hijacking smart devices for cryptocurrency mining. Monitoring data allows detecting anomalies in resource usage and data transmissions, leading to mitigation actions such as deploying secure software versions.

Scenario 3: Economic Harm in Smart Agriculture

Focuses on attacks against smart agriculture, where sensor tampering causes incorrect actuator responses. AI agents compare sensor data with external sources to identify anomalies, employing RF fingerprint changes prediction and enforcing corrective measures for integrity.

3) Use case 3: Security Capability Exposure via NetSecaaS

This use case focuses on leveraging the GSMA Open Gateway framework, integrating ROBUST-6G's AI/ML-driven security (NetSecaaS) for easy application by developers and enterprises. This use case demonstrates extending Open Gateway with security APIs, supported by ROBUST-6G's Data Fabric, to offer secure, on-demand network capabilities. Figure 4c shows the components operated with the gateway.

A. Key values and performance indicators

The ROBUST-6G project is designed to exert a transformative impact on the scientific, technological, economic, and societal landscapes, transcending the anticipated outcomes of the SNS Work Programme 2023-2024 and contributing significantly to the EU's Sustainable Development Goals (SDGs). The project's implications are underpinned by rigorous Key Values and Performance Indicators (KVIs), which embody the core objectives of enhancing trust, security, and robustness in 6G networks. The KVIs are presented in Table I.

VII. Conclusion

The main ambition of the ROBUST-6G project is to develop a robust security platform for AI-driven autonomous adaptations of 6G, with secure, privacy-preserving, reliable, resilient, accountable, trustworthy, and sustainable capabilities. Zero-touch integrated security management in multi-tenant distributed AI deployments across 6G networks is the intrinsic approach for enabling this ambition in a pragmatic context, as the expected automation at the process level demands automation at the deemed security solutions. Evidently, all the specified features should be researched extensively to forecast their impact on the 6G security landscape and to achieve a holistic autonomous system that can serve the heterogeneity envisaged in 6G within a closed-loop context. ROBUST-6G project's systematic validation methodology, with use cases, evaluation framework and testing, highlights a forward-thinking approach to developing secure, trustworthy, and sustainable AI/ML for the 6G era.

Acknowledgement

This work has been funded by the European Commission through the Horizon Europe JU SNS project ROBUST-6G (Grant Agreement no. 101139068) and supported by TUBITAK through the 1515 Program under Project 5169902.

References

[1] W. Saad, M. Bennis, and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, 2020.

[2] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nature Electronics*, vol. 3, no. 1, pp. 20–29, 2020.

[3] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G Networks: Use Cases and Technologies," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 55–61, 2020.

[4] J. Ordonez-Lucena and F. Dsouza, "Pathways towards network-as-a-service: the camara project," in *Proceedings of the ACM SIGCOMM Workshop on Network-Application Integration*, 2022, pp. 53–59.

[5] H. Liu, Y. Wang, W. Fan, X. Liu, Y. Li, S. Jain *et al.*, "Trustworthy AI: A Computational Perspective," *ACM Trans. Intell. Syst. Technol.*, 2022.

[6] S. F. Zamanian, M. H. Kahaei, S. M. Razavizadeh, and T. Svensson, "Attacking massive mimo cognitive radio networks by optimized jamming," *IEEE Open Journal of the Communications Society*, 2021.

[7] M. Mitev, A. Chorti, H. V. Poor, and G. Fettweis, "What physical layer security can do for 6g security," *IEEE Open Journal of Vehicular Technology*, 2023.

[8] A. Chorti, A. N. Barreto, S. Köpsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6g wireless: The role of physical layer security," *IEEE Communications Standards Magazine*, vol. 6, no. 1, pp. 102–108, 2022.

[9] M. Mitev, T. M. Pham, A. Chorti, A. N. Barreto, and G. Fettweis, "Physical layer security-from theory to practice," *IEEE BITS the Information Theory Magazine*, 2023.

[10] M. Srinivasan, S. Skaperas, M. S. Herfeh, and A. Chorti, "Joint localization-based node authentication and secret key generation," in *ICC International Conference on Communications*. IEEE, 2022.

[11] S. Gil, S. Kumar, M. Mazumder, D. Katabi, and D. Rus, "Guaranteeing spoof-resilient multi-robot networks," *Autonomous Robots*, 2017.