ROBUST-6G

NEWSLETTER DECEMBER 2025

Welcome to the newsletter of ROBUST-6G!

ROBUST-6G is a European research project (HORIZON-JU-SNS-2023-STREAM-B-01-04) that pioneers the development of data-driven, AI/ML-based security solutions, addressing the evolving challenges presented by the dynamic landscape of forthcoming 6G services and networks within the future cyber-physical continuum.

Our mission encompasses not only advancing security measures but also safeguarding the integrity of AI/ML systems from potential security breaches and upholding the privacy rights of individuals whose data fuels these systems. ROBUST-6G initiative extends to the promotion of green and sustainable AI/ML methodologies, aiming to optimize energy efficiency in 6G network design.

Enjoy reading!

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

6GSNS

Co-funded by the European Union

ROBUST 6G 6th Plenary Meeting in Athens

The 6th Plenary Meeting of the ROBUST-6G project was successfully held in Athens, Greece, bringing project partners together as the project moves into its final phase. The meeting highlighted the strong progress made across the consortium, with the overall architecture, integration activities, and demonstration plan clearly taking shape.

Discussions focused on the final alignment of use cases and demonstration scenarios, the definition of a validation and evaluation strategy with measurable outcomes, and cross–work package integration toward the project's final deliverables. These exchanges confirmed that ROBUST-6G is progressing in a coordinated manner and remains on track to achieve its technical objectives and targeted TRL levels.

We would like to thank our host, the AXON team, for their warm hospitality and excellent organization. The meeting once again demonstrated the strength of collaboration within the ROBUST-6G consortium as we work toward resilient, secure, and intelligent 6G networks.

ROBUST-6G Coordination Update

In September, Dr. Ramin Fuladi was appointed as the Project Coordinator of the ROBUST-6G project ensuring continuity in project coordination and close alignment across work packages and partners.

SNS Steering Board Meeting in Madrid

As the coordinator of the ROBUST-6G project, Dr. Ramin Fuladi represented the consortium at the SNS Steering Board meeting held on 15 October at Telefónica headquarters in Madrid.

The meeting provided a valuable platform to exchange updates on the progress of other SNS projects and to engage with fellow project coordinators on cross-project collaboration, overall advancements, and future directions within the SNS framework. This participation reflects Ericsson Research's active role in shaping the strategic coordination and evolution of Europe's 6G research ecosystem.

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

6GSNS

Co-funded by the European Union

ROBUST-6G Deliverable D5.2 is Out!

The ROBUST-6G project has released Deliverable D5.2, which provides a consolidated framework for the implementation and evaluation of the project's key solutions.

This deliverable builds on earlier design and validation work, translating project concepts into structured implementation and assessment activities. It outlines how the developed solutions will be applied, tested, and evaluated in line with the project objectives, ensuring consistency across work packages and partners.

D5.2 plays a key role in supporting the systematic execution of upcoming activities, contributing to a coherent and well-aligned approach as the project progresses toward its later phases.

🔗 The full deliverable is available on the ROBUST-6G website.

ROBUST-6G Deliverables

Deliv. #	Deliverable Name
D2.1	6G Threat Analysis Report
D2.2	Use Cases, Requirements, ROBUST-6G Initial Architecture and Initial ROBUST-6G Dataspace
D3.1	Threat Assessment and Prevention Report
D3.2	Initial Report on ROBUST-6G Trustworthy and Sustainable AI Architecture and Requirements for Integrating Selected XAI Measures
D4.1	Security Automation for 6G
D5.1	Library of Known PHY Attacks and PLS Dataset
D5.2	Report on the use of PLS in 6G
D6.1	Use Case Validation Plan and Testbed Design

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

6GSNS

Co-funded by the European Union

ROBUST-6G Publications

Title	Authors
Secret Key Generation Rates for Line of Sight Multipath Channels in the Prescence of Eavesdroppers	Amitha Mayya, Arsenia Chorti, Rafael F. Schaefer, Gerhard P. Fettweis
Divergence-minimizing Attack Against Challenge-response Authentication with IRSs	L. Crosara, A. V. Guglielmi, N. Laurenti, and S. Tomasin
Physical-layer Challenge-response Authentication with IRS and Single-antenna Devices	A. V. Guglielmi, L. Crosara, S. Tomasin, and N. Laurenti
Energy-Based Optimization of Physical-Layer Challenge-Response Authentication with Drones	Francesco Ardizzon, Damiano Salvaterra, Mattia Piana, and Stefano Tomasin
One-Class Classification and the GLRT for Jamming Detection in Private 5G Networks	Matteo Varotto, Stefan Valentin, Francesco Ardizzon, Samuele Marzotto, and Stefano Tomasin
A Latent Space Metric for Enhancing Prediction Confidence in Earth Observation Data	I. Pitsiorlas, A. Tsantalidou, G. Arvanitakis, M. Kountouris, Ch. Kontoes
Decentralized LLM Inference over Edge Networks with Energy Harvesting	Aria Khoshsirat, Giovanni Perin, Michele Rossi
Semantics-Aware Active Fault Detection in Status Updating Systems	G. Stamatakis, N. Pappas, A. Fragkiadakis, N. Petroulakis and A. Traganitis
Version Age-based Client Scheduling Policy for Federating Learning	X. Hu, N. Pappas, H. Yang
Secure Status Updates under Eavesdropping: Age of Information-Based Secrecy Metrics	Q. Wang, H. Chen, P. Mohapatra, N. Pappas
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 Gunes Kesik, Betul Guvenc Paltun, Giovanni Perin, Michele Rossi, Stefano Tomasin, Arsenia Chorti, Pietro G. Giardina, Alberto Garcıa Perez, Jose Marıa Jorquera Valero, Tommy Svensson, Nikolaos Pappas, Marios Kountouris
Advancing Security for 6G Smart Networks and Services	Madhusanka Liyanage, Pawani Porambage, Engin Zeydan, Thulitha Senevirathna, Yushan Siriwardhana, Awaneesh Kumar Yadav, Bartlomiej Siniarski
Explainable AI for 6G Use Cases: Technical Aspects and Research Challenges	Shen Wang, M. Atif Qureshi, Luis Miralles-Pechuan, Thien Huynh-The, Thippa Reddy Gadekallu, Madhusanka Liyanage
SHERPA: Explainable Robust Algorithms for Privacy-Preserved Federated Learning in Future Networks to Defend Against Data Poisoning Attacks	Chamara Sandeepa, Bartlomiej Siniarski, Shen Wang, Madhusanka Liyanage
A Novel Method to Mitigate Adversarial Attacks Against AI-as-a-Service Functionality	Ömer Faruk Tuna, Leyli Karaçay, Utku Gülen

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

6GSNS

Co-funded by the European Union

ROBUST-6G Publications

Title	Authors
One-Class Classification as GLRT for Jamming Detection in Private 5G Networks	Matteo Varotto, Stefan Valentin, Francesco Ardizzon, Samuele Marzotto, and Stefano Tomasin
Analysis of Challenge-Response Authentication With Reconfigurable Intelligent Surfaces	Stefano Tomasin and Tarek N. M. Mohamed Elwakeel and Anna Valeria Guglielmi and Robin Maes and Nele Noels and Marc Moeneclaey
Securing Networks of the Future: A Programmable Security Monitoring Platform for Cloud Continuum	José María Jorquera Valero and Alberto García Pérez; Gunes Kesik; Ömer Faruk Tuna; Pietro Giardina and Enrico Alberti; Lucía Cabanillas Rodríguez; Ignacio Dominguez; Diego Lopez; Dhouha Ayed; Manuel Gil Pérez and Gregorio Martinez Perez
VREM-FL: mobility-aware computation-scheduling co-design for vehicular federated learning	Luca Ballotta, Nicolò Dal Fabbro, Giovanni Perin, Luca Schenato, Michele Rossi, Giuseppe Piro
Generalized Multi-Layer ML-IDS for Smart Buildings	Marco Ruta, Pietro Giuseppe Giardiana, Giada Lendi, Rosario Garroppo
Trustworthy Intrusion Detection: Confidence Estimation Using Latent Space	I. Pitsiorlas, G. Arvanitakis, M. Kountouris
Blocked Job Offloading Based Computing Resources Sharing in LEO Satellite Networks	Pei Peng, Tianheng Xu, Xianfu Chen, Charilaos C. Zarakovitis, Celimuge Wu
Impact of Residual Hardware Impairments on RIS-aided Authentication	Bilal Çiçek, Hakan Alakoca
Physical Layer Authentication Using Information Reconciliation	Atsu Kokuvi Angélo Passah, Rodrigo C. de Lamare, and Arsenia Chorti
Detecting 5G Signal Jammers Using Spectrograms with Supervised and Unsupervised Learning	Matteo Varotto, Stefan Valentin, and Stefano Tomasin
Minimizing the Age of Missed and False Alarms in Remote Estimation of Markov Sources	Jiping Luo and Nikolaos Pappas
A Survey on XAI for 5G and Beyond Security: Technical Aspects, Challenges and Research Directions	Thulitha Senevirathna, Vinh Hoa La, Samuel Marchal, Bartlomiej Siniarski, Madhusanka Liyanage, Shen Wang
A Framework for Global Trust and Reputation Management in 6G Networks	Bac Trinh-Nguyen, Sara Berri, Sin G. Teo, Tram Truong-Huu, Arsenia Chorti
Enhanced Multiuser CSI-based Physical Layer Authentication Based on Information Reconciliation	Passah, Atsu Kokuvi Angélo; Chorti, Arsenia; de Lamare, Rodrigo
ProFe: Communication-Efficient Decentralized Federated Learning via Distillation and Prototypes	Pedro Miguel Sanchez Sanchez, Enrique Tomas Martinez Beltran, Miguel Fernandez Llamas, Gerome Bovet, Gregorio Martinez Perez, Alberto Huertas Celdran
HyperDtct: Hypervisor-based Ransomware Detection using System Calls	Jan von der Assen, Alberto Huertas Celdran, Jan Marc Luthi, Jose Maria Jorquera Valero, Francisco Enguix, Gerome Bovet, Burkhard Stiller

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

6GSNS

Co-funded by the European Union

ROBUST-6G Publications

Title	Authors
S-VOTE: Similarity-based Voting for Client Selection in Decentralized Federated Learning	Enrique Tomás, Alberto Huertas Celdrán, Gregorio Martínez Pérez
DRACO: Decentralized Asynchronous Federated Learning over Row-Stochastic Wireless Networks	Eunjeong Jeong, Marios Kountouris
Leveraging Angle of Arrival Estimation against Impersonation Attacks in Physical Layer Authentication	T. M. Pham, L. Senigagliesi, M. Baldi, R. F. Schaefer, G. P. Fettweis, and A. Chorti
High-accuracy AoA-based Localization using Hierarchical ML Classifiers in Outdoor Environments	B. Trinh-Nguyen, S. Berri, S. G. Teo, T. Truong-Huu, and A. Chorti
Multi-Strategy Optimization Approach for Location Privacy and Latency Trade-Offs in 6G Networks	M. Sharara and S. Berri
From Insight to Action: XAI-Enhanced Detection of DDoS Attacks in Software Defined Networks	Thulitha Senevirathna, Betül Güvenç Paltun, Ramin Fuladi, Shen Wang, Madhusanka Liyanage
Robust Intrusion Detection System with Explainable Artificial Intelligence	Betül Güvenç Paltun, Ramin Fuladi, Rim El Malki

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

6GSNS

Co-funded by the European Union