ROBUST-6G

NEWSLETTER APRIL 2026

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

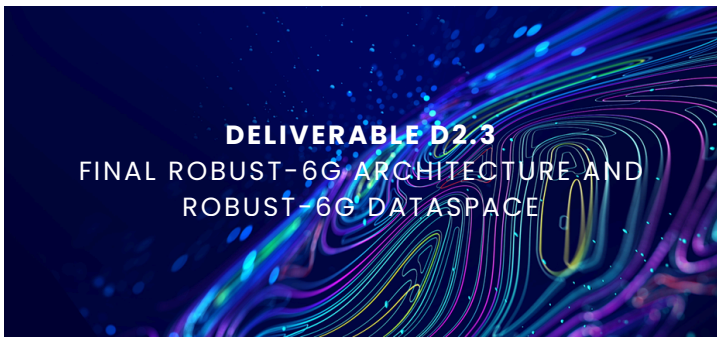
ROBUST-6G Deliverable D2.3 is Out!

The ROBUST-6G project has released Deliverable D2.3, focusing on the project's final end-to-end security architecture for future 6G systems, integrating programmable pervasive monitoring, secure data management, trustworthy AI services, zero-touch security orchestration, and physical-layer protection into a unified framework.

The architecture emphasizes autonomous, AI-native security management — supporting explainable AI, federated learning, adversarial robustness, and automated closed-loop threat mitigation in real time.

This work marks a significant step toward smart, automated, and reliable security services for next-generation 6G networks.

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



ROBUST-6G Deliverable D5.3 is Out!

The ROBUST-6G project has released Deliverable D5.3, introducing nine open Physical Layer Security Challenges designed to engage the research community in testing security techniques under realistic 6G conditions.

Each challenge provides a publicly available dataset, a clear problem definition, and measurable evaluation criteria — covering topics such as RF fingerprinting, secret key generation, physical layer authentication, and device classification under hardware impairments.

Following the established practice in cryptography of issuing public challenges to stress-test security schemes, D5.3 brings this approach to the physical layer security community, inviting researchers to tackle adversarial scenarios and submit their solutions.

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

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

Physical Layer Security Challenges Are Now Live!

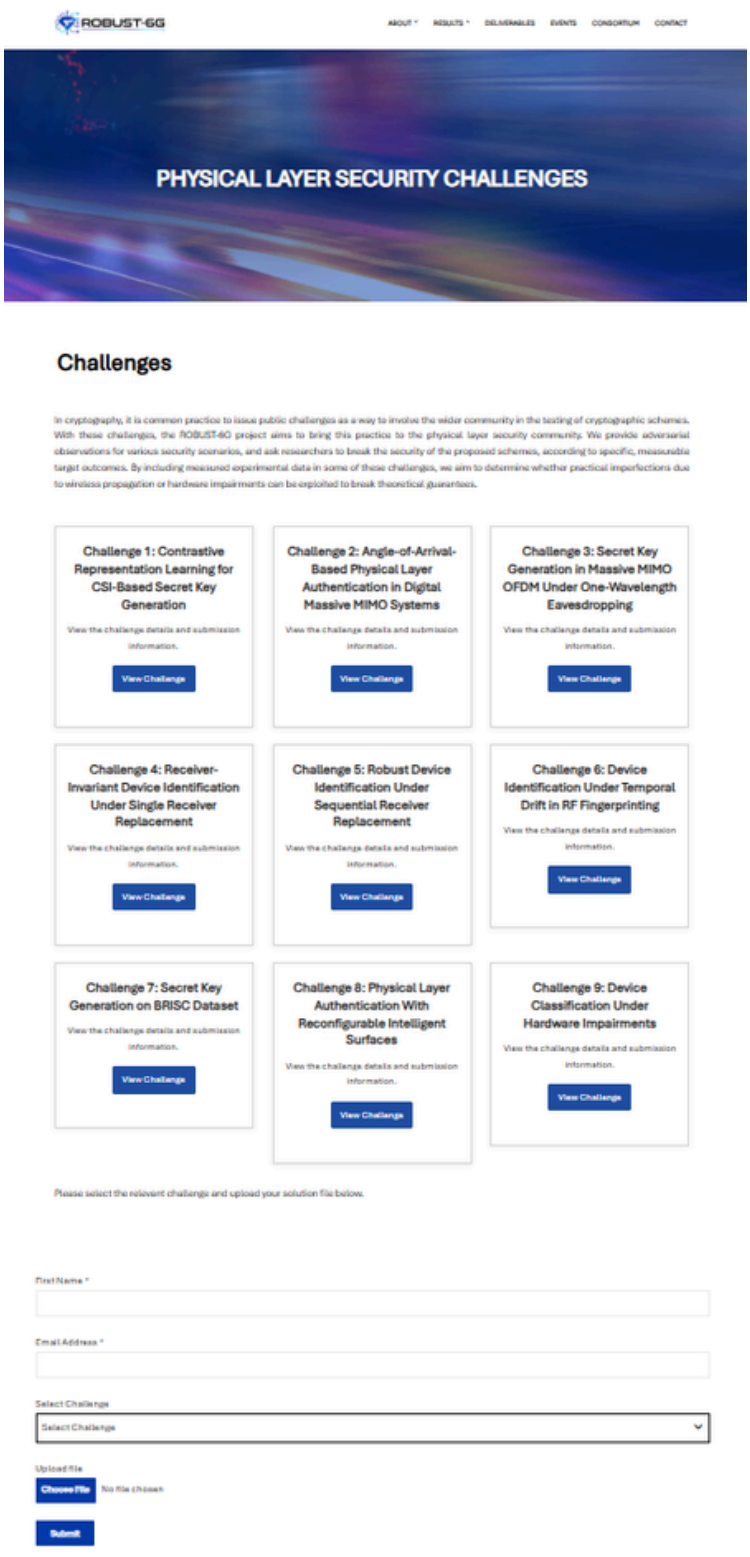
The ROBUST-6G project has officially launched nine open Physical Layer Security Challenges, inviting the research community to push the boundaries of 6G security research.

As part of Deliverable D5.3, these challenges are designed to test physical layer security techniques under realistic conditions. Following the established practice in cryptography of issuing public challenges to stress-test security schemes, ROBUST-6G brings this approach to the physical layer security community — providing adversarial observations and asking researchers to break proposed schemes according to specific, measurable outcomes.

The challenges cover a wide range of topics, including RF fingerprinting under receiver replacement and temporal drift, secret key generation in massive MIMO and RIS-assisted systems, physical layer authentication with angle-of-arrival and RIS, and device classification under hardware impairments. Each challenge comes with a publicly available dataset, a clear problem definition, and measurable evaluation criteria.

Researchers and practitioners are invited to explore the challenges, download the datasets, and submit their solutions via the submission form on the challenges page.

👉 Explore all 9 challenges here!



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

Meet ROBUST-6G at EuCNC & 6G Summit 2026!

ROBUST-6G will participate in EuCNC & 6G Summit 2026, taking place from 2–5 June 2026 in Malaga, Spain, with its exhibition booth showcasing the project's latest innovations in AI-native, trustworthy, and autonomous 6G security.

Visitors will have the opportunity to explore ROBUST-6G's work on Zero-Touch Security Management, Physical Layer Security, Trustworthy AI Services, programmable monitoring, and secure 6G architectures through interactive demonstrations and technical discussions.

In addition, ROBUST-6G will organize a special session titled "ROBUST-6G: Advancing Security and Automation for Next-Generation 6G Networks" on Friday, 5 June 2026. The session will bring together experts from academia and industry to discuss trustworthy AI, zero-touch security automation, physical-layer security, data governance, and 6G standardization efforts.

Join us in Malaga to discover how ROBUST-6G is shaping secure and resilient next-generation networks.

See you at the ROBUST-6G booth!

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
D2.3	Final ROBUST-6G Architecture and 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
D3.4	Final Report on ROBUST-6G Trustworthy and Sustainable AI Architecture and Requirements for Integrating Selected XAI Measures
D4.1	Security Automation for 6G
D4.4	ROBUST-6G AI/ML Driven Zero-Touch Security Management Platform Final Prototype
D5.1	Library of Known PHY Attacks and PLS Dataset
D5.2	Report on the use of PLS in 6G
D5.3	Release of Physical Layer Security Challenges
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
Physical Layer Authentication Using Information Reconciliation	Atsu Kokuvi Angélo Passah, Rodrigo C. de Lamare, and Arsenia Chorti
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
Detecting 5G Signal Jammers Using Spectrograms with Supervised and Unsupervised Learning	Matteo Varotto, Stefan Valentin, 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
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
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
SHERPA: Explainable Robust Algorithms for Privacy-Preserved Federated Learning inFuture Networks to Defend Against Data Poisoning Attacks	Chamara Sandeepa, Bartlomiej Siniarski, Shen Wang, Madhusanka Liyanage

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
A Novel Method to Mitigate Adversarial Attacks Against AI-as-a-Service Functionality	Ömer Faruk Tuna, Leyli Karaçay, Utku Gülen
One-Class Classification as GLRT for Jamming Detection in Private 5G Networks	Matteo Varotto, Stefan Valentin, Francesco Ardizzon, Samuele Marzotto,Stefano Tomasin
Analysis of Challenge-Response Authentication With Reconfigurable Intelligent Surfaces	Stefano Tomasin, Tarek N. M. Mohamed Elwakeel, Anna Valeria Guglielmi,Robin Maes, Nele Noels, Marc Moeneclaey
Securing Networks of the Future: A Programmable Security Monitoring Platform for Cloud Continuum	José María Jorquera Valero, Alberto García Pérez, Gunes Kesik,Ömer Faruk Tuna, Pietro Giardina, Enrico Alberti,Lucía Cabanillas Rodríguez, Ignacio Dominguez,Diego Lopez, Dhouha Ayed, Manuel Gil Pérez, Gregorio Martinez Perez
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 Generalized Multi-Layer IDS for Smart Buildings	Marco Ruta; Pietro Giardina; Giada Landi; Rosario G. Garroppo
Impact of Residual Hardware Impairments on RIS-aided Authentication	Bilal Çiçek, Hakan Alakoca
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
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

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
Multi-Strategy Optimization Approach for Location Privacy and Latency Trade-Offs in 6G Networks	M. Sharara and S. Berri
A Comparative Study of DDoS Attack Detection in Traditional Networks and SDN Using Time and Frequency Domain Features	E. Aksoy, R. Fouladi, B. U. Töreyin
ADMM-Based Training for Spiking Neural Networks	G. Perin, C. Bidini, R. Mazzieri, and M. Rossi
Challenge-Response to Authenticate Drone Communications: A Game Theoretic Approach	M. Piana, F. Ardizzon, and S. Tomasin
Image-Based Frequency-Domain Analysis for Robust DDoS Detection in SDN	R. Fuladi and B. Çiçek
VREM-FL: Mobility-Aware Computation-Scheduling Co-Design for Vehicular Federated Learning	L. Ballotta , N. Dal Fabbro, G. Perin, L. Schenato, M. Rossi, G. Piro
Context-Aware Secret Key Generation Demonstrator based on Physical Layer Security	A. Mayya, Ya Richhariya, A. Khandan Boroujeni, S. Vorberg, M. Matthé and R. Vinz
NEBULA – Decentralized Federated Learning for Heterogeneous Networks	Enrique Tomás Martínez Beltrán, Gérôme Bovet, Gregorio Martínez Pérez, Alberto Huertas Celdrán
Enhancing Secret Key Generation in Low-Mobility Scenarios by Locally Generated Pilots	Thuy M. Pham, Arsenia Chorti, Gerhard P. Fettweis and Rafael F. Schaefer
Jamming Detection in Cell-Free MIMO with Dynamic Graphs	A. Hossary, L. Crosara, and S. Tomasin
From Insight to Action: XAI-Enhanced Detection of DDoS Attacks in Software Defined Networks	T. T. Senevirathna, B. Güvenç Paltun, R. Fouladi and S. Wang
Robust Intrusion Detection System with Explainable Artificial Intelligence	B. Güvenç Paltun, R. Fouladi and R. 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