ROBUST-6G

NEWSLETTER JULY 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 Featured at Cyber Ireland's AI & Cybersecurity Event

On March 12, 2025, the ROBUST-6G project was proudly presented at the Cybersecurity and AI in Software Development event hosted by Cyber Ireland. Representing University College Dublin and the Network Softwarization and Security Labs (NetsLab), Thulitha T. introduced our cutting-edge work on AI/ML-driven security solutions tailored for the next generation of 6G networks.

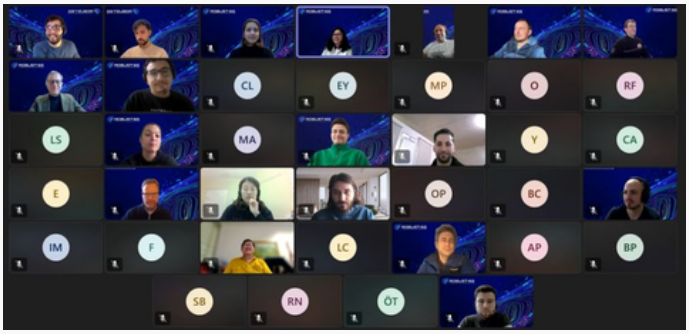
The event, jointly organized with UCD School of Computer Science and the Advance Centre for Digital Transformation, brought together experts to explore the transformative role of AI in enhancing security across the software development lifecycle.

Assoc. Prof. Madhusanka Liyanage, ROBUST-6G's Principal Investigator at UCD, also joined a thought-provoking panel discussion on AI Security and Privacy, alongside industry leaders including Liliana Pasquale, Fergus Harney, Ray Genoe, Adam D'Arcy, Fabio Cerullo, and Dr. Louise O'Hagan.

ROBUST-6G Holds 4th Plenary Meeting for the Upcoming Project Review

The 4th Plenary Meeting of the ROBUST-6G project was successfully held online, bringing together consortium partners to align on recent progress and prepare for the upcoming Project Review Meeting in March 2025.

Throughout the session, partners shared updates on key developments across all work packages, addressed ongoing technical challenges, and coordinated strategies to ensure a strong and cohesive review process. The meeting also served as a valuable touchpoint to reinforce collaboration and maintain momentum across the project's diverse activities.



RROBUST-6G Holds Successful First Project Review

On March 18, 2025, the first official review of the ROBUST-6G project took place as a full-day session, bringing together all consortium partners and esteemed external reviewers. The review was held under the coordination of Ericsson Research Türkiye.

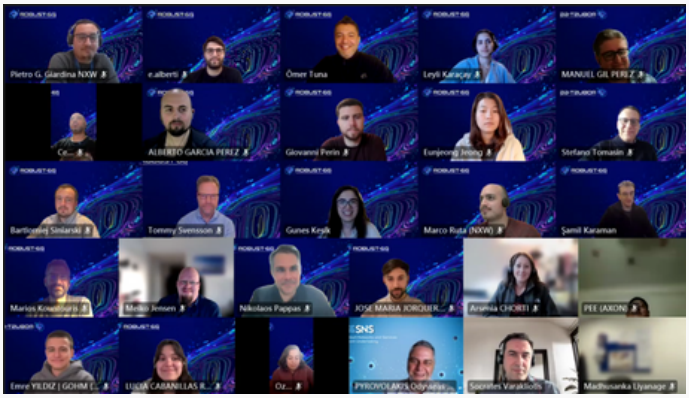
ROBUST - 6G project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101139068.

6GSNS

Co-funded by the European Union

The session highlighted the project's key achievements, ongoing technical progress, and upcoming milestones. The reviewers; Elisa Ruth Heymann Pignolo, Meiko Jensen, and Frank Fransen provided valuable feedback that will shape the project's next phase.

We sincerely thank all participants for their contributions and engagement as we continue building a secure and resilient 6G future.



ROBUST-6G Highlighted at WiOpt 2025 in Linköping

The ROBUST-6G project was recently featured at WiOpt 2025 – the 23rd International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks, held at Linköping University from May 26–29.

The project was represented through a poster presentation and through the contributions of Prof. Nikolaos Pappas, who served as General Chair of the organizing committee.

In addition, Dr. Eunjeong Jeong delivered an invited talk in the Workshop on Machine Learning in Wireless Communications, titled "Scalable and Robust Optimization for Decentralized Asynchronous Federated Learning Systems." Her talk, which acknowledged ROBUST-6G, explored how continuous timelines in autonomous client environments can enhance resilience while reducing communication and computational overhead.

We are proud to see ROBUST-6G shared with leading voices in the wireless research community, thanks to our partners at Linköping University.

ROBUST-6G Partners Contribute to the 3rd SECURENET Summit

On May 27, 2025, the 3rd SECURENET Summit was held at University College Dublin, bringing together leading academic and industry experts to explore the security and privacy challenges of future mobile networks.

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

The ROBUST-6G consortium was well represented, with active contributions from several partners across key research areas.

Topics included physical-layer security, zero-touch automation, explainable AI, and post-quantum cryptography—reflecting the core focus areas of the ROBUST-6G project and its commitment to building secure and trustworthy 6G systems.

We thank the organizers at University College Dublin and the CONNECT Centre, along with all participating colleagues, for facilitating a highly collaborative and insightful event.

ROBUST-6G 5th Plenary Meeting Hosted by University College Dublin

The 5th Plenary Meeting of the ROBUST-6G project was held face-to-face on May 28–29, 2025, at University College Dublin (UCD), bringing together consortium partners for a comprehensive two-day working session.

The meeting provided an in-depth opportunity to align on project progress and explore the collaborative work driving secure, intelligent, and trustworthy 6G systems. The agenda featured updates from all work packages, in-depth discussions on use case development and integration strategies, and planning for upcoming deliverables and review cycles.

Hosted by the UCD team, the event fostered rich dialogue and strengthened coordination across academic and industrial partners alike. Special thanks to the entire UCD team for their warm hospitality and seamless organization.

ROBUST-6G Showcased at EuCNC & 6G Summit 2025 in Poznań

The ROBUST-6G project was prominently featured at the EuCNC & 6G Summit 2025, held from June 3–6 in Poznań, Poland. Bringing together key stakeholders from across Europe's 6G research and innovation ecosystem, the event provided a valuable platform for visibility, collaboration, and exchange.

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

Throughout the summit, ROBUST-6G was showcased at a joint exhibition booth alongside the SNS iTrust6G project. The booth highlighted the project's advancements in AI/ML-based security and explainability, privacy-preserving mechanisms, and zero-touch security orchestration—core elements in the mission to build trustworthy and resilient 6G systems.

In addition to the booth presence, the project was also represented in the Second International Workshop on Holistic 6G Radio Design (WS7). Tommy Svensson (Chalmers University) delivered a technical talk on "The Role of Physical Layer Security in 6G", showcasing ROBUST-6G's contributions to foundational 6G security research. The workshop was jointly organized by leading SNS JU projects, covering topics such as AI-driven air interfaces, in-X subnetworks, and wireless energy transfer, with ROBUST-6G prominently featured among them. Workshop Link

The project team also welcomed Project Officer Socrates Varakliotis, sharing insights on current progress and impact within the broader SNS JU portfolio. The booth attracted strong interest from industry leaders, researchers, and policymakers, underscoring ROBUST-6G's growing role in shaping secure and sustainable next-generation networks.

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
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

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