CELTIC-NEXT
Proposers Brokerage Day

18th September 2024, London

Pitch of the Project Proposal

Robust and Trustworthy AI for 6G Satcom

Han Wang, Shahid Raza, RISE Sweden, han.wang@ri.se
Kim Seonghyun, Ericsson Sweden, kim.seonghyun@ericsson.com

Teaser

Making AI robust and trustworthy when deployed in future 6G Satellite communication

Han.Wang@ri.se

Organisation Profile

RISE, Cybersecurity Unit

RISE has the most comprehensive cybersecurity research and innovation expertise in Sweden. We have coordinated and participated in dozens of cybersecurity projects on national and international levels. RISE also owns a cyber range that is a state-of-the-art cybersecurity test and demonstration facility in Kista, Stockholm.

Care of expertise:

- *IoT Security*
- *Cloud Security*
- *Software Security*
- *5G Security*
- *AI security*
- *Cybersecurity Certification*

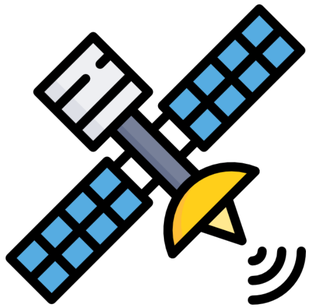
Ericsson Research Security

Our mission is to provide security expertise, develop innovative solutions, and deliver proof of concept to support various divisions within Ericsson.

We are committed to advancing technical research, driving standardization efforts, and fostering academic collaboration.

- *5G/6G and IoT security*
- *Identify Management*
- *Platform and Software Security*
- *Monitoring and Auditing*
- *Privacy*
- *Cryptography*

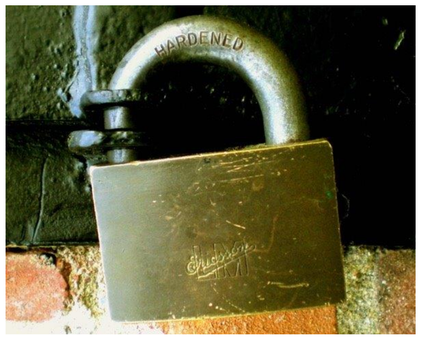
Proposal Introduction (1)



- **Robust AI for 6G**: AI systems are vulnerable to security attacks. 6G satellite communication is being treated as critical infrastructure and requires robust AI solutions.

- *For example, adversarial manipulation could misguide positioning systems or disable critical surveillance functions.*

- *Future **telecom, especially 6G**, will be managed by AI and attackers could interrupt connectivity, intercept sensitive data, or cripple emergency response systems.*



- *We aim to focus on 6G (including Edge) as a target domain*

Proposal Introduction (2)

- *Potential adversarial attacks on ML-based systems:*
  - *Data poisoning attack*
  - *Model evasion attack*
  - *Inference attack*
  - *…*
- *Solutions (e.g.):*
  - *Design privacy-preserving ML-based systems*
    - *by adding differential privacy*
    - *by data synthetization*
  - *Using decentralized training, such as federated learning*
- *Securing (distributed) AI supply chain will also be a focus*
- *Related projects:*
  - *H2020 CONCORDIA, ARCADIAN-IoT*
  - *Horizon Europe HARPOCRATES, INTEND*

Partners

Sweden: RISE, Ericsson, a telecom operator (to be confirmed), and an SME(s)

Looking for an EU consortium. We can coordinate the Swedish application.

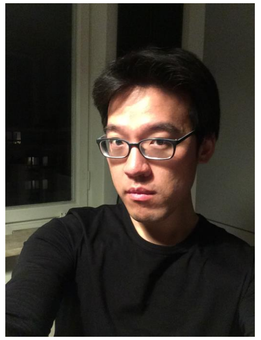
Contact Info

For more information and for interest to participate please contact:

Shahid Raza
Research Director, RISE Cybersecurity
shahid.raza@ri.se
+46 76 883 17 97
Isafjordsgatan 22
16440 Kista
Sweden

Han Wang,
Researcher, RISE Cybersecurity
han.wang@ri.se
+46 73 089 55 12
Isafjordsgatan 22
16440 Kista
Sweden

Kim Seonghyun, Ericsson Research
kim.seonghyun@ericsson.com
+46 70 986 55 32
Torshamnsgatan 23, 164 83,
Stockholm,
Sweden



Join the Consortium Building Session Thursday 19th at 15 CEST

Join meeting

Join by meeting number
Meeting number (access code): 2743 729 0349
Meeting password: 3CwQyv7HJC2