CELTIC-NEXT
Proposers Brokerage Day

24th February 2025, Barcelona

Pitch of the Project Proposal

ARAISE

Attack Resistant AI-driven and Quantum-Safe techniques for beyond 5G and IoT

Prof. Mika Ylianttila, University of Oulu, Finland
Centre for Wireless Communications, NetSEC research group
mika.ylianttila@oulu.fi

Organisation Profile

NetSEC research group *at the* ***University of Oulu, Finland*** *aims to develop essential security technologies to enable secure, trustworthy and privacy-driven 6G, and solve some of the remaining research problems in 5G and beyond, as part of the active research and industrial community, in joint research projects and programs. NetSEC seeks actively new partners in the academic and industrial community. NetSEC belongs to* ***CWC Networks and Systems*** *research unit and contributes to the* ***6G Flagship program****.*

https://www.6gflagship.com/
https://www.oulu.fi/en/research-groups/network-security-trust-and-privacy

Teaser

Vision

Towards attack-resilient machine learning that ensures secure, efficient, and sustainable AI-driven B5G networks, safeguarding against emerging threats from adversarial AI and quantum computing.

Added value and benefits

Increased relicense against adversary attacks (including powered with AI and quantum computers of the future) to companies in their products and for the society at large. Benefits include cost-savings, customer satisfaction and brand integrity, with increased assurances to the continuity of services.

Proposal Introduction (1)

Motivation

The urgent need to secure ML-integrated B5G networks against AI-driven and quantum-enabled adversaries, ensuring robust, privacy-preserving, and sustainable next-generation communications.

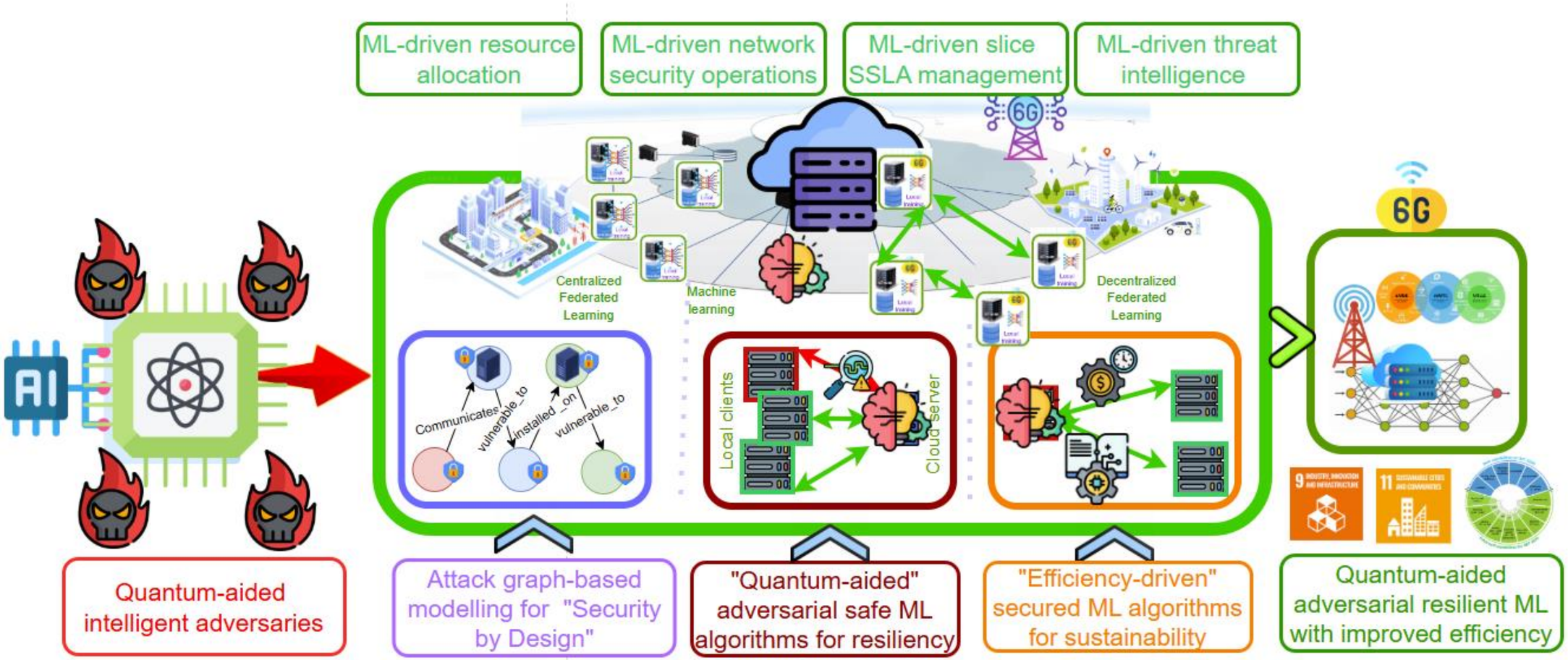
Approach

*I) An AI-driven quantum-aided **attack modelling framework** for ML-integrated B5G, using attack graphs and information theory.*

*II) Quantum-aided adversarial **resilient ML algorithms**, to secure the B5G systems with privacy and model integrity.*

*III) Secured **quantum-safe algorithms** with efficiency and sustainability.*

Proposal Introduction (2)



ARAISE, Mika Ylianttila, University of Oulu, mika.ylianttila@oulu.fi

Proposal Introduction (3)

Expected outcomes

Futuristic AI-driven and quantum-enabled adversarial attack-safe ML-algorithms and datasets for resilient B5G systems that preserve privacy, integrity, compliance and sustainability goals

Impact

Novel AI-driven and quantum-enabled adversarial robust ML algorithms and training datasets for empowering resilient industrial and societal innovations, while achieving sustainability goals

Partners

Consortium to be decided *(potentially to be merged with some other proposals)*

Potential partners

- *Cloud service providers and mobile operators needing ensure quantum safety and resiliency towards AI-related and Quantum security threats*
- *Manufacturing enterprises with ML-integrated B5G connectivity*
- *Enterprises and organizations that need secure quantum and AI/ML safety in their products and services*

Contact Info

For more information and for interest to participate please contact:

Prof. Mika Ylianttila
mika.ylianttila@oulu.fi
+358 40 535 0505
P.O.Box 4500 FI-90014 University of Oulu Finland
https://www.oulu.fi/en/researchers/mika-ylianttila

Presentation is available via: