Secure Communications and Signal Processing Group (SCSP)

- Group leader: Prof. Timo Hämäläinen
- PostDocs/Docents: Reijo Savola, Andrei Costin, Zheng Chang, Mikhail. Zolotukhin, Di. Zhang, Tero Kokkonen, Jarmo Siltanen
- Prof. of practice Tapio Frantti
- Several PhD. and MSc. students involved to the research activities and projects all the time.
- Active phD. Students: Hannu-Tapani Turtiainen, Riku Immonen, Rony Leppänen, Saro Kaharinen, Tero Bodström, Sanjay Kumar, Pares Rathod, Chen Zhonghua, Heinilä Erkka, Hu Ruxue, Khandker Syed, Liu Jia, Liu Wenya, Puoliväli Tuomas, Shao Shuai, Song Liting, Sun Jiayi, Sun Xiaobang, Wang Biying, Wang Xiaoshuang, Wang Xiulin, Xu Huashuai, Yan Rui, Zhang Guanghui, Zhou Dongdong, Zhu Yongjie etc.
- The group has achieved a significant position in the IT Faculty's research and PhD&MSc. trainer : Supervised 70+ PhD dissertations and 250+ Master theses since year 2000.

Goals of the research:

- The focus is on the resource management methods of the wired and wireless telecommunication systems (IoT, NG). The technology developments with the industry and standardization work. Industrial collaborators eg. With: Nokia, Magister Solutions, Telia, Elisa, Airbus defense and space, Samsung, Huld etc.

- Dynamic network resource management technologies will be investigated, where software-defined networking (SDN), network function virtualization (NFV) and network slicing are used to provide an agile and dynamic networking platform for supporting multiple virtual networks on demand on top of a common shared physical network infrastructure.

- Networking security is an essential part of the resource management. We'll develop methods for monitoring and analysing network devices and traffic, as well as methods to mitigate attacks.

- We are developing methods for monitoring, analysing and managing the network traffic (security, QoS etc.)

Some recent external funded research projects:

- Autonomous Vehicular Edge Computing and Networking for Intelligent Transportation (EU, 2023-2027)
- Keski-Suomen kyberturvallisuuden tunnetuksi tekeminen (KSKTK), participants: JAMK, Telia, city of Jyväskylä, K-S liitto, (2022-2024)
- ADDing VAlue by Computing in Manufacturing (coADDVA), participants: Are, Windside, JAMK (2021-2023)
- Ecological, intelligent and secured IoT services, paricipants: Valtra, MetsäGroup, Mevea, Mantsinen Group, Are, city of Jyväskylä (2020-2022)
- IoTLi- business growth from IoT, participants: Etteplan, Metsä Group, AGCO/Valtra, Vapo, Ficonic Solutions, city of Jyväskylä (2019-2021)
- Lipa, mobility and services in IP networks, participants: Metso Paper, Ixonos, Cynetkey, Resolute and Elisa.(2017-2020)
- Tiepal, Mobile service development to Open IMS service platform, participants: Anvia, Arena Interactive, Digita, Kilosoft, Metso Paper (2016-2018)
- Laila, Service management in multi-access networks, participants: Nokia, Digita, Arena Partners, and WTS. (2016-2018)
- NGNAP, Developement and use of next generation network architecture in process automation industry, participants: Metso Paper, Telia Sonera, Liqum. (2015-2018)
- End to End QoS and IMS, JKL Innovation (2015-206)
- Imola, IMS and Mobile services, participants: Vaasan Läänin puhelin, Digia, Digita, KOAS, JYY. (2014-2016)
- Tiepal, new mobile services and management in Open IMS", participants: Vaasan Läänin puhelin, Digita, ArenaInteractive, Kilosoft, KOAS, JYY. (2014-2016)
- ISSM- Intelligent Systems for Security Management", participants: Ixonos, TUT. (2013-2015)

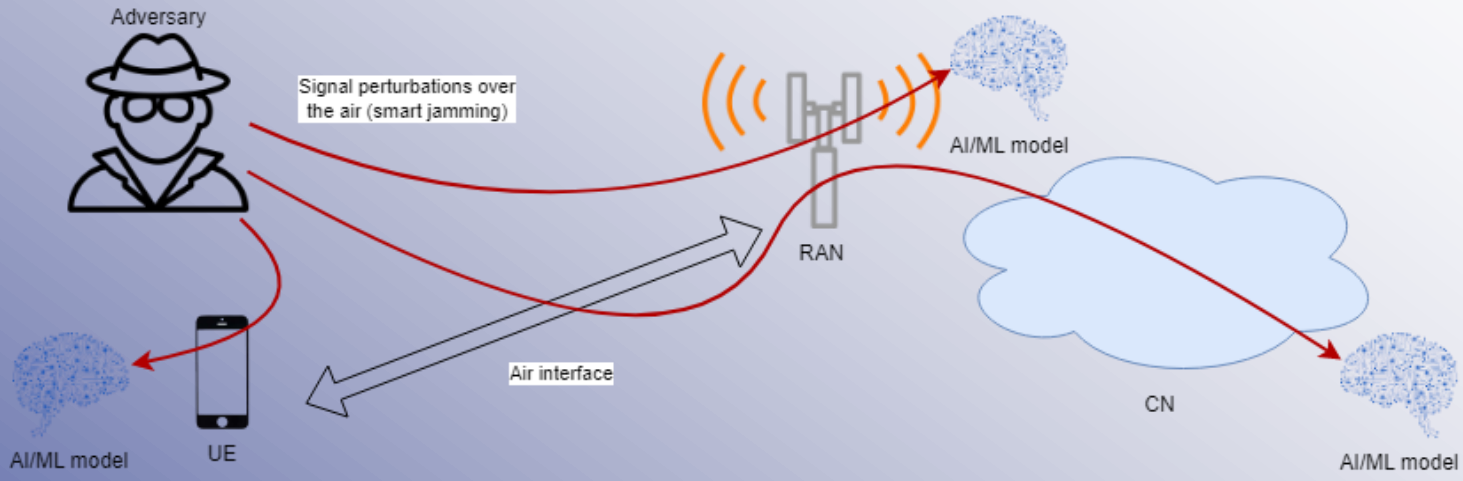
SCSP group's CyberSecLab

SCSP group has CyberSecLab, which works on research and teaching for the cybersecurity techniques to cope with all kind of cyberattacks and unknown and potential threats, such as ones for wireless and wired networks, critical infrastructure, and emerging IoT devices and networks in particular. Some lab environments:

- Private 5G network from Nokia
  - low latency, high security for the different kind of IoT etc. applications
  - E2E configurations from the sensors to cloud/wherever
- ESAT nanosatellite model, https://www.theia.eusoc.upm.es/esat/
    - Essential part of the 5G network
    - Satellite networks security (firmware, apps security)
- Franka Emika robot, https://www.franka.de/production
  - Security issues (firmware, apps security) in different kind of industrial environments
- Matrice 300 RTK drone, https://www.dji.com/fi/matrice-300
  - Security issues in aviation and drones (firmware, apps security)
  - Includes eg. high resolution camera eg. pattern recognition
- Other stuff: sensors, apps (pfSense, Snort, Zeek, Wireshark) and clouds (Azure, AWS)

Use Case: Attacks against ML Models in 5G Networks

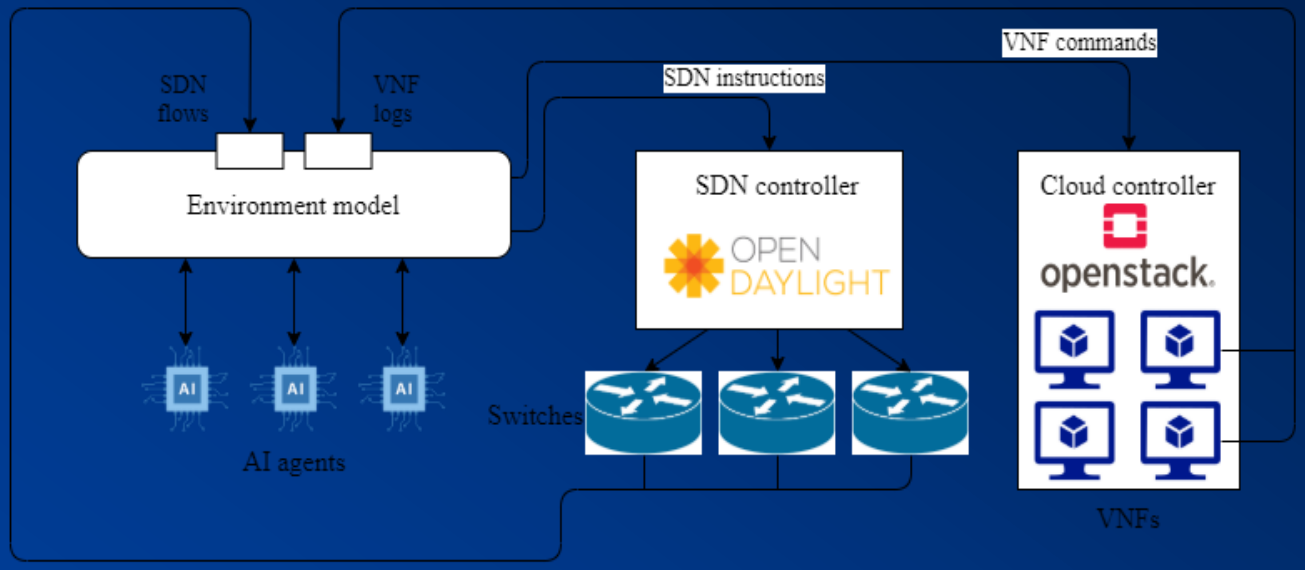
- AI/ML frameworks deployed in mobile networks are susceptible to adversaries that have an ability to manipulate the inputs to the models during the inference stage over the air due to the shared and open nature of wireless medium.



- Depending on the information available to the adversary, such adversarial example attacks can be either white-box (the adversary has perfect knowledge of the ML model and/or the training data) or black-box (the adversary's only capability is to observe labels assigned by the model for the inputs supplied)
- In our research, we focus on black-box attacks against AI/ML-based beamforming which is proposed to be used in future mobile networks to reduce delays and transmission feedback overheads

Use Case: Intelligent zero-trust networking for IoT

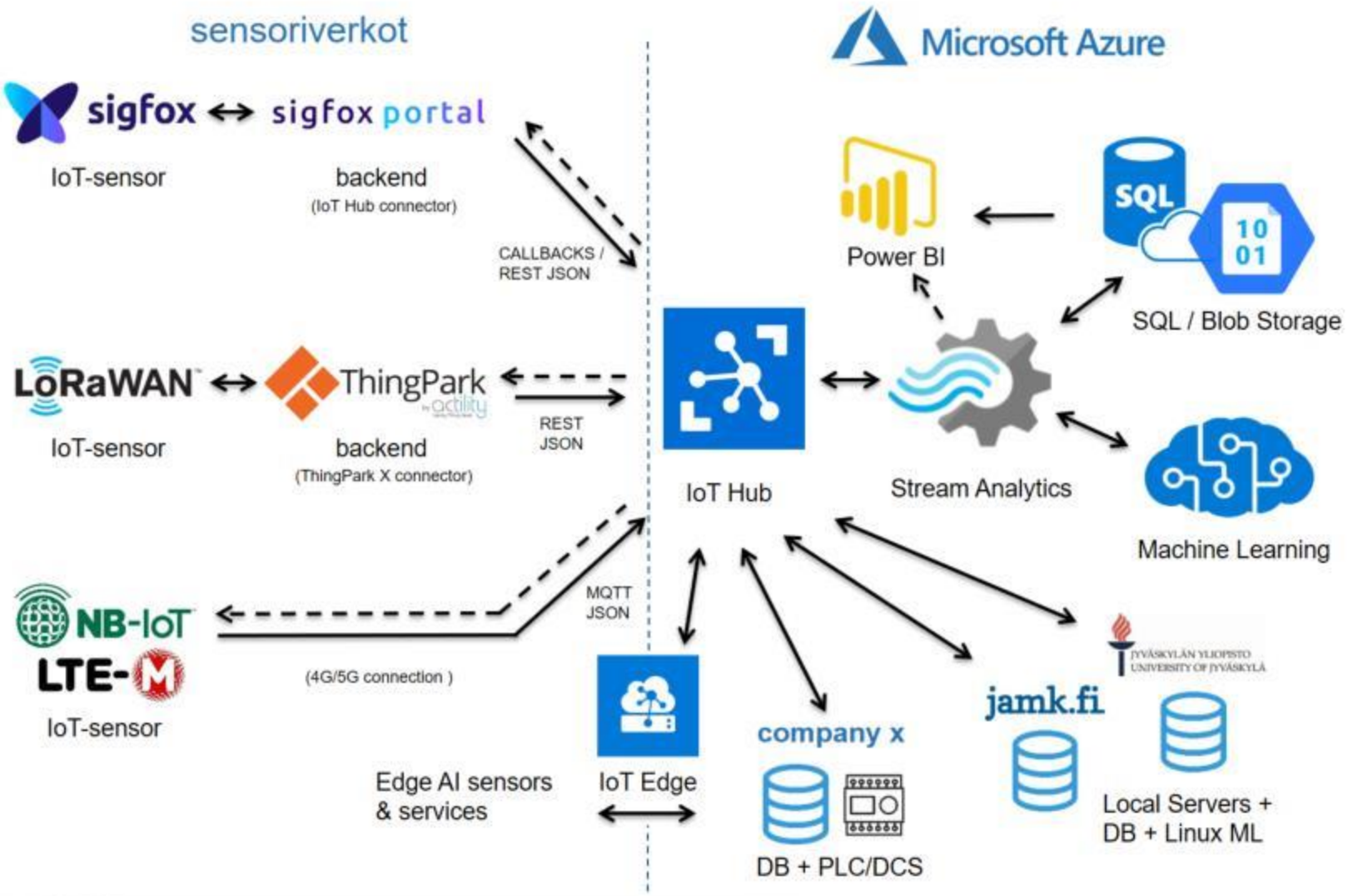
- An intelligent network defense system which relies on SDN and NFV technologies to launch and configure security appliances and redirect certain slices of the traffic to these appliances as well as chain the appliances between each other



- The key component of the defense system proposed is an AI engine that resides on top of the SDN and NFV controllers and is responsible for manipulating security policies depending on the current network state

- AI engine consists of several reinforcement learning agents which aim to minimize the attack surface and the risk of subsequent attacks in the future

Use Case: IoT / cloud configuration



Ongoing Projects

Autonomous Vehicular Edge Computing and Networking for Intelligent Transportation (ACENT) (EU, 2023-2027)

- Develop a ultra-reliable vehicular edge intelligence framework that leverages novel hierarchical and personalized Federated Learning (FL) techniques at the vehicular edge to efficiently process large volumes of data generated by smart vehicles and RSUs.

ADDing VAlue by Computing in Manufacturing (coADDVA). Participants: Are, Windside, JAMK (2021-2023)

- Develop TinyML and Edge AI solutions for different IoT environments

1. **Wind speed estimation (Winside).** The estimations are carried out using electric current time-series observed during the recent time interval on a wind turbine. The rationale behind this task is that wind speed estimations obtained can be monitored by the turbine operators in real time for more efficient power extraction and detection of anomalous patterns which may be indicative of a fault.

2. **Anomalous vibration detection (Are).** The detection is conducted by analysing data recorded by an accelerometer. The task is to train a model of normal behavior which can then be used to classify anomalous vibrations that significantly deviate from the norms described by the model. The training is expected to be carried out on the device itself.

Ongoing Projects (with Dr. Reijo Savola)

QU-ENABLER – Quantum-safety enabling infrastructures for edge intelligence in future networks, BF (2023-2024)

- QU-ENABLER aims for effective infrastructural advances in enabling the migration to PQC (Post-Quantum Cryptography) in edge and access services.
- The project will construct a generic reference quantum-safe infrastructure model for edge and access services. The focus of the model is on feasibility and effectiveness, architectural choices and connection of networks to support different types of use scenarios. The reference model will support migration into PQC.

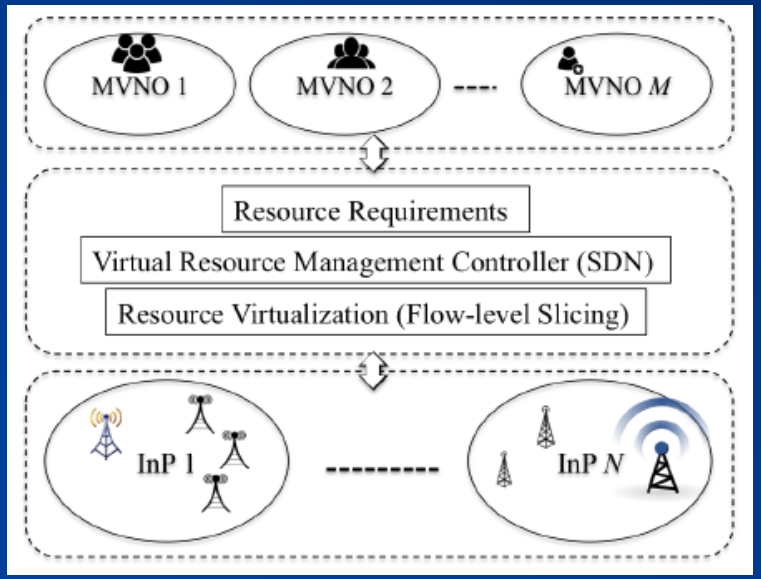
AIQUSEC – AI-based quantum-safe cybersecurity automation and orchestration for edge intelligence in future networks BF (2023-2025)

- AIQUSEC makes measurable advances in cybersecurity for access and edge services, and operational technology (OT).
- The project will design a leading-edge security assurance and validation environment, with a supporting cybersecurity system integration reference model, with a focus on architectural choices and connection of networks from different vertical use cases. The environment and reference model created will enable building, testing and validating joint cybersecurity capabilities. In addition to the above-mentioned environment, the project's results will be demonstrated in critical telecommunications, water utility, physical access solutions, industrial automation and remote work scenarios.
- The project aims for significant cybersecurity scalability, effectiveness and efficiency through enhanced device and sensor security, security assurance, quantum safety and Artificial Intelligence (AI)-based automation solutions.

Other Project Activities

Network resource management:

- Virtual Resource Allocation in SDN- based Cellular Network
- Energy efficiency improvement in mobile networks
- Intelligent routing in next generation Satellite Communication
- Massive stable transmissions in a strong interference,high uncertainty,and mobility scenario
- Intelligent networking, mobile edge computing (MEC), computation offloading



- Ports ≠ Applications
- IP Addresses ≠ Users

Networking security:

- Mitigation of DoS attacks in SDN cloud environments
- Detection of saturation attacks against SDN controller
- Collaborative filtering for multi-stage attack prediction
- Detection of malicious data exfiltration over DNS tunnels
- Mobile device malware analysis (Android etc.)

If you are interested in development of the future secure networks and services in our national/international projects, contact us !

timo.t.hamalainen@jyu.fi