



STACK

Pushing back against IoT attacks

The ITEA project STACK (Smart, Attack-resistant IoT Networks) will enable Internet of Things (IoT) applications with a high Quality of Service (QoS) even under non-benign circumstances. Goals include more robust IoT communication, attack detection/mitigation through performance and interference monitoring and algorithms leveraging a tight integration with a smart edge.

Addressing the challenge

Many IoT devices lack guaranteed reliability, latency and security – a concern given the rise in cyber-attacks. IoT mesh networks of embedded devices are especially vulnerable due to their wireless communication and relatively low output power; even so, they increasingly influence our safety and livelihood in domains like autonomous driving and healthcare. As resource constraints prevent devices from running sophisticated defences, the challenge is to ensure that IoT networks can maintain functionality in difficult situations such as attacks and cross-technology interference.

Proposed solutions

STACK offers several innovations to meet this challenge. As non-benign environments require both attack detection and mitigation, the project will exploit the computational power of the smart edge. Simulation support to generate the necessary training data to enable the creation of new detection and mitigation methods will be provided. Compressed models based on this data can be installed on IoT devices or gateways. Novel attack mitigation mechanisms will be based on frequency, data rate and protocol diversity and will provide QoS levels and message prioritisation during attacks.

Other innovations include the combination of multiple standard-based communication technologies to improve robustness and a machine learning model offloading scheme to split data

processing between resource-limited IoT devices and a smart gateway. Lightweight, standard-compliant security mechanisms and ARM TrustZone technology will increase protection. The outcomes will be made open source where possible.

Projected results and impact

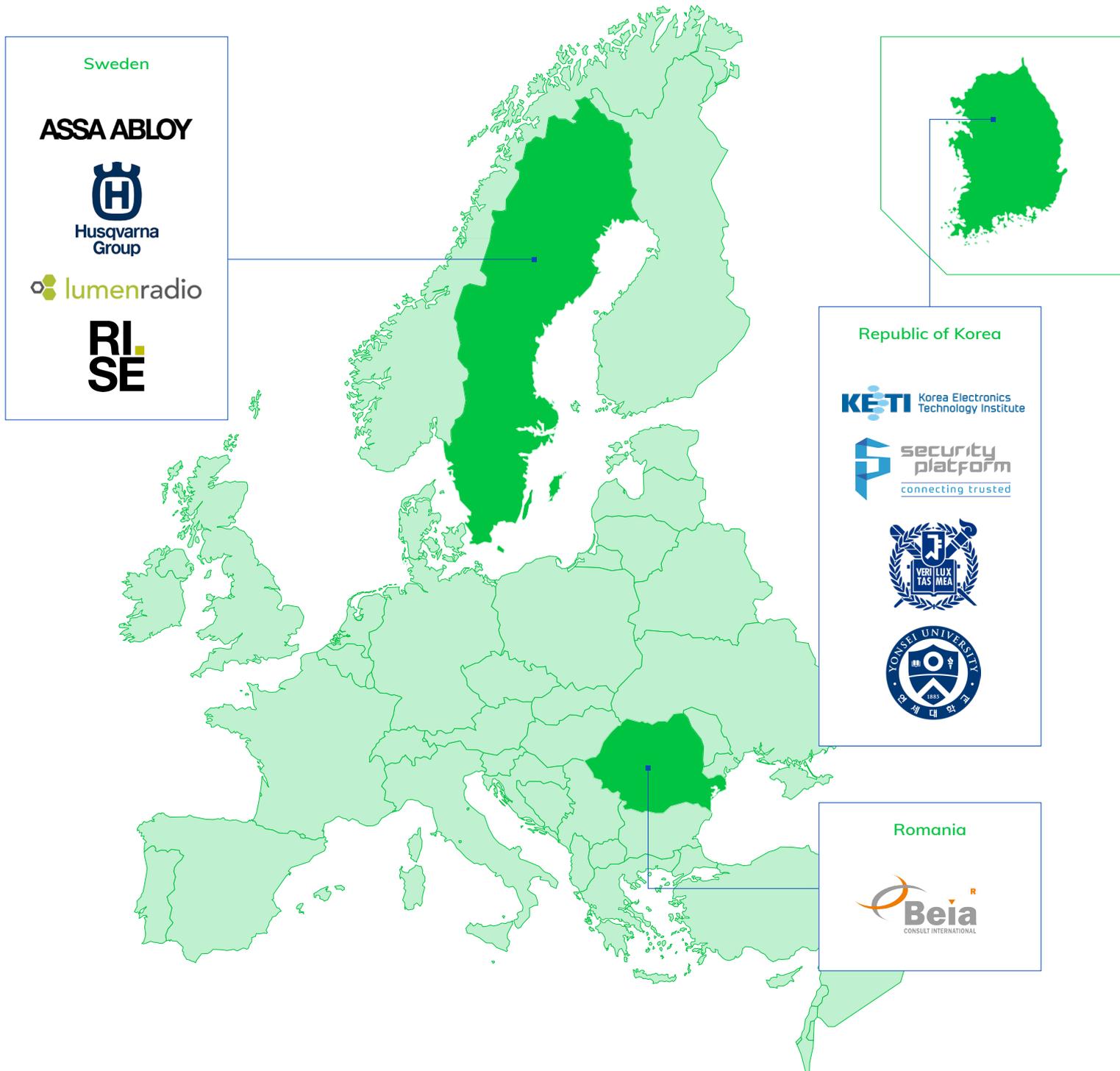
STACK's core results will be a reduction in the time taken to detect disturbances on IoT systems and networks, as well as an increase in the number of attacks which can be detected and mitigated and lower energy costs in the detection process. Additional benefits include better communication performance in environments with strong interference and faster deployment of IoT systems with battery-powered, resource-constrained nodes. For end-users, this means significantly lower costs for a

AI-based Attack Detection & Mitigation



^ STACK aims to provide more secure and robust IoT networks.

secure IoT system. Approximately 10% of current IoT-connected devices could benefit from STACK, the total number of which will increase to 75.44 billion by 2025. The project will also give the consortium a competitive edge in a global IoT security market expected to reach USD 35.2 billion by 2023.



Project start
December 2020

Project leader
Thiemo Voigt, RISE

Project website
<https://agile.ro/stack/>

Project end
December 2023

Project email
thiemo.voigt@ri.se

ITEA is the Eureka R&D&I Cluster on software innovation, enabling a large international community of large industry, SMEs, start-ups, academia and customer organisations, to collaborate in funded projects that turn innovative ideas into new businesses, jobs, economic growth and benefits for society. ITEA is part of the Eureka Clusters Programme (ECP).

<https://itea4.org>