ITEA 4

Project Results

STACK

Enhancing security in IoT mesh networks

The ITEA project STACK (Smart, Attack-resistant IoT Networks) developed various tools, methods and support systems to detect and mitigate attacks on Internet of Things (IoT) mesh networks, which offer energy and efficiency benefits but face strong cybersecurity risks.

Interest is growing in mesh networks of embedded devices as they enhance network efficiency and minimise power consumption, yet very few security-related products target such networks. With no large traces for machine learning (ML) algorithms, no tests in real testbeds/applications and less standardised infrastructure or complete ecosystems, the state of the art remains low. This lack of development presents a security issue: the wireless communication and relatively low output power of mesh networks leaves them particularly vulnerable to cyber-attacks.

With a focus on these mesh networks, STACK aimed to enable a new class of critical IoT applications that can operate securely and provide quality of service even in malicious conditions. This was achieved through tools and methods for attack detection and mitigation on IoT devices and the edge, as well as more robust IoT mesh networks. For smart attack detection and mitigation, the focus was on detection at several layers (including AI-based malicious network activity detection based on new traces) and sensor testing and identification. For attack prevention, the approach was to develop network security support, hardware support, and protocols and mechanisms for predictable networking. Such innovations have been demonstrated in use-cases such as smart meters and lock systems.

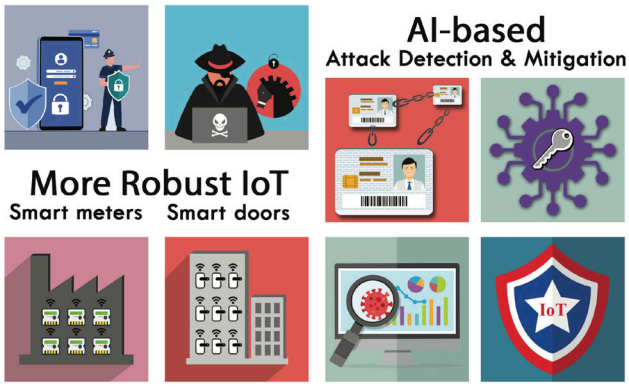
Technology applied

IoT mesh networks are composed of resource-constrained devices such as sensors and actuators and feature gateways or servers that communicate with devices close to them. Certain nodes may be too distant from the base station, necessitating data transmission through intermediary nodes (multi-hop routing). With limited computing resources, security becomes an issue. Additionally, these nodes are susceptible to interference and jamming due to their low radio output power. Finally, resource limitations prevent the use of sophisticated operating systems in favour of, for instance, low-level C programming, which increases the attack surface. One of STACK's key innovations was therefore the adaption of TrustZone – a hardware mechanism that breaks execution environments into (non-)secure memory, peripherals and functions – for use with Contiki-NG, an operating system for networked, resource-constrained systems on which some partners have developed their own products.

For attack detection and mitigation, an important development has been the Multi-Trace tool. In current attack detection for IoT networks, ML algorithms learn to identify abnormal network behaviour. However, state-of-the-art algorithms have only been trained for very specific situations due to a limited number of traces. With Multi-Trace, STACK turned the Cooja simulator, a network simulator that runs deployable code, into a trace generator machine that can generate hundreds of traces (with and without attacks) in a short timeframe. This allows ML algorithms to be trained more quickly and compressed models based on this data can be installed on IoT devices or gateways.

Making the difference

Few products previously contained attack detection and mitigation for multi-hop networks. STACK is therefore a pioneering project as the partners have devised ten methods for this and can detect over ten different attack types. Ten systems and services have also been developed, many of which are open source to boost their uptake and enhancement by third parties. This will give companies a quick start when taking advantage of the efficiency, low power consumption and prolonged battery life of mesh networks. A particular achievement is a detection accuracy of 80-90% across all use-



The STACK project has devised novel tools, methods and support systems to detect and mitigate attacks on Internet of Things (IoT) mesh networks.

cases, reaching as high as 93% for naïve attackers in ML-based flooding attacks. Given the starting point of zero, even 80% is an excellent foundation for further development.

For the consortium, the project has brought a mix of internal improvements, human capital and stronger business cases. As a smaller company, LumenRadio has added STACK innovations to its existing software to achieve a competitive edge by addressing security concerns that are lacking in other standards; during the project, it saw its total employees almost double and its turnover more than triple. Husqvarna has similarly improved the open-source software used in their products but has also gained new knowledge that they intend to use to double their current 3.6 million connected devices by 2026, making STACK important to their longer-term strategy.

Commercialisation is also taking place already: Security Platform developed technology to embed cryptographic modules within TrustZone-based microcontroller units and applied this to smart power meters. This reduces costs by removing the need for additional security hardware and improves encryption/decryption performance. One of their clients, KEPCO, is the largest electric utility in South Korea and replaces five million units per year – all of which will soon contain STACK technology. In preventing attacks, STACK also protects companies from brand damage. ASSA ABLOY, for instance, is a global leader in access solutions, a field in which customers expect security at a minimum. They now have the opportunity to expand their offerings without risking their reputation. Ultimately, this will make mesh networks a more attractive proposition and help to grow a domain that the consortium believes will become increasingly crucial to the future of IoT.

Major project outcomes

Dissemination

- More than 10 publications and more than 15 presentations at conferences/fairs.

Exploitation (so far)

New products:

- New smart meter platforms.
- Trusted firmware SDK in Cortex-M TrustZone.

New services:

- Sensor error detection of contextual and formal sensor errors.
- Coulomb counters for wireless IoT network stacks to estimate current consumption of devices.
- New attack traces for wireless multi-hop networks.

New systems:

- Federated learning framework for resource-limited platforms.
- Machine learning-based flooding attack detection framework for RPL networks.
- On-node jamming attack detection and classification.
- Time synchronisation for multi-gateway time slotted channel hopping networks.
- Tool for Trace Generation to train attack detection algorithms.
- Coalesced network and storage security for DTLS.
- Fast & secure on-device neural network inference framework for TrustZone-enabled devices.
- Framework for efficiently optimising memory resources for on-device DNN training.
- TrustZone support for the Contiki-NG operating system.
- Contributions to Wakaama Open Source System.
- Adaptive Frequency Hopping aims to actively avoid frequencies with high disturbance.
- Certified cryptomodule in Cortex-M TrustZone.

Standardisation

- Participating in the IETF COSE group, developing and actively pushing for standardisation of compact certificate encodings.

Patents

- One patent on attack detection and two patents on media access filed.

ITEA is the Eureka RD&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

STACK

19045

Partners

Republic of Korea

- Korea Electronics Technology Institute
- Security Platform
- Seoul National University
- Yonsei University

Romania

- BEIA Consult International

Sweden

- ASSA ABLOY
- Husqvarna
- LumenRadio
- RISE - Research institutes of Sweden

Project start

December 2020

Project end

December 2023

Project leader

Thiemo Voigt, RISE

Project email

thiemo.voigt@ri.se

Project website

https://agile.ro/stack/

ITEA 4

eureka