STACK: Smart, Attack-Resistant Internet of Things Networks

Thiemo Voigt, Joakim Eriksson, Niclas Finne, Joel Höglund, Nicolas Tsiftes, Saptarshi Hazra, RISE, Sweden

Tomas Jonsson, Zhitao He, ASSA ABLOY, Sweden

Johannes Arvidsson, LumenRadio, Sweden

Anders Mattsson, Husqvarna, Sweden

George Suciu, Mari-Anais Sachian, Sorina Mitroi BEIA, Romania

Pusik Park, KETI, South Korea

JeongGil Ko, Yonsei University, South Korea

Youngki Lee, Seoul National University, South Korea

Kyung mo Kim, Security Platform, South Korea

Abstract

This white paper presents an overview of the STACK project. The goal of STACK is to let IoT networks maintain their functionality in both benign environments and more challenging situations, such as when IoT networks are under attack or exposed to harsh radio environments and cross-technology interference. Solving these challenges will enable a new class of IoT applications that provide a certain Quality of Service (QoS), even when under attack. Our major innovations towards this goal include more robust IoT communication, attack detection and mitigation by performance and interference monitoring and smart algorithms that leverage a tight integration of IoT devices with a smart edge. In this white paper we present an overview of the project. We motivate why the STACK project focuses on wireless IoT mesh networks. We briefly present potential attacks on such networks and discuss why machine learning is important to detect attacks and intrusions. Finally, we present one of the early results of our project: Multi-Trace, a tool that is able to generate traces that can be used to train machine learning algorithms for attack and intrusion detection.

1. STACK Overview

The Internet of Things (IoT) was expected to enable applications of utmost societal value, such as energy-efficient buildings, smart cities, intelligent grids, and next-generation healthcare. Such a promise is only partly fulfilled. The more demanding and critical applications still fall short of expectations. These applications require sensor data and actuation commands to be delivered in a timely fashion with high reliability, while the battery-powered devices must last for years.

Simultaneously, we witnessed a tremendous increase in attacks on the Internet infrastructures. For instance, IoT devices were hacked and used in a DDoS attack by the Mirai botnet in October 2016. IoT networks of embedded devices are even more vulnerable than the existing Internet infrastructure, since they usually communicate wirelessly and at a much lower output power than other devices such as WiFi, which makes them more vulnerable to, e.g., jamming attacks.

Furthermore, due to resource constraints, these devices cannot run the most sophisticated cryptography algorithms and other defences against attacks. The challenge is thus to make IoT networks maintain their functionality not only under benign circumstances but also in more challenging situations; for example, when IoT networks are under attack or exposed to harsh radio environments and cross-technology interference. Solving these challenges enables a new class of IoT applications that provide a certain Quality of Service (QoS) even under attacks.

While there exist commercial products for WiFi networks such as Cisco's Wireless Intrusion Prevention System, similar tools are missing for the more resource-constrained IoT networks. Note that such tools are not easily adapted to many IoT scenarios due to the resource-constraints of the IoT devices and in particular to IoT mesh networks. In addition, mechanisms to mitigate attacks and sustain QoS under severe circumstances cannot be adapted from the less resource-constrained world for the same reasons.

Our major innovations towards this goal include more robust IoT communication, attack detection and mitigation by performance and interference monitoring as well as smart algorithms leveraging a tight integration with a smart edge. Training data for learning the best strategies will be collected primarily in our testbeds and deployments. We will evaluate and validate our developed concepts through several challenging use cases that address critical application areas which adhere to stated QoS levels when being under attack. This way, STACK will enable more demanding and critical IoT applications than the "best effort" applications that are deployed today, discusses some attacks and

2. IoT Mesh Networking

While many recent IoT wireless technologies such as LoRa and NB-IoT are based on single-hop (also called start) networks, there is also a need for IoT multi-hop networks, where some IoT devices forward packet from other IoT devices towards the base station (see Figure 1).

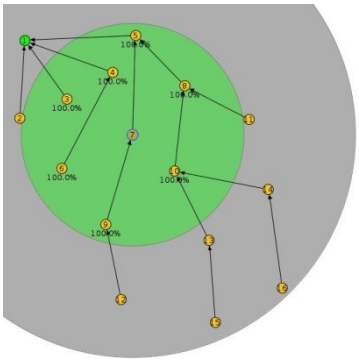

Figure 1: Multi-hop Network in the Cooja Simulator

For example, in residential and smart homes the Matter ecosystem forecasts itself as a common standard for the future. It contains the Thread mesh standard which is good for small buildings as homes and small offices where users have full control of the Wi-Fi network and can avoid co-existence problems between Wi-Fi and Thread. Here, a Thread mesh provides high reliability against interfering objects due to its redundant routing paths. Matter also contains BLE for configuration and Wi-Fi for devices which need higher throughput. In China, the BLE-mesh standard for lightning in residentials is gaining momentum. Here, the main driver is the reduced cost and the avoidance of multi-stack support in future devices.

In commercial buildings there are no mature and standard wireless technologies for low-power and low-cost IoT devices. Wi-Fi and macro cellular technologies consume too much power and do not have good enough coverage in all buildings. Therefore, device manufacturers often build their own wireless infrastructure and use different standard wireless technologies or proprietary solutions. This is challenging and only companies that have competence to build a full wireless infrastructure can be capable. The wireless networks need to be operated and today the building/system owner are forced to do that even though in many cases they do not have necessary competence. Therefore, there is a need for self-healing and self-organizing networks.

For lock systems, one of the core application areas of the STACK project, the most common technologies in commercial buildings today are star networks based on BLE, 802.15.4 and 802.15.4g. Today, these star networks are based on 2.4GHz; thus are often not very reliable since they do not offer redundant routing paths. The 802.15.4g (sub-gig Hz) can penetrate through objects in a better way and is also more reliable. Hence, there is need for redundant routing paths as a form of increasing the reliability of the system. These networks are, however, costly and require a lot of wiring to the hubs (access points or coordinators). They often lead to high maintenance costs since they do not have any built-in self-healing. In such application scenarios, mesh networks can increase reliability and decrease the total cost of ownership compared to start networks. Other applications as for example lightning and control of HVAC use mesh networks based on BLE or proprietary solutions.

There are new wireless technologies and initiatives for commercial buildings. The DECT2020 mesh standard is based on 5G hardware, but a new standard mesh stack will have low power products available 2022. The Matter standard/ecosystem starts to discuss opportunities to have a standard for commercial buildings also. The 5G private networks which use small cells inside buildings will enable lower power devices and the plan is also to support mesh in the future (see below). This will

allow better coverage than Wi-Fi. For 6G, first deployments are expected in 2028. 6G plans for extremely low-power and low-cost devices. Hence, 6G devices will most likely compete with the low-power and low-cost IoT networks today.

To summarize it seems that the most important new wireless technologies inside buildings for low power and low cost will be based on mesh in the future. In the far future, the IoT networks will be standardized. All this together will lead to lower total cost of ownership for customers but also better coverage and interoperability between devices. A key issue for the success will be security which is a focus of the STACK project.

3. 5G (private) networks

The development of the internet and networks is one of the most important innovations of the history of industrial communication. Industrial networks are much more valuable and profitable than traditional point-to-point networks. They play an essential role in a wide range of areas, such as energy and IoT. As the environment and technologies continue to evolve, high-performance wireless communications are becoming a crucial tool in the digitalization of industries and companies. Therefore, 5G networks have great potential in terms of wireless technologies [Aijaz,2020].

During the last decade, but especially during the COVID-19 pandemic, an increasing number of companies are choosing to digitise all their processes. Thus, private 5G networks are the most popular choice for building secure and flexible wireless networks within the vertical industry to enable services and device connectivity in the digitisation process.

Companies especially choose to use private 5g networks because of the very low latency and high reliability in supporting the devices. A private 5G network is a Local Area Network (LAN) that allows devices to create a network with dedicated bandwidth. Thus, as 5G connectivity is 100 times faster than 4G LTE (which stands for Long Term Evolution), companies are able to achieve the desired speed standard. Such approaches are opening up a new segment of the business market and the operator service provision market [Li,2021].

Version 16 of private networks or non-public networks (NPN) comes with several improvements, including the fact that the network is completely isolated, allowing only subscribed users to connect to it. This new version, 16, allows for both Authentication and Key Agreement (AKA) mechanisms without universal subscriber identification. There is further support for the private network in version 17 by introducing support for neutral host models, under which the service provider and the network owner do not have to be the same entity [Bertenyi, 2021]. It is evident that private networks will be an essential element in 5G technologies, and not only here. Private networks allow companies, institutions and factories to deploy a smart, flexible and fast infrastructure. Private 5G networks are an agile yet simple solution for reliability, reconfigurability and the redistribution of resources needed to deliver services efficiently [Maman,2021]. A considerable advantage of 5G technology is that it can support large sensor networks used in the IoT industry. When it comes to large industries, private 5G networks are the best choice because they are very flexible, allowing the creation of several "mini-networks" through the network slicing procedure, which facilitates the connection and use of more devices and sensors at the same time. 5G is based on spatial diversity, which means using variable arrival times, thus creating multiple TDD (time division duplexing) channels that facilitate channel redundancy. Because 5G networks have very high bandwidths, they are at the top of the list of choices for artificial intelligence-based application manufacturers because

such networks allow for collecting, processing and cloud storage of a vast amount of sensor data [A.Aijaz, 2020].

The 5G Public-Private Partnership (5G-PPP) anticipates that 5G technology will shorten the creation time from 90 hours to 90 minutes. On top of that, the technology will offer users high privacy and will underpin the connection of at least 7 trillion devices. Since companies and vertical industries are in a continuous process of digitisation, 5G is the most popular choice since it provides high availability and secure services using several specific techniques. These include Network Function Virtualization (NFV) and Software-Defined Networking (SDN) technologies because they meet the highest user demands. NFV is an efficient solution because instead of installing a more complex hardware system, system enhancement can be achieved by using virtual machines. Installing network components with network function virtualization takes hours instead of months, thus drastically reducing time and financial costs. NFV is running software that behaves like traditional physical networking components, with load balancing, routing and security covered by the software functionality. Also, running in virtualization mode allows standardization on a generic server, controlled in turn by a hypervisor. SDN enables a better organization of networking with programmable software, so the entire network can be managed consistently and holistically. The main attributes that make this approach advantageous are network programmability (which allows the network to be controlled by an application, thus supporting new services), abstraction of the network (use of APIs to retrieve data) and logically centralized intelligence (which allows intelligent resource management) [Bonati, 2020].

4. Attacks on IoT Mesh Networking

Low-power IoT mesh networks form the foundation of many Internet of Things systems that promise applications in domains of high industrial and societal relevance such as healthcare, agriculture, aviation and aerospace, civil infrastructure monitoring and process control in industrial settings. However, these networks also introduce new attack vectors mainly due to their constraints in memory, computing power and energy and the lossy nature of wireless communication [Aris 2018, Boo 2019]. These new attack vectors include, for example, denial of service attacks through jamming that aim to degrade network performance, by depleting devices' batteries by causing additional packet loss and delays. There are also a set of new attack vectors on routing protocols for IoT mesh networks. Aris et al. provide an overview on attacks on one such routing protocol, namely the Routing Protocol for Low-Power and Lossy Networks (RPL) [Aris 2018].

5. Machine Learning to Detect Attacks on IoT Mesh Networking

While there are different types of attacks, one focus of the STACK project is to detect attackers that have managed to intrude into the network. To defend against attacks on IoT mesh networks, existing solutions typically consist of three main components [Butun 2013]. First, there are components with the task to prevent attacks. Second, there are components that aim at detecting attacks. Finally, components are needed to mitigate an attack that has been detected. If the first component was not able to prevent an attack, the task of the second line of defense is to detect any suspicious behaviour. The latter is performed by so-called intrusion detection systems (IDS). Due to the characteristics of IoT mesh networks, in particular the resource-constraints of the embedded IoT devices, designing efficient intrusion detection systems is far from trivial [Butun 2013]. Therefore,

there has been a large body of research papers on this topic. As an example, one of the earliest papers on intrusion detection by Raza et al. [Raza 2013] has been cited more than 650 times. Most intrusion detection systems make use of machine learning techniques [Tsai 2009], [Wagh 2013]. Unfortunately, most of the proposed IDS for IoT mesh networks have been trained on a very limited range of network topologies, scenarios and attacks. This shortcoming is mostly caused by the lack of sufficient data traces required to train attack-detecting machine learning algorithms. Nevertheless, to be effective in various attack scenarios, machine learning-based algorithms require a lot of training data.

6. Early Results: Multi-Trace

To enable the generation of training data for machine-learning algorithms, we have modified the Cooja simulator [Österlind 2006] to support efficient trace generation. The Cooja simulator has originally been designed to simulate networks of resource-constraint embedded devices running the Contiki operating system but it is also able to run binaries of other operating systems.

With Multi-Trace [Finne 2021] , we extract four different types of data from Cooja simulations: First, application developers can print data specific to their application using standard Contiki log messages. At this level, users have the full freedom to customize their log messages. Second, Cooja has a radio logger plugin that logs all data traffic in the network. This data is available in pcap format, a format originally used by the pcap API of tcpdump. Third, we enable radio transmissions logging at the radio medium level. While the radio logger plugin logs all in-air messages, it does not include information about which nodes received a particular radio transmission. Specifically, it is difficult to derive which nodes received an omni-directional broadcast message transmission using only the radio logger in multihop networks. Fourth, there is an event log for events during the simulation. For example, a simulation can log an event when the network has reached a steady state to make it easier to ignore the startup phase of a simulation or when an attack is started or stopped to indicate during which times an attack is active.

Note that while we offer opportunities for logging at different levels, they all share a global simulation time, which facilitates the fusion of the information from heterogeneous logs. Our results have demonstrated that Multi-Trace can generate traces at high speed which makes it a valuable tool for the research community. Multi-Trace can be found at the STACK's github page: https://github.com/STACK-ITEA-Project/

7. Summary

This white paper has presented an overview of the STACK project. We have motivated the focus of the project on wireless IoT mesh networks that we believe will become more important in the future. We have also discussed attacks on such networks and the importance of machine learning to detect and defend against such attacks. Finally, we have described Multi-Trace, our tool that can generate traces for training such machine learning algorithms.

References

[Aijaz 2020] Aijaz, A. (2020). Private 5G: The Future of Industrial Wireless. IEEE Industrial Electronics Magazine, 14(4), 136–145. doi:10.1109/mie.2020.3004975

[Aris 2018] A. Arıs, S. F. Oktug, and T. Voigt, “Security of internet of things for a reliable internet of services,” Autonomous Control for a Reliable Internet of Services, 2018.

[Bertenyi 2021] Bertenyi, B. (2021). 5G Evolution: What’s Next? IEEE Wireless Communications, 28(1), 4–8. doi:10.1109/mwc.2021.9363048

[Bonati 2020] Bonati, L., Polese, M., D’Oro, S., Basagni, S., & Melodia, T. (2020). Open, programmable, and virtualized 5G networks: State-of-the-art and the road ahead. Computer Networks, 182, 107516.

[Boo 2019] E. Boo, S. Raza, J. Höglund, J. Ko. "FDTLS: Supporting DTLS-based Combined Storage and Communication Security for IoT Devices," IEEE International Conference on Mobile Ad-hoc and Smart Systems (IEEE MASS 2019), (Monterey, CA) Nov. 2019.

[Butun 2013] I. Butun, S. D. Morgera, and R. Sankar, “A survey of intrusion detection systems in wireless sensor networks,” IEEE communications surveys & tutorials, vol. 16, no. 1, pp. 266–282, 2013.

[Finne 2021] Niclas Finne, Joakim Eriksson, Thiemo Voigt, George Suciu, Mari-Anais Sachian, JeongGil Ko, and Hossein Keipour. "Multi-Trace: Multi-level Data Trace Generation with the Cooja Simulator." In 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS), pp. 390-395. IEEE, 2021.

[Li 2021] Li, X., Guimaraes, C., Landi, G., Brenes, J., Mangues-Bafalluy, J., Baranda, J., … Costa-Perez, X. (2021). Multi-Domain Solutions for the Deployment of Private 5G Networks. IEEE Access, 9, 106865–106884. doi:10.1109/access.2021.3100120

[Maman 2021] Maman, M., Calvanese-Strinati, E., Dinh, L.N. et al. Beyond private 5G networks: applications, architectures, operator models and technological enablers. J Wireless Com Network 2021, 195 (2021). https://doi.org/10.1186/s13638-021-02067-2

[Österlind 2006] F. Österlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, “Cross-level sensor network simulation with cooja,” in Proceedings of the First IEEE International Workshop on Practical Issues in Building Sensor Network Applications (SenseApp 2006), (Tampa, Florida, USA), Nov. 2006.

[Raza 2013] S. Raza, L. Wallgren, and T. Voigt, “Svelte: Real-time intrusion detection in the internet of things,” Ad hoc networks, vol. 11, no. 8, pp. 2661–2674, 2013.

[Tasi 2009] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, “Intrusion detection by machine learning: A review,” expert systems with applications, vol. 36, no. 10, pp. 11994–12000, 2009.

[Wagh 2013] S. K. Wagh, V. K. Pachghare, and S. R. Kolhe, “Survey on intrusion detection system using machine learning techniques,” International Journal of Computer Applications, vol. 78, no. 16, 2013.