Security and Trust in IoT networks: Network Intrusion Detection and Blockchain Transactions

Christos Profentzas, Charalampos Stylianopoulos, Magnus Almgren, Olaf Landsiedel, Marina Papatriantafilou
Chalmers University of Technology, Sweden - {chrpro, chasty, magnus.almgren, olafl, ptrianta}@chalmers.se

***Abstract*—With the introduction of the Internet of Things (IoT), physical objects now have cyber counterparts that create and communicate data. In order to use that data in a secure manner, it is essential to a) trust the devices that generate data and the way these devices interact with each other, b) protect the devices from malicious attacks and finally, c) record the data on permanent storage for further analysis of potential malicious behavior. Satisfying these requirements is challenging due to the resource- and energy-constrained nature of IoT devices, as well as their intermittent connectivity with the rest of the Internet. Our research directions focus on proposing solutions for these challenges.**

I. Intrusion Detection on Embedded Devices with GPUs

While IoT is becoming widespread, cyber security of its devices is still a limiting factor where recent attacks (e.g., the Mirai botnet) underline the need for countermeasures. One commonly-used security mechanism is a Network Intrusion Detection System (NIDS), but the processing needs of NIDS have been a significant bottleneck for large dedicated machines, and a show-stopper for resource-constrained IoT devices. However, the topologies of IoT are evolving, adding intermediate nodes between the weak devices on the edges and the powerful cloud in the center. Also, the hardware of the devices is maturing, with new CPU instruction sets, caches as well as co-processors. As an example, modern single board computers, such as the Odroid XU4, come with integrated Graphics Processing Units (GPUs) that support general purpose computing. Even though using all available hardware efficiently is still an open issue, it has the promise to run NIDS more efficiently.

In our work we introduce *CLort*, an extension to the well-known NIDS Snort that a) is designed for IoT devices b) alleviates the burden of pattern matching for intrusion detection by offloading it to the GPU. We thoroughly explain how our design is used as part of the latest release of Snort and suggest various optimizations to enable processing on the GPU. We evaluate *CLort* in regards to throughput, packet drops in Snort, and power consumption using publicly available traffic traces. *CLort* achieves up to 52% faster processing throughput than its CPU counterpart. *CLort* can also analyze up to 12% more packets than its CPU counterpart when sniffing a network. Finally, the experimental evaluation shows that *CLort* consumes up to 32% less energy than the CPU counterpart, an important consideration for IoT devices.

II. Recording IoT Transactions using Blockchain

For any distributed system, and especially for the Internet of Things, recording interactions between devices is essential. At first glance, blockchain seems to be suitable for storing these interactions, as they allow multiple parties to share a distributed ledger. However, at a closer look, blockchain requires heavy computations, large memory capacity, and always-on communication to the cloud; these are three properties that are challenging for IoT devices with limited resources.

In our work, we present IoTLogBlock to address these challenges. IoTLogBlock connects resource-constrained IoT devices to the blockchain, and it consists of three building blocks jointly enabling recording transactions: a lightweight contract signing protocol, a blockchain network, and a smart contract. The contract signing protocol allows devices to interact locally to perform transactions, even if no communication to the cloud and the blockchain exists at that moment. At a later time, devices forward the stored transactions to the blockchain, where a smart contract ultimately verifies the transactions.

We evaluate our design on low-power devices and quantify the performance in terms of memory, computation, and energy consumption. Our results show that a constrained device can create and sign a transaction on average of 3 s. Finally, we expose the devices in different network scenarios with an edge connection ranging from 15 min up to 2 h.