Security and Reliability in Pervasive Computing

Pietro Chiavassa

1 Abstract

The thesis presents research work exploring security and reliability in pervasive IoT systems. At first, these topics are closely analyzed in relation to state-of-the-art IoT technologies and infrastructures. Subsequently, two main fields of application are investigated: Particulate Matter (PM) monitoring with low-cost light-scattering sensors and secure intermittent computing (ImC) for energy harvesting systems.

Low-cost light-scattering PM sensors are often proposed as an IoT solution for the creation of dense monitoring networks. These devices are a miniaturization of traditional full-size optical particle counters (OPCs) and nephelometers. However, due to intrinsic technological limitations, they are often considered to be unreliable and imprecise. Multiple monitoring campaigns are conducted by placing a large number of low-cost PM sensors at an official monitoring site in the city of Turin, Italy. At first, the collected measurements are compared to the high-precision instruments of the Metropolitan City of Turin, to understand the benefits that their integration into the official monitoring network could provide. Secondly, a pipeline that performs failure detection, filtering, and calibration of these sensors is presented and evaluated on the collected data. Then, it is analyzed how the introduction of a duty cycle in their operation affects measurement quality. Finally, an improved version of a low-cost monitoring station is designed, together with the entire IoT infrastructure, to transmit, store, and visualize the collected measurements. The infrastructure also provides data validation functionalities by storing the hash of the collected data inside a blockchain.

In the context of intermittent computing, instead, a secure checkpointing utility is designed and tested on a target architecture supporting a Trusted Execution Environment (TEE): ARM Truszone for Cortex-M. Differently from other state-of-the-art approaches, the entire security chain of the platform is considered. This results in a solution that is directly applicable without the need for custom or hardware non-available MCU features. The performance of the utility is compared with other state-of-the-art works, by also evaluating the lifetime of the device.