Ph.D. Project: IoT Security Techniques

Work Package 2

Advisors: Cíntia Borges Margi and A. Chorti (ENSEA)

Abstract

This project proposes the development of IoT security techniques and their integration in IoT platforms. In particular, we will focus on the requirements for the design of a secure SDN-based framework, such as: communication protocols, node programming middleware, communication and computation resource management features and security services. Moreover, we also plan to integrate the contributions from other tasks from the workpackage (such as PLS, key generation and techniques for prevention and mitigation of DDoS Attacks) with a view to building long-term security solutions for IoT networks.

1 Scholarship Requirements

The fellowship will be granted to a student of PPGEE/EPUSP (Graduate Program in Electrical Engineering (PPGEE) - Escola Politécnica da Universidade de São Paulo). Information about the application process for PPGEE is available at `http://ppgee.poli.usp.br/?page_id=1914`.

Notice the application period is 02/05/2019 to 17/05/2019.

The Direct Doctorate scholarship is intended for students who are regularly enrolled in stricto sensu post-graduate programs of public or private higher education institutions in the State of São Paulo, without the title of master, for the development of a research project that results in thesis. The analysis of direct doctoral scholarship applications prioritizes a candidate who has just graduated, within the normal term of his / her term with an excellent academic record and, preferably, a successful scientific initiation stage. More information at: `http://www.fapesp.br/bolsas/dd`

2 Goals

IoT networks will require security guarantees and protocols in the future in order to become suitable for adoption in many envisaged applications whose information security is of utmost importance. Several approaches to ensuring security have been reported in the last decade or so. However, they have not been specifically tailored to IoT networks and their applications. Concerning security, we intend to address the main services, the type of algorithms to achieve them, and how their secure implementation is needed to avoid attacks. Wireless sensor networks' (WSN) challenges due to resources constraints have been faced in different ways. One of those ways is using collaborative techniques to minimize the consumption of scarce resources, concept we propose to exploit.

3 Methods

The student will initially perform a literature review in the subjects of security techniques, including SDN approach (and mainly the IT-SDN framework, which will be used as its basis), IoT networks and network security. During the initial phase, the student will also take courses on sensor networks, computer networks and hardware design. These two tasks will be completed during the first year of work. At the beginning of the second year the student will take the qualifying exam, and start the research by first reproducing known algorithms in simulations that takes into account the specific aspects of the IoT environment. At the end of the second year, the student should propose the first algorithms to achieve our goal and evaluate them in IoT scenarios using simulations and IoT platforms. In the third and fourth years, the student will work on security issues related to SDN-based platforms, developing techniques and protocols, and will integrate the techniques developed so far. In addition, in the third and fourth years the student will write papers and the dissertation. We expect that the research will result in two or three conference and two journal papers.