Smart Grids Cyberphysical Security

Thesis subject IETR/IRISA

Keywords: Intrusion detection, Cyber-resilience-methods-attack-resistance, Cyber-physical security, Observer synthesis for detection

Localisation: CentraleSupélec, campus de Rennes, France

Laboratories: - IETR - Institut d'Electronique et des technologies du numérique, équipe Automatique
- IRISA - Institut de Recherche en Informatique et Systèmes Aléatoires, équipe Pirat

Date : April/May 2025 - 2028

General context

In the critical context of intelligent energy management, the cybersecurity of connected infrastructures is a crucial issue: the information systems that drive the physical systems are the target of growing threats, and the safety of the operations must be guaranteed. This physical dimension of cybersecurity is in addition to the classic aspect of securing networks and their nodes: we speak of cyber-physical security. Most current work on security is compartmentalized, studying the problem in a highly disciplinary way. This thesis aims to define new detection and remediation methods against attacks targeting energy management systems in buildings equipped with electrical production and connected to the power grid. The hypothesis adopted for this thesis project is that an attacker can corrupt one or more system components (a sensor, a PLC, an inverter), components that do not host a security solution for technical and economic reasons. It is then impossible to detect the compromise in isolation, and only an analysis of the system as a whole, exploiting the inconsistencies between the digital dimension of sensor data and the physical and energy dimensions, can detect the compromise.

To make the most of energy interactions between components, the proposed approach is based on the implementation of consumption and production models, which will be helpful in the synthesis of observers and state estimators. By combining these tools with low-level compromise study approaches, we hope to develop new detection and mitigation mechanisms. This trans-disciplinary combination offers an original working approach in a very concurrent field. The PhD candidate must test the results on the laboratory's "Smart And Secure Room" platform.

Work description

One of the first objectives of the thesis is to provide an experimental framework that can collect traces (digital and physical) in an IoT system coupled to an energy network. The second objective is to simulate and emulate realistic attacks (IoT, energy production automaton) to label the dataset with ground truth. These scenarios will serve as a benchmark to the community, and the experimental data can be valorized as a dataset so that the community can test compromise detection methods. The scientific challenges underlying these objectives are linked to the difficulty

of labeling and certifying heterogeneous datasets, which consider the diversity of protocols and the different physical natures of signals.

The second part of the thesis will be devoted to attack detection in Smart-Grids, a subject in which the literature has proliferated over the past two years. The methods developed exploit observer synthesis techniques but are always limited to the "high" level in a particular context: a given type of attack on a specific element. In our case study, the assumption is that the connected objects (sensors, actuators, inverters, etc.) contributing to the management of the energy network are not equipped with security systems. It is, therefore, not possible to detect compromise at the component level, but rather from a global perspective. Therefore, the inherent scientific challenge is to study the vulnerability of the energy system in its whole by combining the different levels of study, which requires a trans-disciplinary construction that we intend to exploit.

The third objective of this thesis is to design models linking energy consumption and production with other physical quantities based on the data collected. The models obtained will be used to predict the system's proper functioning as a whole. This approach will enable us to develop detection methods based on observed traces coupled with the determined energy models, representing an actual departure from existing work. These detection methods will be tested in simulation and real-life experimentation using the "Smart And Secure Room" platform, an IETR and IRISA experimental platform dedicated to energy system vulnerabilities (https://www.ietr.fr/smart-and-secure-room).

Profile and skills

The profile required for this work is that of a student with a solid grounding in automatic control (observer synthesis) and an understanding of the energy system and/or computer science. Proficiency in Matlab/Simulink is also desirable, as is computer development (Python, Java or C).

To apply

Send an e-mail to Romain Bourdais (romain.bourdais@centralesupelec.fr) and Jean-François Lalande (jean-francois.lalande@centralesupelec.fr), along with a short CV and recent transcripts.

The deadline for applications is 01/03/2025.