POST DOC POSITION (24 MONTHS)

CAMTAR: Collecting Attacks in MoniTored and Autonomous Room

INTRODUCTION

Cybersecurity of critical infrastructures (energy networks, industrial processes, water production plants, etc.) is a national and sensitive issue. Within these infrastructures, the information collected, transmitted, and processing results in actions on physical systems whose proper functioning is essential for society.
Beyond the cybersecurity of control systems, which is the first level, it is necessary to extend the security considerations by considering the possible cooperation between the physical dimensions of the systems, the sensors, and the information systems. Indeed, physical systems carry information and the possibility of action. This global consideration leads to the concept of cyber-physical security, which is at the center of this research project and offers real challenges [1].

These issues can be addressed either by a "cyber security" approach: research in this area that focuses on physical systems depends on the technologies used. The security challenges are also particular [4,5]. Consequently, it is challenging to evaluate the effectiveness of cybersecurity solutions (detection, protection of a system, tolerance to an attack). Therefore, researchers often use simulators representing the system or protocols involved [2,3]. Even if these approaches are tolerable, e.g. for protocol design, it is not reasonable to work on the resistance to a network attack on a sensor or the analysis of a compromised firmware. No dataset for the connected objects of an intelligent and zero-net building exists to date. Consequently, the reproducibility of results is very difficult, and the community cannot rely on such datasets to design their contributions.

They can also be treated from a control science point of view: indeed, the exchanges between agents can be complex, but modern control science techniques should allow, by observing them, to understand and characterize them to set up monitoring procedures to detect a behavior change.
Therefore, one possible course of action is to set up adaptive estimation techniques to detect corruption of one of the agents of the energy system. These estimations can be done both on the observation of the physical quantities of the network (energy vector) or the communication signals exchanged by the agents, thus participating in the cyber-physical security of the energy network.

SCIENTIFIC AND TECHNICAL ISSUES

The "smart and secure room" platform consists of a room, a photovoltaic energy production system, and a set of sensors that enable the room's users to make decisions. The sensors allow building different types of networks: short-range (zigbee, z-wave), medium-range (wifi, lora), long-range (IP). This platform enables to play automation scenarios, for example, to regulate the energy produced and automatically predict the room's heating according to the users' actions (voluntary ventilation, door opening). Therefore, the platform is capable of recording scenarios representative of its use and can host simulated attacks.

For a candidate with a "cybersecurity" oriented profile, this research project seeks to achieve the following objectives:

- To develop a benchmarking platform for cybersecurity analysis of a connected component of an energy system: evaluation of the degree of software vulnerability, the capacity for intrusion, and harm in the energy system.
- To collect traces (network, system) for the constitution of a dataset allows to work a posteriori on detection methods (machine learning, correlation of alerts).
- To propose mediation methods for piloting an autonomous energy building undergoing a cyber attack.

POST-DOCTORAL RESEARCH – IRISA/IETR - CentraleSupélec

For a candidate with a "control-science" oriented profile, this research project seeks to achieve the following objectives:

- To characterize the nominal behavior of the exchanges between the energy system agents. As developed within the team [6,7], online parameter estimation techniques are the first track to be privileged.
- To understand the impact of non-cooperative behavior on these parameters. These studies could also contribute to identifying the most vulnerable elements of the energy system and those that can be the most destabilizing for the network.
- To propose real-time methods for detecting changes in the behavior of the various agents. This detection must allow the rest of the agents to review their organization and their decision-making because of the agent's corruption to preserve the proper functioning of the network.

SALARY

The annual gross salary is 48K€.

APPLICATION

Send an email to Jean-François Lalande (jean-francois.lalande@centralesupelec.fr) and Romain Bourdais (romain.bourdais@centralesupelec.fr) with a motivation letter, a short CV, and a transcript of academic records. The candidate has to have spent more than 18 months out of France since 2018. Only appropriate and complete applications will be considered.

REFERENCES BIBLIOGRAPHIQUES

[1] I. Ahmad, M. K. Zarrar, T. Saeed and S. Rehman, "Security Aspects of Cyber Physical Systems," 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, 2018

[2] Xianghui Cao et al. “Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks”. In: IEEE Internet Things J. 3.5 (Oct. 2016), pp. 816–829. issn: 2327-4662.

[3] David Airehrour, Jairo A. Gutierrez, and Sayan Kumar Ray. “SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things”. In: Future Generation Computer Systems 93 (2019), pp. 860–876. issn:0167-739X.

[4] Mardiana binti Mohamad Noor, Wan Haslina Hassan, Current research on Internet of Things (IoT) security: A survey, Computer Networks, Volume 148, 2019, Pages 283-294.

[5] M. M. Hossain, M. Fotouhi and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," *2015 IEEE World Congress on Services*, 2015, pp. 21-28, doi: 10.1109/SERVICES.2015.12.

[6] Y. Pan, S. Aranovskiy, A. Bobtsov, H. Yu. *Efficient learning from adaptive control under sufficient excitation*. International Journal of Robust and Nonlinear Control, vol. 29, no. 10, pp. 3111-3124, 2019.

[7] Aranovskiy S., Bobtsov A., Ortega R., Pyrkin A.. *Performance Enhancement of Parameter Estimators via Dynamic Regressor Extension and Mixing*, IEEE Transactions on Automatic Control, vol. 62, no 7, pp. 3546-3550, 2017.