Cybersecurity with Machine Learning for industrial networks

We invite applications for a fully funded joint Ph.D research position between:

- Technology & Strategy (https://www.technologyandstrategy.com), Strasbourg, France
- ICube Lab (http://icube.unistra.fr), CNRS / University of Strasbourg, France

The position is for 36 months (the usual duration in France for a PhD)

Keywords: AI technologies, Machine Learning, Cybersecurity, Intrusion Detection, Anomaly Detection, Outliers

Application

Industry 4.0 is the novel industrial revolution, where objects are connected to a global network infrastructure. Fieldbus (e.g., CAN [1], modbus [2], TSN [3]) interconnect the different devices to controllers. These objects are constrained in memory and computational capacity and may endanger the network infrastructure if they are corrupted. They may even jeopardize the safety of industrial applications.

Thus, cybersecurity for the Industrial Internet of Things is a major concern, while most of the technologies in this area have not been designed with this problem in mind. For instance, CAN communications are neither ciphered, nor authenticated.

We need to deploy Intrusion Detection Systems able to detect anomalies, i.e., when the infrastructure doesn’t behave as expected. It may come from e.g., a human misconfiguration, an attack.

Scientific Objectives

Penetration testing already exploits Machine Learning techniques (e.g., [4]) to detect and identify attacks. Indeed, signature-based solutions are not sufficient since they may disguise themselves into a legal traffic flow but inserting noise [5].

We want to go there further, to identify anomalies that may be e.g., attacks, misconfigurations, faults. Industrial networks are known to be predictable [6] and we must identify outliers. Some work exists that consider the spatial and temporal correlations [7] but they are application specific, i.e., they need to manipulate directly data chunks. Approaches exist that exploit a RNN to identify anomalies [8], but we are convinced that industrial networks are predictable, and techniques that exploit this predictability should be more accurate. The network controller that has a complete knowledge of the network topology may efficiently detect intrusions [9].

The objective of this PhD thesis is to first propose techniques to identify automatically patterns when exploiting the list of packets transmitted in the network infrastructure. Indeed, a networked control application relies on a control loop (sensor à controller à actuator) to control the Cyber Physical System (CPS). It is important to characterize each of these control loops (period, source / destination, correlations, etc.) [10]. The PhD student will both exploit existing datasets as well as the networked control system testbed deployed at Technology & Strategy.

Then, we will derive Network Intrusion Detection Systems (IDS) to identify anomalies for each of these control loops, extending what has been done for home networks [11], or generic IP networks [12]. We need to propose techniques to define what corresponds to a *normal* state, and what corresponds to an outlier / anomaly. The proposition must be sufficiently robust to detect sophisticated attacks such as the Schedule-Based Attacks [9].

[1] H. Olufowobi, C. Young, J. Zambreno, et G. Bloom, « SAIDuCANT: Specification-Based Automotive Intrusion Detection Using Controller Area Network (CAN) Timing », *IEEE Trans. Veh. Technol.*, vol. 69, n° 2, p. 1484-1494, févr. 2020, doi: 10.1109/TVT.2019.2961344.

[2] N. Goldenberg, « Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems », *Int. J. Crit. Infrastruct. Prot.*, p. 13, 2013, doi: 10.1016/j.ijcip.2013.05.001.

[3] J. Farkas, « IEEE 802.1 TSN - An Introduction », p. 18, 2019.

[4] A. Chowdhary, D. Huang, J. S. Mahendran, D. Romo, Y. Deng, et A. Sabur, « Autonomous Security Analysis and Penetration Testing », in *2020 16th International Conference on Mobility, Sensing and Networking (MSN)*, Tokyo, Japan, déc. 2020, p. 508-515. doi: 10.1109/MSN50589.2020.00086.

[5] N. Wang, Y. Chen, Y. Hu, W. Lou, et Y. T. Hou, « MANDA: On Adversarial Example Detection for Network Intrusion Detection System », in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, Vancouver, BC, Canada, mai 2021, p. 1-10. doi: 10.1109/INFOCOM42981.2021.9488874.

[6] M. R. Moore, R. A. Bridges, F. L. Combs, M. S. Starr, et S. J. Prowell, « Modeling inter-signal arrival times for accurate detection of CAN bus signal injection attacks », in *Annual Conference on Cyber and Information Security Research*, 2017, p. 4. doi: 10.1145/3064814.3064816.

[7] G. Han, J. Tu, L. Liu, M. Martinez-Garcia, et Y. Peng, « Anomaly Detection Based on Multidimensional Data Processing for Protecting Vital Devices in 6G-Enabled Massive IIoT », *IEEE Internet Things J.*, vol. 8, n° 7, p. 5219-5229, avr. 2021, doi: 10.1109/JIOT.2021.3051935.

[8] M. Abdel-Basset, V. Chang, H. Hawash, R. K. Chakrabortty, et M. Ryan, « Deep-IFS: Intrusion Detection Approach for Industrial Internet of Things Traffic in Fog Environment », *IEEE Trans. Ind. Inform.*, vol. 17, n° 11, p. 7704-7715, nov. 2021, doi: 10.1109/TII.2020.3025755.

[9] S. Hounsinou, M. Stidd, U. Ezeobi, H. Olufowobi, M. Nasri, et G. Bloom, « Vulnerability of Controller Area Network to Schedule-Based Attacks », in *2021 IEEE Real-Time Systems Symposium (RTSS)*, Dortmund, DE, déc. 2021, p. 495-507. doi: 10.1109/RTSS52674.2021.00051.

[10] U. Ezeobi, H. Olufowobi, C. Young, J. Zambreno, et G. Bloom, « Reverse Engineering Controller Area Network Messages Using Unsupervised Machine Learning », *IEEE Consum. Electron. Mag.*, vol. 11, n° 1, p. 50-56, janv. 2022, doi: 10.1109/MCE.2020.3023538.

[11] P. Illy, G. Kaddoum, K. Kaur, et S. Garg, « ML-Based IDPS Enhancement With Complementary Features for Home IoT Networks », *IEEE Trans. Netw. Serv. Manag.*, vol. 19, n° 2, p. 772-783, juin 2022, doi: 10.1109/TNSM.2022.3141942.

[12] A. Blaise, « Novel anomaly detection and classification algorithms for IP and mobile networks », Sorbonne Université, Paris, 2020.

Location

The PhD student will be co-hosted by Technology & Strategy and the University of Strasbourg, both located in Strasbourg, France.

Technology & Strategy was created in 2008 in Strasbourg. Specialized in Engineering, IT, Digital and Project Management, Technology & Strategy is a reference partner for its customers in the development of innovative projects. Technology & Strategy also has an integrated engineering service to meet the requirements of its customers who are primarily R&D departments of industrial companies.

With a strong international focus and a Franco-German DNA, Technology & Strategy is proud of its 1,800 employees and is present with more than 40 nationalities in 16 offices in 6 countries (France, Germany, Switzerland, Belgium, UK, South East Asia). Technology & Strategy is proud to keep its headquarters in the East of France, near Strasbourg.

Since its creation, Technology & Strategy has specialized in the development of embedded solutions for real time applications integrating both software and electronics. Our activities have a strong orientation on the automotive market covering active and passive safety systems (e.g. autonomous vehicle) but also the whole control-command part (engine), and the energy supply (battery, fuel cell).

Our know-how has since been extended to mechatronic systems by integrating the mechanical component. With this knowledge and noting the increasing importance of intelligent and connected systems in the industry, part of the know-how has been transferred to this field and expanded to new know-how such as virtual reality, augmented reality, cybersecurity, artificial intelligence, Big Data and multiphysics modeling.

Founded in the 16th century, the University of Strasbourg has a long history of excellence in higher education, rooted in Renaissance humanism. The University of Strasbourg is a public research university located in Strasbourg, with over 52,000 students.

With its 2 universities, 12 *Grandes Ecoles*, 250 laboratories and over 4,300 researchers, Alsace is the third largest scientific hub in France

A city mixing cultural diversity and firmly rooted traditions, Strasbourg is the country's top city for international students**.** Its human size, its pedestrian city center and 500 km of cycling paths make it a very pleasant city to wander around. Vibrant and affordable, Strasbourg is a true student city providing a great learning and living environment.

Skills

Applicants should have solid skills in:

- Excellent knowledge of Machine Learning techniques (not only as a user);
- Excellent data science language skills (R, or Python);
- Background knowledge to implement measurements in a real production line;
- Excellent communication and writing skills. Note that knowledge of French is not required for this position.

Knowledge of the following technologies is not mandatory but will be considered as a plus:

- Knowledges in industrial networking protocols and stacks;
- Knowledges of embedded software

Application

Applications should be submitted by email to tands-cifre@icube.unistra.fr.

They must include:

- A Curriculum Vitae;
- List of 2 or 3 references to contact (position, email address);
- Transcripts of undergraduate and graduate studies;
- Link to MSc thesis, and publications if applicable;
- Link to personal software repositories (e.g. GitHub)

Please prefix the filenames of your application with your lastname.