Networks Research Group
Cybersec-TS-Icube

PhD thesis
2023–2026

Cybersecurity with Machine Learning for industrial networks

Location	Network research group – ICube (UMR CNRS 7357), University of Strasbourg (France) Technology & Strategy, Strasbourg (France)
Supervision	Dr. Fabrice THÉOLEYRE (fabrice.theoleyre@cnrs.fr) Dr. Baptiste LAFABREGUE (lafabregue@unistra.fr) Thomas Gaberan (t.gaeran@technologyandstrategy.com)

Keywords

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

Context

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]. 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].

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.

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

Please send an email to fabrice.theoleyre@cnrs.fr comprising :

- A detailed CV ;
- Your possible list of publications if applicable ;
- Transcripts of undergraduate and graduate studies ;
- List of 2 or 3 references to contact (position, email address) ;
- A cover letter.

Références

[1] Habeeb Olufowobi, Clinton Young, Joseph Zambreno, and Gedare Bloom. Saiducant : Specification-based automotive intrusion detection using controller area network (can) timing. IEEE Transactions on Vehicular Technology, 69(2) :1484–1494, 2020.

[2] Niv Goldenberg and Avishai Wool. Accurate modeling of modbus/tcp for intrusion detection in scada systems. International Journal of Critical Infrastructure Protection, 6(2) :63–75, 2013.

[3] Norman Finn. Introduction to time-sensitive networking. IEEE Communications Standards Magazine, 6(4) :8–13, 2022.

[4] Ankur Chowdhary, Dijiang Huang, Jayasurya Sevalur Mahendran, Daniel Romo, Yuli Deng, and Abdulhakim Sabur. Autonomous security analysis and penetration testing. In 2020 16th International Conference on Mobility, Sensing and Networking (MSN), pages 508–515, 2020.

[5] Ning Wang, Yimin Chen, Yang Hu, Wenjing Lou, and Y. Thomas Hou. Manda : On adversarial example detection for network intrusion detection system. In IEEE INFOCOM 2021 - IEEE Conference on Computer Communications, pages 1–10, 2021.

[6] Michael R. Moore, Robert A. Bridges, Frank L. Combs, Michael S. Starr, and Stacy J. Prowell. Modeling inter-signal arrival times for accurate detection of can bus signal injection attacks : A data-driven approach to in-vehicle intrusion detection. In Proceedings of the 12th Annual Conference on Cyber and Information Security Research, CISRC '17, New York, NY, USA, 2017. Association for Computing Machinery.

[7] Guangjie Han, Juntao Tu, Li Liu, Miguel Martínez-García, and Yan Peng. Anomaly detection based on multidimensional data processing for protecting vital devices in 6g-enabled massive iiot. IEEE Internet of Things Journal, 8(7) :5219–5229, 2021.

[8] Mohamed Abdel-Basset, Victor Chang, Hossam Hawash, Ripon K. Chakrabortty, and Michael Ryan. Deep-ifs : Intrusion detection approach for industrial internet of things traffic in fog environment. IEEE Transactions on Industrial Informatics, 17(11) :7704–7715, 2021.

[9] Sena Hounsinou, Mark Stidd, Uchenna Ezeobi, Habeeb Olufowobi, Mitra Nasri, and Gedare Bloom. Vulnerability of controller area network to schedule-based attacks. In 2021 IEEE Real-Time Systems Symposium (RTSS), pages 495–507, 2021.

[10] Uchenna Ezeobi, Habeeb Olufowobi, Clinton Young, Joseph Zambreno, and Gedare Bloom. Reverse engineering controller area network messages using unsupervised machine learning. IEEE Consumer Electronics Magazine, 11(1) :50–56, 2022.

[11] Poulmanogo Illy, Georges Kaddoum, Kuljeet Kaur, and Sahil Garg. Ml-based idps enhancement with complementary features for home iot networks. IEEE Transactions on Network and Service Management, 19(2) :772–783, 2022.