PhD Thesis Proposal 2023-2026

Title: Petri Net Formalisms for Attacks Detection in Networked Control Systems

Laboratories	Laboratoire d'Informatique et Systèmes (LIS – UMR CNRS 7020) Groupe de Recherche en Electrotechnique et Automatique du Havre (GREAH - EA 3220)
Research groups	Modèles et Formalismes à Evénements Discrets (MoFED - LIS) Commande et Sûreté de Fonctionnement des Systèmes (CSFS - GREAH)
Supervisors	Pr. Isabel Demongodin (LIS), Pr. Dimitri Lefebvre (GREAH), Dr. Rabah Ammour (LIS)
Funding, Duration and, Starting date	Funding available for a 3 years contract with a flexible starting date around September/October 2023.
Location	The PhD work will be carried out in the LIS laboratory located in Marseille, France She/he will be registered at École Doctorale de Mathématiques et Informatique (ED 184) Several visits to the GREAH laboratory will be planned throughout the thesis period
Project	This PhD proposal is a part of project MENACES (Timed Event-Based Methods for Networked Control Systems Security) funded by the French National Research Agency (ANR).

Context:

Security against cyber-attacks is one of the main challenges for Industry 4.0 and in particular for networked control systems (NCSs). Considered as a special form of cyber-physical systems, NCSs are control systems in which the system to be controlled and the various components such as actuators, controllers, and sensors are spatially distributed while communication between these components is achieved by using a digital communication network that is shared by other applications and control systems. This type of implementation differs significantly from conventional control systems, where all components of the system are directly connected to the controllers and exchange information using dedicated wiring. In industry, NCSs offer many advantages, such as cost-efficiency and improved functionality, but new problems arise with the use of this control implementation. One of them is the security issue for NCSs [1] and more generally for Industry 4.0. Indeed, the communication capabilities of NCSs make them more vulnerable to various threats and cyberattacks with major potential consequences for users. More specifically, cyberattacks may cause the interruption of the operations, and worst, could manipulate the control process to threaten the system integrity. For instance, malicious intruders can corrupt the measurements of remote sensors in the NCS that will lead in return to wrong control inputs. This leads the physical system to possibly reach undesirable and critical operational conditions. In recent years, several cyberattacks have been performed against NCSs and, according to the latest IBM Security report, the manufacturing sector has become in 2021 the second most targeted sector for cyberattacks. In this context, the proposed research work aims to propose a framework of models and methods to track the system behaviour and generate an alarm at earliest once the system is attacked improving the early detection schemes of cyberattacks in NCSs.

Objectives:

Various works can be found in the literature related to the security issues of cyber physical systems and more specifically to cyberattacks. Recently, by a systematic mapping methodology, the authors of [2] present a powerful comparison framework for existing research on this topic. From a control perspective, the development of efficient algorithms and architectures for the detection of cyberattacks in NCSs is an active and expanding area of research [3]. The heterogeneity of the NCS components and the continuous emergence of new threats make the cyberattacks detection issue very challenging. Using model-based

methods, is a very suitable approach as the model describes the states as well as the behaviour of the system allowing from the temporal analysis of orders/reports sequences to track the evolution of the system to a critical state and to predict any attack to the sensor or controller data by comparing the expected output with the received sequence. In this context, discrete event systems (DES) theory has proved to be a powerful tool for the modelling of dynamical complex systems and a plenty of formalisms allows model-based methods to be applied. Despite the recent advances in this theory, improvements of the existing formalisms and theoretical developments are still needed to cope with the modelling and analysis of NCSs for detecting cyberattacks considering temporal aspects such as communication delays. For this purpose, the **first objective of this research will be to represent NCSs with suitable DES formalisms to capture the temporal altered behaviour of such complex systems**.

Then, the detection scheme will be based on the analysis of the sequences of (possibly altered) control orders and sensor reports, with regard to the behaviour of the timed model of the process. In particular, the research focuses on the design of some particular detection structures used in the detection schemes: verifiers (used to reformulate event detection problems with state isolation properties), observers (used to solve state estimation problems), and detectors (used to reduce the computational complexity of observers). The detection schemes rely on the discrimination of not only logical deviations of the system behaviour but also any temporal inconsistencies caused by the attack. To achieve this goal, the central question that will be addressed is to study the timing aspects, i.e., the time samples associated with the exchanged data between the controller and the plant in order to improve the attack detection. Such aspects have been rarely considered thus far and existing approaches are mainly based on the logical or untimed behaviour of the studied systems [4]. For this purpose, **the second objective will be to develop DES model-based methods with temporal aspects for the detection scheme of stealthy attacks on NCSs.** Consequently, this work aims to study scientific issues regarding the timing aspects, the proposed approaches will be implemented and validated in simulation and on a testbed platform.

Methodology:

Discrete Event Systems (DESs) are dynamical systems whose dynamics depend on the interaction of asynchronous discrete qualitative changes called events [5]. For the modelling and analysis of such systems, DES theory provides mathematical abstractions and formalisms including automata and Petri nets (PNs) [6]. Considering the security of NCS, suitable modelling formalisms are needed to cope with this issue. For this purpose, a preliminary work on the modelling aspects has led to the development of a new formalism called Output Synchronized Petri Nets (OutSynPNs) [7]. OutSynPNs are derived from synchronized Petri nets (SynPNs) where input events (symbols) are associated with the transitions. To model the sensor's information delivered during the functioning of the NCS, SynPNs are enriched with output events (labels) to form OutSynPNs. Thus OutSynPNs allow to provide an abstracted discrete event model of a considered NCS along with its associated input/output information that circulates through the network between the controller and the plant. Some preliminary works on observer [7, 8, 11] and vulnerability analysis [8, 10] have already been proposed on automata and particularly on Labeled Finite Automata with Inputs (LFAI), i.e., the state space representation of an OutSynPN model. A first step of this research work is to extend to temporal aspects the formalism of OutSynPNs in order to model the temporal behaviour of the NCS. The temporal semantics of this new formalism will be defined, and its properties will be studied.

For improving the detection methods of cyberattacks that exploit the temporal aspects, two steps will be considered.
A first step is to develop timed verifiers and to compose these new structures with logical observers or detectors. In this case, the timing aspects will be restricted to the system behaviours whereas the observers/detectors ignore such aspects. The challenge is to adapt existing timed composition operators or to propose new operators that will be suitable to design timed verifiers. The advantage of such timed verifiers is to allow the capture of the timing aspects of the system and attack in a single structure.
A second and more challenging step is to also include timing aspects in the observers/detectors. This study will start from some preliminary works about region automata. The advantage of a timed observer is to

embed explicitly the timing aspects. With this structure it will become possible to detect an attack not only because the sequence of observed events (symbols and labels) is different from the sequence that one can expect but also because the timestamps of the events are inconsistent with the dynamics of the systems in normal conditions. Consequently, we expect to improve attack detection to a class of attacks that remain stealthy from a logical perspective.

Moreover, another ambition is to investigate the modelling of the hybrid aspects of the NCS. The idea for the modelling of NCSs is to exploit the hybrid PN formalisms, such as generalised batches Petri nets (GBPNs) formalisms [12, 13] designed for systems that include not only delays but also various speeds [14]. A first step will be to adapt the timed verifier developed to the GBPN formalism. To do so, an "hybrid" LFAI that captures the continuous-time and event driven dynamics of such hybrid formalism has to be defined. Next, both formalisms, timed OutSynPNs and (extended) controlled GBPNs, will be merged for studying the attacks of hybrid physical systems in terms of delay and speed.

Expected profile of the PhD candidate:

The candidate should have a strong background in automation and/or computer science and good programming skills (Matlab, C/C++ or Python, knowledge of mathematical libraries). A good knowledge about discrete event systems including Petri nets and automata will be appreciated. He/she must be motivated by research in security of networked control systems and able to work in a multidisciplinary team.

Send by **may 10, 2023**: a CV, a cover letter (explaining the motivations and the choice of the thesis topic), transcripts of previous 3 years (including the current one), references and, internship/project reports to rabah.ammour@lis-lab.fr, in preparation for a potential interview.

Keywords: Discrete Event Systems, Petri nets, networked control systems security, attacks detection.

References

[1] Sandberg H., Amin S., and Johansson K. H. (2015). Cyberphysical security in networked control systems: An introduction to the issue. IEEE Control Systems Magazine, 35(1), 20-23.
[2] Lun, Y. Z., D'Innocenzo, A., Smarra, F., Malavolta, I., and Di Benedetto, M. D. (2019). State of the art of cyber-physical systems security: An automatic control perspective. J. of Systems and Software, 149, 174-216.
[3] Mao Y., Jafarnejadsani H., Zhao P., Akyol E., and Hovakimyan N. (2020). Novel stealthy attack and defense strategies for networked control systems. IEEE Trans. on Automatic Control, 65(9), 3847-3862.
[4] Fritz R., Schwarz P., and Zhang P. (2019). Modeling of cyberattacks and a time guard detection for ICS based on discrete event systems. European Control Conference (ECC).
[5] Cassandras C. G. and S. Lafortune (2008). Introduction to Discrete Event Systems, Springer.
[6] David R., and Alla H. (2010). Discrete, continuous, and hybrid Petri nets. Berlin: Springer.
[7] Ammour R., Amari S., Brenner L., Demongodin I., and Lefebvre D. (2021). Observer design for output synchronized Petri nets. European Control Conference (ECC).
[8] Ammour, R., Amari, S., Brenner, L., Demongodin, I., & Lefebvre, D. (2022). Observer design for labeled finite automata with inputs under stealthy actuators attacks. *16th IFAC Workshop on Discrete Event Systems WODES*, Sep 2022, Prague, Czech Republic. pp.46-51, ⟨10.1016/j.ifacol.2022.10.322⟩. ⟨hal-03879792⟩
[9] Ammour R., Amari S., Brenner L., Demongodin I., and Lefebvre D. (2021). Costs analysis of stealthy attacks with bounded output synchronized Petri nets. IEEE Int. Conf. on Automation Science and Engineering (CASE), 799-804.
[10] Ammour, R., Amari, S., Brenner, L., Demongodin, I., & Lefebvre, D. (2023). Robust stealthy attacks based on uncertain costs and labeled finite automata with inputs. *IEEE Robotics and Automation Letters*. doi: 10.1109/LRA.2023.3250007.
[11] Hadjicostis C. N. (2020). Estimation and Inference in Discrete Event Systems. Springer Int. Publishing.
[12] Demongodin I. (2001). Generalised batches Petri net: hybrid model for high-speed systems with variable delays. Discrete Event Dynamic Systems, 11(1), 137-162.
[13] Liu R., Ammour R., Brenner L., and Demongodin I. (2020). Event-driven control for reaching a steady state in controlled generalized batches Petri nets. IFAC-PapersOnLine, 53(4), 180-186.
[14] Demongodin I., and Giua A. (2014). Dynamics and steady state analysis of controlled Generalized Batches Petri Nets. Nonlinear Analysis: Hybrid Systems, 12, 33-49.