Doctorate Thesis with scholarship

Doctoral School Orléans-Tours MIPTIS. PhD in Automatic Control.

Subject: **Secure event-based interval observer for resilient stabilization of cyber-physical systems.**

PhD Superviseur (*Directeur de thèse*): **Prof. Nacim Ramdani**
Research center (*Laboratoire d'accueil*): **PRISME EA 4229 Univ. Orléans,**
Location: PRISME, campus de Bourges, av. de Lattre de Tassigny, 18000 **Bourges**.
Personal webpage: https://agora.bourges.univ-orleans.fr/ramdani/

Scientific objective. Most of today's critical infrastructures, such as energy supply networks, water distribution networks, and autonomous vehicle fleets, are distributed Cyber-Physical Systems (CPS) that operate in highly networked environments as they need to communicate remotely with control and management systems. The tight integration of information, communication, and computation with physically engineered systems that constitutes distributed CPS make them more vulnerable to cyber-physical attacks and unwanted access, while until recently, their security has often been an afterthought. The cyber-physical attacks correspond to customized, malicious and active inputs that continuously increase in complexity as the CPS evolves, while deploying proven IT security technology alone neither is a viable solution nor can mitigate the impact of adversarial attacks [1]. Therefore, it is of prime importance to develop secure and resilient-by-design solutions for the control and operation of CPS [2-4].
Secure observers and secure state estimation are a viable strategy to achieve resiliency to adversarial attacks in CPSs when several sensors and actuators are available [5-9]. The idea is to equip CPSs with algorithms that reconstruct the actual system state despite attacks on sensors or actuators, while knowing only an upper bound on the relative of number of manipulated sensors and actuators, and without knowing their identities. For instance, in case of sensor attacks, secure observers use a family of observers sharing a single dynamical equation for the states, but different output equations, to generate estimates corresponding to different subsets of sensors. This problem is in general NP-hard. Given an upper bound on the number of attacked sensors, and so-called sparse observability condition (assuming that the unmeasurable state vector can be reconstructed using the unknown subset of safe sensors) scalable algorithms have been proposed combining Luenberger observers and satisfiability checkers.
The Doctoral Thesis aims to develop new attack-resilient set-theoretic estimators that can reconstruct the state vector with guaranteed uncertainty intervals even if a subset of sensors or actuators are subject to adversarial attacks. The thesis will consider switched systems in presence of multi-rate aperiodic sampling, and sparse cyber-physical attacks on sensors and actuators, while leveraging the interval impulsive observer framework developed previously by the team [10-13]. We will extend previous own work on interval impulsive observers with controlled sampling to switched systems. Controlled sampling improves systems resilience as in the case with event triggered control. Extension of interval observer paradigm to partial state reconstruction may lead to a tractable algorithm for secure state reconstruction.
The PhD candidate will work within the European project H2020 MSCA RISE RESPECT 2021-2024 (https://cordis.europa.eu/project/id/101007673) which addresses security and resilience of indoor mobile robotics solutions for logistics applications in healthcare. There is funding for research stays up to 12 months within the leading European companies in cyber security and intelligence, located in Spain, Cyprus and Greece.

Expected qualifications for the applicants and how to apply.
The ideal applicant possesses good background in control theory or related subjects. They have completed or about to complete a Master 2 or Engineering degree in the appropriate field.

Please send preferably by 8 April 2022 to nacim.ramdani@univ-orleans.fr :
Cover letter, CV, Grades of Master studies (or Engineering degree), One or two references.

References

[1] David Kuipers and Mark Fabro, "Control Systems Cyber Security: Defense in Depth Strategies," 2006, https://doi.org/10.2172/911553.

[2] Derui Ding et al., "A Survey on Security Control and Attack Detection for Industrial Cyber-Physical Systems," Neurocomputing 275 (2018): 1674–83;

[3] Yuriy Zacchia Lun et al., "State of the Art of Cyber-Physical Systems Security: An Automatic Control Perspective," Journal of Systems and Software 149 (2019): 174–216.

[4] Seyed Mehran Dibaji et al., "A Systems and Control Perspective of CPS Security," Annual Reviews in Control 47 (2019): 394–411.

[5] André Teixeira et al., "A Secure Control Framework for Resource-Limited Adversaries," Automatica 51 (2015): 135– 48.

[6] Gianluca Bianchin, Yin-Chen Liu, and Fabio Pasqualetti, "Secure Navigation of Robots in Adversarial Environments," IEEE Control Systems Letters 4, no. 1 (2020): 1–6.

[7] Y. Shoukry, P. Nuzzo, A. L. Sangiovanni-Vincentelli, S. A. Seshia, G. J. Pappas and P. Tabuada, « SMC: Satisfiability Modulo Convex Programming », in Proceedings of the IEEE, vol. 106, no. 9, pp. 1655-1679, Sept. 2018

[8] T. Yang, C. Murguia, M. Kuijper, and D. Nesic, "An Unknown Input Multiobserver Approach for Estimation and Control Under Adversarial Attacks," IEEE Transactions on Control of Network Systems, vol. 8, no. 1, pp. 475–486, Mar. 2021, doi: 10.1109/tcns.2020.3029160.

[9] M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G. J. Pappas, and I. Lee, "Design and Implementation of Attack-Resilient Cyberphysical Systems: With a Focus on Attack-Resilient State Estimators," IEEE Control Systems, vol. 37, no. 2, pp. 66–81, Apr. 2017, doi: 10.1109/mcs.2016.2643239.

[10] Djahid Rabehi, Interval Estimation for Cyber-Physical Systems, Thèse de Doctorat Univ Orléans, 2019.

[11] Djahid Rabehi, Nacim Meslem, Nacim Ramdani. Finite-gain L1 Event-triggered Interval Observers design for Continuous-time Linear Systems. Int. Journal of Robust and Nonlinear Control, 31: 4131-4153, 2021. doi: 10.1002/rnc.5463.

[12] Djahid Rabehi, Nacim Meslem, Adnen Amraoui, Nacim Ramdani. Interval impulsive observer for linear systems with aperiodic discrete measurements. IEEE Transactions on Automatic Control 66(11), pp. 5407–5413, 2021, doi:10.1109/TAC.2020.3046126

[13] D. Rabehi, N. Meslem, and N. Ramdani, "Secure interval observer for linear continuous-time systems with discrete measurements subject to cyber-attacks," in 2019 4th Conference on Control and Fault Tolerant Systems (SysTol), 2019, pp. 336–341, doi: 10.1109/systol.2019.8864782.