NATIONAL PH.D. PROGRAM IN AUTONOMOUS SYSTEMS

Model based security and monitoring system for resilient industrial control systems

A hybrid distributed Intrusion Detection System for the protection of Critical Infrastructures

Ph.D. candidate

Valeria BONAGURA

Cycle

XXXVIII

Tutors

Prof.ssa Federica PASCUCCI

Prof. Stefano PANZIERI

1. Description of the research program

The PhD project addresses the problem of Critical Infrastructures (CI) protection. The key idea is to design a distributed and scalable network-based intrusion detection system (IDS) to identify outer and inner cyber-attacks. Specifically, a model-based approach will be adopted to detect anomalies. Thus, a network of digital twins based on hybrid automata and machine learning techniques will be developed to monitor and detect anomalies in the behavior of the cyber-physical systems that compose the CI.

STATE OF THE ART

There are growing concerns and debates in the scientific community about the protection of CIs, given their vital positions in social and economic developments. The emphasis on these concerns is increased since CIs rarely exist or function in isolation [7,8].

As highlighted, the security of CIs is tightly related to the integrity of Industrial Control Systems (ICSs). A comprehensive introduction to threats in ICS can be found in [9], while an interesting overview on securing ICS is sketched in [10]. Most of the approaches presented in the literature, however, are borrowed from the Information Technology (IT) field and do not properly consider the interactions between the cyber and physical systems composing the Operational Technology (OT) world.

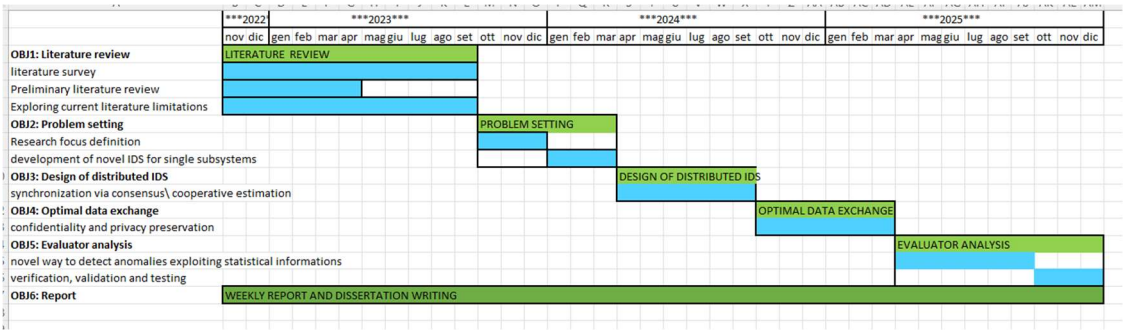
More recently, some solutions propose to build a digital twin of the whole system to monitor the behavior of an interconnected organization. Some digital twins are based on black box approaches: a machine learning algorithm is adopted to simulate the system [10]. Some drawbacks in adopting these techniques are considered in [10] and can be easily overcome by applying model-based digital twins, built on physical dynamics. These approaches are derived from fault diagnosis domain [11] where one or more observers are set up to identify anomalies. In this context, a continuous or discrete time linear system is adopted to model the plant and different attacks are considered according to the model proposed in [12]. In [13], the steps to build a stealthy attack are theoretically derived. The plant is regarded as a discrete time linear system controlled by a linear quadratic Gaussian controller. In [14, 15], light encryption algorithms are proposed to detect this sophisticated stealthy attack. Few works consider hardware in the loop simulation. In this case the digital twin is modeled as hybrid automata (the continuous states are represented by the plant, the discrete jumps by the control actions). In [21] the Salted Kalman Filter is introduced to estimate hybrid systems state having linear dynamics and further extended to nonlinear system in [22]. However, it is necessary to specify that the solution proposed in [21-22] is not meant to be used in a model-based anomaly\fault detection context. In ICS security context, only a few approaches considering hybrid automata have been presented [16,17], however they have been successfully applied in different fields [18-20].

Concerning the distributed estimation problem, the major results can be found in the field of sensor networks [23] and are based on consensus [24]. Also in this case, limited attention is paid to hybrid systems. Moreover, when dealing with ICS, synchronization problems need to be approached, due to hard real time constraints as well as data confidentiality and privacy considerations. Thus, one of the key challenges when developing a distributed estimator for ICS, is to determine how to synchronise and properly exchange the information among the different sites.

RESEARCH OBJECTIVES AND METHODOLOGIES

The proposed research aims at answering to the open questions on CIs protection. Specifically, the project target is the design of distributed model-based IDS to identify cyber-attacks against CIs. To this end a bottom-up approach will be considered. The design of an IDS for single subsystem will be developed. Thereafter, the interconnection between IDS will be considered.

2. Schedule of the research activities



Insert the research activities that you plan, or you have completed for the three years, including any period abroad.

First academic year (planned)

	Description	Period	Activity abroad
Literature review on distributed model-based fault/attack detection	Searches for relevant literature will be performed exploiting scientific databases (e.g., IEEExplore, Scopus). Results will be restricted to peer-reviewed articles to ensure quality and reliability of outcomes. Thereafter, the papers will be classified on the basis of modelling approaches, considered CIs, type of testbed (if adopted). The expected outcome is a systematic review of literature and the definition of the research gaps to be addressed.	From nov. 2022 to sempt. 2023	NO
Problem setting	According to the results of the first activity, a novel IDS for multiple subsystems will be developed. It is foreseen to consider a hardware in the loop approach and use of hybrid models. Thus, the methodologies used to achieve OBJ2 will be the related to hybrid system and discrete event system (i.e., hybrid automata, Petri nets, etc).	From oct. 2023 to mar. 2024	NO

Second academic year (planned)

	Description	Period	Activity abroad
Problem setting	According to the results of the first activity, a novel IDS for single subsystems will be developed. It is foreseen to consider a hardware in the loop approach and use hybrid models. Thus, the methodologies used to achieve OBJ2 will be the related to hybrid system and discrete event system (i.e., hybrid automata, Petri nets, etc).	From oct. 2023 to mar. 2024	NO
Designing of distributed IDS	The IDSs of a set of systems will be connected to perform distributed estimation of the state of ICSs for CIs. In this context, different	From apr. 2024 to SETT. 2024	NO

	methodologies, such as synchronization via consensus and cooperative estimation will be adopted.		

Third academic year (planned)

	Description	Period	Activity abroad
Optimal data exchange	An optimal way to exchange information among different subsystems to preserve confidentiality and privacy will be identified. To this aim, methodologies used for authentication (e.g., lightweight encryption, watermarking) will be adopted.	From opt. 2024 to mar. 2025	YES, university of Coimbra
Evaluator analysis	To identify the attacks in the CIs, a comparison between the real behaviour of the plant and the expected one will be performed. This step will be devoted to design novel strategies to detect anomalies exploiting both data gathered from the single IDS and data exchanged with the network of IDSs. The methodologies used in this step are based on statistical information (e.g., confusion matrices, cumsum analisys, c-square test).	From apr. 2025 to opt. 2025	NO

3. Provisional training and research activities plan

First academic year (planned)

	Description	Period	Final Exam	ECTS
A. Ph.D. courses	Multi-Agent Optimization and Learning: Resilient and Adaptive Solutions	13/02/2023-17/02/2023	No	3
	Distributed optimization for cooperative robotics and decision-making theory, numerical methods and toolboxes	12/06/2023-16/06/2023	No	3
	Introduction to Nonlinear Systems & Control	09/05/2023-12/05/2023	No	3
	Sidra Sumer school	II semester 2022-2023	No	3
B. Master's degree courses	Research Methodology	II semester 2022-2023	No	2
	Industry 4.0: Optimization, Control and Security	12/01/2023-7/02/2023	No	2
C. Soft skill courses	Poliba Soft Skills course	To be defined		3
D. Participation to seminars	Hacking the control systems	January-February or July 2023	No	1.5

E. Participation to international congresses or workshops	Attendance of at leastthree international conferences - to be defined			4
F. Presentation of research products at international congresses or workshops	Presentation of at least three research products – to be defined			4
	TOTAL OF ECTS FOR TRAINING ACTIVITIES			27,5
G. Individual research activity	Research activity in the topic of model based attack detection			17
H. Supervision of students	tutoring activities for students in undergraduate and master's degree programs			6
I. Integrative teaching activities	practical exercises			1,5
J. Preparation of manuscripts for conferences or journals	Verbalization of the results obtained, in the form of a paper for a conference or a journal.			8
	TOTAL OF ECTS FOR RESEARCH ACTIVITIES			32,5
	TOTAL OF ECTS			**60**

Second academic year (planned)

	Description	**Period**	**Final Exam**	**ECTS**
A. Ph.D. courses	Ph.d Courses to be defined			3
B. Master's degree courses	Courses to be defined			2
C. Soft skill courses	Courses to be defined			1
D. Participation to seminars	Seminars to be defined			1,5
E. Participation to international congresses or workshops	Attendance of at least three international conferences - to be defined			4
F. Presentation of research products at international congresses or workshops	Presentation of at least three research products – to be defined			4
	TOTAL OF ECTS FOR TRAINING ACTIVITIES			18,5
G. Individual research activity				22
H. Supervision of students	tutoring activities for students in undergraduate and master's degree programs			8
I. Integrative teaching activities	practical exercises			1,5
J. Preparation of manuscripts for conferences or journals				10
	TOTAL OF ECTS FOR RESEARCH ACTIVITIES			41,5
	TOTAL OF ECTS			**60**

Third academic year (planned)

	Description	**Period**	**Final Exam**	**ECTS**
A. Ph.D. courses	Ph.D course to be defined			3

B. Soft skill courses				
C. Participation to seminars				
D. Participation to international congresses or workshops	Attendance of at least three international conferences - to be defined			4
E. Presentation of research products at international congresses or workshops	Presentation of at least three research products - to be defined			4
	TOTAL OF ECTS FOR TRAINING ACTIVITIES			123
F. Individual research activity				68,5
G. Supervision of students	tutoring activities for students in undergraduate and master's degree programs			22
H. Integrative teaching activities	practical exercises			4,5
I. Preparation of manuscripts for conferences or journals				28,5
	TOTAL OF ECTS FOR RESEARCH ACTIVITIES			180
	TOTAL OF ECTS			**60**

4. List of the publications written by the candidate in the triennium

International Journal Articles

[j1] V. Bonagura, C.Foglietta, S.Panzieri, F.Pascucci, "Consensus Based Kalman Filtering for Attack/Fault Detection in Distributed Systems" **(under preparation)**

International Conference Proceedings

[c1] V. Bonagura, C. Fioravanti, G. Oliva and S. Panzieri, "Resilient Consensus Based on Evidence Theory and Weight Correction". *Atlantic Coast Conference 2023* (**submitted**)

Valeria BONAGURA

Prof.ssa Federica PASCUCCI

Prof. Stefano PANZIERI