PhD in Information Technology and Electrical Engineering
Università degli Studi di Napoli Federico II

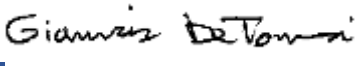
PhD Student:

Cycle:XXXVI

Training and Research Activities Report

Year: First

student signature 

Tutor: Prof. Gianmaria De Tommasi *tutor signature* 

Co-Tutor: Prof. Stefania Santini

Date: October 21, 2020

1. Information:

- **PhD student: Carlo Motta**
- **DR number: DR995143**
- **Date of birth: 25/03/1996**
- **Master Science degree: Automation Engineering**
- **University: University of Naples Federico II**
- **Doctoral Cycle: XXXVI**
- **Scholarship type: UNINA**
- **Tutor: Prof. Gianmaria De Tommasi**
- **Co-tutor: Prof. Stefania Santini**

2. Study and training activities:

Activity	Type[1]	Hours	Credits	Dates	Organizer	Certificate[2]
Digital Forensics	**Course**	**10**	**3**	**03-05-06-09-10 /11/2020**	**Prof. Cozzolino**	**Y**
Stohastic Modeling	**Course**	**24**	**6**	**10/11/2020-17/12/2020**	**Prof. Giorgio**	**Y**
Robot Manipulation and Control	**Seminar**	**2.5**	**0.5**	**17/11/2020**	**Prof. Dario**	**Y**
Digital Project Management	**Seminar**	**1**	**0.2**	**18/11/2020**	**Prof. Amato**	**Y**
Beyond Einstein Gravity: Dark Energy and Dark Matter as Curvature Effects	**Seminar**	**1.5**	**0.3**	**19/11/2020**	**Prof. Di Bernardo**	**Y**
Science, Reality and Credibility	**Seminar**	**1.5**	**0.3**	**24/11/2020**	**Prof. Di Bernardo**	**Y**
Images, Texts, Emojis & Geodata in a Sentiment Analysis Pipeline	**Seminar**	**1.5**	**0.3**	**25/11/2020**	**Prof. Amato**	**Y**
The Ohta-Kawasaki model for 2eblock copolymers: stability and minimality of critical points	**Seminar**	**1.5**	**0.3**	**26/11/2020**	**Prof. Di Bernardo**	**Y**
Patent Searching Best Practice with IEEE Xplore	**Seminar**	**1**	**0.2**	**27/11/2020**	**Dr. Eszter Lukacs**	**Y**

At the Nexus of Big Data, Machine Intelligence and human cognition	**Seminar**	**1**	**0.2**	**02/12/2020**	**Prof. Amato**	**Y**
The Ohta-Kawasaki model for 3eblock copolymers: stability and minimality of critical points	**Seminar**	**1.5**	**0.3**	**03/12/2020**	**Prof. Di Bernardo**	**Y**
Exploiting Deep Learning and Probabilistic Modeling for Behaviour Analytics	**Seminar**	**1**	**0.3**	**09/12/2020**	**Prof. Amato**	**Y**
Quasars as high Redshift Standard Candles	**Seminar**	**1.5**	**0.3**	**10/12/2020**	**Prof. Di Bernardo**	**Y**
GDPR basics for computer scientists	**Seminar**	**1.5**	**0.3**	**10/11/2020**	**Prof. Bonatti**	**Y**
From observability to privacy and security in discrete event systems	**Course**	**19**	**5**	**14-21/12/2020**	**Prof. De Tommasi**	**Y**
AIRO: Optimization and Data Science: Trends and Applications,	**PhD schoool**	**32**	**3.6**	**08-12/02/2021**	**Prof. Speranza**	**Y**
From Photometric Redshifts to Improved Weather Forecasts: an interdisciplinary view on machine learning	**Seminar**	**1**	**0.2**	**13/01/2021**	**Prof. Amato**	**Y**
Synchronization: A Universal Concept in Nonlinear Sciences	**Seminar**	**1.5**	**0.3**	**14/01/2021**	**Prof. Di Bernardo**	**Y**
Cybercrime and e-evidence: the criminal justice response	**Seminar**	**2**	**0.4**	**20/01/2021**	**Prof. Amato**	**Y**
State Estimation and Event Inference in DES: Implications to Detectability, Diagnosability and Opacity.	**Seminar**	**1.5**	**0.3**	**21/01/2021**	**Prof. Kai Cai**	**Y**
AI: Artificial Intelligence for notary's sector – a case study	**Seminar**	**1**	**0.2**	**27/01/2021**	**Prof. Amato**	**Y**

Quantum Simulators	**Seminar**	**1**	**0.2**	**28/01/2021**	**Prof. Di Bernardo**	**Y**
Dynamical Systems Laboratory	**Seminar**	**1.5**	**0.3**	**04/02/2021**	**Prof. Di Bernardo**	**Y**
Scientific Programming and Visualization with Python	**Course**	**2**	**18**	**08-10/03/2021**	**Prof. Botta**	**Y**
Corso di Imprenditorialità Accademica	**Course**	**4**	**20**	**7-8-14-15-21-22-23/07/2021**	**Prof. Rippa**	**Y**

1) Courses, Seminar, Doctoral School, Research, Tutorship
2) Choose: Y or N

2.1. Study and training activities - credits earned

	Courses	Seminars	Research	Tutorship	Total
Bimonth 1	**9**	**3.5**	**1**	**0**	**13.5**
Bimonth 2	**8.6**	**1.9**	**3**	**0**	**13.5**
Bimonth 3	**2**	**0**	**4**	**0**	**6**
Bimonth 4	**0**	**0**	**9**	**0**	**9**
Bimonth 5	**4**	**0**	**5**	**0**	**9**
Bimonth 6	**0**	**0**	**9**	**0**	**9**
Total	**23.6**	**5.4**	**31**	**0**	**60**
Expected	**30 - 70**	**10 - 30**	**80 - 140**	**0 – 4.8**	

3. Research activity:

The focus for this year's research has been the study of cyber-physical systems and the related attacks in the framework of Discrete Event Systems (DES). Indeed, in a distributed system, information leaks and deceptions represent a threat to the privacy and security of the system itself[1], since they may enable external cyber attackers to infer information about the system state, and consequently interact in a malicious way with safety-critical functions. The objective was finding resilient control systems able to make those cyber-physical systems robust to external attacks which can either be active or passive. When dealing with active attacks, the attacker can corrupt some parts of the systems such as actuators or sensors while trying to inflict damage on the system; on the other hand, passive attacks tend to violate the privacy or confidentiality by learning secrets about the system. We decided to approach those attacks on a high level, the so-called supervisory level, in which the whole Cyber-Physical System (CPS) is modeled as a DES.

To this aim we started dealing with passive attacks by studying two main information-flow concepts which have already been widely used to characterize privacy when the CPSs are modelled at the DES level: opacity[2] and non-interference[3] security properties. In an opaque system, a user with full

knowledge of the model, but with partial capabilities about the observation of the event occurrences cannot infer any secret, no matter for how long the system dynamic is partially observed. Supervisory control can be used to enforce opacity by restricting the closed-loop behavior in presence of controllable events[4]. We dealt with Initial State Opaque (ISO) in DESs. A DES is said to be ISO if, for every trajectory originating from a secret state, there exists another trajectory originated from a non-secret state, such that both are equivalent from an external, potentially malicious, observer's point of view. We introduced a sufficient condition to conclude if a DES modeled as a Petri Net system is not ISO. Such a condition is based on the solution of optimization problems in the form of Integer Linear Programming (ILP) problems. A system can be designed so that it fulfills the opacity property; therefore, at design-time, it is possible to check the opacity property and enforce it if not fulfilled.

As for non-interference, the users that can interact with the system belong to different domains. The simplest notions of non-interference refer just to two domains: high-level and low-level[5]. It is assumed that both high-level and low-level users know the system model, but they interact with it with two different views. A leak of information occurs when a low-level user, which is the intruder, obtains information meant to be visible only to the high-level ones.

We dealt with two specific non-interference concepts, namely Strong Non-Deterministic Non-Interference (SNNI) and Bisimulation SNNI (BSNNI); when talking about SNNI, we refer to the net's property of preventing an intruder from infer the occurrence of any secret modeled as high-level event, which cannot be directly observed by the intruder; when talking about BSNNI, the objective extends to avoiding the detection of the disabling of the high-level events. Similar to what has been done for opacity, we proposed some conditions based on the solution of ILP problems to check both SNNI and BSNNI. In the case of non-interference, the proposed conditions turn out to be necessary and sufficient. Moreover, also in this case, the proposed results can be exploited offline during the system design phase.

As for the active attacks we are currently studying attack models and ways of applying them to real world systems. We are focusing on Intelligent Transportation Systems (ITS), more specifically to the automated highway system (AHS). We considered multiple platoons on a three-lane highway, for every platoon the first vehicle is called leader while the other ones are the followers. Those platoons interact with one another through some maneuvers such as the merging (when two platoons join to form one platoon with only one leader) or the splitting (one platoon separates to form two platoons with two different leader). To carry out a maneuver safely, a structured exchange of messages with the leaders of neighboring platoons is initialized to ensure coordination between the movement of neighboring vehicles. We supposed an attacker trying to trick the supervisor by counterfeiting the information exchanged between the leader vehicles of those platoons. The first step for this topic has been finding and editing a realistic model for the plant and the attacker and building up a software, through the usage of Matlab, able to imitate their behavior in different scenarios. Next in progress we are conducting tests to find resilient supervisors, confront them and expose their flaws.

References:

1. Alberto Petrillo, Antonio Pescapé, and Stefania Santini. A secure adaptive control for co-operative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks. IEEE Transactions on Cybernetics, 51(3):1134–1149,2021.
2. Y.C. Wu and S. Lafortune. Comparative analysis of related notions of opacity in centralized and coordinated architectures. Discrete Event Dynamic Systems, 23(3):307–339, 2013.
3. N. Busi and R. Gorrieri. A Survey on Non-interference with Petri Nets. In Lectures on Concurrency and Petri Nets, pages 328–344. 2004.
4. A. Saboori and C. N. Hadjicostis. Opacity-enforcing supervisory strategies via state estimator constructions. IEEE Transactions on Automatic Control, 57(5):1155–1165, 2011.
5. F. Basile, G. De Tommasi, Assessment of bisimulation non-interference in discrete event systems modelled with bounded Petri nets, IEEE Control Systems Letters 5 (2020) 1151–1156.

4. Research products:

Papers:

Gianmaria De Tommasi; Carlo Motta; Alberto Petrillo; Stefania Santini
AIRO Springer Series
Optimization-based assessment of Initial-StateOpacity in Petri Nets
Accepted June 2021.

Francesco Basile; Maurizio Boccia; Gianmaria De Tommasi; Carlo Motta; Claudio Sterle
Nonlinear Analysis: Hybrid Systems
An optimization-based approach to assess non-interference in labeled and bounded Petri net systems
Submitted

5. Conferences and seminars attended

AIRO - Associazione Italiana di Ricerca Operativa, University of Naples Federico II, 08-12/02/2021
5th AIRO Young Workshop and AIRO PhD School 2021
Presented the paper: “Optimization-based assessment of Initial-StateOpacity in Petri Nets”

6. Activity abroad:

7. Tutorship