Multi-Agent System and Digital Twin Models for Security Study of Cyber-Physical System

Individual Plan
September 2022

Student	Zoé Lagache[1]
KTH Examiner	Roberto Guanciale
KTH Supervisor	Musard Balliu
LCIS supervisor	Oum-El-Kheir Aktouf[2]

[1] lagache@kth.com

[2] oum-el-kheir.aktouf@lcis.grenoble-inp.fr

Keywords: MAS, Digital Twins, Cyber-Physical systems, Security

1 Background & main objective

This internship is the occasion for the LCIS and the Fraunhofer IESE to collaborate on this project through the communication with Emilia Cioroaica who already worked on Digital Twins[1][2] and already collaborated with the LCIS[3].

The research work should provide the following outcomes:

- State of the art of most important security issues of cyber-physical systems;
- Development of a simple model for security analysis of Cyber-Physical systems using Digital Twins and Multi-Agent Systems, in a combined way;
- Experimental analysis and evaluation of the proposed model by simulation

During the thesis work, I will provide preliminary results to the research questions bellow such as highlighting main features of both models with regards to a security study.

To carry out the project, it could be useful to have some basic knowledge on the Digital Twins and Multi-Agent Systems concepts since it will be at the center of this research work. Moreover, it is important to be comfortable with the main key words related to the security of cyber-physical systems.

2 Research question & method

2.1 Questions

The aim of this internship project is to investigate three research questions:

1. What are the interesting features of both digital twins and multi-agent systems for studying security of cyber-physical systems?
2. How could digital twins and multi-agent systems be combined to offer a better support for a security study of cyber-physical systems?
3. What security claims of a system can be made from integrating multi-agent systems and digital twins?

2.2 Objectives and tasks

From the three questions above, we can derive these objectives which are then divided into tasks:

- Find the main attacks model on cyber-physical systems
  - Look for the various existing attack models
  - Choose one and explain the choice
  - If enough time, choose other ones
- Define a multi-agent system model to study security

  - Define what a multi-agent system is: the concept is quite old which implies that a lot of people had the time to add their own idea of it making it hard to have a clear grasp on the subject
  - Choose a suitable model for our usage
  - Look for a multi-agent system simulator: the simulator have to be simple enough to be used in the time allotted for the project
- Define a digital twin model to study security
  - Define what a digital twin is
  - Choose a suitable model for our usage
  - Look for a Digital Twin simulator: the simulator have to be simple enough to be used in the time allotted for the project
- Define a multi-agent and digital twin combined model from the comparison
  - Compare both models from the security study perspective
  - Establish how both models can complement each other: there are many ways to combine them. We could imagine an hybrid model, or create a bigger model including the two other separated.

2.3 Method

2.4 Ethics and Sustainability

2.5 Limitations

Both definitions of Multi-Agent systems and Digital Twins does not have a consensus on their definition. I will have to choose one that could limit the set of possible interpretations of these two concepts.

2.6 Risks

Falling behind schedule on the state of the art.

3 Evaluation & news value

Peer-review? Feedback meetings?

4 Pre-study

DT, SMA, most important security issues of cyber-physical systems

Lab preliminary ressources, gscholar.

cf zotero ?

5 Condition & schedule

Computers, internet, zotero, MESA

- Setting up the project: 2 weeks
- State of the art: 1 month
- Personal contribution: 3 months
- Personal contribution writing refining: 3 weeks

A regular supervision will be done on the basis of weekly meetings and additional meetings if needed in which I will present the work in progress which will be analysed by the supervising team.

6 References

References

[1] E. Cioroaica, T. Kuhn, and B. Buhnova, "(Do Not) Trust in Ecosystems," in *2019 IEEE/ACM 41st International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER)*, pp. 9–12, 2019.

[2] E. Cioroaica, B. Buhnova, and E. Tomur, "A paradigm for safe adaptation of collaborating robots," in *Proceedings of the 17th Symposium on Software Engineering for Adaptive and Self-Managing Systems*, SEAMS '22, (New York, NY, USA), pp. 113–119, Association for Computing Machinery, 2022.

[3] E. Cioroaica, S. Chren, O.-E.-K. Aktouf, A. Larsson, R. Chillarege, T. Kuhn, D. Schneider, and C. Wolschke, "Towards Creation of Automated Prediction Systems for Trust and Dependability Evaluation," in *2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp. 1–6, 2020.