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 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, We will provide preliminary results to the research questions below 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 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 attack models on cyber-physical systems
  - Look for the various existing attack models
  - Choose one and explain the choice
  - If time allows, 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 of the subject
  - Choose a suitable model for our usage
  - Look for a multi-agent system simulator: the simulator has 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 has 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 others separated.

2.3 Method

In order to establish the state of the art, we are going to use mainly Google Scholar and Scopus to look for papers or articles.

The results from the state of the art will lead us to our model creation. Then we will simulate this model with the chosen simulator to check if it works as we want and if we can extract some security claims in relation with the chosen attack model.

2.4 Ethics and Sustainability

This work will talk about attacks on cyber-physical systems and may present examples which could be used outside of this work context. However, since the project is primarily concerned with theoretical concepts, this is unlikely.

2.5 Limitations

Definitions of both Multi-Agent systems and Digital Twins do not have a consensus on their definition. We will have to choose one that could limit the set of possible interpretations of these two concepts.

As a limitation, we can also take the duration of the project into consideration. Indeed this is a 5 months project.

2.6 Risks

Falling behind schedule, especially during the state of the art, is a real risk. Indeed, this is an exploratory project and if we do not converge into conclusion quickly enough, we might run out of time. That is what the regular meetings are for. The supervisors have the occasion to give feedback and advices in order to avoid this.

Another risk could be to enter lockdown again, meaning that we lose the access to the lab supplies. But this possibility is unlikely and this project does not need any more equipment than the computer we are working on and several software. We could easily deal with this problem by taking the computer at home and staying in close communication with the lab (through mails and remote meetings).

3 Evaluation & news value

3.1 Evaluation

As a qualitative measure to evaluate our work, it is asked to report all the progress we made during the week, and what we are planning to do the following week, during each meeting. This way, a regular feedback on our work is given. It is also possible to submit our paper for peer review in order to obtain more, and a more diverse, feedback.

3.2 News value

The Multi-agent system is an interesting concept nowadays since systems tends to become decentralized[4], in order, for instance, to avoid any potential single point of failure vulnerabilities. In the other hand, Digital Twins are emerging in the industry field to monitor machines or systems thanks to their virtual copies[5]. However, only few examples of the combination of both have been done, making this research work interesting to study further.

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 supervision will be done regularly on the basis of weekly meetings and additional meetings if needed, in which We 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.

[4] Y. K. Renuka Kamdar, Priyanka Paliwal, "A State of Art Review on Various Aspect of Multi-Agent System," *Journal of Circuits, Systems and Computers*, vol. 27, no. 11, 2017.

[5] Fei Tao and Qinglin Qi, "Make more digital twins," *Springer Nature Limited*, vol. 573, 2019.