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

Pre-study

October 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: Multi-Agent System, Digital Twin, Cyber-Physical system, Security

Acronyms

CPS Cyber-Physical System. 1, 3, 4

DDoS Distributed Denial of Service. 5

DoS Denial of Service. 4, 5

DT Digital Twin. 2

MITM Man-In-The-Middle. 4

Contents

Chapter 1

Introduction

1.1 Background

In a world in an increasing need of control over physical processes, monitoring became mandatory. In order to be accurate enough, more an more systems use electronic systems for monitoring, or even in order to create a digital interface to manipulate physical processes more easily. As an example, cars are for several years now equipped with many sensors to ensure their proper functioning and the safety of the passengers [1]. This is what we call Cyber-Physical System (CPS).

1.2 Problem

According to the CPS Steering Group [2], CPS are defined as the interaction between physical systems and processes using computations and communication abilities. However, these systems were and are still vulnerable to cyberattacks [3] [4] which could have a huge impact. We can imagine the Cyber-Physical System in an airport monitoring each planes entering or leaving the airport. If such a system undergoes, for instance, a DoS attack, the consequences could be devastating. This is why CPS need to be protected against cyberattacks.

1.3 Purpose

Cyber-Physical Systems can be found in a large range of fields, going from healthcare to the electrical power grid management. Numerous applications of it exist and could benefit from a stronger degree of security.

As an ethical and sustainability perspective, we have to say that this work will discuss attacks on CPS and may present examples that could be used outside of this work context. However, since the project is primarily concerned with theoretical concepts, this is unlikely. Furthermore, in computer science, simulation is often an energy-intensive process. We will try to tend to optimized solutions but this is not the main goal of this project as we will not focus on a sustainable solution for security of Cyber-Physical systems.

1.4 Goals

In this master thesis, we propose to study how Multi-Agent System (MAS) and Digital Twin (DT) models can help with this goal and how they complete each other. A Multi-Agent System is a system composed of agents collaborating with each other in order to achieve a common goal. The agents are able to communicate with their local neighbours and, most of the time, only have a local view of the system. MAS are now a trend in the Internet of Things (IoT) field thanks to its decentralization aspect. In the other hand Digital Twins are often associated to a way to track and analyse a system in real time, often in order to predict its behaviour. Both models have the potential to be very useful tools for protecting and preventing cyberattacks on CPS.

1.5 Research methodology

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 and Zotero to save them.

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.

From a reproducibility perspective, we will try to provide every sources of paper and tool we use when possible, and will state when it is not possible, which is unlikely in our case. Indeed, most of the tool we will use should be free. However, some papers may require institutional access or a fee to access the full document.

1.6 Delimitations

1.7 Structure of the thesis

Chapter 2

Background

In this chapter, we are going to introduce the main areas of the subject by providing the basic background on them. The related work will also be discussed.

2.1 Cyber-physical Systems

In this section, we are going to explain how CPS are defined for this thesis and focus on what kind of vulnerability this kind of system is facing.

2.1.1 What are Cyber-physical Systems

As indicated in 1.2, CPS are the combination of the physical world and the cyber space interacting with one another. Most of the time, the cooperation consists in the cyber system monitoring the physical one as seen in Chen et al. [5], Lei et al. [6] and Tsang et al. [7] papers.

2.1.2 Cyber-physical System vulnerabilities

In figure 2.1, we represented a CPS by two parts: the physical process(es) part and the cyber system. Both of these parts are interacting with each other through sensors and actuators which compose the interface between the two worlds. The cyber system is composed of computing devices receiving data from the sensors, processing it, and sending the result to the actuators. The green arrows are indicating the monitoring interaction, while the red ones represent the communication within the cyber system. The numbers point to the parts of the CPS that are subject to vulnerabilities.

By summarizing the classifications done by Wang et al. [3], Wazid et al. [8] and Singh et al. [4], we obtained the resulting vulnerabilities:

Communication attacks

These attacks have the potential to be operated on all communication links, i. e. at 2, 4, 6 and 7 in figure 2.1. Communication attacks can include:

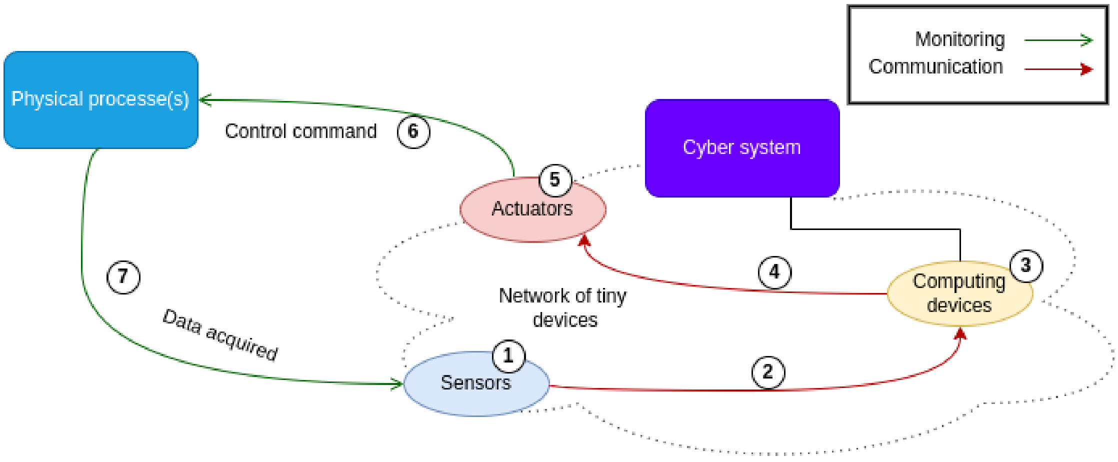

Figure 2.1: CPS main vulnerabilities

Eavesdropping: a passive attack where the attacker is listening to a communication between the two or more nodes of the system.

Man-In-The-Middle (MITM): the base concept is the same as the eavesdropping attack except that the attacker is able to intercept the communication packets and thus to modify them.

Physical attacks

Physical attacks can be done on the devices that are the closest to the real world, thus on the actuators and on the sensors (1 and 5 in figure 2.1). They can be:

Side channel attack: the attacker analyze physical parameters that may vary depending on algorithms implementations and their inputs and are then able to find secret information.

Fault injection: the attacker injects a physical fault in the device to change its behaviour in order for it to be malicious. This can be done by injecting quick voltage faults or electromagnetic faults, etc. Such attack have the potential to extract secret information or bypass system security, for example.

Jamming attack: the attacker jams the communication hence no packets can be sent and received between the sensor and the signal transforming device.

Application attacks

Malware spreading attack: the attacker spread a piece of malicious code into one or more devices of the system. What the code does vary a lot from revealing secret key to making a service unavailable, and thus create a Denial of Service (DoS), for example. This kind of attack is mostly observable on the computing devices (3 in figure 2.1).

Other kind of attacks

Here are attacks that can be part of several of the previous sections.

DoS attack: the attacker put down a device so it cannot work anymore. This device is often chosen strategically. Ways to achieve this attack are numerous. For example, it can be by sending an extremely high number of messages so a server receiving them is flooded and cannot work properly. If the attack is carried out by several device instead of one, we call that a Distributed Denial of Service (DDoS) attack.

2.1.3 CPS simulation

2.2 Multi-Agent Systems

As specified in section 1.4, MAS have been discussed a lot in the computer science field. It is a model that can be used at different level and in different fields. For example, . This diversity of application areas comes from the high customisability and scalability of MAS.

2.2.1 MAS features

Centralization

MAS can either be centralized, part centralized or decentralized. A centralized MAS means that information of all the system is gathered in one point. This point can be a central unit or an agent itself that interacts with each agent of the system to collect the wanted information.

Agents

Agents are entities containing an algorithm defining their behavior and making them autonomous in their decisions making. If we put capabilities constraints like computing or memory limitations, then we are talking about embedded MAS.

2.2.2 MAS for security

2.2.3 MAS simulators

2.3 Digital Twins

2.3.1 DT for security

2.3.2 DT simulators

Chapter 3

References

Bibliography

[1] N. Navet, Y. Song, F. Simonot-Lion, and C. Wilwert, "Trends in automotive communication systems," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1204–1223, 2005.

[2] CPS Steering Group, "Cyber-Physical Systems Executive Summary," Chicago, IL, USA., Mar. 2008.

[3] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Security Issues and Challenges for Cyber Physical System," in *2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*, Dec. 2010, pp. 733–738.

[4] S. Singh, N. Yadav, and P. K. Chuarasia, "A Review on Cyber Physical System Attacks: Issues and Challenges," in *2020 International Conference on Communication and Signal Processing (ICCSP)*, Jul. 2020, pp. 1133–1138.

[5] L. Chen, F. Hu, S. Wang, and J. Chen, "Cyber-physical system fusion modeling and robustness evaluation," *Electric Power Systems Research*, vol. 213, p. 108654, Dec. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378779622007246

[6] C.-U. Lei, K. Wan, and K. L. Man, "Developing a Smart Learning Environment in Universities Via Cyber-Physical Systems," *Procedia Computer Science*, vol. 17, pp. 583–585, Jan. 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050913002081

[7] Y. P. Tsang, T. Yang, Z. S. Chen, C. H. Wu, and K. H. Tan, "How is extended reality bridging human and cyber-physical systems in the IoT-empowered logistics and supply chain management?" *Internet of Things*, vol. 20, p. 100623, Nov. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660522001044

[8] M. Wazid, A. K. Das, S. Kumari, and M. K. Khan, "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 17, pp. 4596–4614, 2016. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1652