PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

UNIVERSITY OF AUGUST 20, 1955 SKIKDA

Faculty of Technology

Department : Petrochemistry

Thesis

In View of Obtaining the Master's degree.

Sector: Petrochemical industry

Specialty: Automation

By: HADJAIDJI Yassine & BOUDIAB Haythem

Theme:

Stability and control design of networked petrochemical system subject to network-induced delay and Cyber-Attacks.

Presented publicly on: 09 / 07 / 2023 before the jury composed of:

President	**MENIGHED Kamel**	**U- 20 Août 1955-Skikda**
Reporter	**Mohamed ROUAMEL**	**U- 20 Août 1955-Skikda**
Examiner	**Bourahala Faycel**	**U- 20 Août 1955-Skikda**
Examiner	**Nafir Noureddine**	**U- 20 Août 1955-Skikda**

Promotion: 2022/2023

Acknowledgment

We would like to take this opportunity to express our heartfelt gratitude to the many individuals and organizations who have contributed to the successful completion of this thesis.

First and foremost, we are profoundly grateful to our families for their unwavering support, love, and encouragement throughout our academic journey. Their belief in our abilities has been a constant source of motivation, and we are truly fortunate to have them in our lives.

We extend our deepest appreciation to our friends and colleagues who have been by our side during this challenging yet rewarding endeavor. Their camaraderie, discussions, and constructive feedback have played an integral role in shaping our ideas and refining our work.

We are indebted to the teaching faculty at the University 20 August 1955 Skikda, especially those in the automation and petrochemical departments. Their dedication, expertise, and passion for knowledge have been instrumental in expanding our horizons and nurturing our intellectual growth.

A special word of gratitude goes to our thesis supervisor, Mohamed Laid Rouamel, for his exceptional guidance, mentorship, and unwavering support. His profound knowledge in the field of automation in the petrochemical industry, coupled with his willingness to share his insights, has been invaluable. His constructive criticism, patience, and encouragement have pushed us to strive for excellence and have significantly contributed to the quality of this thesis.

We would also like to acknowledge the members of petrochemical administration for their administrative support and facilitation of our research work. Their efforts behind the scenes have played a crucial role in creating an environment conducive to learning and research.

Furthermore, we express our gratitude to the participants who contributed their time and expertise to this study. Their willingness to be a part of our research has enriched the depth and validity of our findings.

Lastly, we would like to acknowledge the support and guidance provided by the funding organizations and institutions that have contributed to this research. While their support may have been financial, it has been a catalyst for the realization of this work.

To all those who have played a part, big or small, in the completion of this thesis, we are truly grateful. Your contributions have left an indelible mark on our academic journey, and we are honored to have had you as part of this process.

HADJAIDJI Yassine & BOUDIAB Haythem

Abbreviations

CPSs	Cyber-Physical Systems
DCS	Distributed Control System
DoS	Denial of Service
FDI	False Data Injection
GAS	Globally Asymptotically Stable
ILC	iterative learning control
LKF	Lyapunov-Krasovskii Functionals
LMI	Linear Matrix Inequality
MAUB	Maximum allowable upper bound
NCSs	Networked Control Systems
NN	Neural Networks
PWM	Pulse-width-modulated
ZOH	Zero-Order Hold

Abstract:

This Memoir investigates the stability and controller synthesis of Networked Control Systems (NCSs) under cyber-attack constraints. It provides an overview of NCSs, their advantages, applications, and a literature review. The main focus is on analyzing NCS stability and controller synthesis under cyber-attacks. The architecture of NCSs is discussed, including components and their impact on system stability. Different types of cyber-attacks and their effects on performance are examined. A case study using the quadruple-tank process analyzes NCSs considering network-induced delay and deception attacks. Control design conditions for stability and robustness are discussed. The research contributes to designing secure and reliable NCSs, addressing stability and cyber-attack challenges.

Keywords: Networked Control Systems, NCSs, stability analysis,, cyber-attacks, network-induced delay, deception attacks, control design, robustness.

ملخص:

تبحث هذه المذكرات في الاستقرار وتوليف وحدة التحكم لأنظمة التحكم الشبكية (NCS) في ظل قيود الهجوم السيبراني. يوفر نظرة عامة على محطات التحكم في الشبكة ومزاياها وتطبيقاتها ومراجعة الأدبيات. ينصب التركيز الرئيسي على تحليل استقرار NCS وتوليف وحدة التحكم في ظل الهجمات الإلكترونية. تمت مناقشة بنية NCS ، بما في ذلك المكونات وتأثيرها على استقرار النظام. يتم فحص أنواع مختلفة من الهجمات الإلكترونية وتأثيراتها على الأداء. دراسة حالة باستخدام عملية الخزان الرباعي تحلل NCSs مع الأخذ في الاعتبار هجمات التأخير والخداع الناتجة عن الشبكة. تمت مناقشة شروط تصميم التحكم من أجل الاستقرار والمتانة. يساهم البحث في تصميم محطات تحكم وطنية آمنة وموثوقة ، ومعالجة تحديات الاستقرار والهجوم الإلكتروني.

الكلمات الرئيسية: أنظمة التحكم الشبكية ، NCS ، تحليل الاستقرار ، الهجمات الإلكترونية ، التأخير الناجم عن الشبكة ، هجمات الخداع ، تصميم التحكم ، المتانة

.Résumer :

Ce mémoire étudie la stabilité et la synthèse des contrôleurs des systèmes de contrôle en réseau (NCS) sous les contraintes des cybers attaques. Il donne un aperçu des SNC, leurs avantages, leurs applications et une revue de la littérature. L'accent est mis sur l'analyse de la stabilité du NCS et de la synthèse des contrôleurs lors de cyber attaques. L'architecture des NCS est discutée, y compris les composants et leur impact sur la stabilité du système.

Différents types de cyber attaques et leurs effets sur les performances sont examinés. Une étude de cas utilisant le processus à quatre réservoirs analyse les NCS en tenant compte des retards induits par le réseau et des attaques de tromperie. Les conditions de conception des commandes pour la stabilité et la robustesse sont discutées. La recherche contribue à la conception de NCS sécurisés et fiables, répondant aux défis de la stabilité et des cyber-attaques.

Mots-clés : Systèmes de contrôle en réseau, NCS, analyse de stabilité, cyber-attaques, retard induit par le réseau, attaques par tromperie, conception de contrôle, robustesse.

Table of Contents

Acknowledgements iii

Abstract vii

List of Figures xi

List of Tables xiii

1 General introduction 3

1.1 Brief history of the NCS research field 5

1.2 Our Contribution 6

1.3 Thesis organization 7

2 Networked Control Systems (NCSs) and Cyber security 9

2.1 Introduction 9

2.1.1 NCS components 9

2.2 Structures of networked control system 10

2.2.1 Direct structure 10

2.2.2 Hierarchical structure 10

2.3 Modeling of the Networked control system (NCSs) and its imperfections . 11

2.3.1 Network-induced delay 13

2.3.1.1 Mutually stochastic delay model 15

2.3.2 Input delay system approach 16

2.4 Cyber-attacks 17

2.4.1 The influence of Cyber-attack on system performance 18

2.4.2 False Data Injection Attacks 18

2.4.2.1 False Data Injection Attacks Modeling 19

2.4.3 Denail Of Service Attacks 20
2.4.3.1 Denial of Service Attacks Modeling 20
2.4.4 Deception attacks 22
2.4.4.1 Deception Attacks Model 23
2.4.5 Replay attacks 23
2.4.5.1 Replay Attacks Modeling 24
2.5 Conclusion 25

3 Stability analysis and robust control of NCSs 27
3.1 Introduction 27
3.2 Petrochemical system Modeling 28
3.2.1 Quadruple-Tank Process Modeling 28
3.3 Preliminaries and Problem Statement 30
3.4 Main result 33
3.4.1 Stability Analysis 33
3.4.2 Control Design Condition 37
3.5 Simulation results 38
3.5.1 Stability analysis results 38
3.5.2 Control design results 41
3.6 Conclusion 43

5 General Conclusion 59

References 47

5 General Conclusion 59

List of Figures

1.1 Networked Control System Architecture 5

2.1 Direct Structure of NCS 11
2.2 Hierarchical Structure of NCS 11
2.3 The interval of DoS attacks 21

3.1 The quadruple-tank process shown together with a controller interface running on a PC [82]. 28
3.2 Schematic representation of the quadruple-tank process 29
3.3 NCS subject to deception attacks. 31
3.4 States trajectories 39
3.5 States trajectories. 40
3.6 The Occurrence of the deception attacks $\sigma_u(t_k)$. 40
3.7 The Occurrence of the deception attacks $\sigma_x(t_k)$. 41
3.8 States trajectories. 42
3.9 States trajectories. 42
3.10 The Occurrence of the deception attacks $\sigma_u(t_k)$. 43
3.11 The Occurrence of the deception attacks $\sigma_x(t_k)$. 43

List of Tables

3.1 $\bar{\eta}$ for various $\bar{\sigma}_u$ and $\bar{\sigma}_x$ (Example A) 40

Abbreviations

CPSs Cyber-Physical Systems

DCS Distributed Control System

DoS Denial of Service

FDI False Data Injection

GAS Globally Asymptotically Stable

ILC iterative learning control

LKF Lyapunov-Krasovskii Functionals

LMI Linear Matrix Inequality

MAUB Maximum allowable upper bound

NCSs Networked Control Systems

NN Neural Networks

PWM Pulse-width-modulated

ZOH Zero-Order Hold

Chapter 1

General introduction

In industrial factories, the monitoring of precision and production quality is one of the most important aspects, as efficient monitoring and control processes significantly impact production outcomes. This includes the effectiveness of devices and algorithms involved in the process, leading researchers to make concerted efforts to improve and develop monitoring and control processes, particularly in the areas of control and sensors. The monitoring and control process can be defined as the process of maintaining a physical quantity at a constant value despite external disturbances [40]. For many years, researchers have provided precise and exemplary control strategies stemming from classical control theory, ranging from open-loop control to advanced control strategies. In classical (traditional) control, the system components, including controllers, sensors, and actuators, are typically located within the same physical area. Each different system node is individually connected through electrical wiring, and the systems are designed to bring all sensor information to a central location for monitoring and decision-making. This approach has been successfully implemented in the industry for decades. However, due to the increasing number of expanding physical configurations, the traditional point-to-point architecture has limitations and struggles to meet strict control requirements such as decentralized control and remote control. Consequently, the concept of introducing communication networks into the remote control concept has emerged, leading to the development of Networked Control Systems (NCSs). NCSs are decentralized or distributed control systems (DCS) in which control loops (sensors, actuators, and controllers) are closed through a real-time digital communication channel (Fig. 1.1). As a result, the scale of networked control systems is generally much larger than that of conventional control

systems. Implementing this paradigm introduces new challenges in a control loop design. These challenges include the increased complexity of the networked control system, as well as the negative effects of the communication channel, such as communication delay, packet loss, packet disorder, and more. It is evident that these challenges place a heavy burden on control engineers who must address these issues during control loop design.
A networked control system(NCSs) is a system in which the control loops are closed via a communication network so that the signals of the system (control and measurement signals) can be exchanged between all the components (sensors, controllers and actuators) via a common network, Fig. 1.1 shows a typical structure of an NCSs. Compared to traditional control systems such as point-to-point or distributed control systems (DCS)...etc, an NCSs has several advantages, including less wiring, less cost, lighter weight, easier to install, and more system flexibility and maintainability. also, an NCSs can be modified or upgraded easily without big changes in the structure. As a result, NCSs have been widely used over the last decades in many fields such as control industrial, process control engineering systems, smart grids, remote surgery, aerospace systems, remote operation and intelligent systems [1]. On another side, the use of a network system introduces new challenges for the system itself, such as system imperfections that include quantization errors, delays variables, dropouts, etc., and the most serious defect affecting the system is the hackers who try to hack or attack the system through attacks we call cyber-attacks. cyber-attacks could affect the behavior NCSs by degrading performance or causing instability. As a result, it is essential to correctly model the NCSs and design controllers that achieve stability in these circumstances [78].

A cyber-attack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system, or digital device. The lack of knowledge about a system's dynamics and continuous monitoring and maintenance of compromised systems are the fundamental constraint faced by hackers [34]. Gaining access to detailed information regarding an NCS system's architecture or its internal components can be challenging for attackers without insider assistance. This limited understanding may restrict their ability to launch sophisticated attacks such as replay attacks or denial of service attacks.

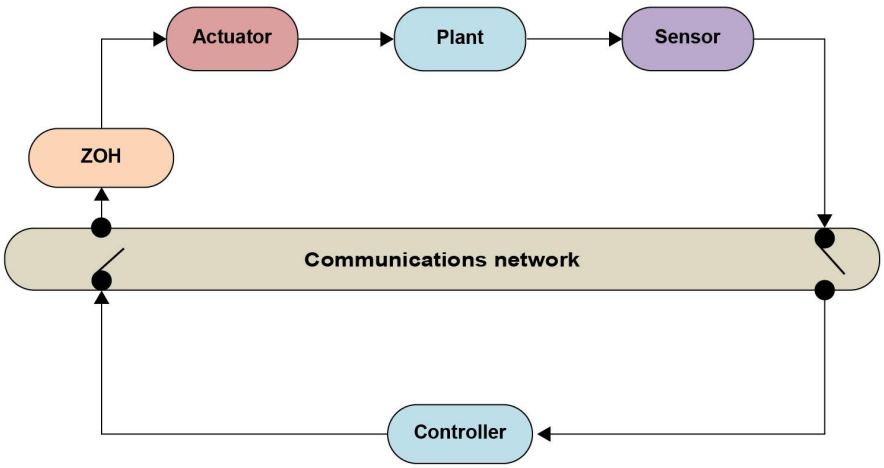

Figure 1.1: Networked Control System Architecture

1.1 Brief history of the NCS research field

At the end of the 1990s, the advent of the development of access technologies to the network and wireless systems provided a huge base for systems controlled via the network, which sparked the development and research of distributed NCSs. As the concept of NCSs began to develop due to its potential in various applications such as district heating systems, automation of large-scale installations ladder, intelligent transport systems, monitoring, remote surgery, systems distributed power, and smart grids [44] [8] [5] [45], he also posed many challenges for researchers to achieve reliable and effective control. Thus, the domain NCSs have been researched for decades and have resulted in many topics important to research. A large branch of the literature focuses on different control strategies, modeling, and stability analysis of NCSs among the articles study the modeling of NCS, the works [38], [35], [52], [79] where the authors study the path tracking problem based on the H_∞ observer of the control systems of output feedback taking into account data transmission delays, loss data packets and sampling effects. stochastic modeling includes the behavior of network-induced imperfections and their effects on the analysis stability and performance of NCS, between them we mention the articles of [20], [60], [68]. Whereas in [76] the controller design problem for such network-based iterative learning control (ILC) process is handled by taking into account data dropout occurring during remote facility transfers to the ILC controller. A study in [86] examines the fuzzy control problem of Adaptive event-triggered dynamic output feedback for NCS not linear subject

to packet loss. The predictive control of the control system of the network with packet loss in the reverse and forward channels is presented in [55], introducing a data-based network predictive control method in which a sequence of control increment predictions is computed in the controller, where the number of consecutive packet losses in the two channels is supposed to be limited. On the other hand, when we present the review of the literature on stability analysis of NCSs, we mention the article in [61], [33], [17], [80], [83] where the authors focus on constructing a proper LKF with integral terms doubles, triples and quadruples to provide greater delay limits in stability analysis.

On the other hand, it is worth noticing that NCSs can be corrupted by cyber-attacks, leading to loss of stability guarantees and so security breaches and impairments [81]. Three types of cyber-attacks are often considered in the literature: Denial of Service (DoS) attacks, replay attacks, and deception attacks [9, 18]. DoS attacks can block the communication channel. Replay attacks usually replace the current transmitted signals with past ones. Deception attacks replace the originally transmitted signals with malicious ones, providing harmful consequences to NCS security. Several recent works have been done to cope with such issues, especially by considering that the NCS is subject to stochastic deception attacks, e.g. [65, 70]. The design of NCS subject to deception attacks remains on the stability analysis of closed-loop systems with input time-varying delays, disturbed by stochastic entries. The stability analysis is often made via Lyapunov-Krasovskii Functionals (LKF) in the Linear Matrix Inequality (LMI) framework but with conservatism. Hence, relaxing the conservatism may help to improve the resilience against deception attacks of the designed closed-loop NCS, which is the goal of the control design procedure presented in Chapter 3.

1.2 Our Contribution

The robust control design of Networked Control Systems (NCSs) against hackers has emerged as a crucial field of study. However, as we talk earlier that the presence of network-induced delays and hacker attacks poses significant challenges to the stability and efficiency of these systems. the main contributions of this memory are as follows:

• Obtain a maximum allowable network-induced delay bound guaranteeing the stability and stabilization of NCSs. We used the idea of addressing NCSs as a sampled-data sys-

tem by constructing new LKFs including simple, double integral terms and also new augmented LKFs vector, and also used novel lemmas (Wirtinger and extended reciprocally lemmas) to estimate the LKFs vector derivatives we obtained the stability and control design conditions.

• Propose a new scenario of Cyber attacks methodology that affects both the sensor-to-controller channel and controller-to-actuator channel.

• Developing a robust output feedback networked controller against deception attacks and so enhances the system's resilience against Cyber attacks.

• Verify the Condition obtained on the special case of networked control system architecture with and without deception attacks.

1.3 Thesis organization

The thesis is organized as follows: Chapter 1 starts with a general introduction to Networked Control Systems (NCSs), highlighting their advantages, disadvantages, applications, and comparisons with point-to-point or traditional control structures. After that, we find a section that presents the history of NCSs by presenting a literature review covering its evolution and development over time. The main contribution of this thesis is the analysis of NCS stability and controller synthesis under cyber attack constraints. Lastly, an overview of the organization for the remainder of the thesis is provided.

In Chapter 2, we discuss in detail the architecture of NCSs along with various components within a control loop such as sensors, networks, controllers, Zero Order Hold (ZOH) devices, etc. We model NCS as a sampled-data system operating under communication network constraints while considering different challenges posed by communication channels on system stability. This chapter also explores how various types of cyber attacks can impact system performance by modeling each attack type individually, before concluding with key insights.

Chapter 3 of this thesis focuses on the networked control system analysis for the quadruple-tank process. The chapter begins by describing the modeling of the petrochemical system, specifically the quadruple-tank process, including the identification methods used to obtain system parameters. Next, the integration of the quadruple-tank process into a networked control system framework is presented, considering the impact of network-

induced delay and the vulnerabilities associated with deception attacks. The stability of the networked control system is then analyzed, first taking into account the network-induced delay and subsequently evaluating the stability after deception attacks. Control design conditions are discussed, highlighting the design requirements for achieving stability and robustness in the presence of delays and attacks. Simulation results are provided, demonstrating the stability analysis findings and the performance of the control design approach. The chapter concludes by summarizing the key findings, emphasizing the contributions to the overall thesis objectives.

Chapter 2

Networked Control Systems (NCSs) and Cyber security

2.1 Introduction

In this chapter, different components and structures of NCSs are presented which include the different structures between the components of closed-loop interconnected through the network. an NCS modeling that includes network-induced delay and Cyber-attack imperfections is discussed. finally, the Lyapunov technique is presented to analyze the stability and synthesis controller for NCSs while considering one or more of the imperfections.

2.1.1 NCS components : As mentioned above that in a networked control system (NCS), the control loop is composed of interconnected devices that communicate through a dedicated communication channel. Each device within the control loop has a specific role to ensure the effective operation of the system. There are four fundamental functions that must be performed by the devices in an NCS: information acquisition (sensors), control (controllers), communication (communication protocols), and execution (actuators). In a networked control system, the traditional control loop is replaced by a communication channel through which devices interact. Instead of converting physical quantities to analog signals, the measurements are transformed into numerical signals by the sensors. The networked controller receives these measurement packets, processes them in a discrete-time format, and generates control signals transmitted through the same communication channel. However, challenges arise due to congestion and delays caused by

sharing the channel with other control nodes, leading to potential signal loss or disordering. To bridge the gap between discrete and continuous-time signals, the Zero-Order Hold (ZOH) algorithm is used to convert the numerical signal into an analog form. Actuators play a crucial role in executing control actions, converting the control signal coming from the ZOH into mechanical motion. The implementation of networked systems heavily relies on the performance of the communication network, considering factors such as quantization, transmission rate, delays, and packet losses [**?**]. Understanding the impact of the network on system stability and performance is essential in designing networked control systems.

2.2 Structures of networked control system

In the domain of Networked Control Systems (NCSs), the overall architecture exhibits decentralization, wherein the closed-loop elements are dispersed across the industrial region employing two distinct structures: the direct structure and the hierarchical structure. The hierarchical structure, being a hybrid system, offers the capability to investigate the interconnection between various plants. On the other hand, the direct structure serves as an independent control application [27].

2.2.1 Direct structure : The direct structure represented by Figure 2.1, encompasses the controller, sensors, and actuators. Within the network, each node establishes a closed-loop feedback control system by utilizing a shared access link. Additionally, the network includes other nodes within the control loop that utilize available resources. The controllers, sensors, and actuators have the flexibility to operate in either a time-driven or event-driven mode [27].

2.2.2 Hierarchical structure : The NCS hierarchical structure depicted in Figure 2.2, employs a network that interconnects distributed subsystems. Each subsystem constitutes a self-contained closed-loop control system, comprising its own controller, sensors, and actuators. The host controller assumes the responsibility of setting the control parameters for each subsystem, thereby coordinating the entire process [27].

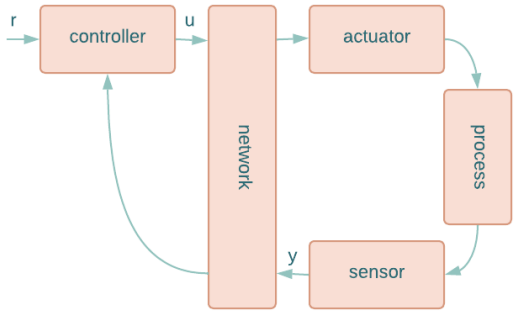

Figure 2.1: Direct Structure of NCS

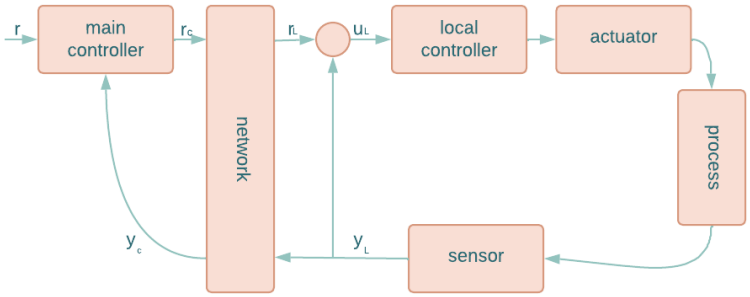

Figure 2.2: Hierarchical Structure of NCS

2.3 Modeling of the Networked control system (NCSs) and its imperfections

This section focuses on the modeling methodology for networked control systems (NCSs). The modeling of networked control systems (NCSs) is a well-researched field with rich literature. Various aspects of NCS modeling are covered, including the characterization of different imperfections present in NCSs. These imperfections encompass phenomena such as time-varying delays, fluctuations in sampling intervals, and occurrences of packet dropouts. NCSs can be modeled using both discrete-time and continuous-time approaches, accommodating diverse system dynamics. Furthermore, models can be developed for both linear and non-linear NCSs, considering the specific characteristics and complexities of each case. Additionally, modeling techniques are available to address uncertainty and disturbances in NCSs, enabling robust analysis and control design. Figure (1.1) illustrates the interconnected components of networked control systems (NCSs). Within this system, the plant is represented as a continuous-time system, while the con-

troller operates in a discrete-time manner, utilizing a computer to generate discrete control signals at its output. Before being transmitted to the plant, the discrete control signal is reconstructed into a continuous signal using a zero-order hold (ZOH) mechanism. The ZOH maintains the control signal constant until the next sampling instant. Considering these aspects, the NCSs model can be described as a linear continuous-time model using the following closed-loop linear.

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) + Du(t) \end{cases} \tag{2.1}$$

$x(t)$ is the system state vector,$u(t)$ is the input vector,$y(t)$ is the output vector, and A, B, C and D are real constant matrices with appropriate dimensions. As highlighted earlier in this section, the integration of communication networks within the components of Networked Control Systems (NCSs) introduces additional complexities and limitations that must be accounted for when modeling the entire networked system.

Hence, it is crucial to address the modeling of these imperfections and constraints in NCSs prior to commencing the modeling procedure. These imperfections and constraints can be classified into five distinct types, each playing a significant role in the overall system performance and behavior: network-induced delays, packet dropouts, quantization errors, variable sampling/Transmission Intervals, bandwidth Limitations, Cyber-Attacks, and other communication constraints. Considering and accurately modeling these imperfections and constraints in NCSs are essential for understanding their impact on system behavior, stability, and performance. By incorporating these factors into the modeling process, researchers and engineers can develop effective strategies to mitigate their effects, optimize system performance, and design robust control algorithms that account for the limitations imposed by the communication network. Therefore, it is crucial to address these imperfections and constraints as integral parts of NCS modeling to ensure a comprehensive understanding of the system's behavior and to devise appropriate control strategies that can adapt to the challenges posed by the communication environment. In our study, we focus on modeling network defects, exactly the network-induced delay [49], and Cyber-Attacks.

2.3.1 Network-induced delay

The network control systems exhibit a significant flaw known as network-induced delay, as various researchers have observed. In Figure (2.1), it becomes evident that there are two distinct types of time delays. The first type of delay occurs from the sensor to the controller, representing the time interval between the signal being sampled by the sensors and its reception by the controller. The second type of delay arises from the controller to the actuator, signifying the time lapse between the generation of the control signal and its availability at the actuator. These delays can be attributed to factors such as restricted data bandwidth, network traffic, and network protocols, which commonly serve as the underlying causes [72]. Nevertheless, in the majority of cases, these two types of delays are not typically treated as separate entities, and the focus is primarily placed on the round-trip delay. However, it is important to note that NCSs employ a variety of communication networks, and this usage results in diverse characteristics of network-induced delays. These characteristics can vary depending on the specific communication network being utilized. For instance, cyclic service networks such as Toking-Ring and Toking-Bus exhibit bounded constant delays [7]. However, it is worth noting that network-induced delays can vary significantly depending on the type of communication network employed in NCSs. For instance, random access networks like Ethernet and CAN introduce random and unbounded delays. In these networks, delays are not limited or predictable, which can pose challenges to real-time control systems. The inherent nature of random access networks leads to varying delays, impacting the overall performance and responsiveness of the NCS. Therefore, understanding and mitigating these random and unbounded delays becomes crucial in designing robust and reliable control systems [42].In contrast, priority order networks, such as DeviceNet, introduce distinctive characteristics of network-induced delays. In these networks, delays are determined by the priority assigned to data packets. Specifically, lower-priority data packets experience unbounded delays, meaning their transmission times can vary significantly. On the other hand, higher-priority data packets are subjected to bounded delays, ensuring their timely delivery and a higher level of responsiveness. The prioritization mechanism in priority order networks aims to optimize communication efficiency and guarantee the timely transmission of critical information within the NCS. By carefully managing the delays based on packet priority, these networks enhance the overall performance and reliability of the control systems [43]. The estimation and modeling of network-induced

delays in NCSs can be achieved through various techniques, such as the time-stamp technique. Researchers have proposed different models to capture the characteristics of these delays. Some models consider constant delays, random delays within specific bounds, independent stochastic delays, and random delays governed by a Markov process. In many existing studies, NCSs have been modeled with constant time delays. In this modeling approach, the delay is typically set to the maximum network-induced delay in the system, representing either the sensor-to-controller delay or the controller-to-actuator delay. To ensure accurate representation, a buffer with a length greater than the worst-case delay is introduced. This buffer serves to accommodate the delay variations and provide a safety margin for the system's operation. By employing these modeling techniques, researchers aim to analyze and understand the impact of network-induced delays on the performance and stability of NCSs. These models contribute to the development of strategies and algorithms that can mitigate the effects of delays and improve the overall reliability of networked control systems [56]. Moreover, it is important to note that the assumption of constant delays in NCSs provides an accurate model only when the introduced delays are significantly shorter than the system's processing time constant. However, when the sampling period exceeds the duration of the delays, the analysis becomes more intricate. In such cases, NCSs can be treated as deterministic systems, allowing for the application of various deterministic control methods. The closed-loop representation of NCSs with constant delays can be expressed as follows:

$$\begin{cases} \dot{x}(t) = Ax(t) + BKx(t-\tau) \\ y(t) = Cx(t) + DKx(t-\tau) \\ x(t) = \phi(t), t \in [0, \tau] \end{cases} \tag{2.2}$$

In the context of networked control systems (NCSs), the total network-induced delay denoted as $\tau(t)$, is the sum of three distinct components: τ_{sc}, representing the sensor-to-controller delay, τ_{ca}, representing the controller-to-actuator delay, and τ_c, representing the processing delay. These delays collectively contribute to the overall time delay experienced by the system. To analyze the behavior of the NCS, the characteristic equation $|sI - A - BKe^{-\tau s}| = 0$ is commonly employed. However, it is important to note that this equation is transcendental in nature, making it challenging to solve directly. Conse-

quently, it is desirable to eliminate the delay term from the characteristic equation. By removing the delay, the equation can be transformed into a more manageable form, enabling the application of conventional analysis and design techniques. Eliminating the delay from the characteristic equation simplifies the analysis and design process for NCSs. It allows for the utilization of well-established control methodologies that are applicable to systems without time delays. This approach facilitates the implementation of control strategies and the evaluation of system performance in networked control systems [49].

2.3.1.1 Mutually stochastic delay model In Networked Control Systems (NCSs), the network-induced delay is influenced by various stochastic factors, including network load, node competition, and network congestion. As a result, the delay tends to exhibit stochastic behavior. Consequently, the utilization of constant delay and deterministic control methodologies is often inadequate in meeting the system's performance requirements. The stochastic delay model can be classified into two categories: one where delays exhibit probabilistic dependence, and another where delays are mutually independent. The mutually independent stochastic delay model is commonly employed for modeling and controlling NCSs with random delays when the probabilistic dependence is unknown [26]. The stochastic network-induced delay can be represented by utilizing signal distribution and a Bernoulli process, which is described as follows: The stochastic network-induced delay is partitioned into two distinct delays, with its interval further divided into sub-intervals:

$$\tau(t) = \tau_1(t) + \tau_2(t) \tag{2.3}$$

with:

$$\begin{cases} \tau_1(t) = \sigma(t)\tau(t) \\ \tau_2(t) = (1 - \sigma(t))\tau(t) \end{cases} \tag{2.4}$$

with $\tau(t) \in [\tau_{min}, \tau_{max}]$ and where τ_{max} and τ_{min} is a given the upper and the lower of the network-induce delay, respectively, and $\sigma(t)$ is Bernoulli process describe the delay distribution describe as:

$$\sigma(t) = \begin{cases} 1 \text{if} t \in \Omega_1 = t : \tau(t) \in [\tau_{min}, \tau_{med}] \\ 0 \text{if} t \in \Omega_2 = t : \tau(t) \in \tau_{min}, \tau_{max}] \end{cases} \tag{2.5}$$

with $\tau_{med} \in [\tau_{min}, \tau_{max}]$ a parameter to be chosen in order to take benefit of distribution of the delay. From (2.5), we can notice that the network-induced delay $\tau(t)$ changes randomly, and the probability of $\tau(t) \in \Omega_1$ and $\tau(t) \in \Omega_2$ can be known. Moreover, it is straightforward that $\Omega_1 \cup \Omega_2$=$[\tau_{min}, \tau_{max}]$ and $\Omega_1 \cap \Omega_2$=0 Therefore, he closed-loop dynamics expressed as:

$$\begin{cases} \dot{x}(t) = Ax(t) + \sigma(t)BKx(t - \tau_1(t)) + (1 - \sigma(t))BKx(t - \tau_2(t)) \\ y(t) = Cx(t) + \sigma(t)DKx(t - \tau_1(t)) + (1 - \sigma(t))DKx(t - \tau_2(t)) \\ x(t) = \phi(t), \forall t \in [-\tau_{min}, -\tau - max] \end{cases} \tag{2.6}$$

2.3.2 Input delay system approach The input delay approach models Networked Control Systems (NCSs) as a system with time-varying delay. This time-varying delay comprises several components, including the delay from the sensor to the controller, the delay from the controller to the actuator, computation delay, and the representation of packet dropout as a delay. This approach was developed to address the synchronization problem in complex networks by considering signal sampling.

A crucial aspect of this approach is determining the maximum allowable upper bound (MAUB) of transmission delay. This MAUB ensures the stability and optimal performance of NCSs. Determining the maximum allowable upper bound of transmission delay is also crucial for practical applications. As a result, the NCSs closed-loop system can be described by the following time-varying system with input delay:

$$\begin{cases} \dot{x}(t) = Ax(t) + BKx(t - \tau(t)) \\ x(t) = \phi(t), \tau(t) \in [-\tau_M, -\tau_m] \end{cases} \tag{2.7}$$

with:

$$\begin{cases} 0 \leq \tau_m \leq \tau(t) \leq \tau_M or (\tau_M + (\eta + 1)h \text{if packet dropout} \\ \tau_m > 0, \tau_M > 0, \eta \geq 0 \end{cases} \tag{2.8}$$

where τ_m, τ_M, η are the upper value and lower value and number of packet loss, respectively. A sufficient condition of stability of these NCSs is derived based on a proper Lyapunov function and presented using the LMI method.

2.4 Cyber-attacks

A cyber-attack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system, or digital device. Cyber-attacks pose a significant threat to our ability to utilize communication securely, efficiently, and innovatively on a global scale, and they are at the center of numerous security concerns. However, the academic literature has yet to fully explore and develop the concept of Cyber-attacks. To advance our understanding, it is essential to define the fundamental attributes of the "concept of Cyber-attack," enabling us to enhance theoretical frameworks, design and implement comprehensive databases to facilitate scholarly research, conduct empirical observations, and compare different types of Cyber-attacks [31].

Cyber attacks serve a range of malicious purposes, including the dissemination of false information, disruption of critical services, unauthorized access to sensitive data, espionage activities, data theft, and causing financial harm [13]. Over time, these attacks have witnessed an increase in their nature, complexity, and severity. Currently, there is a relative lack of understanding surrounding the different types of Cyber-attacks, their methods of propagation, and their relative levels of severity. This knowledge gap has left many organizations and countries susceptible to such attacks. It is imperative to develop effective security measures, which necessitates a comprehensive understanding of these attacks and their classification. Therefore, the creation of a comprehensive catalog that encompasses various Cyber attacks and their classifications becomes a vital component of Cyber security initiatives. This study endeavors to classify attacks based on various characteristics, such as severity, purpose, and legality, with the aim of providing insights into the motivations behind such attacks. Such understanding can enable programmers to develop security devices and mechanisms tailored to counteract specific modes of attack [58].

In order to combat Cyber threats effectively, it is crucial to stay updated with the evolving landscape of Cyber-attacks and continually enhance defensive strategies. Ongoing research, analysis, and collaboration between security experts, organizations, and government entities are essential to counter the increasing risks posed by Cyber-attacks and ensure the protection of critical infrastructure, sensitive information, and economic sta-

bility.

2.4.1 The influence of Cyber-attack on system performance

With the increasing exploitation of Cyber vulnerabilities in control systems, which are critical components of interconnected infrastructure, it has become crucial to develop methodologies for risk analysis and mitigation strategies. In the past decade, significant progress has been made within the control systems community to gain a better understanding of Cyber threats and their potential impacts. Inspired by recent Cyber attacks targeting the power grid, connected road vehicles, and process industries, a system model has been introduced to encompass various research studies on control system vulnerabilities. An attack space has been delineated to illustrate the allocation of adversarial resources in common attacks. In this discussion, we will focus on four primary types of attacks: false data injection, deception attacks, denial-of-service attacks and replay attacks. For each attack type, representative models and mathematical formulations have been devised to provide a structured understanding of their characteristics and potential implications. These models enable system designers and operators to assess the risks associated with such attacks and develop effective mitigation strategies to safeguard the integrity and functionality of control systems. It is worth noting that the specific formulations and models for these attacks may vary depending on the particular research studies and scenarios considered. Nonetheless, by studying and analyzing these attack types, valuable insights can be gained to enhance the security and resilience of control systems in the face of evolving Cyber threats [63].

2.4.2 False Data Injection Attacks

False Data Injection (FDI) attacks are a common form of cyber attack that threaten the integrity of transmitted data by injecting false information, leading to disruptions in system performance. These attacks have been studied extensively in various domains, including disturbed cyber-physical systems [50], multiagent systems [29], power systems [32], and Markov jump systems [36]. In FDI attacks, adversaries gain access to communication channels within Networked Control Systems (NCS) and inject intentionally inaccurate data packets, causing erroneous state estimation and unpredictable or unstable responses that can disrupt system operations [54]. Several learning-based FDI detection methods make use of artificial intelligence techniques like neural networks (NN) [6] [30] and machine learning [51] for observing sys-

tem states. While these approaches provide an effective framework for estimating complex nonlinear dynamical systems, they impose significant computational burdens on the system; scalability is limited as a result. Stability analysis also becomes more complex with these methods. Existing research on FDI attacks has addressed stealthy strategies targeting all sensor measurements [4] [53]. However, fewer studies have explored partial sensor measurement-focused FDI attacks considering resource constraints [84] [74]. Stealthy FDI attack designs against partial sensor measurements have been developed primarily for open-loop unstable systems but warrant further investigation into broader applications. As cyber-security threats continue to evolve, understanding and mitigating false data injection attacks remain crucial aspects in maintaining the integrity of networked control systems across various industries.

2.4.2.1 False Data Injection Attacks Modeling In real-world systems, FDI can sabotage data integrity and cause a significant security issue. Attackers specifically introduce erroneous data into the communication channel between the controller and actuator of a system by taking advantage of a network protocol weakness. Design options for the FDI model that injects additive components into the control input include $\forall t \in (t_k h, t_{k+1} h$

$$\bar{u}(t) = u(t) + g(\hat{x}(t_k h)) \tag{2.9}$$

Where $g(\hat{x}(t_k h)) \in R$ stands for the unidentified FDI state-dependent signal and $u(t)$ represents the designed calculated control input. To adapt the FDI model to the current situation, $g(\hat{x}(t_k h))$ is made up of bogus data and original transmission data, suggesting that FDI may occur covertly and be challenging for detectors to pick up on.

Remark: The sensor to controller channel uses the dynamic PETM to conserve its limited network resources, while the controller actuator channel uses FDIA for transmitting control signals. In actuality, sensor-to-controller communication is susceptible to FDIA. To achieve this, an FDIA detection algorithm may be utilized to determine the attack channel, after which the control technique mentioned above can be employed to counteract the impact of FDIA. Additionally, dynamic PETM may be used on the controller-actuator channel to address resource limitations, which is likewise deserving of more investigation and debate. [77]

2.4.3 Denail Of Service Attacks

DoS attacks, whose purpose is to prevent the attacked computer or network from providing normal service or resource access, make the target service system stop responding or even crash. In fact, the most common cyber attack in NCSs is DoS attacks, and the most common DoS attacks are computer network bandwidth attacks and connectivity attacks. Denial of Service (DoS) attacks pose a significant threat to modern communication networks, as they aim to disrupt the flow of information between connected agents and destabilize systems. These attacks target either one or both channels in a networked system, such as sensor-controller and controller-actuator channels [10, 66]. DoS attackers seek to interrupt data transmission or alter its integrity, compromising the stability and functionality of control systems [2]. There are several types of DoS attacks, including periodic or pulse-width-modulated (PWM) ones that have been widely studied due to their energy constraints, detection avoidance capabilities, and implementation simplicity. The consequences of these attacks on real-time control systems can be severe; for instance, deadline corrective controls may become unstable under DoS conditions [24]. To mitigate the effects of DoS attacks on Networked Control Systems (NCS), researchers have explored various strategies like simulating potential attack scenarios [28], analyzing optimal control through zero-sum games between controllers and strategic jammers [69], developing general models with explicit characterizations for frequency and duration limits while maintaining closed-loop stability using state feedback controllers [15]. Despite these efforts in tackling denial-of-service threats within cyber-physical systems contextually different approaches continue being investigated to ensure reliability and resilience against evolving cyber-security challenges. Some recent advancements include designing resilient observer-based control strategies for continuous-time cyber-physical systems with disturbances and measurement noise under asynchronous DoS attacks on both S-C and C-A channels, packet-based control architectures relying on buffering [22], maximally robust controllers along with other works focused addressing this issue [39] [64].

2.4.3.1 Denial of Service Attacks Modeling

Considering the signal transmitted between the sensor and the controller in the networked control system is vulnerable to DoS attacks which can affect the stable performance and even destroy stability. we consider periodic DoS attacks and the attacker is a power-constraint that needs to consume energy

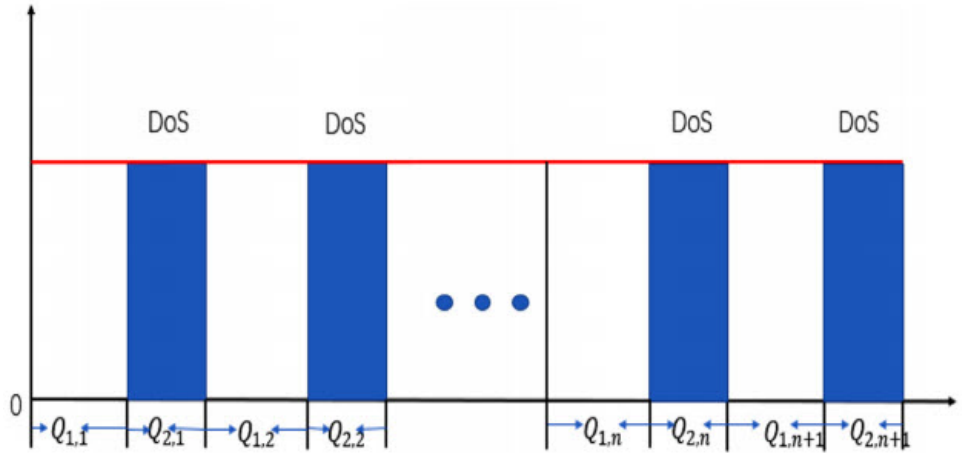

Figure 2.3: The interval of DoS attacks

to carry out the next attack. So we consider the following sequences of DoS interval, and we introduce a model of DoS which blocks the communication channels by taking into consideration a particular power-constraint periodic jamming signal [24], which blocks the communication channels as follows:

$$Z_{DoS}(t) = \begin{cases} 0, t \in ((n-1)T, (n-1)T + T_{Off}), \\ 1, (n-1)T + T_{Off}, nT), \end{cases} \tag{2.10}$$

Where $n \in N$ is the period number : $T \in R_{>0}$ denotes action-period of the jammer: $T_{Off} \in R_{>0}(T_{Off} < T)$ indicates the jammer's sleeping time. The sets $U_{n\in N}(nT, nT + T_{Off})$ indicate the times when the jamming signal is turned off and communication is permitted, and the sets $U_{n\in N}(nT + T_{Off}, nT + T)$ indicate the times when the jamming signal is active and communication is prohibited. During these times, no data may be communicated. It should be noted that contrary to what is claimed in [16], pulse-width modulated jamming does not require that the parameter T_{Off} be time-invariant.Consequently, we presume that there is a real scalar $T_{Off}^{min} \in (0, \infty)$ such that $T_{Off}^{min} \leq T_{Off} < T < \infty$ [12] In general, the DoS jamming signal can affect forward and feedback channels separately. In this paper, we consider the scenario that DoS jamming signals simultaneously affect both forward and feedback channels as in [15]. That is to say, under DoS jamming attacks, the released sampled state cannot reach the controller successfully, and the control signal cannot arrive at the actuator successfully too. In view of this, the output of the actuator $u(t)$ under DoS

attacks can be represented as:

$$u(t) = \begin{cases} Kx(t_{k,n+1}h), t \in [t_{k,n+1}h, t_{k+1,n+1}h] \cap [nT, nT + T_{pff}] \\ 0, t \in [nT + T_{off}, nT + T] \end{cases} \tag{2.11}$$

where $[t_{k,n}h]$ denotes the set of successful control update instants ($t_{0,n+1}h \triangleq nT$). The state equation can be written as:

$$\dot{x}(t) = \begin{cases} Ax(t) + BKx(t_{k,n+1}h) t \in \Re_{k,n} \cap \Im_{1,n} \\ Ax(t), t \in \Im_{2,n} \end{cases} \tag{2.12}$$

2.4.4 Deception attacks Deception attacks, recognized as one of the most critical cyber threats, can severely compromise the integrity of transmitted data by modifying its content or replacing it with malicious signals [25] [71]. As network technologies advance rapidly, the risks posed by deception attacks have become increasingly significant and cannot be ignored. Control problems under deception attacks have attracted considerable attention in recent years due to their potential harmful consequences on Networked Control Systems (NCS) security [18] [75], [37]. These types of cyber attacks involve reconstructing transmitted signals with malicious attack signals that corrupt system states and potentially lead to severe damage to network security. Several studies have been conducted to address control problems subject to deception attacks, such as investigating attack scheduling for a class of stochastic linear systems and addressing H1 filter design problems under these circumstances [18] [37]. Recent works also focus on coping with issues related to deception attacks within NCSs [70]; [65]. However, despite ongoing research in this area, new attack methods continue emerging alongside technological advancements. It is crucial for researchers and cyber-security professionals alike not only to study existing strategies but also to develop novel techniques that mitigate potential vulnerabilities associated with future deception threats. As networks grow more complex and interconnected across various industries and applications, understanding how deception attacks operate becomes essential in safeguarding overall system stability while maintaining robust communication channels against ever-evolving cyber-security challenges.

2.4.4.1 Deception Attacks Model It is presupposed that the attacker may seize control of the system's dynamic $x(t_k h)$ and randomly emit aggressive signals $f(x(t-d(t))$. When deception assaults occur, the simulated signal joins the real signal in the controller's buffer. It is difficult to tell counterfeit signals from non-attacked ones. The following scheduling guidelines are created by us in order to solve this problem: Every time a signal is issued, the event-generator will package together m previous signals $(x(t_k h), ..., x(t_{k-m+1} h))$and deliver them all to the controller at once. This allows for the following expression of the NCSs [73] under randomly occurring deception attacks:

$$\dot{x}(t) = Ax(t) + \theta(t)BKf(x(t - d(t)))+(1 - \theta(t))BK(x(t - \tau(t))) \tag{2.13}$$

where $\theta(t) \in (0, 1)$ denotes the occurring probability of deception attacks. When $\theta(t) = 0$, it means there are no attacks, when $\theta(t) = 1$, the original signal $(x(t_k h), ..., x(t_{k-m+1} h))$ is captured by the attacker and replaced by an aggressive signal $f(x(t-d(t))$. The mathematical characters of $\theta(t)$ are assumed to be known as $\mathbb{E}(\theta(t)) = \bar{\theta}$. The aggressive signals $f(x(t-d(t))$ are assumed to satisfy

$$\|f(x(t-d(t)))\|_2 \leq \|G(x(t-d(t)))\|_2 \tag{2.14}$$

where G is a respective known matrix representing the upper bound of the non-linearity $f(.), 0 \leq d(t) \leq d_M$. Without loss of generality, assume that G_{max} is the largest one among G [70].

2.4.5 Replay attacks

Replay attacks, also known as playback attacks, are a type of cyber attack that exploits the lack of knowledge about a system's dynamics by an attacker [46]. These attacks have been successfully used in real-world situations such as the Stuxnet worm that targeted Iranian uranium enrichment facilities [23], [21], [47]. The basic strategy behind replay attacks is fairly simple. The attacker hijacks the sensors, observes and records their readings for a certain amount of time, and then repeats them while carrying out their attack [11]. This method is particularly appealing to attackers who do not possess knowledge about the system's dynamics but are aware that it should remain in a steady state during their attack. Various security measures against replay attacks have been proposed in literature. Some studies suggest injecting noise into control signals or

utilizing existing communication noise within Cyber-Physical Systems (CPSs) as authentication signals to detect potential intrusions [62], [67]. In addition to these approaches, recent advancements in cyber-security research propose developing more sophisticated detection mechanisms against such threats. For instance, machine learning algorithms can be employed to identify anomalies and unusual patterns indicative of replay attacks. Furthermore, implementing secure hardware-based solutions like secure enclaves may serve as another layer of protection against this class of threats [41]. Overall, protecting systems from replay attacks remains an important area within cyber-security research due to its potential impact on critical infrastructure.

2.4.5.1 Replay Attacks Modeling We assume the attacker has the ability to can get the sampling values at the sampling instant and can memorize these values. For some certain transition instant, it can replace these values with previously stored sampling values [48]. Without sacrificing generality, we presumptively assume that the data collection and data replaying actions might occur at random without mentioning specified patterns or distributions for the occurrences of replay assaults, with the intention of implementing triggerring requirements that are less met. Keep in mind that an opponent with limited energy will experience reduced attack impacts from many discrete attacks within any given period. When eroding system stability, the adversary is more inclined to undertake continuous attacks as opposed to discrete ones since they need less energy. We assume $t_k h$ as the time instant at which the control signal is successfully transmitted. The adversary will launch $m(k)$ consecutive replay packets between the $k-th$ transmitted instant $t_k h$ and the next successful transmitted instant is $t_{k+1} h$. A new notation is indicated by $[s_1^k h, s_2^k h, ...s_{m(k)}^k h]$ which represents the set of consecutive data-replaying instants between two successfully transmission instants $(t_k h, t_{k+1} h)$.

$$t_{k+1} h = t_k h + min_{l \in N}[(x(i_k h) - x(t_k h))^T \Phi (x(i_k h) - x(t_k h)) > \sigma x(t_k h)^T \Phi x(t_k h)] \quad (2.15)$$

where $x(t_k h)$ represents the correct transmitted state at $t_k h$; $i_k h = t_k h + lh, l \in N, i.e. x(i_k h) - x(t_k h)$ represents the state error between the current sampling instant and the latest successful instant; σ is a pre-selected constant and Φ is a positive definite weighting matrix to be designed. Due to the effects of attacks, some state signals of desiring transmitted control action may be altered. The ETC strategy mentioned above can not be applied

to determine whether or not to transmit the control signal. The following resilient ETC strategy is proposed to solve the problems, the triggering condition under replay attacks will be:

$$s^k_{m(i)+1}h = s^k_{m(i)}h + min_{\gamma\in N}[e(l^k_{m(i)}h)^T \Phi e(l^k_{m(i)}h) > \delta x(s^k_{m(i)})^T \Phi x(s^k_{m(i)})] \tag{2.16}$$

where $0 \leq m(i) \leq m(k)$, $e(l^k_{m(i)}h) = x(l^k_{m(i)}h) - x(s^k_{m(i)})$, $l^k_{m(i)}h = s^k_{m(i)}h + \gamma h, \gamma \in N$. Moreover, a considered time delay τ_k is stochastic according to a certain distribution, which is different from paper [59] and it shows a more practical situation in NCSs. Also, we have considered noise disturbance at the plant side. Based on (2.15) and (2.16), this paper constructs a resilient ETC strategy for compensating the undesiring data replaying induced by replay attacks and network time delays.

2.5 Conclusion

In this chapter, we have explored the fundamental aspects of networked control systems and their relationship with cyber-security. firstly, we delved into the various components of networked control systems and examined their respective roles. Understanding these components is crucial for comprehending the system's overall architecture and functionality. An essential aspect of this thesis was the modeling of networked control systems and their imperfections. By studying the system's behavior and performance under various conditions, we gained insights into its resilience and vulnerability to cyber threats. Moving further, we focused on cyber attacks, a critical concern in the realm of networked control systems. We defined cyber attacks and emphasized their impact on system performance. Specifically, we highlighted four prominent types of cyber attacks: false data injection attacks (FDI), denial of service attacks (DoS), deception attacks, and replay attacks. For each type, we explored their specific characteristics and potential consequences on the system's functionality. This chapter underscores the critical importance of considering cyber-security in the design, implementation, and operation of networked control systems. By understanding the components, structures, and vulnerabilities, as well as the types and implications of cyber attacks, researchers and practitioners can make informed decisions and develop robust security measures to protect networked control systems from potential threats.

Chapter 3

Stability analysis and robust control of NCSs

3.1 Introduction

This chapter is devoted to the linear Networked Control Systems (NCS) subject to transmission delays and stochastic deception attacks. Randomly occurring deception attacks are considered in both sensor-to-controller and controller-to-actuator channels, assuming $\mathcal{L}_2$ norm bounded malicious signals injected by the attacker. Based on a suitable asymmetric Lyapunov functional, relaxed LMI-based control design conditions are obtained. Finally, a numerical example is considered to illustrate the effectiveness of the proposed results, compared to previous related ones. The main contribution of this paper is to propose a controller who make the system robust and resilient for network delays and cyber attacks. In this context, to cope with the security problem of NCSs, randomly occurring deception attacks are considered in both the sensors-to-controller and controller-to-actuators channels, where bounded malicious signals can be injected by attackers. Based on the considired controller gain matrix, new relaxed LMIs-based design conditions are proposed by selecting an asymmetric LKF. The effec- tiveness of the proposed resilient NCS design approach will be illustrated and compared to previous related results with a simulation example.

Notations 3.1 *The symbol * in matrices indicates block transpose quantities. For a square matrix M,* $\mathcal{H}(M) = M + M^T$ *and* $M > 0$ (< 0) *denotes their positive (negative) definiteness.* $\| \, . \, \|_2$ *stands for the* $L_2[0, \infty)$ *norm. For column vectors* v_1, ..., v_n,

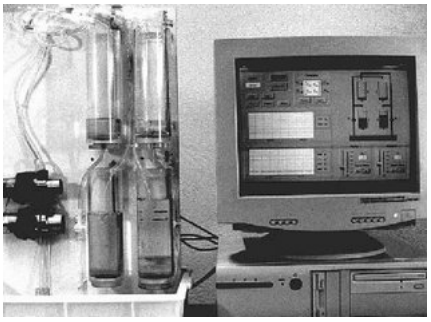

Figure 3.1: The quadruple-tank process shown together with a controller interface running on a PC [82].

$\text{col}\{v_1, v_2, ..., v_n\} = \begin{bmatrix} v_1^T & \dots & v_n^T \end{bmatrix}^T$. $\mathcal{I}_r = \{1, ..., r\}$ *is a finite set of positive integers. Finally,* $\forall j \in \mathcal{I}_{10}$*, we denote the block entry matrices* $e_j = \begin{bmatrix} 0_{n\times(j-1)n} & I_{n\times n} & 0_{n\times(10-j)n} \end{bmatrix}^T \in \mathbb{R}^{10n\times n}$*, e.g.* $e_4 = \begin{bmatrix} 0 & 0 & 0 & I & 0 & 0 & \dots & 0 & 0 \end{bmatrix}^T$.

3.2 Petrochemical system Modeling

Among the plethora of petrochemical systems available for modeling, we have carefully selected the quadruple-tank process as our focal point.

3.2.1 Quadruple-Tank Process Modeling

The quadruple-tank process represents a combination of two double-tank processes, commonly employed in control laboratories as standard models [3]. This configuration, while straightforward, offers valuable insights into complex multi-variable dynamics.

Our main objective is to effectively regulate the levels, y_1 and y_2, in the lower two tanks utilizing a pair of pumps. To achieve this, we manipulate the process inputs, v_1 and v_2, which correspond to the voltage signals applied to the pumps. It is important to note that the model utilized in our virtual lab takes into account disturbances arising from inflows and outflows in the upper-level tanks, ensuring a more comprehensive understanding of the system. [19]

$$\frac{dh_1}{dt} = -\frac{a_1}{A_1}\sqrt{2gh_1} + \frac{a_3}{A_1}\sqrt{2gh_3} + \frac{\gamma_1 K_1}{A_1}v_1 \tag{3.1}$$

$$\frac{dh_2}{dt} = -\frac{a_2}{A_2}\sqrt{2gh_2} + \frac{a_4}{A_2}\sqrt{2gh_4} + \frac{\gamma_2 K_2}{A_2}v_2 \tag{3.2}$$

$$\frac{dh_3}{dt} = -\frac{a_3}{A_3}\sqrt{2gh_3} + \frac{(1-\gamma_2)K_2}{A_3}v_2 \tag{3.3}$$

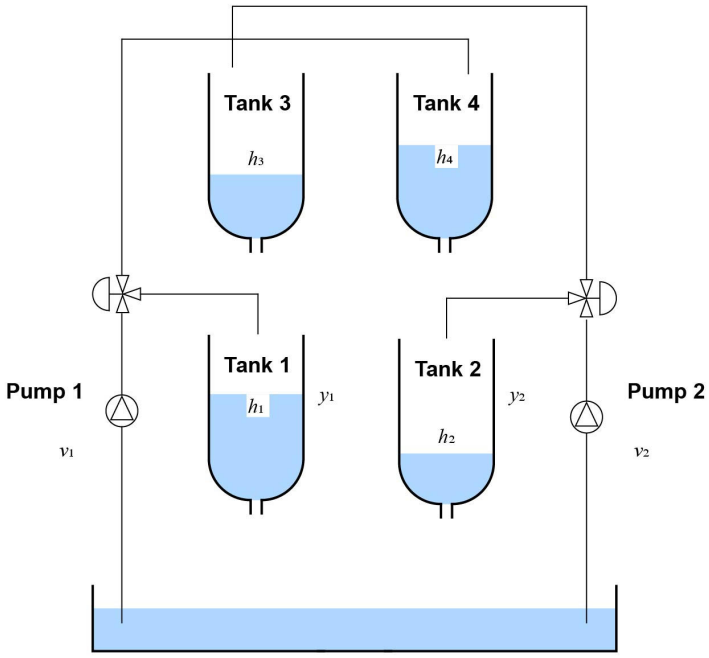

Figure 3.2: Schematic representation of the quadruple-tank process

$$\frac{dh_4}{dt} = -\frac{a_4}{A_4}\sqrt{2gh_4} + \frac{(1-\gamma_1)K_1}{A_4}v_1 \tag{3.4}$$

with: $A_i$cross-section of Tank, a_i cross-section of the outlet hole, h_i water level. Pump i is subjected to a voltage, denoted as v_i, which results in a flow denoted as $k_i v_i$. The parameters γ_1 and $\gamma_2 \in (0, 1)$, are determined based on the valve settings prior to conducting an experiment. The flow rate into Tank 1 is γ_1 times k_1 times v_1, while the flow rate into Tank 4 is $(1 - \gamma_1)$ times k_1 times v_1. Similarly, the flow rates into Tank 2 and Tank 3 can be determined. The acceleration due to gravity is represented by the symbol g. The measured level signals are $k_c H_1$ and $k_c H_2$. The specific values for the laboratory process parameters can be found in the table provided below:

A_1, A_3	$[cm^2]$	23
A_2, A_4	$[cm^2]$	32
a_1, a_3	$[cm^2]$	0.071
a_2, a_4	$[cm^2]$	0.057
k_c	[V/cm]	0.50
g	$[cm/s^2]$	981

Consequently, the complete physical model is governed by a mathematical equation derived from the experimental problem, which proposed the state-space equation for the quadruple-tank process and devised the state feedback controller in the following manner:

$$\bar{A}_1 = \begin{bmatrix} -0.0021 & 0 & 0 & 0 \\ 0 & -0.0021 & 0 & 0 \\ 0 & 0 & -0.0424 & 0 \\ 0 & 0 & 0 & -0.0424 \end{bmatrix}, \bar{A}_2 = \begin{bmatrix} 0 & 0 & 0.0424 & 0 \\ 0 & 0 & 0 & 0.0424 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$
$$\bar{B}_1 = \begin{bmatrix} 0.1113\gamma_1 & 0 & 0 & 0 \\ 0 & 0.1042\gamma_2 & 0 & 0 \end{bmatrix}^T, \bar{B}_2 = \begin{bmatrix} 0. & 0 & 0 & 0.1113(1-\gamma_1) \\ 0 & 0 & 0.1042(1-\gamma_2) & 0 \end{bmatrix}^T \tag{3.5}$$

$\gamma_1 = 0.333$, $\gamma_2 = 0.307$, $\bar{u} = K\bar{x}(t_k)$ For simplicity, it was assumed that $\tau_1 = 0$ and $\tau_2 = \tau_3 = \tau(t)$. Then, the controller is $\bar{u}(t) = Kx(t - \tau(t))$. Let $A = \bar{A}_1 + \bar{A}_2$, and $B = \bar{B}_1 + \bar{B}_2$. Then, the quadruple-tank process can be rewritten to the form of system (3.12).

The quadruple-tank process can be accurately described using Networked Control Systems (NCSs). The main goals are to analyze the stability of this petrochemical system over a communication network and so design a new state feedback control gains robust against deception attack. For that, we need to recall the following preliminaries.

3.3 Preliminaries and Problem Statement

The block diagram of the considered NCS and subject to network-induced delay and deception attack is shown in Fig 3.3 In this NCS scheme, we assume that the plant is represented by linear state space models given by:

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) \end{cases} \tag{3.6}$$

where $x(t) \in \mathbb{R}^n$ and $u(t) \in \mathbb{R}^m$ are the state and input vectors, $A \in \mathbb{R}^{n\times n}$ and $B \in \mathbb{R}^{n\times m}$ are constant matrices.

Assumption 3.1 *The state variables are available from the sensors' measurements. Their*

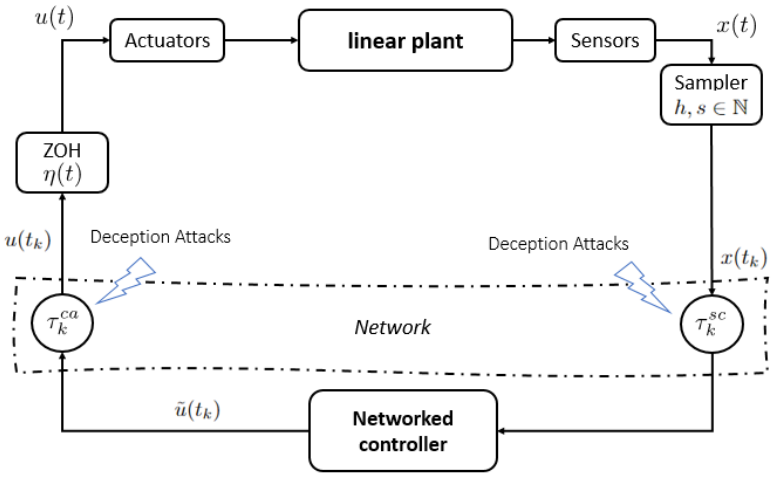

Figure 3.3: NCS subject to deception attacks.

values are broadcast together as single packets at each sampling instant to the controller device through the sensors-to-controller channel.

Assumption 3.2 *The sensors are clock-driven with a fixed sampling period h and the controller and actuators are event-driven.*

Let $k \in \mathbb{N}$ be the actual sampling number, we denote τ_k^{sc} and τ_k^{ca}, respectively the sensors-to-controller and the controller-to-actuators network-induced delays, and so $\tau_k = \tau_k^{sc} + \tau_k^{ca}$ the overall network-induced delay on the feedback loop. With the considered NCS, the ZOH allows keeping the control signal constant during the interval $\mathbb{I}_z = [t_k + \eta_k, t_{k+1} + \eta_{k+1})$, Moreover, $\forall t \in \mathbb{I}_z$, let $\eta(t) = t - t_k$, which satisfies $0 \leq \tau_1 = \eta_1 \leq \tau_k \leq \eta(t) \leq \bar{\tau} + h = \eta_2$ and $\dot{\eta}(t) = 1$. Hence we can write $x(t_k) = x(t - \eta(t))$. In this context, we consider the following ideal networked sampled-data control law:

$$u(t) = Kx(t_k) = Kx(t - \eta(t)) \tag{3.7}$$

where $K \in \mathbb{R}^{m \times n}$ is a gain matrix to be synthesized.

The communication channels are vulnerable to an attacker who can alter the transmitted information. That is to say, an attacker can replace the system's state $x(t_k)$ measurement and controller's output signal $\tilde{u}(t_k)$ by aggressive signals $f(x(t_k)) \in \mathbb{R}^n$ and $g(\tilde{u}(t_k)) \in \mathbb{R}^m$ respectively, released randomly. When such deception attacks occur, the actual faked signal (at t_k) would join the buffer of the controller together with the previously transmitted true or eventually fake signal (at t_k).

Hence, the control law (3.7) becomes:

$$u(t_k) = \sigma_u(t_k)\tilde{u}(t_k) + (1 - \sigma_u(t_k))g(\tilde{u}(t_k)) \tag{3.8}$$

with

$$\tilde{u}(t_k) = \sigma_x(t_k)Kx(t_k) + (1 - \sigma_x(t_k))Kf(x(t_k)) \tag{3.9}$$

, Then

$$u(t_k)=\sigma_{ux}(t_k)Kx(t_k)+(\sigma_u(t_k)-\sigma_{ux}(t_k))Kf(x(t_k))+(1-\sigma_u(t_k))g(\tilde{u}(t_k)) \tag{3.10}$$

where $\sigma_u(t_k) \in \{0, 1\}$, $\sigma_x(t_k) \in \{0, 1\}$ and $\sigma_{ux}(t_k) = \sigma_u(t_k)\sigma_x(t_k)$ are the occurring functions of the deception attacks. That is to say, if $\sigma_u(t_k) = 1$ and $\sigma_x(t_k) = 1$, there are no attacks. Else, if $\sigma_u(t_k) = 0$ or $\sigma_x(t_k) = 0$, the original signals $x(t_k)$ or $u(t_k)$ are respectively replaced by the attacker as the aggressive signals $f(x(t_k))$ or $g(\tilde{u}(t_k))$. Note that it is hard to distinguish the faked signals from the non-attacked ones. To get rid of this dilemma, similarly to [70], the following assumption is made.

Assumption 3.3 *The mathematical expectation $\bar{\sigma}_u$ and $\bar{\sigma}_x$ of respectively $\sigma_u(t_k)$ and $\sigma_x(t_k)$ are known, i.e.* $\mathrm{E}(\sigma_x(t_k)) = \bar{\sigma}_x \in [0, 1]$ *and* $\mathrm{E}(\sigma_u(t_k)) = \bar{\sigma}_u \in [0, 1]$. *Moreover, we assume that $f(x(t_k))$ and $g(\tilde{u}(t_k))$ are $\mathcal{L}_2$-norm bounded such that:*

$$\|f(x(t_k))\|_2 \leq \|G_1 x(t_k)\|_2, \ \|g(\tilde{u}(t_k))\|_2 \leq \|G_2\tilde{u}(t_k)\|_2 \tag{3.11}$$

where $G_1 \in \mathbb{R}^{n\times n}$ and $G_2 \in \mathbb{R}^{m\times m}$ are known matrices.

Substituting (3.10) into (3.6), yields the closed-loop dynamics:

$$\begin{cases} \dot{x}(t) = Ax(t) + \sigma_{ux}(t_k)BKx(t-\eta(t)) + (\sigma_u(t_k) - \sigma_{ux}(t_k))BKf(x(t_k)) + (1-\sigma_u(t_k))Bg(\tilde{u}(t_k)) \\ y(t) = Cx(t) \end{cases} \tag{3.12}$$

Problem statement. Provide LMI-based design conditions for the gain matrix K, such that the closed-loop NCS (3.12) is Globally Asymptotically Stable (GAS) and resilient to deception attacks under Assumption 3.3.

Lemma 1 *[14] Let $\xi \in \mathbb{R}^n$, $G \in \mathbb{R}^{m\times n}$ and $Q = Q^T \in \mathbb{R}^{n\times n}$ such that rank$(G) < n$. Then,*

$\xi^T Q\xi < 0$, $\forall \xi \in \{\xi \in \mathbb{R}^n : \xi \neq 0, G\xi = 0\}$, *iff:*

$$\exists T \in \mathbb{R}^{n\times m} : Q + \mathcal{H}(TG) \prec 0 \tag{3.13}$$

Lemma 2 *(Extended Jensen's Inequality [57]) For any constant matrix* $\begin{bmatrix} Q & S \\ * & Q \end{bmatrix} > 0$, *a positive scalar* $\bar{\tau}$ *satisfying* $0 < \tau(t) < \bar{\tau}$ *and vector function* $\dot{x} : [-\bar{\tau}, 0] \to \mathbb{R}^n$ *such that the concerned integrals are well defined, we have:*

$$\begin{aligned} &-\bar{\tau}\int_{t-\bar{\tau}}^{t} \dot{x}^T(s)Q\dot{x}(s)ds \\ &\leq \begin{bmatrix} x(t)-x(t-\tau(t)) \\ x(t-\tau(t))-x(t-\bar{\tau}) \end{bmatrix}^T \begin{bmatrix} Q & S \\ * & Q \end{bmatrix} \begin{bmatrix} x(t)-x(t-\tau(t)) \\ x(t-\tau(t))-x(t-\bar{\tau}) \end{bmatrix} \end{aligned}$$

Lemma 3 *[85] For* $f(s) = s^2\Phi_2 + s\Phi_1 + \Phi_0$, $f(s) < 0$ *for* $s \in [0, \bar{\tau}]$ *if and only if there exists a matrix* $M \in \mathbb{R}^{p\times p}$ *with* $M + M^T > 0$ *such that*

$$\begin{bmatrix} \Phi_0 & \frac{1}{2}\Phi_1 + \bar{\tau}M \\ \star & \Phi_2 - M - M^T \end{bmatrix} < 0$$

Corollary 3.1 *For* $f(q) = q^2\Phi_2 + q\Phi_1 + \Phi_0$, $f(q) < 0$ *for* $q \in [\eta_1, \eta_2]$ *if and only if there exists a matrix* $M \in \mathbb{R}^{p\times p}$ *with* $M + M^T > 0$ *such that*

$$\begin{bmatrix} f(\eta_1) & \eta_1\Phi_2 + \frac{1}{2}\Phi_1 + (\eta_2 - \eta_1)M \\ \star & \Phi_2 - M - M^T \end{bmatrix} < 0$$

Proof 3.1 *Straightforward from the conditions of lemma 3 with the change of variable* $q = s - \tau_1 \in [0, \eta_2 - \eta_1]$.

3.4 Main result

3.4.1 Stability Analysis We will first consider the case where the controller gain matrix K is priory known, namely the LMI closed-loop stability conditions. The following theorem summarizes LMI-based conditions satisfying the above problem statement.

Theorem 3.1 *For given scalars* $\eta_2 > \eta_1 > 0$, $\bar{\sigma}_u \in \begin{bmatrix} 0 & 1 \end{bmatrix}$ *and* $\bar{\sigma}_x \in \begin{bmatrix} 0 & 1 \end{bmatrix}$, *the closed-loop*

NCS (3.12) *is GAS and resilient to deception attack under Assumption 3.3, if there exist the matrices* $P>0$, $Q_1>0$, $Q_2>0$, $S_1>0$, $S_2>0$, $R_1>0$, $R_2>0$, $\mathcal{W}$, $\mathcal{T}$, M, W *and* K *such that:*

$$\begin{bmatrix} R_2 & W \\ * & R_2 \end{bmatrix} > 0$$
$$\begin{bmatrix} \sum_{i=1}^{3}(\eta_4^i\Phi_4^i+\Phi_i)+\mathcal{H}(\mathcal{TG}) & \star \\ \eta_1\Phi_3^{2T}+\frac{1}{2}\Phi_3^{1T}+(\eta_2-\eta_1)\mathcal{W}^T & \Phi_3^2-\mathcal{W}-\mathcal{W}^T \end{bmatrix} < 0 \tag{3.14}$$

and are satisfied with:

$$\mathcal{G} = [\ A \quad 0 \quad \bar{\sigma}_{ux}BK \quad 0 \quad -I \quad 0 \quad 0 \quad \bar{\sigma}_{ux}BK \quad (\bar{\sigma}_u - \bar{\sigma}_{ux})BK \quad (1-\bar{\sigma}_u)B\ ], \tag{3.15}$$

$$\Phi_1 = \mathcal{H}(e_1Pe_5^T)+e_5(S_1+S_2)e_5^T-e_6S_1e_6^T-e_7S_2e_7^T, \tag{3.16}$$

$$\begin{aligned}\Phi_2 =& e_1(Q_1+Q_2-R_1)e_1^T+\mathcal{H}(e_1R_1e_2^T)-e_2(R_2+R_1+Q_1)e_2^T+\mathcal{H}(e_2(R_2-W)e_3^T)\\ &+\mathcal{H}(e_2We_4^T)+e_3(\mathcal{H}(W)-2R_2)e_3^T+\mathcal{H}(e_3(R_2-W)e_4^T)-e_4(R_2+Q_2)e_4^T\\ &+e_5(\eta_1^2R_1+(\eta_2-\eta_1)^2R_2)e_5^T,\end{aligned} \tag{3.17}$$

$$\Phi_3 = (e_3+e_8)K^TG_1^TG_1K(e_3+e_8)^T \tag{3.18}$$

$$\Phi_4^0 = \eta_2(\Pi_1^2\mathcal{M}\Pi_2-\eta_2\Pi_3^2\mathcal{M}\Pi_2-\eta_2\Pi_1^2\mathcal{M}\Pi_4$$

$$\Phi_4^1 = -\Pi_1^1\mathcal{M}\Pi_2+(\eta_2+\eta_1)\left(\Pi_3^1\mathcal{M}\Pi_2+\Pi_3^2\mathcal{M}\Pi_2+\Pi_1^1\mathcal{M}\Pi_4+\Pi_1^2\mathcal{M}\Pi_4\right)$$

$$\Phi_4^2 = -\Pi_1^1\mathcal{M}\Pi_4-\Pi_3^1\mathcal{M}\Pi_2$$

$$\Pi_1^1 = \begin{bmatrix} \frac{1}{\eta_1}(e_2-e_3) \\ e_2-e_1 \\ e_4-e_2 \end{bmatrix}, \Pi_1^2 = \begin{bmatrix} 0 \\ e_1-e_2 \\ e_2-e_4 \end{bmatrix}, \Pi_2 = \begin{bmatrix} e_2-e_3 \\ e_1-e_2 \\ e_2-e_4 \end{bmatrix},$$

$$\Pi_3^1 = \begin{bmatrix} \frac{1}{\eta_1}e_6 \\ \frac{1}{\eta_1}(e_1-e_2)-e_5+e_6 \\ \frac{1}{\eta_1}(e_2-e_4)-e_6+e_7 \end{bmatrix}, \Pi_3^2 = \begin{bmatrix} 0 \\ e_5-e_6 \\ e_6-e_7 \end{bmatrix}, \Pi_4 = \begin{bmatrix} e_6 \\ e_5-e_6 \\ e_6-e_7 \end{bmatrix}.$$

Proof 3.2 *let us Consider an asymmetric LKF candidate given by:*

$$V(t) = V_1(t)+V_2(t)+V_3(t) \tag{3.19}$$

with:

$$V_1(t) = x^T(t)Px(t) + \int_{t-\eta_1}^{t} \dot{x}^T(s)S_1\dot{x}(s)ds + \int_{t-\eta_2}^{t} \dot{x}^T(s)S_2\dot{x}(s)ds, \tag{3.20}$$

$$\begin{aligned} V_2(t) = &\int_{t-\eta_1}^{t} x^T(s)Q_1x(s)ds + \eta_1 \int_{-\eta_1}^{0}\int_{t+v}^{t} \dot{x}^T(s)R_1\dot{x}(s)dsdv \\ &+ \int_{t-\eta_2}^{t} x^T(s)Q_2x(s)ds + (\eta_2-\eta_1)\int_{-\eta_2}^{-\eta_1}\int_{t+v}^{t} \dot{x}^T(s)R_2\dot{x}(s)dsdv, \end{aligned} \tag{3.21}$$

$$V_3(t) = (\eta_2 - \eta(t))\xi_1^T(t)M\xi_2(t), \tag{3.22}$$

where $\xi_1(t) = \mathrm{col}\Big\{x(t-\eta_1) - x(t-\eta(t)), (\eta(t)-\eta_1)\int_{t-\eta_1}^{t} \dot{x}(s)ds,$
$(\eta(t)-\eta_1)\int_{t-\eta_2}^{t-\eta_1} \dot{x}(s)ds\Big\}$ *and* $\xi_2(t) = \mathrm{col}\Big\{x(t-\eta_1) - x(t-\eta(t)), \int_{t-\eta_1}^{t} \dot{x}(s)ds, \int_{t-\eta_2}^{t-\eta_1} \dot{x}(s)ds\Big\}$. *The LKF candidate* (3.19) *is positive if* $P>0$, $S_1>0$, $S_2>0$, $Q_1>0$, $Q_2>0$, $R_1>0$ *and* $R_2>0$. *Note that, at the release instants, i.e. when* $\eta(t)=\eta_1$ *and* $\eta(t)=\eta_2$, *we have* $V_3(x(t))=0$. *Hence, we don't need M to be symmetric positive definite if the whole LKF* $V(t)$ *in* (3.19) *is monotonously decreasing* $\forall t \in [t-\eta_2, t-\eta_1)$. *In this case, the NCS* (3.12) *is GAS if:*

$$\dot{V}(t) = \dot{V}_1(t) + \dot{V}_2(t) + \dot{V}_3(t) < 0 \tag{3.23}$$

Let us first define

$$\zeta(t) = \mathrm{col}\{x(t), x(t-\eta_1), x(t-\eta(t), x(t-\eta_2), \dot{x}(t), \dot{x}(t-\eta_1), \dot{x}(t-\eta_2), e(t_k), f(x(t_k)), g(\tilde{u}(t_k))\}$$

. Then, the derivative of $V_1(t)$ *(see* (3.20)*) yields:*

$$\begin{aligned} \dot{V}_1(t) &= 2x^T(t)P\dot{x}(t) + \dot{x}^T(t)(S_1+S_2)\dot{x}(t) \\ &- \dot{x}^T(t-\eta_1)S_1\dot{x}(t-\eta_1) - \dot{x}^T(t-\eta_2)S_2\dot{x}(t-\eta_2) \\ &= \zeta^T(t)\Phi_1\zeta(t) \end{aligned} \tag{3.24}$$

with Φ_1 *is defined in Theorem 1. Now, let us focus on the time derivative of* (3.21)*, one has:*

$$\begin{aligned} \dot{V}_2(t) &= x^T(t)(Q_1+Q_2)x(t) - x^T(t-\eta_1)Q_1x(t-\eta_1) \\ &- x^T(t-\eta_2)Q_2x(t-\eta_2) + \dot{x}^T(t)\left(\eta_1^2R_1 + (\eta_2-\eta_1)^2R_2\right)\dot{x}(t) \\ &- \eta_1\int_{t-\eta_1}^{t} \dot{x}^T(s)R_1\dot{x}(s)ds - (\eta_2-\eta_1)\int_{t-\eta_2}^{t-\eta_1} \dot{x}^T(s)R_2\dot{x}(s)ds \end{aligned} \tag{3.25}$$

Applying Jensen's Lemma (2)*, yields:*

$$-\eta_1 \int_{t-\eta_1}^{t} \dot{x}^T(s) R_1 \dot{x}(s) ds \leq -\zeta^T(t)(e_1-e_2) R_1 (e_1-e_2)^T \zeta(t) \tag{3.26}$$

Also, from Theorem 1 in [57], if $\begin{bmatrix} R_2 & W \\ * & R_2 \end{bmatrix} > 0$*, we can write:*

$$-(\eta_2-\eta_1)\int_{t-\eta_2}^{t-\eta_1} \dot{x}^T(s) R_2 \dot{x}(s) ds \leq \begin{bmatrix} x(t-\eta_1) \\ x(t-\eta(t)) \\ x(t-\eta_2) \end{bmatrix}^T \begin{bmatrix} -R_2 & R_2-W & W \\ * & -2R_2+\mathcal{H}(W) & R_2-W \\ * & * & -R_2 \end{bmatrix} \begin{bmatrix} x(t-\eta_1) \\ x(t-\eta(t)) \\ x(t-\eta_2) \end{bmatrix} \tag{3.27}$$

Therefore, from (3.26) *and* (3.27)*, we obtain:*

$$\dot{V}_2(t) \leq \zeta^T(t) \Phi_2 \zeta(t) \tag{3.28}$$

with Φ_2 *is defined in Theorem 1.*

Taking the derivative of (3.22)*, we get:*

$$\begin{aligned} \dot{V}_3(t) &= (\eta_2-\eta(t))(\dot{\xi}_1^T(t) M \xi_2(t) + \xi_1^T(t) M \dot{\xi}_2(t)) - \xi_1^T(t) M \xi_2(t) \\ &= \zeta^T(t)(\eta^2(t)\Phi_3^2 + \eta(t)\Phi_3^1 + \Phi_3^0)\zeta(t) \end{aligned} \tag{3.29}$$

with $\Phi_3^0 = \eta_2 \Pi_1^2 \mathcal{M} \Pi_2 - \eta_2 \Pi_3^2 \mathcal{M} \Pi_2 - \eta_2 \Pi_1^2 \mathcal{M} \Pi_4$, $\Phi_3^1 = -\Pi_1^1 \mathcal{M} \Pi_2 + (\eta_2+\eta_1)(\Pi_3^1 \mathcal{M} \Pi_2 + \Pi_3^2 \mathcal{M} \Pi_2 + \Pi_1^1 \mathcal{M} \Pi_4 + \Pi_1^2 \mathcal{M} \Pi_4)$, $\Phi_3^2 = -\Pi_1^1 \mathcal{M} \Pi_4 - \Pi_3^1 \mathcal{M} \Pi_2$ *and where* Π_1^1, Π_1^2, Π_2, Π_3^1, Π_3^2 *and* Π_4 *are defined in Theorem 1. From* (3.24)-(3.29)*, the inequality (3.23) is satisfied if:*

$$\zeta^T(t)\left(\eta^2(t)\Phi_3^2 + \eta(t)\Phi_3^1 + \Phi_3^0 + \Phi_1 + \Phi_2\right)\zeta(t) < 0 \tag{3.30}$$

Let us rewrite (3.12) *as* $\mathcal{G}\zeta(t) = 0$ *with:*

$$\mathcal{G} = \begin{bmatrix} A & 0 & \bar{\sigma}_{ux} BK & 0 & -I & 0 & 0 & \bar{\sigma}_{ux} BK & (\bar{\sigma}_u - \bar{\sigma}_{ux}) BK & (1-\bar{\sigma}_u) B \end{bmatrix} \tag{3.31}$$

Applying the Finsler's lemma (1)*, the inequality (3.30) holds if* $\exists \mathcal{K} \in \mathbb{R}^{10n \times n}$ *such that:*

$$\zeta^T(t)(\eta^2(t)\Phi_3^2 + \eta(t)\Phi_3^1 + \Phi_3^0 + \Phi_1 + \Phi_2 + \mathcal{H}(\mathcal{K}\mathcal{G}))\zeta(t) < 0 \tag{3.32}$$

Introducing the deception attack condition (3.11)*, then* $\forall t \in \mathbb{I}_l$*,* (3.32) *holds if:*

$$\begin{aligned}
&\zeta^T(t)(\eta^2(t)\Phi_3^2+\eta(t)\Phi_3^1+\Phi_3^0+\Phi_1+\Phi_2+\mathcal{H}(\mathcal{KG}))\zeta(t)\\
&+x^T(t_k)\Big(\sigma_x(t_k)G_2^TG_2+\sigma_u(t_k)K^TG_1^TG_1K\Big)x(t_k)\\
&-\sigma_u(t_k)g^T(\tilde{u}(t_k))g(\tilde{u}(t_k))\\
&+f^T(x(t_k))\Big(\sigma_u(t_k)K^TG_1^TG_1K-\sigma_xI\Big)f(x(t_k)<0
\end{aligned} \tag{3.33}$$

Since $\mathbb{E}(\sigma_u(t_k)) = \bar{\sigma}_u$ *and* $\mathbb{E}(\sigma_x(t_k)) = \bar{\sigma}_x$*, the mathematical expectation* $\mathbb{E}(\dot{V}(t)) \leq 0$ *if,* $\forall\zeta(t) \neq 0$*:*

$$\begin{aligned}
&\eta^2(t)\Phi_3^2+\eta(t)\Phi_3^1+\Phi_3^0+\Phi_1+\Phi_2+\mathcal{H}(\mathcal{KG})+(e_3+e_8)\Big(\bar{\sigma}_xG_2^TG_2+\bar{\sigma}_uK^TG_1^TG_1K\Big)(e_3+e_8)^T\\
&+e_9\Big(\bar{\sigma}_uK^TG_1^TG_1K-\bar{\sigma}_xI\Big)e_9^T-\bar{\sigma}_ue_{10}e_{10}^T<0
\end{aligned} \tag{3.34}$$

By applying corollary 1 extended from lemma (3)*, we get* (3.14)*.*

3.4.2 Control Design Condition

Theorem 3.2 *For given scalars* $\eta_2>\eta_1>0$*,* $\varepsilon_1\geq 0$*,* $\varepsilon_2\geq 0$*,* $\bar{\sigma}_u\in\begin{bmatrix}0 & 1\end{bmatrix}$ *and* $\bar{\sigma}_x\in\begin{bmatrix}0 & 1\end{bmatrix}$*, the closed-loop NCS* (3.12) *is GAS and resilient to deception attack under Assumption 3.3, if there exist the matrices* $X>0$*,* $\tilde{P}>0$*,* $\tilde{Q}_1>0$*,* $\tilde{Q}_2>0$*,* $\tilde{S}_1>0$*,* $\tilde{S}_2>0$*,* $\tilde{R}_1>0$*,* $\tilde{R}_2>0$*,* $\tilde{M}$*,* $\tilde{W}$*,* $\tilde{\mathcal{W}}$ *and* $\tilde{K}$ *such that:*

$$\begin{aligned}
&\begin{bmatrix}\tilde{R}_2 & \tilde{W}\\ * & \tilde{R}_2\end{bmatrix}>0\\
&\begin{bmatrix}
\sum\limits_{\substack{j=0\\ i=1}}^{2}(\eta_1^j\Phi_3^j+\Phi_i)+\mathcal{H}(I_\varepsilon^TX) & \star & \star & \star\\
\eta_1\Phi_3^{2T}+\frac{1}{2}\Phi_3^{1T}+(\eta_2-\eta_1)W^T & \Phi_3^2-W-W^T & \star & \star\\
\sigma_uG_2\tilde{K}(e_3+e_8)^T & 0 & -\bar{\sigma}_u^{-1}I & \star\\
\bar{\sigma}_uG_2\tilde{K}e_9^T & 0 & 0 & -\bar{\sigma}_u^{-1}I
\end{bmatrix}<0
\end{aligned} \tag{3.35}$$

and are satisfied with:

$$\mathcal{X}=[\ AX\quad 0\quad \bar{\sigma}_{ux}B\tilde{K}\quad 0\quad -X\quad 0\quad 0\quad \bar{\sigma}_{ux}B\tilde{K}\quad (\bar{\sigma}_u-\bar{\sigma}_{ux})B\tilde{K}\quad (1-\bar{\sigma}_u)B\ ], \tag{3.36}$$

$$I_\varepsilon=\begin{bmatrix}\varepsilon_1I & 0 & \varepsilon_2I & 0 & \varepsilon_3I & 0 & 0 & 0 & 0 & 0\end{bmatrix}$$

$$\tilde{\Phi}_1^1 = \mathcal{H}(e_1 \tilde{P} e_5^T) + e_5(S_1 + S_2)e_5^T - e_6 \tilde{S}_1 e_6^T - e_7 \tilde{S}_2 e_7^T, \tag{3.37}$$

$$\begin{aligned}\tilde{\Phi}_2^1 =& e_1(\tilde{Q}_1 + \tilde{Q}_2 - \tilde{R}_1)e_1^T + \mathcal{H}(e_1 \tilde{R}_1 e_2^T) - e_2(\tilde{R}_2 + \tilde{R}_1 + \tilde{Q}_1)e_2^T + \mathcal{H}(e_2(\tilde{R}_2 - \tilde{W})e_3^T) \\ &+ \mathcal{H}(e_2 \tilde{W} e_4^T) + e_3(\mathcal{H}(\tilde{W}) - 2\tilde{R}_2)e_3^T + \mathcal{H}(e_3(\tilde{R}_2 - \tilde{W})e_4^T) - e_4(\tilde{R}_2 + \tilde{Q}_2)e_4^T \\ &+ e_5(\eta_1^2 \tilde{R}_1 + (\eta_2 - \eta_1)^2 \tilde{R}_2)e_5^T,\end{aligned} \tag{3.38}$$

$$\tilde{\Phi}_3^0 = \eta_2(\Pi_1^2 \tilde{\mathcal{M}} \Pi_2 - \eta_2 \Pi_3^2 \tilde{\mathcal{M}} \Pi_2 - \eta_2 \Pi_1^2 \tilde{\mathcal{M}} \Pi_4$$

$$\Phi_3^1 = -\Pi_1^1 \tilde{\mathcal{M}} \Pi_2 + (\eta_2 + \eta_1)\left(\Pi_3^1 \tilde{\mathcal{M}} \Pi_2 + \Pi_3^2 \tilde{\mathcal{M}} \Pi_2 + \Pi_1^1 \tilde{\mathcal{M}} \Pi_4 + \Pi_1^2 \tilde{\mathcal{M}} \Pi_4\right)$$

$$\tilde{\Phi}_3^2 = -\Pi_1^1 \tilde{\mathcal{M}} \Pi_4 - \Pi_3^1 \tilde{\mathcal{M}} \Pi_2$$

$$\Pi_1^1 = \begin{bmatrix} \frac{1}{\eta_1}(e_2 - e_3) \\ e_2 - e_1 \\ e_4 - e_2 \end{bmatrix}, \Pi_1^2 = \begin{bmatrix} 0 \\ e_1 - e_2 \\ e_2 - e_4 \end{bmatrix}, \Pi_2 = \begin{bmatrix} e_2 - e_3 \\ e_1 - e_2 \\ e_2 - e_4 \end{bmatrix},$$

$$\Pi_3^1 = \begin{bmatrix} \frac{1}{\eta_1} e_6 \\ \frac{1}{\eta_1}(e_1 - e_2) - e_5 + e_6 \\ \frac{1}{\eta_1}(e_2 - e_4) - e_6 + e_7 \end{bmatrix}, \Pi_3^2 = \begin{bmatrix} 0 \\ e_5 - e_6 \\ e_6 - e_7 \end{bmatrix}, \Pi_4 = \begin{bmatrix} e_6 \\ e_5 - e_6 \\ e_6 - e_7 \end{bmatrix}.$$

The controller gain is recovered as $K = \tilde{K} X^{-1}$.

Proof 3.3 *To cope with the term* $\mathcal{KG}$*, let* $X \in \mathbb{R}^{n \times n}$ *regular and* $\mathcal{K} = X^{-T} I_\varepsilon^T$*. Then, take the congruence of* (3.34) *by* $\text{diag}\{X, \ldots, X, I\} \in \mathbb{R}^{10n \times 10n}$ *and do the changes of variables* $\tilde{Z} = X^T Z X$*, with* $Z \in \{P, Q_1, Q_2, S_1, S_2, R_1, R_2, W, \Omega_1, \Omega_2, M\}$ *and* $\tilde{K} = KX$*. By applying corollary 1 extended from lemma* (3)*, then the Schur complement, we get* (3.35)*.*

3.5 Simulation results

To illustrate the effectiveness of the proposed strategy and networked controller design conditions.

3.5.1 Stability analysis results

To illustrate the proposed stability analysis methodology, two cases are proposed in the sequel. In the first case, we assume that there are no deception attacks. Then, in the second case, we consider randomly occurring attacks.

Case 1. Suppose that there are no deception attacks (i.e. $\bar{\sigma}_u = 1$ and $\bar{\sigma}_x = 1$). For given

values of $\eta_1 = 100ms$ and the state feedback gain matrix from [82]

$$K = \begin{bmatrix} -1.0162 & -5.4438 & 1.5681 & -6.1000 \\ -5.7141 & -0.5565 & -6.4960 & 1.9179 \end{bmatrix} \tag{3.39}$$

The conditions of Theorem 3.1 have been solved via the Matlab LMI Toolbox. We have obtained a maximal value of $\bar{\eta} = 17\ s$.

Assuming $h = 10\ ms$, the allowed maximal network-induced delay is $\bar{\tau} = \bar{\eta} - h = 16.90\ s$. The following simulations are performed with the initial condition $x(0) = \begin{bmatrix} -0.6 & 0.7 & -0.2 & 0.4 \end{bmatrix}^T$ and the maximal allowed network-induced delay, i.e. $\eta(t) = \bar{\eta}$ (most critical delay).The state trajectories of the closed-loop system (3.12) are plotted in Fig.3.4.

As expected, for both these simulations, the NCS is asymptotically stabilized by the

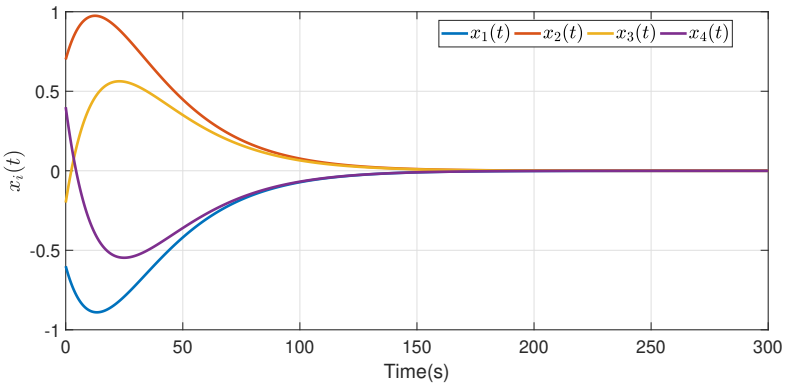

Figure 3.4: States trajectories .

designed networked control law (3.10).

Case 2.. Consider now that the NCS faced randomly occurring deception attacks satisfying Assumption 3.3 with $f(x(t_k)) = \text{col}\{\tanh(0.08x_1(t_k)), -\tanh(0.3x_2(t_k))\}$, $G_1 = \text{diag}\{0.08, 0.3\}$, $g(\tilde{u}(t_k)) = -\tanh(0.5\tilde{u}(t_k))$, $G_2 = 0.5$. To show the influence of the deception attacks on the system's performances, the conditions of Theorem 3.1 have been solved for different values of $\bar{\sigma}_u$, $\bar{\sigma}_x$. Table 1 lists the value of η_2 with these different values. For instance, when $\bar{\sigma}_u = 0.5$ and $\bar{\sigma}_x = 0.5$, about 50% of the system state are attacked and 50% of the control actions are attacked. Hence, under the above-defined deception attacks with the state trajectories of the system in Fig. 3.5, time occurrences of attacks on the sensor are plotted in Fig. 3.6, and time occurrences of attacks on the actuator are plotted in Fig. 3.7.

Table 3.1: $\bar{\eta}$ for various $\bar{\sigma}_u$ and $\bar{\sigma}_x$ (Example A)

Methods, $t \in [0, 800s]$	$\bar{\sigma}_u$	$\bar{\sigma}_x$	$\bar{\eta}\,(s)$
Theorem 1	1.0	1.0	17.0
Theorem 1	0.5	1.0	5.25
Theorem 1	0.5	0.5	2.10
Theorem 1	0.4	0.7	4.02
Theorem 1	0.7	0.9	2.9

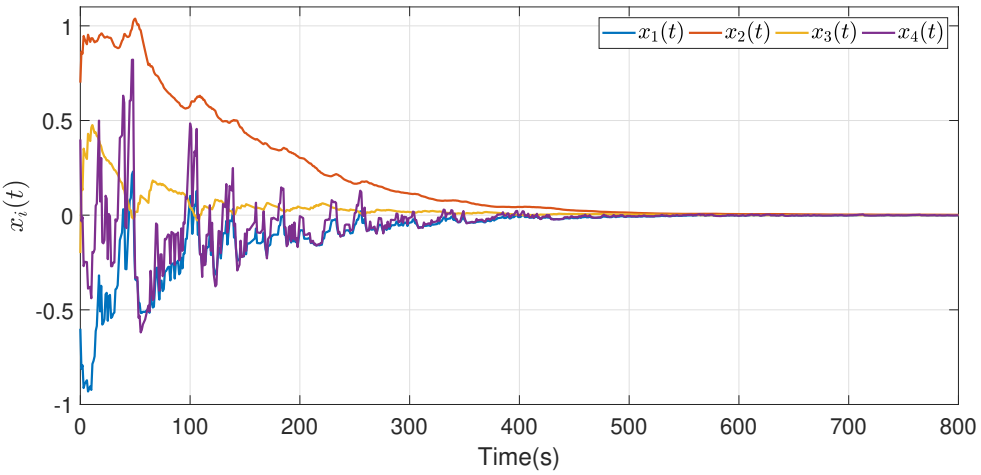

Figure 3.5: States trajectories.

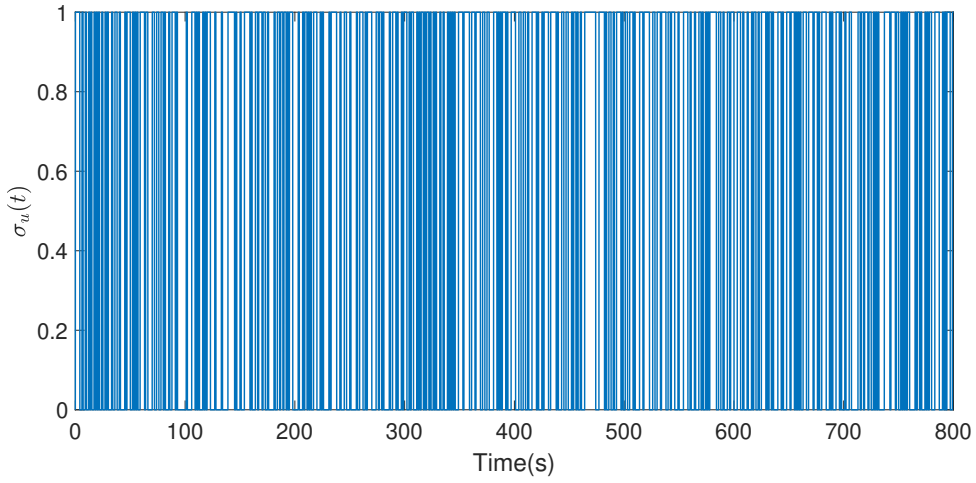

Figure 3.6: The Occurrence of the deception attacks $\sigma_u(t_k)$.

We observe that the closed-loop NCS is stable, which confirms the effectiveness of our proposal.

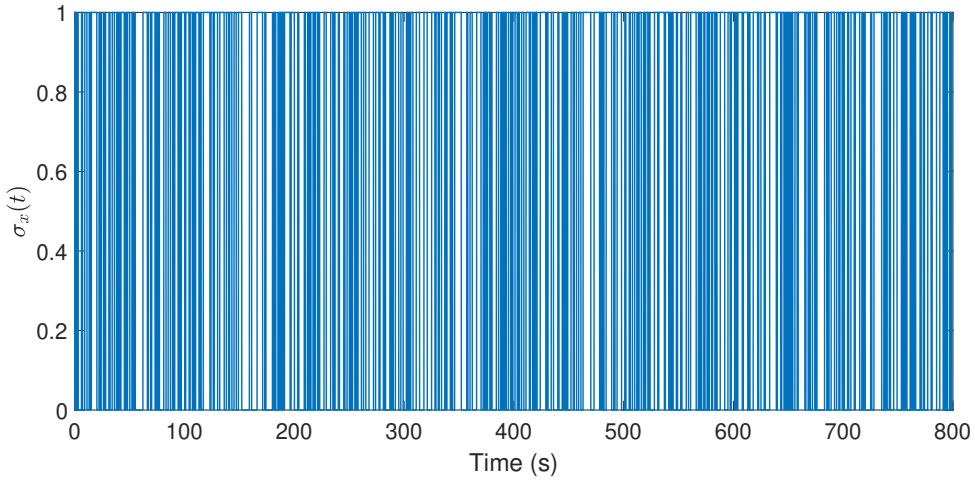

Figure 3.7: The Occurrence of the deception attacks $\sigma_x(t_k)$.

3.5.2 Control design results

We consider also two cases in the control design procedure.

Case 1 when we do not consider the effect of deception attacks on the NCS, let us assume that $\varepsilon_1 = 10$, $\varepsilon_2 = 5$, and use the same other parameters fixed in section 3.5.1, the conditions of Theorem 3.2 have been solved via the Matlab LMI Toolbox, providing a maximal value of $\eta_2 = 1.82\ s$, as well as the controller (3.10) gains:

$$K = \begin{bmatrix} -1.4437 & 1.0050 & 0.6528 & -3.8421 \\ 1.0218 & -1.2842 & -4.0280 & 0.6505 \end{bmatrix},$$

Assuming that $h = 10\,ms$, which allows a maximal network-induced delay $\bar{\tau} = \eta_2 - h = 1.81\ s$, with the initial condition $x_0 = \begin{bmatrix} 0.2 & -0.3 & 0.3 & -0.2 \end{bmatrix}$, the closed-loop NCS state trajectories are plotted in Fig. 3.8.

Case 2 when we consider the effect of deception attacks on the NCS, let us assume that $\varepsilon_1 = 0.5$, $\varepsilon_2 = 0.1$, under randomly occurring deception attacks $\bar{\sigma}_u = 0.9$ and $\bar{\sigma}_x = 0.8$ satisfying Assumption 3.3 with $f(x(t_k)) = \text{col}\{\tanh(0.8x_1(t_k)), -\tanh(0.1x_2(t_k)), \tanh(0.5x_3(t_k)), -\tanh(0.1x_4(t_k))\}$, $G_1 = \text{diag}\{0.8, 0.1, 0.5, 0.1\}$, $g(\tilde{u}(t_k)) = -sin(0.1\tilde{u}(t))$, $G_2 = 0.1$. The conditions of Theorem 3.1 have been solved via the Matlab LMI Toolbox, providing a maximal value of $\eta_2 = 1.75\ s$, as well as the controller (3.10) gains:

$$K = \begin{bmatrix} -2.3333 & 1.5211 & 1.4009 & -5.9330 \\ 1.5716 & -2.1014 & -6.2430 & 1.4228 \end{bmatrix},$$

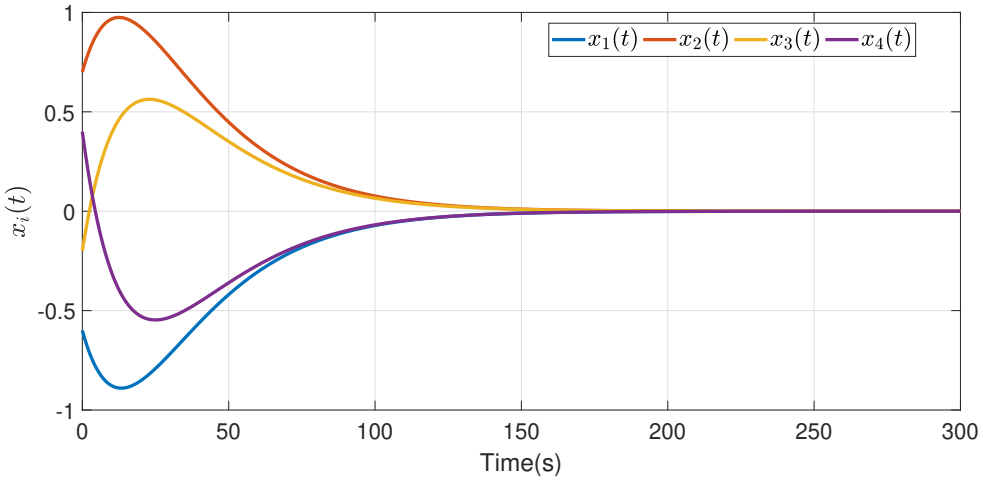

Figure 3.8: States trajectories.

Assuming that $h = 10\,ms$, which allows a maximal network-induced delay $\bar{\tau} = \eta_2 - h = 1.74\,s$, with the initial condition $x_0 = \begin{bmatrix} 0.2 & -0.3 & 0.3 & -0.2 \end{bmatrix}$, the closed-loop NCS state trajectories, as well as the occurrence of the deception attacks $\sigma_u(t_k)$ and $\sigma_x(t_k)$ are plotted in Fig. 3.9.time occurrences of attacks on the sensor are plotted in Fig. 3.10, and time occurrences of attacks on the actuator are plotted in Fig. 3.11.

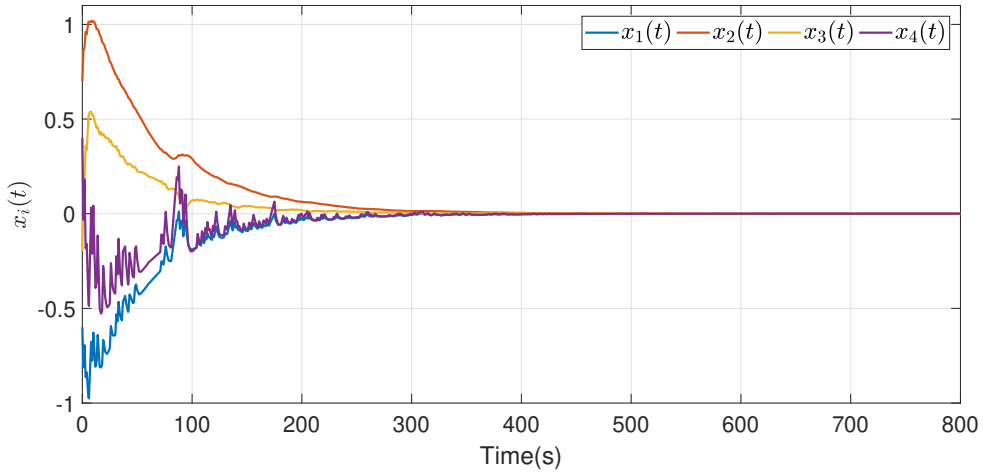

Figure 3.9: States trajectories.

We observe that the designed closed-loop NCS is properly stabilized and achieved the origin. This confirms the effectiveness of the proposed networked sampled-data controller design for NCS.

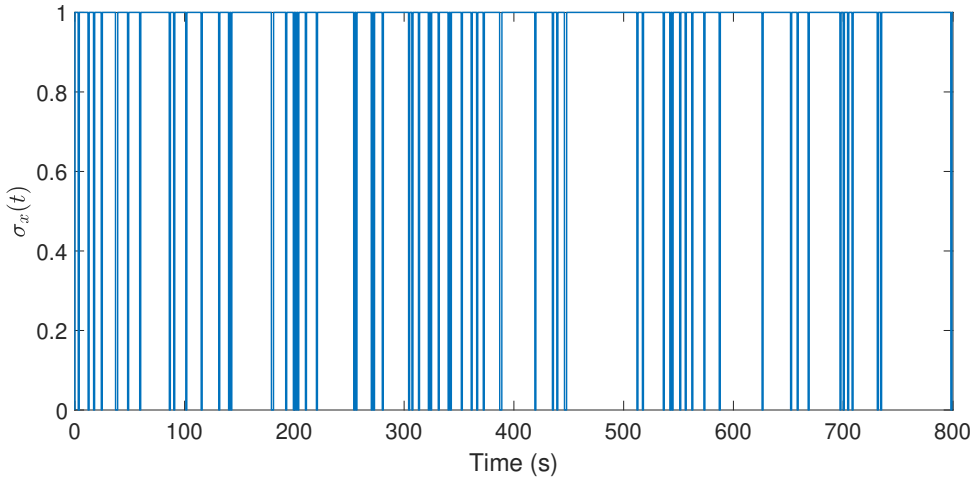

Figure 3.10: The Occurrence of the deception attacks $\sigma_u(t_k)$.

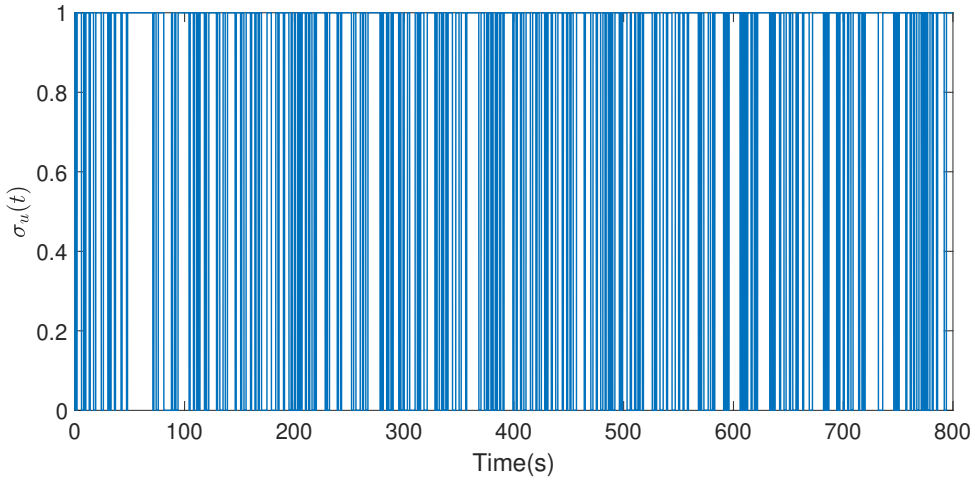

Figure 3.11: The Occurrence of the deception attacks $\sigma_x(t_k)$.

3.6 Conclusion

In this paper, a new controller gain matrix is proposed to mitigate the network loads in sampled-data controller design for NCSs subject to network-induced delay and deception attacks. The goal was to Provide LMI-based design conditions for the controller gain matrix, such that the closed-loop NCS is Globally Asymptotically Stable and resilient to deception attacks .Hence, based on the selection of a suitable asymmetric LKF, relaxed LMI-based design conditions have been proposed. a numerical example have been considered to illustrate the effectiveness of the proposal and the improvements raised, in terms of conservatism.

Chapter 4

General Conclusion

In conclusion, this thesis has provided an analysis of Networked Control Systems (NCSs) with a focus on stability and controller synthesis under cyber attack constraints.
Chapter 1 served as an introduction to NCSs, highlighting their advantages, disadvantages, applications, and comparisons with traditional control structures. The historical perspective presented in the literature review section offered valuable insights into the evolution and development of NCSs over time.

Chapter 2 delved into the architecture of NCSs, examining various components within a control loop and considering the challenges posed by communication channels on system stability. The modeling of different types of cyber attacks and their impact on system performance provided a deep understanding of the vulnerabilities associated with NCSs.

In Chapter 3, the analysis focused specifically on the quadruple-tank process as a case study. The integration of this process into the NCS framework allowed for the evaluation of network-induced delays and deception attacks. The stability analysis, accounting for both delays and attacks, provided valuable design requirements for achieving stability and robustness. The simulation results demonstrated the effectiveness of the control design approach in maintaining stability and performance in the presence of these challenges.

Overall, this thesis contributes to the body of knowledge on NCSs by addressing the crucial aspects of stability and controller synthesis under cyber attack constraints. The findings and insights obtained from this research expand our understanding of the behavior of NCSs and provide a foundation for future research in this field. The analysis and control design methodologies presented can serve as a valuable resource for engineers and researchers working on NCSs and related applications.

In light of the contributions made in this thesis, there are several potential areas for future research. These include exploring more advanced attack models, developing enhanced defense mechanisms against cyber attacks, investigating the scalability of the proposed control design approach, and exploring the applicability of the findings to different industrial processes or domains.

In conclusion, this thesis has shed light on the complex dynamics of NCSs, their vulnerabilities to cyber attacks, and the design considerations necessary for achieving stability and robustness. The knowledge gained from this research contributes to the advancement of NCS theory and provides valuable insights for practical implementations in real-world systems.

References

[1] Khalid Abidi and Jian-Xin Xu. Iterative learning control for sampled-data systems: From theory to practice. *IEEE Transactions on Industrial Electronics*, 58(7):3002–3015, 2010.

[2] Saurabh Amin, Alvaro A Cárdenas, and S Shankar Sastry. Safe and secure networked control systems under denial-of-service attacks. In *Hybrid Systems: Computation and Control: 12th International Conference, HSCC 2009, San Francisco, CA, USA, April 13-15, 2009. Proceedings 12*, pages 31–45. Springer, 2009.

[3] Karl J Astrom and Michael Lundh. Lund control program combines theory with hands-on experience. *IEEE Control Systems Magazine*, 12(3):22–30, 1992.

[4] Cheng-Zong Bai, Vijay Gupta, and Fabio Pasqualetti. On kalman filtering with compromised sensors: Attack stealthiness and performance bounds. *IEEE Transactions on Automatic Control*, 62(12):6641–6648, 2017.

[5] Lubomir Bakule. Decentralized control: An overview. *Annual reviews in control*, 32(1):87–98, 2008.

[6] Pramod Bangalore and Lina Bertling Tjernberg. An artificial neural network approach for early fault detection of gearbox bearings. *IEEE Transactions on Smart Grid*, 6(2):980–987, 2015.

[7] Lei Bao, Mikael Skoglund, and Karl Henrik Johansson. Encoder˜ decoder design for event-triggered feedback control over bandlimited channels. In *2006 American Control Conference*, pages 4183–4188. IEEE, 2006.

[8] Saverio Bolognani and Sandro Zampieri. A gossip-like distributed optimization algorithm for reactive power flow control. *IFAC Proceedings Volumes*, 44(1):5700–5705, 2011.

[9] Jie Cao, Da Ding, Jinliang Liu, Engang Tian, Songlin Hu, and Xiangpeng Xie. Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks. *Inf. Sci.*, 548:69–84, 2021.

[10] Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa. Event-triggered output feedback control resilient against jamming attacks and random packet losses. *IFAC-PapersOnLine*, 48(22):270–275, 2015.

[11] Bo Chen, Daniel WC Ho, Guoqiang Hu, and Li Yu. Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks. *IEEE transactions on cybernetics*, 48(6):1862–1876, 2017.

[12] Xiaoli Chen, Youguo Wang, and Songlin Hu. Event-based robust stabilization of uncertain networked control systems under quantization and denial-of-service attacks. *Information Sciences*, 459:369–386, 2018.

[13] Steven Cheung, Ulf Lindqvist, and Martin W Fong. Modeling multistep cyber attacks for scenario recognition. In *Proceedings DARPA Information Survivability Conference And Exposition*, volume 1, pages 284–292. IEEE, 2003.

[14] Maurício C. de Oliveira and Robert E. Skelton. Stability tests for constrained linear systems. In S.O. Reza Moheimani, editor, *Perspectives in robust control*, pages 241–257, London, 2001. Springer London.

[15] Claudio De Persis and Pietro Tesi. Input-to-state stabilizing control under denial-of-service. *IEEE Transactions on Automatic Control*, 60(11):2930–2944, 2015.

[16] Claudio De Persis and Pietro Tesi. Networked control of nonlinear systems under denial-of-service. *Systems & Control Letters*, 96:124–131, 2016.

[17] Burak Demirel, Corentin Briat, and Mikael Johansson. Deterministic and stochastic approaches to supervisory control design for networked systems with time-varying communication delays. *Nonlinear Analysis: Hybrid Systems*, 10:94–110, 2013.

[18] Derui Ding, Guoliang Wei, Sunjie Zhang, Yurong Liu, and Fuad E Alsaadi. On scheduling of deception attacks for discrete-time networked systems equipped with attack detectors. *Neurocomputing*, 219:99–106, 2017.

[19] Sebastián Dormido and Francisco Esquembre. The quadruple-tank process: An interactive tool for control education. In *2003 European Control Conference (ECC)*, pages 3267–3272. IEEE, 2003.

[20] Arezou Elahi and Alireza Alfi. Finite-time h_∞ control of uncertain networked control systems with randomly varying communication delays. *ISA transactions*, 69:65–88, 2017.

[21] N Falliere, LO Murchu, and E Chien. Bw32. stuxnet dossier,[symantec corporation. Technical report, Tech. Rep, 2011.

[22] Shuai Feng and Pietro Tesi. Networked systems under denial-of-service: co-located vs. remote control architectures. *IFAC-PapersOnLine*, 50(1):2627–2632, 2017.

[23] David P Fidler. Was stuxnet an act of war? decoding a cyberattack. *IEEE Security & Privacy*, 9(4):56–59, 2011.

[24] Hamed Shisheh Foroush and Sonia Martinez. On event-triggered control of linear systems under periodic denial-of-service jamming attacks. In *2012 IEEE 51st IEEE Conference on Decision and Control (CDC)*, pages 2551–2556. IEEE, 2012.

[25] Xiaohua Ge, Qing-Long Han, Maiying Zhong, and Xian-Ming Zhang. Distributed krein space-based attack detection over sensor networks under deception attacks. *Automatica*, 109:108557, 2019.

[26] Yuan Ge, Qigong Chen, Ming Jiang, and Yiqing Huang. Modeling of random delays in networked control systems. *Journal of Control Science and Engineering*, 2013:8–8, 2013.

[27] Lejiang Guo, Yuanmin Tang, Zhou Liu, and Wei Xiong. The theory and architecture of network control system. In *2010 International Conference on Intelligent Computing and Cognitive Informatics*, pages 183–186. IEEE, 2010.

[28] Stefan Hofmann, Mohamed Louizi, and Dieter Stoll. A novel approach to counter denial of service attacks against transport network resources. *Bell Labs Technical Journal*, 14(1):219–242, 2009.

[29] Xin Huang and Jiuxiang Dong. Reliable leader-to-follower formation control of multiagent systems under communication quantization and attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(1):89–99, 2019.

[30] Subhra Jana and Abhinandan De. A novel zone division approach for power system fault detection using ann-based pattern recognition technique. *Canadian Journal of Electrical and Computer Engineering*, 40(4):275–283, 2017.

[31] Mehdi Kadivar. Cyber-attack attributes. *Technology Innovation Management Review*, 4(11), 2014.

[32] Zahra Kazemi, Ali Akbar Safavi, Farshid Naseri, Leon Urbas, and Peyman Setoodeh. A secure hybrid dynamic-state estimation approach for power systems under false data injection attacks. *IEEE Transactions on Industrial Informatics*, 16(12):7275–7286, 2020.

[33] Oh-Min Kwon, Myeong-Jin Park, Ju H Park, Sang-Moon Lee, and Eun-Jong Cha. Analysis on robust h_∞ performance and stability for linear systems with interval time-varying state delays via some new augmented lyapunov–krasovskii functional. *Applied Mathematics and Computation*, 224:108–122, 2013.

[34] Ralph Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3):49–51, 2011.

[35] Lu Lei, Lin Jinxing, and Kanglei Ren. h_1 output tracking control for networked control systems with network-induced delays. page 1416–1421, 2018.

[36] Wenshuai Lin, Bin Zhang, Deyin Yao, Hongyi Li, and Renquan Lu. Adaptive neural sliding mode control of markov jump systems subject to malicious attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 51(12):7870–7881, 2020.

[37] Jinliang Liu, Jilei Xia, Engang Tian, and Shumin Fei. Hybrid-driven-based h_∞ filter design for neural networks subject to deception attacks. *Applied Mathematics and Computation*, 320:158–174, 2018.

[38] Leipo Liu and Xiaona Song. Static output tracking control of nonlinear systems with one-sided lipschitz condition. *Mathematical Problems in Engineering*, 2014, 2014.

[39] An-Yang Lu and Guang-Hong Yang. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service. *IEEE Transactions on Automatic Control*, 63(6):1813–1820, 2017.

[40] Lei Lu, Jinxing Lin, and Kanglei Ren. h_∞ output tracking control for networked control systems with network-induced delays. In *2018 Chinese Control And Decision Conference (CCDC)*, pages 1416–1421. IEEE, 2018.

[41] Pieter Maene, Johannes Götzfried, Ruan de Clercq, Tilo Müller, Felix Freiling, and Ingrid Verbauwhede. Hardware-based trusted computing architectures for isolation and attestation. *IEEE Transactions on Computers*, 67(3):361–374, 2018.

[42] Magdi S Mahmoud, SZ Selim, and Peng Shi. Global exponential stability criteria for neural networks with probabilistic delays. *IET control theory & applications*, 4(11):2405–2415, 2010.

[43] MS Mahmoud, SZ Selim, P Shi, and MH Baig. New results on networked control systems with non-stationary packet dropouts. *IET Control Theory & Applications*, 6(15):2442–2452, 2012.

[44] S. Massoud Amin and B.F. Wollenberg. Toward a smart grid: power delivery for the 21st century. *IEEE Power and Energy Magazine*, 3(5):34–41, 2005.

[45] Cai Meng, Tianmiao Wang, Wusheng Chou, Sheng Luan, Yuru Zhang, and Zengmin Tian. Remote surgery case: robot-assisted teleneurosurgery. In *IEEE International Conference on Robotics and Automation, 2004. Proceedings. ICRA'04. 2004*, volume 1, pages 819–823. IEEE, 2004.

[46] Yilin Mo, Emanuele Garone, Alessandro Casavola, and Bruno Sinopoli. False data injection attacks against state estimation in wireless sensor networks. In *49th IEEE Conference on Decision and Control (CDC)*, pages 5967–5972. IEEE, 2010.

[47] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2011.

[48] Yilin Mo and Bruno Sinopoli. Secure control against replay attacks. In *2009 47th annual Allerton conference on communication, control, and computing (Allerton)*, pages 911–918. IEEE, 2009.

[49] ROUAMEL Mohamed. Commande robuste des systèmes en réseau., 2020.

[50] Abbas Nemati, Mansour Peimani, Saleh Mobayen, and Sayyedjavad Sayyedfattahi. Adaptive non-singular finite time control of nonlinear disturbed cyber-physical systems with actuator cyber-attacks and time-varying delays. *Information Sciences*, 612:1111–1126, 2022.

[51] Mete Ozay, Inaki Esnaola, Fatos Tunay Yarman Vural, Sanjeev R Kulkarni, and H Vincent Poor. Machine learning methods for attack detection in the smart grid. *IEEE transactions on neural networks and learning systems*, 27(8):1773–1786, 2015.

[52] Yingnan Pan and Guang-Hong Yang. Event-based output tracking control for fuzzy networked control systems with network-induced delays. *Applied Mathematics and Computation*, 346:513–530, 2019.

[53] Zhong-Hua Pang, Lan-Zhi Fan, Jian Sun, Kun Liu, and Guo-Ping Liu. Detection of stealthy false data injection attacks against networked control systems via active data modification. *Information Sciences*, 546:192–205, 2021.

[54] Zhong-Hua Pang, Guo-Ping Liu, Donghua Zhou, Fangyuan Hou, and Dehui Sun. Two-channel false data injection attacks against output tracking control of networked systems. *IEEE Transactions on Industrial Electronics*, 63(5):3242–3251, 2016.

[55] Zhong-Hua Pang, Guo-Ping Liu, Donghua Zhou, and Dehui Sun. Data-based predictive control for networked nonlinear systems with network-induced delay and packet dropout. *IEEE Transactions on Industrial Electronics*, 63(2):1249–1257, 2015.

[56] Antonis Papachristodoulou and Stephen Prajna. On the construction of lyapunov functions using the sum of squares decomposition. In *Proceedings of the 41st IEEE Conference on Decision and Control, 2002.*, volume 3, pages 3482–3487. IEEE, 2002.

[57] PooGyeon Park, Jeong Wan Ko, and Changki Jeong. Reciprocally convex approach to stability of systems with time-varying delays. *Automatica*, 47(1):235–238, 2011.

[58] Santi Pattanavichai. Comparison for network security scanner tools between gfi languard and microsoft baseline security analyzer (mbsa). In *2017 15th International Conference on ICT and Knowledge Engineering (ICT&KE)*, pages 1–7. IEEE, 2017.

[59] Chen Peng and Qing-Long Han. On designing a novel self-triggered sampling scheme for networked control systems with data losses and communication delays. *IEEE Transactions on Industrial Electronics*, 63(2):1239–1248, 2015.

[60] Mohamed Rouamel, Sofiane Gherbi, and Faycal Bourahala. Robust stability and stabilization of networked control systems with stochastic time-varying network-induced delays. *Transactions of the Institute of Measurement and Control*, 42(10):1782–1796, 2020.

[61] Mohamed Rouamel, Sofiane Gherbi, and Fayçal Bourahala. Robust stability and stabilization of networked control systems with stochastic time-varying network-induced delays. page 0142331219895931, 2020.

[62] Helem Sabina Sanchez, Damiano Rotondo, Teresa Escobet, Vicenc Puig, Jordi Saludes, and Joseba Quevedo. Detection of replay attacks in cyber-physical systems using a frequency-based signature. *Journal of the Franklin Institute*, 356(5):2798–2824, 2019.

[63] Henrik Sandberg, Vijay Gupta, and Karl H Johansson. Secure networked control systems. *Annual Review of Control, Robotics, and Autonomous Systems*, 5:445–464, 2022.

[64] Lei Su and Dan Ye. A cooperative detection and compensation mechanism against denial-of-service attack for cyber-physical systems. *Information Sciences*, 444:122–134, 2018.

[65] Xiang Sun, Zhou Gu, Fan Yang, and Shen Yan. Memory-event-trigger-based secure control of cloud-aided active suspension systems against deception attacks. *Inf. Sci.*, 543:1–17, 2021.

[66] Yuan-Cheng Sun and Guang-Hong Yang. Event-triggered resilient control for cyber-physical systems under asynchronous dos attacks. *Information Sciences*, 465:340–352, 2018.

[67] Bixiang Tang, Luis D Alvergue, and Guoxiang Gu. Secure networked control systems against replay attacks without injecting authentication noise. In *2015 American Control Conference (ACC)*, pages 6028–6033. IEEE, 2015.

[68] Domagoj Tolić. Stabilizing transmission intervals and delays in nonlinear networked control systems through hybrid-system-with-memory modeling and lyapunov–krasovskii arguments. *Nonlinear Analysis: Hybrid Systems*, 36:100834, 2020.

[69] V Ugrinovskii and Cedric Langbort. Control over adversarial packet-dropping communication networks revisited. In *2014 American Control Conference*, pages 3305–3309. IEEE, 2014.

[70] Kunyu Wang, Engang Tian, Jinliang Liu, Linnan Wei, and Dong Yue. Resilient control of networked control systems under deception attacks: a memory-event-triggered communication scheme. *International Journal of Robust and Nonlinear Control*, 30(4):1534–1548, 2020.

[71] Yan-Wu Wang, Hua O Wang, Jiang-Wen Xiao, and Zhi-Hong Guan. Synchronization of complex dynamical networks under recoverable attacks. *Automatica*, 46(1):197–203, 2010.

[72] Yu-Long Wang and Qing-Long Han. Modelling and controller design for discrete-time networked control systems with limited channels and data drift. *Information Sciences*, 269:332–348, 2014.

[73] Yu-Long Wang and Qing-Long Han. Network-based modelling and dynamic output feedback control for unmanned marine vehicles in network environments. *Automatica*, 91:43–53, 2018.

[74] Guangyu Wu, Gang Wang, Jian Sun, and Jie Chen. Optimal partial feedback attacks in cyber-physical power systems. *IEEE Transactions on Automatic Control*, 65(9):3919–3926, 2020.

[75] Jiancun Wu, Chen Peng, Jin Zhang, and Bao-Lin Zhang. Event-triggered finite-time h_∞ filtering for networked systems under deception attacks. *Journal of the Franklin Institute*, 357(6):3792–3808, 2020.

[76] Bu Xuhui, Hou Zhongsheng, Jin Shangtai, and Chi Ronghu. An iterative learning control design approach for networked control systems with data dropouts. *International Journal of Robust and Nonlinear Control*, 26(1):91–109, 2016.

[77] Meng Yang and Junyong Zhai. Observer-based dynamic event-triggered secure control for nonlinear networked control systems with false data injection attacks. *Information Sciences*, page 119262, 2023.

[78] Dawei Zhang, Qing-Long Han, and Xinchun Jia. Network-based output tracking control for a class of ts fuzzy systems that can not be stabilized by nondelayed output feedback controllers. *IEEE Transactions on Cybernetics*, 45(8):1511–1524, 2014.

[79] Dawei Zhang, Zhiyong Zhou, and Xinchun Jia. Network-based pi control for output tracking of continuous-time systems with time-varying sampling and network-induced delays. *Journal of the Franklin Institute*, 355(12):4794–4808, 2018.

[80] Jun ZHANG, Da-yong LUO, and Miao-ping SUN. A new stability condition for networked control system with time-varying delay based on time delay uneven-partitioning approach. *ACTA ELECTONICA SINICA*, 44(1):54, 2016.

[81] Long Zhang and Ge Guo. Observer-based adaptive event-triggered sliding mode control of saturated nonlinear networked systems with cyber-attacks. *Inf. Sci.*, 543:180–201, 2021.

[82] Ruimei Zhang, Deqiang Zeng, Xinzhi Liu, Shouming Zhong, and Qishui Zhong. Improved results on state feedback stabilization for a networked control system with additive time-varying delay components' controller. *ISA transactions*, 75:1–14, 2018.

[83] Ruimei Zhang, Deqiang Zeng, Xinzhi Liu, Shouming Zhong, and Qishui Zhong. Improved results on state feedback stabilization for a networked control system

with additive time-varying delay components' controller. *ISA transactions*, 75:1–14, 2018.

[84] Tian-Yu Zhang and Dan Ye. False data injection attacks with complete stealthiness in cyber–physical systems: A self-generated approach. *Automatica*, 120:109117, 2020.

[85] Xian-Ming Zhang, Qing-Long Han, and Xiaohua Ge. The construction of augmented lyapunov-krasovskii functionals and the estimation of their derivatives in stability analysis of time-delay systems: A survey. *International Journal of Systems Science*, 53(12):2480–2495, 2022.

[86] Zhenxing Zhang, Hongjing Liang, Chengwei Wu, and Choon Ki Ahn. Adaptive event-triggered output feedback fuzzy control for nonlinear networked systems with packet dropouts and actuator failure. *IEEE Transactions on fuzzy systems*, 27(9):1793–1806, 2019.

Abbreviations

CPSs Cyber-Physical Systems

DCS Distributed Control System

DoS Denial of Service

FDI False Data Injection

GAS Globally Asymptotically Stable

ILC iterative learning control

LKF Lyapunov-Krasovskii Functionals

LMI Linear Matrix Inequality

MAUB Maximum allowable upper bound

NCSs Networked Control Systems

NN Neural Networks

PWM Pulse-width-modulated

ZOH Zero-Order Hold

Chapter 5

General Conclusion

In conclusion, this thesis has provided an analysis of Networked Control Systems (NCSs) with a focus on stability and controller synthesis under cyber attack constraints.
Chapter 1 served as an introduction to NCSs, highlighting their advantages, disadvantages, applications, and comparisons with traditional control structures. The historical perspective presented in the literature review section offered valuable insights into the evolution and development of NCSs over time.

Chapter 2 delved into the architecture of NCSs, examining various components within a control loop and considering the challenges posed by communication channels on system stability. The modeling of different types of cyber attacks and their impact on system performance provided a deep understanding of the vulnerabilities associated with NCSs.

In Chapter 3, the analysis focused specifically on the quadruple-tank process as a case study. The integration of this process into the NCS framework allowed for the evaluation of network-induced delays and deception attacks. The stability analysis, accounting for both delays and attacks, provided valuable design requirements for achieving stability and robustness. The simulation results demonstrated the effectiveness of the control design approach in maintaining stability and performance in the presence of these challenges.

Overall, this thesis contributes to the body of knowledge on NCSs by addressing the crucial aspects of stability and controller synthesis under cyber attack constraints. The findings and insights obtained from this research expand our understanding of the behavior of NCSs and provide a foundation for future research in this field. The analysis and control design methodologies presented can serve as a valuable resource for engineers and researchers working on NCSs and related applications.

In light of the contributions made in this thesis, there are several potential areas for future research. These include exploring more advanced attack models, developing enhanced defense mechanisms against cyber attacks, investigating the scalability of the proposed control design approach, and exploring the applicability of the findings to different industrial processes or domains.

In conclusion, this thesis has shed light on the complex dynamics of NCSs, their vulnerabilities to cyber attacks, and the design considerations necessary for achieving stability and robustness. The knowledge gained from this research contributes to the advancement of NCS theory and provides valuable insights for practical implementations in real-world systems.