STATE-FEEDBACK CONTROL AND FILTER DESIGN FOR CYBER-PHYSICAL UNCERTAIN SYSTEMS UNDER DOS ATTACKS AND UNRELIABLE MARKOVIAN NETWORK

PEDRO MOREIRA DE OLIVEIRA

Federal University of São João del-Rei
Department of Electrical Engineering
Electrical Engineering Graduate Program CEFET-MG and UFSJ

supervisor: Prof. Dr. Márcio J. Lacerda
co-supervisor: Prof. Dr. Jonathan M. Palma

São João del-Rei
March 2023

STATE-FEEDBACK CONTROL AND FILTER DESIGN FOR CYBER-PHYSICAL UNCERTAIN SYSTEMS UNDER DOS ATTACKS AND UNRELIABLE MARKOVIAN NETWORK

PEDRO MOREIRA DE OLIVEIRA

Dissertation presented to the Graduate Program in Electrical Engineering (PPGEL CEFET-MG / UFSJ) at Federal University of São João del-Rei (UFSJ) in partial fulfillment of the requirements to obtain the degree of Master in Electrical Engineering.

SUPERVISOR: Prof. Dr. Márcio J. Lacerda
CO-SUPERVISOR: Prof. Dr. Jonathan M. Palma

São João del-Rei
March 2023

Federal University of São João del-Rei
Department of Electrical Engineering
Electrical Engineering Graduate Program CEFET-MG and UFSJ

Dissertation titled "*State-feedback control and Filter Design for Cyber-Physical uncertain Systems under DoS attacks and unreliable Markovian network*", by Pedro Moreira de Oliveira, presented to the Electrical Engineering Graduate Program CEFET-MG and UFSJ, approved by the following Professors:

Prof. Dr. Márcio Júnior Lacerda
Federal University of São João Del-Rei - PPGEL CEFET-MG / UFSJ

Prof. Dr. Jonathan Matias Palma Olate
Universidad de Talca, Curicó, Chile

Prof. Dr. Valter Júnior de Souza Leite
CEFET-MG / Campus Divinópolis - PPGEL CEFET-MG / UFSJ

Prof. Dr. André Marcorin de Oliveira
Federal University of São Paulo - UNIFESP

São João del-Rei
March, 2023

ACKNOWLEDGEMENTS

I want to thank my advisor Prof. Márcio Júnior Lacerda, and my co-advisor Prof. Jonathan Matias Palma Olate, for their support in the development of this research, for their dedication, and for all the opportunities they provided.

I would like to thank my father, my mother, and all my family for always standing by me and helping and supporting me at all times.

I would like to thank my partner, Carol, for supporting me and putting up with me during the whole period of my research. I am also grateful for my friends and colleagues that helped me in whichever way to get where I am now.

I would like to thank FAPEMIG for the financial support granted throughout my Master's degree, and UFSJ and CEFET for the Post-graduate program. I also want to thank the Fondecyt Iniciación ANID project of Prof. Jonathan Palma for the academic and personal opportunities provided.

I am also thankful for every piece of art, music, writing, game, and every result of human creativity that inspires us and drives us all forward. And I am grateful for every person from the past that contributed to advancing humankind's knowledge, as well as for everyone from the present and the future that continues and will continue this quest alive. We build upon the works of predecessors.

"A man may die yet still endure if his work enters the greater work, for time is carried upon a current of forgotten deeds, and events of great moment are but the culmination of a single carefully placed thought. As all men must thank progenitors obscured by the past, so we must endure the present so that those who follow may continue the endeavour"

Garba Mojaro, Tech-priest of the Adeptus Mechanicus

ABSTRACT

This work addresses both the state-feedback control problem and filter design for discrete-time cyber-physical systems (CPS) with polytopic uncertainties. The CPS is subject to the presence of Denial-of-service (DoS) attacks and an unreliable network. The attacker is deemed energetically bounded, which limits the maximum duration of the attacks. Two scenarios are explored throughout this work: i) Only DoS attacks are considered, with the closed-loop system dynamics modeled after a switched system; ii) A non-homogeneous Markov chain is proposed to model the attacks (with its deterministic energy limitations) and stochastic transmission faults due to an unreliable network's limitations (unrelated to the attacks). The utilized Markovian network model is capable of tackling the presence of uncertain and unknown probabilities, which are modeled by using time-varying parameters that aim to include a wider range of scenarios. A packet-based control strategy is employed in the control applications, and a mode-dependent robust filter is designed for the filtering problem. All the design conditions are obtained through parameter-dependent Linear Matrix Inequalities (LMIs) conditions derived from the Lyapunov Theory. The $\mathscr{H}_2$ and the $\mathscr{H}_\infty$ performance criteria are employed to evaluate the effects of the DoS attacks in the studied problems. Adaptations to both control and filtering strategies are discussed based on the hold and zero-input strategies, which are featured in numerical simulations presented to illustrate the performance of the designed controllers and filters.

Keywords: Cyber-Physical Systems, DoS Attacks, Communication Constraints, Control Design, Filter Design, Polytopic Uncertainty, Lyapunov Theory.

RESUMO

Esse trabalho aborda o problema de controle por realimentação de estados e o projeto de filtros para sistemas ciber-físicos (CPS, do inglês *Cyber-Physical Systems*) de tempo discreto com incertezas politópicas. Os CPS estão sujeitos à presença de ataques de Negação de Serviço (DoS, do inglês *Denial-of-Service*) e a uma rede não-confiável. O atacante é considerado energeticamente limitado, o que limita a duração máxima dos ataques. Dois cenários são explorados ao longo deste trabalho: i) Apenas ataques DoS são considerados, com a dinâmica do sistema em malha fechada modelada a partir de um sistema chaveado; ii) Uma cadeia de Markov não homogênea é proposta para modelar os ataques (com suas limitações energéticas determinísticas) e falhas estocásticas de transmissão devido a limitações de uma rede não confiável (as quais não são relacionadas aos ataques). O modelo de rede Markoviana utilizado é capaz de lidar com a presença de probabilidades incertas e desconhecidas, as quais são modeladas a partir de parâmetros variantes no tempo que buscam incluir uma gama maior de cenários. Uma estratégia de controle baseado em pacotes é empregada nas aplicações de controle e um filtro robusto dependente do modo é projetado para o problema de filtragem. Todas as condições de projeto são obtidas através de Desigualdades Matriciais Lineares (LMIs, do inglês *Linear Matrix Inequalities*) dependentes de parâmetros e derivadas da Teoria de Lyapunov. Os critérios de desempenho $\mathscr{H}_2$ e $\mathscr{H}_\infty$ são empregados para avaliar os efeitos dos ataques DoS nos problemas estudados. Adaptações para as estratégias de controle e filtragem são discutidas baseadas nas estratégias *hold* e *zero-input*, as quais são apresentadas em simulaçãoes numéricas que ilustram o desempenho dos controladores e dos filtros projetados.

Palavras Chave: Sistemas Ciber-Físicos, Ataques DoS, Restrições de Comunicação, Projeto de Controladores, Projeto de Filtros, Incertezas Politópicas, Teoria de Lyapunov

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

APS Angular Positioning System

CPS Cyber-Physical System

DoS attack Denial of Service attack

ESMS-CI Exponential stability in the mean square sense with conditioning I

IoT Internet of Things

LMI Linear Matrix Inequalities
LPV system Linear Parameter-Varying system

MJLS Markov jump linear system

NCS Networked Control System
NSF National Science Foundation

SMS Second Moment Stability

NOTATION

$\mathbb{R}^n$	Denotes the n-dimensional Euclidean space;
$P > (<)\ 0$	Indicates that P is a positive (negative) definite matrix;
I	Indicates an identity matrix of appropriate dimension;
0	Indicates a null matrix of appropriate dimension;
Ω_Z	Is the multi-simplex of dimension Z;
$\mathbb{R}^{m\times n}$	Set of all $m \times n$ real matrices;
$\star$	Stands for symmetric blocks in matrices;
A^T	Denotes the transpose of matrix A;
Λ_Z	Is the unit simplex of dimension Z;
$\mathscr{E}\{\cdot\}$	Is the mathematical expectation of $\{\cdot\}$;
$He(A)$	Denotes $A + A^T$.

1 INTRODUCTION

With the advancements in computational processing capabilities, and the advent of the 4.0 Industry, there has been an increasing interest in the topic of Cyber-Physical Systems (CPSs). CPSs consist of a combination of physical and computer or cyber components, where the latter are involved in processing, communicating, and controlling information [1]. These cyber components can take place through embedded computers that, coupled with physical sensors and actuators, monitor and control physical processes, forming a loop where the cyber influences the physical and vice-versa [2]. The cyber element may also consist of a whole collection of computing devices that communicate among themselves while interfacing with the physical components of the wider CPS [3]. This class of systems offers a vast field of study, as they feature both the versatility to be employed in a myriad of applications [4], as well as introduce a new array of challenges, given that, as put by [5], it represents the intersection, not the union, of the cyber and physical elements.

Discussions over "cybernetics" go back to the 40's [6], with the term "Cyber-Physical System" having been coined by the National Science Foundation (NSF) in 2006, which emphasized them as a promising field of research [4]. Applications for CPSs involve various fields, such as industry [7, 8], healthcare [9], power-grids [10], Internet of Things (IoT) [11], automotive systems [12] among many others [13]. Networked systems and Networked Control Systems (NCSs) also come as a subcategory of Cyber-Physical systems [1], where a computational network intermediates, for instance, the data transmission between a physical plant and its geographically distant central controller.

NCSs present their own assortment of challenges [14]. When considering the context of networked CPSs, one may mention time delays in the transmission [15], packet dropouts due to network limitations [14, 16, 17] and, specifically because of the presence of the computational components, the possibility of cyberattacks by malicious agents, which aim to disrupt and degrade the system performance [18]. In recent times, cyberattacks have been the cause of numerous incidents, with some of them being summarized in [19] and in [20].

The cyberattacks may be divided into three main categories [18]: i) Deception (or false data injection) attacks, where the transmitted information is compromised and the agent inserts false measurements through the system network; ii) Replay attacks, where the attacker, in possession of valid past signals from the CPS, transmits these measurements again to jeopardize the system performance with the outdated information; iii) Denial of Service attacks (DoS attacks), where the attacker overloads the network by seizing its communication or computational resources, rendering transmission of information impossible and generating packet dropouts, with some sources also indicating the introduction of time-delayed dynamics in the system [21, 22]. Among these attacks, the DoS attacks are one of the easiest to implement, as the attacker does not

necessarily require any previous knowledge about how the system operates [23]. This justifies the importance of approaching this sort of attack.

The topic of attack detection has been addressed in the literature [24–26], together with the development of strategies aiming to maximize the attack impact on the system [27, 28]. On what regards secure control and filtering techniques, which are the focus of this work, many surveys have shown different perspectives and approaches to the theme [23, 29–31].

In relation to the packet dropouts due to network failure or limitations, the main approach to model them, given their stochastic nature, is by utilizing Bernoulli processes [16] or Markov chains [17, 32]. Furthermore, some works in the literature explore the use of non-homogeneous Markov chains [33, 34], as they allow to include time-varying transition probabilities that translate possible alterations concerning the network, as well as dismissing the need for precisely knowing the network behavior. Some relevant works on control and filtering under stochastic packet losses include [17, 32–35].

On the topic of DoS attacks, the use of the queuing model can be cited [21]. Furthermore, departing from the deterministic assumption that the attacker has energetic constraints (which limits the maximum duration of the attacks) it is possible to model the system under attack as a switched system [36, 37]. This same approach can also be applied in traditional NCS problems [38]. Among the possible strategies to tackle this class of problem, the packet-based control strategies [36] come as a promising one, besides allowing the incorporation of strategies like the Hold-input and Zero-input [16]. The work [39] summarizes this approach for Linear Parameter-Varying systems (LPV systems) in the state-feedback [40], output-feedback [41] and $\mathscr{H}_\infty$ control [37] problems. To the author's knowledge, however, the topic of $\mathscr{H}_2$ cost in this context for uncertain systems is yet to be explored. Moreover, some works show the validity of accounting for stochastic models to depict the DoS attacks. In [42, 43] a Bernoulli process is employed whereas in [44] a Markov chain is utilized. In [45] the attacker modulates his attack strategy based on a hidden Markov process. Some works also consider that the attacker operates in a periodic manner, switching between moments of inactivity and attack [46], or as in [47], where a cyclic downtime switching strategy is considered.

Many of the works, however, do not account for the simultaneous presence of parametric uncertainties in the system model, which may be unrelated to the network operation. This introduces more complexity in the CPSs control and filtering problem, as design techniques must account for both packet dropouts (stochastic or attack-related) as well as the parametric uncertainties themselves.

Lyapunov Theory is widely used in control theory. With it, it is possible to obtain stability analysis conditions, control, and filter design techniques, among various other performance criteria conditions with the use of Linear Matrix Inequalities (LMIs). They, in turn, can be solved by convex optimization through computational packages and solvers. When considering uncertainties or LPV systems, the first conditions derived from this theory, which were based on quadratic stability, could be perceived as conservative, as a single constant Lyapunov matrix would have to account for the whole domain [48]. Nevertheless, there exists the possibility of augmenting or changing the structure of the Lyapunov function: Parameter-dependent Lyapunov functions for uncertain systems [49]; Switched parameter-dependent Lyapunov functions [50]; matrices with

polynomial structures [51]; the use of non-monotonic terms in stability analysis of uncertain systems [52] and in control design and stability analysis of LPV systems [48], to name a few, are possible techniques to decrease conservativeness in LMI conditions. Lyapunov Theory can also be applied to acquire stability and other costs conditions to Markovian systems, as presented in [53–55], which, amalgamated with the aforementioned structure modifications, may provide less conservative conditions when tackling stochastic systems.

Given this discussion, it can be seen that there is still room to explore the impact of DoS attacks using the $\mathscr{H}_2$ cost on uncertain CPSs modeled as switched systems. Additionally, there are few works that address both the presence of packet dropouts caused by DoS attacks and generated by an unreliable network's limitations when considering an CPSs with uncertainties. [46, 47] consider both but to a precisely known system and considering a periodic attack strategy. In [56] the precisely known case and packet dropouts due to network limitations are approached as well as DoS attacks, with the attacker almost always bounded by a ratio relative to the total number of exchanged packets.

There is also a potential in creating a network model combining the deterministic assumption of energetic constraints with a stochastic model of unreliable network's packet dropout through a finite state discrete-time Markov chain, which aims to be less conservative than a traditional Gilbert-Elliot model [57, 58]. Since it is difficult to obtain precisely known probabilities that describe both the attacker behavior and the network limitations, a non-homogeneous Markov chain is proposed, in an approach similar to [33, 34], aiming to take into account a wider array of more or less conservative scenarios when designing the controllers and filters. The use of parameter-dependent slack variables and Lyapunov functions could also provide more complex, but less conservative conditions. Existing methods such as [59–61], for the filtering problem, whilst applied to uncertain systems without any network (noting that the latter is applied to a Markov jump linear system (MJLS) with uncertain transition rates), show possible paths to be taken in this sense.

1.1 OBJECTIVE

The main objective of this dissertation is to investigate secure control techniques for discrete-time CPSs with polytopic uncertainties under DoS attacks, and to model the inclusion of stochastic packet losses due to network limitations, proposing secure control and filtering techniques in this context. The switched system approach of [36] is utilized when only considering DoS attacks. A new Markovian network model is proposed that accounts for both the attacks and the stochastic packet losses. Parameter-dependent Lyapunov functions are employed to obtain LMI conditions for the addressed problems.

1.2 CONTRIBUTIONS

This work provides contributions to control and filter design of CPSs under DoS attacks and stochastic packet losses, and in network modeling. The main contributions can be summarized as follows:

- New studies concerning the presence of exogenous disturbances in a discrete-time CPS with polytopic uncertainties and under DoS attacks from an energetically-bounded attacker. The state-feedback control framework is considered and the system is modeled as a switched system based on the deterministic assumption of the attacker's energy constraints. The $\mathscr{H}_2$ criterion is employed to evaluate the impact of the exogenous disturbances.
- A new network model based on Markov chains that consider: i) successful transmission, ii) transmission failure due to network problems, and iii) the existence of DoS attacks. This Markovian model is based on a non-homogeneous Markov chain, that includes uncertain and unknown probabilities dependent on time-varying parameters and aims to incorporate the attacker energy constraints through a finite state chain.
- New state-feedback control and filter design methods that aim, respectively, to stabilize and minimize the $\mathscr{H}_\infty$ cost of a discrete-time CPS with polytopic uncertainties, which is connected through a network defined by the aforementioned proposed model.

1.3 OUTLINE

The remainder of this manuscript is structured as follows:

- Chapter 2: Introduces the polytopic uncertainties existing in the addressed CPSs. A packet-based control approach is presented with different implementation strategies, as well as the utilized assumptions. Preliminary results regarding the stability of switched systems and stochastic stability are also presented. The first contribution of this dissertation is also provided, consisting of the proposal of a Markovian network model that accounts for DoS attacks and stochastic packet losses, and is based on a non-homogeneous Markov chain with uncertain and unknown transition probabilities.
- Chapter 3: Exhibits the conditions developed to design state-feedback controllers for discrete-time CPSs with polytopic uncertainties, and accounting only the presence of DoS attacks. The closed-loop system under attack is written as a switched system, and the influence of exogenous disturbances is evaluated through the $\mathscr{H}_2$ cost. Three control strategies are discussed and compared through numerical experiments.
- Chapter 4: Details the state-feedback control technique for discrete-time CPSs with polytopic uncertainties, which accounts for DoS attacks and stochastic packet losses due to network limitations. The closed-loop system is modeled as a MJLS. The proposed Markovian network model is utilized, which is compared with a traditional Gilbert-Elliot model. Three different control strategies are compared.

- Chapter 5: Presents the proposed conditions to design full-order $\mathscr{H}_\infty$ filters for a discrete-time CPSs with polytopic uncertainties, considering DoS attacks and stochastic packet losses because of network limitations. The closed-loop system is modeled as a MJLS. The proposed Markovian network model is taken into account. Mode-dependent and mode-independent approaches to filter design are compared, where both utilize a memory to store the last transmitted output measurement in order to design the filter output. The proposed network model is compared with a Gilbert-Elliot model.
- Chapter 6: Summarizes the conclusions and future directions for this work, as well as the publications developed during the Master's studies.

2

BACKGROUND, PRELIMINARIES AND INITIAL CONTRIBUTIONS

In this chapter, the assumptions and concepts employed in the conditions proposed in this work are provided, as well as the first contributions, which consist of the proposal of the new network model. The polytopic modeling of the discrete-time uncertain Cyber-Physical Systems (CPSs) and the attack characterization are depicted. The utilized packet-based control strategy is detailed with some possible modifications. The new network model is proposed, which is based on a time-varying non-homogeneous Markov process that features uncertain and unknown probabilities, and accounts for both packet losses due to network limitations and Denial of Service attacks (DoS attacks). The inclusion of said probabilities in the resulting transition probability matrix is demonstrated in detail. Moreover, conditions for stochastic stability and stability of switched systems are provided, in addition to Finsler's Lemma, which assists in deriving a number of Linear Matrix Inequalities (LMI) conditions present in this work.

2.1 POLYTOPIC UNCERTAINTIES

There are different types and ways to model parametric uncertainties of plant models. Among them one may cite norm-bounded [62–64], affine [65, 66], interval [67–69] and polytopic uncertainties [62, 70, 71]. In this work, time-invariant polytopic uncertainties are taken into account to model the CPSs. Consider the following general representation for discrete-time uncertain CPSs:

$$\begin{aligned} x(k+1) &= A(\alpha)x(k) + B_u(\alpha)u(k) + B_w(\alpha)w(k), \\ y(k) &= C(\alpha)x(k) + D_u(\alpha)u(k) + D_w(\alpha)w(k), \end{aligned} \tag{2.1}$$

where $x(k) \in \mathbb{R}^{n_x}$ is the state vector, $u(k) \in \mathbb{R}^{n_u}$ the control input, $w(k) \in \mathbb{R}^{n_w}$ is the exogenous disturbance input vector, and k is the time instant. The exogenous disturbance input $w(k)$ are considered to have finite-energy, i.e., $w \in \ell_2^{n_w}[0, \infty)$. The matrices $A(\alpha) \in \mathbb{R}^{n_x \times n_x}$, $B_u(\alpha) \in \mathbb{R}^{n_x \times n_u}$, $B_w(\alpha) \in \mathbb{R}^{n_x \times n_w}$, $C(\alpha) \in \mathbb{R}^{n_y \times n_x}$, $D_u(\alpha) \in \mathbb{R}^{n_y \times n_u}$, and $D_w(\alpha) \in \mathbb{R}^{n_y \times n_w}$ belong to a polytopic domain dependent on the time-invariant parameter $\alpha \in \mathbb{R}^V$. A generic matrix $M(\alpha)$ is given by:

$$M(\alpha) = \sum_{v=1}^{V} \alpha_v M_v \quad \alpha \in \Lambda_V, \tag{2.2}$$

where V is the number of vertices of the polytope, M_v, $v = 1, \ldots, V$, are the known vertices, and Λ_V is the unit simplex, defined as:

$$\Lambda_V = \left\{ \alpha \in \mathbb{R}^V : \sum_{v=1}^{V} \alpha_v = 1,\ \alpha_v \geq 0, \quad v = 1, \ldots, V \right\}. \tag{2.3}$$

Modeling uncertainties in the polytopic domain has been applied in many instances in the literature [72, 73], including when addressing switched systems [70, 74] and Markov jump linear systems (MJLSs) [34, 75]. Other types of uncertainties can also be converted to a polytopic representation, as seen in [76], which provides a method to rewrite affine uncertainties in a polytopic domain.

2.2 DETERMINISTIC ATTACK MODEL

The DoS attacks originate from malicious agents that aim to jeopardize the system performance by jamming its communication channels and, consequently, causing packet dropouts. It has been shown in the literature that if these attacks are not accounted for when designing the control system they may degrade the system performance, or even drive it to instability [40]. In a state-feedback control context, they can make it impossible to transmit state readings from the sensor to the control system and/or to transmit control signals from the controller to the actuator. This is illustrated in Figure 2.1.

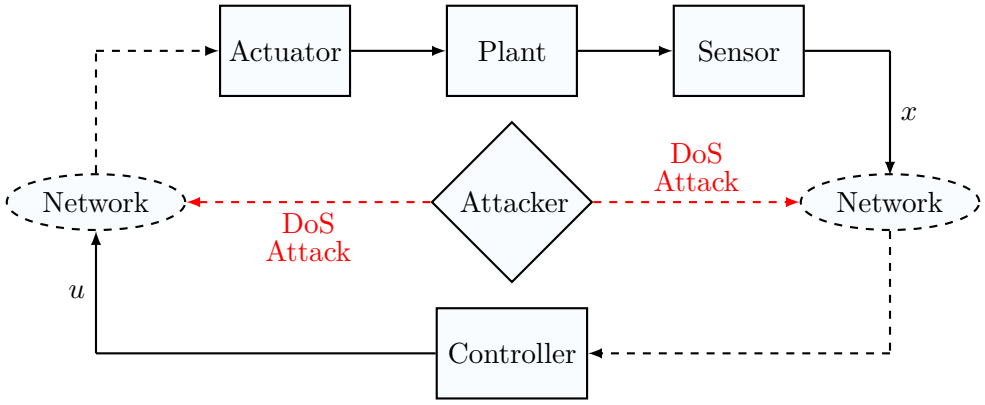

Figure 2.1: Schematic of the state-feedback control with the presence of DoS attacks.

In a filtering context, the DoS attacks attacks may interrupt the transmission of the measured output between the plant and the filter, as depicted by Figure 2.2.

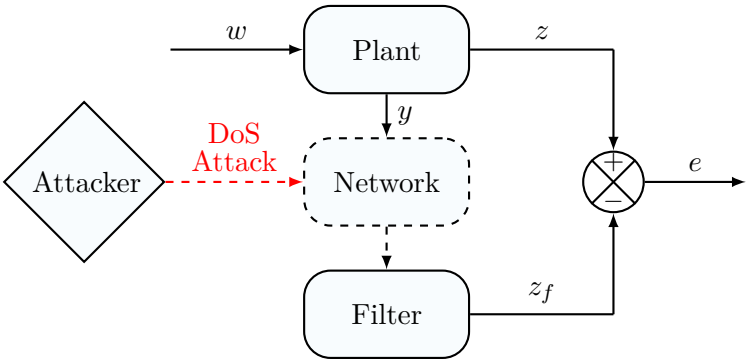

Figure 2.2: Schematic of the filtering system with the presence of DoS Attacks.

Note that in Figure 2.2, w is the exogenous disturbance, y is the measured output, z is the estimated output, z_f is the filter output and e is the error, where $e = z - z_f$.

Predicting the exact attacker's behavior is a difficult task. However, it is possible to assume that the attacker is energy-bounded, which translates into attacks having a bounded duration [36, 37]. Thus, the following deterministic assumption is established:

Assumption 2.1

The DoS attacks display a bounded duration of N consecutive time-instants, with the network staying free of attacks for at least one time instant before the next attack begins.

Based on Assumption 2.1, the control system will remain devoid of new measurements and/or, most importantly, the actuator will remain without new control inputs for N time-instants, in a worst-case scenario. This scenario brought forth the packet-based strategies [36, 37, 48], where at each time instant a packet $U(k_t)$ with $N+1$ control inputs is created by the controller and sent to the actuator, where they are successively utilized if an attack ensues, guaranteeing the CPS stability. This mitigates an attack in the controller-actuator channel. Moreover, since this packet is created with only measurements from a given k instant of time, the sensor-controller channel may also be jammed for N time instants without loss of stability, as this condition is simultaneously solved by the packet-based strategy.

Given the above discussion, and following the procedure described in higher detail in [77], a new time-scale k_t is introduced, which indicates the time instant when a new packet of control inputs arrives at the actuator. In this new time-scale, k_t updates as follows:

$$k_{t+1} = k_t + \kappa(k_t) + 1, \quad (k_0 = 0), \tag{2.4}$$

where $\kappa(k_t)$ is a time-varying switching signal that draws values from a finite set $\mathbb{H} \triangleq \{0, 1, \ldots, N\}$, and represents the number of consecutive attacks starting at the time $k_t + 1$. If $\kappa(k_t) = 0$, then no attack starts at $k_t + 1$ For clarity's sake, the correspondence between both time scales is illustrated considering the example in the sequel:

- Consider $N = 3$ the maximum number of consecutive DoS attacks;

- Consider the switching signal of $\kappa(k_t) = \{2, 0, 3\}$, indicating the sequence of consecutive time instants of attack;

Figure 2.3 depicts the relation between the two established time scales according to the switching signal $\kappa(k_t)$. The symbol ⊗ indicates that in the referred time instant, an attack is taking place and there is no transmission. Each time increment of k_t indicates the absence of attacks and the arrival of a new packet at the actuator.

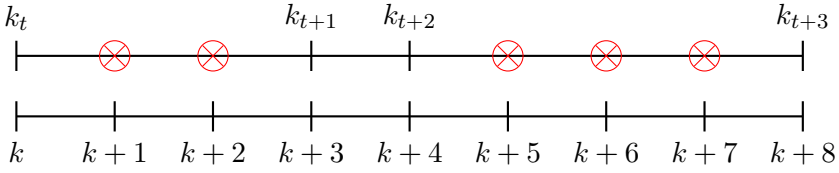

Figure 2.3: Correspondence between time scales k and k_t for $\kappa(k_t) = \{2, 0, 3\}$. ⊗ represents the packet dropouts caused by DoS attacks.

2.2.1 *Packet-based control strategy*

Departing from the aforementioned time scale, the state-feedback control law for the packet of $N + 1$ inputs is delineated by:

$$u(k_t + r) = K_r x(k_t), \tag{2.5}$$

where $r = 0, 1, \ldots, \kappa(k_t)$, being $\kappa(k_t)$ the previously defined time-varying switching signal. Furthermore, the package of inputs is composed by

$$U(k_t) = \begin{bmatrix} u(k_t)^T & u(k_t + 1)^T & \ldots & u(k_t + N)^T \end{bmatrix}^T.$$

At each time instant free of attacks, a new packet $U(k_t)$ is transmitted to the actuator. The control strategy, then, is implemented by the following rules:

1. If a new packet arrives at the actuator at $k_t + 1$, $u(k_t)$ is the only control input applied, and the rest of the inputs from $U(k_t)$ are discarded.

2. If a DoS attacks starts at $k_t + 1$, then the control inputs $u(k_t + 1), \ldots, u(k_t + r)$ previously designed and transmitted in $U(k_t)$ will be successively applied to the actuator until the attack ceases and a new packet arrives at the actuator.

Remark 2.1

As can be seen in the implementation rules, if the number of designed control signals is higher than the number of attacks, the remaining inputs will be discarded with the arrival of a new packet, which may be seen as a waste of network load. However, as seen in [36],

the increase in network load required for this strategy is not sufficient to create a significant increase in network traffic.

To illustrate the implementation rules, the example case depicted by Figure 2.3 is utilized again. In this case, there will be 3 packets with $N+1$ control inputs each. According to the aforementioned implementation rules and the considered attack sequence, the control inputs in blue are utilized while the ones in red are discarded due to the transmission of a new packet.

$$U(k_t) = \begin{bmatrix} u(k_t)^T & u(k_t+1)^T & u(k_t+2)^T & u(k_t+3)^T \end{bmatrix}^T,$$
$$U(k_{t+1}) = \begin{bmatrix} u(k_{t+1})^T & u(k_{t+1}+1)^T & u(k_{t+1}+2)^T & u(k_{t+1}+3)^T \end{bmatrix}^T,$$
$$U(k_{t+2}) = \begin{bmatrix} u(k_{t+2})^T & u(k_{t+2}+1)^T & u(k_{t+2}+2)^T & u(k_{t+2}+3)^T \end{bmatrix}^T.$$

The approach exposed so far can be called **Full packet strategy**, as it designs and uses a distinct control input for each time instant under attack. Alternatively, one may also consider the packet-based framework with strategies like the hold and zero-input, which have been investigated in control [16] and filtering [32] problems. Their definition in the packet-based context is presented in the sequence:

- Hold-input Strategy: A fixed gain and a unique control input is designed for when the network is operational, and when a packet dropout phenomenon takes place. This translates in the packet of inputs as:

$$U(k_t) = \begin{bmatrix} u(k_t) & u(k_t) & \dots & u(k_t) \end{bmatrix};$$

- Zero-input Strategy: The control inputs are set to zero whenever a packet dropout phenomenon takes place. This translates in the packet of inputs as:

$$U(k_t) = \begin{bmatrix} u(k_t) & 0 & \dots & 0 \end{bmatrix}.$$

Even though there is evidence that the Full packet strategy is less conservative than the hold and zero-input strategies in the context of DoS attacks [37], these strategies are worth investigating given their increased simplicity, and for not requiring a distinction on what concerns control input value between consecutive time instants of packet loss.

2.3 STABILITY OF SWITCHED SYSTEMS

Switched systems consist of a class of hybrid systems that switch between different subsystems (modes), generating discontinuities in the system dynamics [78]. This way, a two-level dynamic emerges where the lower level consists of the differential and/or difference equations of the subsystems and an upper level that defines when the switching between modes takes place [79].

Different aspects may govern the switching rule of such systems. For instance, the switching may be state-dependent, time-dependent, controlled, or autonomous [80, 81]. In the latter, which

is also called arbitrary switching, there is no control or knowledge over the switching rule, being necessary to consider all possible switching trajectories on what concerns stability analysis and control design. Moreover, the individual modes of the system may also be subjected to uncertainties or time-varying parameters in a polytopic domain [74, 82].

In the considered context of DoS attacks, there is no knowledge concerning the attacker's behavior. This way, by modeling the closed-loop dynamics after a switched system with arbitrary switching, one accounts for whichever behavior the attacker may display (under the energetic restriction depicted by Assumption 2.1). Thus, when only considering the presence of attacks, this work will model the closed-loop dynamics of the system under DoS attacks using a switched uncertain system.

Consider the following switched discrete-time uncertain system:

$$x(k+1) = A_{\kappa(k)}(\alpha)x(k), \tag{2.6}$$

where $x(k) \in \mathbb{R}^{n_x}$ is the state vector, $\kappa(k)$ is a time-varying switching signal that takes values from the set $G \triangleq \{1, \ldots, N_m\}$ where N_m is the number of modes. Each mode $A_i(\alpha)$, $i = 1, \ldots, N_m$ is part of a polytopic domain dependent on the time-invariant parameter α as described in Section 2.1.

Since only one mode is active at a time, it is possible to combine all modes of (2.6) through the following:

$$x(k+1) = A(\zeta(k), \alpha)x(k), \tag{2.7}$$

where $\zeta(k) = \left[\zeta_1(k), \ldots, \zeta_{N_m}(k)\right]^T$. $\zeta(k)$ is then described by the following indicator function that depicts the switching behavior:

$$\zeta_i(k) = \begin{cases} 1, & \text{if } \kappa(k) = i, \\ 0, & \text{otherwise,} \end{cases} \tag{2.8}$$

where, $A(\zeta(k), \alpha) = \zeta_1(k)A_1(\alpha) + \cdots + \zeta_{N_m}(k)A_{N_m}(\alpha)$. Through (2.8), one may highlight that $\sum_{i=1}^{N_m} \zeta_i(k) = 1$, $\zeta_i(k)^2 = 1$, and $\zeta_i\zeta_j = 0$, when $i \neq j$.

Aiming to obtain a less conservative sufficient stability certificate for system (2.6), a switched parameter-dependent Lyapunov function is considered in the following Lemma.

Lemma 2.1

If there exist symmetric positive definite matrices $P_i(\alpha) \in \mathbb{R}^{n_x \times n_x}$ such that

$$\begin{bmatrix} P_i(\alpha) & A_i(\alpha)^T P_j(\alpha) \\ P_j(\alpha)A_i(\alpha) & P_j(\alpha) \end{bmatrix} > 0, \tag{2.9}$$

with $i, j \in G$, $G \triangleq \{1, \ldots, N_m\}$, then the switched uncertain system (2.6) is asymptotically stable under arbitrary switching, for all $\alpha \in \Lambda_V$.

Proof.

Multiplying (2.9) by $\zeta_i(k)$, for $i = 1, \ldots, N_m$, and summing it up, yields

$$\begin{bmatrix} P(\zeta(k),\alpha) & A(\zeta(k),\alpha)^T P_j(\alpha) \\ P_j(\alpha)A(\zeta(k),\alpha) & P_j(\alpha) \end{bmatrix} > 0.$$

Then, applying the same procedure with $\zeta_j(k+1)$, for $j = 1, \ldots, N_m$ returns

$$\begin{bmatrix} P(\zeta(k),\alpha) & A(\zeta(k),\alpha)^T P(\zeta(k+1),\alpha) \\ P(\zeta(k+1),\alpha)A(\zeta(k),\alpha) & P(\zeta(k+1),\alpha) \end{bmatrix} > 0.$$

In the sequel, applying Schur complement results on:

$$A(\zeta(k),\alpha)^T P(\zeta(k+1),\alpha)A(\zeta(k),\alpha) - P(\zeta(k),\alpha) < 0.$$

Pre- and post-multiplying it by $x(k)^T$ and $x(k)$, respectively, one obtains $\Delta V(x(k),\zeta(k)) < 0$, considering the Lyapunov function $V(x(k),\zeta(k)) = x(k)^T P(\zeta(k),\alpha)x(k)$, which, given that $P(\zeta(k),\alpha)$ is a positive definite matrix, implies that $V(x(k),\zeta(k)) > 0$. This way, as supported by [74, Theorem 3] for the time-varying case, the switched uncertain system (2.6) is asymptotically stable under arbitrary switching. This concludes the proof. □

Remark 2.2

Handling matrices in the polytopic domain may offer an infinite dimension problem, given the structure of the simplex itself. The parser ROLMIP [83], however, is able to write such matrices and parameter-dependent LMIs as finite dimension conditions.

2.4 NON-HOMOGENEOUS MARKOV NETWORK MODEL

Networked Control Systems (NCSs) is a topic with growing interest [84] and comes as a necessity in systems whose elements are geographically distant and in the context of CPSs. Including a network in the closed loop, however, brings forth problems like the already mentioned cyberattacks [18], time-delays [85], and packet-losses due to network unreliability and limitations [84, 86]. Focusing on the latter, it is often assumed that the packet losses are stochastic in nature, which allows the use of discrete-time MJLSs [87] to model the abrupt changes in the system operation. A classic model for unreliable networks consists of the Gilbert-Elliot model [57, 58, 88], which divides the operation between two modes: Successful packet transmission and packet loss, as it is illustrated in Figure 2.4.

In Figure 2.4, when in mode 1, the network is operating properly and has just transmitted successfully, and has a probability of p_{11} of continuing to transmit successfully, and a probability p_{12} of suffering a packet dropout. When in mode 2, the network has just suffered a packet

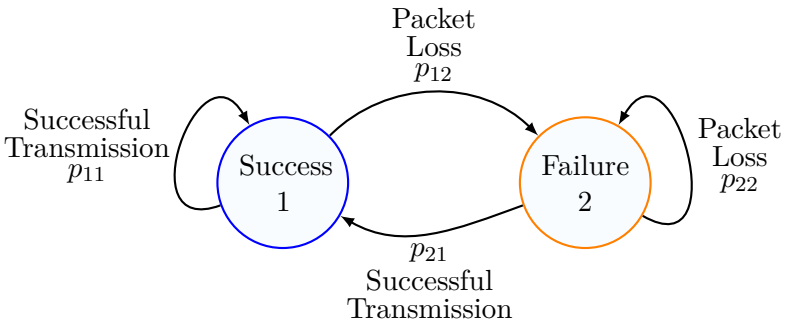

Figure 2.4: Markov chain for the Gilbert-Elliot model.

dropout and has a probability p_{22} of suffering another one, and a probability p_{21} of transmitting successfully.

Many works based on MJLSs to model packet losses, however, consider time-invariant probabilities and, consequently, homogeneous Markov chains. This assumption may prove to be unrealistic, as environmental factors or network characteristics may vary with time, changing the transmission failure chances. The inclusion of DoS attacks further introduces a time-varying nature to the packet losses, as the attacker's behavior may change with time. As a way to circumvent this problem, two strategies may be mentioned: using finite piecewise homogeneous Markov chains [89, 90], or the use of non-homogeneous Markov chains with time-varying probabilities [33, 34]. The probabilities of the non-homogeneous Markov chain can be modeled in the polytopic domain depending on time-varying parameters that change arbitrarily with time [33], and even the existence of uncertain or unknown probabilities may be taken into account [91, 92].

As mentioned in Section 2.2, it is possible to make the deterministic assumption that the attacker is energetically bounded. This assumption could not be so easily included in a classic Gilbert-Elliot model. Furthermore, the combination of the lack of knowledge of the attacker's behavior, and the possibility of DoS attacks not reaching its maximum possible duration every time an attack begins allows the creation of a new network model that accounts for both DoS attacks and packet losses due to network unreliability and limitations, aiming to offer a less conservative approach to this problem. In this Section, this model will be proposed based on a non-homogeneous Markov chain that will account for a wider range of scenarios through the use of uncertain and unknown transition probabilities that arbitrarily change with time. This model can, then, be applied to portray the network featured in the schematics of Figure 2.1 and Figure 2.2.

Consider a discrete-time non-homogeneous Markov chain $\{\theta_k; k \geq 0\}$ with a finite state-space $\mathbb{K} = \{1, \ldots, \sigma\}$ where the mode transition probabilities are as follows

$$p_{ij}(k) = Pr(\theta_{k+1} = j \mid \theta_k = i), \tag{2.10}$$

which satisfies $p_{ij}(k) \geq 0$ and $\sum_{j=1}^{\sigma} p_{ij}(k) = 1,\ \forall k \geq 0$. These mode transition probabilities are all contained in the transition probabilities matrix $\Psi(k) = |p_{ij}(k)|,\ i, j \in \mathbb{K}$.

With the previously defined Markov chain, the stochastic network model will be constructed. The presence of DoS attacks from malicious agents is considered in addition to possible com-

munication failures caused by the unreliability and limitations of the communication channels. Both phenomena will translate into packet dropouts in the network. To combine both problems, the deterministic Assumption 2.1 of the attacker's energy limitation will be taken into account, binding the duration of a DoS attack to N time instants. This enables modeling a finite number of modes indicating each consecutive time instant with the presence of DoS attacks.

Figure 2.5 illustrates the schematic of the proposed Markovian network model. The modes indicate three types of situations: i) Successful transmission, ii) Transmission failure, and iii) DoS attacks.

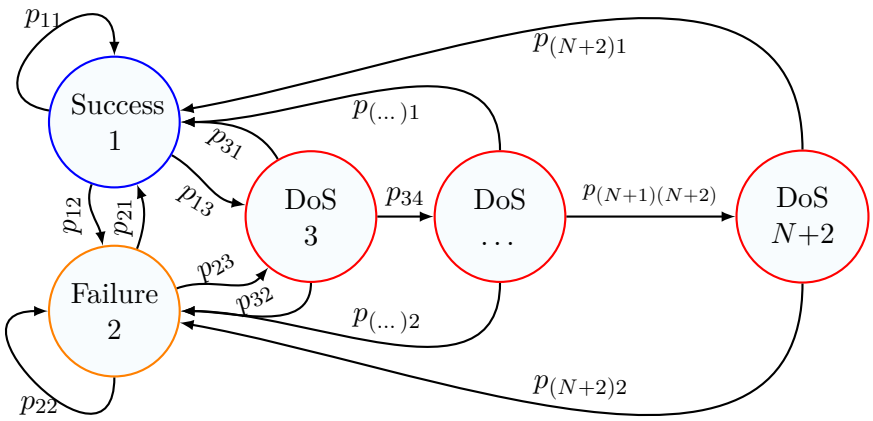

Figure 2.5: Markov chain of the Network considering Transmission Failures and DoS attacks.

The modes definition and transitions are discussed in further detail in the sequel:

i) There are neither transmission failures nor DoS attacks and the transmission is successful ($\theta_k = 1$). In this mode, there is a probability p_{11} of the network remaining operational; a probability p_{12} of having a communication failure due to network limitations (mode 2); and a probability p_{13} of suffering the first time instant of a DoS attacks (mode 3). See mode 1 in Figure 2.5.

ii) A transmission failure happens because of communication channel limitations ($\theta_k = 2$). In this mode, there is a probability p_{21} of the network returning to regular operation (mode 1); a probability p_{22} of occurring another transmission failure (mode 2); and a probability p_{23} of a DoS attacks (mode 3). See mode 2 in Figure 2.5.

iii) The communication channels are under a DoS attack ($\theta_k = 3, \dots, N+2$). Starting from mode 3, there is a probability p_{31} of the attack ceasing and the network returning to regular operation (mode 1); a probability p_{32} of the attack ceasing, followed by a transmission failure (mode 2); and a probability p_{34} of the attack persisting for another consecutive time instant. This applies to $\theta_k = 4$ up to $\theta_k = N+1$. In mode $N+2$, however, the attacker has

reached his energy bounds and the DoS attacks will have to cease. From there on, regular network operation (mode 1) may be restored with a probability $p_{(N+2)1}$ or a transmission failure (mode 2) may follow, with a probability of $p_{(N+2)2}$.

It can be highlighted that the combination of i) and ii) represent a simplified Gilbert-Elliot model, while the rest of the modes stochastically model the attack whilst considering its deterministic energy constraint. The combination of i), ii), and iii) results in the proposed network model.

Given the aforementioned $N+2$ modes of the Markovian network and its possible transitions, the transition probability matrix $\Psi \in \mathbb{R}^{(N+2)\times(N+2)}$ derived from Figure 2.5 is as follows

$$\Psi = \begin{bmatrix} p_{11} & p_{12} & p_{13} & 0 & \dots & 0 \\ p_{21} & p_{22} & p_{23} & 0 & \dots & 0 \\ p_{31} & p_{32} & 0 & p_{34} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{(N+1)1} & p_{(N+1)2} & 0 & 0 & \dots & p_{(N+1)(N+2)} \\ p_{(N+2)1} & p_{(N+2)2} & 0 & 0 & \dots & 0 \end{bmatrix}. \tag{2.11}$$

For the sake of clarity, the same colors indicating the operation modes and their probabilities, as featured in the Markov chain from Figure 2.5, are employed in matrix (2.11). Concerning the state-space $\mathbb{K} = \{1, \dots, \sigma\}$ of the network Markov chain, $\sigma = N+2$ will be considered hereafter.

The presented framework seeks to add nuance to the network model, not oversimplifying the packet dropout problem of an unreliable network with DoS attacks into a traditional Gilbert-Elliot model, since we can bind the number of consecutive attacks to a maximum finite number. This can be particularly useful if we consider the following assumption:

Assumption 2.2

The control or filtering system is able to differentiate between a transmission failure due to a network limitation and a packet dropout caused by a DoS attacks.

In this scenario, it is possible to design mode-dependent controllers and filters for the proposed problem. In turn, attack and failure detection are open problems, and distinct fields of study and are not the focus of this work. However, [93, 94] for example, indicate that there may be feasible solutions. Nevertheless, as will be shown in Chapter 4 and Chapter 5, even not utilizing a different controller or filter for each network mode yields better results than considering a traditional Gilbert-Elliot model to depict the network.

2.4.1 *Time-varying Transition Probability Matrix*

Obtaining the transition probabilities p_{ij} is a challenging task in the proposed model. This happens mainly because, aside from the attacker's energy limitation, it is difficult to know the attack

behavior. As a way to circumvent this problem, the transition probability matrix (2.11) considered features uncertain and unknown probabilities, which will be modeled with time-varying parameters. This enables considering a wider range of probabilities with more or less conservative scenarios, while not requiring an exact knowledge of the transmission failure frequency and attacker's behavior.

To model these transition probability matrices, each of the m rows that feature uncertain or unknown probabilities is written in a polytopic representation dependent on the time-varying parameter $\xi_{k,q}$, where $q = 1, \ldots, m$, in the same lines as in [91, 92]. This representation is originated from the conditions $\sum_{j=1}^{\sigma} p_{ij}(k) = 1$ and $p_{ij}(k) \geq 0$. A generic matrix $M(\xi_{k,q})$ in this framework, referring to the q row from the total of m rows, is as follows

$$M(\xi_{k,q}) = \sum_{z=1}^{Z_q} \xi_{k,qz} M_z, \quad \xi_k \in \Lambda_{Z_q}, \tag{2.12}$$

where Z_q is the number of vertices for the q row, and Λ_{Z_q} is the unit simplex described by

$$\Lambda_{Z_q} = \left\{ \xi_{k,q} \in \mathbb{R}^{Z_q} : \sum_{z=1}^{Z_q} \xi_{k,z} = 1; \xi_{k,qz} \geq 0, z = 1, \ldots, Z_q \right\}, \tag{2.13}$$

To illustrate, an example matrix is considered based in (2.11) with $N = 2$. The first row has unknown probabilities (represented by $'?'$), and the third row has uncertain probabilities. Therefore, $m = 2$.

$$\Psi = \begin{bmatrix} 0.5 & ? & ? & 0.0 \\ 0.6 & 0.1 & 0.3 & 0.0 \\ 0.3 & \begin{bmatrix} 0.1 & 0.5 \end{bmatrix} & 0.0 & \begin{bmatrix} 0.2 & 0.6 \end{bmatrix} \\ 0.8 & 0.2 & 0.0 & 0.0 \end{bmatrix}. \tag{2.14}$$

The vertices of the polytopes of the first and third row must respect the conditions $p_{ij}(k) \geq 0$ and $\sum_{j=1}^{4} p_{ij}(k) = 1$. This way, the first row vertices are:

$$p1_{(1)} = \begin{bmatrix} 0.5 & 0.5 & 0.0 & 0.0 \end{bmatrix}, \quad \text{and} \quad p1_{(2)} = \begin{bmatrix} 0.5 & 0.0 & 0.5 & 0.0 \end{bmatrix}.$$

Being the convex vertices combination that depicts the first row unit simplex as follows

$$p_1(k) = \xi_{k,11} p1_{(1)} + \xi_{k,12} p1_{(2)}, \quad \xi_{k,1} = (\xi_{k,11}, \xi_{k,12}) \in \Lambda_2.$$

The same procedure is applied to obtain the vertices of the third row:

$$p3_{(1)} = \begin{bmatrix} 0.3 & 0.1 & 0.0 & 0.6 \end{bmatrix}, \quad \text{and} \quad p3_{(2)} = \begin{bmatrix} 0.3 & 0.5 & 0.0 & 0.2 \end{bmatrix}.$$

The polytope representing the third row's uncertain probabilities is inserted in a different unit simplex since each row's probabilities are independent of one another:

$$p_3(k) = \xi_{k,21} p_{3_{(1)}} + \xi_{k,22} p_{3_{(2)}}, \quad \xi_{k,2} = (\xi_{k,21}, \xi_{k,22}) \in \Lambda_2.$$

Note that the different simplexes depend on different parameters. The first row's polytope depends on the time-varying parameter $\xi_{k,1}$ while the third row depends on $\xi_{k,2}$. The second and fourth row display precisely known probabilities, and can be written simply as $p_2 = \begin{bmatrix} 0.6 & 0.1 & 0.3 & 0.0 \end{bmatrix}$ and $p_4 = \begin{bmatrix} 0.8 & 0.2 & 0.0 & 0.0 \end{bmatrix}$.

Combining the polytopic description of the first and third row, as well as the second and fourth constant rows results in

$$\Psi(k) = \xi_{k,11} \begin{bmatrix} p_{1_{(1)}} \\ 0 \\ 0 \\ 0 \end{bmatrix} + \xi_{k,12} \begin{bmatrix} p_{1_{(2)}} \\ 0 \\ 0 \\ 0 \end{bmatrix} + \xi_{k,21} \begin{bmatrix} 0 \\ 0 \\ p_{3_{(1)}} \\ 0 \end{bmatrix} + \xi_{k,22} \begin{bmatrix} 0 \\ 0 \\ p_{3_{(2)}} \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ p_2 \\ 0 \\ p_4 \end{bmatrix}.$$

This representation, however, is not a homogeneous polynomial with relation to the parameters $\xi_{k,1}$ and $\xi_{k,2}$. Thus, to obtain an homogeneous equivalent, noting that $\xi_{k,11} + \xi_{k,12} = 1$, and $\xi_{k,21} + \xi_{k,22} = 1$, the procedure in the sequel is employed.

$$\begin{aligned} \Psi(k) = (\xi_{k,21} + \xi_{k,22}) & \left(\xi_{k,11} \begin{bmatrix} p_{1_{(1)}} \\ 0 \\ 0 \\ 0 \end{bmatrix} + \xi_{k,12} \begin{bmatrix} p_{1_{(2)}} \\ 0 \\ 0 \\ 0 \end{bmatrix} \right) \\ + (\xi_{k,11} + \xi_{k,12}) & \left(\xi_{k,21} \begin{bmatrix} 0 \\ 0 \\ p_{3_{(1)}} \\ 0 \end{bmatrix} + \xi_{k,22} \begin{bmatrix} 0 \\ 0 \\ p_{3_{(2)}} \\ 0 \end{bmatrix} \right) + (\xi_{k,11} + \xi_{k,12})(\xi_{k,21} + \xi_{k,22}) \begin{bmatrix} 0 \\ p_2 \\ 0 \\ p_4 \end{bmatrix}. \end{aligned}$$

The resulting transition probability matrix $\Psi(\xi_k)$ is, then, the following

$$\Psi(\xi_k) = \xi_{k,11}\xi_{k,21} \begin{bmatrix} p_{1_{(1)}} \\ p_2 \\ p_{3_{(1)}} \\ p_4 \end{bmatrix} + \xi_{k,11}\xi_{k,22} \begin{bmatrix} p_{1_{(1)}} \\ p_2 \\ p_{3_{(2)}} \\ p_4 \end{bmatrix}$$

$$+\xi_{k,12}\xi_{k,21}\begin{bmatrix} p_{1_{(2)}} \\ p_2 \\ p_{3_{(1)}} \\ p_4 \end{bmatrix} + \xi_{k,12}\xi_{k,22}\begin{bmatrix} p_{1_{(2)}} \\ p_2 \\ p_{3_{(2)}} \\ p_4 \end{bmatrix}, \quad \xi_k \in \Omega, \quad (2.15)$$

where $\xi_k = (\xi_{k,1}, \xi_{k,2}) \in (\Lambda_2 \times \Lambda_2)$ and consists in a homogeneous polynomial in function of the combination of the time-varying parameters $\xi_k = (\xi_{k,1}, \xi_{k,2})$. This concludes the example. It is also worthy of note that $\Omega = (\Lambda_2 \times \Lambda_2)$ represents the Cartesian product of both simplexes, called a multi-simplex. More upon that can be found in [95].

In the sequel, the formal definitions of a multi-simplex and a Λ-homogeneous polynomial are presented:

Definition 2.1: [76]

A multi-simplex Ω is the Cartesian product $\Lambda_{Z_1} \times \cdots \times \Lambda_{Z_m}$ of a finite number of simplexes, where Λ_Z has a dimension defined by the index $Z = (Z_1, \ldots, Z_m)$. The given parameter ξ of a simplex Λ_Z consists on $(\xi_1, \xi_2, \ldots, \xi_m)$, depending on the number of vertices of Λ_Z. Each ξ_i is then decomposed in $(\xi_{i1}, \xi_{i2}, \ldots, \xi_{iZ_i})$.

Definition 2.2: [91]

Given a multi-simplex Ω of dimension Z, a polynomial $S(\xi)$ defined on $\mathbb{R}^Z$ and taking values in a finite-dimensional vector space is said Λ-homogeneous if, for any $r_0 \in \{1, \ldots, m\}$, and for any given $\xi_Z \in \mathbb{R}^{Z_q}$, $q \in \{1, \ldots, m\} \backslash \{q_0\}$, the partial application $\xi_{Z_{q_0}} \mapsto P(\xi)$ is a homogeneous polynomial.

In a generic formulation, the utilized Λ-homogeneous polynomial transition probability matrix with m rows with uncertain or unknown probabilities is

$$\Psi(\xi_k) = \sum_{z=1}^{\psi} \xi_k(z)\Psi_z, \quad \xi_k = (\xi_{k,1}, \ldots, \xi_{k,m}) \in (\Lambda_{Z_1} \times \cdots \times \Lambda_{Z_m}) = \Omega_\psi, \quad (2.16)$$

where $z = 1, 2, \ldots, \psi$, with $\psi = Z_1 Z_2 \ldots Z_m$ vertices and $\xi_k = (\xi_{k,1}, \ldots, \xi_{k,m})$. $\xi_k(z)$ are homogeneous monomials with degree m which are created by the ψ-tuple with all the ψ possible combinations obtained between the sets $\mathscr{K}_1 = \{\xi_{k,11}, \ldots, \xi_{k,1Z_1}\}$ up to $\mathscr{K}_m = \{\xi_{k,m1}, \ldots, \xi_{k,mZ_m}\}$, i.e.,

$$\begin{aligned} \xi_k(1) &= \xi_{k,11}\xi_{k,21}\ldots\xi_{k,m1}, \\ \xi_k(2) &= \xi_{k,12}\xi_{k,21}\ldots\xi_{k,m1}, \\ &\vdots \qquad\quad \vdots \\ \xi_k(\psi) &= \xi_{k,1Z_1}\xi_{k,2Z_2}\ldots\xi_{k,mZ_m}. \end{aligned}$$

To demonstrate how this general case applies, the example matrix (2.14) is utilized again. The matrix has $m = 2$ rows with uncertain or unknown probabilities, which translates into 2 simplexes ($\xi_{k,1} \in \Lambda_2$ and $\xi_{k,2} \in \Lambda_2$). The resulting multi-simplex $\Lambda_2 \times \Lambda_2$ has $\psi = Z_1 Z_2 = 4$ vertices, and is written in function of monomials $\xi_k(z)$ of degree $m = 2$, for $z = 1, 2, 3, 4$. These monomials are composed by the 4-tuple with the combination of the sets $\mathscr{K}_1 = \{\xi_{k,11}, \xi_{k,12}\}$ and $\mathscr{K}_2 = \{\xi_{k,21}, \xi_{k,22}\}$, namely

$$\begin{aligned}
\xi_k(1) &= \xi_{k,11}\xi_{k,21}, \\
\xi_k(2) &= \xi_{k,12}\xi_{k,21}, \\
\xi_k(3) &= \xi_{k,11}\xi_{k,22}, \\
\xi_k(4) &= \xi_{k,12}\xi_{k,22},
\end{aligned}$$

which, in turn, can be confirmed in (2.15).

Remark 2.3

More details on the homogenization of multi-simplexes, Λ-homogeneous polynomial matrices manipulations, and how to write finite LMI conditions utilizing them can be found in [91]. In this work, however, the writing of polynomial matrices, LMI conditions in a multi-simplex as finite dimension conditions, and the process of polynomial homogenization presented are handled automatically by using the parser ROLMIP [83].

2.5 STABILITY OF NON-HOMOGENEOUS MARKOV JUMP LINEAR SYSTEMS

There are different possible definitions of stability for MJLSs. For instance, mean-square stability, stochastic stability, and exponential mean-square stability [96]. These definitions are based on the Second Moment Stability (SMS) concept [97–99], and, on what concerns MJLSs with homogenous Markov chains, the three definitions are equivalent. When dealing with non-homogeneous Markov chains with time-varying probabilities, however, such equivalence is not met. It is then important to consider the time-varying dynamics and uncertainties of the probabilities in the design conditions, as not doing so may result in performance degradation or even instability [53]

Consider the following MJLS with polytopic uncertainties in function of time-invariant parameter α. The system also depends on a network based on the non-homogeneous Markov chain proposed in Section 2.4 and 2.4.1.

$$x(k+1) = A(\theta_k, \alpha)x(k), \tag{2.17}$$

where $x(k) \in \mathbb{R}^{n_x}$ is the state vector, α is a time-invariant parameter that describes the system polytopic uncertainties as in (2.2). θ_k is a random variable that assumes values from the finite set $\mathbb{K} = \{1, \ldots, \sigma\}$ according to a given transition probability matrix $\Psi(\xi_k)$ that is dependent on the time-varying parameters ξ_k and written as in (2.16). To simplify, $A(\theta_k = i, \alpha) = A_i(\alpha)$.

As to obtain a stochastic stability definition for the approached non-homogeneous MJLSs, the concept of Exponential stability in the mean square sense with conditioning I (ESMS-CI), as defined by [54, Proposition 1], [55, Definition 3.1(c)] is considered in this work. The formal definition is depicted in the sequel:

Definition 2.3

The system (2.17) is ESMS-CI if there exist $\beta \geq 1$, $q \in (0,1)$ such that for any Markov Chain $(\{\theta_k\}_{k\geq 0}, \{\Psi_k\}_{k\geq 0}, \mathbb{K})$ under nondegenerate stochastic matrices Ψ_k we have

$$\mathscr{E}[|\Phi(k,k_0)x_{k_0}|^2|\theta_{k_0}=i] \leq \beta|x(k_0)|^2 q^{k-k_0}, \forall k \geq k_0 \geq 0, i \in \mathbb{K}_{k_0}, x(k_0) \in \mathbb{R}^{n_x}, \quad (2.18)$$

where $\Phi(k,k_0)$ is the fundamental random matrix solution of system (2.17) (more on this in [55, pages 60-64]) and $\mathbb{K}_{k_0} \in \{i \in \mathbb{K} | \Psi\{\theta_{k_0}=i\} > 0\}$

The following Lemma gives the sufficient conditions to guarantee that the MJLS system (2.17) is ESMS-CI:

Lemma 2.2

If there exists symmetric positive definite matrices $P_i(\xi_k, \alpha) \in \mathbb{R}^{n_x \times n_x}$ such that

$$A_i(\alpha)^T P_i^+ A_i(\alpha) - P_i(\xi_k, \alpha) < 0, \quad (2.19)$$

where

$$P_i^+ = \sum_{j=1}^{\sigma} p_{ij}(\xi_k) P_j(\xi_{k+1}, \alpha), \quad (2.20)$$

hold for each $i \in \mathbb{K}$, then (2.17) is ESMS-CI for all $(\alpha, \xi_k, \xi_{k+1}) \in \Lambda_V \times \Omega_\psi \times \Omega_\psi$, for $k \geq 0$.

Proof. More details and the proof of this Lemma can be found in [55, Pages 76-77]. □

Remark 2.4

It is worthy of note that ξ_{k+1} is considered by the parser as a new unit (multi-)simplex. This idea was introduced by [100] and utilized in [48].

2.6 FINSLER'S LEMMA

In this work, Finsler's Lemma will be utilized to introduce new slack variables to the LMI conditions, i.e., by going from *i*) to *iv*) or *ii*) to *iv*). The addition of slack variables is useful to expand the search space when pursuing feasible solutions, as it results in less conservative conditions. Examples of this can be found in [60, 101–103].

Lemma 2.3

If there exist $\omega \in \mathbb{R}^{n_1}$, $\mathscr{Q} \in \mathbb{R}^{n_1 \times n_1}$, and $\mathscr{B} \in \mathbb{R}^{n_2 \times n_1}$ with $rank(\mathscr{B}) < n_1$, being $\mathscr{B}^{\perp}$ a basis for the Nullspace of $\mathscr{B}$ (i.e., $\mathscr{B}\mathscr{B}^{\perp} = 0$), then the following conditions are equivalent

i) $\omega^T \mathscr{Q} \omega < 0,\ \forall\ \omega \neq 0 : \mathscr{B}\omega = 0,$

ii) $\mathscr{B}^{\perp T} \mathscr{Q} \mathscr{B} < 0,$

iii) $\exists \mu \in \mathbb{R} : \mathscr{Q} - \mu \mathscr{B}^T \mathscr{B} < 0,$

iv) $\exists \mathscr{X} \in \mathbb{R}^{n_1 \times n_2} : \mathscr{Q} + \mathscr{X}\mathscr{B} + \mathscr{B}^T \mathscr{X}^T < 0.$

Proof. The proof of this Lemma can be found in [104]. □

3

$\mathscr{H}_2$ STATE-FEEDBACK CONTROL FOR CYBER-PHYSICAL UNCERTAIN SYSTEMS UNDER DOS ATTACKS

This chapter addresses the packet-based state-feedback control problem for discrete-time Cyber-physical uncertain systems under the presence of energy-limited exogenous disturbances and Denial of Service attacks (DoS attacks). The deterministic assumption of the attacker's energetic bounds (as stated in Section 2.2) is taken into account and the closed-loop system dynamics under attacks are modeled after a switched system. The full packet, hold-input and zero-input strategies as described in Subsection 2.2.1 are addressed and tested in the presented context. The presence of exogenous disturbances is investigated under the $\mathscr{H}_2$ cost, which is utilized to evaluate each strategy performance.

3.1 PROBLEM STATEMENT

Consider the following discrete-time uncertain model of a CPS plant:

$$\begin{aligned} x(k+1) &= A(\alpha)x(k) + B_u(\alpha)u(k) + B_w(\alpha)w(k), \\ y(k) &= C(\alpha)x(k) + D_u(\alpha)u(k) + D_w(\alpha)w(k), \end{aligned} \tag{3.1}$$

where $x(k) \in \mathbb{R}^{n_x}$ is the state vector, $u(k) \in \mathbb{R}^{n_u}$ is the control input, $w(k) \in \mathbb{R}^{n_w}$ is the exogenous disturbance with finite energy (i.e., $w \in \ell_2^{n_w}[0,\infty)$), and $y(k) \in \mathbb{R}^{n_y}$ is the output vector at the time instant k. The matrices $A(\alpha) \in \mathbb{R}^{n_x \times n_x}$, $B_u(\alpha) \in \mathbb{R}^{n_x \times n_u}$, $B_w(\alpha) \in \mathbb{R}^{n_x \times n_w}$, $C(\alpha) \in \mathbb{R}^{n_y \times n_x}$, $D_u(\alpha) \in \mathbb{R}^{n_y \times n_u}$, and $D_w(\alpha) \in \mathbb{R}^{n_y \times n_w}$ as in (3.1) belong to a polytopic domain with V vertices as presented in Section 2.1 with (2.2).

The general packet-based control law utilized (based on what was described in Subsection 2.2.1) is as follows:

$$u(k_t + r) = K_r x(k_t). \tag{3.2}$$

The closed-loop system dynamics under attack will be derived from the approach in Section 2.2, based on the deterministic Assumption 2.1 and with the attacks operating as in Figure 2.1. This way, applying (3.2) to (3.1) yields the following cases between switching points:

- Case 0: DoS-free

$$\begin{aligned} & x(k_t+1) = \left(A(\alpha) + B_u(\alpha)K_0\right) x(k_t) + B_w(\alpha)w(k_t), \\ & \rightarrow x(k_{t+1}) = x(k_t+1) = F_0(\alpha)x(k_t) + B_0(\alpha)\tilde{w}(k_t), \end{aligned} \tag{3.3}$$

$$F_0(\alpha) = A(\alpha) + B_u(\alpha)K_0,$$

$$B_0(\alpha) \triangleq \left[B_w(\alpha)\right], \quad \tilde{w}(k_t) = \left[w(k_t)\right]. \tag{3.4}$$

- Case 1: One time instant is jammed by DoS attacks. $x(k_t+1)$ as in Case 0 and

$$\begin{aligned} &x(k_t+2) = A(\alpha)x(k_t+1) + B_u(\alpha)K_1x(k_t) + B_w(\alpha)w(k_t+1),\\ &\rightarrow x(k_{t+1}) = x(k_t+2) = F_1(\alpha)x(k_t) + B_1(\alpha)\tilde{w}(k_t),\\ &F_1(\alpha) \triangleq A(\alpha)F_0(\alpha) + B_u(\alpha)K_1, \end{aligned} \tag{3.5}$$

$$B_1(\alpha) \triangleq \begin{bmatrix} A(\alpha)B_w(\alpha) & B_w(\alpha) \end{bmatrix}, \quad \tilde{w}(k_t) = \begin{bmatrix} w(k_t) \\ w(k_t+1) \end{bmatrix}. \tag{3.6}$$

- Case N: N time instants jammed by DoS attacks. $x(k_t+1)$ as in Case 0, $x(k_t+2)$ as in Case 1 and

$$\begin{aligned} &x(k_t+N+1) = A(\alpha)x(k_t+N) + B_u(\alpha)K_Nx(k_t) + B_w(\alpha)w(k_t+N),\\ &\rightarrow x(k_{t+1}) = x(k_t+N+1) = F_N(\alpha)x(k_t) + B_N(\alpha)\tilde{w}(k_t),\\ &F_N(\alpha) \triangleq A(\alpha)F_{N-1}(\alpha) + B_u(\alpha)K_N, \end{aligned} \tag{3.7}$$

with

$$B_N(\alpha) \triangleq \begin{bmatrix} \Phi_N & \Phi_{N-1} & \dots & \Phi_0 \end{bmatrix}, \quad \Phi_0 = B_w(\alpha), \tag{3.8}$$

$$\Phi_j = A^j(\alpha)B_w(\alpha), \quad j = 1, 2, \dots, N, \tag{3.9}$$

$$\tilde{w}(k_t) = \begin{bmatrix} w(k_t) \\ w(k_t+1) \\ \vdots \\ w(k_t+N) \end{bmatrix}.$$

Matrices $C(\alpha)$ and $D_u(\alpha)$ remain the same during all cases. To match the matrix $D_w(\alpha)$ dimensions to the augmented vector $\tilde{w}(k_t)$, the following is established:

- Case 0: DoS-free

$$D_0(\alpha) = \begin{bmatrix} D_w(\alpha) \end{bmatrix}. \tag{3.10}$$

- Case 1: One time instant is jammed by DoS attacks

$$D_1(\alpha) = \begin{bmatrix} D_w(\alpha) & 0_{n_y \times n_w} \end{bmatrix}. \tag{3.11}$$

- Case N: N time instants jammed by DoS attacks

$$D_N(\alpha) = \begin{bmatrix} D_w(\alpha) & 0_{n_y \times n_w} & \dots & 0_{n_y \times n_w} \end{bmatrix} = \begin{bmatrix} D_w(\alpha) & 0_{n_y \times Nn_w} \end{bmatrix}. \tag{3.12}$$

Remark 3.1

To simplify the notation, hereafter the term (α) will be omitted from the matrices F_i, B_i and D_i, for $i = 0, 1, \ldots, N$.

Combining the $N+1$ modes from (3.3)-(3.7) with the output assumptions, and the matrices from (3.10)-(3.12), the system dynamics can be depicted by the following switched system:

$$\begin{aligned} x(k_{t+1}) &= F_{\kappa(k_t)}x(k_t) + B_{\kappa(k_t)}\tilde{w}(k_t), \\ y(k_t) &= \left(C(\alpha) + D_u(\alpha)K_{\kappa(k_t)}\right)x(k_t) + D_{\kappa(k_t)}\tilde{w}(k_t), \end{aligned} \tag{3.13}$$

where the time-varying switching signal $\kappa(k_t)$ utilizes values from the set $\mathbb{H} \triangleq \{0, 1, \ldots, N\}$. Utilizing the indicator function (2.8) to represent that only a single mode is active at a time, (3.13) is rewritten as

$$\begin{aligned} x(k_{t+1}) &= F(\zeta(k_t))x(k_t) + B(\zeta(k_t))\tilde{w}(k_t), \\ y(k_t) &= \left(C(\alpha) + D_u(\alpha)K(\zeta(k_t))\right)x(k_t) + D(\zeta(k_t))\tilde{w}(k_t), \end{aligned} \tag{3.14}$$

where the matrices $F(\zeta(k_t))$, $B(\zeta(k_t))$, $K(\zeta(k_t))$, and $D(\zeta(k_t))$ can be generically written as

$$M(\zeta(k_t), \alpha) = \zeta_0(k_t)M_0(\alpha) + \zeta_1(k_t)M_1(\alpha) + \cdots + \zeta_N(k_t)M_N(\alpha).$$

3.1.1 $\mathscr{H}_2$ *definition*

The packet-based control strategy proposed in this chapter aims to guarantee asymptotic stability to (3.14) when $\tilde{w}(k_t) = 0$ while minimizing the $\mathscr{H}_2$ cost when $\tilde{w}(k_t) \neq 0$.

In [72], the different definitions for the $\mathscr{H}_2$ norm are discussed in the context of Linear Time-Varying systems. It settles for the following definition, which will be adapted to switched systems and utilized in this chapter:

Definition 3.1

The infinite horizon $\mathscr{H}_2$ performance of the discrete-time uncertain switched system (3.14) is defined by

$$\|\mathscr{H}_2\|^2 := \limsup_{T\to\infty} \mathscr{E}\left\{\frac{1}{\mathbf{T}}\sum_{k=0}^{\mathbf{T}} y(k)^T y(k)\right\},$$

where $y(k)$ is the system output when applied an input $w(k)$ consisting of a zero-mean white noise Gaussian process with identity covariance matrix and the positive integer $\mathbf{T}$ is the time horizon.

This definition allows bounding the $\mathscr{H}_2$ performance through conditions derived from the Controllability and Observability Gramians. Based on the former, the following Lemma is proposed, as an adaptation of [72, Theorem 2].

Lemma 3.1

If there exist symmetric positive definite matrices $P_i(\alpha) \in \mathbb{R}^{n_x \times n_x}$ and $Q(\alpha) \in \mathbb{R}^{n_y \times n_y}$ such that

$$\begin{bmatrix} Q(\alpha) - D(\zeta(k_t))D(\zeta(k_t))^T & (C(\alpha) + D_u(\alpha)K(\zeta(k_t)))\, P(\zeta(k_t), \alpha) \\ \star & P(\zeta(k_t), \alpha) \end{bmatrix} > 0, \tag{3.15}$$

and

$$\begin{bmatrix} P(\zeta(k_t+1), \alpha) - F(\zeta(k_t))P(\zeta(k_t), \alpha)F(\zeta(k_t))^T & B(\zeta(k_t)) \\ \star & I \end{bmatrix} > 0, \tag{3.16}$$

then the system (3.14) is asymptotically stable when $w = 0$ and

$$Tr(Q(\alpha)) \leq \gamma, \tag{3.17}$$

with $\mathscr{H}_2$ cost being bounded by $\sqrt{\gamma}$ for non-null $w \in \ell_2^{n_w}$ signals, and for all $\alpha \in \Lambda_V$.

Proof. The proof of this Lemma follows the same lines as the proof found in [72] when considering a switched uncertain system. □

3.2 MAIN RESULTS

In this section, the conditions to design a packet-based state-feedback control strategy that aims to minimize the $\mathscr{H}_2$ cost (as depicted by Lemma 3.1) of closed-loop (3.14) are described. A switched parameter-dependent Lyapunov function is utilized. For clarity's sake, a particular case considering a maximum DoS attack duration of $N = 1$ (i.e., $\mathbb{H} \triangleq \{0, 1\}$) is presented in the following Lemma.

Lemma 3.2

If there exist symmetric positive definite matrices $P_i(\alpha) \in \mathbb{R}^{n_x \times n_x}$, $Q(\alpha) \in \mathbb{R}^{n_y \times n_y}$, matrices $X \in \mathbb{R}^{n_x \times n_x}$ and $Z_i \in \mathbb{R}^{n_u \times n_x}$, and the scalar γ such that

$$min\ \gamma, \tag{3.18}$$

$$Tr(Q(\alpha)) < \gamma, \tag{3.19}$$

$$\begin{bmatrix} Q(\alpha) - D_0 D_0^T & C(\alpha)X + D_u(\alpha)Z_0 \\ \star & X + X^T - P_0(\alpha) \end{bmatrix} > 0, \tag{3.20}$$

$$\begin{bmatrix} Q(\alpha) - D_1 D_1^T & C(\alpha)X + D_u(\alpha)Z_1 \\ \star & X + X^T - P_1(\alpha) \end{bmatrix} > 0, \tag{3.21}$$

$$\begin{bmatrix} P_j(\alpha) & \Gamma_0 & B_0 \\ \star & X + X^T - P_0(\alpha) & 0_{n_x \times n_w} \\ \star & \star & I_{n_w} \end{bmatrix} > 0, \tag{3.22}$$

$$\begin{bmatrix} P_j(\alpha) & \Gamma_1 & B_1 \\ \star & X + X^T - P_1(\alpha) & 0_{n_x \times 2n_w} \\ \star & \star & I_{2n_w} \end{bmatrix} > 0, \tag{3.23}$$

where,

$$\Gamma_0 = A(\alpha)X + B_u(\alpha)Z_0,$$

$$\Gamma_1 = A^2(\alpha)X + A(\alpha)B_u(\alpha)Z_0 + B_u(\alpha)Z_1,$$

with $i, j \in \mathbb{H}$, $\mathbb{H} \in \{0, 1\}$, then $K_0 = Z_0 X^{-1}$, $K_1 = Z_1 X^{-1}$ are the state-feedback gains of control law (3.2) that assure the closed-loop system (3.14) (with $N = 1$ and $F_0(\alpha)$ and $F_1(\alpha)$ as in (3.3)-(3.5), B_0 and B_1 as in (3.4)-(3.6), and D_0 and D_1 as in (3.10)-(3.11)) is asymptotically stable for all $\alpha \in \Lambda_V$ when $w = 0$ and whose $\mathscr{H}_2$ cost is bounded by $\sqrt{\gamma}$ for non-null $w \in \ell_2^{n_w}$ signals.

Proof. Departing from the relation

$$(X - P_i(\alpha))^T P_i(\alpha)^{-1} (X - P_i(\alpha)) = X^T P_i(\alpha) X - X - X^T + P_i(\alpha) > 0, \tag{3.24}$$

one has

$$X^T P_i(\alpha)^{-1} X > X + X^T - P_i(\alpha). \tag{3.25}$$

Setting $Z_0 = K_0 X$ and $Z_1 = K_1 X$, and applying relation (3.25), the conditions (3.20)-(3.21) yield

$$\begin{bmatrix} Q(\alpha) - D_0 D_0^T & (C(\alpha) + D_u(\alpha)K_0)\, X \\ \star & X^T P_0(\alpha)^{-1} X \end{bmatrix} > 0, \tag{3.26}$$

$$\begin{bmatrix} Q(\alpha) - D_1 D_1^T & (C(\alpha) + D_u(\alpha)K_1)\, X \\ \star & X^T P_1(\alpha)^{-1} X \end{bmatrix} > 0, \tag{3.27}$$

Pre and post-multiplying (3.26) by $\mathscr{M}_0^T = diag(I_{n_y}, P_0(\alpha)X^{-T})$ and its transpose, and (3.27) by $\mathscr{M}_1^T = diag(I_{n_y}, P_1(\alpha)X^{-T})$ and its transpose results in

$$\begin{bmatrix} Q(\alpha) - D_0 D_0^T & (C(\alpha) + D_u(\alpha)K_0)\, P_0(\alpha) \\ \star & P_0(\alpha) \end{bmatrix} > 0, \tag{3.28}$$

$$\begin{bmatrix} Q(\alpha) - D_1 D_1^T & (C(\alpha) + D_u(\alpha)K_1)\, P_1(\alpha) \\ \star & P_1(\alpha) \end{bmatrix} > 0. \tag{3.29}$$

Multiplying (3.28) by $\zeta_0(k_t)^2$ and (3.29) by $\zeta_1(k_t)^2$ and summing up the results, one has

$$\begin{bmatrix} Q(\alpha) - D(\zeta(k_t))D(\zeta(k_t))^T & (C(\alpha) + D_u(\alpha)K(\zeta(k_t)))\, P(\zeta(k_t), \alpha) \\ \star & P(\zeta(k_t), \alpha) \end{bmatrix} > 0, \tag{3.30}$$

which is equivalent to condition (3.15) in Lemma 3.1. The square of the $\mathscr{H}_2$ norm is then bounded by the trace of matrix $Q(\alpha)$, which, in turn, is bounded by the scalar γ. Thus, introducing the optimization problem of minimizing γ assures that one finds the minimum bound for the $\mathscr{H}_2$ performance that still ensures feasible solutions.

Moreover, departing from (3.22) and (3.23), setting $Z_0 = K_0 X$ and $Z_1 = K_1 X$ and utilizing relation (3.25), results in

$$\begin{bmatrix} P_j(\alpha) & F_0 X & B_0 \\ \star & X^T P_0(\alpha)^{-1} X & 0_{n_x \times n_w} \\ \star & \star & I_{n_w} \end{bmatrix} > 0, \tag{3.31}$$

$$\begin{bmatrix} P_j(\alpha) & F_1 X & B_1 \\ \star & X^T P_1(\alpha)^{-1} X & 0_{n_x \times 2n_w} \\ \star & \star & I_{2n_w} \end{bmatrix} > 0. \tag{3.32}$$

Pre and post-multiplying (3.31) by $\mathscr{R}_0^T = diag(I_{n_x}, P_0(\alpha)X^{-T}, I_{n_w})$ and its transpose, and (3.32) by $\mathscr{R}_1^T = diag(I_{n_x}, P_1(\alpha)X^{-T}, I_{2n_w})$ and its transpose yields

$$\begin{bmatrix} P_j(\alpha) & F_0 P_0(\alpha) & B_0 \\ \star & P_0(\alpha) & 0_{n_x \times n_w} \\ \star & \star & I_{n_w} \end{bmatrix} > 0, \tag{3.33}$$

$$\begin{bmatrix} P_j(\alpha) & F_1 P_1(\alpha) & B_1 \\ \star & P_1(\alpha) & 0_{n_x \times 2n_w} \\ \star & \star & I_{2n_w} \end{bmatrix} > 0. \tag{3.34}$$

Multiplying (3.33) by $\zeta_0(k_t)^2$ and (3.34) by $\zeta_1(k_t)^2$, and summing up the results gives

$$\begin{bmatrix} P_j(\alpha) & F(\zeta(k_t))P(\zeta(k_t),\alpha) & B(\zeta(k_t)) \\ \star & P(\zeta(k_t),\alpha) & 0 \\ \star & \star & I \end{bmatrix} > 0. \tag{3.35}$$

Making the same procedure, multiplying (3.35) by $\zeta_j(k_t+1)^2$, for $j = 0, 1$ and summing the results up yields

$$\begin{bmatrix} P(\zeta(k_t+1),\alpha) & F(\zeta(k_t))P(\zeta(k_t),\alpha) & B(\zeta(k_t)) \\ \star & P(\zeta(k_t),\alpha) & 0 \\ \star & \star & I \end{bmatrix} > 0. \tag{3.36}$$

Applying Schur's complement lemma results in

$$\begin{bmatrix} P(\zeta(k_t+1),\alpha) - F(\zeta(k_t))P(\zeta(k_t),\alpha)F(\zeta(k_t))^T & B(\zeta(k_t)) \\ \star & I \end{bmatrix} > 0, \tag{3.37}$$

which is equivalent to (3.16) from Lemma 3.1. This concludes the proof. □

In the sequel, the general case considering a maximum of N consecutive DoS attacks is presented.

Theorem 3.1

If there exist symmetric positive definite matrices $P_i(\alpha) \in \mathbb{R}^{n_x \times n_x}$, $Q(\alpha) \in \mathbb{R}^{n_y \times n_y}$, matrices $X \in \mathbb{R}^{n_x \times n_x}$ and $Z_i \in \mathbb{R}^{n_u \times n_x}$, and the scalar γ such that

$$min\ \gamma, \tag{3.38}$$

$$Tr(Q(\alpha)) < \gamma, \tag{3.39}$$

$$\begin{bmatrix} Q(\alpha) - D_i D_i^T & C(\alpha)X + D_u(\alpha)Z_i \\ \star & X + X^T - P_i(\alpha) \end{bmatrix} > 0, \tag{3.40}$$

$$\begin{bmatrix} P_j(\alpha) & \Gamma_i & B_i \\ \star & X + X^T - P_i(\alpha) & 0_{n_x \times (i+1)n_w} \\ \star & \star & I_{(i+1)n_w} \end{bmatrix} > 0, \tag{3.41}$$

where,

$$\Gamma_i = A^{i+1}(\alpha)X + \sum_{h=0}^{i} A^{i-h}(\alpha)B(\alpha)Z_h, \tag{3.42}$$

with $i, j \in \mathbb{H}, \mathbb{H} \triangleq \{0, 1, \ldots, N\}$, where $A^0(\alpha) = I_{n_x}$, B_i as in (3.8)-(3.9) and D_i as in (3.10)-(3.12), then $K_i = Z_i X^{-1}$ are the state-feedback gains of control law (3.2) that assure the closed-loop system (3.14) (with $F_i(\alpha)$ as in (3.3)-(3.7)) is asymptotically stable for all $\alpha \in \Lambda_V$ when $w = 0$ and whose $\mathscr{H}_2$ cost is bounded by $\sqrt{\gamma}$ for non-null $w \in \ell_2^{n_w}$ signals.

Proof. The same steps pursued in the proof presented for Lemma 3.2 can be used in the proof of Theorem 3.1. Therefore, they shall not be repeated. □

Theorem 3.1 presents the full packet strategy. In the sequel, the conditions to consider the hold and zero-input strategies (as described in Subsection 2.2.1) in Theorem 3.1 are respectively presented. Note that their proofs follow the same lines as the proof for Theorem 3.1.

Corollary 3.1

If there exist symmetric positive definite matrices $P_i(\alpha) \in \mathbb{R}^{n_x \times n_x}$, $Q(\alpha) \in \mathbb{R}^{n_y \times n_y}$, matrices $X \in \mathbb{R}^{n_x \times n_x}$, $Z_0 \in \mathbb{R}^{n_u \times n_x}$ and $Z_l = Z_0$ for $l = 1, \ldots, N$, and the scalar γ such that (3.38)-(3.41) then $K_i = Z_i X^{-1}$ for $i \in \mathbb{H}$, $\mathbb{H} \in \{0, 1, \ldots, N\}$ are the state-feedback gains using the hold-input strategy that assure the closed-loop system (3.14) (with $F_i(\alpha)$ as in (3.3)-(3.7)) is asymptotically stable for all $\alpha \in \Lambda_V$ when $w = 0$ and whose $\mathscr{H}_2$ cost is bounded by $\sqrt{\gamma}$ for non-null $w \in \ell_2^{n_w}$ signals.

Corollary 3.2

If there exist symmetric positive definite matrices $P_i(\alpha) \in \mathbb{R}^{n_x \times n_x}$ $Q(\alpha) \in \mathbb{R}^{n_y \times n_y}$, matrices $X \in \mathbb{R}^{n_x \times n_x}$, $Z_0 \in \mathbb{R}^{n_u \times n_x}$ and $Z_l = 0_{n_y \times n_x}$ for $l = 1, \ldots, N$, and the scalar γ such that (3.38)-(3.41) then $K_i = Z_i X^{-1}$ for $i \in \mathbb{H}$, $\mathbb{H} \in \{0, 1, \ldots, N\}$ are the state-feedback gains using the zero-input strategy that assure the closed-loop system (3.14) (with $F_i(\alpha)$ as in (3.3)-(3.7)) is asymptotically stable for all $\alpha \in \Lambda_V$ when $w = 0$ and whose $\mathscr{H}_2$ cost is bounded by $\sqrt{\gamma}$ for non-null $w \in \ell_2^{n_w}$ signals.

Remark 3.2

The number of scalar decision variables employed by Theorem 3.1 (NV_{T1}), Corollary 3.1 (NV_{hold}) and Corollary 3.2 (NV_{zero}) are calculated as follows:

$$NV_{T1} = n_x^2 + V\frac{n_y^2 + n_y}{2} + (N+1)(V\frac{n_x^2 + n_x}{2} + n_u n_x) + 1,$$

$$NV_{hold} = NV_{zero} = n_x^2 + V\frac{n_y^2 + n_y}{2} + (N+1)V\frac{n_x^2 + n_x}{2} + n_u n_x + 1.$$

3.3 NUMERICAL EXAMPLES

Two numerical examples are presented to illustrate the proposed method's performance. The parameter-dependent Linear Matrix Inequalities (LMIs) are written using MATLAB with the parsers YALMIP [105], ROLMIP [83] and the solver MOSEK [106]. The three strategies: full packet, hold-input, and zero-input are compared on what concerns the utilized $\mathscr{H}_2$ performance criterion.

3.3.1 *Example 1:*

Consider the following discrete-time uncertain CPS borrowed and adapted from [107]:

$$A_1 = \begin{bmatrix} 0.9813 & 0.3420 & 1.3986 \\ 0.0052 & 0.9840 & -0.1656 \\ 0 & 0 & 0.5488 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0.9872 & 0.3575 & 1.2273 \\ 0.0016 & 0.9872 & -0.1603 \\ 0 & 0 & 0.5488 \end{bmatrix},$$

$$A_3 = \begin{bmatrix} 0.9687 & 0.9840 & 3.6304 \\ 0.0043 & 0.9742 & -0.4647 \\ 0 & 0 & 0.5488 \end{bmatrix}, \quad A_4 = \begin{bmatrix} 0.9857 & 0.5881 & 2.5226 \\ -0.0135 & 0.9717 & -0.4702 \\ 0 & 0 & 0.5488 \end{bmatrix},$$

$$[B_{u1} \mid B_{u2} \mid B_{u3} \mid B_{u4}] = \left[\begin{array}{c|c|c|c} -1.4700 & -4.999 & -0.4376 & -1.4700 \\ -0.0604 & -0.0576 & -0.1589 & -0.0604 \\ 0.4512 & 0.4512 & 0.4512 & 0.4512 \end{array}\right],$$

$$B_{w1} = \begin{bmatrix} 0.0198 & 0.0034 & 0.0156 \\ 0.0001 & 0.0198 & -0.0018 \\ 0 & 0 & 0.0150 \end{bmatrix}, \quad B_{w2} = \begin{bmatrix} 0.0199 & 0.0036 & 0.0137 \\ 0.0000 & 0.0199 & -0.0018 \\ 0 & 0 & 0.0150 \end{bmatrix},$$

$$B_{w3} = \begin{bmatrix} 0.0197 & 0.0099 & 0.0412 \\ 0.0000 & 0.0197 & -0.0052 \\ 0 & 0 & 0.0150 \end{bmatrix}, \quad B_{w4} = \begin{bmatrix} 0.0199 & 0.0059 & 0.0284 \\ -0.0001 & 0.0197 & -0.0051 \\ 0 & 0 & 0.0150 \end{bmatrix},$$

$$C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad D_u = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad D_w = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

The presented strategies were tested in function of N, with $N = 0$ up until $N = 9$. Figure 3.1 illustrates the $\mathscr{H}_2$ cost obtained, which is bounded by $\sqrt{\gamma}$, for the full packet (—) (Theorem 3.1), zero-input (– – –) (Corollary 3.2) and hold strategies (· · ·) (Corollary 3.2) in function of the N considered in the design. It can be seen that for all strategies the higher the value of the integer N, that is, the longer the maximum attack taken into account, the higher the $\mathscr{H}_2$ cost. It is also evident that the full packet strategy presented the best results, while the hold and zero-input strategies provided similar results, with the zero-input strategy being more effective for higher numbers of N than the hold-input strategy.

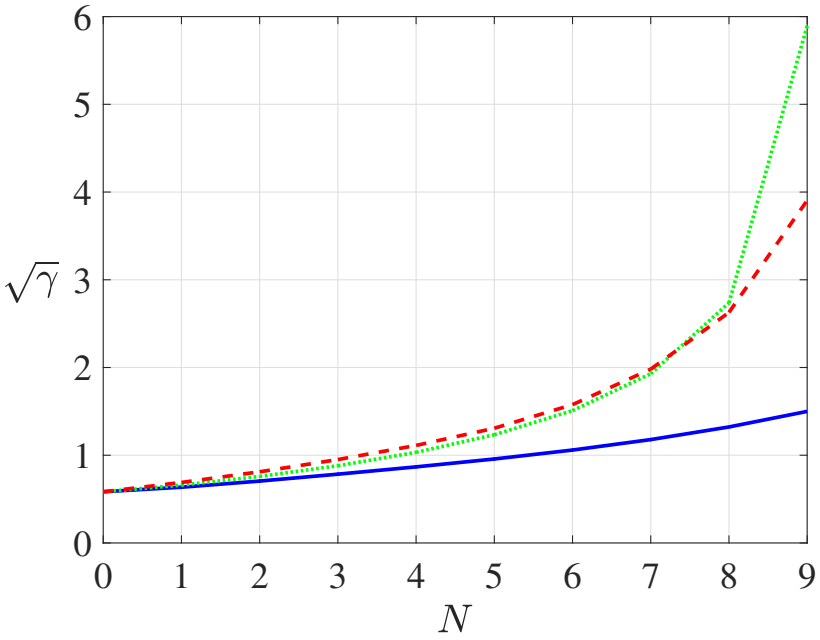

Figure 3.1: $\sqrt{\gamma}$ bounds for the $\mathscr{H}_2$ cost for Example 1, as a function of N, obtained with controllers designed by: Full Packet (—), Zero-input (– – –), and Hold Strategy (· · ·).

Moreover, Table 3.1 displays the number of scalar decision variables required in the design of the three strategies, in function of N. The increase of the integer N results in the need for a higher number of decision variables, which translates into a problem of higher complexity that needs to be solved. Among the three strategies, the full packet strategy required the highest number of decision variables, while the hold and zero-input strategies required the same number. This depicts that the full packet strategy displays a trade-off between better performance and higher computational complexity.

Table 3.1: Number of scalar decision variables (NV) for the different strategies and percentage difference between the full packet strategy and the rest.

N	Theorem 3.1	Corollary 3.2	Corollary 3.1	Percentage difference
1	76	73	73	+3.94%
2	103	97	97	+5.82%
3	130	121	121	+6.92%
4	157	145	145	+7.64%
5	184	169	169	+8.15%
6	211	193	193	+8.53%
7	238	217	217	+8.82%
8	265	241	241	+9.05%
9	292	265	265	+9.24%

3.3.2 *Example 2:*

Consider the following system proposed in [108, 109], which was discretized and analysed with the $\mathscr{H}_2$ cost in [110]. It consists of a satellite system composed of two rigid bodies connected by a flexible link with uncertain torque constants and viscous damping. The parameters range, respectively, between $e \in \begin{bmatrix} 0.09 & 0.4 \end{bmatrix}$ and $f \in \begin{bmatrix} 0.0038 & 0.04 \end{bmatrix}$. The state-space representation of the system is as follows:

$$x(k+1) = \begin{bmatrix} 1 & 0 & 0.1 & 0 \\ 0 & 1 & 0 & 0.1 \\ -0.1e & 0.1e & 1-0.1e & 0.1f \\ 0.1e & -0.1e & 0.1f & 1-0.1f \end{bmatrix} x(k) + \begin{bmatrix} 0 \\ 0 \\ 0.1 \\ 0 \end{bmatrix} u(k) + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0.1 \end{bmatrix} w(k),$$

$$y(k) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} x(k) + \begin{bmatrix} 0 \\ 0.01 \end{bmatrix} u(k) + \begin{bmatrix} 0 \\ 0 \end{bmatrix} w(k).$$

The system was tested with the strategies featured in Theorem 3.1, Corollary 3.1, and Corollary 3.2. Results considering $N = 0$ up to $N = 9$ were obtained, and the guaranteed $\mathscr{H}_2$ cost is depicted in Table 3.2. The full packet strategy of Theorem 3.1 presented the best results among the three strategies for all the values of N, and the zero-input strategy appears to perform better than the hold-input strategy when considering longer consecutive attacks. Moreover, it is worthy of note that considering no attacks i.e., $N = 0$ presents the same cost as the method in [111].

In the sequel, the designed controllers were tested in time-based simulations. The value of α was randomly selected and null initial conditions were considered. An energy-limited exogenous disturbance consisting of a 0 dBW Gaussian noise signal with a variance of 1.1099 was created. The same disturbance vector was applied during the interval $k \in [0, 100]$ in the examples depicted in the sequel, in order to compare each strategy's performance. Firstly, the controllers designed

Table 3.2: $\mathscr{H}_2$ cost with the different strategies for Example 2 in function of N

N	Theorem 3.1	Corollary 3.1	Corollary 3.2
0	0.7538	0.7538	0.7538
1	0.8279	0.8416	0.9557
2	0.9267	0.9847	1.1300
3	1.0400	1.1973	1.1294
4	1.1614	1.4758	1.4560
5	1.2895	1.7789	1.6198
6	1.4177	2.0669	1.7850
7	1.5428	2.3170	1.9506
8	1.6630	2.5232	2.1151
9	1.7666	2.6914	2.5295

for $N = 2$ were tested for the worst-case scenario of $\kappa(k_t) = \{2, 2, 2, \dots\}$. Figure 3.2 depicts the system's first output under the three strategies.

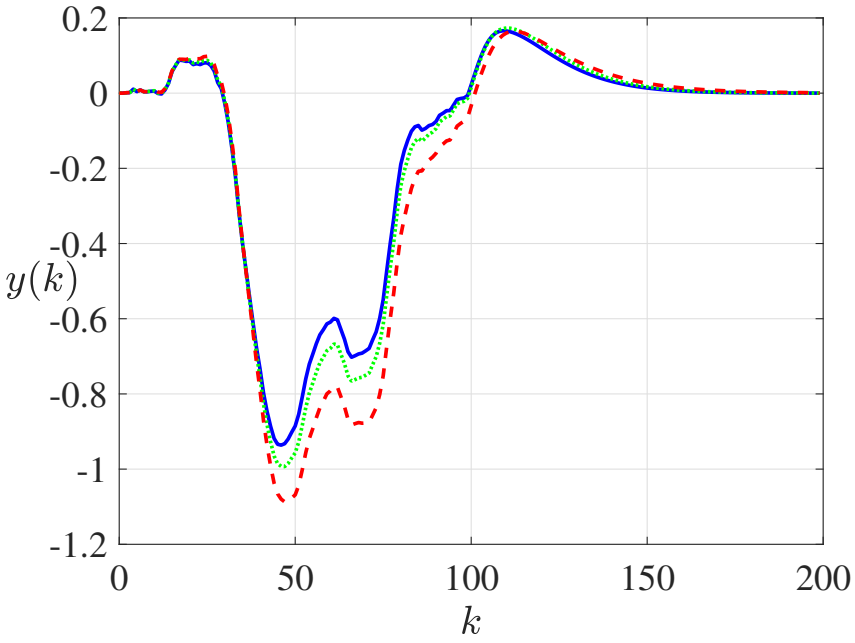

Figure 3.2: System output with control strategies considering $N = 2$: Full Packet (—), Zero-input (– – –), and Hold Strategy (· · ·). Initial conditions are $x_0 = [0\ 0\ 0\ 0]^T$ and $\alpha = [0.2258\ 0.3709\ 0.1502\ 0.2531]$. Attack sequence is $\kappa(k_t) = \{2,\ 2,\ 2,\ \dots\}$.

Then, the design considering $N = 9$ for the three strategies is taken into account to analyze the impact of longer attack sequences on the system performance. Once more, the worst-case scenario is contemplated as in $\kappa(k_t) = \{9, 9, 9, \dots\}$. The time-based simulations are depicted in Figure 3.3.

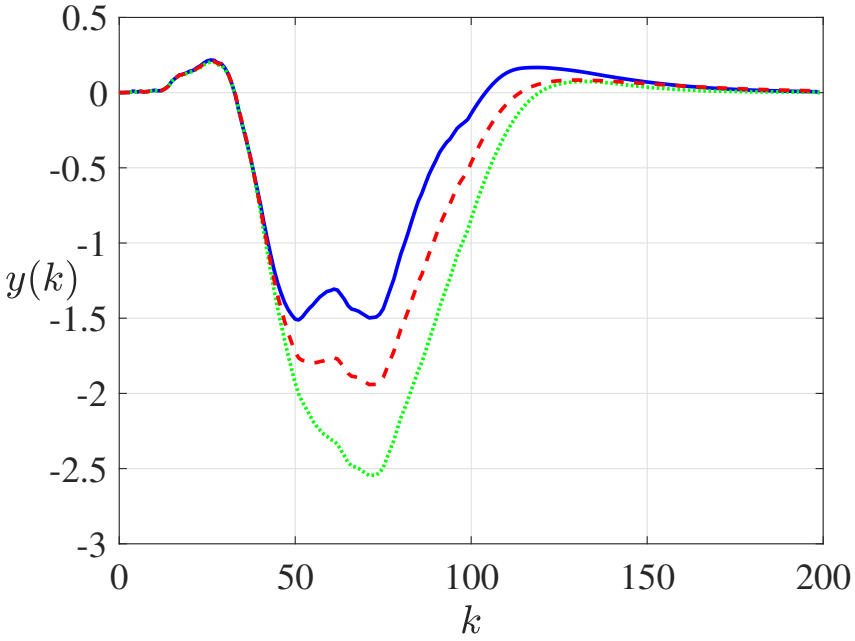

Figure 3.3: System output with control strategies considering $N = 9$: Full Packet (—), Zero-input (– – –), and Hold Strategy (· · ·). Initial conditions are $x_0 = [0\ 0\ 0\ 0]^T$ and $\alpha = [0.2258\ 0.3709\ 0.1502\ 0.2531]$. Attack sequence is $\kappa(k_t) = \{9,\ 9,\ 9,\ \ldots\}$.

The time-based simulations showed that all of the strategies were able to stabilize the system, even with the presence of energy-limited disturbances and DoS attacks. In both Figure 3.2 and Figure 3.3 the full packet strategy of Theorem 3.1 provided the best results in comparison to the other strategies. This could be evidenced by the smaller oscillation caused by the exogenous disturbance signal. In Figure 3.2 hold-input performed better than the zero-input strategy, while in Figure 3.3 the opposite is depicted. This is corroborated by Table 3.2, and somewhat in accordance with what was seen in Example 1, on what concerns the zero-input strategy performing better than the hold-input for higher values of N. However, further studies are required to make this an affirmative, as the zero-input strategy depends upon the open-loop dynamics of the approached system.

The presence of the overshoot in the response is expected, as minimizing the $\mathscr{H}_2$ cost aims to reduce the average magnitude of the response, and not necessarily its maximum magnitude. Considering a mixed $\mathscr{H}_\infty/\mathscr{H}_2$ control technique might reduce said overshoot while keeping a lower average response, but this is beyond the scope of this chapter.

To obtain a more general view of the controller performance, 10000 time-based simulations were conducted with distinct disturbance vectors generated following the aforementioned procedure. A new set α was also randomly selected at the beginning of each new simulation. The scenario and controllers for $N = 9$ were taken into account, and the average output with a range of one standard deviation is featured in Figure 3.4. Once more, it can be seen that the full packet strategy was the best candidate to mitigate the influence of the exogenous disturbance, even when accounting for a wider range of scenarios. Moreover, in accordance with Table 3.2, the hold-input strategy performed more poorly than the zero-input.

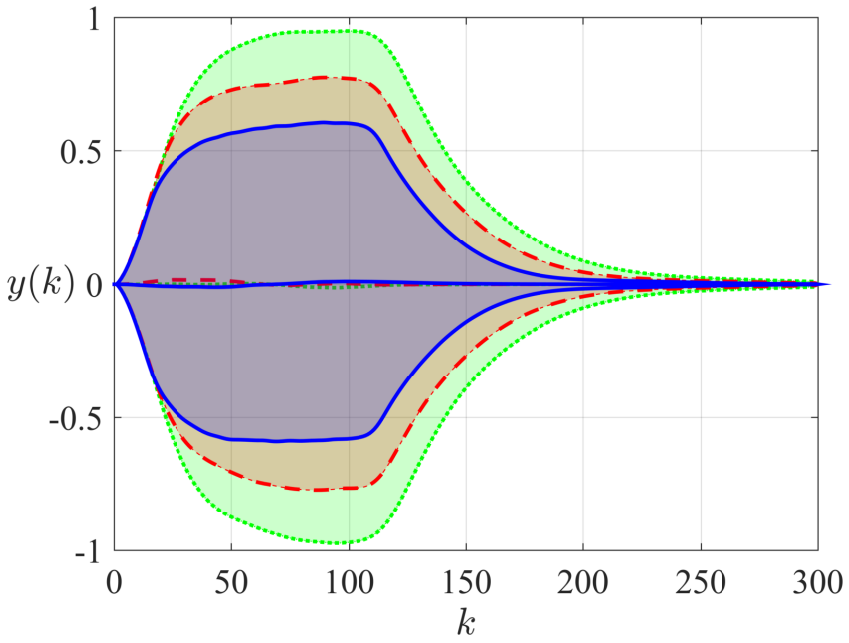

Figure 3.4: Mean system output with one standard deviation of 10000 time-based simulations with the control strategies considering $N = 9$: Full Packet (—), Zero-input (– – –), and Hold Strategy (· · ·). Initial conditions are $x_0 = [0\ 0\ 0\ 0]^T$. Attack sequence is $\kappa(k_t) = \{9,\ 9,\ 9,\ \ldots\}$. A new set of α and a new exogenous disturbance vector w with duration $k \in [0, 100]$ was randomly selected at the start of each time-based simulation.

3.4 FINAL REMARKS

This chapter presented design conditions for a packet-based state-feedback control for discrete-time uncertain Cyber-Physical Systems (CPSs) under the presence of energy-limited exogenous disturbances and DoS attacks from an energy-bounded attacker. The full packet strategy was presented as well as adaptations to implement the hold and zero-input strategies. The $\mathscr{H}_2$ cost was considered in the design of the controller and as a performance criterion. The proposed strategies were able to stabilize the system, even under the presence of DoS attacks, and, as shown in Table 3.1 and Table 3.2, the system becomes more difficult to stabilize and the $\mathscr{H}_2$ cost becomes higher as longer consecutive attacks are taken into account. In all of the considered scenarios, the full packet control presented the best performance, when compared to the hold and zero-input strategies.

4

CONTROL DESIGN FOR CYBER-PHYSICAL UNCERTAIN SYSTEMS UNDER UNRELIABLE MARKOVIAN NETWORK SUSCEPTIBLE TO DENIAL-OF-SERVICE ATTACKS

In this chapter, the problem of packet-based state-feedback control for discrete-time Cyber-Physical System (CPS) with time-invariant polytopic uncertainties is tackled. The design conditions will aim to guarantee closed-loop stability even with the system utilizing an unreliable network that may feature packet dropouts due to stochastic network limitations and Denial of Service attacks (DoS attacks) from an energy-bounded attacker. The utilized network model is presented in Section 2.4. Parameter-dependent Linear Matrix Inequalities (LMI) conditions will be proposed with the goal of guaranteeing that the closed-loop system features Exponential stability in the mean square sense with conditioning I (ESMS-CI). Numerical experiments are provided comparing the full packet, hold-input, and zero-input strategies (as depicted in Subsection 2.2.1), as well as comparing the proposed network model with an adapted Gilbert-Elliot model.

4.1 PROBLEM STATEMENT

Consider the following discrete-time uncertain model of the plant of a CPS:

$$x(k+1) = A(\alpha)x(k) + B(\alpha)u_{\theta_k}(k), \tag{4.1}$$

where $x(k) \in \mathbb{R}^{n_x}$ is the state vector and $u_{\theta_k}(k) \in \mathbb{R}^{n_u}$ is the mode-dependent control input vector. The matrices $A(\alpha) \in \mathbb{R}^{n_x \times n_x}$ and $B(\alpha) \in \mathbb{R}^{n_x \times n_u}$ belong to a polytopic domain depending on the vector α of time-invariant parameters, as presented in Section 2.1 with (2.2).

The utilized network model was presented in Section 2.4, with the attacks operating as seen in Figure 2.1. Consider a discrete-time non-homogeneous Markov chain $\{\theta_k; k \geq 0\}$ with a finite state-space $\mathbb{K} = \{1, \ldots, N+2\}$ where N is the maximum number of consecutive DoS attacks, and the mode transition probabilities are as follows

$$p_{ij}(k) = Pr(\theta_{k+1} = j \mid \theta_k = i),$$

which satisfies $p_{ij}(k) \geq 0$ and $\sum_{j=1}^{N+2} p_{ij}(k) = 1,\ \forall k \geq 0$. These mode transition probabilities are all contained in the transition probabilities matrix $\Psi(k) = |p_{ij}(k)|,\ i, j \in \mathbb{K}$. Matrix $\Psi(k)$ features m rows with uncertain or unknown probabilities. The resulting Λ-homogeneous polynomial transition probability matrix $\Psi(\xi_k)$ is defined as follows:

$$\Psi(\xi_k) = \sum_{z=1}^{\psi} \xi_k(z)\Psi_z, \quad \xi_k = (\xi_{k,1}, \ldots, \xi_{k,m}) \in (\Lambda_{Z_1} \times \cdots \times \Lambda_{Z_m}) = \Omega_\psi, \tag{4.2}$$

where $z = 1, 2, \ldots, \psi$, with $\psi = Z_1 Z_2 \ldots Z_m$ vertices and $\xi_k = (\xi_{k,1}, \ldots, \xi_{k,m})$. $\xi_k(z)$ are homogeneous monomials with degree m which are created by the ψ-tuple with all the ψ possible combinations obtained between the sets $\mathscr{K}_1 = \{\xi_{k,11}, \ldots, \xi_{k,1Z_1}\}$ up to $\mathscr{K}_m = \{\xi_{k,m1}, \ldots, \xi_{k,mZ_m}\}$. See Section 2.4.1 for more details.

The mode-dependent control law utilized is as follows:

$$u_{\theta_k}(k) = \delta_{\theta_k} K_{\theta_k} x(k) + (1 - \delta_{\theta_k}) K_{\theta_k} x_l(k-1), \tag{4.3}$$

where $K_{\theta_k} \in \mathbb{R}^{n_u \times n_x}$ is the mode-dependent state feedback gain. A binary variable indicating transmission success or packet loss is defined based on the Markovian network state-space $\mathbb{K} = \{1, \ldots, N+2\}$, and is described by

$$\delta_{\theta_k} = \begin{cases} 1, & \text{if } \theta_k = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{4.4}$$

Noting that $\theta_k = 1$ indicates a successful data transmission. If $\delta_{\theta_k} = 0$, the controller has no access to the current state measurement. It is, then, considered that the controller retains the last transmitted state in its memory, denoted $x_l(k-1)$. Moreover, $x_l(k)$ is updated by the following equation:

$$x_l(k) = \delta_{\theta_k} x(k) + (1 - \delta_{\theta_k}) x_l(k-1). \tag{4.5}$$

By applying the control law (4.3) to system (4.1), the following closed-loop augmented Markov jump linear system (MJLS) can be defined:

$$\eta(k+1) = F(\theta_k, \alpha)\eta(k), \tag{4.6}$$

where $\eta(k) = \begin{bmatrix} x(k)^T & x_l(k-1)^T \end{bmatrix}^T \in \mathbb{R}^{2n_x}$ is the augmented state vector, and

$$F(\theta_k, \alpha) = \begin{bmatrix} A(\alpha) + \delta_{\theta_k} B(\alpha) K_{\theta_k} & (1 - \delta_{\theta_k}) B(\alpha) K_{\theta_k} \\ \delta_{\theta_k} I_{n_x} & (1 - \delta_{\theta_k}) I_{n_x} \end{bmatrix}. \tag{4.7}$$

Note that the augmented system considers the current state measurement and includes the update of the last transmitted measurement in the controller memory. Moreover, the plant parametric uncertainties in function of the time-invariant parameter α do not depend on the Markovian network, while the control law and $x_l(k)$ update rule do. This aspect is what defines the overall augmented system as a MJLS.

The zero-input strategy, in turn, presents itself as a particular case, since it does not require saving the last transmitted state measurement $x_l(k-1)$. This way, the closed-loop system needs not to be augmented and is described by

$$x(k+1) = G(\theta_k, \alpha)x(k), \tag{4.8}$$

where

$$G_i(\theta_k, \alpha) = A(\alpha) + \delta_{\theta_k} B(\alpha) K_{\theta_k}. \tag{4.9}$$

In the approached problem, the packet-based strategy can be employed to guarantee that the actuator will have a different input for each mode, even if the communication channels are unavailable. This strategy can be applied because of Assumption 2.1 that assumes a bounded duration for the existence of attacks. The packet of control inputs is defined by

$$U(K) = \begin{bmatrix} K_1 x(k) & K_2 x(k) & \dots & K_{N+2} x(k) \end{bmatrix}. \tag{4.10}$$

The control inputs of the packet are designed based on the current state measurement. From the actuator viewpoint, however, (4.6) applies, since in the presence of a transmission failure or DoS attack, the utilized control input will be derived from a past measurement, as defined by (4.3) and (4.5).

Remark 4.1

Hereafter in this chapter, the notation $F(\theta_k = i, \alpha) = F_i(\alpha)$ will be employed. The same will apply to every other mode-dependent matrix or parameter.

4.2 MAIN RESULTS

In this section, the design conditions for the mode-dependent state-feedback gains K_i for $i = 1, \dots, N+2$ as in (4.3) through parameter-dependent LMIs are presented. The gains aim to guarantee that (4.6) is ESMS-CI. The design conditions are presented in the following Theorem.

Theorem 4.1

If there exist symmetric positive definite matrices $P_i(\xi_k, \alpha) \in \mathbb{R}^{2n_x \times 2n_x}$, and matrices $W \in \mathbb{R}^{n_x \times n_x}$, $Y \in \mathbb{R}^{n_x \times n_x}$, and $Z_i \in \mathbb{R}^{n_u \times n_x}$ such that

$$\begin{bmatrix} -P_i(\xi_k, \alpha) & \star \\ \Phi_i & P_i^+ - X - X^T \end{bmatrix} < 0, \tag{4.11}$$

with

$$\Phi_i = \begin{bmatrix} A(\alpha)W + \delta_i B(\alpha) Z_i & (1-\delta_i) B(\alpha) Z_i \\ \delta_i W & (1-\delta_i) Y \end{bmatrix}, \tag{4.12}$$

$$\delta_i = \begin{cases} 1, & \text{if } i = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{4.13}$$

$$P_i^+ = \sum_{j=1}^{N+2} p_{ij}(\xi_k) P_j(\xi_{k+1}, \alpha), \tag{4.14}$$

$$X = diag(W, Y), \tag{4.15}$$

then, the gains $K_1 = Z_1 W^{-1}$, and $K_j = Z_j Y^{-1}$ for $j = 2, \ldots, N+2$ guarantee that the closed-loop system (4.6) is ESMS-CI for all $i \in \mathbb{K}$, $(\alpha, \xi_k, \xi_{k+1}) \in \Lambda_V \times \Omega_\psi \times \Omega_\psi$.

Proof. Setting $Z_1 = K_1 W$, and $Z_j = K_j Y$ for $j = \{2, \ldots, N+2\}$, one can write (4.12) as

$$\mathbf{\Phi}_i = \begin{bmatrix} A(\alpha) + \delta_i B(\alpha) K_i & (1-\delta_i) B(\alpha) K_i \\ \delta_i I_{n_x} & (1-\delta_i) I_{n_x} \end{bmatrix} \begin{bmatrix} W & \star \\ 0_{n_x \times n_x} & Y \end{bmatrix}. \tag{4.16}$$

Considering (4.15) and (4.7), it is possible to see that (4.16) is equivalent to $F_i(\alpha) X$. This way, (4.11) may be written as

$$\begin{bmatrix} -P_i(\xi_k, \alpha) & \star \\ F_i(\alpha) X & P_i^+ - X - X^T \end{bmatrix} < 0. \tag{4.17}$$

Pre and post-multiplying (4.17) by $\mathscr{M}^T = diag(X^{-T}, X^{-T})$ and its transpose yields

$$\begin{bmatrix} -X^{-T} P_i(\xi_k, \alpha) X^{-1} & \star \\ X^{-T} F_i(\alpha) & X^{-T} P_i^+ X^{-1} - X^{-T} - X^{-1} \end{bmatrix} < 0. \tag{4.18}$$

Then, pre and post-multiplying (4.18) by $\mathscr{R}^T = \begin{bmatrix} I_{n_x} & F_i(\alpha)^T \end{bmatrix}$ and its transpose gives

$$F_i(\alpha)^T X^{-T} P_i^+ X^{-1} F_i(\alpha) - X^{-T} P_i(\xi_k, \alpha) X^{-1} < 0, \tag{4.19}$$

which, considering P_i^+ as in (4.14), yields the same condition presented by Lemma 2.2 for $V(\xi_k, \alpha, k) = \eta(k)^T X^{-T} P_i(\xi_k, \alpha) X^{-1} \eta(k)$. This concludes the proof. □

The mode-dependent controller just presented departs from Assumption 2.2 that dictates that the system is able to differentiate between packet losses due to network limitations and DoS attacks, as well as having a way to track how many consecutive time instants of attack the network is under. This, however, may not be always possible. A solution would be utilizing a mode-independent control akin to the Hold-input strategy, or employing the Zero-input strategy and rendering the control inputs null whenever the transmission is not successful. On what concern the Hold-input strategy, the design conditions are depicted in Corollary 4.1.

Corollary 4.1

If there exist symmetric positive definite matrices $P_i(\xi_k, \alpha) \in \mathbb{R}^{2n_x \times 2n_x}$, and matrices $W \in \mathbb{R}^{n_x \times n_x}$, $Z \in \mathbb{R}^{n_u \times n_x}$, such that (4.11)holds with (4.13)-(4.14) and

$$\Phi_i = \begin{bmatrix} A(\alpha)W + \delta_i B(\alpha)Z & (1-\delta_i)B(\alpha)Z \\ \delta_i W & (1-\delta_i)W \end{bmatrix}, \tag{4.20}$$

$$X = diag(W, W), \tag{4.21}$$

then $K = ZW^{-1}$ for $i \in \mathbb{K}$ is the state-feedback gains using the hold-input strategy that assure the closed-loop system (4.6) is ESMS-CI for all $(\alpha, \xi_k, \xi_{k+1}) \in \Lambda_V \times \Omega_\psi \times \Omega_\psi$.

The proof of Corollary (4.1) follows the same lines as the proof of Theorem 4.1. The equivalent packet of (4.10) utilized by this strategy is

$$U(K) = \begin{bmatrix} Kx(k) & Kx(k) & \dots & Kx(k) \end{bmatrix}. \tag{4.22}$$

The design conditions for the zero-input strategy are presented in the following Corollary:

Corollary 4.2

If there exist symmetric positive definite matrices $P_i(\xi_k, \alpha) \in \mathbb{R}^{n_x \times n_x}$, and matrices $X \in \mathbb{R}^{n_x \times n_x}$, $Z \in \mathbb{R}^{n_u \times n_x}$, such that (4.11) is satisfied with

$$\Phi_i = A(\alpha)X + \delta_i B(\alpha)Z, \tag{4.23}$$

and considering (4.13)-(4.14), then $K = ZX^{-1}$ is the state-feedback gain using the zero-input strategy that assure the closed-loop system (4.8) is ESMS-CI for $i \in \mathbb{K}$, and for all $(\alpha, \xi_k, \xi_{k+1}) \in \Lambda_V \times \Omega_\psi \times \Omega_\psi$.

The proof of this Corollary follows the same steps as in Theorem 4.1, with the appropriated dimensions, by rewriting $K = ZX$, considering (4.8) as the closed-loop system and proceeding from (4.17) onward. The equivalent packet of (4.10) for this strategy is:

$$U(K) = \begin{bmatrix} Kx(k) & 0 & \dots & 0 \end{bmatrix}. \tag{4.24}$$

Remark 4.2

The number of scalar decision variables employed by Theorem 4.1 (NV_{T1}), Corollary 4.1 (NV_{hold}) and Corollary 4.2 (NV_{zero}) is calculated as follows:

$$NV_{T1} = 2(n_x)^2 + (N+2)(V\psi(2n_x^2 + n_x) + n_u n_x),$$

$$NV_{hold} = (n_x)^2 + V\psi(N+2)(2n_x^2 + n_x) + n_u n_x,$$

$$NV_{zero} = (n_x)^2 + V\psi(N+2)\left(\frac{n_x^2 + n_x}{2}\right) + n_u n_x,$$

with ψ as defined by (4.2).

4.3 NUMERICAL EXAMPLES

In this section, numerical experiments will be conducted to test the proposed mode-dependent state-feedback control design technique considering a discrete-time uncertain CPS. The network is unreliable and subjected to DoS attacks, and is modeled as described in Section 2.4 and Figure 2.2. Comparisons between the proposed network model and a classic Gilbert-Elliot model will be conducted. Furthermore, comparisons will be drawn between the use of the full packet, hold, and zero-input strategies. All tests were performed using the parsers YALMIP [105], ROLMIP [112], and the solver MOSEK [106] combined with MATLAB 2016b.

4.3.1 *Example 1:*

Consider the following system borrowed from [40]:

$$A(\alpha) = \alpha_1 \begin{bmatrix} 0.9520 & 0.0936 \\ -0.9358 & 0.8584 \end{bmatrix} + \alpha_2 \lambda \begin{bmatrix} 0.9996 & 0.0824 \\ -0.0082 & 0.6699 \end{bmatrix}, \quad B(\alpha) = \alpha_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

where higher values of λ render the system more difficult to stabilize.

The transition probability matrix is created following (2.11) considering a maximum of $N = 5$ consecutive attacks and $m = 2$ rows with uncertain or unknown probabilities, and is presented in the sequel:

$$\Psi = \begin{bmatrix} 0.5 & c & d & 0 & 0 & 0 & 0 \\ 0.4 & ? & ? & 0 & 0 & 0 & 0 \\ g & 0.05 & 0 & \rho & 0 & 0 & 0 \\ g & 0.05 & 0 & 0 & \rho & 0 & 0 \\ g & 0.05 & 0 & 0 & 0 & \rho & 0 \\ g & 0.05 & 0 & 0 & 0 & 0 & \rho \\ 0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{4.25}$$

where $g = (1 - 0.05 - \rho)$, $c = \begin{bmatrix} 0.05 & 0.15 \end{bmatrix}$ and $d = \begin{bmatrix} 0.35 & 0.45 \end{bmatrix}$. ρ is a parameter that defines if the attacks will be longer. The closer ρ is to 1, the more likely the attacks will persist until completing N consecutive time instants.

The scenario with $N = 5$ described by (4.25) is considered, as well as a scenario with $N = 10$, which can be easily obtained by using the values of rows 3 to 6 of (4.25), extending them in accordance to the positioning defined by (2.11). The value of λ is used to evaluate how conservative both the control strategy and the network model were in function of ρ. Theorem 4.1 is used to design a full packet control strategy, as well as Corollary 4.1 for the hold-input and Corollary 4.2 for the zero-input strategy. The results are displayed in Table 4.1.

	Theorem 4.1		Corollary 4.2	
ρ \ N	5	10	5	10
0.50	1.1156	1.1156	1.1156	1.1156
0.60	1.1056	1.1016	1.1056	1.1016
0.70	1.0850	1.0765	1.0850	1.0765
0.80	1.0649	1.0518	1.0649	1.0518
0.85	1.0551	1.0399	1.0551	1.0399
0.90	1.0457	1.0284	1.0457	1.0284
0.95	1.0367	1.0174	1.0367	1.0174
NV	582	992	174	294

Table 4.1: λ in function of different values of ρ.

The hold-input strategy of Corollary 4.1 did not return any feasible solutions, indicating it to be a far too conservative approach to the addressed problem. As seen in Table 4.1, the increase in the probability of longer attacks renders the system more difficult to stabilize than accounting for higher values of N. In Chapter 3, the use of Full packet control provided better results in comparison to the zero-input strategy on what concerned $\mathscr{H}_2$, however, as seen here, there is evidence that in problems aiming only to stabilize the closed-loop system, using robust full packet controllers shows no advantage in comparison to the zero-input strategy, as they obtained virtually the same results, with the difference laying in the fact that the zero-input required fewer decision variables.

In the sequel, in order to compare how the network model influences how conservative the approach is, an adapted Gilbert-Elliot model will be constructed based on (4.25). To do so, the probabilities of its first row of the transition probability matrix will be utilized to refer to the successful transmission mode, while the second row will have a lower bound according to the second row of (4.1), and an upper bound following the modes 3 to 6. The transition probability matrix will then be modeled with uncertain time-varying probabilities in its second row:

$$\Psi = \begin{bmatrix} 0.5 & 0.5 \\ \begin{bmatrix} 0.4 & (1-\rho-0.05) \end{bmatrix} & \begin{bmatrix} 0.6 & (\rho+0.05) \end{bmatrix} \end{bmatrix}. \tag{4.26}$$

Then, by using (4.26), ρ is increased and the highest feasible value of λ is found in the same approach as in Table 4.1. The value of N is irrelevant since a Gilbert-Elliot model features only two modes. This way, the following are considered to calculate the required number of decision variables when using the Gilbert-Elliot model:

$$NV_{GB,T1} = 2(n_x)^2 + 2(V\psi(2n_x^2 + n_x) + n_u n_x),$$

$$NV_{GB,hold} = (n_x)^2 + 2V\psi 2(2n_x^2 + n_x) + n_u n_x,$$

$$NV_{GB,zero} = (n_x)^2 + 2V\psi\left(\frac{n_x^2 + n_x}{2}\right) + n_u n_x.$$

The results are then featured in Table 4.2. The Hold-input strategy returned no feasible solutions.

ρ	Theorem 4.1	Corollary 4.2
0.50	1.1129	1.1129
0.60	1.0985	1.0985
0.70	1.0694	1.0694
0.80	1.0409	1.0409
0.85	1.0273	1.0273
0.90	1.0142	1.0142
0.95	-	-
NV	92	54

Table 4.2: λ in function of different values of ρ for the Gilbert-Elliot model.

The results of Table 4.2 show that, once again, the full packet and zero-input strategies were equivalent, with the latter requiring fewer decision variables. The use of a Gilbert-Elliot model, however, proved to be more conservative than utilizing the proposed network model, as the values of λ were lower, and there were even cases where feasible results could not be found (as for $\rho = 0.95$), in comparison to Table 4.1. This can stem from the fact that the Gilbert-Elliot model is not able to so easily model the deterministic assumption of the attacker's energetic limitation, which bounds the attacks to a maximum N consecutive time instants.

4.3.2 *Example 2:*

An Angular Positioning System (APS) borrowed from [46] is considered. In this system, a motor points an antenna towards a flying moving target. Considering a sample time of $0.1s$, the discretized APS model is as follows:

$$A(\alpha) = \begin{bmatrix} 1 & 0.1 \\ 0 & 1 - 0.1\lambda \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0.1\kappa \end{bmatrix},$$

where $0.1s^{-1} \leq \lambda \leq 10s^{-1}$ is an uncertain parameter proportional to the coefficient of viscous friction $\kappa = 0.787rad^{-1}V^{-1}s^{-2}$.

Considering the transition probability matrix (4.25), where $N = 5$, a full packet state feedback controller is designed utilizing Theorem 4.1 and $\rho = 0.9$. 1000 time-based simulations are conducted, in which a new set of α is selected at the beginning of each new simulation, and a new set of ξ_k is randomly selected at each time instant. Figure 4.1 illustrates the mean value of the states in the 1000 time-based simulations, as well as the interval defined by one standard deviation. The considered initial condition is $\eta(0) = \begin{bmatrix} \pi & -1.7 & 0 & 0 \end{bmatrix}^T$.

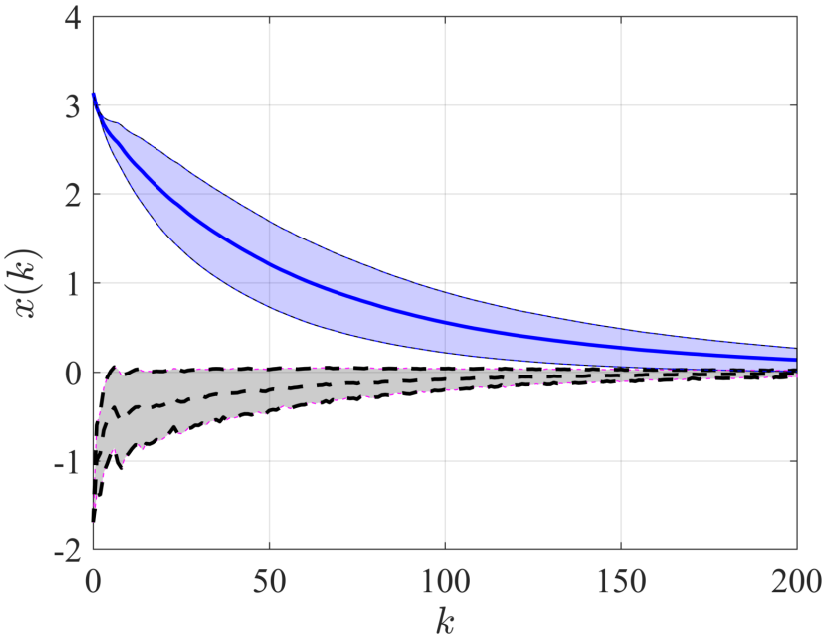

Figure 4.1: Mean value of states $x_1(k)$ (—) and $x_2(k)$ (- - -) with confidence interval of 1 standard-deviation from the 1000 time-based simulations with randomly selected ξ_k and α parameters. The mode-dependent full packet state-feedback control generated by Theorem 4.1 is considered and $\eta(0) = \begin{bmatrix} \pi & -1.7 & 0 & 0 \end{bmatrix}^T$.

In the sequel, the histogram indicating how often the system found itself in each mode during the 1000 simulations is displayed in Figure 4.2.

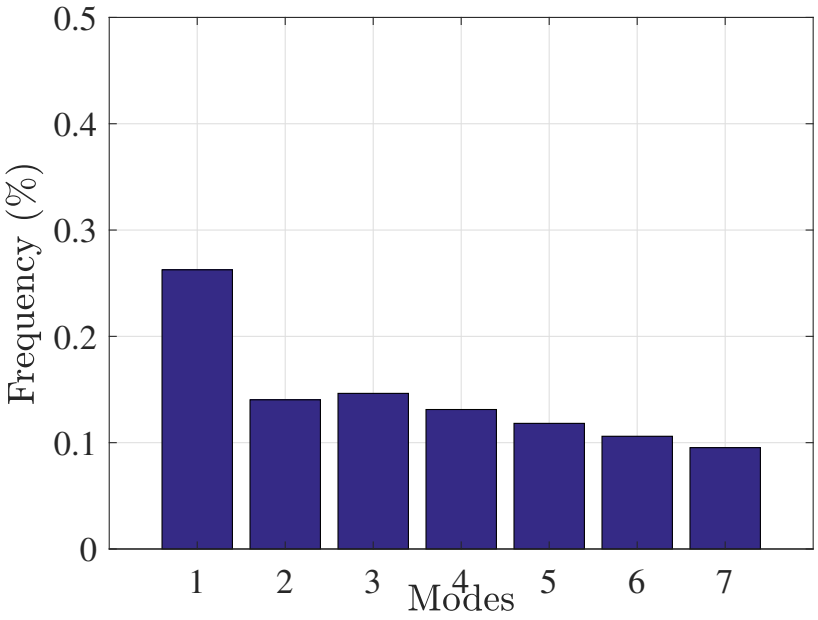

Figure 4.2: Histogram with the frequency of occurrence of each mode in the 1000 time-based simulations.

It can be seen that the proposed method resulted in a control strategy able to stabilize the system even when, on average, the network was successfully transmitting in less than 30% of the time.

To further illustrate the proposed control technique, a time-based simulation was randomly selected from the previous set. States $x_1(k)$ (—) and $x_2(k)$ (- - -) are plotted in Figure 4.3. The occurrence of the mode representing transmission failure is depicted in orange and the mode of the DoS attacks is illustrated in red.

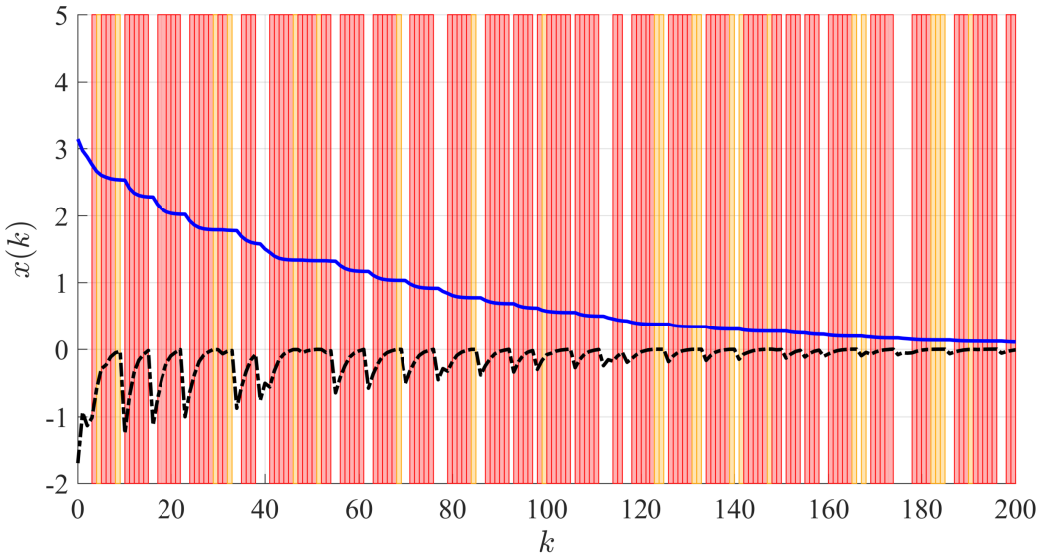

Figure 4.3: Time-based simulation of $x_1(k)$ (—) and $x_2(k)$ (- - -) with the mode-dependent full packet state-feedback control created with Theorem 4.1 considering a different randomly selected ξ_k for each time instant. $\alpha = \begin{bmatrix} 0.4911 & 0.5089 \end{bmatrix}$ and $\eta(0) = \begin{bmatrix} \pi & -1.7 & 0 & 0 \end{bmatrix}^T$. Transmission failures are depicted in orange and DoS attacks in red.

As it is reinforced in higher detail by Figure 4.3, the designed control strategy was able to stabilize the system even when suffering a high number of consecutive packet losses.

4.4 FINAL REMARKS

This chapter has proposed new conditions to design mode-dependent packet-based state-feedback controllers for discrete-time CPSs with time-invariant polytopic uncertainties. The CPSs utilizes an unreliable network that suffers packet losses because of network limitations and DoS attacks, which is modeled as depicted in Section 2.4 utilizing a non-homogeneous Markov chain with uncertain and unknown transition probabilities. Comparisons between the full packet, hold-input, and zero-input strategies were conducted, as well as a comparison between the proposed network model and a traditional Gilbert-Elliot model. With the conducted numerical experiments, the hold-input strategy proved to be the most ineffective and conservative approach, while the full packet strategy and zero-input provided virtually the same performance. This may indicate that for robust state-feedback controllers aiming only to stabilize the system under packet dropouts the use of the full packet strategy may provide no advantage. However, future investigations are required to prove this, mainly when considering parameter-dependent controllers. Moreover, the reference tracking problem with the proposed network model and techniques is a promising application to be analyzed, as the full packet strategy may prove to be more suitable for it. On what concerns the network models comparison, the proposed network model proved to be, in the considered example, less conservative than the Gilbert-Elliot model, with the latter even being unable to provide feasible solutions in more extreme cases.

5

$\mathscr{H}_\infty$ FILTER DESIGN FOR CYBER-PHYSICAL UNCERTAIN SYSTEMS UNDER UNRELIABLE MARKOVIAN NETWORK SUSCEPTIBLE TO DENIAL-OF-SERVICE ATTACKS

This chapter approaches the $\mathscr{H}_\infty$ filtering problem for discrete-time Cyber-Physical System (CPS) with time-invariant polytopic uncertainties. The system utilizes an unreliable network that features stochastic packet losses due to transmission limitations and is subject to Denial of Service attacks (DoS attacks). The attacker here considered is energetically bounded. The network model presented in Section 2.4 is accounted for here. Linear Matrix Inequalities (LMI) conditions that feature parameter-dependent slack variables are proposed aiming to obtain less conservative conditions to design mode-dependent and mode-independent full-order robust filters. Numerical experiments are presented to test the method's performance, and comparisons are drawn between the proposed network model and the traditional Gilbert-Elliot model.

5.1 PROBLEM STATEMENT

Consider the following discrete-time uncertain model of a CPS plant:

$$\begin{aligned} x(k+1) &= A(\alpha)x(k) + B(\alpha)w(k), \\ z(k) &= Cz(\alpha)x(k) + Dz(\alpha)w(k), \\ y(k) &= Cy(\alpha)x(k) + Dy(\alpha)w(k), \end{aligned} \tag{5.1}$$

where $x(k) \in \mathbb{R}^{n_x}$ is the state vector, $u(k) \in \mathbb{R}^{n_u}$ is the control input, $w(k) \in \mathbb{R}^{n_w}$ is the exogenous input with finite energy (i.e., $w \in \ell_2^{n_w}[0,\infty)$)), $y(k) \in \mathbb{R}^{n_y}$ is the measured output, and $z(k) \in \mathbb{R}^{n_z}$ is the estimated output. The matrices $A(\alpha) \in \mathbb{R}^{n_x \times n_x}$, $B(\alpha) \in \mathbb{R}^{n_x \times n_w}$, $Cy(\alpha) \in \mathbb{R}^{n_y \times n_x}$, $Dy(\alpha) \in \mathbb{R}^{n_y \times n_w}$, $Cz(\alpha) \in \mathbb{R}^{n_z \times n_x}$ and $Dz(\alpha) \in \mathbb{R}^{n_z \times n_w}$ belong to a polytopic domain as presented in Section 2.1 with (2.2). It is assumed that $A(\alpha)$ is Schur stable.

The utilized network model is presented in Section 2.4, with the attacks operating as seen in Figure 2.2. Consider a discrete-time non-homogeneous Markov chain $\{\theta_k; k \geq 0\}$ with a finite state-space $\mathbb{K} = \{1, \ldots, N+2\}$ where N is the maximum number of consecutive DoS attacks, and the mode transition probabilities are as follows

$$p_{ij}(k) = Pr(\theta_{k+1} = j \mid \theta_k = i),$$

which satisfies $p_{ij}(k) \geq 0$ and $\sum_{j=1}^{N+2} p_{ij}(k) = 1$, $\forall k \geq 0$. These mode transition probabilities are all contained in the transition probabilities matrix $\Psi(k) = |p_{ij}(k)|$, $i, j \in \mathbb{K}$. Matrix $\Psi(k)$ fea-

tures m rows with uncertain or unknown probabilities. The resulting Λ-homogeneous polynomial transition probability matrix $\Psi(\xi_k)$ is defined as follows:

$$\Psi(\xi_k) = \sum_{z=1}^{\psi} \xi_k(z)\Psi_z, \quad \xi_k = (\xi_{k,1}, \ldots, \xi_{k,m}) \in (\Lambda_{Z_1} \times \cdots \times \Lambda_{Z_m}) = \Omega_\psi, \tag{5.2}$$

where $z = 1, 2, \ldots, \psi$, with $\psi = Z_1 Z_2 \ldots Z_m$ vertices and $\xi_k = (\xi_{k,1}, \ldots, \xi_{k,m})$. $\xi_k(z)$ are homogeneous monomials with degree m which are created by the ψ-tuple with all the ψ possible combinations obtained between the sets $\mathscr{K}_1 = \{\xi_{k,11}, \ldots, \xi_{k,1Z_1}\}$ up to $\mathscr{K}_m = \{\xi_{k,m1}, \ldots, \xi_{k,mZ_m}\}$. See Section 2.4.1 for more details.

The packet dropouts due to the network unreliability and DoS attacks will affect the measured output $y(k)$, as stated in Figure 2.2. To circumvent it, in an approach inspired by [35], it is assumed that the last transmitted measurement $y_m(k)$ is stored in memory in the filter, here defined by:

$$y_m(k) = \delta_{\theta_k} y(k) + (1 - \delta_{\theta_k}) y_m(k-1), \tag{5.3}$$

where the δ_{θ_k} is a binary variable that follows the Markovian network state space $\mathbb{K} = \{1, \ldots, N+2\}$, and which indicates if the transmission was successful, or was thwarted by transmission failure or DoS attacks. δ_{θ_k} is depicted by the following:

$$\delta_{\theta_k} = \begin{cases} 1, & \text{if } \theta_k = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{5.4}$$

Consider the following full-order mode-dependent filter:

$$\begin{aligned} x_f(k+1) &= Af_{\theta_k} x_f(k) + Bf_{\theta_k} y_m(k), \\ z_f(k) &= Cf_{\theta_k} x_f(k) + Df_{\theta_k} y_m(k), \end{aligned} \tag{5.5}$$

where $x_f(k) \in \mathbb{R}^{n_x}$ is the filter state vector, $z_f(k) \in \mathbb{R}^{n_z}$ is the filter output, and $y_m(k) \in \mathbb{R}^{n_y}$ is the measured output that arrives at the filter, as defined in (5.3). $Af_{\theta_k} \in \mathbb{R}^{n_x \times n_x}$, $Bf_{\theta_k} \in \mathbb{R}^{n_x \times n_y}$, $Cf_{\theta_k} \in \mathbb{R}^{n_z \times n_x}$, $Df_{\theta_k} \in \mathbb{R}^{n_z \times n_y}$. For simplicity's sake, mode-dependent matrices will be described as $Af_{\theta_k = i} = Af_i$.

The estimation error is given by $e(k) = z(k) - z_f(k)$. Ultimately, by combining (5.1) with (5.3) and the full-order filter (5.5), the augmented system that evaluates the filtering error is described in the sequel:

$$\begin{aligned} \eta(k+1) &= \tilde{A}_i(\alpha)\eta(k) + \tilde{B}_i(\alpha)w(k), \\ e(k) &= \tilde{C}_i(\alpha)\eta(k) + \tilde{D}_i(\alpha)w(k), \end{aligned} \tag{5.6}$$

where $\eta(k) = \begin{bmatrix} x(k)^T & y_m(k-1)^T & x_f(k)^T \end{bmatrix}^T \in \mathbb{R}^n$ and $e(k) \in \mathbb{R}^{n_z}$, with $n = 2n_x + n_y$. The matrices have compatible dimensions and are described by:

$$\tilde{A}_i(\alpha) = \begin{bmatrix} A(\alpha) & 0_{n_x \times n_x} & 0_{n_x \times n_x} \\ \delta_i C y(\alpha) & (1-\delta_i) I_{n_y} & 0_{n_y \times n_x} \\ \delta_i B f_i C y(\alpha) & (1-\delta_i) B f_i & A f_i \end{bmatrix}, \qquad \tilde{B}_i(\alpha) = \begin{bmatrix} B(\alpha) \\ \delta_i D y(\alpha) \\ \delta_i B f_i D y(\alpha) \end{bmatrix}, \tag{5.7}$$

$$\tilde{C}_i(\alpha) = \begin{bmatrix} Cz(\alpha) - \delta_i D f_i C y(\alpha) & -(1-\delta_i) D f_i & -C f_i \end{bmatrix}, \quad \tilde{D}_i(\alpha) = Dz(\alpha) - \delta_i D f_i D y(\alpha).$$

5.2 MAIN RESULTS

In this section, the conditions to define and obtain the upper bounds of the $\mathscr{H}_\infty$ are presented. Then, the conditions to design a robust filter as in (5.5) with the goal of minimizing the $\mathscr{H}_\infty$ norm of the closed-loop system (5.6) are provided. The proposed technique was based on and adapted from [60], as well as took inspiration upon [61], in a Networked Control System (NCS) context. The method in said work allows the introduction of parameter-dependent slack variables to design a dynamic filter for systems with polytopic uncertainties. Here, it is adapted to account for the non-homogeneous Markovian network framework and to design a mode-dependent dynamic filter.

Firstly, the definition of the $\mathscr{H}_\infty$ norm from [35] is adapted for a Markov jump linear system (MJLS) that uses a non-homogeneous Markov chain:

Definition 5.1

If the exists the scalar γ, then given an initial $\eta(0)$ and θ_0, (5.6) $\|\mathscr{H}_\infty\|^2$ norm is bounded by γ such that

$$\sum_{k=0}^{\infty} \mathscr{E}(e(k)^T e(k)) < \gamma \sum_{k=0}^{\infty} w(k)^T w(k),$$

for all $w(k) \in \ell_2^{n_w}[0, \infty)$. $\mathscr{E}(\cdot)$ is the mathematical expectation.

Moreover, the bounded real lemma that considers the proposed framework and system is presented [34, 54].

Lemma 5.1

If there exist symmetric positive definite matrices $P_i(\xi_k, \alpha) \in \mathbb{R}^{n \times n}$, such that

$$\begin{bmatrix} \tilde{A}_i(\alpha) & \tilde{B}_i(\alpha) \\ \tilde{C}_i(\alpha) & \tilde{D}_i(\alpha) \end{bmatrix}^T \begin{bmatrix} P_i^+ & 0 \\ 0 & I_{n_z} \end{bmatrix} \begin{bmatrix} \tilde{A}_i(\alpha) & \tilde{B}_i(\alpha) \\ \tilde{C}_i(\alpha) & \tilde{D}_i(\alpha) \end{bmatrix} - \begin{bmatrix} P_i(\xi_k, \alpha) & 0 \\ 0 & \gamma I_{n_w} \end{bmatrix} < 0, \tag{5.8}$$

with

$$P_i^+ = \sum_{j=1}^{N+2} p_{ij}(\xi_k) P_j(\xi_{k+1}, \alpha), \tag{5.9}$$

hold for $i \in \mathbb{K}$, then (5.6) has a $\mathscr{H}_\infty$ norm bounded by $\sqrt{\gamma}$ for non-null $w \in \ell_2^{n_w}$ signals, and is Exponential stability in the mean square sense with conditioning I (ESMS-CI) for all $(\alpha, \xi_k, \xi_{k+1}) \in \Lambda_V \times \Omega_\psi \times \Omega_\psi$, $\forall k \geq 0$.

Proof. The proof for this Lemma is found, in detail, in [54]. □

Performing some manipulations, the following Lemma can be derived from Lemma 5.1:

Lemma 5.2

If there exist symmetric positive definite matrices $P_i(\xi_k, \alpha) \in \mathbb{R}^{n \times n}$, such that

$$\begin{bmatrix} P_i(\xi_k,\alpha) & \tilde{A}_i(\alpha)^T P_i^+ & 0 & \tilde{C}_i(\alpha)^T \\ \star & P_i^+ & P_i^+ \tilde{B}_i(\alpha) & 0 \\ \star & \star & I_{n_w} & \tilde{D}_i(\xi)^T \\ \star & \star & \star & \gamma I_{n_z} \end{bmatrix} > 0, \tag{5.10}$$

hold for $i \in \mathbb{K}$ and with P_i^+ as in (5.9), then (5.6) has a $\mathscr{H}_\infty$ norm bounded by $\sqrt{\gamma}$ for non-null $w \in \ell_2^{n_w}$ signals, and is ESMS-CI for all $(\alpha, \xi_k, \xi_{k+1}) \in \Lambda_V \times \Omega_\psi \times \Omega_\psi$, $\forall k \geq 0$.

Proof. Pre and post-multiplying (5.10) by $diag(\gamma^{\frac{1}{2}} I_n, \gamma^{\frac{1}{2}} I_n, \gamma^{\frac{1}{2}} I_{n_w}, \gamma^{-\frac{1}{2}} I_{n_z})$ and its transpose yields

$$\begin{bmatrix} (\gamma P_i(\xi_k,\alpha)) & \tilde{A}_i(\alpha)^T (\gamma P_i^+) & 0 & \tilde{C}_i(\alpha)^T \\ \star & (\gamma P_i^+) & (\gamma P_i^+)\tilde{B}_i(\alpha) & 0 \\ \star & \star & \gamma I_{n_w} & \tilde{D}_i(\xi)^T \\ \star & \star & \star & I_{n_z} \end{bmatrix} > 0,$$

Setting $P_i(\xi_k, \alpha) = (\gamma P_i(\xi_k, \alpha))$ and $P_i^+ = (\gamma P_i^+)$ allows to write

$$\begin{bmatrix} P_i(\xi_k,\alpha) & \tilde{A}_i(\alpha)^T P_i^+ & 0 & \tilde{C}_i(\alpha)^T \\ \star & P_i^+ & P_i^+ \tilde{B}_i(\alpha) & 0 \\ \star & \star & \gamma I_{n_w} & \tilde{D}_i(\xi)^T \\ \star & \star & \star & I_{n_z} \end{bmatrix} > 0. \tag{5.11}$$

By pre and post-multiplying (5.11) by $\mathscr{L}^T$ and its transpose, where

$$\mathscr{L}^T = \begin{bmatrix} I_n & 0 & 0 & 0 \\ 0 & 0 & I_{n_w} & 0 \\ 0 & 0 & 0 & I_{n_z} \\ 0 & I_n & 0 & 0 \end{bmatrix},$$

the following is obtained

$$\begin{bmatrix} P_i(\xi_k,\alpha) & 0 & \tilde{C}_i(\alpha)^T & \tilde{A}_i(\alpha)^T P_i^+ \\ \star & \gamma I_{n_w} & \tilde{D}_i(\alpha)^T & \tilde{B}_i(\alpha)^T P_i^+ \\ \star & \star & I_{n_z} & 0 \\ \star & \star & \star & P_i^+ \end{bmatrix} > 0.$$

Through Schur's complement, the following is found

$$\begin{bmatrix} P_i(\xi_k,\alpha) & 0 \\ 0 & \gamma I_{n_w} \end{bmatrix} - \begin{bmatrix} \tilde{A}_i(\alpha) & \tilde{B}_i(\alpha) \\ \tilde{C}_i(\alpha) & \tilde{D}_i(\alpha) \end{bmatrix}^T \begin{bmatrix} P_i^+ & 0 \\ 0 & I_{n_z} \end{bmatrix} \begin{bmatrix} \tilde{A}_i(\alpha) & \tilde{B}_i(\alpha) \\ \tilde{C}_i(\alpha) & \tilde{D}_i(\alpha) \end{bmatrix} > 0,$$

which is equivalent to the bounded real lemma condition of Lemma 5.1. □

With the aid of Finsler's Lemma, as described in Section 2.6, parameter-dependent slack variables will be selected to create less conservative LMI conditions to design the mode-dependent filter departing from the following Lemma:

Lemma 5.3

If there exists the symmetric positive definite matrices $P_i(\xi_k,\alpha) \in \mathbb{R}^{n\times n}$, and matrices $\mathscr{J}(\alpha) \in \mathbb{R}^{n\times n}$, $\mathscr{O}(\alpha) \in \mathbb{R}^{n_w\times n}$, $\mathscr{G}(\alpha) \in \mathbb{R}^{n\times n}$, $\mathscr{F}(\alpha) \in \mathbb{R}^{n_z\times n}$, and the scalar variable γ, such that

$$\begin{bmatrix} P_i(\xi_k,\alpha) + \mathscr{J}(\alpha)\tilde{A}_i(\alpha) + \tilde{A}_i(\alpha)^T\mathscr{J}(\alpha)^T & \star \\ -\mathscr{J}(\alpha)^T + \mathscr{G}(\alpha)\tilde{A}_i(\alpha) & -P_i^+ - \mathscr{G}(\alpha) - \mathscr{G}(\alpha)^T \\ \tilde{B}_i(\alpha)^T\mathscr{J}(\alpha)^T + \mathscr{O}(\alpha)\tilde{A}_i(\alpha) & \tilde{B}_i(\alpha)^T\mathscr{G}(\alpha)^T - \mathscr{O}(\alpha)^T \\ \mathscr{F}(\alpha)\tilde{A}_i(\alpha) + \tilde{C}_i(\alpha) & -\mathscr{F}(\alpha) \\ \star & \star \\ \star & \star \\ \tilde{B}_i(\alpha)^T\mathscr{O}(\alpha)^T + \mathscr{O}(\alpha)\tilde{B}_i(\alpha) + I_{n_z} & \star \\ \mathscr{F}(\alpha)\tilde{B}_i(\alpha) + \tilde{D}_i(\alpha) & \gamma I_{n_z} \end{bmatrix} > 0, \tag{5.12}$$

hold for $i \in \mathbb{K}$, with P_i^+ as in (5.9), then (5.6) has a $\mathscr{H}_\infty$ norm bounded by $\sqrt{\gamma}$ for non-null $w \in \ell_2^{n_w}$ signals, and is ESMS-CI for all $(\alpha, \xi_k, \xi_{k+1}) \in \Lambda_V \times \Omega_\psi \times \Omega_\psi$, $\forall k \geq 0$.

Proof. The condition (5.12) is equivalent to condition (iv) of Finsler's Lemma, by considering the following:

$$\mathscr{X} = \begin{bmatrix} \mathscr{J}(\alpha) \\ \mathscr{G}(\alpha) \\ \mathscr{O}(\alpha) \\ \mathscr{F}(\alpha) \end{bmatrix}, \quad \mathscr{Q} = \begin{bmatrix} P_i(\xi_k, \alpha) & 0_{n\times n} & 0_{n\times n_w} & \tilde{C}_i(\alpha)^T \\ \star & -P_i^+ & 0_{n\times n_w} & 0_{n\times n_z} \\ \star & \star & I_{n_w} & \tilde{D}_i(\alpha)^T \\ \star & \star & \star & \gamma I_{n_z} \end{bmatrix}, \quad \mathscr{B}^T = \begin{bmatrix} \tilde{A}_i(\alpha)^T \\ -I_n \\ \tilde{B}_i(\alpha)^T \\ 0_{n_z\times n} \end{bmatrix}, \tag{5.13}$$

where a basis for the Nullspace of $\mathscr{B}^T$ is

$$\mathscr{B}^{\perp T} = \begin{bmatrix} I_n & \tilde{A}_i(\alpha)^T & 0_{n\times n_w} & 0_{n\times n_z} \\ 0_{n_w\times n} & \tilde{B}_i(\alpha)^T & I_{n_w} & 0_{n_w\times n_z} \\ 0_{n_z\times n} & 0_{n_z\times n} & 0_{n_z\times n_w} & I_{n_z} \end{bmatrix}. \tag{5.14}$$

Pre and post-multiplying (5.12) by $\mathscr{B}^{\perp T}$ and its transpose yields the modified bounded real lemma condition (5.10) of Lemma (5.2). □

The slack variables can be partitioned with the following structure:

$$\mathscr{J}(\alpha) = \begin{bmatrix} K_{11}(\alpha) & K_{12}(\alpha) & 0_{n_x\times n_x} \\ K_{21}(\alpha) & K_{22}(\alpha) & 0_{n_y\times n_x} \\ K_{31}(\alpha) & K_{32}(\alpha) & 0_{n_x\times n_x} \end{bmatrix}, \quad \begin{array}{c} K_{11}(\alpha), K_{31}(\alpha) \in \mathbb{R}^{n_x\times n_x}, \\ K_{12}(\alpha), K_{32}(\alpha) \in \mathbb{R}^{n_x\times n_y}, \\ K_{21}(\alpha) \in \mathbb{R}^{n_y\times n_x}, \\ K_{22}(\alpha) \in \mathbb{R}^{n_y\times n_y}, \end{array} \tag{5.15}$$

$$\mathscr{O}(\alpha) = \begin{bmatrix} Q_1(\alpha) & Q_2(\alpha) & 0_{n_w\times n_x} \end{bmatrix}, \quad Q_1(\alpha) \in \mathbb{R}^{n_w\times n_x}, \quad Q_2(\alpha) \in \mathbb{R}^{n_w\times n_y}, \tag{5.16}$$

$$\mathscr{G}(\alpha) = \begin{bmatrix} E_{11}(\alpha) & E_{12}(\alpha) & K \\ E_{21}(\alpha) & E_{22}(\alpha) & 0_{n_y\times n_x} \\ E_{31}(\alpha) & E_{32}(\alpha) & K \end{bmatrix}, \quad \begin{array}{c} E_{11}(\alpha), E_{31}(\alpha), K \in \mathbb{R}^{n_x\times n_x}, \\ E_{12}(\alpha), E_{32}(\alpha) \in \mathbb{R}^{n_x\times n_y}, \\ E_{21}(\alpha) \in \mathbb{R}^{n_y\times n_x}, \\ E_{22}(\alpha) \in \mathbb{R}^{n_x\times n_y}, \end{array} \tag{5.17}$$

$$\mathscr{F}(\alpha) = \begin{bmatrix} F_1(\alpha) & F_2(\alpha) & 0_{n_z\times n_x} \end{bmatrix}, \quad F_1(\alpha) \in \mathbb{R}^{n_z\times n_x}, \quad F_2(\alpha) \in \mathbb{R}^{n_z\times n_y}, \tag{5.18}$$

while $P_i(\xi_k,\alpha)$ can be subdivided by the symmetric matrices $P_{11,i}(\xi_k,\alpha), P_{33,i}(\xi_k,\alpha) \in \mathbb{R}^{n_x\times n_x}$, $P_{22,i}(\xi_k,\alpha) \in \mathbb{R}^{n_y\times n_y}$, and matrices $P_{12,i}(\xi_k,\alpha) \in \mathbb{R}^{n_x\times n_y}$, $P_{13,i}(\xi_k,\alpha) \in \mathbb{R}^{n_x\times n_x}$, $P_{23,i}(\xi_k,\alpha) \in \mathbb{R}^{n_y\times n_x}$, for $i \in \mathbb{K}$:

$$P_i(\xi_k,\alpha) = \begin{bmatrix} P_{11,i}(\xi_k,\alpha) & P_{12,i}(\xi_k,\alpha) & P_{13,i}(\xi_k,\alpha) \\ P_{12,i}(\xi_k,\alpha)^T & P_{22,i}(\xi_k,\alpha) & P_{23,i}(\xi_k,\alpha) \\ P_{13,i}(\xi_k,\alpha)^T & P_{23,i}(\xi_k,\alpha)^T & P_{33,i}(\xi_k,\alpha) \end{bmatrix}. \tag{5.19}$$

With these defined, the general Theorem for designing the dynamic filter is presented as follows.

Theorem 5.1

If there exist symmetric matrices $P_{11,i}(\xi_k,\alpha)$, $P_{33,i}(\xi_k,\alpha) \in \mathbb{R}^{n_x\times n_x}$, $P_{22,i}(\xi_k,\alpha) \in \mathbb{R}^{n_y\times n_y}$, and matrices $P_{12,i}(\xi_k,\alpha)$, $K_{12}(\alpha)$, $K_{32}(\alpha)$, $E_{12}(\alpha)$, $E_{32}(\alpha)$, $K_{2,i} \in \mathbb{R}^{n_x\times n_y}$, $P_{13,i}(\xi_k,\alpha)$, $K_{11}(\alpha)$, $K_{31}(\alpha)$, $E_{11}(\alpha)$, $E_{31}(\alpha)$, K, $K_{1,i} \in \mathbb{R}^{n_x\times n_x}$, $P_{23,i}(\xi_k,\alpha) \in \mathbb{R}^{n_y\times n_x}$, $K_{21}(\alpha)$, $E_{21}(\alpha) \in \mathbb{R}^{n_y\times n_x}$, $K_{22}(\alpha)$, $E_{22}(\alpha) \in \mathbb{R}^{n_y\times n_y}$, $Q_1(\alpha) \in \mathbb{R}^{n_w\times n_x}$, $F_1(\alpha) \in \mathbb{R}^{n_z\times n_x}$, $Q_2(\alpha) \in \mathbb{R}^{n_w\times n_y}$, $Cf_i \in \mathbb{R}^{n_z\times n_x}$, $F_2(\alpha)$, $Df_i \in \mathbb{R}^{n_z\times n_y}$ and the scalar positive parameter γ such that,

$$\min \gamma, \tag{5.20}$$

$$P_i(\xi_k,\alpha) = \begin{bmatrix} P_{11,i}(\xi_k,\alpha) & P_{12,i}(\xi_k,\alpha) & P_{13,i}(\xi_k,\alpha) \\ P_{12,i}(\xi_k,\alpha)^T & P_{22,i}(\xi_k,\alpha) & P_{23,i}(\xi_k,\alpha) \\ P_{13,i}(\xi_k,\alpha)^T & P_{23,i}(\xi_k,\alpha)^T & P_{33,i}(\xi_k,\alpha) \end{bmatrix} > 0, \tag{5.21}$$

$$\begin{bmatrix} \phi_{11} & \phi_{12} & \phi_{13} & \phi_{14} & \phi_{15} & \phi_{16} & \phi_{17} & \phi_{18} \\ \star & \phi_{22} & \phi_{23} & \phi_{24} & \phi_{25} & \phi_{26} & \phi_{27} & \phi_{28} \\ \star & \star & \phi_{33} & \phi_{34} & \phi_{35} & \phi_{36} & \phi_{37} & \phi_{38} \\ \star & \star & \star & \phi_{44} & \phi_{45} & \phi_{46} & \phi_{47} & \phi_{48} \\ \star & \star & \star & \star & \phi_{55} & \phi_{56} & \phi_{57} & \phi_{58} \\ \star & \star & \star & \star & \star & \phi_{66} & \phi_{67} & \phi_{68} \\ \star & \star & \star & \star & \star & \star & \phi_{77} & \phi_{78} \\ \star & \star & \star & \star & \star & \star & \star & \phi_{88} \end{bmatrix} > 0, \tag{5.22}$$

where,

$$\phi_{11} = P_{11,i}(\xi_k,\alpha) + He(K_{11}(\alpha)A(\alpha) + \delta_i K_{12}(\alpha)Cy(\alpha)),$$

$$
\begin{aligned}
\phi_{12} &= P_{12,i}(\xi_k,\alpha) + (1-\delta_i)K_{12} + A(\alpha)^T K_{21}(\alpha)^T + \delta_i Cy(\alpha)^T K_{22}(\alpha)^T,\\
\phi_{13} &= P_{13,i}(\xi_k,\alpha) + A(\alpha)^T K_{31}(\alpha)^T + \delta_i Cy(\alpha)^T K_{32}(\alpha)^T,\\
\phi_{14} &= A(\alpha)^T E_{11}(\alpha)^T - K_{11}(\alpha) + \delta_i(Cy(\alpha)^T E_{12}(\alpha)^T + Cy(\alpha)^T K_{2,i}^T),\\
\phi_{15} &= A(\alpha)^T E_{21}(\alpha)^T - K_{12}(\alpha) + \delta_i Cy(\alpha)^T E_{22}(\alpha)^T,\\
\phi_{16} &= A(\alpha)^T E_{31}(\alpha)^T + \delta_i(Cy(\alpha)^T E_{32}(\alpha)^T + Cy(\alpha)^T K_{2,i}^T),\\
\phi_{17} &= A(\alpha)^T Q_1(\alpha)^T + K_{11}(\alpha)B(\alpha) + \delta_i(K_{12}(\alpha)Dy(\alpha) + Cy(\alpha)^T Q_2(\alpha)^T),\\
\phi_{18} &= A(\alpha)^T F_1(\alpha)^T + Cz(\alpha)^T + \delta_i(Cy(\alpha)^T F_2(\alpha)^T - Cy(\alpha)^T Df_i^T),\\
\phi_{22} &= P_{22,i}(\xi_k,\alpha) + (1-\delta_i)He(K_{22}(\alpha)),\\
\phi_{23} &= P_{23,i}(\xi_k,\alpha) + (1-\delta_i)K_{32}(\alpha)^T,\\
\phi_{24} &= (1-\delta_i)(E_{12}(\alpha)^T + K_{2,i}^T) - K_{21}(\alpha),\\
\phi_{25} &= (1-\delta_i)E_{22}(\alpha)^T - K_{22}(\alpha),\\
\phi_{26} &= (1-\delta_i)(E_{32}(\alpha)^T + K_{2,i}^T),\\
\phi_{27} &= (1-\delta_i)Q_2(\alpha)^T + \delta_i K_{22}(\alpha)Dy(\alpha) + K_{21}(\alpha)B(\alpha),\\
\phi_{28} &= (1-\delta_i)(F_2(\alpha)^T - Df_i),\\
\phi_{33} &= W_{33,i}(\xi_k,\alpha),\\
\phi_{34} &= K_{1,i}^T - K_{31}(\alpha),\\
\phi_{35} &= -K_{32}(\alpha),\\
\phi_{36} &= K_{1,i}^T,\\
\phi_{37} &= K_{31}(\alpha)B(\alpha) + \delta_i K_{32}(\alpha)Dy(\alpha),\\
\phi_{38} &= -Cf_i^T,\\
\phi_{44} &= -P_{11,i}^+ - He(E_{11}(\alpha)),\\
\phi_{45} &= -P_{12,i}^+ - E_{21}(\alpha)^T - E_{12}(\alpha),\\
\phi_{46} &= -P_{13,i}^+ - E_{31}(\alpha)^T - K,\\
\phi_{47} &= E_{11}(\alpha)B(\alpha) - Q_1(\alpha)^T + \delta_i(E_{12}(\alpha)Dy(\alpha) + K_{2,i}Dy(\alpha)),\\
\phi_{48} &= -F_1(\alpha)^T,\\
\phi_{55} &= -P_{22,i}^+ - He(E_{22}(\alpha)),\\
\phi_{56} &= -P_{23,i}^+ - E_{32}(\alpha)^T,\\
\phi_{57} &= E_{21}(\alpha)B(\alpha) - Q_2(\alpha)^T + \delta_i E_{22}(\alpha)Dy(\alpha),\\
\phi_{58} &= -F_2(\alpha)^T,\\
\phi_{66} &= -P_{33,1}^+ - He(K),\\
\phi_{67} &= E_{31}(\alpha)B(\alpha) + \delta_i(E_{32}(\alpha)Dy(\alpha) + K_{2,i}Dy(\alpha)),\\
\phi_{68} &= 0_{n_x \times n_z},\\
\phi_{77} &= He(Q_1(\alpha)B(\alpha) + \delta_i Q_2(\alpha)Dy(\alpha)) + I_{n_w},\\
\phi_{78} &= B(\alpha)^T F_1(\alpha)^T + Dz(\alpha)^T + \delta_i(Dy(\alpha)^T F_2(\alpha)^T - Dy(\alpha)^T Df_i^T),\\
\phi_{88} &= \gamma I_{n_z},
\end{aligned}
$$

with,

$$\delta_i = \begin{cases} 1, & \text{if } i = 1, \\ 0, & \text{otherwise.} \end{cases}$$

and where $P^+_{11,i}$, $P^+_{12,i}$, $P^+_{13,i}$, $P^+_{22,i}$, $P^+_{23,i}$, $P^+_{33,i}$ are written after the generic matrix M^+_i, with

$$M^+_i = \sum_{j=1}^{N+2} p_{ij}(\xi_k) M_j(\xi_{k+1}, \alpha), \tag{5.23}$$

then for all $i \in \mathbb{K}$, $Af_i = K^{-1}K_{1,i}$, $Bf_i = K^{-1}K_{2,i}$, Cf_i and Df_i are the mode-dependent matrices of the filter (5.5) that assures that (5.6) has a guaranteed cost $\mathscr{H}_\infty$ bounded by $\sqrt{\gamma}$ for non-null $w \in \ell_2^{n_w}$ signals, and is ESMS-CI for all $(\alpha, \xi_k, \xi_{k+1}) \in \Lambda_V \times \Omega_\psi \times \Omega_\psi$, $\forall k \geq 0$.

Proof. The proof follows the same line as in Lemma 5.3 considering (5.15)-(5.19). □

The mode-dependent filter just presented departs from Assumption 2.2 that dictates that the system is able to differentiate between packet losses due to network limitations and DoS attacks, as well as having a way to track how many consecutive time instants of attack the network is under. This however may not be always possible. A solution to it, whereas a more conservative one, is to utilize a mode-independent filter. The design conditions to do so are presented in Corollary 5.1.

Corollary 5.1

If open-loop ($w = 0$) system (5.1) is stable, and there exist symmetric matrices $P_{11,i}(\xi_k, \alpha)$, $P_{22,i}(\xi_k, \alpha) \in \mathbb{R}^{n_y \times n_y}$, $P_{33,i} \in \mathbb{R}^{n_x \times n_x}$, and matrices $P_{12,i}(\xi_k, \alpha)$, K_{12}, K_{32}, E_{12}, E_{32}, $K_2 \in \mathbb{R}^{n_x \times n_y}$, $P_{13,i}(\alpha)$, $K_{11}(\alpha)$, $K_{13}(\alpha)$, $E_{11}(\alpha)$, $E_{13}(\alpha)$, K, $K_1 \in \mathbb{R}^{n_x \times n_x}$, $P_{23,i} \in \mathbb{R}^{n_y \times n_x}$, K_{21}, $E_{21} \in \mathbb{R}^{n_y \times n_x}$, K_{22}, $E_{22} \in \mathbb{R}^{n_y \times n_y}$, $Q_1 \in \mathbb{R}^{n_w \times n_x}$, $F_1(\alpha) \in \mathbb{R}^{n_z \times n_x}$, $Q_2(\alpha) \in \mathbb{R}^{n_w \times n_y}$, $F_2(\alpha)$, $Cf \in \mathbb{R}^{n_z \times n_x}$, $Df \in \mathbb{R}^{n_z \times n_y}$ and the scalar positive parameter γ, such that (5.21) and (5.22) are feasible, then $Af = K^{-1}K_1$, $Bf_i = K^{-1}K_2$, Cf and Df are the mode-independent matrices of the filter (5.5) for $Af_i = Af$, $Bf_i = Bf$, $Cf_i = Cf$, and $Df_i = Df$ that assures that (5.6) has a guaranteed cost $\mathscr{H}_\infty$ bounded by $\sqrt{\gamma}$ for non-null $w \in \ell_2^{n_w}$ signals, and is ESMS-CI for all $i \in \mathbb{K}$, $(\alpha, \xi_k, \xi_{k+1}) \in \Lambda_V \times \Omega_\psi \times \Omega_\psi$, and $\forall k \geq 0$.

Remark 5.1

The number of scalar decision variables employed by Theorem 5.1 (NV_{T1}) and Corollary 5.1 (NV_{C1}) is defined by the following:

$$NV_{T1} = n_x^2 + (N+2)(n_x+n_y)(n_x+n_z) + V(n_x+n_y)(n_w+4n_x+2n_y+n_z) + V\psi(N+2)(2n_x^2+2n_xn_y+n_x+\frac{n_y^2}{2}+\frac{n_y}{2})+1,$$

$$NV_{C1} = n_x^2 + (n_x+n_y)(n_x+n_z) + V(n_x+n_y)(n_w+4n_x+2n_y+n_z) + V\psi(N+2)(2n_x^2+2n_xn_y+n_x+\frac{n_y^2}{2}+\frac{ny}{2})+1,$$

with ψ as seen in (5.2).

5.3 NUMERICAL EXPERIMENTS

In this section, numerical experiments will be conducted to test the proposed mode-dependent and mode-independent filter design technique considering an uncertain CPS. The network is unreliable and modeled as described in section 2.4 and Figure 2.2. Comparisons between the proposed network model and a classic Gilbert-Elliot model will be conducted. All tests were performed and the parameter-dependent LMIs were written using the parsers YALMIP [105], ROLMIP [112], and the solver MOSEK [106] combined with MATLAB 2016b.

5.3.1 *Example 1:*

Consider the following discrete-time uncertain system, borrowed from [59]

$$A = \begin{bmatrix} 0 & -0.5 \\ 1 & 1+\mu \end{bmatrix}, \quad B = \begin{bmatrix} -6 & 0 \\ 1 & 0 \end{bmatrix},$$
$$C_y = \begin{bmatrix} -100 & 10 \end{bmatrix}, \quad D_y = \begin{bmatrix} 0 & 1 \end{bmatrix},$$
$$C_z = \begin{bmatrix} 1 & 0 \end{bmatrix}, \quad D_z = \begin{bmatrix} 0 & 0 \end{bmatrix},$$

where $|\mu| \leq 0.45$, resulting in $V = 2$ vertices, and whose closed-loop system is described as in (5.6).

Considering a maximum of $N = 5$ consecutive attacks, the utilized transition probability matrix (created based on (2.11)) with $m = 2$ rows with uncertain and unknown probabilities is as follows:

$$\Psi = \begin{bmatrix} 0.45 & c & d & 0 & 0 & 0 & 0 \\ 0.5 & ? & ? & 0 & 0 & 0 & 0 \\ f & 0.05 & 0 & \rho & 0 & 0 & 0 \\ f & 0.05 & 0 & 0 & \rho & 0 & 0 \\ f & 0.05 & 0 & 0 & 0 & \rho & 0 \\ f & 0.05 & 0 & 0 & 0 & 0 & \rho \\ 0.45 & 0.55 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{5.24}$$

where $f = (1 - 0.05 - \rho)$, $c = \begin{bmatrix} 0.05 & 0.15 \end{bmatrix}$ and $d = \begin{bmatrix} 0.4 & 0.5 \end{bmatrix}$. ρ is a parameter that establishes if longer attacks are more likely to occur. The closer the value of ρ is to 1, the higher the probability that each attack that initiates will have a duration of N time instants.

Theorem 5.1 is utilized to obtain a mode-dependent filter and Corollary 5.1 to obtain a mode-independent filter. The scenario with $N = 5$ described by (5.24) is taken into account, as well as a scenario with $N = 10$, which is easily obtained by using the same values of rows 3 to 6 in (5.24), in accordance to the positioning defined by (2.11). The norm value in function of the parameter ρ and the number of decision variables in function of N is displayed in Table 5.1

	Theorem 5.1		Corollary 5.1	
ρ \ N	5	10	5	10
0.50	10.73	10.73	11.79	11.79
0.60	12.09	12.14	13.07	13.19
0.70	13.87	14.25	15.13	15.98
0.80	16.12	17.92	17.98	20.87
0.85	17.49	20.70	19.82	24.60
0.90	19.08	24.11	22.10	29.50
0.95	20.96	28.59	24.90	35.55
NV	986	1631	932	1532

Table 5.1: $\|\mathscr{H}_\infty\|$ cost in function of different values of ρ.

Through Table 5.1, it is evident that the probability of persisting in an attack (as seen in the parameter ρ) affects the $\mathscr{H}_\infty$ cost more than the maximum number N of attacks considered. Moreover, even with higher probabilities of consecutive attacks, the method was able to provide feasible results, whereas at the cost of needing to solve a somewhat high complexity problem, as seen in the number of variables required. The mode-dependent filter designed by Theorem 5.1 provided the best costs. However, the mode-independent filter of Corollary 5.1 was also able to supply competitive performances while requiring a relatively lower number of decision variables.

This is useful to know, as it is far simpler to implement a filtering system that does not need to detect in which mode the system finds itself.

In the sequel, a Gilbert-Elliot model as described by Figure 2.4 is proposed. The adapted transition probability matrix is constructed using the first row of (5.24) to refer to the successful transmission mode, while the second row of the adapted matrix has a lower bound according to the second row of (5.24) and an upper-bound according to modes 3 to 6. This results in the following, which is modeled as a matrix with uncertain time-varying probabilities in the second row:

$$\Psi = \begin{bmatrix} 0.45 & 0.55 \\ \begin{bmatrix} 0.5 & (1-\rho-0.05) \end{bmatrix} & \begin{bmatrix} 0.5 & (\rho+0.05) \end{bmatrix} \end{bmatrix}. \tag{5.25}$$

Theorem 5.1 and Corollary 5.1 are once again utilized to respectively design a mode-dependent and mode-independent filter according to (5.25). The value of N is irrelevant since a Gilbert-Elliot model features only two modes. Thus, in this specific case, to calculate the number of scalar decision variables required, the following holds

$$\begin{aligned} NV_{GB,T1} = n_x^2 + 2(n_x+n_y)(n_x+n_z) + V(n_x+n_y)(n_w+4n_x+2n_y+n_z) \\ + 2V\psi(2n_x^2+2n_xn_y+n_x+\frac{n_y^2}{2}+\frac{n_y}{2})+1, \end{aligned}$$

$$\begin{aligned} NV_{GB,C1} = n_x^2 + (n_x+n_y)(n_x+n_z) + V(n_x+n_y)(n_w+4n_x+2n_y+n_z) \\ + 2V\psi(2n_x^2+2n_xn_y+n_x+\frac{n_y^2}{2}+\frac{ny}{2})+1. \end{aligned}$$

Table 5.2 displays the performance cost in function of ρ, as well as the number of decision variables required.

ρ	Theorem 5.1	Corollary 5.1
0.50	10.80	10.80
0.60	12.40	13.47
0.70	14.87	16.75
0.80	19.62	24.28
0.85	24.42	31.03
0.90	32.20	39.22
0.95	-	-
NV	221	212

Table 5.2: $\|\mathscr{H}_\infty\|$ cost in function of different values of ρ for the Gilbert-Elliot model.

As seen in Table 5.2, using the equivalent Gilbert-Elliot model is a less complex problem from the viewpoint of the number of decision variables required. However, the case for $\rho = 0.95$ did not provide feasible solutions. Moreover, the performance of the resulting filters is more

conservative than what was obtained with the proposed network model (featured in Table 5.1), mainly in scenarios with a higher value of ρ. This shows that the proposed network model is less conservative and better represented the deterministic assumption of energy limitation of the attacker.

5.3.2 *Example 2:*

Consider the system from [113], which consists of a mechanical system with two masses and two springs. The discretized model with sample time $0.1s$, borrowed from [114], is presented in the sequel.

$$A_1 = A_2 = \begin{bmatrix} 0.99 & 0 & 0.1 & 0 \\ 0.01 & 0.99 & 0 & 0.1 \\ -0.19 & 0.10 & 0.94 & 0 \\ 0.19 & -0.19 & 0.01 & 0.90 \end{bmatrix}, \qquad B_1 = B_2 = \begin{bmatrix} 0 \\ 0 \\ 0.01 \\ 0 \end{bmatrix},$$

$$Cy_1 = \begin{bmatrix} 0.3 & 0 & 0 & 0 \end{bmatrix}, \quad Dy_1 = Dy_2 = 0, \quad Cz_1 = Cz_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix},$$
$$Cy_2 = \begin{bmatrix} 1.7 & 0 & 0 & 0 \end{bmatrix}, \quad Dz_1 = Dz_2 = 0.$$

For simplicity's sake, the transition probability matrix (5.24) will be utilized considering $\rho = 0.9$ and $N = 5$. The mode-dependent filter of Theorem 5.1 returned a guaranteed cost of $\sqrt{\gamma} = 0.0967$, having required 2912 decision variables.

To further test the method's performance, 1000 time-based simulations, with a randomly selected set of α for each simulation and ξ_k for each time instant, and null $\eta(0)$. The interval $k \in [0, 170]$ and the exogenous disturbance $w(k) = 10e^{-0.05k}\cos(0.1k)$ were considered. Utilizing $\sqrt{\sum_{k=0}^{\infty} e(k)^2 / \sum_{k=0}^{\infty} w(k)^2}$ the $\mathscr{H}_\infty$ cost of each simulation is calculated. The mean response and the standard deviation of the $\mathscr{H}_\infty$ cost was, respectively, 0.0354 and 0.0098. The mean response with one standard deviation of $z_f(k)$ (- - -) and the mean response of the estimated output $z(k)$ (—) of the 1000 simulations are obtained and are featured in Figure 5.1. Note that $z(k)$ showed a null value of standard deviation, given that it does not depend on the network, nor (in this particular system) is influenced by the parametric uncertainties.

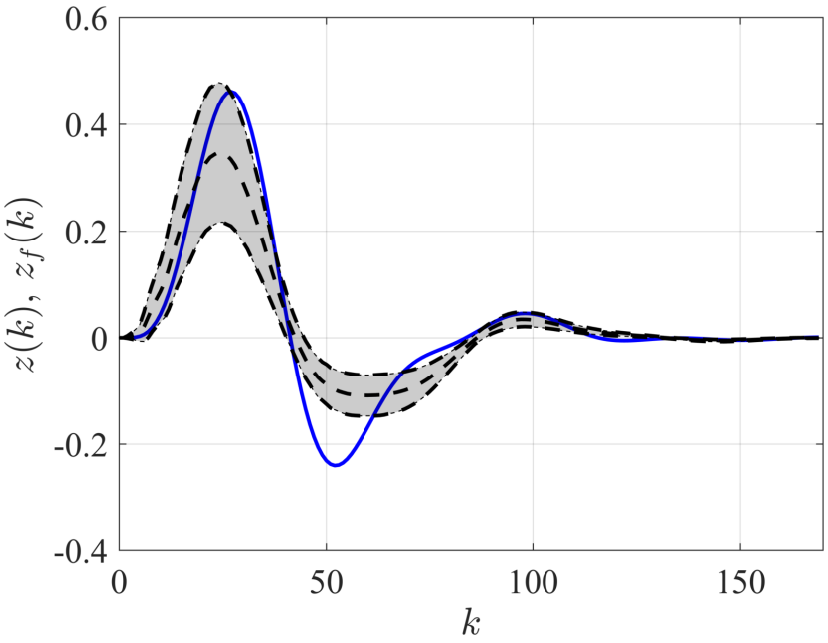

Figure 5.1: Mean $z(k)$ (—) and mean $z_f(k)$ (- - -) with confidence interval of 1 standard-deviation from the 1000 time-based simulations. A new set of α was randomly selected at each simulation and a new ξ_k is randomly selected at each time instant. The mode-dependent filter of Theorem 5.1 is considered and $\eta(0)$ is null.

Moreover, Figure 5.2 shows the histogram of how often the system found itself in each of the modes in the 1000 simulations.

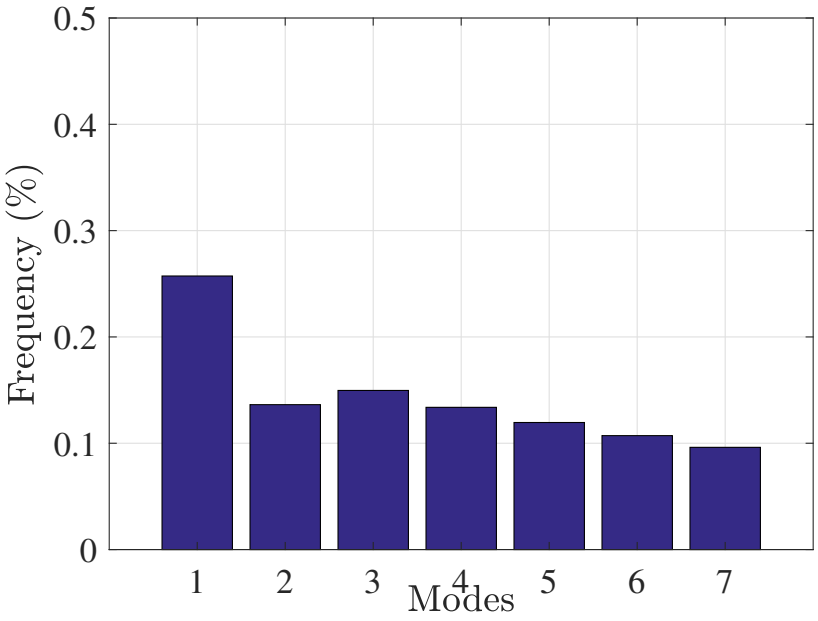

Figure 5.2: Histogram with the frequency of occurrence of each mode in the 1000 time-based simulations.

It can be seen that even with successful transmissions less than 30% of the time, the filter was able to perform its function and mitigate the impact of the exogenous disturbance in the output. The obtained mean value of the $\mathscr{H}_\infty$ cost showed that it was even smaller than the one guaranteed by design, indicating that the latter shows a somewhat conservative value compared to the actual operation of the filter.

In the sequel, a random simulation is selected to better illustrate the evolution of the modes in function of time and is shown in Figure 5.3. The filter output $z_f(k)$ (- - -) and the estimated output $z(k)$ (—) are displayed. The modes representing transmission failure are depicted in orange and DoS attacks in red. Using $\sqrt{\sum_{k=0}^{\infty} e(k)^2 / \sum_{k=0}^{\infty} w(k)^2}$ returns a cost of 0.0303. Once again, it can be seen that the filter was able to perform as expected, even with frequent consecutive packet losses, and that the calculated cost had a value lower than the one guaranteed in the design stage.

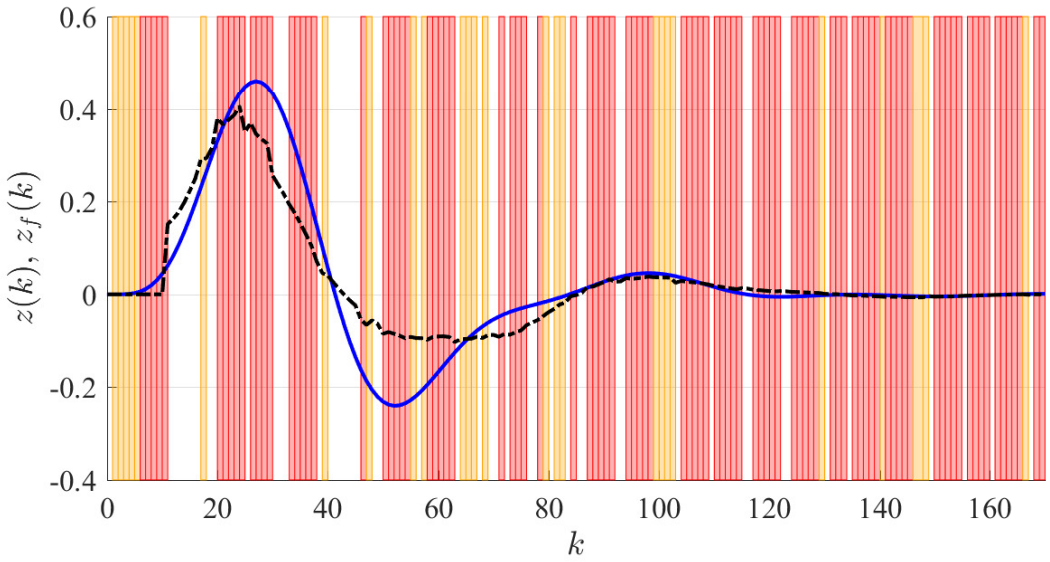

Figure 5.3: $z(k)$ (—) and $z_f(k)$ (- - -) with the mode-dependent filter considering a different randomly selected ξ_k for each time instant. $\alpha = \begin{bmatrix} 0.5234 & 0.4766 \end{bmatrix}$ and $\eta(0)$ is null. Transmission failures are depicted in orange and DoS attacks in red.

The values of $y(k)$ (—) and $y_m(k)$ (- - -) of the previous case are then displayed in Figure 5.4 to illustrate how the attack impacts the measured output that arrives at the filter.

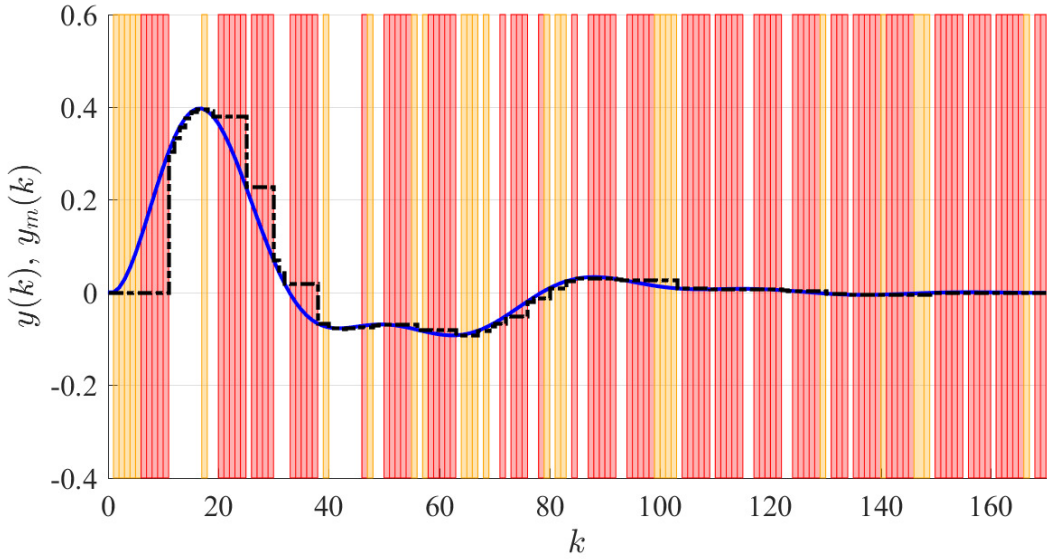

Figure 5.4: $y(k)$ (—) and $y_m(k)$ (- - -) considering a different randomly selected ξ_k for each time instant. $\alpha = \begin{bmatrix} 0.5234 & 0.4766 \end{bmatrix}$ and $\eta(0)$ is null. Transmission failures are depicted in orange and DoS attacks in red.

5.4 FINAL REMARKS

This chapter presented parameter-dependent LMI conditions to design mode-dependent and mode-independent full-order filters considering the $\mathscr{H}_\infty$ cost for discrete-time CPSs with time-invariant polytopic uncertainties and in an unreliable network subject to DoS attacks. The proposed method utilizes parameter-dependent slack variables in order to obtain less conservative results. The network model utilized is the one proposed in Section 2.4, which is created using a non-homogeneous Markov chain that contains uncertain and unknown transition probabilities combined with a finite state chain that accounts for the deterministic assumption of the attacker's energetic limitations. Numerical tests illustrated the method performance, and that a high probability of longer attacks affects the $\mathscr{H}_\infty$ cost more than accounting for larger numbers of maximum consecutive attacks. Moreover, comparisons showed that utilizing a Gilbert-Elliot model instead of the proposed one returned more conservative results, or even resulted in unfeasible problems.

6

CONCLUSIONS AND POSSIBLE FUTURE DIRECTIONS

This work has proposed new Linear Matrix Inequalities (LMI) conditions for the state-feedback control design of discrete-time Cyber-Physical Systems (CPSs) with polytopic uncertainties with the presence of exogenous disturbances and Denial of Service attacks (DoS attacks) from an attacker with energetic constraints. A packet-based approach based on three different strategies was considered. At the first moment, only the attacks were taken into account, with the closed-loop system being modeled as an uncertain switched system.

In the sequel, a new Markovian network model was proposed to model both stochastic transmission failures due to network limitations and energy-bounded DoS attacks, both in the context of an unreliable network. The proposed model was constructed upon a non-homogeneous Markov chain with a finite number of states (reflecting the energetic limitations of the attacker) and uncertain and unknown probabilities that are modeled after time-varying parameters, aiming to easily encompass a wider array of more or less conservative scenarios. Moreover, accounting for the proposed network model, the problems of state-feedback control and filter design were tackled, both with mode-dependent and mode-independent strategies.

Several numerical experiments were conducted to test the design methods, and many conclusions could be drawn from the different strategies employed, both in what concerns performance as well as numerical complexity in the design stage. The proposed control methods and strategies were able to guarantee stability, while the filter design technique provided satisfactory performance even in scenarios where the network operation was more precarious. Furthermore, tests were made comparing the suggested network model with a traditional network model with packet loss from the literature, which resulted in promising evidence that the proposed model is relatively less conservative, more versatile, and more adequate to model the approached problem.

6.1 FUTURE DIRECTIONS

- **Event-based control strategies**: Event-based control strategies can be employed in a network subjected to DoS attacks and stochastic packet losses in order to reduce packet transmission rates and mitigate the attacker impact in the system. Some works have shown them to be a promising technique in this sort of problem [115].
- **Fault-tolerant control**: Fault-tolerant control may be employed to mitigate the impact of the packet losses, more specifically, techniques based on Fault Hiding [116, 117]. These techniques do not require changing the controller structure or design, as they, instead, insert reconfiguration blocks (virtual sensors and/or virtual actuators) in the link sensor/controller and/or controller/actuator seeking to maintain the system performance and stability during an attack or transmission failure. In [118], for instance, virtual actuators

were utilized against DoS attacks in the controller/actuator network. However, there is more to explore in this approach like, for instance, considering the simultaneous use of virtual sensors and actuators [119] in the problem addressed in this dissertation.

- **Data-driven control**: Data-driven techniques may be applied to obtain model-free control design methods. This would reduce the necessity for precise knowledge of both system and network models to design effective control strategies. Works like [120–122] have provided some steps in this path.

6.2 PUBLICATIONS

The publications with the contributions found in this manuscript are listed below

(i) **P. M. Oliveira**, J. M. Palma, M. J. Lacerda, "$\mathscr{H}_2$ state-feedback control for discrete-time cyber-physical uncertain systems under DoS attacks", In *Applied Mathematics and Computation*, vol 452, pp. 127091, (2022).

(ii) **P. M. Oliveira**, J. M. Palma, M. J. Lacerda, "Control Design for Cyber-physical uncertain systems under Unreliable Markovian Network Susceptible to Denial-of-Service Attacks".

(iii) **P. M. Oliveira**, J. M. Palma, M. J. Lacerda, "Filter design for Cyber-physical systems against DoS attacks and unreliable networks: A Markovian approach".

Where (ii) and (iii) are under revision. Additional publications concerning related topics, and that were developed during the Master's research, are listed in the sequel

(i) **P. M. Oliveira**, J. M. Palma, E.G. Nepomuceno, M. J. Lacerda, "Reinforcement learning for control design of uncertain polytopic systems", In *Information Sciences*, vol 625, pp. 417-429, (2023).

(ii) M. J. Lacerda, **P. M. Oliveira** and J. M. Palma, "Control design for cyber-physical systems under DoS attacks", In *2022 IEEE International Conference on Automation/XXV Congress of the Chilean Association of Automatic Control (ICA-ACCA)*, Curicó, Chile, pp. 1-6 (2022).

(iii) R. Fuentes, **P. M. Oliveira**, L. P. Carvalho, M. J. Lacerda, J. M. Palma, "Autonomous Vehicle Platoon Packet-Based Control Problem Under Denial-of-Service Attacks", In *CONTROLO 2022: Proceedings of the 15th APCA International Conference on Automatic Control and Soft Computing*, Caparica, Portugal. Cham: Springer International Publishing, p. 474-486 (2022).

(iv) **P. M. Oliveira**, P. S. P. Pessim, J. M. Palma, M. J. Lacerda, "Reference tracking control for cyber-physical systems under DoS attacks", In *2021 IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, Valparaíso, Chile, p. 1-6 (2021).

(v) **P. M. Oliveira**, R. C. L. F. Oliveira, J. M. Palma, M. J. Lacerda, "State-feedback memory control for uncertain cyber-physical systems under Denial-of-Service attacks" In *Proceedings of the 22nd IFAC World Congress*, Yokohama, Japan (2023).

Where (v) has been accepted, but not yet published.

BIBLIOGRAPHY

[1] D. B. Rawat, J. J. Rodrigues, and I. Stojmenovic. *Cyber-Physical Systems: From Theory to Practice*. CRC Press, 2015.

[2] E. A. Lee. "Cyber physical systems: Design challenges." In: *2008 11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC)*. IEEE. 2008, pp. 363–369.

[3] R. Alur. *Principles of Cyber-Physical Systems*. MIT Press, 2015.

[4] D. P. Möller. *Guide to Computing Fundamentals in Cyber-Physical Systems: Concepts, Design Methods, and Applications*. Springer, 2016.

[5] E. A. Lee. "The past, present and future of cyber-physical systems: A focus on models." In: *Sensors* 15.3 (2015), pp. 4837–4869.

[6] N. Wiener. *Cybernetics or Control and Communication in the Animal and the Machine*. 2nd. revised ed. MIT press, 1961.

[7] Y. Lu. "Cyber physical system (CPS)-based industry 4.0: A survey." In: *Journal of Industrial Integration and Management* 2.03 (2017), p. 1750014.

[8] B. Dafflon, N. Moalla, and Y. Ouzrout. "The challenges, approaches, and used techniques of CPS for manufacturing in Industry 4.0: a literature review." In: *The International Journal of Advanced Manufacturing Technology* 113 (2021), pp. 2395–2412.

[9] S. A. Haque, S. M. Aziz, and M. Rahman. "Review of Cyber-Physical System in Healthcare." In: *International Journal of Distributed Sensor Networks* 10.4 (2014), p. 217415. DOI: 10.1155/2014/217415.

[10] Q. Wang, G. Zhang, and F. Wen. "A survey on policies, modelling and security of cyber-physical systems in smart grids." In: *Energy Conversion and Economics* 2.4 (2021), pp. 197–211.

[11] C.-S. Shih, J.-J. Chou, N. Reijers, and T.-W. Kuo. "Designing CPS/IoT applications for smart buildings and cities." In: *IET Cyber-Physical Systems: Theory & Applications* 1.1 (2016), pp. 3–12.

[12] J. Wang, J. Liu, and N. Kato. "Networking and communications in autonomous driving: A survey." In: *IEEE Communications Surveys & Tutorials* 21.2 (2018), pp. 1243–1274.

[13] H. Chen. "Applications of Cyber-Physical System: A Literature Review." In: *Journal of Industrial Integration and Management* 02.03 (2017), p. 1750012. DOI: 10.1142/S2424862217500129.

[14] M. S. Mahmoud and M. M. Hamdan. "Fundamental issues in networked control systems." In: *IEEE/CAA Journal of Automatica Sinica* 5.5 (2018), pp. 902–922.

[15] A. Shrivastava, P. Derler, Y.-S. L. Baboud, K. Stanton, M. Khayatian, H. A. Andrade, M. Weiss, J. Eidson, and S. Chandhoke. "Time in cyber-physical systems." In: *Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis*. 2016, pp. 1–10.

[16] L. Schenato. "To zero or to hold control inputs with lossy links?" In: *IEEE Transactions on Automatic Control* 54.5 (2009), pp. 1093–1099.

[17] A. M. de Oliveira, V. S. Varma, R. Postoyan, I.-C. Morărescu, J. Daafouz, and O. L. Costa. "Network-aware design of state-feedback controllers for linear wireless networked control systems." In: *IFAC-PapersOnLine* 51.16 (2018), pp. 205–210.

[18] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang. "A survey on security control and attack detection for industrial cyber-physical systems." In: *Neurocomputing* 275 (2018), pp. 1674 –1683. DOI: https://doi.org/10.1016/j.neucom.2017.10.009.

[19] M. N. Al-Mhiqani, R. Ahmad, W. Yassin, A. Hassan, Z. Z. Abidin, N. S. Ali, and K. H. Abdulkareem. "Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems." In: *International Journal of Advanced Computer Science and Applications* 9.1 (2018). DOI: 10.14569/IJACSA.2018.090169.

[20] Y. Ashibani and Q. H. Mahmoud. "Cyber physical systems security: Analysis, challenges and solutions." In: *Computers & Security* 68 (2017), pp. 81 –97. DOI: https://doi.org/10.1016/j.cose.2017.04.005.

[21] M. Long, C.-H. Wu, and J. Y. Hung. "Denial of service attacks on network-based control systems: impact and mitigation." In: *IEEE Transactions on Industrial Informatics* 1.2 (2005), pp. 85–96.

[22] I. Ortega-Fernandez and F. Liberati. "A Review of Denial of Service Attack and Mitigation in the Smart Grid Using Reinforcement Learning." In: *Energies* 16.2 (2023), p. 635.

[23] D. Ding, Q. L. Han, X. Ge, and J. Wang. "Secure State Estimation and Control of Cyber-Physical Systems: A Survey." In: *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 51.1 (2021), pp. 176–190. DOI: 10.1109/TSMC.2020.3041121.

[24] L. Li, W. Wang, Q. Ma, K. Pan, X. Liu, L. Lin, and J. Li. "Cyber attack estimation and detection for cyber-physical power systems." In: *Applied Mathematics and Computation* 400 (2021), p. 126056.

[25] F. Pasqualetti, F. Dörfler, and F. Bullo. "Attack detection and identification in cyber-physical systems." In: *IEEE transactions on automatic control* 58.11 (2013), pp. 2715–2729.

[26] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell. "A survey of physics-based attack detection in cyber-physical systems." In: *ACM Computing Surveys (CSUR)* 51.4 (2018), pp. 1–36.

[27] J. Qin, M. Li, L. Shi, and X. Yu. "Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks." In: *IEEE Transactions on Automatic Control* 63.6 (2017), pp. 1648–1663.

[28] Z. Zhang, R. Deng, P. Cheng, and Q. Wei. "On feasibility of coordinated time-delay and false data injection attacks on cyber–physical systems." In: *IEEE Internet of Things Journal* 9.11 (2021), pp. 8720–8736.

[29] D. Zhang, Q.-G. Wang, G. Feng, Y. Shi, and A. V. Vasilakos. "A survey on attack detection, estimation and control of industrial cyber–physical systems." In: *ISA Transactions* (2021). ISSN: 0019-0578. DOI: https://doi.org/10.1016/j.isatra.2021.01.036.

[30] D. Wang, Z. Wang, B. Shen, F. E. Alsaadi, and T. Hayat. "Recent advances on filtering and control for cyber-physical systems under security and resource constraints." In: *Journal of the Franklin Institute* 353.11 (2016), pp. 2451–2466. DOI: https://doi.org/10.1016/j.jfranklin.2016.04.011.

[31] D. Ding, Q.-L. Han, Z. Wang, and X. Ge. "A survey on model-based distributed control and filtering for industrial cyber-physical systems." In: *IEEE Transactions on Industrial Informatics* 15.5 (2019), pp. 2483–2499.

[32] A. R. Fioravanti, A. P. C. Gonçalves, and J. C. Geromel. "Filter inputs with Markovian lossy links: Zero or hold?" In: *Proceedings of the 9th IEEE International Conference on Control and Automation (ICCA)*. Santiago, Chile, 2011, pp. 656–661.

[33] A. R. C. Serafini, L. Delforno, J. M. Palma, F. H. Behrens, and C. F. Morais. "Robust Static Output-Feedback Control for MJLS with Non-Homogeneous Markov Chains: A Comparative Study Considering a Wireless Sensor Network with Time-Varying PER." In: *Sensors* 21.19 (2021).

[34] J. M. Palma, C. F. Morais, and R. C. Oliveira. "$\mathscr{H}_\infty$ state-feedback gain-scheduled control for MJLS with non-homogeneous Markov chains." In: *2018 Annual American Control Conference (ACC)*. IEEE. 2018, pp. 5718–5723.

[35] W.-A. Zhang, L. Yu, and H. Song. "$\mathscr{H}_\infty$ filtering of networked discrete-time systems with random packet losses." In: *Information Sciences* 179.22 (2009), pp. 3944–3955.

[36] S. Lai, B. Chen, T. Li, and L. Yu. "Packet-Based State Feedback Control Under DoS Attacks in Cyber-Physical Systems." In: *IEEE Transactions on Circuits and Systems II: Express Briefs* 66.8 (2019), pp. 1421–1425. DOI: 10.1109/TCSII.2018.2881984.

[37] P. S. Pessim and M. J. Lacerda. "On the robustness of cyber-physical LPV systems under DoS attacks." In: *Journal of the Franklin Institute* 359.2 (2022), pp. 677–696.

[38] M. Yu, L. Wang, G. Xie, and T. Chu. "Stabilization of networked control systems with data packet dropout via switched system approach." In: *2004 IEEE International Conference on Robotics and Automation*. 2004, pp. 362–367. DOI: 10.1109/CACSD.2004.1393903.

[39] P. S. P. Pessim. "Control design for Cyber-Physical LPV Systems under DoS Attacks: A packet-based approach." M.Sc. Thesis. São João del-Rei, MG: Universidade Federal de São João del-Rei (UFSJ), 2021.

[40] P. S. P. Pessim and M. J. Lacerda. "State-feedback control for Cyber-physical LPV systems under DoS attacks." In: *IEEE Control Systems Letters* 5.3 (2021), pp. 1043–1048.

[41] P. S. Pessim, M. L. Peixoto, R. M. Palhares, and M. J. Lacerda. "Static output-feedback control for Cyber-physical LPV systems under DoS attacks." In: *Information Sciences* 563 (2021), pp. 241–255.

[42] Y. Liu. "Secure control of networked switched systems with random DoS attacks via event-triggered approach." In: *International Journal of Control, Automation and Systems* 18.10 (2020), pp. 2572–2579.

[43] H. Zhao, Y. Niu, and J. Zhao. "Event-triggered sliding mode control of uncertain switched systems under denial-of-service attacks." In: *Journal of the Franklin Institute* 356.18 (2019), pp. 11414 –11433.

[44] S. Liu, S. Li, and B. Xu. "Event-triggered resilient control for cyber-physical system under denial-of-service attacks." In: *International Journal of Control* 93.8 (2020), pp. 1907–1919.

[45] G. K. Befekadu, V. Gupta, and P. J. Antsaklis. "Risk-sensitive control under Markov modulated denial-of-service (DoS) attack strategies." In: *IEEE Transactions on Automatic Control* 60.12 (2015), pp. 3299–3304.

[46] M. Wang and B. Xu. "Observer-based guaranteed cost control of Cyber-Physical Systems under DoS jamming attacks." In: *European Journal of Control* 48 (2019), pp. 21 –29. DOI: https://doi.org/10.1016/j.ejcon.2019.01.003.

[47] Y. Zhu and W. X. Zheng. "Observer-Based Control for Cyber-Physical Systems With Periodic DoS Attacks Via A Cyclic Switching Strategy." In: *IEEE Transactions on Automatic Control* 65.8 (2020), pp. 3714–3721. DOI: 10.1109/TAC.2019.2953210.

[48] M. Peixoto, P. Pessim, M. Lacerda, and R. Palhares. "Stability and stabilization for LPV systems based on Lyapunov functions with non-monotonic terms." In: *Journal of the Franklin Institute* 357.11 (2020), pp. 6595–6614. DOI: 10.1016/j.jfranklin.2020.04.019.

[49] M. C. de Oliveira, J. Bernussou, and J. C. Geromel. "A new discrete-time robust stability condition." In: *Systems & Control Letters* 37.4 (1999), pp. 261–265.

[50] L. Hetel, J. Daafouz, and C. Iung. "Stabilization of arbitrary switched linear systems with unknown time-varying delays." In: *IEEE Transactions on Automatic Control* 51 (10 2006), pp. 1668–1674.

[51] P. J. de Oliveira, R. C. L. F. Oliveira, and P. L. D. Peres. "A new LMI condition for robust stability of polynomial matrix polytopes." In: *IEEE Transactions on Automatic Control* 47.10 (2002), pp. 1775–1779.

[52] M. J. Lacerda and P. Seiler. "Stability of uncertain systems using Lyapunov functions with non-monotonic terms." In: *Automatica* 82 (2017), pp. 187–193. DOI: https://doi.org/10.1016/j.automatica.2017.04.042.

[53] S. Aberkane. "Stochastic stabilization of a class of nonhomogeneous Markovian jump linear systems." In: *Systems & Control Letters* 60.3 (2011), pp. 156–160.

[54] S. Aberkane. "Bounded real lemma for nonhomogeneous Markovian jump linear systems." In: *IEEE Transactions on Automatic Control* 58.3 (2012), pp. 797–801.

[55] V. Dragan, T. Morozan, and A.-M. Stoica. *Mathematical methods in robust control of discrete-time linear stochastic systems*. Springer, 2010.

[56] A. Cetinkaya, H. Ishii, and T. Hayakawa. "Networked control under random and malicious packet losses." In: *IEEE Transactions on Automatic Control* 62.5 (2016), pp. 2434–2449.

[57] E. N. Gilbert. "Capacity of a burst-noise channel." In: *Bell system technical journal* 39.5 (1960), pp. 1253–1265.

[58] E. O. Elliott. "Estimates of error rates for codes on burst-noise channels." In: *The Bell System Technical Journal* 42.5 (1963), pp. 1977–1997.

[59] Z. S. Duan, J. X. Zhang, C. S. Zhang, and E. Mosca. "Robust $\mathscr{H}_2$ and $\mathscr{H}_\infty$ filtering for uncertain linear systems." In: *Automatica* 42.11 (2006), pp. 1919–1926.

[60] M. J. Lacerda, R. C. L. F. Oliveira, and P. L. D. Peres. "Robust $\mathscr{H}_2$ and $\mathscr{H}_\infty$ filter design for uncertain linear systems via LMIs and polynomial matrices." In: *Signal Processing* 91.5 (2011), pp. 1115–1122.

[61] C. F. Morais, M. F. Braga, M. J. Lacerda, R. C. L. F. Oliveira, and P. L. D. Peres. "$\mathscr{H}_2$ and $\mathscr{H}_\infty$ Filter Design for Polytopic Continuous-time Markov Jump Linear Systems with Uncertain Transition Rates." In: *International Journal of Adaptive Control and Signal Processing* (2014). to appear.

[62] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan. *Linear Matrix Inequalities in System and Control Theory*. Philadelphia, PA: SIAM Studies in Applied Mathematics, 1994.

[63] I. R. Petersen and D. C. McFarlane. "Optimal guaranteed cost control and filtering for uncertain linear systems." In: *IEEE Transactions on Automatic Control* 39.9 (1994), pp. 1971–1977.

[64] P. Shi, E. K. Boukas, and R. K. Agarwal. "Control of Markovian jump discrete-time systems with norm bounded uncertainty and unknown delay." In: *IEEE Transactions on Automatic Control* 44.11 (1999), pp. 2139–2144.

[65] P. Gahinet, P. Apkarian, and M. Chilali. "Affine parameter-dependent Lypunov functions for real parametric uncertainty." In: *Proceedings of the 33rd IEEE Conference on Decision and Control*. Lake Buena Vista, FL, USA, 1994, pp. 2026–2031.

[66] N. Aouani, S. Salhi, G. Garcia, and M. Ksouri. "Robust control analysis and synthesis for LPV systems under affine uncertainty structure." In: *6th International Multi-Conference on Systems, Signals and Devices (SSD 2009)*. Djerba , Tunisia, 2009.

[67] R. E. Moore. *Interval analysis*. Vol. 4. Prentice-Hall Englewood Cliffs, 1966.

[68] R. E. Moore. *Methods and applications of interval analysis*. SIAM, 1979.

[69] Z. Qiu, P. C. Müller, and A. Frommer. "Ellipsoidal set-theoretic approach for stability of linear state-space models with interval uncertainty." In: *Mathematics and computers in simulation* 57.1-2 (2001), pp. 45–59.

[70] G. S. Zhai, H. Lin, and P. J. Antsaklis. "Quadratic stabilizability of switched linear systems with polytopic uncertainties." In: *International Journal of Control* 76.7 (2003), pp. 747–753.

[71] J. Dong and G.-H. Yang. "Robust static output feedback control for linear discrete-time systems with time-varying uncertainties." In: *Systems & Control Letters* 57.2 (2008), pp. 123–131.

[72] J. De Caigny, J. F. Camino, R. C. L. F. Oliveira, P. L. D. Peres, and J. Swevers. "Gain-scheduled $\mathscr{H}_2$ and $\mathscr{H}_\infty$ control of discrete-time polytopic time-varying systems." In: *IET Control Theory & Applications* 4.3 (2010), pp. 362–380. DOI: 10.1049/iet-cta.2008.0364.

[73] P. S. P. Pessim, V. J. S. Leite, and M. J. Lacerda. "Robust performance for uncertain systems via Lyapunov functions with higher order terms." In: *Journal of The Franklin Institute* 356.5 (2019), pp. 3139–3156. DOI: https://doi.org/10.1016/j.jfranklin.2019.02.004.

[74] L. Hetel, J. Daafouz, and C. Iung. "Robust stability analysis and control design for switched uncertain polytopic systems." In: *Proceedings of the 5th IFAC Symposium on Robust Control Design (ROCOND 2006)*. Toulouse, France, 2006, pp. 166–171. DOI: https://doi.org/10.3182/20060705-3-FR-2907.00030.

[75] L. d. P. Carvalho, A. M. de Oliveira, and O. L. d. V. Costa. "Mixed fault detection filter for Markovian jump linear systems." In: *Mathematical Problems in Engineering* 2018 (2018).

[76] M. J. Lacerda, E. S. Tognetti, R. C. L. F. Oliveira, and P. L. D. Peres. "A new approach to handle additive and multiplicative uncertainties in the measurement for $\mathscr{H}_\infty$ LPV filtering." In: *International Journal of Systems Science* 47.5 (2016), pp. 1042–1053. DOI: https://doi.org/10.1080/00207721.2014.911389.

[77] M. J. Lacerda, P. M. Oliveira, and J. M. Palma. "Control design for cyber-physical systems under DoS attacks." In: *2022 IEEE International Conference on Automation/XXV Congress of the Chilean Association of Automatic Control (ICA-ACCA)*. IEEE. 2022, pp. 1–6.

[78] A. Benzaouia. *Saturated switching systems*. Vol. 426. Springer Science & Business Media, 2012.

[79] Z. Sun and S. S. Ge. *Stability Theory of Switched Dynamical Systems*. Springer-Verlag London, 2011. DOI: 10.1007/978-0-85729-256-8.

[80] M. J. Lacerda and T. d. S. Gomide. "Stability and stabilisability of switched discrete-time systems based on structured Lyapunov functions." In: *IET Control Theory & Applications* 14.5 (2020), pp. 781–789.

[81] D. Liberzon. *Switching in Systems and Control*. Systems and Control: Foundations and Applications. Boston, MA: Birkhäuser, 2003.

[82] M. J. Lacerda and C. M. Agulhari. "Stability analysis of discrete-time LPV switched systems." In: *IFAC-PapersOnLine* 53.2 (2020). 21th IFAC World Congress, pp. 6145–6150. DOI: https://doi.org/10.1016/j.ifacol.2020.12.1695.

[83] C. M. Agulhari, A. Felipe, R. C. L. F. Oliveira, and P. L. D. Peres. "Algorithm 998: The Robust LMI Parser — A toolbox to construct LMI conditions for uncertain systems." In: *ACM Transactions on Mathematical Software* 45.3 (2019), 36:1–36:25.

[84] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu. "A survey of recent results in networked control systems." In: *Proceedings of the IEEE* 95.1 (2007), pp. 138–162.

[85] M. F. Braga, C. F. Morais, E. S. Tognetti, R. C. L. F. Oliveira, and P. L. D. Peres. "Discretisation and control of polytopic systems with uncertain sampling rates and network-induced delays." In: *International Journal of Control* 87.11 (2014), pp. 2398–2411.

[86] J. M. Palma, L. de Paula Carvalho, T. E. Rosa, C. de Freitas Morais, and R. C. Oliveira. "$\mathscr{H}_2$ and $\mathscr{H}_\infty$ state-feedback control through multi-hop networks: Trade-off analysis between the network load and performance degradation." In: *IEEE Latin America Transactions* 16.9 (2018), pp. 2377–2384.

[87] O. L. V. Costa, M. D. Fragoso, and R. P. Marques. *Discrete-Time Markovian Jump Linear Systems*. New York, NY, USA: Springer-Verlag, 2005.

[88] P. Almström, M. Rabi, and M. Johansson. "Networked state estimation over a Gilbert-Elliot type channel." In: *Proceedings of the 48h IEEE Conference on Decision and Control (CDC) held jointly with 2009 28th Chinese Control Conference*. IEEE. 2009, pp. 2711–2716.

[89] D. Zhai, L. An, J. Li, and Q. Zhang. "Stabilisation of discrete-time piecewise homogeneous Markov jump linear system with imperfect transition probabilities." In: *Mathematical Problems in Engineering* 2015 (2015).

[90] L. Zhang. "$\mathscr{H}_\infty$ estimation for discrete-time piecewise homogeneous Markov jump linear systems." In: *Automatica* 45.11 (2009), pp. 2570–2576.

[91] C. F. Morais, M. F. Braga, R. C. L. F. Oliveira, and P. L. D. Peres. "$\mathscr{H}_2$ control of discrete-time Markov jump linear systems with uncertain transition probability matrix: Improved linear matrix inequality relaxations and multi-simplex modeling." In: *IET Control Theory & Applications* 7 (2013), pp. 1665–1674.

[92] A. P. C. Gonçalves, A. R. Fioravanti, and J. C. Geromel. "$\mathscr{H}_\infty$ robust and networked control of discrete-time MJLS through LMIs." In: *Journal of The Franklin Institute* 349.6 (2012), pp. 2171–2181.

[93] A. Cetinkaya, H. Ishii, and T. Hayakawa. "The effect of time-varying jamming interference on networked stabilization." In: *SIAM Journal on Control and Optimization* 56.3 (2018), pp. 2398–2435.

[94] W. Xu, W. Trappe, Y. Zhang, and T. Wood. "The feasibility of launching and detecting jamming attacks in wireless networks." In: *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. 2005, pp. 46–57.

[95] C. F. Morais, M. F. Braga, R. C. L. F. Oliveira, and P. L. D. Peres. "Robust state feedback control for discrete-time linear systems via LMIs with a scalar parameter." In: *Proceedings of the 2013 American Control Conference*. Washington, DC, USA, 2013, pp. 3876–3881.

[96] A. P. C. Gonçalves, A. R. Fioravanti, and J. C. Geromel. "Filtering of discrete-time Markov jump linear systems with uncertain transition probabilities." In: *International Journal of Robust and Nonlinear Control* 21.6 (2011), pp. 613–624.

[97] Y. Ji and H. J. Chizeck. "Jump linear quadratic Gaussian control: steady-state and testable conditions." In: *Control Theory and Advanced Technology* 6 (1990), pp. 289–319.

[98] Y. Ji, H. J. Chizeck, X. Feng, and K. A. Loparo. "Stability and control of discrete-time jump linear systems." In: *Control Theory and Advanced Technology* 7 (1991), pp. 247–270.

[99] O. L. V. Costa and M. D. Fragoso. "Stability results for discrete-time linear systems with Markovian jumping parameters." In: *Journal of Mathematical Analysis and Applications* 179 (1993), pp. 154–178.

[100] J. Daafouz and J. Bernussou. "Parameter dependent Lyapunov functions for discrete time systems with time varying parameter uncertainties." In: *Systems & Control Letters* 43.5 (2001), pp. 355–359. DOI: https://doi.org/10.1016/S0167-6911(01)00118-9.

[101] M. C. de Oliveira. "Novos testes de estabilidade para sistemas lineares." In: *Sba: Controle & Automação Sociedade Brasileira de Automatica* 15 (2004), pp. 17–23.

[102] R. E. Skelton, T. Iwasaki, and K. Grigoriadis. *A Unified Algebraic Approach to Linear Control Design*. Bristol, PA: Taylor & Francis, 1998.

[103] C. E. de Souza, A. Trofino, and K. A. Barbosa. "Mode-independent $\mathscr{H}_\infty$ filters for Markovian jump linear systems." In: *IEEE Transactions on Automatic Control* 51.11 (2006), pp. 1837–1841.

[104] M. C. de Oliveira and R. E. Skelton. "Stability tests for constrained linear systems." In: *Perspectives in Robust Control*. Ed. by S. O. Reza Moheimani. Vol. 268. Lecture Notes in Control and Information Science. New York, NY: Springer-Verlag, 2001, pp. 241–257.

[105] J. Löfberg. "YALMIP: A toolbox for modeling and optimization in MATLAB." In: *Proceedings of the 2004 IEEE International Symposium on Computer Aided Control Systems Design*. Taipei, Taiwan, 2004, pp. 284–289. DOI: 10.1109/CACSD.2004.1393890.

[106] E. D. Andersen and K. D. Andersen. "The MOSEK Interior Point Optimizer for Linear Programming: An Implementation of the Homogeneous Algorithm." English. In: *High Performance Optimization*. Ed. by H. Frenk, K. Roos, T. Terlaky, and S. Zhang. Vol. 33. Applied Optimization. Springer US, 2000, pp. 197–232. ISBN: 978-1-4419-4819-9.

[107] E. Gershon and U. Shaked. "Static $\mathscr{H}_2$ and $\mathscr{H}_\infty$ output-feedback of discrete-time LTI systems with state multiplicative noise." In: *Systems & Control Letters* 55.3 (2006), pp. 232–239.

[108] W. Xie. "An equivalent LMI representation of Bounded Real Lemma for continuous-time systems." In: *Journal of Inequalities and Applications* 2008.1 (2008), pp. 1–8.

[109] U. Shaked. "Improved LMI representations for the analysis and the design of continuous-time systems with polytopic type uncertainty." In: *IEEE Transactions on Automatic Control* 46.4 (2001), pp. 652–656.

[110] C. Hu and I. M. Jaimoukha. "Robust $\mathscr{H}_2$ and $\mathscr{H}_\infty$ State Feedback Control for Discrete-time Polytopic Systems Using an Iterative LMI Based Procedure." In: *2020 European Control Conference (ECC)*. IEEE. 2020, pp. 621–626.

[111] M. C. de Oliveira, J. C. Geromel, and J. Bernussou. "Extended $\mathscr{H}_2$ and $\mathscr{H}_\infty$ characterization and controller parametrizations for discrete-time systems." In: *International Journal of Control* 75.9 (2002), pp. 666–679.

[112] C. M. Agulhari, A. Felipe, R. C. L. F. Oliveira, and P. L. D. Peres. "Algorithm 998: The Robust LMI Parser - A Toolbox to Construct LMI Conditions for Uncertain Systems." In: *ACM Transactions on Mathematical Software* 45.3 (2019), 36:1–36:25. DOI: https://doi.org/10.1145/3323925.

[113] R. A. Borges, V. F. Montagner, R. C. L. F. Oliveira, P. L. D. Peres, and P.-A. Bliman. "Parameter-dependent $\mathscr{H}_2$ and $\mathscr{H}_\infty$ filter design for linear systems with arbitrarily time-varying parameters in polytopic domains." In: *Signal Processing* 88.7 (2008), pp. 1801–1816.

[114] D. H. Lee, Y. H. Joo, and M. H. Tak. "Periodically time-varying $\mathscr{H}_\infty$ memory filter design for discrete-time LTI systems with polytopic uncertainty." In: *IEEE Transactions on Automatic Control* 59.5 (2014), pp. 1380–1385.

[115] V. Dolk, P. Tesi, C. De Persis, and W. Heemels. "Event-triggered control systems under denial-of-service attacks." In: *IEEE Transactions on Control of Network Systems* 4.1 (2016), pp. 93–105.

[116] T. Steffen. *Control reconfiguration of dynamical systems: linear approaches and structural tests*. Vol. 320. Springer Science & Business Media, 2005.

[117] J. H. Richter. *Reconfigurable control of nonlinear dynamical systems: a fault-hiding approach*. Vol. 408. Springer, 2011.

[118] D. Rotondo, H. S. Sánchez, V. Puig, T. Escobet, and J. Quevedo. "A virtual actuator approach for the secure control of networked LPV systems under pulse-width modulated DoS attacks." In: *Neurocomputing* 365 (2019), pp. 21 –30. ISSN: 0925-2312.

[119] M. M. Quadros, I. V. de Bessa, V. J. S. Leite, and R. M. Palhares. "Fault tolerant control for LPV systems: An improved robust virtual actuator and sensor approach." In: *ISA Transactions* 104 (2020), pp. 356–369.

[120] Z. Li, L. Zhu, Z. Wang, and W. Che. "Data-Driven Event-Triggered Platoon Control under Denial-of-Service Attacks." In: *Mathematics* 10.21 (2022), p. 3985.

[121] W. Liu, J. Sun, G. Wang, and J. Chen. "A Resilient Data-Driven Controller Against DoS Attacks." In: *2022 41st Chinese Control Conference (CCC)*. IEEE. 2022, pp. 4305–4310.

[122] W. Che, C. Deng, and D. Liu. "Data-driven-based distributed security control for vehicle-following platoon." In: *2020 IEEE 9th Data Driven Control and Learning Systems Conference (DDCLS)*. IEEE. 2020, pp. 1109–1113.