Received: 6 February 2024 | Revised: 14 May 2024 | Accepted: 28 May 2024

DOI: 10.1049/cth2.12703

IET Control Theory & Applications

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Filter design for cyber-physical systems against DoS attacks and unreliable networks: A Markovian approach

Pedro M. Oliveira[1] | **Jonathan M. Palma**[2] | **Márcio J. Lacerda**[3]

[1]Graduate Program in Electrical Engineering, Federal University of Minas Gerais, Belo Horizonte, Brazil

[2]Faculty of Engineering, Universidad de Talca, Curicó, Chile

[3]Centre for Communications Technology, School of Computing and Digital Media, London Metropolitan University, London, UK

Correspondence
Márcio J. Lacerda, Centre for Communications Technology, School of Computing and Digital Media, London Metropolitan University, London, UK.
Email: m.lacerda@londonmet.ac.uk

Funding information
Conselho Nacional de Desenvolvimento Científico e Tecnológico, Grant/Award Number: 315538/2021-0; Fundação de Amparo à Pesquisa do Estado de Minas Gerais, Grant/Award Number: PAPG-13121; Fondo Nacional de Desarrollo Científico y Tecnológico, Grant/Award Number: 11201049; Agencia Nacional de Investigación y Desarrollo, Grant/Award Number: 1241305

Abstract

This article proposes a novel approach for designing a mode-dependent $\mathcal{H}_\infty$ full-order dynamic filter for a cyber-physical system (CPS) that is subject to polytopic uncertainties. The CPS operates on an unreliable network that is susceptible to transmission failures and Denial of Service (DoS) attacks. The attackers have limited energy resources, and the duration of the DoS attack is limited to a maximum number of consecutive time instants. The network is modeled after a proposed non-homogeneous Markov chain whose transition probability matrix may feature uncertain and unknown probabilities, which are dependent on time-varying parameters. The design conditions for the filter are obtained using parameter-dependent linear matrix inequalities. The proposed filter is shown to be effective in reducing the impact of DoS attacks and transmission failures on the CPS. Numerical experiments are presented to illustrate the efficacy of the proposed filter design method, demonstrating its ability to mitigate the effects of uncertainties and attacks on the CPS.

1 | INTRODUCTION

In the last decades, the way devices communicate has evolved significantly, allowing the connection of physical and computational components through networks. This integration has given rise to a new class of systems called cyber-physical systems (CPS) [1]. However, this new class also posed new challenges for control systems, including the existence of malicious agents that seek to deteriorate the performance of CPS. As a result, the study of CPS under the presence of attacks has received a lot of attention from the control community [2, 3]. The main types of attacks are: the false data injection [4, 5], deception [6], and Denial of Service (DoS) attacks [6], with the latter being of particular interest because it does not need any information from the system to be effective, since it can be performed by simply launching a lot of information into the communication channels trying to block it [7].

Strategies considering deterministic and stochastic approaches for modeling the presence of DoS attacks have emerged. For instance, in the deterministic framework, state-feedback control [8, 9], and output feedback control [10] were considered by employing a switching model for the CPS in the presence of attacks, that departs from the assumption that the malicious agent is energetically bounded [11], which may constraint the maximum attack duration [8] or, as seen in [12], limits the number of communication channels affected at the same time. Event-based strategies are also utilized to tackle DoS attacks [13]. While in the stochastic scenario, state-feedback control [14], state estimation [4], and output-feedback control [15] have been explored by considering a Bernoulli process. Moreover, using networked controlled systems may result in stochastic packet losses due to network errors or limitations, unrelated to the attacker. These packet dropouts can be modeled after Bernoulli [16] and Markov processes [17, 18]. The

use of non-homogeneous Markov chains with uncertain and unknown probabilities [19, 20] comes as a way to obtain less conservative and more faithful representations of the network's packet dropout behavior [21], whereas it is still under-explored in the context of DoS attacks. Some works also propose control design strategies for systems simultaneously under DoS attacks and other faults not related to the attacker [22], as well as game theory strategies; see [23, 24] for its application in the estimation problem. In [24], both the sensor and the attacker present energy constraints.

The filtering problem also has received attention from the CPS community. The problem of quantization was addressed in [25], while [26] tackles the fading channels problem. Results concerned with event-triggered filter design for CPS under deception attacks were reported in [27]. Continuous-time Fuzzy models were employed to describe the CPS. In [28], a Riccati-based solution was employed to design resilient filters for power systems under DoS attacks in a distributed scenario. Precisely known discrete-time dynamics were considered for the distributed power system. Filter design for stochastic nonlinear systems with time-varying parameters under periodic DoS attacks appeared in [29]. A type of pulse-width-modulated signal was used to model the DoS attacks. A periodic DoS attack was also considered in [30] for continuous-time nonlinear fuzzy systems. The $\mathcal{H}_\infty$ performance was employed, and an event-triggered approach with a multi-sensor structure was proposed to deal with the presence of DoS attacks. Last, but not least, [31] considers $\mathcal{H}_\infty$ performance while assuming limitations in the duration and frequency of the DoS attacks.

As can be seen, several methods have been developed to deal with this important topic. However, there are still issues to be tackled for filter design when dealing with CPS. An important issue is which model is employed for the occurrence of the DoS attacks and transmission failures. In networked controlled systems, the Gilber-Elliot model [21, 32] is one of the most widespread. Albeit there is a consensus that no single model could be employed for all malicious agents, it is also recognized that a more general model could imply more effective strategies to reduce the undesirable effects of the attacks. Moreover, unreliable networks in communication channels are usually considered to have the same characteristics as the DoS attack which is not always the case, as seen, for instance, in the energetically constrained behavior displayed by the attackers. The use of non-homogeneous Markov chains in the DoS attack context, while also considering stochastic losses due to network transmission failure, has also not been widely discussed, and may prove to be a way to design filters while also accounting for changes in the attack and packet loss behavior.

This paper contributes therefore in two ways: (i) By proposing a network model that better encompasses the attack-transmission failure context; (ii) By proposing a filter design strategy that operates considering both the DoS attacks and transmission failures. In summary, this paper advances in the following aspects:

1. A new model to describe the occurrence of the attacks is proposed. The model is based on a Markov chain that makes it possible to differentiate the probabilities of (i) successful transmission, (ii) transmission failure due to network problems, and (iii) the existence of DoS attacks.
2. The transition among the modes of the system is governed by a time-varying probability matrix stemmed from a non-homogeneous Markov chain. This means that the probabilities do not need to be precisely known. Instead, they can have known bounds, or even be unknown.
3. A new filter design condition to deal with the presence of DoS attacks. A full-order filter is synthesized, which accounts for the last-transmitted output.
4. The filter to be designed can be mode-dependent, that is, as the DoS attack evolves, different filters can be employed, or can be mode-independent, not requiring any switching of filters, with both guaranteeing the $\mathcal{H}_\infty$ performance from the exogenous input to the error.
5. A comparison with a classic Gilbert-Elliot model that is used to consider the presence of attacks and unreliable networks is presented, aiming to compare the proposed network model to this widespread network representation from the literature. Furthermore, a comparison concerning the proposed technique and a filter obtained by another method from the literature is provided.

The paper is organized as follows. Section 2 describes the new network model, as well as how to include the uncertain and unknown probabilities in the resulting Markov chain's transition probability matrix. Section 3 presents the augmented system considering the plant and the filter that accounts for the last transmitted output when under attack or transmission failure. The design conditions for the mode-dependent filter are derived, in addition to extensions to consider the mode-independent filter design. Section 4 demonstrates the efficacy of the proposed approach through numerical experiments. The performance of the proposed approach using the proposed network model is discussed, and compared to a classic Gilbert-Elliot model, and the filter design technique is compared to another method from the literature showing that our approach can provide less conservative results. Section 5 concludes the paper and highlights future directions for this work.

Notation

The set $\mathbb{R}^n$ denotes the n-dimensional Euclidean space, and the set $\mathbb{R}^{m\times n}$ denotes the set of all $m \times n$ matrices with real entries. The operator $\times$ denotes the Cartesian product, and the operator $diag(A, B)$ indicates a block diagonal matrix composed of matrices A and B. I_n and $0_{n\times n}$ denote, respectively, the identity and a zero matrix of appropriate dimensions. $M > (<)\ 0$ indicates a positive (negative) definite matrix. The symbol $(^T)$ indicates transpose and $\star$ represents a block induced by symmetry in a symmetric matrix. The operator $He(A)$ indicates $A + A^T$. The symbol $\mathcal{E}\{\cdot\}$ indicates the mathematical expectation. The fundamental probability space is described by $(\Omega, \mathcal{F}, \{\mathcal{F}_k\}, \Psi)$. For each $k \geq 0$, $\mathcal{F}_k = \sigma\{\theta_t; 0 \leq t \leq k\}$ is the σ-algebra generated by $\{\theta_t; 0 \leq t \leq k\}$. Furthermore, $\ell_2(\mathcal{F}_k)$ is defined as the

Hilbert space formed by $\mathcal{F}_k$-measurable sequences $\{\chi_k\}_{k=0}^{\infty}$ for $\|\chi\|_2 \triangleq [\sum_{k=0}^{\infty} \|\chi(k)\|^2]^{1/2} < \infty \; \forall \, \chi(k) \in \mathbb{R}^n_\chi$.

2 | PROBLEM FORMULATION

This paper considers a discrete-time non-homogeneous Markov chain $\{\theta_k; k \geq 0\}$ with a finite state-space $\mathbb{K} = \{1, \dots, \sigma\}$. The mode transition probabilities are as follows

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

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 $\Psi(k) = |p_{ij}(k)|, \; i, j \in \mathbb{K}$.

2.1 | Communication channel Markov model

The communication channels here considered are unreliable and may feature communication failures. At the same time, the presence of DoS attacks originating from malicious agents is taken into account. In such cyber-attacks, the communication channels are jammed via the frequent injection of data, which overloads the network. Both phenomena result in packet losses between the elements connected via the network. In the approached problem, these problems will manifest themselves in the link between the system's measured output and the filter. Concerning the DoS attacks, the following deterministic assumption can be made.

Assumption 1. The attacker is energy-bounded [8, 9], which denotes that the DoS attacks may last only up to N consecutive time-instants.

The following assumption may be considered in the implementation of a mode-dependent scheme to better accommodate the particularities of the network model.

Assumption 2. The system can detect and differentiate between packet losses due to transmission failures caused by network unreliability, and due to DoS attacks.

Attack and transmission failure detection is a separate open problem that is not the focus of this paper. However, some techniques indicate that it is feasible [33, 34]. It is important to highlight that when a robust filter is designed, Assumption 2 can be disregarded.

By combining the deterministic assumption concerning DoS attacks' maximum duration with the stochastic nature with which both transmission failures and the attacks may be modeled, one may obtain a Markov chain that combines both characteristics, allowing one to delineate a mode-dependent filter that better adapts to a finite state-space.

Figure 1 illustrates the schematic for the proposed Markov chain that models the network. The modes indicate three possible types of situation: (i) Successful transmission, (ii) Transmission failure, and (iii) DoS attacks.

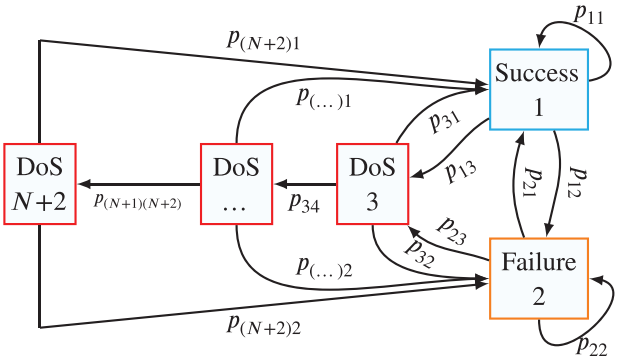

FIGURE 1 Markov chain of the network considering transmission failures and DoS attacks.

The modes transition and definition are further discussed in the sequel

(i) The transmission is successful and the network is operational ($\theta_k = 1$). From this mode, the network may remain operating regularly with probability p_{11}; it may suffer a transmission failure due to communication channel limitations with a probability of p_{12} (mode 2); or it may suffer a DoS attack (mode 3) with a probability of p_{13}. This can be seen in mode 1 of Figure 1.

(ii) Due to communication channel limitations, a transmission failure happens ($\theta_k = 2$). In this mode, there is a probability p_{22} of the limitations persisting and another failure taking place; a probability p_{21} of the network returning to regular operation (mode 1); or the network may suffer a DoS attack (mode 3) with a probability of p_{23}. This can be seen in mode 2 of Figure 1.

(iii) The communication channels suffer a DoS attack ($\theta_k = 3, \dots, N+2$), which start in mode 3. From this point on, the attack may persist with a probability p_{34}; the attack may cease and the network return to regular operation (mode 1) with probability p_{31}; or the attack may cease, but the transmission fails due to communication channels limitations (mode 2) with probability p_{32}. The same idea applies to $\theta_k = 4$ up to $\theta_k = N+1$ which indicates that the attack persists. If $\theta_k = N+2$ is reached, the attack will cease because of the energy limitation of the attacker. From there on, the only possible transitions are to mode 1 or mode 2, with probabilities $p_{(N+2)1}$, and $p_{(N+2)2}$, respectively.

It is worthy of note that the combination of (i) and (ii) represents a simplified Gilbert-Elliot model [21, 32], 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 $N+2$ modes of the CPS network and its possible transitions, the generic transition probability matrix $\Psi \in \mathbb{R}^{(N+2)\times(N+2)}$ is

given by:

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

Note that, for clarity's sake, the same colors indicating the operation modes and their probabilities, as featured in the Markov chain from Figure 1, are employed in matrix (2).

Concerning the state-space $\mathbb{K} = \{1, \dots, \sigma\}$ of the network, $\sigma = N + 2$ will be considered hereafter.

2.2 | Time-varying transition probability matrix

Obtaining the transition probabilities p_{ij} is a very challenging task in the proposed network model, mainly when taking into account the attack dynamics. As ways to circumvent this obstacle and introduce flexibility and robustness to the approach, uncertain probabilities with known bounds ($0 \leq \underline{p_{ij}} \leq p_{ij}(k) \leq \overline{p_{ij}} \leq 1$) and unknown probabilities (represented by $'?'$) where ($0 = \underline{p_{ij}} \leq p_{ij}(k) \leq \overline{p_{ij}} \leq 1$) are modeled after time-varying parameters. The technique used to model this follows the same lines as in [19, 20]. To do so, the principle that $\sum_{j=1}^{N+2} p_{ij}(k) = 1$ is put to use. Each of the m rows containing uncertain or unknown probabilities is composed by a distinct unit simplex dependent on a time-varying parameter $\xi_{k,r} = (\xi_{k,r1}, \dots, \xi_{k,rZ_r})$. A generic unit simplex set is defined as follows:

$$\Lambda_{Z_r} = \left\{ \xi_{k,r} \in \mathbb{R}^{Z_r} : \sum_{\mathfrak{z}=1}^{Z_r} \xi_{k,r\mathfrak{z}} = 1; \xi_{k,r\mathfrak{z}} \geq 0, \mathfrak{z} = 1, \dots, Z_r \right\}, \quad (3)$$

where Z_r is the number of vertices. The transition probability matrix $\Psi(\xi_k)$ is then written after a single domain, which encompasses each of the m rows that display uncertain and unknown probabilities. This is done by considering the multi-simplex $\Lambda_Z = \Lambda_{Z_1} \times \cdots \times \Lambda_{Z_m}$, where $Z = (Z_1, \dots, Z_m)$ and by obtaining a Λ-homogeneous polynomial of the resulting combination. More on that can be found in [20].

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

Definition 1 [35]. A multi-simplex Λ 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 $Z = (Z_1, \dots, Z_m)$. The given parameter ξ of a simplex Λ_Z consists on $(\xi_1, \xi_2, \dots, \xi_m)$, depending on the number of vertices of Λ_Z. Each ξ_i is then decomposed in $(\xi_{i1}, \xi_{i2}, \dots, \xi_{iZ_i})$.

Definition 2 [20]. Given a multi-simplex Λ 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 $r_0 \in \{1, \dots, m\}$, and for any given $\xi_Z \in \mathbb{R}^{Z_r}$, $r \in \{1, \dots, m\} \backslash \{r_0\}$, the partial application $\xi_{Z_{r_0}} \mapsto P(\xi)$ is a homogeneous polynomial.

3 | MAIN RESULTS

3.1 | System declaration

Consider the discrete-time uncertain model of a CPS:

$$\begin{cases} x(k+1) = A(\alpha)x(k) + B(\alpha)w(k), \\ z(k) = C_z(\alpha)x(k) + D_z(\alpha)w(k), \\ y(k) = C_y(\alpha)x(k) + D_y(\alpha)w(k), \end{cases} \quad (4)$$

where $x(k) \in \mathbb{R}^{n_x}$ is the state vector and $w(k) \in \mathbb{R}^{n_w}$ is an exogenous disturbance, $y(k) \in \mathbb{R}^{n_y}$ is the measured output of the plant and $z(k) \in \mathbb{R}^{n_z}$ is the output that is going to be estimated. The matrix $A(\alpha)$ is assumed to be Schur stable. All the matrices have compatible dimensions and may feature uncertainties, belonging to a polytopic domain depending on the time-invariant parameter α. They are written equivalently to the generic matrix $H(\alpha)$ where

$$H(\alpha) = \sum_{v=1}^{V} \alpha_v H_v, \quad \alpha \in \Lambda_V, \quad (5)$$

where V is the number of vertices of the polytope. The vector of time-invariant parameters α belongs to the unit simplex Λ_V, which is defined as

$$\Lambda_V = \left\{ \alpha \in \mathbb{R}^V : \sum_{v=1}^{V} \alpha_v = 1;\ \alpha_v \geq 0,\ v = 1, \dots, V \right\}. \quad (6)$$

The package dropouts due to network unreliability and DoS attacks may render the measured output $y(k)$ unreachable. To circumvent this, in an approach similar to [18], it is assumed that the last transmitted measurement $y_m(k)$ may be stored in a memory in the filter by employing a Zero-Order Hold (ZOH), being described by the following

$$y_m(k) = \delta_{\theta_k} y(k) + (1 - \delta_{\theta_k}) y_m(k-1), \quad (7)$$

where the binary variable δ_{θ_k} follows the defined network state-space $\mathbb{K} = \{1, \dots, N+2\}$, and indicates if the transmission was successful, or a failure/attack has prevented it,

$$\delta_{\theta_k} = \begin{cases} 1, & \text{if } \theta_k = 1, \\ 0, & \text{otherwise.} \end{cases} \quad (8)$$

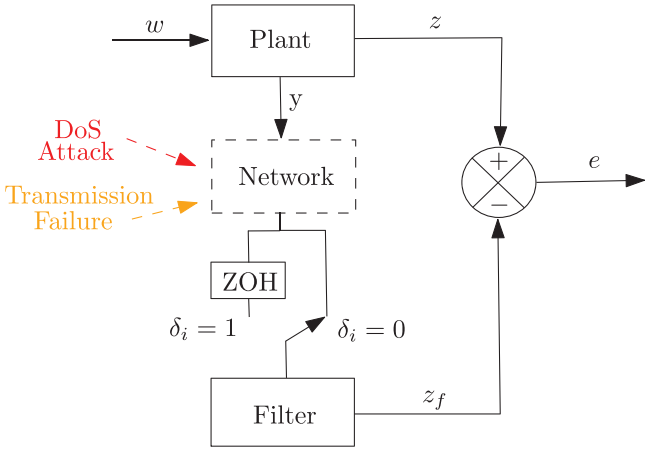

FIGURE 2 Schematic of the filtering system with Zero-Order Hold and with an unreliable network susceptible to DoS Attacks. Where $\delta_i = 0$ indicates successful transmission and $\delta_i = 1$ denotes the presence of DoS attacks or transmission failures.

A full-order mode-dependent filter is then considered, which is described by

$$\mathcal{F} = \begin{cases} x_f(k+1) = Af_{\theta_k} x_f(k) + Bf_{\theta_k} y_m(k), \\ z_f(k) = Cf_{\theta_k} x_f(k) + Df_{\theta_k} y_m(k), \end{cases} \tag{9}$$

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 employed by the filter, defined as in (7). To ease the notation, any mode-dependent matrices will be written as $Af_{\theta_k=i} = Af_i$. The filter is connected to the system (4) with an unreliable network susceptible to attacks as illustrated by Figure 2.

The estimation error is $e(k) = z(k) - z_f(k)$. By combining (4) with (9) and (7), the augmented system that evaluates the filtering error is described by the following Markov Jump Linear System (MJLS).

$$\begin{cases} \eta(k+1) = \bar{A}_i(\alpha)\eta(k) + \bar{B}_i(\alpha)w(k), \\ e(k) = \bar{C}_i(\alpha)\eta(k) + \bar{D}_i(\alpha)w(k), \end{cases} \tag{10}$$

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 $e(k) \in \mathbb{R}^{n_z}$, where $n = 2n_x + n_y$. The matrices have compatible dimensions and are described in the sequel

$$\begin{aligned} \bar{A}_i(\alpha) &= \begin{bmatrix} A(\alpha) & 0 & 0 \\ \delta_i C_y(\alpha) & (1-\delta_i) I_{n_y} & 0 \\ \delta_i B f_i C_y(\alpha) & (1-\delta_i) B f_i & A f_i \end{bmatrix}, \\ \bar{B}_i(\alpha) &= \begin{bmatrix} B(\alpha) \\ \delta_i D_y(\alpha) \\ \delta_i B f_i D_y(\alpha) \end{bmatrix}, \\ \bar{C}_i(\alpha) &= \begin{bmatrix} C_z(\alpha) - \delta_i D f_i C_y(\alpha) & -(1-\delta_i) D f_i & -C f_i \end{bmatrix}, \\ \bar{D}_i(\alpha) &= D_z(\alpha) - \delta_i D f_i D_y(\alpha). \end{aligned} \tag{11}$$

3.2 | Analysis & design conditions

In this section, we present design conditions for a full-order mode-dependent filter that aims to minimize the $\mathcal{H}_\infty$ norm of the estimation error system (10).

First, the definition of the $\|\mathcal{H}_\infty\|^2$ norm is presented, following the same lines as in [18]:

Definition 3. If the exists the scalar γ, then given an initial $\eta(0)$ and θ_0, (10) $\|\mathcal{H}_\infty\|^2$ norm is bounded by γ such that

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

for all $w(k) \in \ell_2^{n_w}[0, \infty)$.

Since the network is modeled after a non-homogeneous Markov chain with arbitrary variation of the transition probabilities, the concept of exponential stability in the mean square sense with conditioning of type I (ESMS-CI) [36, 37] is employed. Furthermore, the bounded real lemma conditions for the MJLS in question, as featured in [36, 37], are presented in the sequel.

Lemma 1. *The system (10) is ESMS-CI and displays a norm $\|\mathcal{H}_\infty\|^2 < \gamma$ if and only if there exist positive definite symmetric matrices $W_i(\xi_k, \alpha) \in \mathbb{R}^{n \times n}$, such that*

$$\Phi_i(\alpha)^T \begin{bmatrix} W_i^+ & 0 \\ 0 & I_{n_z} \end{bmatrix} \Phi_i(\alpha) - \begin{bmatrix} W_i(\xi_k, \alpha) & 0 \\ 0 & \gamma I_{n_w} \end{bmatrix} < 0, \tag{12}$$

where

$$\Phi_i(\alpha) = \begin{bmatrix} \bar{A}_i(\alpha) & \bar{B}_i(\alpha) \\ \bar{C}_i(\alpha) & \bar{D}_i(\alpha) \end{bmatrix}, \tag{13}$$

$$W_i^+ = \sum_{j=1}^{N+2} p_{ij}(\xi_k) W_j(\xi_{k+1}, \alpha), \tag{14}$$

hold for $i \in \mathbb{K}$ and for all $(\alpha, \xi_k, \xi_{k+1}) \in \Lambda_V \times \Lambda_Z \times \Lambda_Z, \forall k \geq 0$.

The following Lemma presents an equivalent condition to Lemma 1.

Lemma 2. *The system (10) is ESMS-CI and displays a norm $\|\mathcal{H}_\infty\|^2 < \gamma$ if and only if there exist positive definite symmetric matrices $W_i(\xi_k, \alpha) \in \mathbb{R}^{n \times n}$, and W_i^+ as in (14), such that*

$$\begin{bmatrix} W_i(\xi_k, \alpha) & \bar{A}_i(\alpha)^T W_i^+ & 0 & \bar{C}_i(\alpha) \\ W_i^+ \bar{A}_i(\alpha) & W_i^+ & W_i^+ \bar{B}_i(\alpha) & 0 \\ 0 & \bar{B}_i(\alpha)^T W_i^+ & I_{n_w} & \bar{D}_i(\alpha)^T \\ \bar{C}_i(\alpha) & 0 & \bar{D}_i(\alpha) & \gamma I_{n_z} \end{bmatrix} > 0, \tag{15}$$

hold for $i \in \mathbb{K}$ and for all $(\alpha, \xi_k, \xi_{k+1}) \in \Lambda_V \times \Lambda_Z \times \Lambda_Z, \forall k \geq 0$.

Proof. Pre and post-multiplying (15) by $diag(\gamma^{\frac{1}{2}} I_n, \gamma^{\frac{1}{2}} I_n, \gamma^{\frac{1}{2}} I_{n_w}, \gamma^{-\frac{1}{2}} I_{n_z})$ yields

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

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

$$\begin{bmatrix} W_i(\xi_k,\alpha) & \bar{A}_i(\alpha)^T W_i^+ & 0 & \bar{C}_i(\alpha) \\ W_i^+\bar{A}_i(\alpha) & W_i^+ & W_i^+\bar{B}_i(\alpha) & 0 \\ 0 & \bar{B}_i(\alpha)^T W_i^+ & \gamma I_{n_w} & \bar{D}_i(\alpha)^T \\ \bar{C}_i(\alpha) & 0 & \bar{D}_i(\alpha) & I_{n_z} \end{bmatrix} > 0. \quad (16)$$

By pre and post-multiplying (16) by $\mathcal{L}^T$ and its transpose, where

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

The following is obtained

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

Through Schur's complement, the following equivalent is found

$$\begin{bmatrix} W_i(\xi_k,\alpha) & 0 \\ 0 & \gamma I_{n_w} \end{bmatrix} - \Phi_i(\alpha)^T \begin{bmatrix} W_i^+ & 0 \\ 0 & I_{n_z} \end{bmatrix} \Phi_i(\alpha) > 0,$$

with $\Phi_i(\alpha)$ as in (13). Note that this is equivalent to condition (12), concluding the proof. □

With these defined, conditions to design a mode-dependent filter based on the use of parameter-dependent slack variables aiming to reduce the conservatism of the method, and inspired by [38, 39], are presented in the sequel.

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

$$\min \gamma, \quad (17)$$

$$W_i(\xi_k,\alpha) = \begin{bmatrix} W_{11,i}(\xi_k,\alpha) & W_{12,i}(\xi_k,\alpha) & W_{13,i}(\xi_k,\alpha) \\ W_{12,i}(\xi_k,\alpha)^T & W_{22,i}(\xi_k,\alpha) & W_{23,i}(\xi_k,\alpha) \\ W_{13,i}(\xi_k,\alpha)^T & W_{23,i}(\xi_k,\alpha)^T & W_{33,i}(\xi_k,\alpha) \end{bmatrix} > 0, \quad (18)$$

$$\begin{bmatrix} \phi_{11} & \phi_{12} & \phi_{13} & \phi_{14} & \phi_{15} & \phi_{16} & \phi_{17} & \phi_{18} \\ \star & \phi_{22} & \phi_{23} & \phi_{24} & \phi_{25} & \phi_{26} & \phi_{27} & \phi_{28} \\ \star & \star & \phi_{33} & \phi_{34} & \phi_{35} & \phi_{36} & \phi_{37} & \phi_{38} \\ \star & \star & \star & \phi_{44} & \phi_{45} & \phi_{46} & \phi_{47} & \phi_{48} \\ \star & \star & \star & \star & \phi_{55} & \phi_{56} & \phi_{57} & \phi_{58} \\ \star & \star & \star & \star & \star & \phi_{66} & \phi_{67} & \phi_{68} \\ \star & \star & \star & \star & \star & \star & \phi_{77} & \phi_{78} \\ \star & \star & \star & \star & \star & \star & \star & \phi_{88} \end{bmatrix} > 0, \quad (19)$$

where,

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

$$\phi_{12} = W_{12,i}(\xi_k,\alpha) + (1-\delta_i)K_{12} + A(\alpha)^T K_{21}(\alpha)^T + \delta_i C_y(\alpha)^T K_{22}(\alpha)^T,$$

$$\phi_{13} = W_{13,i}(\xi_k,\alpha) + A(\alpha)^T K_{31}(\alpha)^T + \delta_i C_y(\alpha)^T K_{32}(\alpha)^T,$$

$$\phi_{14} = A(\alpha)^T E_{11}(\alpha)^T - K_{11}(\alpha) + \delta_i (C_y(\alpha)^T E_{12}(\alpha)^T + C_y(\alpha)^T K_{2,i}^T),$$

$$\phi_{15} = A(\alpha)^T E_{21}(\alpha)^T - K_{12}(\alpha) + \delta_i C_y(\alpha)^T E_{22}(\alpha)^T,$$

$$\phi_{16} = A(\alpha)^T E_{31}(\alpha)^T + \delta_i (C_y(\alpha)^T E_{32}(\alpha)^T + C_y(\alpha)^T K_{2,i}^T),$$

$$\phi_{17} = A(\alpha)^T Q_1(\alpha)^T + K_{11}(\alpha)B(\alpha) + \delta_i (K_{12}(\alpha)D_y(\alpha) + C_y(\alpha)^T Q_2(\alpha)^T),$$

$$\phi_{18} = A(\alpha)^T F_1(\alpha)^T + C_{\tilde{z}}(\alpha)^T + \delta_i (C_y(\alpha)^T F_2(\alpha)^T - C_y(\alpha)^T Df_i^T),$$

$$\phi_{22} = W_{22,i}(\xi_k,\alpha) + (1-\delta_i)He(K_{22}(\alpha)),$$

$$\phi_{23} = W_{23,i}(\xi_k,\alpha) + (1-\delta_i)K_{32}(\alpha)^T,$$

$$\phi_{24} = (1-\delta_i)(E_{12}(\alpha)^T + K_{2,i}^T) - K_{21}(\alpha),$$

$$\phi_{25} = (1-\delta_i)E_{22}(\alpha)^T - K_{22}(\alpha),$$

$$\phi_{26} = (1-\delta_i)(E_{32}(\alpha)^T + K_{2,i}^T),$$

$$\phi_{27} = (1-\delta_i)Q_2(\alpha)^T + \delta_i K_{22}(\alpha)D_y(\alpha) + K_{21}(\alpha)B(\alpha),$$

$$\phi_{28} = (1-\delta_i)(F_2(\alpha)^T - Df_i),$$

$$\phi_{33} = W_{33,i}(\xi_k,\alpha),$$

$$\phi_{34} = K_{1,i}^T - K_{31}(\alpha),$$

$$\phi_{35} = -K_{32}(\alpha),$$

$$\phi_{36} = K_{1,i}^T,$$

$$\phi_{37} = K_{31}(\alpha)B(\alpha) + \delta_i K_{32}(\alpha)D_y(\alpha),$$
$$\phi_{38} = -Cf_i^T,$$
$$\phi_{44} = -W_{11,i}^+ - He(E_{11}(\alpha)),$$
$$\phi_{45} = -W_{12,i}^+ - E_{21}(\alpha)^T - E_{12}(\alpha),$$
$$\phi_{46} = -W_{13,i}^+ - E_{31}(\alpha)^T - K,$$
$$\phi_{47} = E_{11}(\alpha)B(\alpha) - Q_1(\alpha)^T + \delta_i(E_{12}(\alpha)D_y(\alpha) + K_{2,i}D_y(\alpha)),$$
$$\phi_{48} = -F_1(\alpha)^T,$$
$$\phi_{55} = -W_{22,i}^+ - He(E_{22}(\alpha)),$$
$$\phi_{56} = -W_{23,i}^+ - E_{32}(\alpha)^T,$$
$$\phi_{57} = E_{21}(\alpha)B(\alpha) - Q_2(\alpha)^T + \delta_i E_{22}(\alpha)D_y(\alpha),$$
$$\phi_{58} = -F_2(\alpha)^T,$$
$$\phi_{66} = -W_{33,1}^+ - He(K),$$
$$\phi_{67} = E_{31}(\alpha)B(\alpha) + \delta_i(E_{32}(\alpha)D_y(\alpha) + K_{2,i}D_y(\alpha)),$$
$$\phi_{68} = 0_{n_x \times n_z},$$
$$\phi_{77} = He(Q_1(\alpha)B(\alpha) + \delta_i Q_2(\alpha)D_y(\alpha)) + I_{n_w},$$
$$\phi_{78} = B(\alpha)^T F_1(\alpha)^T + D_z(\alpha)^T + \delta_i(D_y(\alpha)^T F_2(\alpha)^T - D_y(\alpha)^T Df_i^T),$$
$$\phi_{88} = \gamma I_{n_z},$$

with,

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

and where $W_{11,i}^+$, $W_{12,i}^+$, $W_{13,i}^+$, $W_{22,i}^+$, $W_{23,i}^+$, $W_{33,i}^+$ *are written after the generic matrix* M_i^+, *with*

$$M_i^+ = \sum_{j=1}^{N+2} p_{ij}(\xi_k)M_j(\xi_{k+1}, \alpha), \tag{20}$$

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 (9) that assures that (10) has a guaranteed cost* $\mathcal{H}_\infty$ *bounded by* $\sqrt{\gamma}$ *when* $w \neq 0$ *and is ESMS-CI for all* $(\alpha, \xi_k, \xi_{k+1}) \in \Lambda_V \times \Lambda_Z \times \Lambda_Z$, $\forall k \geq 0$.

Proof. First, in what regards W_i^+ as in (14), since it consists of a linear combination, the structuring described in (18) can be applied as it was presented in (20) without further problems. Substituting $K_{1,i} = KAf_i$ and $K_{2,i} = KBf_i$ and by pre and post-multiplying (19) by $\mathcal{B}^T$ and its transpose, where

$$\mathcal{B}^T = \begin{bmatrix} I_n & \bar{A}_i(\alpha)^T & 0 & 0 \\ 0 & \bar{B}_i(\alpha)^T & I_{n_w} & 0 \\ 0 & 0 & 0 & I_{n_z} \end{bmatrix}. \tag{21}$$

Then by considering $W_i(\xi_k, \alpha)$ as in (18) and W_i^+ as in (14), the following is obtained

$$\begin{bmatrix} \mathcal{M}_i & \begin{bmatrix} \bar{C}_i(\alpha)^T \\ \bar{D}_i(\alpha)^T \end{bmatrix} \\ \begin{bmatrix} \bar{C}_i(\alpha) & \bar{D}_i(\alpha) \end{bmatrix} & \gamma I_{n_z} \end{bmatrix} > 0, \tag{22}$$

where

$$\mathcal{M}_i = \begin{bmatrix} W_i(\xi_k, \alpha) & 0 \\ 0 & I_{n_w} \end{bmatrix} - \begin{bmatrix} \bar{A}_i(\alpha)^T \\ \bar{B}_i(\alpha)^T \end{bmatrix} W_i^+ \begin{bmatrix} \bar{A}_i(\alpha) & \bar{B}_i(\alpha) \end{bmatrix}.$$

Applying Schur's complement results on

$$\begin{bmatrix} W_i(\xi_k, \alpha) & 0 & \bar{C}_i(\alpha)^T & \bar{A}_i(\alpha)^T W_i^+ \\ 0 & I_{n_w} & \bar{D}_i(\alpha)^T & \bar{B}_i(\alpha)^T W_i^+ \\ \bar{C}_i(\alpha) & \bar{D}_i(\alpha) & \gamma I_{n_z} & 0 \\ W_i^+ \bar{A}_i(\alpha) & W_i^+ \bar{B}_i & 0 & W_i^+ \end{bmatrix} > 0. \tag{23}$$

Pre- and post-multiplying (23) by $\mathcal{N}^T$ and its transpose, where

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

results in an equivalent condition to (15). This concludes the proof. □

Assumption 2 can be disregarded in exchange for a more conservative approach that utilizes a mode-independent filter and to reduce the dependency of the filter implementation on an attack and transmission failure detection scheme. This can be particularly useful as the filter would need neither to differentiate between DoS attacks and transmission failure nor to track how many consecutive time instants the network is under attack. Conditions to design this mode-independent filter are presented in the following Corollary.

Corollary 1. *If there exist symmetric matrices* $W_{11,i}(\xi_k, \alpha)$, $W_{22,i}(\xi_k, \alpha) \in \mathbb{R}^{n_y \times n_y}$, $W_{33,i} \in \mathbb{R}^{n_x \times n_x}$, *and matrices* $W_{12,i}(\xi_k, \alpha)$, K_{12}, K_{32}, E_{12}, E_{32}, $K_2 \in \mathbb{R}^{n_x \times n_y}$, $W_{13,i}(\alpha)$, $K_{11}(\alpha)$, $K_{13}(\alpha)$, $E_{11}(\alpha)$, $E_{13}(\alpha)$, K, $K_1 \in \mathbb{R}^{n_x \times n_x}$, $W_{23,i} \in \mathbb{R}^{n_y \times n_x}$, 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 positive scalar* γ, *such that (18) and (19) 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 (9) for* $Af_i = Af$, $Bf_i = Bf$, $Cf_i = Cf$, *and* $Df_i = Df$ *that assures that (10) has a guaranteed cost* $\mathcal{H}_\infty$ *bounded by* $\sqrt{\gamma}$ *when* $w \neq 0$ *and is ESMS-CI for all* $i \in \mathbb{K}$, $(\alpha, \xi_k, \xi_{k+1}) \in \Lambda_V \times \Lambda_Z \times \Lambda_Z$, *and* $\forall k \geq 0$.

Remark 1. The conditions presented in Theorem 1 are infinite dimensional, given that they depend both on the simplex Λ_V and on the multi-simplex Λ_Z. To obtain a finite set of LMIs to recast the parameter-dependent conditions, as well as to manipulate the Λ-homogeneous polynomial matrices, the Robust LMI Parser (ROLMIP) [40] is employed.

Remark 2. The recast procedure employed by ROLMIP makes it not necessary to know or estimate the parameters ξ_k and α since only a combination of the known vertices is utilized to create the finite set of LMIs. The reader is referred to [40] for more details. Furthermore, the filter design can be performed offline, and it does not depend on the parameters ξ_k and α. These parameters do not need to be known to implement the proposed filter, being necessary only to know the currently active mode of the network in the case of Theorem 1 and not even that in the mode-independent case of Corollary 1.

Remark 3. The number of scalar decision variables employed by Theorem 1 (NV_T) and Corollary 1 (NV_C) is defined by the following

$$\begin{aligned} NV_T &= n_x^2 + (N+2)(n_x+n_y)(n_x+n_{\tilde{z}}) \\ &\quad + V(n_x+n_y)(n_w+4n_x+2n_y+n_{\tilde{z}}) \\ &\quad + VZ(N+2)(2n_x^2+2n_xn_y+n_x+0.5n_y^2+0.5n_y)+1, \end{aligned}$$

$$\begin{aligned} NV_C &= n_x^2 + (n_x+n_y)(n_x+n_{\tilde{z}}) \\ &\quad + V(n_x+n_y)(n_w+4n_x+2n_y+n_{\tilde{z}}) \\ &\quad + VZ(N+2)(2n_x^2+2n_xn_y+n_x+0.5n_y^2+0.5n_y)+1. \end{aligned}$$

Note that employing the mode-dependent scheme of Theorem 1 results in $(N+1)(n_x+n_y)(n_x+n_{\tilde{z}})$ more scalar variables than the mode-independent case of Corollary 1

4 | NUMERICAL EXPERIMENTS

In this section, numerical experiments will be conducted to test the proposed mode-dependent filter design technique considering an uncertain CPS. Scenarios considering the mode-independent approach will also be featured. The network is unreliable and modeled as described in Section 2.1. All tests were conducted using the parsers YALMIP [41], ROLMIP [40], and the solver MOSEK [42] combined with MATLAB 2016b. In the numerical experiments, all the decision variables in Theorem 1 are considered to have an affine dependence on the uncertain parameter α.

4.1 | Example 1

Consider the following discrete-time uncertain system, borrowed from [43]

TABLE 1 $\|H_\infty\|$ norm in function of different values of the probabilistic parameter ρ.

	Theorem 1		Corollary 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

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

where $|\mu| \leq 0.45$, resulting in $V = 2$ vertices, and whose augmented system is as described in (10).

The Markovian network model, as shown by Figure 1 and outlined by (2), is utilized to depict the system network behavior between the plant and the filter, as illustrated by Figure 2. Considering a maximum of $N = 5$ consecutive attacks, the utilized transition probability matrix with uncertain and unknown parameters is as follows

$$\Psi = \begin{bmatrix} 0.45 & e & d & 0 & 0 & 0 & 0 \\ 0.5 & ? & ? & 0 & 0 & 0 & 0 \\ f & 0.05 & 0 & \rho & 0 & 0 & 0 \\ f & 0.05 & 0 & 0 & \rho & 0 & 0 \\ f & 0.05 & 0 & 0 & 0 & \rho & 0 \\ f & 0.05 & 0 & 0 & 0 & 0 & \rho \\ 0.45 & 0.55 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{24}$$

where $f = (1 - 0.05 - \rho)$, $e \in \begin{bmatrix} 0.05 & 0.15 \end{bmatrix}$ and $d \in \begin{bmatrix} 0.4 & 0.5 \end{bmatrix}$. ρ is a parameter whose value defines if longer attacks are more likely to take place. 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.

First, Theorem 1 is utilized to obtain a $\mathcal{H}_\infty$ mode-dependent filter for different values of ρ. Corollary 1 was also employed to obtain a mode-independent filter in the same layout. The scenario with $N = 5$ maximum consecutive attacks was considered as well as a scenario with $N = 10$, which can be easily obtained by using the same values of rows 3 to 6 in (24), in accordance to the positioning defined by (2). The norm value in function of the value of ρ is provided in Table 1.

Table 1 shows that the probability of longer attacks (related to ρ) affects the $\mathcal{H}_\infty$ more than considering a higher value of N. The mode-dependent filter designed by Theorem 1 provided the best results. However, the mode-independent filter of Corollary 1 also yielded a good performance, indicating it

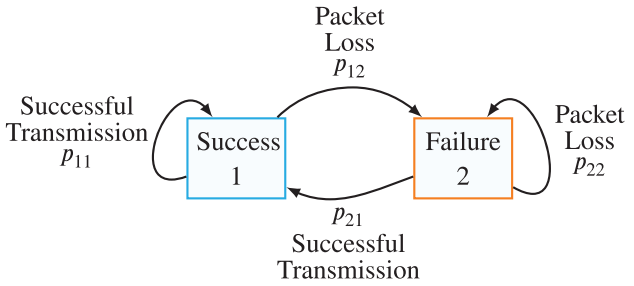

FIGURE 3 Markov chain for the Gilbert-Elliot model.

TABLE 2 $\|H_\infty\|$ cost in function of different values of the probabilistic parameter ρ for the equivalent Gilbert-Elliot model.

ρ	Theorem 1	Corollary 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	-	-

to be a viable strategy, in addition to being easier to implement, and not depending on an attack and transmission failure detection scheme.

In the sequel, a Gilbert-Elliot model (as depicted in Figure 3) is considered to represent the network under transmission failures and DoS attacks. The first row of (24) is used to indicate the successful transmission mode of the new adapted transition probability matrix. By setting the lower bound according to the second row of (24) and the upper bound according to rows 3 − 6, the probabilities regarding the mode representing the failed transmissions of the Gilbert-Elliot equivalent are described. The resulting transition probability matrix is as follows.

$$\Psi = \begin{bmatrix} 0.45 & 0.55 \\ [0.5 \quad (1-\rho-0.05)] & [0.5 \quad (\rho+0.05)] \end{bmatrix}. \tag{25}$$

Theorem 1 and Corollary 1 are employed to (respectively) obtain mode-dependent and mode-independent filters considering (25). Table 2 indicates the norm values in function of the value of ρ considering the aforementioned two cases.

As seen in Table 2, the achieved costs were higher when considering a Gilbert-Elliot equivalent to model the network, mainly in higher values of ρ. Moreover, in $\rho = 0.95$, no feasible answers were obtained. This may indicate that the Gilbert-Elliot model is more conservative than the network model proposed here, as it could not include the deterministic assumption of energy constraints. Another aspect that can be observed is that even the mode-independent filter (i.e. the filter that did not require a detection scheme that differentiates stochastic packet loss to DoS attack) benefited from using the proposed network model, given the less conservative costs obtained when compared to the Gilbert-Elliot's case with higher probabilities of packet loss.

4.2 | Example 2

Consider the following system borrowed from [44], which consists of a discretized model with sample time 0.1 s of a mechanical system composed of two masses and two strings.

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

$$B_1 = B_2 = \begin{bmatrix} 0 \\ 0 \\ 0.01 \\ 0 \end{bmatrix},$$

$$C_{y,1} = \begin{bmatrix} 0.3 & 0 & 0 & 0 \end{bmatrix},$$

$$C_{y,2} = \begin{bmatrix} 1.7 & 0 & 0 & 0 \end{bmatrix},$$

$$C_{z,1} = C_{z,2} = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix},$$

and $D_{y,1} = D_{y,2} = D_{z,1} = D_{z,2} = 0$.

Considering the augmented system as in (10), and employing the same transition probability matrix (24), $\rho = 0.9$ and $N = 5$ was considered to design a mode-dependent filter through Theorem 1, which returned a guaranteed cost of $\sqrt{\gamma} = 0.0967$.

1000 time-based simulations were performed, where a random set of α was selected at the beginning of each simulation, and a new ξ_k was employed at each time instant. Null $\eta(0)$ were considered, as well as the interval $k \in (0, 170)$ and the exogenous disturbance $w(k) = 10e^{-0.05k}\cos(0.1k)$. The $\sqrt{\gamma}$ cost was calculated in each simulation by using $\sqrt{\sum_{k=0}^{\infty} e(k)^2 / \sum_{k=0}^{\infty} w(k)^2}$. In the 1000 simulations, the average cost and its standard deviation were, respectively, 0.0354 and 0.0098. The mean response with the range of one standard deviation of $z_f(k)$ (- - -) and the mean response of $z(k)$ (—) in all the simulations are depicted in Figure 4. Since $z(k)$ is dependent neither on the network nor on the system uncertainties, there was no deviation in its value.

Furthermore, the frequency in which the network found itself in each mode in all the simulations is depicted in Figure 5.

Even with successful transmissions in less than 30% of the time, the filter was able to perform its function, mitigating the effect of the exogenous disturbances. Moreover, the $\sqrt{\gamma}$ cost evidenced in the simulations was lower than the value guaranteed by design, indicating that the filter performance may even be less conservative.

In the sequel, a random simulation is selected to illustrate the network operation under (24) more clearly. The filter output $z_f(k)$ (- - -) and $z(k)$ (—) are displayed in Figure 6, where DoS attacks are depicted in red and transmission failures are indicated in orange. The calculated $\sqrt{\gamma}$ cost was 0.0303. Finally,

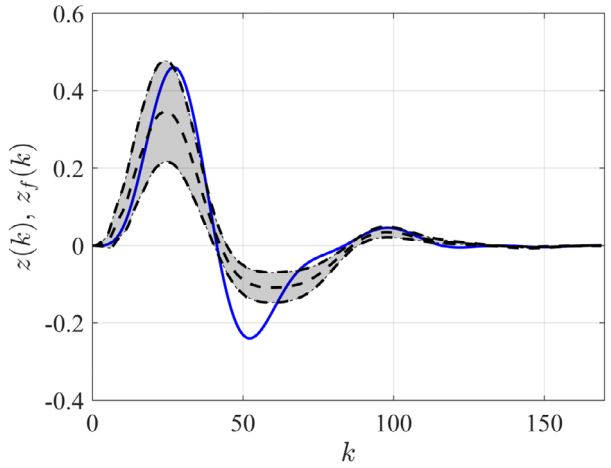

FIGURE 4 Mean $z(k)$ (—) and mean $z_f(k)$ (- - -) with confidence interval of 1 standard-deviation from the 1000 time-based simulations. A new set of α was randomly selected at each simulation and a new ξ_k was randomly selected at each time instant. The mode-dependent filter of Theorem 1 is considered and $\eta(0)$ is null.

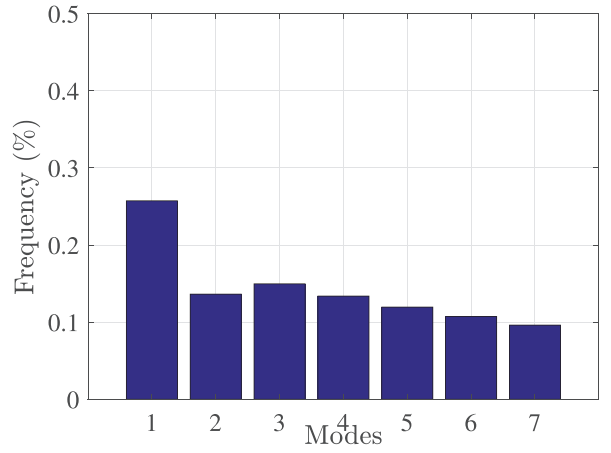

FIGURE 5 Histogram with the frequency of occurrence of each mode in the 1000 time-based simulations.

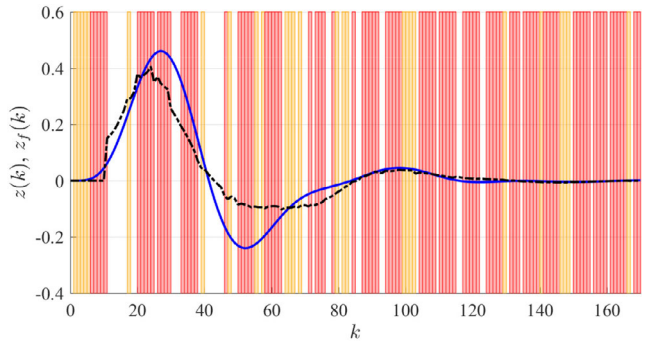

FIGURE 6 $z(k)$ (—) and $z_f(k)$ (- - -) with the mode-dependent filter considering a different randomly selected ξ_k for each time instant. $\alpha = \begin{bmatrix}0.5234 & 0.4766\end{bmatrix}$ and $\eta(0)$ is null. Transmission failures are depicted in orange and DoS attacks in red.

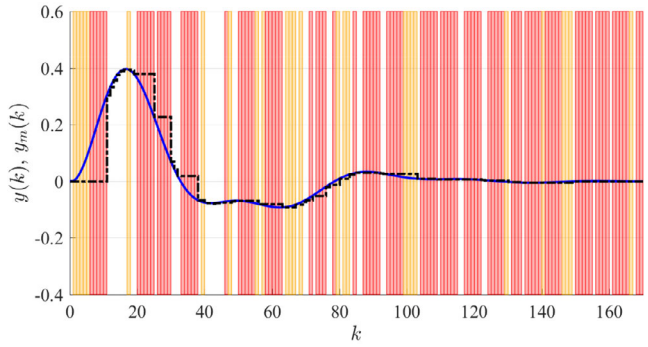

FIGURE 7 $y(k)$ (—) and $y_m(k)$ (- - -) considering a different randomly selected ξ_k for each time instant. $\alpha = \begin{bmatrix}0.5234 & 0.4766\end{bmatrix}$ and $\eta(0)$ is null. Transmission failures are depicted in orange and DoS attacks in red.

in Figure 7, the value of $y(k)$ (—) and $y_m(k)$ (- - -) are plotted, to better demonstrate how the packet losses influence the measured output perceived by the filter

4.3 | Example 3

To compare the proposed method with the existing literature, consider the system matrices borrowed from [31]:

$$A = \begin{bmatrix}-0.6579 & -0.1699\\ 0.6914 & -0.0181\end{bmatrix}, \quad B = \begin{bmatrix}0.3040 & 0.1843\\ 0.1653 & 0.5737\end{bmatrix},$$

$$C_{\tilde{z}} = \begin{bmatrix}-0.0560 & 0.0933\end{bmatrix}, \quad D_{\tilde{z}} = 0,$$

$$C_y = \begin{bmatrix}0.1829 & 0.0862\end{bmatrix}, \quad D_y = \begin{bmatrix}0.0165 & -0.0122\end{bmatrix}.$$

We consider the same scenario presented in [31, Example 1]. The following transition probability matrix in the Gilbert-Elliot framework describes the network behavior:

$$\Psi = \begin{bmatrix}0.86 & 0.14\\ 0.86 & 0.14\end{bmatrix}.$$

The following filtering matrices are reported in [31], which yielded a $\sqrt{\gamma} = 0.0721$.

$$Af_1 = \begin{bmatrix}-0.1694 & 0.0566\\ 0.3700 & -0.1754\end{bmatrix}, \quad Af_2 = \begin{bmatrix}-0.1339 & 0.0700\\ 0.3485 & -0.1920\end{bmatrix},$$

$$Bf_1 = \begin{bmatrix}2.8507 & -1.3603\end{bmatrix}^T, \quad Bf_2 = \begin{bmatrix}3.1778 & -1.3880\end{bmatrix}^T,$$

$$Cf_1 = \begin{bmatrix}0.0669 & -0.0865\end{bmatrix}, \quad Cf_2 = \begin{bmatrix}0.0531 & -0.0951\end{bmatrix},$$

$$Df_1 = Df_2 = 0.$$

Theorem 1 was then employed to obtain a mode-dependent filter for the same system and transition probability matrix. Note that all parameter dependencies were disregarded since both the system and Ψ are precisely known. The resulting filter is

described in the sequence, and returned a $\sqrt{\gamma} = 0.0546$, showing a better performance when compared to the technique of [31].

$$\mathcal{A}f_1 = \begin{bmatrix} -0.2003 & 0.0453 \\ 0.4918 & -0.1126 \end{bmatrix}, \ \mathcal{A}f_2 = \begin{bmatrix} -0.6588 & -0.1710 \\ 0.6907 & -0.0184 \end{bmatrix},$$

$$\mathcal{B}f_1 = \begin{bmatrix} 2.5015 & -1.0864 \end{bmatrix}^T, \ \mathcal{B}f_2 = \begin{bmatrix} 0.0023 & -0.0007 \end{bmatrix}^T,$$

$$\mathcal{C}f_1 = \begin{bmatrix} 0.0561 & -0.0934 \end{bmatrix}, \ \mathcal{C}f_2 = \begin{bmatrix} 0.0559 & -0.0933 \end{bmatrix},$$

$$\mathcal{D}f_1 = \mathcal{D}f_2 = 0.$$

Moreover, we must highlight that the proposed method can deal with many more scenarios, considering uncertainties, network failures, and different probabilities for different sizes of attacks, topics which are not covered by the method in [31].

5 | CONCLUSION

This work proposed a new MJLS model for the network to tackle the problem of CPS $\mathcal{H}_\infty$ filtering through an unreliable network susceptible to DoS attacks. This network model, based on a non-homogeneous Markov chain that combined the deterministic energy limitation of the attacker with uncertain and unknown probabilities, allowed to encompass different levels of network reliability and longer or shorter consecutive attacks. A mode-dependent dynamic filter design technique derived from parameter-dependent linear matrix inequalities that guarantees an upper bound to the $\mathcal{H}_\infty$ norm was presented. Future research concerning the topic involves $\mathcal{H}_2$ or $\mathcal{H}_\infty/\mathcal{H}_2$ filter design and the observer-based control problem in a context of DoS attacks and unreliable networks.

AUTHOR CONTRIBUTIONS

Pedro M. Oliveira: Conceptualization; investigation; validation; writing—original draft. **Jonathan M. Palma**: Conceptualization; investigation; supervision; validation; writing—review & editing. **Márcio J. Lacerda**: Conceptualization; funding acquisition; investigation; supervision; validation; writing—review & editing.

ACKNOWLEDGEMENTS

National Council for Scientific and Technological Development - grant no 315538/2021-0. Agencia Nacional de Investigación y Desarrollo - grant no 1241305. Fondo Nacional de Desarrollo Científico y Tecnológico - grant no 11201049. Fundação de Amparo à Pesquisa do Estado de Minas Gerais - grant PAPG-13121.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

ORCID

Pedro M. Oliveira https://orcid.org/0000-0002-5035-7070
Jonathan M. Palma https://orcid.org/0000-0002-3924-1907
Márcio J. Lacerda https://orcid.org/0000-0001-8487-3535

REFERENCES

1. Rawat, D.B., Rodrigues, J.J., Stojmenovic, I.: Cyber-Physical Systems: From Theory to Practice, vol. 588. CRC Press, Boca Raton, FL (2015)
2. Humayed, A., et al.: Cyber-physical systems security–a survey. IEEE Internet Things J. 4(6), 1802–1831 (2017)
3. Li, J., et al.: Reliable control of cyber-physical systems under state attack: An adaptive integral sliding-mode control approach. IET Control Theory Appl. 18(1), 27–39 (2024)
4. Lin, H., Lam, J., Wang, Z.: Secure state estimation for systems under mixed cyber-attacks: Security and performance analysis. Inf. Sci. 546, 943–960 (2021).
5. Lin, H., et al.: Secure LQG control for a quadrotor under false data injection attacks. IET Control Theory Appl. 16(9), 925–934 (2022)
6. Peixoto, M.L.C., et al.: Event-triggered control for LPV systems under hybrid cyberattacks. Journal of Control. Autom. Electr. Syst. 35, 252–265 (2024)
7. Long, M., Wu, C.-H., Hung, J.: Denial of service attacks on network-based control systems: impact and mitigation. IEEE Trans. Ind. Inf. 1(2), 85–96 (2005)
8. Lai, S., et al.: Packet-based state feedback control under DoS attacks in cyber-physical systems. IEEE Trans. Circuits Syst. II Exp. Briefs 66(8), 1421–1425 (2019)
9. Pessim, P.S.P., Lacerda, M.J.: State-feedback control for Cyber-physical LPV systems under DoS attacks. IEEE Control Syst. Lett. 5(3), 1043–1048 (2021)
10. Pessim, P.S.P., et al.: Static output-feedback control for Cyber-physical LPV systems under DoS attacks. Inf. Sci. 563, 241–255 (2021)
11. Zhang, H., et al.: Optimal dos attack scheduling in wireless networked control system. IEEE Trans. Control Syst. Technol. 24(3), 843–852 (2016)
12. Li, Y., Tong, S.: Bumpless transfer distributed adaptive backstepping control of nonlinear multi-agent systems with circular filtering under DoS attacks. Automatica 157, 111250 (2023)
13. Zhao, N., et al.: Observer-based event-triggered approach for stochastic networked control systems under denial of service attacks. IEEE Trans. Control Network Syst. 8(1), 158–167 (2020)
14. Wang, M., Xu, B.: Guaranteed cost control of cyber-physical systems with packet dropouts under dos jamming attacks. Asian J. Control 22(4), 1659–1669 (2020)
15. Su, L., Ye, D.: Observer-based output feedback $\mathcal{H}_\infty$ control for cyber-physical systems under randomly occurring packet dropout and periodic DoS attacks. ISA Trans. 95, 58–67 (2019)
16. Schenato, L.: To zero or to hold control inputs with lossy links? IEEE Trans. Autom. Control 54(5), 1093–1099 (2009)
17. Fioravanti, A.R., Gonçalves, A.P.C., Geromel, J.C.: Filter inputs with Markovian lossy links: Zero or hold? In: Proceedings of the 9th IEEE International Conference on Control and Automation (ICCA), pp. 656–661. IEEE, Piscataway (2011)
18. Zhang, W.-A., Yu, L., Song, H.: $\mathcal{H}_\infty$ filtering of networked discrete-time systems with random packet losses. Inf. Sci. 179(22), 3944–3955 (2009)
19. Gonçalves, A.P.C., Fioravanti, A.R., Geromel, J.C.: $\mathcal{H}_\infty$ robust and networked control of discrete-time MJLS through LMIs. J. Franklin Inst. 349(6), 2171–2181 (2012)
20. Morais, C.F., et al.: $\mathcal{H}_2$ control of discrete-time Markov jump linear systems with uncertain transition probability matrix: Improved linear matrix inequality relaxations and multi-simplex modeling. IET Control Theory Appl. 7, 1665–1674 (2013)
21. Serafini, A.R., et al.: Robust static output-feedback control for MJLS with non-homogeneous Markov chains: A comparative study considering a wireless sensor network with time-varying PER. Sensors 21(19), 6420 (2021)

22. Deng, C., Wen, C.: Distributed resilient observer-based fault-tolerant control for heterogeneous multiagent systems under actuator faults and DoS attacks. IEEE Trans. Control Network Syst. 7(3), 1308–1318 (2020)
23. Ding, K., et al.: DoS attacks on remote state estimation with asymmetric information. IEEE Trans. Control Network Syst. 6(2), 653–666 (2018)
24. Li, Y., et al.: SINR-based DoS attack on remote state estimation: A game-theoretic approach. IEEE Trans. Control Network Syst. 4(3), 632–642 (2016)
25. Zhao, X.-Y., Chang, X.-H.: $\mathcal{H}_\infty$ filtering for nonlinear discrete-time singular systems in encrypted state. Neural Process. Lett. 55(3), 2843–2866 (2023)
26. Cai, L.-J., Chang, X.-H.: Reduced-order filtering for discrete-time singular systems under fading channels. Int. J. Syst. Sci. 54(1), 99–112 (2023)
27. Gu, Z., et al.: Event-triggered filter design for nonlinear cyber–physical systems subject to deception attacks. ISA Trans. 104, 130–137 (2020)
28. Chen, W., et al.: Distributed resilient filtering for power systems subject to denial-of-service attacks. IEEE Trans. Syst. Man. Cybern.: Systems 49(8), 1688–1697 (2019)
29. Tian, E., Wang, X., Peng, C.: Probabilistic-constrained distributed filtering for a class of nonlinear stochastic systems subject to periodic DoS attacks. IEEE Trans. Circuits Syst. I Regul. Pap. 67(12), 5369–5379 (2020)
30. Gu, Z., et al.: Event-triggered $\mathcal{H}_\infty$ filtering for T–S fuzzy-model-based nonlinear networked systems with multisensors against DoS attacks. IEEE. Trans. Cybern. 52(6), 5311–5321 (2020)
31. Ma, R., et al.: Resilient filtering for cyber-physical systems under denial-of-service attacks. Int. J. Robust Nonlinear Control 30(5), 1754–1769 (2020)
32. Gilbert, E.N.: Capacity of a burst-noise channel. Bell Syst. Tech. J. 39(5), 1253–1265 (1960)
33. Cetinkaya, A., Ishii, H., Hayakawa, T.: The effect of time-varying jamming interference on networked stabilization. SIAM J. Control Optim. 56(3), 2398–2435 (2018)
34. Xu, W., et al.: 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, pp. 46–57. ACM, New York (2005)
35. Lacerda, M.J., et al.: A new approach to handle additive and multiplicative uncertainties in the measurement for $\mathcal{H}_\infty$ LPV filtering. Int. J. Syst. Sci. 47(5), 1042–1053 (2016)
36. Aberkane, S.: Bounded real lemma for nonhomogeneous Markovian jump linear systems. IEEE Trans. Autom. Control 58(3), 797–801 (2012)
37. Palma, J.M., Morais, C.F., Oliveira, R.C.L.F.: $\mathcal{H}_\infty$ state-feedback gain-scheduled control for MJLS with non-homogeneous Markov chains. In: 2018 Annual American Control Conference (ACC), pp. 5718–5723. IEEE, Piscataway (2018)
38. Lacerda, M.J., Oliveira, R.C.L.F., Peres, P.L.D.: Robust $\mathcal{H}_2$ and $\mathcal{H}_\infty$ filter design for uncertain linear systems via LMIs and polynomial matrices. Signal Process. 91(5), 1115–1122 (2011)
39. Morais, C.F., et al.: $\mathcal{H}_2$ and $\mathcal{H}_\infty$ filter design for polytopic continuous-time Markov jump linear systems with uncertain transition rates. Int. J. Adapt. Control Signal Process. 29(10), 1207–1223 (2015)
40. Agulhari, C.M., et al.: Algorithm 998: The Robust LMI Parser - A Toolbox to Construct LMI Conditions for Uncertain Systems. ACM Trans. Math. Software 45(3), 36:1–36:25 (2019)
41. Löfberg, J.: YALMIP: A toolbox for modeling and optimization in MATLAB. In: Proceedings of the 2004 IEEE International Symposium on Computer Aided Control Systems Design, pp. 284–289. IEEE, Piscataway (2004). https://doi.org/10.1109/CACSD.2004.1393890
42. Andersen, E.D., Andersen, K.D.: The MOSEK interior point optimizer for linear programming: An implementation of the homogeneous algorithm. In: Frenk H. et al. (eds.) High Performance Optimization, Applied Optimization, vol. 33, pp. 197–232. Springer, New York (2000)
43. Duan, Z.S., et al.: Robust $\mathcal{H}_2$ and $\mathcal{H}_\infty$ filtering for uncertain linear systems. Automatica 42(11), 1919–1926 (2006)
44. Lee, D.H., Joo, Y.H., Tak, M.H.: Periodically time-varying $\mathcal{H}_\infty$ memory filter design for discrete-time LTI systems with polytopic uncertainty. IEEE Trans. Autom. Control 59(5), 1380–1385 (2014)

How to cite this article: Oliveira, P.M., Palma, J.M., Lacerda, M.J.: Filter design for cyber-physical systems against DoS attacks and unreliable networks: A Markovian approach. IET Control Theory Appl. 1–12 (2024). https://doi.org/10.1049/cth2.12703