A virtual actuator approach for the secure control of networked LPV systems under pulse-width modulated DoS attacks

Damiano Rotondo[a,b], Helem Sabina Sánchez[a,c], Vicenç Puig[a,b,c], Teresa Escobet[a,d], Joseba Quevedo[a,c]

[a]*Research Center for Supervision, Safety and Automatic Control (CS2AC)*
of the Universitat Politècnica de Catalunya (UPC), Spain
[b]*Institut de Robòtica i Informàtica Industrial (IRI), UPC-CSIC*
Carrer de Llorens i Artigas, 4-6, 08028 Barcelona, Spain
[c]*Automatic Control Department, UPC-ESAII,*
Rambla de Sant Nebridi, 11, 08222 Terrassa, Spain
[d]*Department of Mining, Industrial and ICT Engineering, UPC*
Av. de les Bases de Manresa, 61-73, 08242 Manresa, Spain

Abstract

In this paper, we formulate and analyze the problem of secure control in the context of networked linear parameter varying (LPV) systems. We consider an *energy-constrained*, *pulse-width modulated* (PWM) jammer, which corrupts the control communication channel by performing a denial-of-service (DoS) attack. In particular, the malicious attacker is able to erase the data sent to one or more actuators. In order to achieve secure control, we propose a virtual actuator technique under the assumption that the behavior of the attacker has been identified. The main advantage brought by this technique is that the existing components in the control system can be maintained without need of retuning them, since the virtual actuator will perform a reconfiguration of the plant, hiding the attack from the controller point of view. Using Lyapunov-based results that take into account the possible behavior of the attacker, design conditions for calculating the virtual actuators gains are obtained. A numerical example is used to illustrate the proposed secure control strategy.

Keywords: Cyber-physical systems, cyber attacks, denial-of-service, energy constraints, networked control systems, linear parameter varying systems, switched systems, virtual actuators.

1. Introduction

Modern control systems are composed of networked devices such as sensors, actuators and controllers, which transmit their information across a communication network [1]. Hence, networked control systems (NCSs) [2, 3] have become essential for controlling critical infrastructures, such as water distribution systems [4, 5] and smart grids [6]. However, in addition to being prone to failures as any other system, NCSs are also vulnerable to cyber attacks [7, 8], which affect the data management or communication layer, and introduce significant difficulties to secure and protect them [9, 10].

Over the last decades, concerns about the security of NCSs have been raised and related problems have been studied from the control theory point of view, with the application of fault diagnosis [11, 12] and fault tolerant control (FTC) [13, 14] techniques. Fault diagnosis techniques are used to detect, isolate and estimate faults, while FTC techniques are used to maintain the performance close to the desired one and preserve stability conditions despite the fault occurrence. It is worthwhile to highlight that a fault is considered a physical event that affects the system behavior, does not have an objective to fulfill and is a random event. On the other hand, cyber attacks are deliberate, performed in an intelligent way, and can spread in the network within seconds. Even though the existing fault diagnosis and FTC techniques can be a first action to face cyber attacks, the development of new tools, security mechanisms and algorithms is needed in order to address simultaneously physical and cyber disruptions, while also exploiting some known information about the attacker's behavior [15].

Cyber attacks can be classified into deception and denial-of-service (DoS) attacks (a.k.a. jamming attacks) [16]. Deception attacks refer to the possibility of compromising the integrity of control packets or measurements by altering the behavior of sensors and/or actuators [1, 17, 18, 19, 20, 21]; on the other hand, DoS attacks compromise the availability of resources, impeding the exchange of information between two entities by jamming the communication [22]. In this paper, we focus on DoS attacks, which are the most likely threat to NCSs, considering that some of them may be damaged and even become unstable, when affected by this kind of attack.

The design of detection and secure control strategies against DoS attacks has been investigated during the recent years. [16] and [23] have addressed the problem of finding optimal control and attack strategies assuming a maximum number of jamming actions over a prescribed control horizon for a resource-constrained attacker. Moreover, [23] used game theory to design the jamming attack strategy, by presenting a zero sum game to depict the combat between a controller and a strategic jammer. In [24], an integrated game-theoretic framework was developed to investigate the interactive decision making process between a sensor node and an attacker who can launch DoS attacks. The works [25, 26] have developed an explicit characterization of DoS frequency and duration for which closed-loop stability can be preserved by means of state feedback controllers. [27, 28] evaluated the effect of energy-constrained DoS attacks against linear quadratic gaussian (LQG) control and proposed the optimal DoS attack scheduling which can maximize the LQG cost. [29, 30] have studied pulse-width modulated (PWM) jammers attacking the control signals, for which the attack duration in each period is varying, while the attack frequency is fixed and known. On the other hand, [31] considered a DoS attack on the sensor signal, for which both the frequency of the attack and the duration were time-varying. The recent work [32] has addressed the distributed resilient filtering problem for a class of power systems subject to DoS attacks. Furthermore, [33] has proposed an event-triggered estimator design for cyber-physical systems with limited communication resources, sensor saturation and DoS attacks.

Note that in all the above works secure control (or estimation) against DoS attacks is achieved by considering an appropriate controller or observer that takes into account assumptions about the attacks during the design phase. However, in case a set of control system components is already available, it might be of interest to preserve them and achieve secure control by *adding* new components instead of *replacing* the existing ones. To this end, the active FTC technique known as *virtual actuator* might be of interest, since it is based on the idea of performing a reconfiguration of the plant when an unexpected situation occurs, such that the nominal controller can still be used without need of retuning it. Initially proposed for linear time invariant (LTI) systems [34], virtual actuators were later extended to linear parameter varying (LPV) [35, 36], hybrid [37], Takagi-Sugeno [38], piecewise affine [39], Hammerstein-Weiner [40], Lipschitz [41] and uncertain [42] systems. Note that the virtual actuator technique belongs to the wider class of *fault-hiding reconfiguration approaches*, among which there is the dual technique known as *virtual sensors*, that is employed when the considered faults affect the sensor outputs [43].

In this paper, we consider a remote control architecture in which the operator (remote control unit) uses a control channel to send wirelessly a control command to the actuators acting on a possibly unstable plant [29]. We would like to remark that such an architecture is more vulnerable to DoS attacks than co-located architectures (control unit co-located with the actuators), but does not require wired or

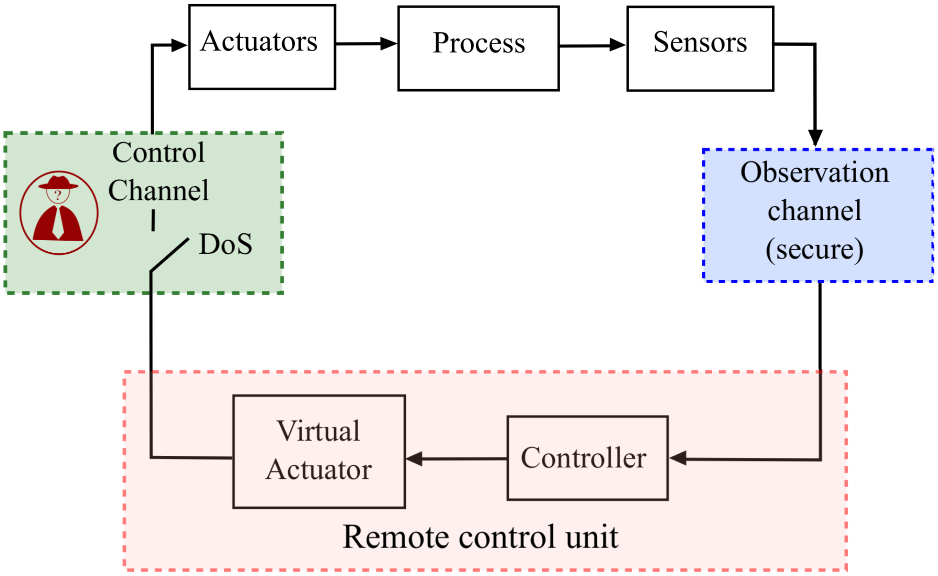

Figure 1: Schematic of the overall secure control architecture.

dedicated actuator channels, such that it might be preferred because of flexibility or economic issues [44]. Within this architecture, we consider that an attacker wishes to induce instability in the control system by denying communication on the control channel [26], and for this reason, we wish to introduce a virtual actuator in the loop in order to preserve stability in spite of the attacks (see Fig. 1 for a schematic of the overall architecture). We would like to point out that so far, the virtual actuator technique has been investigated under the assumption that persistent faults affect the actuators, which makes the design somehow simpler. However, when secure control against DoS attacks is of interest, a common assumption is that the attacker cannot disrupt persistently a communication channel, since it has a limited amount of available energy to perform the attack. As a consequence, state-of-the-art virtual actuator design methodologies are conservative, since they do not take into account the constraints brought by the attacker's behavior.

The main objective and contribution of this paper is to develop an approach for the design of virtual actuators for the secure control against DoS attacks performed by a PWM jammer that overcomes the above-mentioned conservativeness under the assumption that some information about the energy constraints that limit the attacker has been identified. In the proposed approach, the attacked system is modeled as a switched system [45], in which the different modes correspond to different sets of actuators being affected by the attack. Then, following some ideas proposed by [46], the design conditions are obtained by allowing the reconfigured closed-loop system under some attack conditions to not satisfy the desired specification (stability with prescribed decay rate), as long as the resulting effect on the used Lyapunov function is compensated by the behavior of the closed-loop system during the time in which other operating conditions hold, e.g. no attack being performed. The obtained conditions, which are based on multiple Lyapunov matrices, recall the ones available in the literature concerning the stability of switched systems with average dwell-time, see e.g. [47, 48, 49, 50], although they actually differ and are less conservative because they exploit useful information about the mode transitions provided by the constraints of the jamming policy. With the aim of enlarging the applicability of the developed approach, the virtual actuator-based secure control will be formulated within the LPV framework, which allows dealing with nonlinear systems using an extension of linear techniques [51, 52, 53]. Simulation results obtained with a numerical example are used to demonstrate the effectiveness of the proposed approach, as well as its most relevant features.

We would like to point out the existence of strong similarities between the PWM DoS attacks considered in this paper and other undesired phenomena that can affect NCSs. In particular, some works have investigated the case of intermittent faults [54, 55] within a stochastic framework, e.g., modeling the faulty system as a Markovian jump system [56, 57], contrarily to the approach developed in this paper, which makes deterministic assumptions about the attacker's behavior. Another similar problem investigated in the literature concerns the stabilization of NCSs under packet loss [58, 59], for which both stochastic and deterministic settings have been considered. In this latter case, however, the usual assumption is the existence of a fixed upper bound on the number of packets that could be not received by the actuators. On the other hand, the DoS attacks investigated in this paper are considered to be performed on purpose by an attacker who has some available amount of energy. Hence, the attacker could potentially choose between disabling permanently a small set of actuators or disrupt periodically for a shorter amount of time a wider set of actuators, which require different actions by the virtual actuators in order to maintain the overall stability of the NCS.

The paper is structured as follows. Section 2 presents the problem formulation. Then, in Section 3, the main concepts related to the virtual actuator technique are discussed, while in Section 4, the design conditions for the virtual actuator gains are described. Simulation results are shown in Section 5. Finally, the main conclusions are summarized in Section 6.

2. Problem formulation

Let us consider an LPV system described by the following state equation:

$$\dot{x}(t) = A(\theta(t))x(t) + B(\theta(t))u(t) \tag{1}$$

where $x(t) \in \mathbb{R}^{n_x}$ is the state vector, $u(t) \in \mathbb{R}^{n_u}$ is the input vector, and $A(\theta(t)) \in \mathbb{R}^{n_x \times n_x}$, $B(\theta(t)) \in \mathbb{R}^{n_x \times n_u}$ are time-varying matrices, whose values depend on the vector of varying parameters $\theta(t) \in \Theta \subset \mathbb{R}^{n_\theta}$.

The LPV system (1) is controlled by a state feedback control law:

$$u_c(t) = K(\theta(t))x(t) \tag{2}$$

where $K(\theta(t)) \in \mathbb{R}^{n_u \times n_x}$ is the LPV controller gain, which we assume that has been designed to ensure quadratic stability with a desired decay rate $\alpha < 0$ (in the following, this specification will be referred to as *quadratic α-stability*) of the closed-loop system obtained with $u(t) = u_c(t)$. This means that there exists a symmetric matrix $P \succ 0$ such that $\forall \theta \in \Theta$:

$$He\{(A(\theta) + B(\theta)K(\theta))P\} - \alpha P \prec 0 \tag{3}$$

where, for a given matrix A, $He(A) = A + A^T$.

Note that the quadratic α-stability specification corresponds to the Lyapunov function $V(x(t)) = x(t)^T P^{-1} x(t)$ satisfying:

$$\frac{\dot{V}(x(t))}{V(x(t))} < \alpha \qquad \forall t \in \mathbb{R} \tag{4}$$

and, by considering a time interval $[t, t+h]$:

$$V(x(t+h)) < e^{\alpha h} V(x(t)) \tag{5}$$

In this paper, it is assumed that the signal $u(t)$ is sent to the actuators through a network, that can be affected by DoS attacks, by means of which an adversary can destabilize the plant. More specifically, similarly to [23, 60], we assume that a malicious attacker performs a jamming attack in which (s)he is able to erase the data sent to one or more actuators. This type of attack can be modeled as a change in the input matrix of (1), such that the jammed system becomes:

$$\dot{x}(t) = A(\theta(t))x(t) + B_a(\theta(t), \gamma(t))u(t) \tag{6}$$

with:

$$B_a(\theta(t),\gamma(t)) = B(\theta(t))\,\Gamma(\gamma(t)) \tag{7}$$

$$\Gamma(\gamma(t)) = diag\,(\gamma_1(t),\ldots,\gamma_{n_u}(t)), \quad \gamma_i(t) \in \{0,1\} \tag{8}$$

where $\gamma_i(t) = 1$ represents the availability of the i-th actuator, whereas $\gamma_i(t) = 0$ indicates that the i-th actuator is not available anymore due to the jamming attack.

We consider an *energy-constrained*, *PWM* jammer such that the signals $\gamma_i(t)$ satisfy [29]:

$$\gamma_i(t) = \begin{cases} 1 & \text{if}\,(n-1)h \leq t \leq (n-1)h + t_i(n) \\ 0 & \text{if}\,(n-1)h + t_i(n) < t < nh \end{cases} \tag{9}$$

where $n \in \mathbb{N}$ is the period number, $h > 0$, and $[0,h]$ is the action-period of the jammer. Also, $\forall n \in \mathbb{N}$ and $\forall i = 1,\ldots,n_u$, $t_i(n) \in [0,h]$ denotes the time instant in which the jamming attack on the i-th input channel begins, while $\tau_i(n) > 0$ will indicate the duration of the time interval during which the i-th actuator is not available, obviously related to $t_i(n)$ by the relation:

$$\tau_i(n) = h - t_i(n) \tag{10}$$

We assume that, due to the above mentioned energy constraints, a *known* uniform bound $\bar{\tau}$ for $\sum_{i=1}^{n_u} \tau_i(n)$ exists, i.e.:

$$\sum\nolimits_{i=1}^{n_u} \tau_i(n) \leq \bar{\tau} < n_u h \tag{11}$$

which holds for all the periods ($\forall n \in \mathbb{N}$).

Let us recall that, given the set of actuators s_0 (*nominal* or *full* configuration) with cardinality n_u, a configuration is a subset of actuators s_j, $j = 0,1,\ldots,2^{n_u}-1$ (configuration j). Then, the set of all the configurations, denoted with $\mathscr{L}(s_0)$, is the power set of s_0 and is a lattice, which can be represented by a non-directed graph whose vertices are the configurations [61].

It is straightforward to realize that, at each time t, the value of the signal $\gamma(t)$ selects a specific configuration $s(t)$ from $\mathscr{L}(s_0)$. In the following, we will denote as $B_j(\theta(t))$ the value of the input matrix $B_a(\theta(t),\gamma(t))$ arising from $\gamma(t)$ selecting the configuration $s_j \in \mathscr{L}(s_0)$ and, similarly, as $B_0(\theta(t))$ the value of the input matrix corresponding to the configuration s_0, i.e. the nominal input matrix $B(\theta(t))$. Under the assumption that an estimation $\hat{s}(t)$ of $s(t)$ is available, we consider the control law:

$$u(t) = \begin{cases} u_c(t) & \text{if } \hat{s}(t) = s_0 \\ u_f^{(j)}(t) & \text{if } \hat{s}(t) = s_j, \quad j = 1,\ldots,2^{n_u}-1 \end{cases} \tag{12}$$

The problem considered in this paper is the design of $u_f^{(j)}(t)$, $j = 1, \ldots, 2^{n_u} - 1$, in order to ensure the average quadratic α^*-stability with $\alpha \leq \alpha^* < 0$ for any signal $\gamma(t)$ satisfying (9) (when the strict inequality holds, performance degradation with respect to the nominal performances is allowed).

Note that the term *average* has been used, in the sense that we will not require a constraint on the derivative of the Lyapunov function that holds $\forall t \in \mathbb{R}$, as in (4), but a weaker constraint on the decay of the Lyapunov function over a period of the jamming attack $[(n-1)h, nh]$:

$$V\left(x(nh)\right) < e^{\alpha^* h} V\left(x\left((n-1)h\right)\right) \tag{13}$$

In other words, similarly to [46], brief periods of α^*-instability are allowed, as long as their effect on $V\left(x(t)\right)$ is compensated by a stronger-than-α^*-stability during the remaining length of the action-period of the jammer.

In the remaining of the paper, in order to keep the mathematical formulation relatively simple, we will assume that an ideal jamming diagnosis algorithm is available, and we will develop the virtual actuator-based attack-hiding strategy under the assumption that $\hat{s}(t) = s(t)$. Considering a mismatch $\hat{s}(t) \neq s(t)$, although possible as, e.g., taking into account the results in [62], would increase the overall complexity and mathematical burden of the proposed solution, and goes beyond the scope of this paper.

3. Virtual actuator-based attack-hiding strategy

In this paper, the solution to the problem formulated in the previous section relies on the use of the virtual actuator technique. The main idea of this technique is to perform a reconfiguration of the plant such that the nominal controller can still be used without need of retuning it. The plant with the jammed actuators is modified adding the virtual actuator block, whose purpose is to hide the attack from the controller point of view (see Fig. 2 for a conceptual scheme).

More specifically, we employ an LPV virtual actuator whose structure is inspired by the one in [35], with the remarkable difference that it varies online depending on the specific value of $\hat{s}(t)$, i.e. when $\hat{s}(t) = s_j$, then:

$$\begin{aligned} \dot{x}_v(t) = {} & \left(A\left(\theta(t)\right) + B_j^*\left(\theta(t)\right) M_j\left(\theta(t)\right)\right) x_v(t) \\ & + \left(B\left(\theta(t)\right) - B_j^*\left(\theta(t)\right)\right)\left[u_c(t) + K\left(\theta(t)\right) x_v(t)\right] \end{aligned} \tag{14}$$

where $x_v(t) \in \mathbb{R}^{n_x}$ is the virtual actuator state, for which an initial condition $x_v(0) = 0$ is chosen, and $M_j\left(\theta(t)\right) \in \mathbb{R}^{n_u \times n_x}$ denotes the virtual actuator gains. The matrix

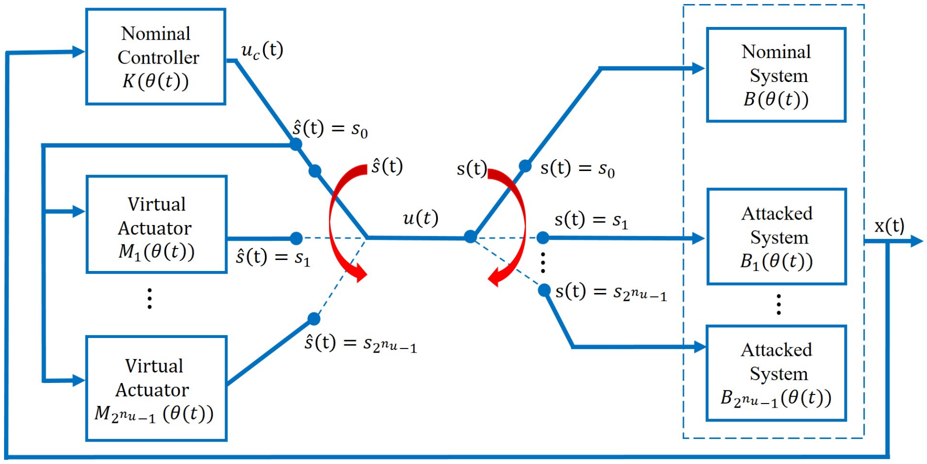
Nominal Controller $K(\theta(t))$
u_c(t)
$\hat{s}$(t) = s_0
$\hat{s}$(t)
Virtual Actuator $M_1(\theta(t))$
$\hat{s}$(t) = s_1
Virtual Actuator $M_{2^{n_u-1}}(\theta(t))$
$\hat{s}$(t) = $s_{2^{n_u-1}}$
$u(t)$
s(t)
s(t) = s_0
s(t) = s_1
s(t) = $s_{2^{n_u-1}}$
Nominal System $B(\theta(t))$
Attacked System $B_1(\theta(t))$
Attacked System $B_{2^{n_u-1}}(\theta(t))$
x(t)

Figure 2: Conceptual scheme of the proposed attack-hiding strategy.

functions $B_j^*(\theta(t))$ are calculated as:

$$B_j^*(\theta(t)) = B_j(\theta(t)) N_j(\theta(t)) \tag{15}$$

with:

$$N_j(\theta(t)) = B_j(\theta(t))^{\dagger} B(\theta(t)) \tag{16}$$

where † denotes the Moore-Penrose pseudoinverse.

Then, $u_f^{(j)}(t)$ in (12) is selected as follows:

$$u_f^{(j)}(t) = N_j(\theta(t)) \left(u_c(t) + K(\theta(t)) x_v(t) - M_j(\theta(t)) x_v(t)\right) \tag{17}$$

Thanks to the introduction of the virtual actuator block, the *separation principle* holds for the augmented system made up by the LPV system and the LPV virtual actuator, i.e. the augmented system can be brought to a block-triangular form, as stated in the following theorem.

Theorem 1. *Consider the augmented system made up by the LPV system's state equation* (6) *with* $B_a(\theta(t), \gamma(t)) = B_j(\theta(t))$*, the control law* (12) *with* $u_c(t)$ *as in* (2) *and* $u_f^{(j)}(t)$ *as in* (17)*, and the LPV virtual actuator's state equation* (14)*:*

$$\begin{pmatrix} \dot{x}(t) \\ \dot{x}_v(t) \end{pmatrix} = \Xi(\theta(t)) \begin{pmatrix} x(t) \\ x_v(t) \end{pmatrix} \tag{18}$$

$$\Xi(\theta) = \begin{pmatrix} A(\theta) + B_j^*(\theta)K(\theta) & \Xi_x(\theta) \\ \Xi_v(\theta) & A(\theta) + B_j^*(\theta)M_j(\theta) + \Xi_v(\theta) \end{pmatrix} \tag{19}$$

$$\Xi_x(\theta) = \begin{cases} 0 & \text{if } \hat{s}(t) = s_0 \\ B_j^*(\theta)\left[K(\theta) - M_j(\theta)\right] & \text{if } \hat{s}(t) = s_j,\ j = 1, \ldots, 2^{n_u} - 1 \end{cases}$$

$$\Xi_v(\theta) = \begin{cases} 0 & \text{if } \hat{s}(t) = s_0 \\ \left[B(\theta) - B_j^*(\theta)\right]K(\theta) & \text{if } \hat{s}(t) = s_j,\ j = 1, \ldots, 2^{n_u} - 1 \end{cases}$$

Then, there exists a similarity transformation such that the state matrix of the augmented system in the new state variables is block-triangular, as follows:

$$\Xi_z(\theta) = \begin{pmatrix} A(\theta) + B(\theta)K(\theta) & 0 \\ \Xi_v(\theta) & A(\theta) + B_j^*(\theta)M_j(\theta) \end{pmatrix} \tag{20}$$

Proof: It follows from considering the change of variables:

$$\begin{pmatrix} z(t) \\ x_v(t) \end{pmatrix} = T \begin{pmatrix} x(t) \\ x_v(t) \end{pmatrix} = \begin{pmatrix} I & I \\ 0 & I \end{pmatrix} \begin{pmatrix} x(t) \\ x_v(t) \end{pmatrix}$$

Then:

$$\Xi_z(\theta(t)) = T\,\Xi(\theta(t))\,T^{-1}$$

with $\Xi_z(\theta)$ given by (20). □

The following theorem shows that for continuous-time LPV systems in block-triangular form, the quadratic α-stability can be obtained from the quadratic α-stability of the subsystems in the diagonal.

Theorem 2. *Consider the following continuous-time LPV system:*

$$\dot{x}(t) = \Xi(\theta(t))x(t) = \begin{pmatrix} \Xi_{11}(\theta(t)) & 0 \\ \Xi_{21}(\theta(t)) & \Xi_{22}(\theta(t)) \end{pmatrix} x(t) \tag{21}$$

and assume that the subsystems $\dot{x}_1(t) = \Xi_{11}(\theta(t))x_1(t)$ and $\dot{x}_2(t) = \Xi_{22}(\theta(t))x_2(t)$ are quadratically α-stable, with $\alpha \in \mathbb{R}$. Then, (21) *is quadratically α-stable.*

Proof: The quadratic α-stability of $\dot{x}_1(t) = \Xi_{11}(\theta(t))$ implies the existence of a symmetric matrix $P_1 \succ 0$ such that $\forall \theta \in \Theta$:

$$\Xi_{11}(\theta)P_1 + P_1\Xi_{11}(\theta)^T - \alpha P_1 \prec 0 \tag{22}$$

Similarly, the quadratic α-stability of $\dot{x}_2(t) = \Xi_{22}(\theta(t))$ implies the existence of a symmetric matrix $P_2 \succ 0$ such that $\forall\theta \in \Theta$:

$$\Xi_{22}(\theta)P_2 + P_2\Xi_{22}(\theta)^T - \alpha P_2 \prec 0 \tag{23}$$

In the following, it is proved that there exists $\varepsilon > 0$ such that:

$$P = \begin{pmatrix} P_1 & 0 \\ 0 & \varepsilon P_2 \end{pmatrix} \succ 0 \tag{24}$$

satisfies:

$$\Xi(\theta)P + P\Xi(\theta)^T - \alpha P \prec 0 \tag{25}$$

In fact, (24) and (25) lead to the equivalent matrix inequality:

$$\begin{pmatrix} \Xi_{11}(\theta)P_1 + P_1\Xi_{11}(\theta)^T - \alpha P_1 & P_1\Xi_{21}(\theta)^T \\ \Xi_{21}(\theta)P_1 & \varepsilon\left(\Xi_{22}(\theta)P_2 + P_2\Xi_{22}(\theta)^T - \alpha P_2\right) \end{pmatrix} \prec 0 \tag{26}$$

that, using Schur complements, is equivalent to (22) and:

$$\begin{aligned} &\varepsilon\left(\Xi_{22}(\theta)P_2 + P_2\Xi_{22}(\theta)^T - \alpha P_2\right) \\ &\quad - \Xi_{21}(\theta)P_1\left(\Xi_{11}(\theta)P_1 + P_1\Xi_{11}(\theta)^T - \alpha P_1\right)^{-1} P_1\Xi_{21}(\theta)^T \prec 0 \end{aligned} \tag{27}$$

Since (23) holds $\forall\theta \in \Theta$, the proof is completed by showing that, given a matrix $Z \prec 0$ and a matrix W of the same order, there exists $\varepsilon > 0$ such that $\varepsilon Z - W \prec 0$. In fact, for any vector v:

$$\begin{aligned} v^T Z v &\leq \sigma_Z \|v\|^2 \\ v^T W v &\leq \sigma_W \|v\|^2 \end{aligned}$$

where σ_Z and σ_W denote the maximum eigenvalues of Z and W, with $\sigma_Z < 0$ due to the negative definiteness of Z. Hence, $v^T(\varepsilon Z - W)v \leq (\varepsilon\sigma_Z - \sigma_W)\|v\|^2$ and $(\varepsilon\sigma_Z - \sigma_W)\|v\|^2 < 0$ when $\varepsilon\sigma_Z < \sigma_W$. Hence, $\varepsilon\sigma_Z - \sigma_W < 0$ from the definition of negative definite matrix, which completes the proof. □

The theoretical result given in Theorem 2 is important because, when combined with Theorem 1, shows that, due to the introduction of the virtual actuator block which hides the attack, the average quadratic α^*-stability of the augmented system (the problem formulated in the previous section) can be achieved as long as the virtual actuator gains $M_j(\theta)$ are designed such that the system $\dot{x}_v(t) = \Big(A\left(\theta(t)\right) + B_j^*\left(\theta(t)\right) M_j\left(\theta(t)\right)\Big) x_v(t)$ is quadratically α^*-stable for each $j = 0,\ldots,2^{n_u}-1$. However, this is not always possible. For example, let us consider the case in which $A(\theta)$ is unstable. Then, for the configuration corresponding to all-jammed actuators ($\gamma_i = 1 \forall i = 1,\ldots,n_u$), $B_j^*(\theta) = 0$, which means that it is impossible to achieve the quadratic α^*-stability of $\dot{x}_v(t) = \Big(A\left(\theta(t)\right) + B_j^*\left(\theta(t)\right)$ $M_j\left(\theta(t)\right)\big) x_v(t)$. Luckily, the information about the jamming attack policy (9) can be exploited in order to obtain design conditions that allow achieving the desired specification of average quadratic α^*-stability in spite of the possible loss of stabilizability caused by the jamming attack.

4. Design conditions

In order to obtain design conditions for the virtual actuator gains, first let us provide the following theorem.

Theorem 3. *Let us consider the switched LPV system:*

$$\dot{x}(t) = A_{\gamma(t)}\left(\theta(t)\right) x(t) \tag{28}$$

where A_γ is a function that assigns to each $\gamma^* \in \mathscr{L}(\gamma) = \{0,1\} \times \ldots \times \{0,1\} \subset \mathbb{N}^{n_u}$ an LPV system $\dot{x}(t) = A_{\gamma^*}\left(\theta(t)\right) x(t)$, and let us denote as $\mathscr{L}_k(\gamma)$, $k = 0,\ldots,n_u$, the sets of $\gamma^* \in \mathscr{L}(\gamma)$ with k elements equal to 0 (obviously, $\bigcup_{k=0}^{n_u} \mathscr{L}_k(\gamma) = \mathscr{L}(\gamma)$), and as $\mathscr{L}_{k\to k+1}^{\gamma^*}(\gamma)$, $k = 0,\ldots,n_u-1$, the set of $\gamma^{**} \in \mathscr{L}_{k+1}(\gamma)$ that can be obtained from $\gamma^* \in \mathscr{L}_k(\gamma)$ by changing one, and only one, of the 1 into 0. Moreover, let $\alpha^* \in \mathbb{R}$ and let $\gamma(t)$ satisfy the energy-constrained, PWM jamming policy defined by (9)-(11). *If there exist 2^{n_u} symmetric matrices $P_{\gamma^*} \succ 0$, $\gamma^* \in \mathscr{L}(\gamma)$, and scalars $\alpha_k, \mu_k \in \mathbb{R}$ with $\mu_k > 1$, $k = 0,\ldots,n_u$, such that:*

$$\sum_{k=0}^{n_u} \ln\left(\mu_k\right) + \alpha_h \leq \alpha^* h \tag{29}$$

$$P_{\gamma^{**}} \preceq \mu_k P_{\gamma^*} \quad \forall \gamma^* \in \mathscr{L}_k(\gamma), \forall \gamma^{**} \in \mathscr{L}_{k\to k+1}^{\gamma^*}(\gamma) \tag{30}$$

$$P_{\{1,1,\ldots,1\}} \preceq \mu_{n_u} P_{\{0,0,\ldots,0\}} \tag{31}$$

$$A_{\gamma^*}(\theta) P_{\gamma^*} + P_{\gamma^*} A_{\gamma^*}(\theta)^T - \alpha_k P_{\gamma^*} \prec 0 \quad \forall \gamma^* \in \mathscr{L}_k(\gamma), \forall \theta \in \Theta \tag{32}$$

with α_h defined as:

$$\alpha_h = \max_{\substack{\tau_1^*, \ldots, \tau_{n_u}^* \\ s.t. \begin{cases} \sum_{k=1}^{n_u} k\tau_k^* \leq \bar{\tau} \\ \tau_k^* \geq 0 \quad \forall k \in \{1,\ldots,n_u\} \end{cases}}} \alpha_0 \left(h - \tau_1^*\right) + \sum_{k=1}^{n_u-1} \alpha_k \left(\tau_k^* - \tau_{k+1}^*\right) + \alpha_{n_u} \tau_{n_u}^* \quad (33)$$

then the switched LPV system (28) *is quadratically α^*-stable in average over the period* $[(n-1)h, nh]$.

Proof: Let us consider the Lyapunov function $V(x(t)) = x(t)^T P_{\{1,1,\ldots,1\}}^{-1} x(t)$, and let us denote as $t_k^*(n) \in [0,h]$, $k = 0,\ldots,n_u$, the time relative to the interval $[(n-1)h, nh]$ starting from which k elements of $\gamma(t)$ are equal to 0. Then, the following holds due to (30)-(32):

$$V(x(nh)) < \prod_{k=0}^{n_u} \mu_k \left(\prod_{k=0}^{n_u-1} e^{\alpha_k \left(t_{k+1}^*(n) - t_k^*(n)\right)} \right) e^{\alpha_{n_u} \left(h - t_{n_u}^*(n)\right)} V\left(x((n-1)h)\right) \quad (34)$$

By combining (34) with (13), it follows that quadratic α^*-stability in average is achieved if:

$$\sum_{k=0}^{n_u} \ln(\mu_k) + \sum_{k=0}^{n_u-1} \alpha_k \left(t_{k+1}^*(n) - t_k^*(n)\right) + \alpha_{n_u} \left(h - t_{n_u}^*(n)\right) \leq \alpha^* h \qquad (35)$$

which, by denoting as $\tau_k^*(n) \geq 0$ the duration of the time interval during which k elements of $\gamma(t)$ are equal to 0, can be rewritten as:

$$\sum_{k=0}^{n_u} \ln(\mu_k) + \alpha_0 \left(h - \tau_1^*(n)\right) + \sum_{k=1}^{n_u-1} \alpha_k \left(\tau_k^*(n) - \tau_{k+1}^*(n)\right) + \alpha_{n_u} \tau_{n_u}^*(n) \leq \alpha^* h \quad (36)$$

From (11), it follows that:

$$\sum_{k=0}^{n_u} k\tau_k^*(n) \leq \bar{\tau} \qquad (37)$$

Hence, since α_h is defined as in (33), if (29) holds, then (35) holds as well, which completes the proof. □

Note that Theorem 3 recalls similar results available in the literature about switched systems, that make use of the concept of average dwell-time in order to assess stability or other specifications, see e.g. [47]. However, a relevant difference is that Theorem 3 is less conservative because it exploits useful information about the mode transitions provided by the constraints of the jamming policy. On the basis of Theorems 1-3, the following corollary can be provided for the design of the virtual actuator gains.

Corollary 1. *Let $\alpha^* \in \mathbb{R}$ and let $\gamma(t)$ satisfy the energy-constrained, PWM jamming policy defined by* (9)-(11)*. If there exist 2^{n_u} symmetric matrices $P_{\gamma^*} \succ 0$, $\gamma^* \in \mathscr{L}(\gamma)$, and scalars $\alpha_k, \mu_k \in \mathbb{R}$ with $\mu_k > 1$, $k = 0, \dots, n_u$, such that* (29)-(31) *hold with α_h defined as in* (33) *and $\forall j \in \{0, \dots, 2^{n_u} - 1\}$, $\forall \theta \in \Theta$:*

$$He\{A(\theta)P_j + B_j^*(\theta)\Gamma_j(\theta)\} - \alpha_{k(j)}P_j \prec 0 \tag{38}$$

where $k(j)$ corresponds to the number of jammed actuators in the configuration s_j, then the augmented system made up by the LPV system's state equation (6) *with $B_a(\theta(t), \gamma(t)) = B_j(\theta(t))$, the control law* (12) *with $u_c(t)$ as in* (2) *and $u_f^{(j)}(t)$ as in* (17)*, and the LPV virtual actuator's state equation* (14)*, with the virtual actuator gains given by $M_j(\theta(t)) = \Gamma_j(\theta(t))P_j^{-1}$, is quadratically α^*-stable in average over the period $[(n-1)h, nh]$.*

Proof: It follows from Theorems 1-3 by considering the change of variables $\Gamma_j(\theta) = M_j(\theta)P_j$. □

The main difficulty using Corollary 1 for design is the infinite number of constraints that (38) imposes. A common approach for obtaining a finite number of LMIs, which are computationally tractable, is to consider polytopic models. Following [63], by considering an LPV system as in (1) for which the input matrix is constant, i.e. $B(\theta(t)) = B\,\forall\theta \in \Theta$, and the state matrix can be represented by a parameter-varying convex combination of the so-called *vertex matrices*, as follows:

$$A(\theta(t)) = \sum_{l=1}^{N} \pi_l(\theta(t))A_l \tag{39}$$

with:

$$\begin{cases} \sum\limits_{l=1}^{N} \pi_l(\theta(t)) = 1 \\ \pi_l(\theta(t)) \geq 0 \end{cases} \qquad \forall\theta \in \Theta \tag{40}$$

where $\pi_l, l = 1, \dots, N$ denote the coefficients of the polytopic decomposition, and N denotes the number of vertex matrices. Hence, by choosing the virtual actuator gains to be polytopic, with the same coefficients of (39):

$$M_j(\theta(t)) = \sum_{l=1}^{N} \pi_l(\theta(t)) M_{j,l} \tag{41}$$

Eq. (38) is equivalent to:

$$He\{A_l P_j + B_j^* \Gamma_{j,l}\} - \alpha_{k(j)} P_j \prec 0 \quad \forall l = 1, \ldots, N \tag{42}$$

5. Numerical example

Let us consider an LPV system as in (1) with matrices:

$$A(\theta(t)) = \begin{bmatrix} 3+\theta(t) & 3 & -5+\theta(t) \\ 3+2\theta(t) & 3 & -1 \\ 5 & 3-\theta(t) & -10 \end{bmatrix} \qquad B = \begin{bmatrix} 10 & 1 \\ 7 & 4 \\ 2 & 1 \end{bmatrix} \tag{43}$$

and $\theta(t) \in [1,2]$, for which a quadratic α-stabilizing controller has been designed with $\alpha = -40$, solving (3) using the YALMIP toolbox [64] with SeDuMi solver [65]:

$$K(\theta(t)) = \begin{bmatrix} -6.70+0.20\theta(t) & 6.12-1.03\theta(t) & -26.22+2.63\theta(t) \\ 20.15+1.18\theta(t) & -32.58-3.23\theta(t) & 100.37+11.56\theta(t) \end{bmatrix} \tag{44}$$

The controlled system has an interesting property to show the relevant features of our secure control approach: it becomes unstable in the case of a jamming attack, independently from whether one or both control inputs are being made unavailable by the jammer. In fact, Fig. 3 shows the real part of the dominant pole of the closed-loop system, obtained for frozen values of the varying parameter $\theta(t)$ and for the four possible configurations $s_0 = \{1,1\}$ (no jammed actuators), $s_1 = \{1,0\}$ (jamming attack on the second actuator), $s_2 = \{0,1\}$ (jamming attack on the first actuator), and $s_3 = \{0,0\}$ (all actuators jammed). It can be seen that for all the configurations s_1, s_2, s_3, and for all the values $\theta \in [1,2]$, the real part of the dominant pole is positive which, through a frozen-value reasoning, is a sufficient condition to state instability of the closed-loop system.

Let us consider an energy-constrained, PWM jammer described by (9)-(11) with $h = 7s$ and $\bar{\tau} = 9s$, and let us apply Corollary 1 for the design of the virtual actuator gains $\alpha^* = 0$, $\alpha_0 = -40$, $\alpha_1 = -10$, $\alpha_2 = 20$ and $\mu_0 = \mu_1 = \mu_2 = 5$. For these values, (29) is verified with $\sum_{k=0}^{n_u} \ln(\mu_k) + \alpha_h = -5.17 \leq 0$, and a feasible

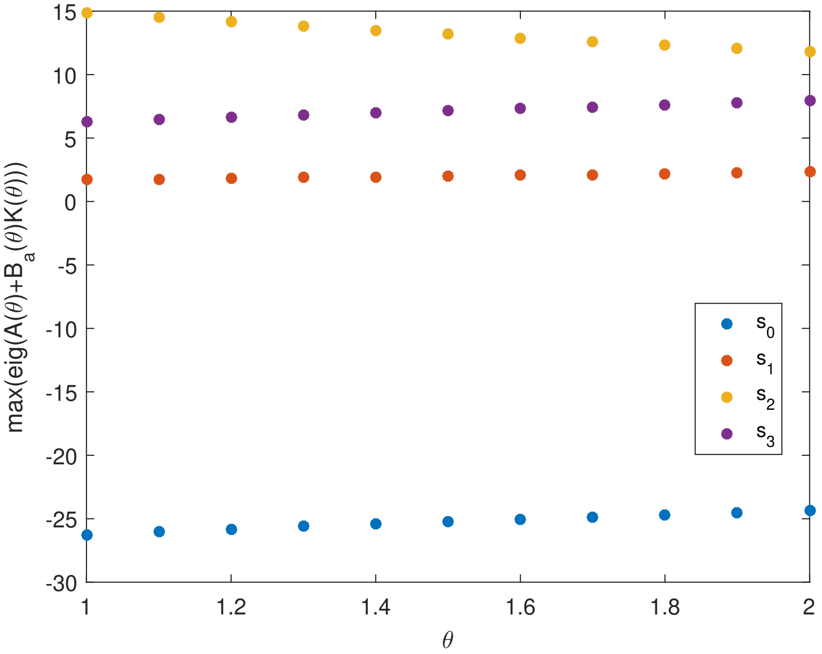

Figure 3: Real part of the dominant pole of the closed-loop system without secure control.

solution for (30)-(31) and (42) is obtained using YALMIP/Sedumi [64, 65], with the symmetric matrices P_{γ^*}, $\gamma^* \in \{(0,0),(0,1),(1,0),(1,1)\}$, given by:

$$P_{\{0,0\}} = \begin{bmatrix} 0.631 & -0.018 & -0.064 \\ -0.018 & 0.558 & 0.169 \\ -0.064 & 0.169 & 0.074 \end{bmatrix} \qquad P_{\{0,1\}} = \begin{bmatrix} 0.788 & 0.421 & 0.154 \\ 0.421 & 0.260 & 0.092 \\ 0.154 & 0.092 & 0.092 \end{bmatrix}$$

$$P_{\{1,0\}} = \begin{bmatrix} 0.064 & 0.246 & 0.059 \\ 0.246 & 1.757 & 0.400 \\ 0.059 & 0.400 & 0.150 \end{bmatrix} \qquad P_{\{1,1\}} = \begin{bmatrix} 0.136 & 0.004 & -0.004 \\ 0.004 & 0.128 & 0.036 \\ -0.004 & 0.036 & 0.059 \end{bmatrix}$$

and the virtual actuator gains obtained as $M_{\{1,1\}}(\theta(t)) = 0$ and:

$$M_{\{0,0\}}(\theta(t)) = \begin{bmatrix} -3.99+0.03\theta(t) & 3.22-0.50\theta(t) & -10.87+1.18\theta(t) \\ 7.49+0.49\theta(t) & -12.24-1.86\theta(t) & 21.55+7.06\theta(t) \end{bmatrix}$$

$$M_{\{0,1\}}(\theta(t)) = \begin{bmatrix} 0.50+1.07\theta(t) & -3.66-2.48\theta(t) & 2.84+0.71\theta(t) \\ 1.02-0.09\theta(t) & 7.56-0.67\theta(t) & -25.95+2.30\theta(t) \end{bmatrix}$$

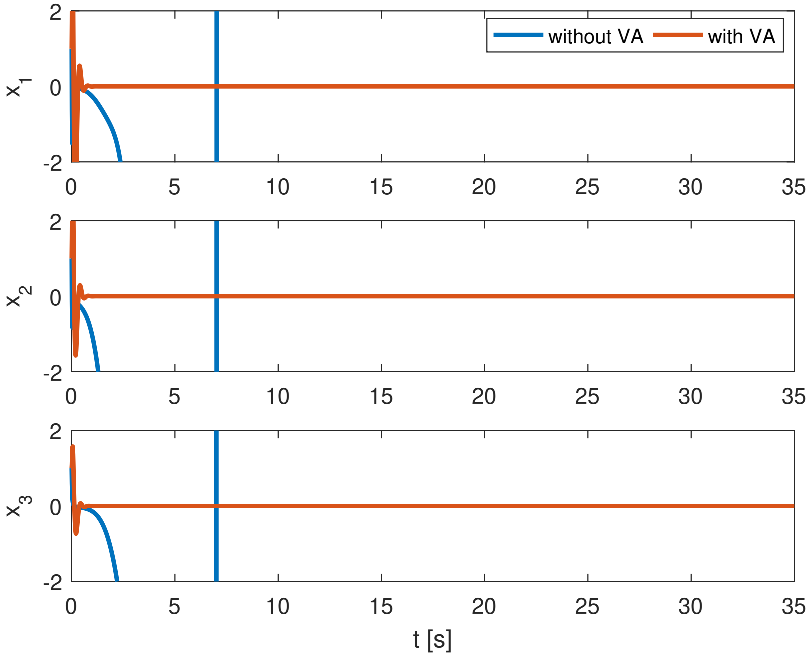

Figure 4: State response in Scenario 1 with and without virtual actuators.

$$M_{\{1,0\}}(\theta(t)) = \begin{bmatrix} -7.14-2.37\theta(t) & -1.48+0.23\theta(t) & 6.73+0.31\theta(t) \\ 1.45-0.61\theta(t) & 3.71-1.55\theta(t) & -17.17+7.18\theta(t) \end{bmatrix}$$

Let us consider the following two scenarios:

- **Scenario 1:** The jammer attacks alternatively the first and the second actuator for the whole action-period $[0,h]$;
- **Scenario 2:** In each action-period, no attack is performed in $[0,h-3\bar{\tau}/4]$. Then, in $[h-3\bar{\tau}/4,h-\bar{\tau}/4]$, the jammer attacks alternatively the first and the second actuator. Finally, in $[h-\bar{\tau}/4,h]$, both actuators are affected by the jamming attack.

For each scenario, a simulation lasting $5h=35\,s$, starting from the initial condition $x(0)=[1,1,1]^T$, and with a trajectory of the varying parameter given by $\theta(t)=1.5+0.5\sin(2\pi t/3)$ has been obtained. Fig. 4 shows a comparison of the state responses in Scenario 1 between the case without virtual actuators and with virtual actuators. It can be seen that, in spite of clear instability in the case

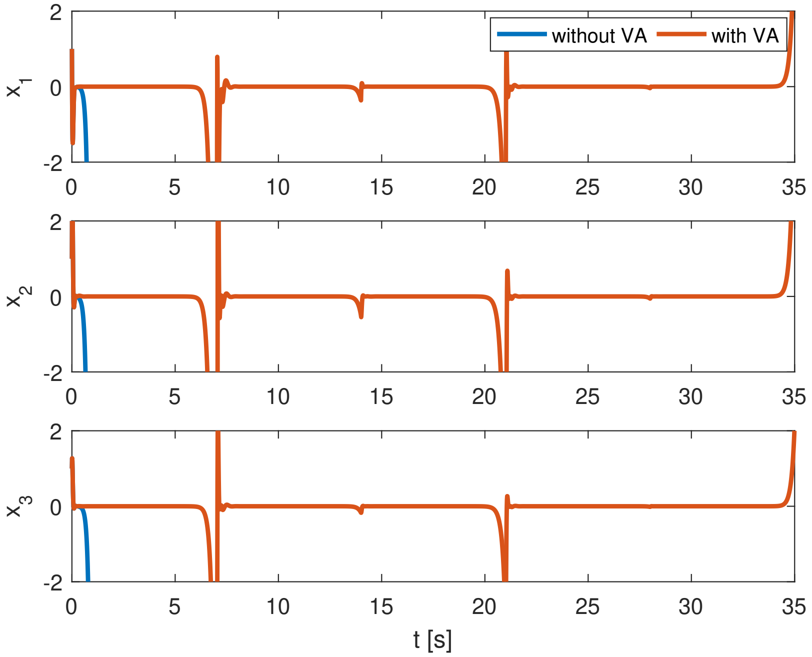

Figure 5: State response in Scenario 2 with and without virtual actuators.

without virtual actuators (blue line), the activation of the secure control technique leads to stability of the closed-loop system in spite of the attack being performed (red line). The same is true for Scenario 2 with the difference that some periods of brief instability appear when both actuators are being attacked. However, thanks to the virtual actuators, the closed-loop system remains stable in average.

Let us now consider a jammer which has less available energy to perform the attack, represented by a lower value $\bar{\tau} = 5\,s$. In this case, Corollary 1 can be applied with $\alpha^* = 0$, $\alpha_0 = -40$, $\alpha_1 = 10$, $\alpha_2 = 20$ and $\mu_0 = \mu_1 = \mu_2 = 5$, thus allowing for instability of the closed-loop system when even only one of the two actuators is being attacked. For these values, (29) is verified with $\sum_{k=0}^{n_u} \ln(\mu_k) + \alpha_h = -0.17 \leq 0$ (presentation of the symmetric matrices P_{γ^*} and virtual actuator gains, which provide feasibility of (30)-(31) and (42), is omitted). For this case, the following scenario will be considered in order to assess the performance of the proposed secure control technique.

- **Scenario 3:** In each action-period, no attack is performed in $[0, h - \bar{\tau}]$. Then, in $[h - \bar{\tau}, h]$, the jammer attacks the second actuator.

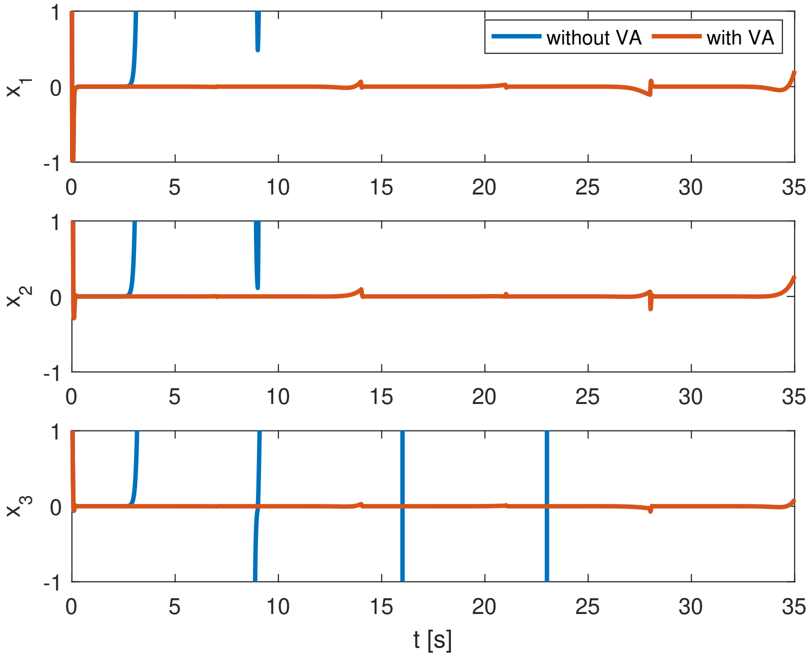

Figure 6: State response in Scenario 3 with and without virtual actuators.

The state response for Scenario 3 is shown in Fig. 6. It can be seen that without the virtual actuator strategy, the closed-loop system exhibits instability, whereas for the case with virtual actuators, in spite of brief instabilities allowed by the choice $\alpha_1 = 10$, the system remains stable in average. It is worth remarking that in this case the role of the virtual actuator in the case of configuration s_2 is to reduce the real part of the dominant pole of the closed-loop system under attack, as shown in Fig. 7, such that, roughly speaking, it presents a *slower* unstable response than without the secure control technique.

Finally, in order to conclude the presentation of the proposed secure control technique, let us analyze the evolution of the Lyapunov function $V(x(t))$ over different action-periods of the jammer, as shown in Fig. 8, where for the sake of illustration, $V(x(t))$ has been normalized with respect to its value at the beginning of each action-period, i.e., at $t = (n-1)h$. The figure shows that before the occurrence of the DoS attack, the Lyapunov function decreases monotonically, whereas during the attack, it could increase again. However, in spite of the brief instabilities induced by the attack, the Lyapunov function is overall decreasing over the

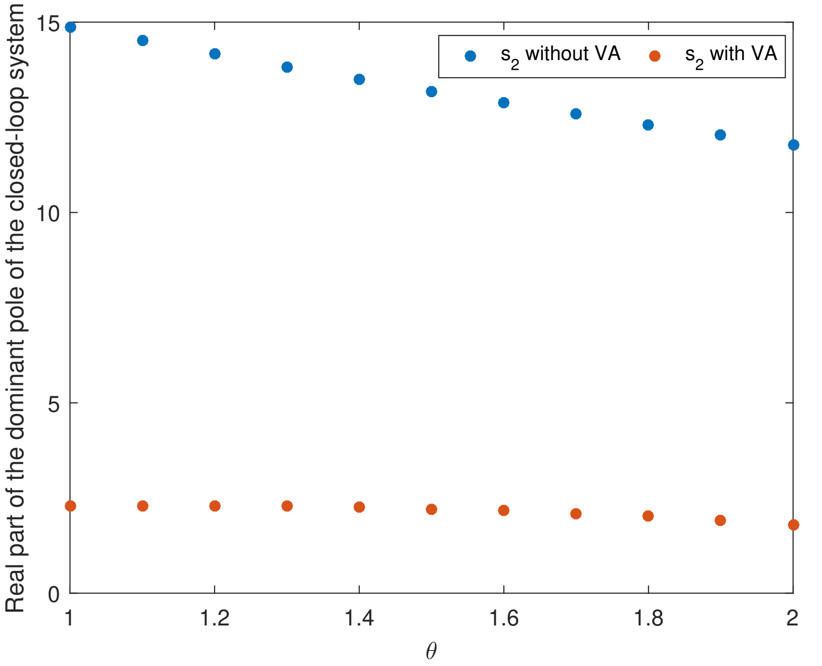

Figure 7: Real part of the dominant pole of the closed-loop system with and without secure control for the configuration s_2.

action-period of the jammer.

6. Conclusions

In this paper, we have considered the secure control against DoS attacks using a virtual actuator-based strategy for networked LPV control systems in which one or more actuators are lost during the attack. It has been shown that, thanks to the introduction of the virtual actuator block, the separation principle holds for the augmented system made up by the LPV plant plus the LPV virtual actuator, i.e. the augmented system can be brought to a block-triangular form. As a consequence, the design of the virtual actuator can be performed independently from the design of the controller. More specifically, the design has been performed by requiring that the desired specification (stability with prescribed decay rate of the Lyapunov function) holds in average, which means that under some attack conditions the reconfigured closed-loop system is allowed to infringe upon the desired specification, as long as the resulting effect of such violation on the Lyapunov function

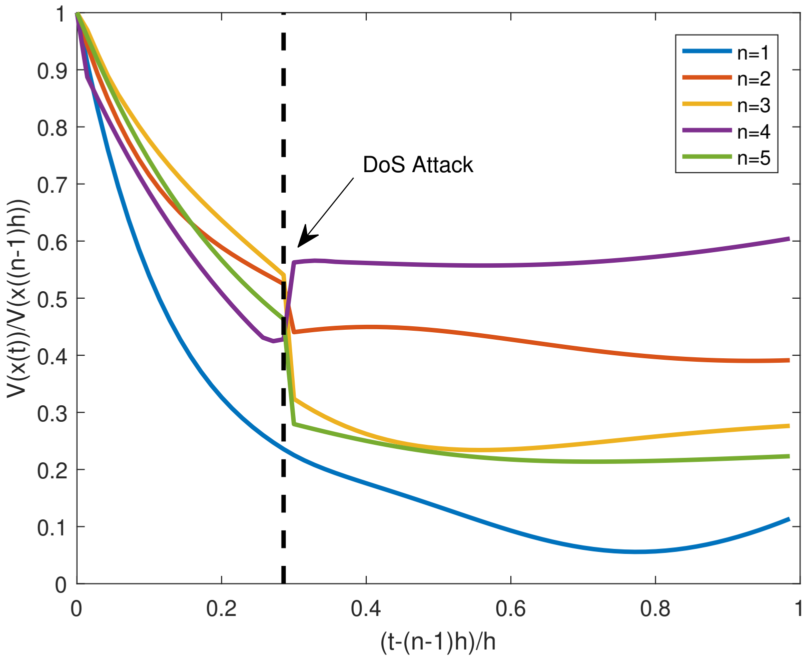

Figure 8: Evolution of the Lyapunov function over different action-periods of the jammer.

is compensated by the behavior under the remaining conditions. By taking into account some information about the energy constraints that limit the attacker, it is possible to obtain design conditions based on multiple Lyapunov matrices, which allow calculating the virtual actuator gains in order to achieve the desired specification. Simulation results obtained with a numerical example have demonstrated the effectiveness of the proposed approach, as well as its most relevant features.

Future work will aim at extending the virtual actuator-based secure control strategy to other types of cyber attacks, as well as to other possible jamming policies and to the case in which the identification of the attacker's behavior is delayed in time. Moreover, the case where the sensor-to-controller channel can be attacked will be considered by means of the virtual sensor approach. Finally, validation of the proposed approach with practically motivated problems, such as secure control of multi-agent systems, will be also addressed by future research.

Acknowledgments

This work has been partially funded by the Spanish State Research Agency (AEI) and the European Regional Development Fund (ERFD) through the projects SCAV (ref. MINECO DPI2017-88403-R) and DEOCS (ref. MINECO DPI2016-76493). This work has been also supported by the AEI through the Maria de Maeztu Seal of Excellence to IRI (MDM-2016- 0656) and the grant Juan de la Cierva-Formacion (FJCI-2016-29019).

Damiano Rotondo was born in Francavilla Fontana, Italy, in 1987. He received the B.S. degree from the Second University of Naples, Italy, the M.S. degree from the University of Pisa, Italy, and the Ph.D. degree from the Universitat Politècnica de Catalunya, Spain in 2008, 2011 and 2016, respectively. Since February 2018, he is a Juan de la Cierva fellow at the Institut de Robòtica i Informàtica Industrial (IRI) at the Spanish National Research Council (CSIC). His main research interests include gain-scheduled control systems, fault detection and isolation (FDI) and fault tolerant control (FTC) of dynamic systems. He has published several papers in international conference proceedings and scientific journals.

Helem Sabina Sánchez was born in Herrera, Panamá, in 1986. She received the Electronics and Telecommunications Engineering degree in 2010 from Universidad Tecnológica de Panamá, the M.Sc. in Multimedia Technologies degree and the Ph.D. degree in Telecommunications and Systems Engineering, both from the Universitat Autònoma de Barcelona, Spain, in 2011 and 2016, respectively. She has visited the Department of Mechanical and Industrial Engineering of the Università degli Studi di Brescia from November 2014 to June 2015. Since January 2017, she is a postdoctoral researcher at the Research Centre for Supervision, Safety and Automatic Control (CS2AC) of the Universitat Politècnica de Catalunya. Her main research interests include computational intelligence methods, multi-objective optimization, multi-criteria decision making for control engineering and secure control systems.

Vicenç Puig was born Spain in 1969. He received the PhD degree in control engineering in 1999 and the telecommunications engineering degree in 1993, both from Universitat Politècnica de Catalunya (UPC), Barcelona, Spain. He is currently a full professor of automatic control and the leader of the Advanced Control Systems (SAC) research group of the Research Center for Supervision, Safety and Automatic Control (CS2AC) at UPC. His main research interests are in fault detection, isolation and fault-tolerant control of dynamic systems. He has been involved in several European projects and networks, and has published many papers in international conference proceedings and scientific journals.

Teresa Escobet received a degree in Industrial Engineering at UPC in 1989 and PhD at the same University in 1997. She began working at UPC as an Assistant Professor in 1986 and she earned the status of Associate Professor in 2001. Her teaching activities are related to issues of Automatic Control. She is a member of the research group in Advanced Control Systems (SAC). Her main research interests are in dynamic system modeling and identification applied to fault detection, isolation, fault-tolerant control and condition-based maintenance. She has been involved in several international and national research projects and networks, and she has published more than 130 journal and conference papers.

Joseba Quevedo is professor at the Universitat Politècnica de Catalunya (UPC) in automatic control domain, where he has been full professor since 1991. Joseba Quevedo has published more than 400 articles in scientific journals and congresses in the areas of advanced control, identification and estimation of parameters, detection and diagnosis of faults, fault-tolerant control and their applications in large-scale systems (water distribution and sewage networks) and industrial processes. He has participated in many Spanish and European research projects in the field of advanced control and supervision and its application in complex systems. Since 2014 he is the director of the CS2AC UPC Research Center, with more than 30 researchers, and from 2014 to 2018 he has been the president of the Spanish Committee of Automatic Control (CEA).

References

[1] A. Teixeira, I. Shames, H. Sandberg, K. H. Johansson, A secure control framework for resource-limited adversaries, Automatica 51 (2015) 135–148.

[2] X. Ge, F. Yang, Q.-L. Han, Distributed networked control systems: A brief overview, Information Sciences 380 (2017) 117–131.

[3] L. Zhao, H. Xu, Y. Yuan, H. Yang, Stabilization for networked control systems subject to actuator saturation and network-induced delays, Neurocomputing 267 (2017) 354–361.

[4] A. Di Nardo, A. Cavallo, M. Di Natale, R. Greco, G. F. Santonastaso, Dynamic control of water distribution system based on network partitioning, Procedia engineering 154 (2016) 1275–1282.

[5] Y. Wang, T. Alamo, V. Puig, G. Cembrano, Economic model predictive control with nonlinear constraint relaxation for the operational management of water distribution networks, Energies 11 (2018) 991.

[6] S. Liu, X. P. Liu, A. El Saddik, Modeling and distributed gain scheduling strategy for load frequency control in smart grids with communication topology changes, ISA transactions 53 (2014) 454–461.

[7] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, S. Sastry, Understanding the physical and economic consequences of attacks on control systems, International Journal of Critical Infrastructure Protection 2 (2009) 73–83.

[8] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, X.-M. Zhang, A survey on security control and attack detection for industrial cyber-physical systems, Neurocomputing 275 (2018) 1674–1683.

[9] H. Sandberg, S. Amin, K. H. Johansson, Cyberphysical security in networked control systems: An introduction to the issue, IEEE Control Systems 35 (2015) 20–23.

[10] M. Cheminod, L. Durante, A. Valenzano, Review of security issues in industrial networks, IEEE Transactions on Industrial Informatics 9 (2013) 277–293.

[11] H. Fang, H. Ye, M. Zhong, Fault diagnosis of networked control systems, Annual Reviews in Control 31 (2007) 55–68.

[12] F. Fu, D. Wang, P. Liu, W. Li, Evaluation of fault diagnosability for networked control systems subject to missing measurements, Journal of the Franklin Institute (2018).

[13] Y. Zhang, J. Jiang, Bibliographical review on reconfigurable fault-tolerant control systems, Annual reviews in control 32 (2008) 229–252.

[14] D. Rotondo, Advances in gain-scheduling and fault tolerant control techniques, Springer, 2017.

[15] D. Ding, Q.-L. Han, Z. Wang, X. Ge, A survey on model-based distributed control and filtering for industrial cyber-physical systems, IEEE Transactions on Industrial Informatics (2019).

[16] S. Amin, A. A. Cárdenas, S. Sastry, Safe and secure networked control systems under denial-of-service attacks, in: International Workshop on Hybrid Systems: Computation and Control, Springer, pp. 31–45.

[17] F. Pasqualetti, F. Dorfler, F. Bullo, Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems, IEEE Control Systems 35 (2015) 110–127.

[18] D. Ding, G. Wei, S. Zhang, Y. Liu, F. E. Alsaadi, On scheduling of deception attacks for discrete-time networked systems equipped with attack detectors, Neurocomputing 219 (2017) 99–106.

[19] J. Liu, E. Tian, X. Xie, H. Lin, Distributed event-triggered control for networked control systems with stochastic cyber-attacks, Journal of the Franklin Institute (2018).

[20] J. Liu, L. Wei, X. Xie, D. Yue, Distributed event-triggered state estimators design for sensor networked systems with deception attacks, IET Control Theory & Applications (2018).

[21] S. Xiao, Q.-L. Han, X. Ge, Y. Zhang, Secure distributed finite-time filtering for positive systems over sensor networks under deception attacks, IEEE Transactions on Cybernetics (2019).

[22] L. Li, H. Zhang, Y. Xia, H. Yang, Security estimation under denial-of-service attack with energy constraint, Neurocomputing 292 (2018) 111–120.

[23] A. Gupta, C. Langbort, T. Başar, Optimal control in the presence of an intelligent jammer with limited actions, in: Decision and Control (CDC), 2010 49th IEEE Conference on, IEEE, pp. 1096–1101.

[24] Y. Li, L. Shi, P. Cheng, J. Chen, D. E. Quevedo, Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach, IEEE Transactions on Automatic Control 60 (2015) 2831–2836.

[25] C. D. Persis, P. Tesi, Resilient control under denial-of-service, IFAC Proceedings Volumes 47 (2014) 134–139.

[26] C. D. Persis, P. Tesi, Input-to-state stabilizing control under denial-of-service, IEEE Transactions on Automatic Control 60 (2015) 2930–2944.

[27] H. Zhang, P. Cheng, L. Shi, J. Chen, Optimal denial-of-service attack scheduling with energy constraint, IEEE Transactions on Automatic Control 60 (2015) 3023–3028.

[28] H. Zhang, P. Cheng, L. Shi, J. Chen, Optimal DoS attack scheduling in wireless networked control system, IEEE Transactions on Control Systems Technology 24 (2016) 843–852.

[29] H. S. Foroush, S. Martínez, On event-triggered control of linear systems under periodic denial-of-service jamming attacks, in: Decision and Control (CDC), 2012 IEEE 51st Annual Conference on, IEEE, pp. 2551–2556.

[30] H. S. Foroush, S. Martínez, On multi-input controllable linear systems under unknown periodic DoS jamming attacks, in: 2013 Proceedings of the Conference on Control and its Applications, SIAM, pp. 222–229.

[31] S. Feng, P. Tesi, Resilient control under Denial-of-Service: Robust design, Automatica 79 (2017) 42–51.

[32] W. Chen, D. Ding, H. Dong, G. Wei, Distributed resilient filtering for power systems subject to denial-of-service attacks, IEEE Transactions on Systems, Man, and Cybernetics: Systems (2019).

[33] J. Liu, T. Yin, M. Shen, X. Xie, J. Cao, State estimation for cyber–physical systems with limited communication resources, sensor saturation and denial-of-service attacks, ISA transactions (2018).

[34] J. Lunze, T. Steffen, Control reconfiguration after actuator failures using disturbance decoupling methods, IEEE Transactions on Automatic Control 51 (2006) 1590–1601.

[35] D. Rotondo, F. Nejjari, V. Puig, A virtual actuator and sensor approach for fault tolerant control of LPV systems, Journal of Process Control 24 (2014) 203–222.

[36] D. Rotondo, F. Nejjari, V. Puig, J. Blesa, Model reference FTC for LPV systems using virtual actuators and set-membership fault estimation, International Journal of Robust and Nonlinear Control 25 (2015) 735–760.

[37] D. Rotondo, V. Puig, F. Nejjari, J. Romera, A fault-hiding approach for the switching quasi-LPV fault-tolerant control of a four-wheeled omnidirectional mobile robot, IEEE Transactions on Industrial Electronics 62 (2015) 3932–3944.

[38] D. Rotondo, F. Nejjari, V. Puig, Fault tolerant control of a proton exchange membrane fuel cell using Takagi–Sugeno virtual actuators, Journal of Process Control 45 (2016) 12–29.

[39] J. H. Richter, W. P. M. H. Heemels, N. van de Wouw, J. Lunze, Reconfigurable control of piecewise affine systems with actuator and sensor faults: stability and tracking, Automatica 47 (2011) 678–691.

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

[41] M. Khosrowjerdi, J. Mohammad, S. Barzegary, Fault tolerant control using virtual actuator for continuous-time Lipschitz nonlinear systems, International Journal of Robust and Nonlinear Control 24 (2014) 2597–2607.

[42] D. Rotondo, A. Cristofaro, T. A. Johansen, Fault tolerant control of uncertain dynamical systems using interval virtual actuators, International Journal of Robust and Nonlinear Control 28 (2018) 611–624.

[43] R. Nazari, M. M. Seron, J. A. De Doná, Fault-tolerant control of systems with convex polytopic linear parameter varying model uncertainty using virtual-sensor-based controller reconfiguration, Annual Reviews in Control 37 (2013) 146–153.

[44] S. Feng, P. Tesi, Networked control systems under denial-of-service: Co-located vs. remote architectures, Systems & Control Letters 108 (2017) 40–47.

[45] D. Yang, Y. Liu, J. Zhao, Guaranteed cost control for switched lpv systems via parameter and state-dependent switching with dwell time and its application, Optimal Control Applications and Methods 38 (2017) 601–617.

[46] J. M. Hespanha, O. A. Yakimenko, I. I. Kaminer, A. M. Pascoal, Linear parametrically varying systems with brief instabilities: An application to vision/inertial navigation, IEEE Transactions on Aerospace and Electronic Systems 40 (2004) 889–902.

[47] B. Lu, F. Wu, Switching LPV control designs using multiple parameter-dependent Lyapunov functions, Automatica 40 (2004) 1973–1980.

[48] L. Zhang, H. Gao, Asynchronously switched control of switched linear systems with average dwell time, Automatica 46 (2010) 953–958.

[49] B. Niu, H. R. Karimi, H. Wang, Y. Liu, Adaptive output-feedback controller design for switched nonlinear stochastic systems with a modified average

dwell-time method, IEEE Transactions on Systems, Man, and Cybernetics: Systems 47 (2017) 1371–1382.

[50] Z. Fei, S. Shi, Z. Wang, L. Wu, Quasi-time-dependent output control for discrete-time switched system with mode-dependent average dwell time, IEEE Transactions on Automatic Control 63 (2018) 2647–2653.

[51] J. S. Shamma, An overview of LPV systems, in: Control of linear parameter varying systems with applications, Springer, 2012, pp. 3–26.

[52] D. Rotondo, F. Nejjari, V. Puig, Quasi-LPV modeling, identification and control of a twin rotor MIMO system, Control Engineering Practice 21 (2013) 829–846.

[53] C. Hoffmann, H. Werner, A survey of linear parameter-varying control applications validated by experiments or high-fidelity simulations, IEEE Transactions on Control Systems Technology 23 (2015) 416–433.

[54] Y. Tao, D. Shen, Y. Wang, Y. Ye, Reliable H_∞ control for uncertain nonlinear discrete-time systems subject to multiple intermittent faults in sensors and/or actuators, Journal of the Franklin Institute 352 (2015) 4721–4740.

[55] L. Cao, Y. Wang, Fault-tolerant control for nonlinear systems with multiple intermittent faults and time-varying delays, International Journal of Control, Automation and Systems 16 (2018) 609–621.

[56] S. Xu, J. Lam, X. Mao, Delay-dependent H_∞ control and filtering for uncertain markovian jump systems with time-varying delays, IEEE Transactions on Circuits and Systems I: Regular Papers 54 (2007) 2070–2077.

[57] X.-D. Zhao, Q.-S. Zeng, H_∞ output feedback control for stochastic systems with mode-dependent time-varying delays and markovian jump parameters, International Journal of Automation and Computing 7 (2010) 447–454.

[58] J. Xiong, J. Lam, Stabilization of linear systems over networks with bounded packet loss, Automatica 43 (2007) 80–87.

[59] W.-A. Zhang, L. Yu, Modelling and control of networked control systems with both network-induced delay and packet-dropout, Automatica 44 (2008) 3206–3210.

[60] G. K. Befekadu, V. Gupta, P. J. Antsaklis, Risk-sensitive control under a class of denial-of-service attack models, in: American Control Conference (ACC), 2011, IEEE, pp. 643–648.

[61] M. Staroswiecki, C. Commault, J.-M. Dion, Fault tolerance evaluation based on the lattice of system configurations, International Journal of Adaptive Control and Signal Processing 26 (2012) 54–72.

[62] D. Rotondo, J.-C. Ponsart, D. Theilliol, F. Nejjari, V. Puig, Fault tolerant control of unstable LPV systems subject to actuator saturations using virtual actuators, IFAC-PapersOnLine 48 (2015) 18–23.

[63] P. Apkarian, P. Gahinet, G. Becker, Self-scheduled H_∞ control of linear parameter-varying systems: a design example, Automatica 31 (1995) 1251–1261.

[64] J. Lofberg, YALMIP: A toolbox for modeling and optimization in MATLAB, in: Computer Aided Control Systems Design, 2004 IEEE International Symposium on, IEEE, pp. 284–289.

[65] J. F. Sturm, Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones, Optimization methods and software 11 (1999) 625–653.