State-feedback control for discrete-time uncertain positive linear systems under denial of service attacks

Paulo S. P. Pessim[1], Felipe A. Silva[2], Márcia L. C. Peixoto[3], Reinaldo M. Palhares[4] and Márcio J. Lacerda[5]

***Abstract*— This paper presents conditions in the form of Linear Matrix Inequalities to design state-feedback controllers for discrete-time uncertain positive linear systems in the presence of denial of service (DoS) attacks. The system under attack is modeled after a switched model that allows us to derive the synthesis conditions. Two strategies for control are considered, a hold strategy and a packet-based approach. Numerical experiments illustrate the efficacy of the proposed method of keeping the positiveness and stability of the closed-loop system under the presence of DoS attacks.**

I. INTRODUCTION

Over the last few years, the advances in communication systems and computation allowed the implementation of control techniques that consider the integration of cyber and physical realms, giving origin to the so-called cyber-physical systems (CPS) [1]. There are several challenges when considering control for cyber-physical systems, and one of the main issues is the presence of malicious agents trying to disrupt the performance of the CPS. Among the threats, one may cite false data injection, denial of service, and the presence of replay attacks. Different problems have been tackled in the CPS literature. When considering deterministic methods one may cite, stability analysis [2], state-feedback control [3], output-feedback control [4], event-triggered control [5], [6], and filter design [7]. In addition, scenarios taking into account the presence of uncertainty [8], and time-varying parameters [9] have been explored.

Concerning the class of positive systems, it has attracted the attention of the control literature in the last decades. This class is of utmost importance for systems that assume only non-negative values in their temporal evolution when non-negative initial conditions are considered. Applications of positive systems can be found in several areas, for instance, hydraulic system networks, industrial processes involving chemical reactors, models involving atmospheric and water pollution, economic models, population control, and also epidemiological models [10]. Synthesis methods for continuous and discrete-time positive systems appeared in the last decades [11], [12]. State-feedback [13], output-feedback control [14], [15], filter design [16], residual filter design [17], and the presence of external disturbances were exploited [18]. Most of the techniques make use of the Lyapunov theory [19] to obtain analysis and design conditions. The Lyapunov theory is an important ally, as it makes it possible to obtain conditions in the form of linear matrix inequalities (LMIs) [20].

In [21] a switched positive system was considered to deal with the presence of DoS attacks for precisely known discrete-time systems. The switched model follows the idea introduced in [3], where a dwell-time method is employed to obtain the design conditions which are solved via linear programming. An iterative algorithm with seven steps is provided for the synthesis of the controller. The problem of distributed robust estimation was investigated in [22], different topological attacks are considered and the resilience to external disturbance is evaluated through the ℓ_1-gain.

Although there are some results for positive cyber-physical systems, there are some gaps in the literature that need to be addressed. More specifically, the problem of designing state-feedback controllers capable of maintaining the stability and positivity of uncertain positive systems under the harmful effects of cyber-attacks it still requires further investigation. Therefore, to deal with this issue, this paper presents conditions in the form of LMIs for the design of state-feedback controllers for discrete-time uncertain positive linear systems under the presence of DoS attacks.

The hypothesis that the attacker is energetically bounded allows us to obtain the dynamics of a switched model that will represent the system under attack. The conditions will then be derived by employing the Lyapunov theory. First, for the sake of clarity, the precisely known case is discussed, and then the solution for the uncertain system is presented. Two strategies are discussed for control design, the hold strategy: based on a single controller used to stabilize the system under attacks, and the packet-based approach: which designs a packet of control gains that will be applied successively in the occurrence of DoS attacks. The proposed method does not rely on the use of iterative or algorithmic approaches. Numerical experiments are employed to test the conditions

*This work was supported by the Brazilian agency CNPq, grant Numbers: 141252/2021-9, 315538/2021-0, 305578/2022-7.

[1]Paulo S. P. Pessim, is with the Graduate Program in Electrical Engineering, Federal University of Minas Gerais, Brazil. pessim@ufmg.br

[2] Felipe A. Silva is with the Department of Electrical Engineering, Federal University of São João del-Rei - UFSJ, Brazil. felipeaugusto120@gmail.com

[3]Márcia L. C. Peixoto is with the LAMIH laboratory, UMR CNRS 8201, Université Polytechnique Hauts-de-France, 59313 Valenciennes, France, and also with the INSA Hauts-de-France, 59313 Valenciennes, France. marcialcpeixoto@gmail.com.br

[4]Reinaldo M. Palhares is with the Department of Electronics Engineering, Federal University of Minas Gerais, Minas Gerais, Brazil. rpalhares@ufmg.br

[5] Márcio J. Lacerda is with the Centre for Communications Technology, School of Computing and Digital Media, London Metropolitan University, UK m.lacerda@londonmet.ac.uk

and to illustrate the efficacy of the proposed method in ensuring the stability and positivity of the positive CPS under the presence of DoS attacks.

Notation: $X \in \mathbb{R}^{m\times n}$ represents a real matrix with dimensions of m rows and n columns. The transpose of a matrix X is given by $X^\top$. $P \succ 0$ ($P \prec 0$) represents a symmetric positive-definite (negative-definite) matrix. The condition $M \geq 0$ states that each element of a matrix M must be non-negative. The symmetric block of a matrix is denoted by $\star$.

II. PROBLEM STATEMENT

A. System Description

Consider the following discrete-time state space representation of the linear time-invariant (LTI) positive system

$$x(k+1) = Ax(k) + Bu(k), \tag{1}$$

where $x \in \mathbb{R}^n$ is the state vector and $u \in \mathbb{R}^{n_u}$ is the control input. The system (1) is said a positive system according to the following definition:

Definition 1 ([10]): The system (1) is said positive if for any nonnegative initial condition $x(0)$ and nonnegative input $u(k)$, the states are nonnegative.

In this paper, we are interested in designing a state-feedback control law that will guarantee the asymptotic stability and positivity of the system (1) under the presence of attacks. Before introducing the DoS attack let us define the closed-loop system in the absence of attacks.

With the state-feedback control law

$$u(k) = Kx(k), \tag{2}$$

where $K \in \mathbb{R}^{n_u\times n}$ is the control gain, the system (1) has the following closed-loop representation

$$x(k+1) = A_{cl}x(k), \tag{3}$$

where $A_{cl} = A + BK$. The next Lemma will play an important role in the main results to guarantee the positivity of the closed-loop system.

Lemma 1 ([10]): The closed-loop system (3) is said positive if, and only if, all the elements of the closed-loop system A_{cl} are nonnegative.

In the literature of positive systems, there are already conditions to solve the state-feedback control problem. However, little attention has been paid to positive systems under the effects of cyber attacks. To take into account the presence of DoS attacks, the model presented in the next section will be employed.

B. DoS attack - Modelling

To construct the proposed model, the following assumption is considered:

Assumption 1: In the presence of attacks, the control input will employ the last state information available.

Notice that the presence of the attacker is preventing the update of information. Therefore, considering only the last successfully transmitted measurement, how can we maintain the stability and positivity of the closed-loop system?

Similar to [23], and to better illustrate the proposed method, first, we will discuss a scenario where a maximum of two consecutive attacks can be performed. This will help to grasp the main idea that will be extended to a generic number N of consecutive DoS attacks. When $N = 2$ the following scenarios are possible, we highlighted in red the information that is not being updated when the attack occurs.

- Case 0: DoS-free case

$$x(k+1) = Ax(k) + BKx(k),$$

- Case 1: The DoS attack occurs during one time-instant

$$\begin{aligned} x(k+1) &= Ax(k) + BKx(k),\\ x(k+2) &= Ax(k+1) + BKx(k),\\ x(k+2) &= A^2x(k) + ABKx(k) + BKx(k), \end{aligned}$$

- Case 2: The DoS attack occurs during two time-instants

$$\begin{aligned} x(k+1) &= Ax(k) + BKx(k),\\ x(k+2) &= Ax(k+1) + BKx(k),\\ x(k+3) &= Ax(k+2) + BKx(k),\\ x(k+3) &= A^3x(k) + A^2BKx(k) + ABKx(k) + BKx(k), \end{aligned}$$

Taking into account the $N+1 = 3$ possible scenarios, we will be able to represent the system under DoS attack as a switched system.

For this end, we will establish a new time scale k_κ that represents the time instant when the updated control input reaches the actuator. The value k_κ is updated as follows

$$k_{\kappa+1} = k_\kappa + \sigma(k_\kappa) + 1, \quad k_0 = 0, \tag{4}$$

where $\sigma(k_\kappa)$ is a switching signal that can assume values in the set $M \triangleq \{0,1,\ldots,N\}$. For instance, consider $N = 2$, and the signal $\sigma(k_\kappa) = \{1,2,0,1\}$. Figure 1 shows the correspondence between the time scales k, and k_κ, $\otimes$ represents the presence of a DoS attack.

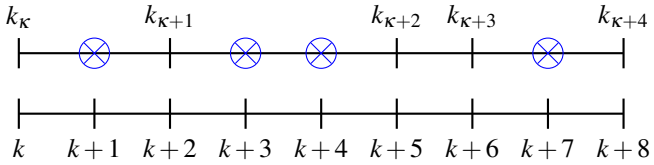

Fig. 1: Correspondence between time scales k and k_κ for $\sigma(k_\kappa) = \{1,2,0,1\}$. $\otimes$ represents the packet dropouts caused by DoS attacks.

Our interest is to analyze the system between the switching points. To achieve this end, we will write each mode as functions of the variable k_κ as follows:

- Case 0: DoS-free case

$$\begin{aligned} x(k_{\kappa+1}) &= (A+BK)x(k_\kappa),\\ x(k_{\kappa+1}) &= F_0x(k_\kappa). \end{aligned} \tag{5}$$

- Case 1: The DoS attack occurs during one time-instant

$$\begin{aligned} x(k_{\kappa+1}) &= \left(A^2 + ABK + BK\right)x(k_\kappa),\\ x(k_{\kappa+1}) &= F_1x(k_\kappa) = (AF_0 + BK)x(k_\kappa). \end{aligned} \tag{6}$$

- Case 2: The DoS attack occurs during two time-instants

$$x(k_{\kappa+1}) = \left(A^3 + A^2BK + ABK + BK\right)x(k_\kappa),$$
$$x(k_{\kappa+1}) = F_2x(k_\kappa) = (AF_1 + BK)\,x(k_\kappa). \tag{7}$$

A generic formulation for the matrices F_i, $i = 1,\ldots,N$, is given as follows

$$F_i = AF_{i-1} + BK, \tag{8}$$

with $F_0 = A + BK$. These matrices are used to construct the following switched system with $N+1$ modes.

$$x(k_{\kappa+1}) = F_{\sigma(k_\kappa)}x(k_\kappa). \tag{9}$$

The sequence $\sigma(k_\kappa)$ is the time-varying switching signal that draws values from the set $M \triangleq \{0,1,\ldots,N\}$. The indicator function $\xi(k_\kappa) = [\xi_0(k_\kappa),\ldots,\xi_N(k_\kappa)]^\top$

$$\xi_i(k_\kappa) = \begin{cases} 1, & \text{if } \sigma(k_\kappa) = i \\ 0, & \text{otherwise} \end{cases}$$

is employed to write (9) as follows

$$x(k_{\kappa+1}) = F(\xi(k_\kappa))x(k_\kappa) \tag{10}$$

with $F(\xi(k_\kappa)) = \xi_0(k_\kappa)F_0 + \xi_1(k_\kappa)F_1 + \cdots + \xi_N(k_\kappa)F_N$.

Remark 1: Notice that the effects of the DoS attacks are similar to communication failures. However, the problem addressed cannot be seen as just packet losses or communication failures between controller and plant, once the problem arises from the attacker's presence, and not due to network limitations.

The challenge at this point is to obtain a new formulation for the design of the control gain K in such a way that DoS attacks do not affect the positivity and stability of the closed-loop system.

III. Main Results

A. The hold-strategy for LTI positive systems

The CPS that is being attacked can be seen as a switched system, where each mode will represent a different number of consecutive attacks. In this sense, before presenting the generic formulation, the next Lemma presents a particular solution to design the state-feedback gain under the occurrence of DoS attacks for $N = 2$.

Lemma 2: If there exist symmetric positive definite matrices $Q_i \in \mathbb{R}^{n\times n}$, a diagonal matrix $X \in \mathbb{R}^{n\times n}$, and matrices $Z \in \mathbb{R}^{n_u\times n}$, such that

$$\begin{bmatrix} -Q_0 & \star \\ AX + BZ & Q_j - X - X \end{bmatrix} \prec 0, \tag{11}$$

$$\begin{bmatrix} -Q_1 & \star \\ A^2X + ABZ + BZ & Q_j - X - X \end{bmatrix} \prec 0, \tag{12}$$

$$\begin{bmatrix} -Q_2 & \star \\ A^3X + A^2BZ + ABZ + BZ & Q_j - X - X \end{bmatrix} \prec 0, \tag{13}$$

$$AX + BZ \geq 0, \tag{14}$$

$$A^2X + ABZ + BZ \geq 0, \tag{15}$$

$$A^3X + A^2BZ + ABZ + BZ \geq 0, \tag{16}$$

with $i, j \in M$, $M \triangleq \{0,1,2\}$, then $K = ZX^{-1}$ is the state-feedback control gain that assures the closed-loop system (10) is positive and asymptotically stable.

Proof: By replacing $Z = KX$ in (11)-(13), and using F_0, F_1, and F_2, as in (5)-(7) yields

$$\begin{bmatrix} -Q_0 & XF_0^\top \\ F_0X & Q_j - X - X \end{bmatrix} \prec 0, \tag{17}$$

$$\begin{bmatrix} -Q_1 & XF_1^\top \\ F_1X & Q_j - X - X \end{bmatrix} \prec 0, \tag{18}$$

$$\begin{bmatrix} -Q_2 & XF_2^\top \\ F_2X & Q_j - X - X \end{bmatrix} \prec 0. \tag{19}$$

Pre- and post-multiplying the conditions above by $diag(X^{-1}, X^{-1})$ results in

$$\begin{bmatrix} -P_i & F_i^\top X^{-1} \\ X^{-1}F_i & P_j - X^{-1} - X^{-1} \end{bmatrix} \prec 0, \tag{20}$$

with $P_i = X^{-1}Q_iX^{-1}$ and $P_j = X^{-1}Q_jX^{-1}$, $i = 0,1,2$, $j = 0,1,2$. By employing the indicator function, it is possible to write (20) as

$$\begin{bmatrix} -P(\xi(k_\kappa)) & F(\xi(k_\kappa))^\top X^{-1} \\ X^{-1}F(\xi(k_\kappa)) & P(\xi(k_{\kappa+1})) - X^{-1} - X^{-1} \end{bmatrix} \prec 0. \tag{21}$$

Pre- and post-multiplying (21) by

$$x(k_\kappa)^\top \begin{bmatrix} I & F(\xi(k_\kappa))^\top \end{bmatrix},$$

and its transpose respectively gives

$$x(k_\kappa)^\top F(\xi(k_\kappa))^\top P(\xi(k_{\kappa+1}))F(\xi(k_\kappa))x(k_\kappa) - x(k_\kappa)^\top P(\xi(k_\kappa))x(k_\kappa) \prec 0, \tag{22}$$

which is equivalent to $V(x(k_{\kappa+1})) - V(x(k_\kappa)) \prec 0$ with $V(x(k_\kappa)) = x(k_\kappa)^\top P(\xi(k_\kappa))x(k_\kappa)$.

Note that $Q_j - X - X \prec 0$ in (11)-(13) yields $Q_j \prec X + X$ guaranteeing that the diagonal matrix X is positive definite. Replacing $Z = KX$, and multiplying (14)-(16) on the right by X^{-1} results in $F_0 \geq 0$, $F_1 \geq 0$, and $F_2 \geq 0$, ensuring that the closed-loop system (10) is positive, since all the elements of $F(\xi(k_\kappa))$ are nonnegative, concluding the proof. ■

The next Theorem is proposed to extend the previous result to deal with N consecutive DoS attacks.

Theorem 1: If there exist symmetric positive definite matrices $Q_i \in \mathbb{R}^{n\times n}$, a diagonal matrix $X \in \mathbb{R}^{n\times n}$, and matrices $Z \in \mathbb{R}^{n_u\times n}$, such that

$$\begin{bmatrix} -Q_i & \star \\ \Psi_i & Q_j - X - X \end{bmatrix} \prec 0, \tag{23}$$

and

$$\Psi_i \geq 0, \tag{24}$$

where

$$\Psi_i = A^{i+1}X + \sum_{m=0}^{i} A^{i-m}BZ, \tag{25}$$

with $A^0 = I_n$, $i, j \in M$, $M \triangleq \{0,1,\ldots,N\}$, then $K = ZX^{-1}$ is the state-feedback control gain that assures the closed-loop system (10) is positive and asymptotically stable.

Proof: The proof follows the same steps performed in the proof of Lemma 2 considering $i, j = \{0,1,\ldots,N\}$. ■

B. The packet-based strategy for uncertain positive systems

Let us consider the presence of uncertainties in the matrices of the system.

$$x(k+1) = A(\alpha)x(k) + B(\alpha)u(k). \tag{26}$$

The uncertain matrices in (26) can be represented as

$$\{A(\alpha), B(\alpha)\} = \sum_{i=1}^{N_v} \alpha_i \{A_i, B_i\}, \quad \alpha_i \in \Lambda_N, \tag{27}$$

where A_i, and B_i, $i = 1,\ldots,N_v$, are the vertices of the polytope and Λ_N is the unit simplex:

$$\Lambda_N = \left\{ \alpha \in \mathbb{R}^{N_v} : \sum_{i=1}^{N_v} \alpha_i = 1,\ \alpha_i \geq 0,\ i = 1,\ldots,N_v \right\}.$$

To reduce the conservativeness of the result proposed in Theorem 1, a packet-based approach will be used to design the state-feedback control. Notice that in Section II-B, a hold-strategy was considered and the same control input $u(k_\kappa)$ is applied when the attack is active. Differently, the packet-based strategy takes advantage of the switched model to design different control gains considering only the information available before the beginning of the attack. In this case, a complete packet with different control inputs is transmitted every time to the actuator. To better illustrate the difference between the strategies, consider the scheme depicted in Figure 2.

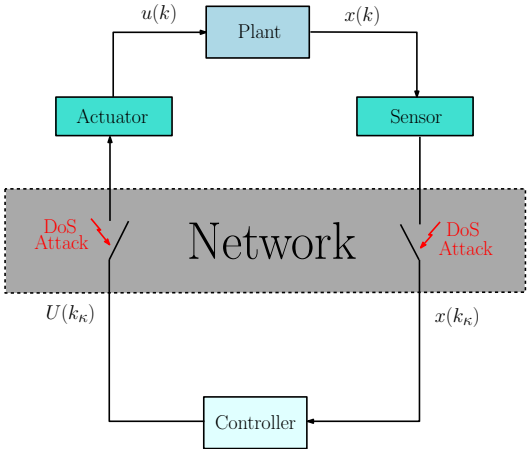

Fig. 2: Structure of the system under DoS attacks.

If the DoS attack on the communication channels is active, a new packet does not arrive at the actuator, and the control inputs of the previously received packet $U(k_\kappa) = [u(k_\kappa)^\top, u(k_\kappa+1)^\top, \ldots u(k_\kappa+N)^\top]^\top$ are successively applied until a new packet arrives. However, if a new packet gets to the actuator at the time $k_\kappa+1$, $u(k_\kappa)$ is the only applied control input of $U(k_\kappa)$. Each control input is defined as presented in next modelling:

- Case 0: DoS-free case

$$x(k+1) = A(\alpha)x(k) + B(\alpha)K_0x(k),$$

- Case 1: The DoS attack occurs during one time-instant

$$x(k+2) = A(\alpha)^2x(k) + A(\alpha)B(\alpha)K_0x(k) + B(\alpha)K_1x(k),$$

- Case 2: The DoS attack occurs during two time-instants

$$x(k+3) = A(\alpha)^3x(k) + A(\alpha)^2B(\alpha)K_0x(k) + A(\alpha)B(\alpha)K_1x(k) + B(\alpha)K_2x(k).$$

It is important to highlight that different control gains are being employed but the state $x(k)$ is from the last successful transmission. In this sense, when the communication channels are free of attack, a new packet of control inputs is sent, regardless if its going to be employed or not.

With this new formulation, the uncertain switched system can be written as

$$x(k_{\kappa+1}) = F(\xi(k_\kappa), \alpha)x(k_\kappa), \tag{28}$$

with $F(\xi(k_\kappa), \alpha) = \xi_0(k_\kappa)F_0(\alpha) + \xi_1(k_\kappa)F_1(\alpha) + \cdots + \xi_N(k_\kappa)F_N(\alpha)$.

$$F_i(\alpha) = A(\alpha)F_{i-1}(\alpha) + B(\alpha)K_i \tag{29}$$

The next result presents the conditions to design the different matrix gains K_i of the packet of controllers.

Theorem 2: If there exist symmetric positive definite matrices $Q_i \in \mathbb{R}^{n\times n}$, a diagonal matrix $X \in \mathbb{R}^{n\times n}$, and matrices $Z_i \in \mathbb{R}^{n_u\times n}$, such that

$$\begin{bmatrix} -Q_i(\alpha) & \star \\ \Psi_i & Q_j(\alpha) - X - X \end{bmatrix} \prec 0, \tag{30}$$

with

$$\Psi_i \geq 0, \tag{31}$$

where

$$\Psi_i = A(\alpha)^{i+1}X + \sum_{m=0}^{i} A(\alpha)^{i-m}B(\alpha)Z_m, \tag{32}$$

with $A(\alpha)^0 = I_n$, $i, j \in M$, $M \triangleq \{0, 1, \ldots, N\}$, then $K_i = Z_iX^{-1}$ are the state-feedback control gains that assure the closed-loop system (10) is positive and asymptotically stable.

Proof: The proof follows the same steps performed in the proof of Lemma 2. ■

Remark 2: There is no restriction preventing the use of the hold strategy for uncertain positive systems, and the packet-based approach can also be employed in the case of positive LTI systems. Since these cases can be derived from the presented developments, they will be omitted due to space limitations.

IV. NUMERICAL EXPERIMENTS

The numerical experiments were performed using MATLAB (R2021b) 64 bits for Windows 11, in a machine with Intel Core i7-10750H (2.6 GHz) processor and 16 GB RAM. The codes were implemented by using the packages YALMIP [24], ROLMIP [25], and the solver Mosek [26]. The ROLMIP [25] uses relaxations based on homogeneous polynomial matrices to get a set of finite LMI conditions from the proposed parameter-dependent conditions.

Consider the uncertain positive discrete-time system borrowed from [11], and described by the following matrices:

$$A_1 = \begin{bmatrix} 0.4 & 0.5 & 0.1 & 0.2 \\ 0.4 & 0.1 & 0.1 & 0.5 \\ 0.4 & 0.4 & 0.3 & 0.3 \\ 0.2 & 0.5 & 0 & 0.3 \end{bmatrix}, \quad B_1 = \begin{bmatrix} 0.1 & 0.5 \\ 0.3 & 0.7 \\ 0.1 & 0.5 \\ 0.3 & 0.8 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 0.3 & 0.2 & 0.4 & 0.1 \\ 0.3 & 0.3 & 0.3 & 0.1 \\ 0.1 & 0.4 & 0.1 & 0.1 \\ 0.2 & 0.3 & 0.5 & 0.5 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 0.8 & 0.4 \\ 0.6 & 0.7 \\ 0.9 & 1.0 \\ 0.3 & 1.0 \end{bmatrix}.$$

The goal of this example is to illustrate the ability of the proposed approach to guarantee the stability and positiveness of the uncertain closed-loop system under DoS attacks, and also highlight the benefits of the packet-based strategy over the use of the hold strategy with a single controller.

Using the hold strategy, that is, similar to Theorem 1 a single robust controller is designed to deal with the presence of uncertainties and cyber-attacks, the proposed conditions render feasible results for up to $N = 7$ consecutive attacks. The obtained state-feedback controller is given by,

$$K = \begin{bmatrix} 0.1211 & 0.1035 & -0.0817 & 0.1379 \\ -0.1325 & -0.1323 & 0.0313 & -0.1367 \end{bmatrix}.$$

For comparison, consider a robust state-feedback controller

$$K_0 = \begin{bmatrix} 0.1813 & 0.0564 & -0.1193 & 0.4257 \\ -0.1761 & -0.1242 & 0.1185 & -0.3536 \end{bmatrix},$$

designed only to guarantee the stability and positiveness of the uncertain closed-loop system (Theorem 2 with $N = 0$). Figure 3 depicts the trajectories of the positive uncertain closed-loop system under the effects of DoS attacks for 100 different initial conditions and uncertain parameters. Notice that when considering the controller K (top), the system can maintain its stability and positiveness even with the presence of the attacker. Meanwhile, when considering the controller K_0 (bottom), the closed-loop system becomes negative due to the DoS attacks depicted in vertical gray stripes.

Similar to [11], we now impose a structural restriction on the controller to obtain a static-output feedback controller $u = K_s y$ with $y = [x_1 \; x_2]^\top$. With this restriction, the proposed approach with the hold strategy is feasible for $N = 3$ consecutive attacks. The obtained state-feedback gain is given by

$$K_s = \begin{bmatrix} 0.1847 & 0.1279 & 0 & 0 \\ -0.2034 & -0.1883 & 0 & 0 \end{bmatrix}.$$

For comparison, consider the controller

$$K_c = \begin{bmatrix} 0.1667 & -0.2105 & 0 & 0 \\ -0.2500 & -0.0526 & 0 & 0 \end{bmatrix},$$

provided in [11]. As depicted in Figure 4 (bottom), the controller design in [11] is not able to maintain the positiveness of the uncertain closed-loop system under DoS attacks. In the meantime, the control input obtained with the proposed approach is once again able to deal with the presence of the malicious agent, maintaining the stability and positiveness of the closed-loop system as shown in Figure 4 (top).

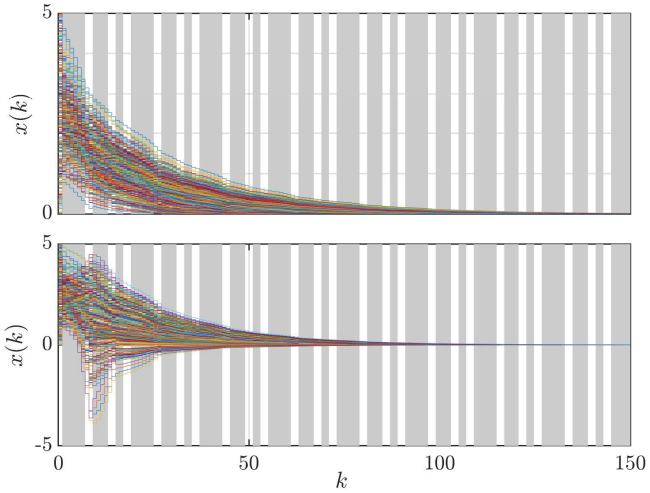

Fig. 3: Trajectories of the closed-loop system with K (top), and K_0 (bottom) under DoS attacks with sequence $\sigma(k_\kappa) = \{7,5,3,7,5,3,...\}$ as depicted in vertical gray stripes.

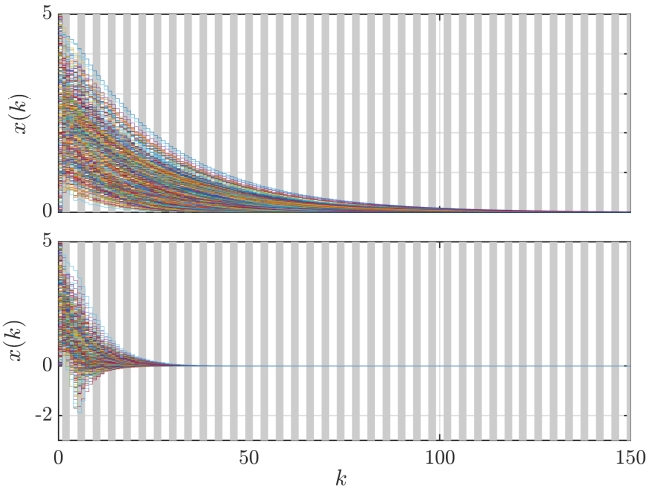

Fig. 4: Trajectories of the closed-loop system with K_s (top), and K_c (bottom) DoS attacks with sequence $\sigma(k_\kappa) = \{3,3,3,3,...\}$ as depicted in vertical gray stripes.

Consider now the design of the full packet of different controllers, with the conditions of Theorem 2. In comparison with the hold strategy, the proposed conditions can increase the number of supported consecutive attacks from $N = 7$ to $N = 18$ attacks. Moreover, consider that the first vertex of the uncertain system is multiplied by a scalar parameter η, that is, $A_1 = \eta A_1$. The goal is to compare the maximum value of η of the hold and full packet strategies for each $N = (0,\ldots,10)$. The Increase of $\eta > 1$ leads to an increase in the eigenvalues of A_1. Consequently, it is more difficult to find feasible solutions. It is worth mentioning that for $\eta < 1$, the eigenvalues of A_1 start to decrease such that with $\eta = 0.8902$ all eigenvalues of A_1 are located inside of the unit circle.

From the obtained results depicted in Figure 5, it is clear that the full packet strategy (solid black line) can provide

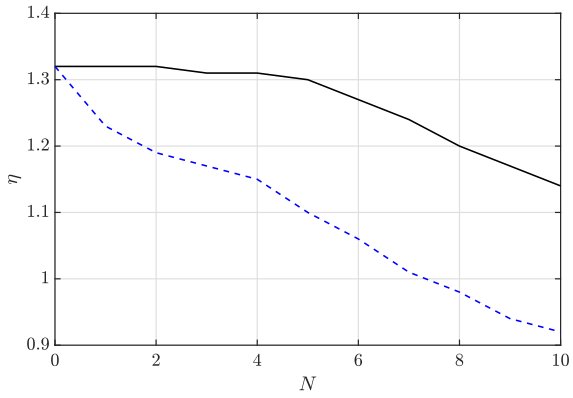

Fig. 5: Maximum value of η per N considering the hold strategy (dashed blue line), and the full packet strategy (black solid line).

feasible solutions for bigger values of η. Notice that with the hold strategy, the maximum value of consecutive attacks such that η is bigger than 1 is $N = 7$ (for $N = 8$ we have $\eta = 0.98$). Meanwhile, with the full packet of controllers, we have that for $N = 10$ the maximum value of η is $\eta = 1.14$. The black solid line will remain above $\eta = 1$ until $N = 18$, the maximum number of attacks supported by the original uncertain system. The curves of the maximum value of η are the same considering symmetric or diagonal structures for the Lyapunov matrices.

V. CONCLUSIONS

This paper has proposed a new method to design state-feedback controllers for discrete-time LTI and uncertain positive systems under the presence of DoS attacks. Two different control strategies based on the construction of a switched system have been considered: the packet of different controllers, and the hold strategy. Numerical experiments have illustrated the ability of the proposed approach to guarantee the stability and positivity of the closed-loop system even with the presence of DoS attacks, a safety guarantee that the methods of the current literature do not provide.

ACKNOWLEDGMENT

This work was carried out with the support of the Coordination for the Improvement of Higher Education Personnel - Brazil (CAPES) through the Academic Excellence Program (PROEX)

REFERENCES

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

[2] A.-Y. Lu and G.-H. Yang, "Stability analysis for cyber-physical systems under denial-of-service attacks," *IEEE Transactions on Cybernetics*, vol. 51, no. 11, pp. 5304–5313, 2020.

[3] S. Lai, B. Chen, T. Li, and L. Yu, "Packet-based state feedback control under DoS attacks in cyber-physical systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 66, no. 8, pp. 1421–1425, 2019.

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

[5] P. H. S. Coutinho, I. Bessa, P. S. P. Pessim, and R. M. Palhares, "A switching approach to event-triggered control systems under denial-of-service attacks," *Nonlinear Analysis: Hybrid Systems*, vol. 50, no. 11, p. 101383, 2023.

[6] M. L. C. Peixoto, P. H. S. Coutinho, I. Bessa, P. S. P. Pessim, and R. M. Palhares, "Event-triggered control of Takagi-Sugeno fuzzy systems under deception attacks," *International Journal of Robust and Nonlinear Control*, vol. 33, no. 13, pp. 7471–7487, 2023.

[7] W. Chen, D. Ding, H. Dong, and G. Wei, "Distributed resilient filtering for power systems subject to denial-of-service attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1688–1697, 2019.

[8] P. M. Oliveira, J. M. Palma, and M. J. Lacerda, "$\mathscr{H}_2$ state-feedback control for discrete-time cyber-physical uncertain systems under DoS attacks," *Applied Mathematics and Computation*, vol. 425, p. 127091, 2022.

[9] P. S. P. Pessim and M. J. Lacerda, "State-feedback control for Cyber-physical LPV systems under DoS attacks," *IEEE Control Systems Letters*, vol. 5, no. 3, pp. 1043–1048, 2021.

[10] L. Farina and S. Rinaldi, *Positive Linear Systems: Theory and Applications*. New York, NY, USA: John Wiley & Sons, 2000.

[11] Y. Ebihara, D. Peaucelle, and D. Arzelier, "LMI approach to linear positive system analysis and synthesis," *Systems & Control Letters*, vol. 63, pp. 50–56, January 2014.

[12] G. S. Deaecto and J. C. Geromel, "$\mathscr{H}_2$ state feedback control design of continuous-time positive linear systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 11, pp. 5844–5849, 2016.

[13] M. A. Rami, F. Tadeo, and A. Benzaouia, "Control of constrained positive discrete systems," in *2007 American Control Conference*, pp. 5851–5856, 2007.

[14] A. Spagolla, C. F. Morais, R. C. L. F. Oliveira, and P. L. D. Peres, "Stabilization and $\mathscr{H}_2$ static output-feedback control of discrete-time positive linear systems," *IEEE Transactions on Automatic Control*, vol. 67, no. 3, pp. 1446–1452, 2022.

[15] J. Shen and J. Lam, "On static output-feedback stabilization for multi-input multi-output positive systems," *International Journal of Robust and Nonlinear Control*, vol. 25, pp. 3154–3162, November 2015.

[16] A. Spagolla, C. F. Morais, R. C. L. F. Oliveira, and P. L. D. Peres, "Reduced order positive filter design for positive uncertain discrete-time linear systems," *IEEE Control Systems Letters*, vol. 6, pp. 1148–1153, 2022.

[17] D. Krokavec and A. Filasová, "$\mathscr{H}_\infty$ norm principle in residual filter design for discrete-time linear positive systems," *European Journal of Control*, vol. 45, pp. 17–29, 2019.

[18] J. Shen and J. Lam, "Some extensions on the bounded real lemma for positive systems," *IEEE Transactions on Automatic Control*, 2016. DOI: 10.1109/TAC.2016.2606426.

[19] H. K. Khalil, *Nonlinear Systems*. Upper Saddle River, NJ: Prentice Hall, 3rd ed., 2002.

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

[21] J. Liu and L. Kang, "Secure control for cyber-physical systems with positive constraint under dos attack," *Circuits, Systems, and Signal Processing*, pp. 1–16, 2022.

[22] S. Xiao, X. Ge, Q.-L. Han, and Y. Zhang, "Distributed resilient estimator design for positive systems under topological attacks," *IEEE Transactions on Cybernetics*, vol. 51, no. 7, pp. 3676–3686, 2020.

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

[24] J. Löfberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in *Proceedings of the 2004 IEEE International Symposium on Computer Aided Control Systems Design*, (Taipei, Taiwan), pp. 284–289, 2004.

[25] C. M. Agulhari, A. Felipe, R. C. L. F. Oliveira, and P. L. D. Peres, "Algorithm 998: The Robust LMI Parser - A Toolbox to Construct LMI Conditions for Uncertain Systems," *ACM Transactions on Mathematical Software*, vol. 45, no. 3, pp. 36:1–36:25, 2019.

[26] E. D. Andersen and K. D. Andersen, "The MOSEK interior point optimizer for linear programming: An implementation of the homogeneous algorithm," in *High Performance Optimization* (H. Frenk, K. Roos, T. Terlaky, and S. Zhang, eds.), vol. 33 of *Applied Optimization*, pp. 197–232, Springer US, 2000.