Enhanced Design Requirements for State-Feedback Control of Cyber-Physical Systems Subject to Denial-of-Service Attacks

Naoual ARMI[a], T. ZOULAGH[b], M. CHARQI [a], A. ABOULKASSIM[c], S. KRIRIM[c], B. BOUKILI[a]

Abstract

This study addresses the design of state-feedback controllers for Cyber–Physical Systems (CPSs) subject to Denial-of-Service (DoS) attacks within a Linear Matrix Inequality (LMI) framework. Due to the uncertainties and discontinuities introduced by such attacks, the CPS is modeled as a switched system to represent multiple operational modes under adversarial conditions. This modeling strategy inherently limits the attacker's capability to sustain prolonged DoS attacks. A numerical case study is provided to illustrate the effectiveness and the applicability of the proposed approach in order to ensure the stability of CPS under various DoS attack scenarios.

Index Terms

Cyber-Physical Systems (CPSs); Denial-of-Service (DoS) attack; robust control;State-Feedback Controllers; Linear Matrix Inequality (LMI).

I. Introduction

Cyber-Physical Systems (CPS) are modern engineering systems where the physical part and the computational part work closely together. They rely on sensors, actuators, controllers, and communication networks to keep track of and influence physical processes in real time. Thanks to this integration, CPS are now found everywhere — in smart grids, self-driving vehicles, automated factories, and healthcare technologies [1]. However, there are additional concerns associated with this increased reliance on communication networks. Since data must constantly flow between components, any communication breakdown might have an immediate impact on the behavior of the system. Because of this, CPS is a prime target for hackers. Denial-of-Service (DoS) attacks are among the most prevalent and hazardous [2]. The network is overwhelmed with harmful or redundant data in such an attack, which slows down or prevents the flow of crucial control signals. When that occurs, system performance may drastically decline, and in vital sectors like energy or transportation, it may even result in complete system failure [3]. Many researchers have been developing new control mechanisms that can maintain system stability and dependability even in the face of network attacks in order to counter these dangers [4], [5], [6]. These tactics frequently rely on feedback control techniques that can modify the system's response in the event of communication breakdowns or delays. To lessen the effects of DoS attacks and other disturbances, strategies like switching controllers, predictive models, or adaptive scheduling are frequently employed. We expand on those concepts in this study and suggest a strong state-feedback control strategy created especially for CPS vulnerable to DoS attacks. The primary objective is to increase the system's resilience and stability, even under challenging communication circumstances.

To address these challenges, growing research efforts have focused on developing control strategies that are resilient to Denial-of-Service (DoS) attacks and capable of ensuring closed-loop stability under such conditions. Various approaches have been proposed, including state-feedback control [7], [8], observer-based designs [9], [10] and H_∞ performance-oriented techniques [11]. These methods often employ switched system models and leverage advanced stability analysis tools, including multiple Lyapunov functions and Finsler's lemma, to effectively handle the time-varying and uncertain

This work was not supported by any organization
[a] Lab-LESSI, Sidi Mohamed Ben Abdellah University, FSDM, Fez, Morocco. bensalem.boukili@usmba.ac.ma
[b] EIDEA School, Euromed University, Fez, Morocco
[c] Lab-LMSSPM, Ibn Zohr University, Higher School of Technology, Guelmim, Morocco.

characteristics inherent to DoS attack patterns. Notably, Linear Matrix Inequality (LMI) frameworks have demonstrated considerable effectiveness in controller synthesis under these constraints, offering a systematic and computationally tractable approach to robust control design [12].

This paper addresses the problem of control design for Cyber-Physical Systems (CPSs) subject to Denial-of-Service (DoS) attacks by adversarial agents. The attacked closed-loop system is modeled as a switching system, where both the onset and duration of switching events correspond to the occurrence and persistence of DoS attacks. A Lyapunov-based stability analysis is conducted to derive sufficient conditions for stability, formulated in terms of Linear Matrix Inequalities (LMIs). Three distinct control strategies are examined: (1) the zero-input strategy, which sets the control input to zero upon attack detection; (2) the hold strategy, which maintains the most recent control input throughout the attack duration; and (3) the scheduled-gain strategy, which switches among a predefined set of feedback gains during attack intervals. To validate the proposed methodology, a numerical case study from the literature is presented, demonstrating both the effectiveness and robustness of the approach, and highlighting the impact of each control strategy under various attack scenarios.

Notation: Let R denotes the set of real numbers. The symbols 0 and I represent, respectively, the zero matrix and the identity matrix of appropriate dimensions. A matrix P is said to be positive definite (respectively, negative definite) if $P > 0$ (respectively, $P < 0$). The symbol * denotes the symmetric term in a block symmetric matrix. The superscript $\top$ represents the symbol of matrix transposition. The notation $\mathrm{He}(D)$ refers to the Hermitian (symmetric) part of a matrix, defined as $\mathrm{He}(D) = D + D^{\top}$.

II. Preliminaries

Let us consider a Cyber-Physical System (CPS) plant characterized by the following discrete-time state-space representation:

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

where, $x(k) \in \mathsf{R}^n$ is the state vector and $u(k) \in \mathsf{R}^{n_u}$ represents the control input. $A \in \mathsf{R}^{n\times n}$ and $B \in \mathsf{R}^{n\times n_u}$ are known constant matrices.

The aim is to perform a control action that will make system (1) asymptotically stable. We design a state feedback controller of the form:

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

The closed-loop system in matrix form, assuming the state-feedback control law is as follows:

$$x(k+1) = (A + BK)x(k) = \mathcal{A}x(k). \tag{3}$$

where $\mathcal{A} = A + BK$.

Under Denial-of-Service (DoS) attacks, the behavior of a Cyber-Physical System (CPS) becomes time-varying and exhibits discontinuities. In such scenarios, the system alternates between distinct operating modes depending on the status of the communication network. Specifically, it functions under nominal conditions when the control signal is transmitted successfully, but switches to degraded or outdated control modes during DoS intervals. This dynamic can be naturally captured using a switched system framework, as described by:

$$x(k+1) = \mathcal{A}_{\delta(k)}x(k), \tag{4}$$

where, values from the set $\mathcal{M} = \{0, 1, ..., N\}$ can be accepted by the switching signal $\sigma(k)$. The switching system (3) only has one active mode at a time. Such behavior will be described by the indicator function. Let us take $\zeta(k) = [\zeta_1(k), ..., \zeta_N(k)]^T$ into account such that:

$$\zeta_i(k) = \begin{cases} 1, & \text{if } \delta(k) = i \\ 0, & \text{otherwise} \end{cases} \tag{5}$$

Consequently, system (3) can be represented as a switched system of the form:

$$x(k+1) = \mathcal{A}(\zeta(k))x(k) \tag{6}$$

Definition 1 *[13]: For all* $x(k) \in \mathbb{R}^n$, $k \geq 0$, *if there exists a Lyapunov function* $V : \mathbb{R}^n \to \mathbb{R}$, *the switched system (6) is Globally Uniformly Asymptotically Stable (GUAS) if the following conditions hold:*

1) $V(k,0) = 0$, $V(k, x(k)) > 0$, $\forall x(k) \neq 0$,

$$\Delta V(k, x(k)) = V(k+1, x(k+1)) - V(k, x(k)) < 0, \qquad \forall x(k) = 0.$$

2) *There exist two positive scalars* α *and* β *such that:*

$$\alpha \|x(k)\|^2 \leq V(k, x(k)) \leq \beta \|x(k)\|^2$$

3) *There exists a small positive scalar* γ *such that:*

$$\Delta V(k, x(k)) < -\gamma \|x(k)\|^2$$

Lemma 1 *[14]: The closed-loop system (2) is asymptotically stable if and only if there exists a symmetric positive definite matrix* $P \in \mathbb{R}^{n \times n}$ *such that:*

$$\mathcal{A}^\top P \mathcal{A} - P < 0 \tag{7}$$

Lemma 2 *[15]: The following two problems are equivalent:*

i) Identify a positive definite matrix $P = P^\top$ *such that*

$$\mathcal{T} + \mathcal{A}^\top P \mathcal{A} < 0 \tag{8}$$

ii) Identify $P = P^\top > 0$, $\mathcal{L}$, $\mathcal{G}$ *such that*

$$\begin{bmatrix} \mathcal{T} + \mathcal{A}^\top \mathcal{L}^\top + \mathcal{L}\mathcal{A} & * \\ -\mathcal{L}^\top + \mathcal{G}^\top \mathcal{A} & P - \mathcal{G} - \mathcal{G}^\top \end{bmatrix} < 0 \tag{9}$$

III. Problem statement

A Denial-of-Service (DoS) attack can severely disrupt the communication network, hindering the transmission of control signals to the actuator (see Fig. 1). As a result, during the attack period, the system operates in open-loop mode, which may threaten its stability and degrade overall performance.

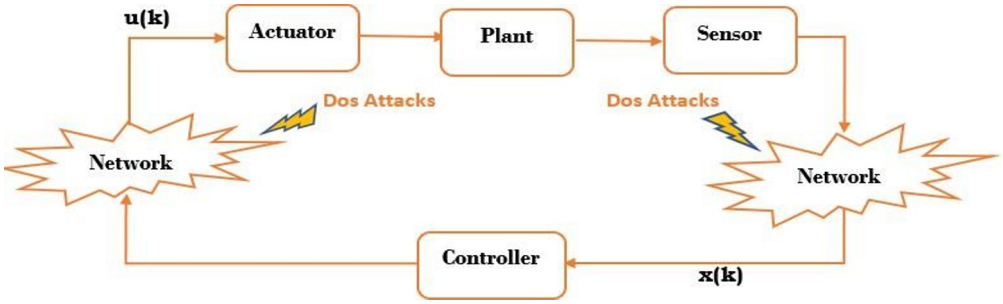

Fig. 1: Block diagram illustrating the structure of a CPS under DoS attacks.

Assumption 1 *[16]: It is assumed that the duration of any consecutive DoS attack is bounded by* N *time steps, reflecting the attacker's limited energy or resource constraints.*

Keeping the final control input constant during the attack is a viable strategy in these situations. We establish a discrete-time scale K_κ that represents the moments when a new control input is successfully applied to capture this behavior. As this time scale evolves,

$$k_{\kappa+1} = k_\kappa + \delta(k_\kappa) + 1, \quad k_0 = 0, \tag{10}$$

where, $\delta(k_\kappa) \in \{0, 1, \ldots, N\}$ indicates a time-varying switching signal. We try to analyze the dynamics between consecutive instances where new control actions are successfully provided to the actuator with the aim of getting a better understanding of how the system acts under DoS conditions.

Case 0: No DoS attack

$$x(k_{\kappa+1}) = (A + BK)x(k_\kappa) = G_0 x(k_\kappa) \tag{11}$$

Case 1 : DoS attack in one step

$$\begin{aligned} x(k_{\kappa+1}) &= \left(A^2 + ABK + BK\right)x(k_\kappa) \\ &= (AG_0 + BK)x(k_\kappa) = G_1 x(k_\kappa) \end{aligned} \tag{12}$$

.

Case N : DoS attack in N steps

$$x(k_{\kappa+1}) = (AG_{N-1} + BK)x(k_\kappa) = G_N x(k_\kappa) \tag{13}$$

The dynamic of the discrete-time switching system with operating modes $N + 1$ can be expressed by the following matrices G_i, with $i = 1..., N$

$$x(k_{\kappa+1}) = G_{\delta(k_\kappa)} x(k_\kappa). \tag{14}$$

Alternatively, by using indicator functions $\zeta_i(k_\kappa)$, the development of the system can be clearly expressed as follows:

$$x(k_{\kappa+1}) = \sum_{i=0}^{N} \zeta_i(k_\kappa) G_i x(k_\kappa) \tag{15}$$

IV. Main results

A. State-feedback control Design under DoS Attacks

Assuming that the number of successive packet losses is bounded by a generic value N, the following theorem establishes sufficient conditions for designing a state-feedback controller that guarantees the stability of a Cyber-Physical System (CPS) under Denial-of-Service (DoS) attacks.

Theorem 1 *: The closed-loop system (14) is asymptotically stable if there exist symmetric positive definite matrices H_i, and matrices $X \in \mathbb{R}^{n\times n}$, $Z \in \mathbb{R}^{n_u \times n}$ such that the following inequalities hold for all $i, j \in \mathcal{M} = \{0, 1, \ldots, N\}$:*

$$\begin{bmatrix} -H_i + He(\Xi_i) & * \\ -X + \Xi_i & H_j - X - X^\top \end{bmatrix} < 0 \tag{16}$$

where,

$$\Xi_i = A^{i+1}X + \sum_{m=0}^{i} A^{i-m} BZ, \quad with\ A^0 = I_n. \tag{17}$$

Then the state-feedback control gain is given by:

$$K = ZX^\top \tag{18}$$

Proof 1 *: Consider the following expression:*

$$\mathcal{A}^\top P\left(\delta(k_{\kappa+1})\right)\mathcal{A} - P\left(\delta(k_\kappa)\right) < 0. \tag{19}$$

Applying Lemma 2, (19) is equivalent to:

$$\begin{bmatrix} -P(\delta(k_\kappa)) + He(\mathcal{L}\mathcal{A}) & * \\ -\mathcal{L}^\top + \mathcal{G}^\top\mathcal{A} & P(\delta(k_{\kappa+1})) - He(\mathcal{G}) \end{bmatrix} < 0. \tag{20}$$

Setting $\delta(k_\kappa) = i$ *and* $\delta(k_{\kappa+1}) = j$*, then pre- and post-multiplying (20) by* $\mathrm{diag}(\mathcal{L}^{-1}, \mathcal{L}^{-1})$ *and its transpose, we obtain:*

$$\begin{bmatrix} -\mathcal{L}^{-1}P_i\mathcal{L}^{-\top} + He(\mathcal{A}\mathcal{L}^{-\top}) & * \\ -\mathcal{L}^{-1} + \mathcal{L}^{-1}\mathcal{G}^\top\mathcal{A}\mathcal{L}^{-\top} & \mathcal{L}^{-1}P_j\mathcal{L}^{-\top} - \mathcal{L}^{-1}(He(\mathcal{G}))\mathcal{L}^{-\top} \end{bmatrix} < 0. \tag{21}$$

By performing a change of variables $\mathcal{G}^\top = \mathcal{L}$*,* $\mathcal{L}^{-1}P_i\mathcal{L}^{-\top} = H_i$*,* $\mathcal{L}^{-1}P_j\mathcal{L}^{-\top} = H_j$*, and setting* $\mathcal{L}^{-1} = X$*, we obtain:*

$$\begin{bmatrix} -H_i + He(\mathcal{A}X^\top) & * \\ -X + \mathcal{A}X^\top & H_j - X - X^\top \end{bmatrix} < 0. \tag{22}$$

Finally, substituting $\mathcal{A}$ *by its expression considering the attack case completes the proof.*

B. State-Feedback Control Design

This method considers a packet-based control strategy. The fundamental idea behind this strategy is to design a package that has $N+1$ control inputs that will be active in addition to the current controller in the case of a DoS attack. Meanwhile, the most recent time-varying parameter is updated throughout the controller packet, and the channel is free of attacks.

In order to ensure the stability of the closed-loop system, a state-feedback control law will be developed:

$$u(k_\kappa + p) = K_p\, x_{k_\kappa} \tag{23}$$

for $p = 0, 1, \ldots, \delta(k_\kappa)$ and all gains are included in a control packet which is sent to the actuator side

$$U(k_\kappa) = \begin{bmatrix} u(k_\kappa)^T \\ u(k_\kappa + 1)^T \\ . \\ u(k_\kappa + N)^T \end{bmatrix} \tag{24}$$

When a new packet arrives, the implementation process is governed by the following rules:

1) $u(k_\kappa)$ is the only control input applied from $U(k_\kappa)$ if a new packet reaches the actuator at time $k_\kappa + 1$.
2) If a DoS attack starts at time $k_\kappa + 1$, all previously designed control inputs $u(k_\kappa + 1), ..., u(k_\kappa + p)$, will be applied over time until a new package comes.

Remark 1 *: If the number of designed controllers exceeds the number of consecutive attacks, a new packet will reach the actuator before all control inputs are applied; in this case, the remaining inputs must be discarded, and a new sequence begins with the newly updated packet.*

The following $N+1$ scenarios represent the closed-loop dynamics under attack when the control law (23) used by the packet-based method is combined with system (1):

Case 0 : No DoS attack

$$x(k_{\kappa+1}) = (A + BK_0)x(k_\kappa) = G_0 x(k_\kappa) \tag{25}$$

Case 1 : DoS attack jams a one-step horizon

$$\begin{aligned} x(k_{\kappa+1}) &= \left(A^2 + ABK_0 + BK_1\right)x(k_\kappa) \\ &= (AG_0 + BK_1)x(k_\kappa) = G_1 x(k_\kappa) \end{aligned} \tag{26}$$

.

Case N : DoS attack jams the N-steps horizon

$$x(k_{\kappa+1}) = (AG_{N-1} + BK_N)x(k_\kappa) = G_N x(k_\kappa) \tag{27}$$

The following Theorem presents the criteria for designing $N+1$ gains for the packet-based technique.

Theorem 2 *: The closed-loop system (14) is asymptotically stable if there exist symmetric positive definite matrices H_i, and matrices $X \in \mathbb{R}^{n\times n}$, $Z_i \in \mathbb{R}^{n_u\times n}$ such that the following inequalities hold for all $i,j \in \mathcal{M} = \{0,1,\ldots,N\}$:*

$$\begin{bmatrix} -H_i + He(\Xi_i) & * \\ -X+\Xi_i & H_j - X - X^\top \end{bmatrix} < 0 with, \tag{28}$$

$$\Xi_i = A^{i+1}X + \sum_{m=0}^{i} A^{i-m}BZ_m, \quad and A^0 = I_n. \tag{29}$$

Then the state-feedback control gain is given by

$$K_i = Z_i X^\top \tag{30}$$

Proof 2 *: Since the expression $K(\zeta(k_\kappa)) = K_i$, the proof matches up to that of Theorem 1 for $i,j \in 0,1,...,N$.*

V. Simulation example

In this section, a numerical example is provided from the literature in order to demonstrate the effectiveness of the developed approach. The system in (1) is described by the following matrices [17]:

$$A = \begin{bmatrix} 0.25 & 1 & 0 \\ 0 & 0.1 & 0 \\ 0 & 0 & 0.6 \end{bmatrix}, \quad B = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \tag{31}$$

The main objective is to assess the system's closed-loop performance using various controller synthesis techniques, both with and without accounting for DoS attacks. The MOSEK [18] solver and the YALMIP [19] parser were used to implement the functions in MATLAB. For comparison, three controllers were synthesized: K_{N0} is a standard state-feedback controller that is obtained by ignoring all potential attack scenarios, and taking into account a maximum of $N = 10$ consecutive packet losses The robust controller obtained from Theorem 1 is K_{Th1}. Furthermore, K_{Th2} combines a set of scheduled gains designed using Theorem 2, where the controller anticipates possible future DoS events by sending packets of control signals in advance.

$$K_{N0} = [0.0862 \quad -0.1149 \quad -0.4635], \qquad K_{Th1} = [0.0370 \quad -0.0024 \quad 0.0383]$$

$$K_{Th2} = \begin{bmatrix} K_0 \\ K_1 \\ K_2 \\ K_3 \\ K_4 \\ K_5 \\ K_6 \\ K_7 \\ K_8 \\ K_9 \\ K_{10} \end{bmatrix} = \begin{bmatrix} 0.0834 & -0.0854 & -0.3297 \\ 0.0267 & -0.0029 & -0.0010 \\ 0.0312 & 0.0115 & 0.0658 \\ 0.0257 & 0.0150 & 0.0801 \\ 0.0227 & 0.0161 & 0.0845 \\ 0.0224 & 0.0168 & 0.0878 \\ 0.0186 & 0.0162 & 0.0834 \\ 0.0215 & 0.0167 & 0.0871 \\ 0.0204 & 0.0167 & 0.0864 \\ 0.0213 & 0.0169 & 0.0881 \\ 0.0256 & 0.0184 & 0.0965 \end{bmatrix}$$

Figure 2 shows the trajectory of the system under the controller K_{N0} in the presence of persistent attacks with $N = 0$. As expected, the system becomes unstable, highlighting the inability of a classical approach to cope with DoS.

Figure 3 illustrates the robustness achieved with the controller K_{Th1} of Theorem 1. The system remains stable even under the worst-case DoS conditions $\delta(K_\kappa) = \in \{10,10,10,\ldots\}$.

As shown in Figure 4, the K_{Th2} method with $\delta(K_\kappa) = \in \{10,10,10,\ldots\}$, demonstrates the effectiveness of the packet-based approach based on Theorem 2. We assume that not only is the stability preserved, but the system also converges more rapidly compared to the previous method.

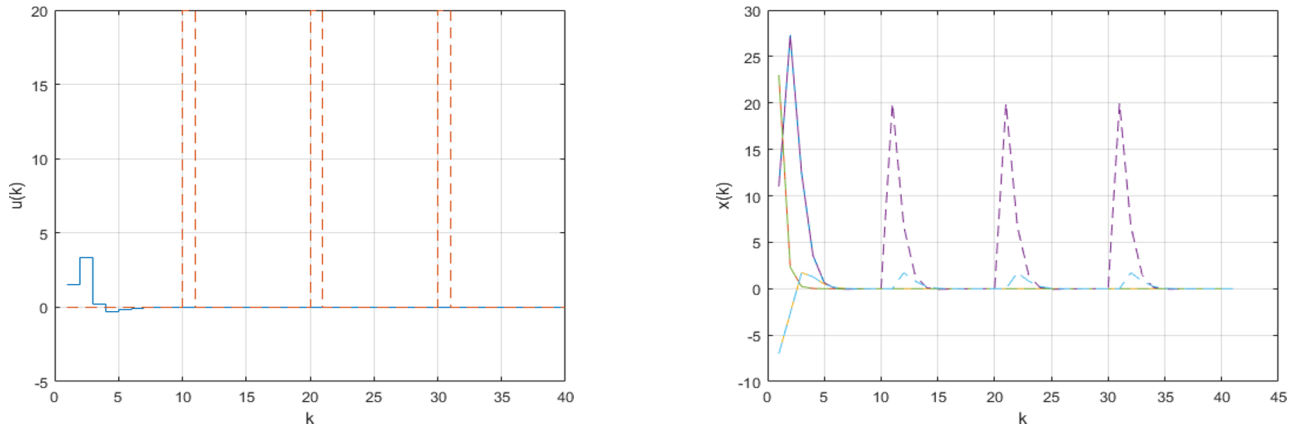

Fig. 2: Trajectories of states $x(k)$ represent a controller that ignores attacks during the design stage , and inputs $u(k)$ that get turned null during an attack , with (...) and without (—) DoS attack with $x_0 = [11 \quad 23 \quad -7]^\top$

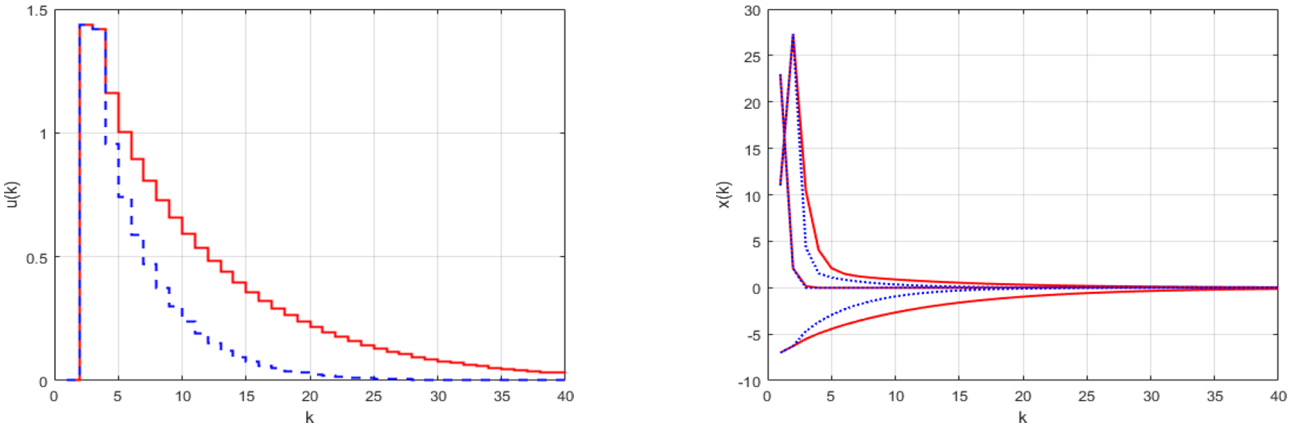

Fig. 3: Trajectories of states x(k) and inputs u(k) that follow Theorem 1's approach, with (...) and without (—) DoS attack with $x_0 = [11 \quad 23 \quad -7]^\top$

These simulations highlight the importance of incorporating resilience into controller design when faced with network-based disruptions.

VI. Conclusion

This paper has proposed strong control techniques for CPSs under DoS attacks. Two control laws were developed through feedback: a state feedback controller with bounded packet losses being considered and a packet-based approach that predicts up to $N + 1$ control decisions. The design conditions were formulated in terms of LMIs and solved using numerical tools. The results of simulations have shown that the proposed methods ensure asymptotic stability of the system considered. Surprisingly, the packet-based strategy resumes more rapidly under continuous attacks. These results highlight the importance of including cyber-resilience in control design.

References

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

[2] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2011.

[3] F. Pasqualetti, F. D¨orfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE transactions on automatic control*, vol. 58, no. 11, pp. 2715–2729, 2013.

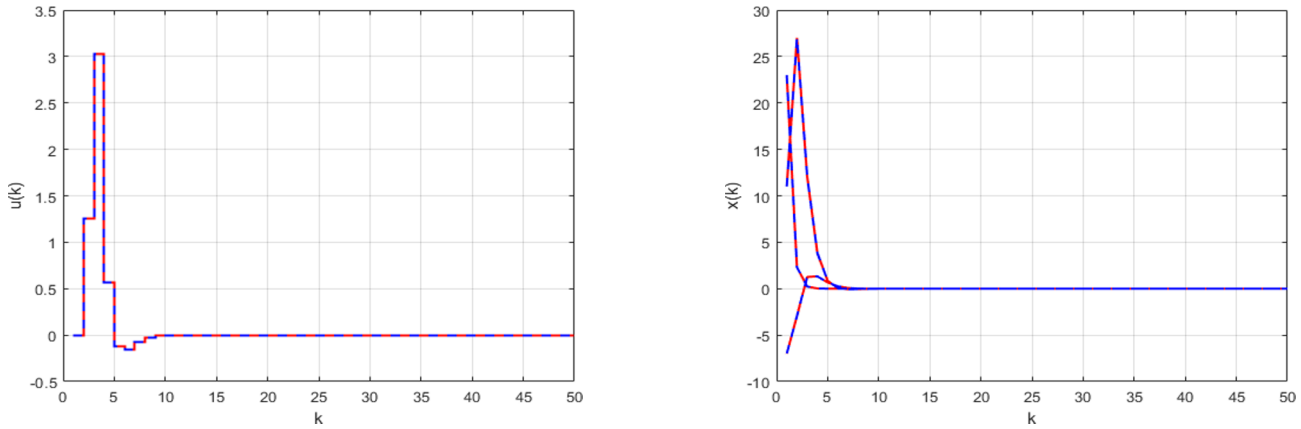

Fig. 4: Trajectories of states x(k) and inputs u(k) that follow Theorem 2's approach, with (...) and without (—) DoS attack .with $x_0 = [11 \quad 23 \quad -7]^\top$

[4] C. Elmakkaoui, F. Z. Darouiche, M. Charqi, N. Chaibi, and B. Boukili, "Robust h_∞ control of markov jump systems with time-delay and actuator saturation," *4th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), Fez, Morocco, DOI: 10.1109/IRASET60544.2024.10548979*, 2024.
[5] Y. El Fadili, B. Boukili, M. N'Diaye, and I. Boumhidi, "Robust state-feedback controller of uncertain systems based on non-monotonic approach," *International Journal of Adaptive Control and Signal Processing*, vol. 39, no. 1, pp. 88–100, 2025.
[6] M. Charqi, E. H. Tissir, I. Boumhidi, A. Hmamed, and B. Boukili, "New criteria for robust exponential stability of uncertain discrete-time switched systems with time-varying delay via average dwell time approach and under arbitrary switching signal," *Journal of Control, Automation and Electrical Systems*, vol. 35, no. 2, pp. 276–290, 2024.
[7] R. Borges, R. Oliveira, C. Abdallah, and P. Peres, "Robust networked control for systems with uncertain sampling rates," *IET control theory & applications*, vol. 4, no. 1, pp. 50–60, 2010.
[8] Z. Wang, L. Li, H. Sun, C. Zhu, and X. Xu, "Dynamic output feedback control of cyber-physical systems under dos attacks," *IEEE Access*, vol. 7, pp. 181032–181040, 2019.
[9] Y. Zhu and W. X. Zheng, "Observer-based control for cyber-physical systems with periodic dos attacks via a cyclic switching strategy," *IEEE Transactions on Automatic Control*, vol. 65, no. 8, pp. 3714–3721, 2019.
[10] P. M. Oliveira, J. M. Palma, and M. J. Lacerda, "H2 state-feedback control for discrete-time cyber-physical uncertain systems under dos attacks," *Applied Mathematics and Computation*, vol. 425, p. 127091, 2022.
[11] L. Zhao and W. Li, "Co-design of dual security control and communication for nonlinear cps under dos attack," *IEEE Access*, vol. 8, pp. 19271–19285, 2020.
[12] P. Gahinet, A. Nemirovskii, A. J. Laub, and M. Chilali, "The lmi control toolbox," in *Proceedings of 1994 33rd IEEE conference on decision and control*, vol. 3, pp. 2038–2041, IEEE, 1994.
[13] M. Vidyasagar, *Nonlinear systems analysis*. SIAM, 2002.
[14] Z. H., S. Y., and M. A.S., "Robust energy-to-peak filtering for networked systems with time-varying delays and randomly missing data," *IET Contr. The. and Applications*, vol. 4, no. 12, pp. 2921–2936, 2012.
[15] B. Boukili, A. Hmamed, A. Benzaouia, and A. E. Hajjaji, "h state control for 2d fuzzy fm systems with stochastic perturbation," *Circuits, Systems, and Signal Processing*, vol. 34, no. 3, pp. 779–796, 2015.
[16] 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, 2018.
[17] W. M. H. Heemels, J. Daafouz, and G. Millerioux, "Observer-based control of discrete-time lpv systems with uncertain parameters," *IEEE transactions on automatic control*, vol. 55, no. 9, pp. 2130–2135, 2010.
[18] 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*, pp. 197–232, Springer, 2000.
[19] J. Lofberg, "Yalmip: A toolbox for modeling and optimization in matlab," in *2004 IEEE international conference on robotics and automation (IEEE Cat. No. 04CH37508)*, pp. 284–289, IEEE, 2004.