On Multi-Input Controllable Linear Systems Under Unknown Periodic DoS Jamming Attacks

Hamed Shisheh Foroush and Sonia Martínez *

Abstract

In this paper, we study remotely controlled and observed multi-input controllable continuous linear systems, subject to periodic Denial-of-Service (DoS) jamming attacks. We first design a control and triggering strategy provenly capable of beating any *partially known* jammer via properly placing the closed-loop poles. Building on it, we then present an algorithm that is able to guarantee the system stability under *unknown* jamming attacks of this class. The functionality of this algorithm is also theoretically proven.

1 Introduction

Novel developments in the area of sensing and communication technologies have led to the emergence of complex *cyber-physical systems*. As first introduced in [6], cyber-physical systems entail network of physical systems which are remotely controlled and monitored. The advantages of cyber-physical systems range from ease of implementation to versatile usage in infrastructure facilities [14]. Whilst posing many advantages, they also bear some inherent challenges, including a higher exposure to external attacks. This has resulted in the emergence of an active research on the topic of *system security*, which aims to assess the safety of cyber-physical systems and establish more resilient designs [7, 1].

Indeed, the topic of cyber-physical systems security has been widely appealed within the controls community. To mention a few, in the context of multiagent systems, [22, 18, 19] aim to identify malicious agents who are part of the network. The main goal of [5, 4] is to maintain group connectivity despite the presence of a malicious agent. Also, within the formation framework, [28] proposes a Receding Horizon Control methodology to deal with a class of deceptive replay attackers inducing system delays. Our problem setup is related to these studies in the way that the jammer has been detected, and the goal is to develop a method to counteract its effect.

The other natural framework to study systems security is Game Theory; to mention a few representative studies, [12, 24, 21]. In these studies, the security problem is formulated as a (dynamic) zero-sum non-cooperative game. In [27], the reinforcement learning technique is employed to beat a deceptive attacker. To the extent of modeling the jammer, the closest work to our studies stated in this paper are [12, 13], nonetheless, the method exploited to guarantee the stability differs greatly in our paper since game theoretical framework is not deployed.

In this paper, we focus on *Denial-of-Service (DoS)* attacks [26, 20], where the attacker aims at dropping the transmitted data. In particular, we narrow our study down to the attacks caused by the so-called *periodic*, or *Pulse-Width Modulated (PWM)* jammers. This type of attack is motivated by the ease of implementation and energy constraints; e.g., see [8, 11].

In particular, we address the problem of system resilience in the context of *triggering control*, i.e., control is updated if required. This is motivated by maintaining the intelligent and economic communications. The recent works [23, 17, 25] have inspired our research; the distinctive feature in our study is that communication is not always feasible. To cover the globe, [15] addresses the security problem and formulates it in the triggering framework, however, it differs in its attacker model, indeed, [15] considers a class of deceptive attack.

In brief, we first address the problem of partially known DoS attacks caused by PWM jammers on multi-input linear systems to be controlled by sporadic feedback. Then, built on the obtained results, we introduce joint identification and control strategy, JAMCOID, to deal with any unknown DoS jammer of the same class. With respect to our earlier works, [10, 9], the contributions of this note are, (i) the proposal of a parameter-dependent resilient triggering and control strategy for multi-input controllable linear systems, and (ii) the design of JAMCOID algorithm to address unknown periodic DoS PWM jamming attacks.

*The authors are with Department of Mechanical and Aerospace Engineering, University of California, San Diego, 9500 Gilman Dr, La Jolla CA, 92093, hshisheh,soniamd@ucsd.edu

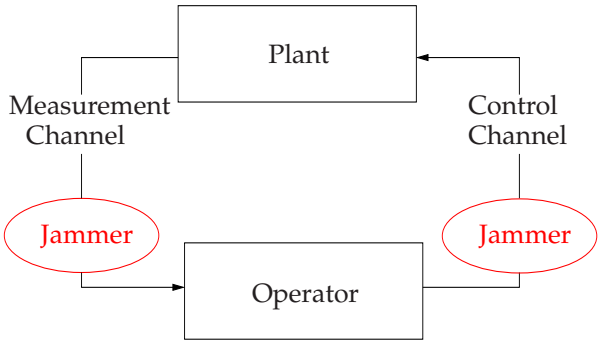

Figure 1: Problem Architecture

2 Problem Formulation

In this section, we state the main problems analyzed in the paper.

We consider a remote operator-plant setup, where the operator uses a control channel to send wirelessly the control command to an open-loop unstable plant, see Figure 1. We assume that the plant has no specific intelligence and is only capable of updating the control based on the data it receives. We also assume that the operator knows the plant dynamics and is able to obtain measurements of its states at particular time-instants.

More precisely, consider the following closed-loop dynamics:

$$\dot{x}(t) = Ax(t) + Bu(t)\,, \tag{2.1a}$$

$$u(t) = Kx(t_k)\,, \quad \forall t \in [t_k, t_{k+1}[\,, \tag{2.1b}$$

where $x \in \mathbb{R}^d$ is the state vector, $u \in \mathbb{R}^m$ is the input, A, B and K are matrices of proper dimensions, and $\{t_k\}_{k\geq 1}$ is a triggering time-sequence. Here, we also assume that: (i) System (2.1a) is open-loop unstable, and, (ii) the pair (A, B) is controllable.

We consider an *energy-constrained* jammer—causing jamming attack on the control and measurement communication channels—whose signal can be represented as follows:

$$u_{\text{jmd}}(t) = \begin{cases} 0\,, & (n-1)T \leq t \leq (n-1)T + T_{\text{off}}^{n-1}\,, \\ 1\,, & (n-1)T + T_{\text{off}}^{n-1} \leq t \leq nT\,, \end{cases} \tag{2.2}$$

where $T \in \mathbb{R}_{>0}$, and $n \in \mathbb{N}$. The sequence $T_{\text{off}}^n \in \mathbb{R}_{>0}$, $T_{\text{off}}^n < T$, defines the time-intervals $[nT, nT + T_{\text{off}}^n]$, when the jammer is sleeping and communication is possible. We further denote $T_{\text{on}}^n \in \mathbb{R}_{>0}$, and, $[T_{\text{on}}^n, (n+1)T]$ be the time-interval where the jammer is active, thus no data can be sent, and nor the system state can be measured. Accordingly, it holds that $T_{\text{off}}^n + T_{\text{on}}^n = T$, $n \in \mathbb{N}$. In this way, the parameter T_{off}^n need not be time-invariant which recalls Pulse-Width Modulated (PWM) jamming. Finally, we denote by $T_{\text{off}}^{\text{cr}}$ a uniform lower-bound for T_{off}^n, i.e., $T_{\text{off}}^{\text{cr}} \leq T_{\text{off}}^n$, $\forall n \in \mathbb{N}$, where also we denote $T_{\text{on}}^{\text{cr}} \triangleq T - T_{\text{off}}^{\text{cr}}$.

In this paper, we shall first assume the type of jammer and the period of jamming signal have been identified, accordingly, we study the system asymptotic stability. Then, we shall address a scenario where the jammer period is not known, we propose a way to tackle this situation. More precisely, we study the following problems:

> *[Problem 1]*: Consider any energy-constrained jammer described by (2.2) with parameters T and T_{off}. Knowing T and $T_{\text{off}}^{\text{cr}}$, design a control and triggering strategy of the form (2.1b) resilient to the action of this jammer.
>
> *[Problem 2]*: Consider any energy-constrained jammer described by (2.2), where also the jammer's and operator's clocks are initially asynchronous by some time, t_j. Knowing $T_{\text{off}}^{\text{cr}}$, propose a method to guarantee the asymptotic stability of the system, despite lack of knowledge on T and asynchronicity, t_j.

3 Background and Preliminary Results

In this section, we briefly discuss the specific canonical form of a multi-input system to be considered in this paper; it is needed to keep the analysis self-contained and given the fact this form is not unique for this class of systems. The employed technique is inspired from [16, 2], it comes with certain advantages useful in our later analyses. We perform here the explanations to the required extent.

The pair (A, B) in (2.1) is controllable iff the following matrix is full rank:

$$\Gamma = [B, AB, A^2B, \ldots, A^{d-1}B]\,,$$

where, $\Gamma \in \mathbb{R}^{d \times d.m}$. Thus, there exist at least d-linearly independent columns in Γ. The paper [2] describes how to extract these d columns. Accordingly, [2] derives certain numbers, p, and $\{r_i\}_{i=1}^p$, which define the static similarity transformation matrix, T_s, to be applied on the system, where it also holds that $\sum_{i=1}^p r_i = d$.

Applying this similarity transformation matrix, T_s, in the following way:

$$A \to \hat{A} = T_s A T_s^{-1}\,, \qquad B \to \hat{B} = T_s B\,,$$

$$K \to \hat{K} = T_s^{-1} K\,, \qquad x \to \hat{x} = T_s x\,,$$

transforms Dynamics (2.1) into:

$$\dot{\hat{x}}(t) = \hat{A}\hat{x}(t) + \hat{B}u(t)\,, \tag{3.3a}$$

$$u(t) = \hat{K}\hat{x}(t_k)\,, \quad \forall t \in [t_k, t_{k+1}[\,, \tag{3.3b}$$

where $\hat{A}$ and $\hat{B}$, shall be in a favorite form. In what follows, and with a slight abuse of notation, we denote $A \equiv \hat{A}$, $B \equiv \hat{B}$, $K \equiv \hat{K}$, and $x \equiv \hat{x}$.

The transformed state-matrix is obtained as follows:

$$A = \begin{array}{c} \\ \\ \\ \\ r_2 \\ \\ \\ r_1 \end{array} \overset{\begin{array}{ccccccc} & & r_2 & & & r_1 & \\ \end{array}}{\left[\begin{array}{ccc:ccc} \cdot & & & 0 & \cdot & 0 & 0 & \cdot & 0 \\ & \cdot & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & \cdot & 0 & \cdot & 0 & 0 & \cdot & 0 \\ \hdashline & & & 0 & \cdot & 0 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & -\beta_{r_2} & \cdot & -\beta_1 & 0 & \cdot & 0 \\ \hdashline & & & -m_1 & \cdot & 0 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & -m_{r_1} & \cdot & 0 & -\alpha_{r_1} & \cdot & -\alpha_1 \end{array}\right]}$$

LEMMA 3.1. ([2]) *The matrix A satisfies the following:*

1. *It is a block-diagonal matrix, with all the elements above the diagonal equal to zero,*
2. *The diagonal blocks are $r_i \times r_i$, where $r_i \in \{r_i\}_{i=1}^{p}$,*
3. *All the diagonal blocks are in the controllable canonical form of a single-input system,*
4. *The elements below the diagonal blocks are all zero, except on the $\sum_{j=1}^{i} r_i$-th, $i \in \{1, \ldots, p\}$ columns, which, depending on the original system, may or may not be zero.*

The transformed input-matrix is given by:

$$B = \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \overset{\begin{array}{cccccccc} & p & & & & & m-p & \\ \end{array}}{\left[\begin{array}{cccc:cccc} 0 & 0 & \cdot & 0 & \times & \cdot & \cdot & \times \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 1 & \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & 0 & \cdot & 0 & \times & \cdot & \cdot & \times \end{array}\right]}.$$

LEMMA 3.2. ([2]) *The matrix B satisfies the following:*

1. *The arrays of B on its $j-$th column, for $j \in \{1, \ldots, p\}$, are given as follows:*

$$b_{ij} = \begin{cases} 1\,, & i = d - \sum_{k=1}^{j-1} r_k\,, \\ 0\,, & \textit{otherwise}\,, \end{cases}$$

which recalls the input-matrix of a single-input system in its controllable canonical form,

2. *The other arrays of B on its $j-$th column, for $j \in \{p+1, \ldots, m\}$, consist of real values dependent on the original system.*

We now introduce a particular choice of control gains to be applied on the transformed system.

PROPOSITION 3.1. *Consider System* (3.3)*, let the control matrix K_λ be as follows:*

$$K_\lambda = \begin{array}{c} \\ p \\ \\ \\ \\ m-p \end{array} \overset{\begin{array}{cccccccccccc} & & & & & & & & & & & \\ \end{array}}{\left[\begin{array}{cccccccccccc} 0 & \cdot & 0 & \cdot & 0 & 0 & \cdot & 0 & \kappa_{r_1} & \cdot & \kappa_1 \\ 0 & \cdot & 0 & \cdot & 0 & \lambda_{r_2} & \cdot & \lambda_1 & 0 & \cdot & 0 \\ 0 & \cdot & \mu_{r_3} & \cdot & \mu_1 & 0 & \cdot & 0 & 0 & \cdot & 0 \\ & & & & & \cdot & & & & & \\ & & & & & \cdot & & & & & \\ & & & & & \cdot & & & & & \\ \hdashline & & & & & \mathbf{0} & & & & & \end{array}\right]},$$

where the elements on its first three rows are chosen as in:

$$\kappa_i = -\binom{r_1}{i}\lambda^i + \alpha_i\,, \quad i \in \{1, \ldots, r_1\}\,,$$

$$\lambda_i = -\binom{r_2}{i}\lambda^i + \beta_i\,, \quad i \in \{1, \ldots, r_2\}\,,$$

$$\mu_i = -\binom{r_3}{i}\lambda^i + \gamma_i\,, \quad i \in \{1, \ldots, r_3\}\,,$$

and, similarly, for the other arrays. Then, all the eigenvalues of the closed-loop matrix, $A + BK_\lambda$, i.e., the closed-loop system poles, are placed at $-\lambda$.

Proof. The proof relies on the exploitation of $A + BK_\lambda$ block diagonal structure, and that every i^{th} block is in canonical form. We omit it here.

We characterize the algebraic and geometric multiplicities of the eigenvalue $-\lambda$ in the next result. Beforehand, we also note that the unconventional arrangement of the arrays in matrices A and K_λ is for the ease and consistency of presentation.

PROPOSITION 3.2. *Consider System* (3.3)*, along with the control gains stated in Proposition 3.1. Also, consider the $\{1 + \sum_{j=0}^{i} r_{p-j}\}_{i=-1}^{p-2}$-th columns of $A + BK_\lambda$ matrix, and let q be the number of columns in this sequence with all the zero-elements below its $\{\sum_{j=0}^{i} r_{p-j}\}_{i=0}^{p-1}$-th row. Then, the algebraic multiplicity of $-\lambda$ is d, moreover, its geometric multiplicity is $1 + q$, where $1 \leq 1 + q \leq p$.*

Proof. It is easy to see that with this choice of K_λ, $\det(sI - (A + BK_\lambda)) = (s + \lambda)^d$ follows. Thus, the algebraic multiplicity of $-\lambda$ is d.

Note that the geometric multiplicity of $-\lambda$ is equal to the kernel of $A+BK_\lambda+\lambda I$, given by [3]:

$$\ker(A+BK_\lambda+\lambda I) = d-\operatorname{rank}(A+BK_\lambda+\lambda I)\,. \tag{3.4}$$

For simplicity, let us assume $p=2$. Then, we get:

$$A+BK_\lambda+\lambda I = \begin{array}{c} \begin{matrix} \quad r_2 & & & \quad r_1 & & & \end{matrix} \\ \left[\begin{array}{ccc:ccc} \lambda & \cdot & 0 & 0 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & 1 & 0 & 0 & \cdot & 0 \\ -\lambda^{r_2} & \cdot & (-r_2+1)\lambda & 0 & 0 & \cdot & 0 \\ \hdashline -m_1 & \cdot & 0 & \lambda & 1 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ -m_{r_1-1} & \cdot & 0 & 0 & 0 & \cdot & 1 \\ -m_{r_1} & \cdot & 0 & -\lambda^{r_1}-r_1\lambda^{r_1-1} & \cdot & (-r_1+1)\lambda & \end{array}\right] \begin{matrix} \\ \\ r_2 \\ \\ \\ r_1 \\ \\ \end{matrix} \end{array}.$$

For this matrix, we note, (i) if $\forall k \in \{1,\dots,r_1\}, m_k = 0$, then there are r_2-1 linearly independent columns in the first r_2-columns, otherwise, there are r_2, (ii) there are r_1-1 linearly independent columns in the second r_1-columns of this matrix, and, (iii) the first r_1-columns cannot influence the linear independence of the second r_2-columns. Therefore, depending on the values of m_k, there are either $r_1-1+r_2 = d-1$, or $r_1-1+r_2-1 = d-2$ linearly independent columns in $A+BK_\lambda+\lambda I$. This implies:

$$\operatorname{rank}(A+BK_\lambda+\lambda I) = \begin{cases} d-2\,, & \text{if } m_k = 0\,,\ \forall k \in \{1,\dots,r_1\}\,, \\ d-1\,, & \text{otherwise}\,. \end{cases}$$

Let q be as defined in the proposition statement, then, the last argument attributed for $p=2$, can be also extended, where we conclude:

$$\operatorname{rank}(A+BK_\lambda+\lambda I) = d-1-q\,.$$

Now, plugging the latter equation into (3.4), yields:

$$\ker(A+BK_\lambda+\lambda I) = q+1\,,$$

which then implies the geometric multiplicity of $-\lambda$ is $q+1$. Moreover, by definition of q, it is at most $p-1$ and at least 0, thus $1 \le 1+q \le p$. The proof is complete.

4 Jordan Decomposition and Triggering Strategy

In this section, we first present the Jordan decomposition of the closed-loop matrix of System (3.3) where K_λ is chosen as in Proposition 3.1. Then, we shall introduce the triggering strategy which solves Problem 1.

According to Proposition 3.2, matrix $A+BK_\lambda$ has at most p linearly independent eigenvectors, where $p \le m < d$. Thus, this matrix is *not* diagonalizable, this fact motivates us to study its Jordan decomposition. Since the eigenvalues of $A+BK_\lambda$ are placed at $-\lambda$, we have:

$$A+BK_\lambda = T_\lambda J_\lambda T_\lambda^{-1}\,, \tag{4.5}$$

where, $J_\lambda = -\lambda I + N$, and, T_λ is a matrix built upon the linearly independent and generalized eigenvectors of $A+BK_\lambda$.

Note that, by Proposition 3.2, the geometric multiplicity of $-\lambda$ is *constant* for all $\lambda \in \mathbb{R}_{>0}$. Therefore, matrix N is *unique* for all values of $\lambda \in \mathbb{R}_{>0}$. Moreover, since the arrays of $A+BK_\lambda$ are polynomial functions of λ, the eigenvectors of $A+BK_\lambda$ are rational functions of λ. Hence, T_λ and T_λ^{-1} also depend on λ in a rational way. These observations are useful in the stability analysis stated in next section.

Based on this Jordan decomposition technique, we introduce a family of coordinate transformations. Let us consider System (3.3a), with the control, $u(t) = K_\lambda x(t_k)$. Then, the closed-loop dynamics is:

$$\dot{x} = (A+BK_\lambda)x + BK_\lambda e\,,$$

where, $e(t) = x(t_k) - x(t)$. Recalling (4.5), the transformations $e(t) = T_\lambda e_\lambda(t)$, and, $x(t) = T_\lambda x_\lambda(t)$ yield:

$$\dot{x}_\lambda = J_\lambda x_\lambda + T_\lambda^{-1} BK_\lambda T_\lambda e_\lambda\,. \tag{4.6}$$

We state the following result as a first step in developing our triggering strategy.

PROPOSITION 4.1. *Take $\lambda > \|N\| + 1/2$ and K_λ as in Proposition 3.1. Then, $V(x_\lambda) = x_\lambda^T x_\lambda$ is an ISS-Lyapunov function for System* (4.6) *and the event-triggering condition:*

$$|e_\lambda(t)|^2 \le \frac{\sigma(2\lambda-1-2\|N\|)}{\|T_\lambda^{-1}BK_\lambda T_\lambda\|^2}|x_\lambda(t)|^2\,, \tag{4.7}$$

guarantees the asymptotic stability of this system, for $\sigma \in (0,1)$.

Proof. The proof is omitted for space reasons. It follows along the lines of Proposition 4.1 in [9].

Let t_k and t_{k+1} be two consecutive time-instants given by event-triggering strategy (4.7). Then, for each λ, the following holds:

$$\exists \tau_\lambda > 0\,, \text{ such that } t_{k+1} - t_k \ge \tau_\lambda\,, \forall k \in \mathbb{N}\,.$$

This is based on Theorem III.1, presented in [23]. In particular, [23] shows how to compute such τ_λ. This implies the time-sequence generated by event-triggering strategy (4.7) does not accumulate. Since in this paper we do *not* assume the operator can continuously measure the plant states, we adopt this τ_λ as the basis of our triggering strategy.

THEOREM 4.1. *The parameter, τ_λ, satisfies the following:*

$$\lim_{\lambda\to\infty} \tau_\lambda = 0\,.$$

Proof. The proof can be found in Theorem 4.3 in [9]. At a sketch level, the main idea is to use $\tau_\lambda \leq t_2 - t_1$, where then letting $t_1 = 0$, and denoting $t_\lambda \triangleq t_2$, we show $\lim_{\lambda\to\infty} t_\lambda = 0$, which then induces $\lim_{\lambda\to\infty} \tau_\lambda = 0$. In this way, the uniqueness of matrix N—for all λ—in the Jordan decomposition technique, and, event-triggering condition (4.7) (at which t_λ holds), play important roles.

In this paper, we assume the jammer is causing a *"worst-case jamming scenario"*, i.e., $T^n_{\text{off}} = T^{\text{cr}}_{\text{off}}$, $\forall n \in \mathbb{N}$. Now, using the parameter τ_λ, we define our triggering strategy as follows.

DEFINITION 4.1. *The triggering strategy used in this paper, despite presence of the jammer and to solve Problem* 1*, is defined as follows:*

$$t^*_{k,n} \in \left\{ l\tau_\lambda \,\middle|\, l\tau_\lambda \in [(n-1)T, (n-1)T + T^{\text{cr}}_{\text{off}}] \right\} \cup \{nT\}\,. \tag{4.8}$$

In this strategy, $k \in \mathbb{N}$ denotes the number of triggering time-instants occurring in the n^{th} jammer period, and $l \in \mathbb{N}$ stands for the multiples of τ_λ starting from $l = 1$ in the first period and adding up afterwards. We also note that based on Theorem 4.1, and for a given T, we can find a λ_c so that the multiples of τ_λ lie in the desired interval, i.e., the set introduced in (4.8) *is never empty. At last, we also note that for a fixed n, the largest $t^*_{k,n}$ is nT whereas $t^*_{1,n+1} = nT + \tau_\lambda$, thus these two time-instants do not coincide.*

5 Stability Analysis of the Control and Triggering Strategy

Here, we present the main result on the control and triggering strategy which addresses Problem 1.

THEOREM 5.1. *Consider System* (3.3)*, given a jamming signal* (2.2) *with a known pair $(T^{\text{cr}}_{\text{off}}, T)$, then $\exists \lambda^* > \|N\| + 1/2$, such that $\forall \lambda \geq \lambda^*$, the system with control gain K_λ as chosen in Proposition 3.1 and with triggering strategy* (4.8) *is asymptotically stable.*

Proof. The analysis is performed in an analogous way as in the proof of Theorem 5.1 in [9], nonetheless for multi-input systems. At a sketch level, the main idea is to characterize the function $C(\lambda)$ with the following property:

$$|x(T)| < C(\lambda)|x_0|\,,$$

and, to further show:

$$\lim_{\lambda\to\infty} C(\lambda) = 0\,, \tag{5.9}$$

whereby, the following can be inferred:

$$\exists \lambda^* \text{ such that } \forall \lambda > \lambda^*, C(\lambda^*) < 1\,.$$

Therefore, by induction argument, we get the sequence $\{x(nT)\}$ is a strictly decreasing sequence; hence, by a Lyapunov argument, the proof will be completed. On this way, the results explained in Section 4, namely, (i) the Jordan decomposition technique, wherein the uniqueness of matrix N for all values of λ is guaranteed, (ii) the rational dependency of T_λ and T_λ^{-1} matrices on λ, (iii) the ISS Lyapunov function introduced in Proposition 4.1, and, (iv) the assertion of Theorem 4.1, are extremely helpful. Due to space limits, the details are omitted here.

6 Stabilization under unknown jamming signals

In this section, we propose a solution to Problem 2. It is built on the control and triggering strategy introduced in Section 4, along with the stability analysis presented in Section 5. First, we shall state our algorithm, and then we analyze the asymptotic stability of the system deploying it.

6.1 The JAMCOID **Algorithm** To begin with, we note that the jammer's and operator's clocks need not be synchronized. Let $t_j \geq 0$ be this asynchronicity, i.e., the time difference between the jammer clock's initial time and the operator's. We then realize there are three unknown parameters, $T^{\text{cr}}_{\text{on}}$, T, and t_j, which characterize the jamming signal, together with the known parameter, $T^{\text{cr}}_{\text{off}}$.

Let $u_{\text{id}} : \mathbb{R}_{\geq 0} \to \{1\} \cup \{\texttt{null}\}$ be the signal which operator uses for jammer identification purposes, where $u_{\text{id}}(t) = 1$ encodes that the operator sends message 1 to the plant, whereas, $u_{\text{id}}(t) = \texttt{null}$ declares no message is submitted. Let also $u_{\text{ste}} : \mathbb{R}_{\geq 0} \to \{\texttt{null}\} \cup \mathbb{R}^d$ be the rebound signal from the plant, such that $u_{\text{ste}}(t) \in \mathbb{R}^d$ is a successfully delivered message containing state information, while $u_{\text{ste}}(t) = \texttt{null}$ represents no message is delivered. Finally, let $u_{\text{ctrl}} : \mathbb{R}^d \to \{\texttt{null}\} \cup \mathbb{R}^m$ be the control

submitted to the plant, where similar to the u_{id}-case, $u_{\text{ctrl}}(t) \neq \texttt{null}$ induces that a control $u_{\text{ctrl}}(t)$ is computed and sent to the plant, whereas $u_{\text{ctrl}}(t) = \texttt{null}$ infers that no message is sent.

In fact, we assume that the submission of u_{id}, receipt of u_{ste}, and submission of u_{ctrl} happen in a sequential and instantaneous manner. That is, first a measurement is requested by sending u_{id}, then upon its receipt, via u_{ste}, a control is sent to the plant, via u_{ctrl}. It is nonetheless worth noting that $u_{\text{ste}}(t) = \texttt{null}$ if and only if $u_{\text{ctrl}}(t) = \texttt{null}$, i.e., we do *not* send any control if we do *not* receive any measurement, and this happens when the jammer is active at t.

Intuitively, the core idea behind JAMCOID is to intelligently plan the triggering time-sequence $\{t_k\}$ in order to (i) bound (not necessarily eliminate) asynchronicity, t_j, (ii) find a valid useful interval to which T, or some multiple of this period, belongs. Our JAMCOID algorithm is formally described in the following lines, wherein the control, $u_{\text{ctrl}}(t_k)$, is computed as explained in Section 3, Proposition 3.1.

Step I: Set $u_{\text{id}}(t_k) = 1$, according to $t_k = kM$, where $k \in \mathbb{N}$, for $M = \tau_\lambda < \frac{T_{\text{off}}^{\text{cr}}}{2}$, and some τ_λ as introduced in Section 4. Because $T_{\text{on}}^{\text{cr}}$ is unknown, we can distinguish between two cases:

> **Case (1):** We do *never* hit the jammer's on-subperiod, that is, $u_{\text{ste}}(t_k) \neq \texttt{null}, \forall\, t_k$. Thus, we keep updating the control at the prescribed times without interruption.
>
> **Case (2):** In this case, we hit the on-subperiod some time on the way. That is:
>
> $$\exists k_1 \text{ such that } u_{\text{ste}}(k_1 M) = \texttt{null} \text{ and } u_{\text{ste}}((k_1+1)M) \neq \texttt{null},$$
>
> where, recalling the jamming signal, following holds:
> (6.10)
> $\exists k_1$ and l_1 such that $k_1 M < t_j^1 + l_1 T \leq (k_1+1)M$.
>
> If this case occurs, we move on to **Step II**.

Step II: At time $t = (k_1+1)M$, the operator resets his clock as $t \leftarrow t - k_1 M$. Let us denote $t_j^2 = t_j^1 + l_1 T - k_1 M$, then by (6.10), we obtain:

$$0 < t_j^2 \leq M\,. \tag{6.11}$$

Step III: Similar to **Step I**, we set $u_{\text{id}}(t_k) = 1$ at $t_k = kM$. Again, two cases are possible:

> **Case (1):** Same as **Case (1)**, in **Step (1)**.
>
> **Case (2):** In this case, we hit the on-subperiod some time on the way. That is:
>
> $$\exists k_2 \text{ such that } u_{\text{ste}}(k_2 M) = \texttt{null} \text{ and } u_{\text{ste}}((k_2+1)M) \neq \texttt{null},$$
>
> where, recalling the jamming signal, following holds:
> (6.12)
> $\exists k_2$ and l_2 such that $k_2 M < t_j^2 + l_2 T \leq (k_2+1)M$.
>
> If this case occurs, we move on to **Step IV**.

Step IV: At time $t = (k_2+1)M$, the operator resets his clock as $t \leftarrow t - k_2 M$. Further, let us also denote $t_j^3 = t_j^2 + l_2 T - k_2 M$, by (6.12), we get:

$$0 < t_j^3 \leq M\,,$$

where, additionally:

$$(k_2-1)M < t_j^3 + l_2 T \leq (k_2+2)M\,. \tag{6.13}$$

Step V: Let $\tilde{l} = \lfloor \frac{T_{\text{off}}^{\text{cr}}}{M} \rfloor$ and consider the time-interval $[M, \tilde{l}M]$. Since $0 < t_j^3 \leq M$, from definition of $\tilde{l}$, $\tilde{l}M \leq T_{\text{off}}^{\text{cr}}$ follows. Also, communication with the plant is feasible at any time in $[M, \tilde{l}M]$. Hence, $[M, \tilde{l}M]$ plays the role of $[0, T_{\text{off}}^{\text{cr}}]$ in known jammer scenario; this observation is used in this step.

From (6.13), note that $(k_2+2)M$ is a valid upper-bound for the unknown parameter $t_j^3 + l_2 T$. Thus we estimate $l_2 T$ by $(k_2+2)M$. We then keep updating the control at time-instants given by the following triggering strategy:
(6.14)
$$t_k \in \big\{ lM \mid lM \in [M, \tilde{l}M] \big\} \cup \{(k_2+2)M\}\,, \forall \lambda \in \mathbb{R}_{>0}\,.$$

In addition to communicating with the plant at the time-instants declared in (6.14), the operator sets $u_{\text{id}}(k_2 M) = 1$ and $u_{\text{id}}((k_2+1)M) = 1$, and obtains $u_{\text{ste}}(k_2 M)$, $u_{\text{ste}}((k_2+1)M)$; two cases may occur:

> **Case (1):** $u_{\text{ste}}(k_2 M) \neq \texttt{null} \neq u_{\text{ste}}((k_2+1)M)$. Thus, the operator does not detect an on-to-off transition of the jammer's signal from $(l_2-1)T$ to $l_2 T$. It also means that the length of $(l_2-1)T$ on-subperiod, is shorter than M. In this case, we reset $M \leftarrow \frac{M}{\delta}$, where $\delta \in (1, \infty)$ is a design parameter. We note that, by construction of τ_λ, $\exists \lambda$, such that $\tau_\lambda = \frac{M}{\delta}$. Then, repeat from **Step I**.
>
> **Case (2):** Either $u_{\text{ste}}(k_2 M) = \texttt{null}$, or $u_{\text{ste}}((k_2+1)M) = \texttt{null}$, or both. In other words, an on-to-off transition of the jammer's signal happens

from $(l_2-1)T$ to l_2T. This is characterized by $\bar{k}M$, where:

$$\bar{k} = \max\{k_2,\, k_2+1 \big| u_{\text{ste}}(k_2M) = \texttt{null},\\ u_{\text{ste}}((k_2+1)M) = \texttt{null}\}\,.$$

Reset $k_2 \leftarrow \bar{k}$, $t \leftarrow t - \bar{k}M$, and $t_j^3 \leftarrow t_j^3 + l_2T - \bar{k}M$, for which (6.13) also holds. Then, repeat from **Step V**.

6.2 The Stability of the JAMCOID **Algorithm** Having stated the jammer identification and control algorithm in Subsection 6.1, we characterize its convergence properties in this subsection.

THEOREM 6.1. *Consider System* (3.3)*, and a jamming signal described by* (2.2)*, with constant parameters* T*,* $T_{\text{off}}^{\text{cr}}$*, and* $T_{\text{on}}^{\text{cr}}$*, where only* $T_{\text{off}}^{\text{cr}}$ *is known. The jammer identification and control algorithm,* JAMCOID*, renders the system asymptotically stable.*

Proof. The asymptotic behavior of JAMCOID is one of the following items:

1. **Case (1)** in **Step I**,
2. **Case (1)** in **Step III**,
3. **Case (2)** in **Step V**.

It cannot be otherwise, since **Case (2)** in **Step I**; **Step II**; **Case (2)** in **Step III**; and **Step IV** are intermediate computations. Moreover, **Case (1)** in **Step V** is out of sight, because repeating this case—with the same parameter δ—yields the triggering period, $\frac{M}{\delta^n}$, where given $T_{\text{on}}^{\text{cr}}$ constant, $\delta \in (1,\infty)$, and $T_{\text{on}}^{\text{cr}} \leq T_{\text{on}}$, then we deduce:

$$\exists n^* < \infty \in \mathbb{N} \,\text{such that}\, \forall n > n^*,\ \frac{M}{\delta^n} < T_{\text{on}}^{\text{cr}}\,.$$

Therefore, in worst case, we shall repeat **Case (1)** in **Step V** only $n^* < \infty$ number of times.

In order to prove asymptotic stability, we assess possible asymptotic behaviors. Under items 1 and 2, the jammer is not corrupting communication channels. Therefore, since the triggering time-sequence is chosen to be $k\tau_\lambda$, with $k \in \mathbb{N}$, thus the asymptotic stability is maintained.

Item 3 leads to the iteration of **Step V** (through **Case (2)**). Stability will follow from the application of Theorem 5.1 for each iteration of this item via approximating $T \equiv (k_2+2)M$. This completes the proof.

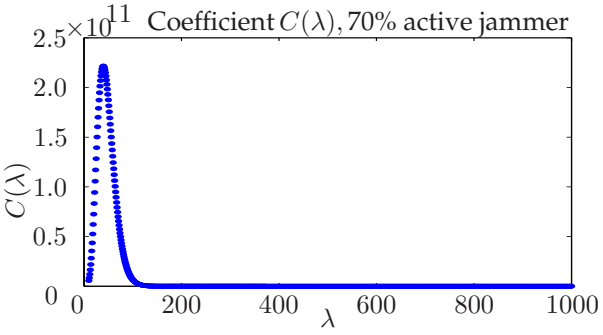

Figure 2: Fourth-order multi-input system: evolution of $C(\lambda)$

7 Simulations

In this section, we demonstrate the functionality of the aforementioned theoretical results on a representative academic example.

We consider the following system:

$$\dot{x} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -5 & 7 & 0 & 0 \\ 3 & 0 & 0 & 1 \\ 2 & 0 & 6.5 & 8 \end{bmatrix} x + \begin{bmatrix} 0 & 0 & -6 \\ 0 & 1 & 7.5 \\ 0 & 0 & 8.3 \\ 1 & 0 & 9 \end{bmatrix} u\,,$$

$$u = \begin{bmatrix} 0 & 0 & -\lambda^2 - 6.5 & -2\lambda - 8 \\ -\lambda^2 + 5 & -2\lambda - 7 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} x\,,$$

wherein, $d = 4$, $m = 3$, $p = 2$, $r_1 = 2$, and $r_2 = 2$. For the sake of brevity, we do not introduce the matrices $A + BK_\lambda$, T_λ, and N, here.

The goal of the simulation is to verify Equation (5.9) stated in the proof sketch of Theorem 5.1. In order to do so, we run the $C(\lambda)$-Seeking Algorithm presented in [9] to obtain the sequence, $\{C(\lambda_k)\}_{k=1}^{1000}$, for $\{\lambda_k = k\}_{k=1}^{1000}$; with set of parameters, $\sigma = 0.001$, $T = 1\,\text{sec}$, $T_{\text{on}}^{\text{cr}} = 0.7T$, and $T_{\text{off}}^{\text{cr}} = 0.3T$. The result is presented in Figure 2. Referring to this figure, we observe that $\lim_{\lambda\to\infty} C(\lambda) = 0$ holds, i.e., (5.9) is verified.

8 Conclusions and Future Work

In this study, we have considered multi-input controllable continuous linear systems, under periodic PWM DoS jamming attacks. We first recalled a specific canonical form for this class of systems and introduced our control strategy. We then elaborated our triggering strategy, entailing the time-instants to update the control. We then proved this control and triggering strategy is able to beat the considered partially known jamming attacks. Consequently, we proposed JAMCOID algorithm, capable of beating considered unknown jamming attacks.

As future work, we are to extend these results to cope with non-periodic PWM DoS jamming attacks; and to stretch our problem formulation to a multiagent setup.

References

[1] N. ADAMS, *Workshop on future directions in cyber-physical systems security*, tech. report, Department of Homeland Security (DHS), 2010.

[2] B.D.O. ANDERSON AND D.G. LUENBERGER, *Design of multivariable feedback systems*, Proceedings of the Institution of Electrical Engineers, 114 (1967), pp. 395–399.

[3] D.S. BERNSTEIN, *Matrix Mathematics: theory, facts, and formulas with application to linear system theory*, Princeton University Press, 2005.

[4] S. BHATTACHARYA AND T. BASAR, *Differential game-theoretic approach to a spatial jamming problem*, in Int. Symposium on Dynamic Games and Applications, Banff, Canada, June 2010.

[5] ———, *Graph-theoretic approach for connectivity maintenance in mobile networks in the presence of a jammer*, in IEEE Int. Conf. on Decision and Control, Atlanta, USA, December 2010.

[6] A. CARDENAS, S. AMIN, AND S.S. SASTRY, *Secure control: Towards survivable cyber-physical systems*, in Int. Workshop on Cyber-Physical Systems, IEEE, June 2008.

[7] A. CARDENAS, S. AMIN, B. SINOPOLI, A. GIANI, A. PERRIG, AND S.S. SASTRY, *Challenges for securing cyber physical systems*, in Workshop on Future Directions of Cyber-Physical Systems, DHS, July 2009.

[8] B. DEBRUHL AND P. TAGUE, *Digital filter design for jamming mitigation in 802.15.4 communication*, in Int. Conf. on Computer Communications and Networks, 2011, pp. 1–6.

[9] H. SHISHEH FOROUSH AND S. MARTÍNEZ, *On single-input controllable linear systems under periodic DoS jamming attacks*. `http://arxiv.org/abs/1209.4101`.

[10] ———, *On event-triggered control of linear systems under periodic Denial of Service attacks*, in IEEE Int. Conf. on Decision and Control, Maui, HI, USA, December 2012, pp. 2551–2556.

[11] A.G. FRAGKIADAKIS, V.A. SIRIS, AND N. PETROULAKIS, *Anomaly-based intrusion detection algorithms for wireless networks*, in Int. Conf. on Wired/Wireless Intenet Communications, 2010, pp. 192–203.

[12] A. GUPTA, C. LANGBORT, AND T. BASAR, *Optimal control in the presence of an intelligent jammer with limited actions*, in IEEE Int. Conf. on Decision and Control, Atlanta, USA, December 2010, pp. 1096–1101.

[13] A. GUPTA, A. NAYYAR, C. LANGBORT, AND T. BASAR, *A dynamic transmitter-jammer game with asymmetric information*, in IEEE Int. Conf. on Decision and Control, Maui, USA, December 2012, pp. 6477–6482.

[14] J. HESPANHA, P. NAGHSHTABRIZI, AND Y. XU, *A survey of recent results in networked control systems*, Proceedings of IEEE Special Issue on Technology of Networked Control Systems, 95 (2007), pp. 138–162.

[15] L. LI, B. HU, AND M.D. LEMMON, *Resilient event triggered systems with limited communication*, in IEEE Int. Conf. on Decision and Control, Hawaii, USA, December 2012, pp. 6577–6582.

[16] D.G. LUENBERGER, *Canonical forms for linear multivariable systems*, IEEE Transactions on Automatic Control, 12 (1967), pp. 290–293.

[17] M. MAZO, A. ANTA, AND P. TABUADA, *An ISS self-triggered implementation of linear controllers*, Automatica, 46 (2010), pp. 1310–1314.

[18] F. PASQUALETTI, A. BICCHI, AND F. BULLO, *Consensus computation in unreliable networks: A system theoretic approach*, IEEE Transactions on Automatic Control, 57 (2012).

[19] F. PASQUALETTI, R. CARLI, AND F. BULLO, *A distributed method for state estimation and false data detection in power networks*, in IEEE Int. Conf. on Smart Grid Communications, October 2011, pp. 469–474.

[20] R.A. POISEL, *Modern Communication Jamming Principles and Techniques*, Artech, 2004.

[21] S. ROY, C. ELLIS, S. SHIVA, D. DASGUPTA, V. SHANDILYA, AND Q. WU, *A survey of game theory as applied to network security*, in Int. Conf. on Systems Sciences, Hawaii, USA, 2010, pp. 1–10.

[22] S. SUNDARAM AND C.N. HADJICOSTIS., *Distributed function calculation via linear iterations in the presence of malicious agents - parts I, II*, in American Control Conference, June 2008, pp. 1350–1362.

[23] P. TABUADA, *Event-triggered real-time scheduling of stabilizing control tasks*, IEEE Transactions on Automatic Control, 52 (2007), pp. 1680–1685.

[24] G. THEODORAKOPOULOS AND J. S. BARAS, *Game theoretic modeling of malicious users in collaborative networks*, IEEE Journal on Selected Areas in Communications, 7 (2008), pp. 1317–1327.

[25] X. WANG AND M.D. LEMMON, *Self-triggered feedback control systems with finite-gain $\mathcal{L}_2$ stability*, IEEE Transactions on Automatic Control, 54 (2009), pp. 452–467.

[26] W. XU, W. TRAPPE, Y. ZHANG, AND T. WOOD, *The feasibility of launching and detecting jamming attacks in wireless networks*, in ACM International Symposium on Mobile Ad-Hoc Networking & Computing, 2005, pp. 46–57.

[27] M. ZHU AND S. MARTÍNEZ, *Attack-resilient distributed formation control via online adaptation*, in IEEE Int. Conf. on Decision and Control, Orlando, FL, USA, December 2011, pp. 6624–6629.

[28] M. ZHU AND S. MARTÍNEZ, *On distributed constrained formation control in operator-vehicle adversarial networks*, Automatica, (2012). Accepted.