On Event-triggered Control of Linear Systems under Periodic Denial-of-Service Jamming Attacks

Hamed Shisheh Foroush and Sonia Martínez

Abstract— **In this paper we study the resilience of a continuous LTI system which is controlled remotely via a wireless channel. An energy-constrained periodic (partially known) jammer is corrupting the control communication channel by imposing Denial-of-Service (DoS) attacks. We derive a triggering time-sequence, addressing when to update the control signal under the assumption that the period of the jammer has been detected. Then, we show that, under some sufficient condition, this triggering time-sequence counteracts the effect of the jammer and assures asymptotic stability of the plant. We prove our results theoretically, and demonstrate their validity in a simulation example.**

I. Introduction

Novel advances in communications and sensing technologies are allowing the remote control and monitoring of a variety of physical plants, spanning from Unmanned Aerial Vehicles (UAVs) to power reactors. These types of systems integrating computation, communication, and physical processes are called *cyber-physical systems*. Whilst their emergence has come along with many advantages, there are some associated challenges, as well. One of them has to do with *system security*, as vulnerability comes at the price of ease of deployment and hard-to-supervise multiple system components; see [8] and [1].

At the communication level, vulnerabilities can be produced by external communication-signal jammers or attackers. One can distinguish between two types of attacks, namely *Denial-of-Service (DoS)* and *Deceptive* attacks. In the former, the jammer tries to drop the transmitted data, whereas, in the latter, the jammer aims to change the transmitted data, see [26] and [18] for more information. According to [7] and [3], DoS is the most likely type of attack to control systems. Amongst DoS jammers, a simple class is that of *periodic* or *Pulse-Width Modulated (PWM)* jammers. From the point of view of the jammer, periodic signals are motivated by energy constraints and and ease of implementation. It represents a main type of jamming signals studied in the communications literature [9], [4], [24], [11]. Motivated by this, we focus on DoS attacks imposed by PWM jammers whose periodic behavior has already been detected. In particular, we propose an event-triggering control sequence that is compatible with the jammer and study under which conditions the strategy guarantees asymptotic stability.

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

The topic of security in cyber-physical systems is receiving wide attention from the controls community and has been studied from different viewpoints in the last years. In the framework of multiagent systems, we refer the reader to [21], [16], [17]. In these papers, the main problem is the identification of the malicious agent, who is part of the network, and the cancellation of its contribution. In [6] and [5], identification is not the main issue, and the specific objective is how to maintain connectivity of the network, despite the presence of the malicious agents. In [27], the authors develop an attack-resilient method subject to deceptive attacks. Our problem formulation is related to the cited previous work in the sense that we assume the jammer has been detected and we propose an algorithm that aims to counteract its effect.

Other references in the context of secure discrete LTI systems are [10], [3]. In [10], the authors consider deceptive attacks where deception occurs in the observation channel. In [3], the attack is DoS, the problem is formulated in a stochastic setup,and moreover, the attacker obeys an Identically Independent Distributed (IID) assumption, similarly to [20].

The references [2], [12], [23], and [19] model the security problem as a (dynamic) zero-sum non-cooperative game, so they can predict the behvior of the attacker. The authors in [2], [23], and [19] study the vulnerability of the network towards deceptive attacks which differs from our problem. The closest reference to our work is [12], which studies a similar problem in a game-theoretic framework. However, a main limitation of [12] is the restriction to scalar dynamics, while the information structure assumed for the jammer is quite rich which might not be realistic. As usually done in Game Theory, a cost functional is assumed for the attacker, which might not be necessarily the case.

Another important topic when it comes to cyber-physical systems, is that of achieving desired control goals with economic communications. This has motivated the topic of *triggering control*, i.e., control actions triggered only when it is necessary. One can distinguish between related *self-triggered control* and *event-triggered control*; see [22], [15] and [25], which study LTI systems. The technique used in [25] is based on

Input-Output stability analysis, whereas, the technique used in [22] and [15] is based on Input-to-State Stability (ISS) Lyapunov concept, which also inspires this work. However, a main distinguishing feature is the fact that communications may not be always feasible in our formulation.

In this paper, we address the problem of system resilience in the context of event-triggering control. The types of attacks considered are DoS attacks which we assume have been partially identified. Other than this, we consider a generic class of continuous LTI systems and a generic class of PWM jammers. In particular, we propose a novel triggering time-sequence to counteract jammer effects and derive a sufficient condition under which the asymptotic stability is ensured, i.e., the system is *safe and secure*.

The rest of the paper is organized as follows. Section II includes the problem formulation and notations. In Section III, we propose a novel attack-resilient event-triggering law consistent with the jammer signal, and in Section IV, we analyze and prove the validity of this law. We then demonstrate the functionality of our theoretical results in a specific simulation in Section V. We then conclude in Section VI summarizing the results and future work.

II. Problem Formulation

In this section, we state, both formally and informally, the main problem analyzed in the paper.

We consider a remote operator-plant setup, where the operator uses a control channel to send wirelessly a control command to an 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 measure its states continuously.[1]

In this paper, we assume that the type of jammer and the period of the jamming signal has been identified. Future work will be devoted to enlarge the triggering time sequence for identification purposes.

Let $x \in \mathbb{R}^n$ be the state vector and $u \in \mathbb{R}^m$ be the input vector. We consider the following dynamics:

$$\dot{x} = Ax + Bu(t)\,, \tag{1a}$$
$$u(t) = Kx(t_k)\,, \quad \forall t \in [t_k, t_{k+1}[\,, \tag{1b}$$

where A, B and K are matrices of proper dimensions, and $\{t_k\}_{k\geq 1}$ is the triggering time-sequence to be defined later. We denote $e(t) = x(t_k) - x(t), \forall t \in [t_k, t_{k+1}[$.

[1]This information can be obtained by using either local "passive" sensors, e.g., camera network or positioning systems, e.g., GPS, where no communication or cheap and safe communication is required.

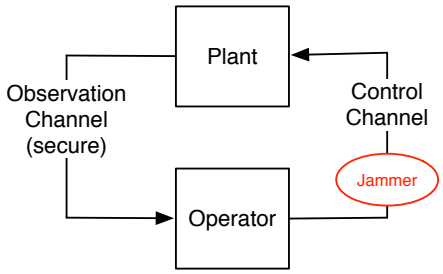

Fig. 1. Problem Architecture

We consider an *energy-constrained*, *periodic* jammer whose signal can be represented as follows:

$$u_{\text{jmd}}(t) = \begin{cases} 1, & (n-1)T \leq t \leq (n-1)T + T_{\text{off}}, \\ 0, & (n-1)T + T_{\text{off}} \leq t \leq nT, \end{cases} \tag{2}$$

where $n \in \mathbb{N}$ is the period number. $T \in \mathbb{R}_{>0}$ and $\mathcal{T} = [0, T]$ is the action-period of the jammer. $T_{\text{off}} \in \mathbb{R}_{>0}$, $T_{\text{off}} < T$ and $\mathcal{T}_{\text{off}} = [0, T_{\text{off}}]$ is the time-period where it is sleeping, so communication is possible. We further denote $T_{\text{on}} \in \mathbb{R}_{>0}$ and $\mathcal{T}_{\text{on}} = [T_{\text{on}}, T]$ to be the time-period where the jammer is active, thus no data can be sent. It is also worth mentioning that the parameter $T_{\text{off}} \in \mathbb{R}$ need not be time-invariant which recalls Pulse-Width Modulated (PWM) jamming. At last, we denote by $T_{\text{off}}^{\text{cr}}$ a uniform lower-bound for T_{off}, i.e., $T_{\text{off}}^{\text{cr}} \leq T_{\text{off}}$ which we assume holds for all the periods and we have identified as well.

Putting these pieces together, we study the following problem:

> *[Problem formulation]*: Knowing T and $T_{\text{off}}^{\text{cr}} \leq T_{\text{off}}$, uniformly for all the periods, determine an event-triggering strategy for the operator that is sufficient for system stabilization despite the presence of the jammer.

III. Attack-resilient event-triggered strategy

In this section, we introduce an event-triggered strategy which is resilient towards the jamming attack. To do so, we make use of the ISS approach of [22] and [15].

Here, we assume that: (i) the system (1a) is open-loop unstable, and (ii) the pair (A, B) is controllable. The latter guarantees that there exists matrix K such that $A + BK$ is Hurwitz. This implies that for every matrix $Q = Q^T \succ 0$, there exists a unique matrix $P = P^T \succ 0$ such that the Lyapunov equation:

$$(A + BK)^T P + P(A + BK) = -Q\,, \tag{3}$$

holds [13]. Given Q, we consider the Lyapunov function $V(x) = x^T P x$. Note that $V(t) = V(x(t)) = x(t)^T P x(t)$, so interchangeably, we shall use $V(x)$ or $V(t)$. Since Q and P are symmetric, positive-definite

matrices, then by applying the Cholesky decomposition, we can express them as $Q = L^T L$ and $P = U^T U$, for some $L, U \in \mathbb{R}^{n\times n}$. We also denote by $\|.\|$ and $|.|$, the Euclidean matrix and vector norms, respectively.

We introduce our ISS-Lyapunov function in the following result.

Proposition 3.1: Consider the system (1a), where (3) holds. Let $V(x) = x^T P x$ be the Lyapunov function. If $\|Q\| > 1$, then the following holds:

$$\theta_1 |x|^2 \leq V(x) \leq \theta_2 |x|^2 , \quad (4)$$

$$\dot{V}(x) \leq -(\|Q\| - 1)|x|^2 + \|PBK\|^2 |e|^2 , \quad (5)$$

where $\theta_1, \theta_2 \in \mathbb{R}_{>0}$. In other words, V is an ISS-Lyapunov function for (1a).

Proof: We can lower- and upper-bound $V(x)$ as follows:

$$\lambda_{\min}(P)|x|^2 \leq V(x) \leq \lambda_{\max}(P)|x|^2 ,$$

where $\lambda_{\min}$ and $\lambda_{\max}$, are the minimum and maximum eigenvalues of P, respectively. Since $P = P^T \succ 0$, then (4) holds with $\theta_1 \triangleq \lambda_{\min} > 0$ and $\theta_2 \triangleq \lambda_{\max} > 0$.

Let $\bar{A} = A + BK$ and $\bar{B} = BK$. By computing the temporal-derivative of V and incorporating the dynamics (1a), we obtain:

$$\dot{V}(x) = x^T \left(\bar{A}^T P + P\bar{A}\right) x + e^T \bar{B}^T P x + x^T P \bar{B} e .$$

Recalling the following inequality:

$$x^T P \bar{B} e + e^T \bar{B}^T P x \leq x^T x + e^T \bar{B}^T P P \bar{B} e ,$$

we can upper-bound $\dot{V}$ as:

$$\dot{V}(x) \leq x^T(\bar{A}^T P + P\bar{A})x + x^T x + e^T \bar{B}^T P P \bar{B} e . \quad (6)$$

Using (3) and the Cholesky decomposition for Q, i.e., $Q = L^T L$, we get:

$$\dot{V}(x) \leq -(Lx)^T(Lx) + (Ix)^T(Ix) + (P\bar{B}e)^T(P\bar{B}e) .$$

Then, recalling $\|L\|^2 = \|Q\| > 1$, the latter inequality yields (5). ■

Similarly to [22],one can use the ISS-Lyapunov function of Proposition 3.1, together with a design parameter $\sigma \in (0, 1)$, to determine a stabilizing event-triggering law as when the jammer is absent:

Proposition 3.2: Consider the system (1a), along with the Lyapunov function $V(x) = x^T P x$ associated with $\|Q\| > 1$. If the control (1b) is updated at times t_k governed by the following triggering law:

$$|e(t_k)|^2 = \sigma \frac{\|Q\| - 1}{\|PBK\|^2} |x(t_k)|^2 , \quad k \geq 1 , \quad (7)$$

then the system is asymptotically stable.

Proof: In order to ensure asymptotic stability, it is sufficient to impose the following constraint on (5):

$$\dot{V}(x) \leq -(\|Q\| - 1)|x|^2 + \|PBK\|^2 |e|^2 < 0 ,$$

which implies:

$$\|PBK\|^2 |e|^2 < (\|Q\| - 1)|x|^2 . \quad (8)$$

Note that in (8), and without loss of generality, we can introduce design parameter $\sigma \in (0, 1)$:

$$\|PBK\|^2 |e|^2 \leq \sigma(\|Q\| - 1)|x|^2 < (\|Q\| - 1)|x|^2 , \quad (9)$$

which still renders the system asymptotically stable. Let t_1 be the first time that (9) is violated. Hence, we obtain the following:

$$|e(t_1)|^2 = \sigma \frac{\|Q\| - 1}{\|PBK\|^2} |x(t_1)|^2 .$$

By updating the control at t_1, we get $e(t_1) = x(t_1) - x(t_1) = 0$ and $\dot{V}(t_1) < 0$. Moreover, for $t > t_1$, the error $e(t)$ evolves with time and increasing from t_1. As long as (9) is not violated, i.e., (7) does not hold, we have $\dot{V}(t) < 0$, by construction. Now, let t_2 be the next time when (7) holds. Note that, again, $e(t_2) = x(t_2) - x(t_2) = 0$ and $\dot{V}(t_2) < 0$. Therefore, it follows by induction that by the definition of the triggering sequence according to (7), $\dot{V}(t) < 0$, $\forall t$. A standard Lyapunov argument guarantees the result follows. ■

In what follows, we shall study the asymptotic stability of the system despite jammer presence under a simple modification of the above triggering law. In what follows, we assume that the jammer is imposing a *"worst-case jamming scenario"*, i.e., $T_{\text{off}} = T_{\text{off}}^{\text{cr}}$.

Definition 3.3: We define the triggering time-sequence despite jammer presence as follows:

$$t_{k,n}^* = \left\{ t_l \text{ satisfying (7)} \middle| t_l \in [(n-1)T, (n-1)T + T_{\text{off}}^{\text{cr}}] \right\} \cup \{nT\} , \quad (10)$$

$\forall k \in \mathbb{N}$, $\forall n \in \mathbb{N}$. In (10), k denotes the number of triggering times occurring in n^{th} jammer action-period.

In order to interpret the triggering law (10), let us consider the n^{th} action-period, i.e., $t \in [(n-1)T, nT]$; Then, we shall take the time-instants given by (7) which also lie in the $[(n-1)T, (n-1)T + T_{\text{off}}^{\text{cr}}]$ time-period along with nT. In this way, if ever it happens that:

$$\left\{ t_l \text{ satisfying (7)} \middle| t_l \in [(n-1)T, (n-1)T + T_{\text{off}}^{\text{cr}}] \right\} = \emptyset ,$$

then the only triggering instant would be nT.

Remark 3.4: In the triggering law (10), the following holds:

$$\exists \tau > 0, \text{ such that } t_{k+1,n}^* - t_{k,n}^* \geq \tau, \forall k \in \mathbb{N} .$$

This is based on Theorem III.1, presented in [22]. In other words, the time sequence generated by the triggering law (10) does not accumulate. This is an important observation used in our analysis.

IV. Analysis of the proposed triggering law

Having introduced the triggering law (10), we present our main result in this section which studies the asymptotic stability of the system under attack.

In [14], the author proves the following bound for a matrix $M \in \mathbb{R}^{n\times n}$:

$$\|\exp(M)\| \leq \exp(\mu(M))\,, \tag{11}$$

where the μ-operator is defined as follows:

$$\mu(M) = \max\left\{\mu \,|\, \mu \in \lambda\left(\frac{M+M^T}{2}\right)\right\}\,.$$

We shall exploit this bound in the proof of our main result.

Theorem 4.1: Consider the system (1a), along with the triggering law (10). The system is asymptotically stable if the following conditions are satisfied:

$$\frac{(1-\sigma)T_{\text{off}}^{\text{cr}}(\|Q\|-1)}{2} > \|P\|\ln(\alpha)\,, \tag{12}$$

where,

$$\begin{aligned}\alpha \triangleq \exp((T-T_{\text{off}}^{\text{cr}})\mu(A+BK)) + \frac{\|BK\|}{\mu(A+BK)}\times\\ \left(\frac{\|BK\|}{\|A\|}+1\right)(1-\exp((T-T_{\text{off}}^{\text{cr}})\|A\|))\times\\ (1-\exp((T-T_{\text{off}}^{\text{cr}})\mu(A+BK)))\,,\end{aligned} \tag{13}$$

and,

$$\mu(A+BK) < 0\,. \tag{14}$$

Proof: We shall focus on the first jammer action-period, i.e., $0 \leq t \leq T$. We then show that under the proposed sufficient condition, it holds that $V(T) < V(0)$, which can be inductively extended to show $V((n+1)T) < V(nT), \quad \forall n \in \mathbb{N}$. From here asymptotic stability can be guaranteed. For the sake of brevity, we drop $n=1$ in the $t_{k,n}^*$ annotation. Without loss of generality, let $\{t_1^*=0, t_2^*, t_3^*, \ldots, t_m^*\}$ be the time-sequence generated by the triggering law (10), where it holds that $t_m^* \leq T_{\text{off}}^{\text{cr}}$ and $t_{m+1}^* > T_{\text{off}}^{\text{cr}}$. We note that there must exist such an $m > 0$, since according to Remark 3.4, this time-sequence does not accumulate.

We consider the evolution of the Lyapunov function in the time-interval $\left[t_i^*, t_{i+1}^*\right]$, where $0 \leq t_i^*, t_{i+1}^* \leq t_m^*$. According to (10), in this interval, Equation (7) is not yet violated, hence the following holds:

$$|e(t)|^2 < \sigma\frac{\|Q\|-1}{\|PBK\|^2}\,|x(t)|^2\,.$$

Upper-bounding (5), by using the latter Equation, yields:

$$\dot{V}(t) < -(1-\sigma)\,(\|Q\|-1)\,|x(t)|^2\,. \tag{15}$$

Now, we note that:

$$V = x^TPx \Rightarrow V \leq \|U\|^2\,|x|^2 \Rightarrow -|x(t)|^2 \leq -\frac{V(t)}{\|U\|^2}\,,$$

with which we can further upper-bound Equation (15) as follows:

$$\dot{V}(t) < -\frac{(1-\sigma)\,(\|Q\|-1)}{\|U\|^2}V(t)\,. \tag{16}$$

By applying the comparison principle on (16), we get:

$$V(t) < V(t_i^*)\exp\left(-\frac{(1-\sigma)\,(\|Q\|-1)}{\|U\|^2}(t-t_i^*)\right), \tag{17}$$

$\forall t \in [t_i^*, t_{i+1}^*]$. Using (17) in an inductive way, we can express the evolution of Lyapunov function for the time-interval $[0, t_m^*]$, as follows:

$$V(t_m^*) < V(0)\prod_{i=1}^{m-1}\exp\left(-\frac{(1-\sigma)\,(\|Q\|-1)}{\|U\|^2}(t_{i+1}^*-t_i^*)\right).$$

We note that, $t_m^* = \sum_{i=1}^{m-1}(t_{i+1}^*-t_i^*)$, so the latter equation yields:

$$V(t_m^*) < V(0)\exp\left(-\frac{(1-\sigma)\,(\|Q\|-1)}{\|U\|^2}t_m^*\right). \tag{18}$$

At this stage, note that, according to the triggering law (10), the control cannot be updated within the time-interval $[t_m^*, T]$. A sufficient condition for asymptotic stability is given by $V(T) < V(0)$. In order for this to hold, we firstly develop some estimate for $x(T)$.

We recall the dynamics (1a), which given the above explanations and notations, can be written under either:

$$\begin{cases}\dot{x}(t) &= Ax(t) + BKx(t_m^*)\,,\\ x(t_m^*) &= x_0\,,\end{cases} \tag{19}$$

or:

$$\begin{cases}\dot{x}(t) &= (A+BK)\,x(t) + BKe(t)\,,\\ x(t_m^*) &= x_0\,,\end{cases} \tag{20}$$

form. Let us consider (20), whose explicit solution evaluated at $t=T$ is given by:

$$\begin{aligned}x(T) = &\exp\left((T-t_m^*)(A+BK)\right)x(t_m^*) +\\ &\int_{t_m^*}^{T}\exp\left((T-s)(A+BK)\right)BKe(s)ds\,.\end{aligned} \tag{21}$$

By applying the triangular-inequality on (21), we find the following bound:

$$\begin{aligned}|x(T)| \leq &|\exp\left((T-t_m^*)(A+BK)\right)|\,|x(t_m^*)| +\\ &\left|\int_{t_m^*}^{T}\exp\left((T-s)(A+BK)\right)BKe(s)ds\right|\,.\end{aligned} \tag{22}$$

Based on (11), Equation (22) can be further bounded, which gives the following:

$$|x(T)| \leq \exp\left((T-t_m^*)\mu(A+BK)\right)|x(t_m^*)| + \int_{t_m^*}^{T} \exp\left((T-s)\mu(A+BK)\right)\|BK\|\,|e(s)|\,ds\,. \tag{23}$$

Applying the sup-operator on (23), yields:

$$|x(T)| \leq \exp\left((T-t_m^*)\mu(A+BK)\right)|x(t_m^*)| + \sup_{s\in[t_m^*,T]}|e(s)|\,\|BK\|\int_{t_m^*}^{T}\exp\left((T-s)\mu(A+BK)\right)ds\,. \tag{24}$$

We can solve the integral term in (24) which gives the following bound:

$$|x(T)| \leq \exp\left((T-t_m^*)\mu(A+BK)\right)|x(t_m^*)| - \frac{\sup_{s\in[t_m^*,T]}|e(s)|\,\|BK\|}{\mu(A+BK)}\times \left(1-\exp\left((T-t_m^*)\mu(A+BK)\right)\right). \tag{25}$$

In order to further progress in our analysis, we need to find an appropriate bound for $\sup_{s\in[t_m^*,T]}|e(s)|$. This is done in the following claim.

Claim 4.2: Consider (25), $\sup_{s\in[t_m^*,T]}|e(s)|$ satisfies the following:

$$\sup_{s\in[t_m^*,T]}|e(s)| \leq -|x(t_m^*)|\left(1+\frac{\|BK\|}{\|A\|}\right)\times \left(1-\exp\left((T-t_m^*)\,\|A\|\right)\right). \tag{26}$$

Proof of Claim 4.2: First, we recall from our notations that $e(s) = x(t_m^*) - x(s)$, which yields:

$$|e(s)| = |x(s) - x(t_m^*)|\,. \tag{27}$$

Now, consider the dynamics (19), we then find an explicit expression for (27):

$$|e(s)| = |x(s)-x(t_m^*)| = |\exp\left((s-t_m^*)A\right)x(t_m^*) - x(t_m^*) + \int_{t_m^*}^{s}\exp\left((s-s')A\right)BKx(t_m^*)ds'|\,.$$

The latter equation can be bounded, by exploiting the triangular inequality, which then results into the following (several algebraic steps are skipped, for the sake of brevity):

$$|e(s)| \leq \|\exp\left((s-t_m^*)A\right)-I\|\,|x(t_m^*)| + \frac{\|BK\|\,|x(t_m^*)|}{\|A\|}\left(\exp\left((s-t_m^*)\,\|A\|\right)-1\right). \tag{28}$$

In (28), we note that the following holds, recalling definition of exponential-matrix and for some $x\in\mathbb{R}^{n\times n}$ for which $|x|=1$:

$$|(\exp\left((s-t_m^*)A\right)-I)x| = \left|\sum_{k=1}^{\infty}\frac{((s-t_m^*)A)^k}{k!}x\right| \tag{29}$$

$$\leq \sum_{k=1}^{\infty}\left|\frac{((s-t_m^*)A)^k}{k!}\right||x| \leq \sum_{k=1}^{\infty}\frac{|s-t_m^*|\,\|A\|^k}{k!}\,|x| \tag{30}$$

$$= \sum_{k=1}^{\infty}\frac{|s-t_m^*|\,\|A\|^k}{k!} = \exp((s-t_m^*)\|A\|)-1\,.$$

Therefore, by definition of the 2-norm of a matrix, we can say $\|\exp\left((s-t_m^*)A\right)-I\| \leq \exp((s-t_m^*)\|A\|)-1$. So, by bounding (28), with this expression, we get:

$$|e(s)| \leq \left(\exp\left((s-t_m^*)\,\|A\|\right)-1\right)|x(t_m^*)| + \frac{\|BK\|\,|x(t_m^*)|}{\|A\|}\left(\exp\left((s-t_m^*)\,\|A\|\right)-1\right).$$

By applying the sup operator on the latter inequality, we obtain:

$$\sup_{s\in[t_m^*,T]}|e(s)| \leq \sup_{s\in[t_m^*,T]}\left(\exp\left((s-t_m^*)\,\|A\|\right)-1\right)|x(t_m^*)| + \frac{\|BK\|\,|x(t_m^*)|}{\|A\|}\times \sup_{s\in[t_m^*,T]}\left(\exp\left((s-t_m^*)\,\|A\|\right)-1\right).$$

In this equation, we note that $\|A\|>0$, as $A\neq 0$. So, we can compute the sup's, appearing on its RHS, to get:

$$\sup_{s\in[t_m^*,T]}|e(s)| \leq \left(\exp\left((T-t_m^*)\,\|A\|\right)-1\right)|x(t_m^*)| + \frac{\|BK\|\,|x(t_m^*)|}{\|A\|}\left(\exp\left((T-t_m^*)\,\|A\|\right)-1\right). \tag{31}$$

Performing some simplifications on (31), we obtain (26), which then completes the proof of this claim. •

Now, we plug (26) into (25) which then by some simplifications yields:

$$|x(T)| \leq \alpha'\,|x(t_m^*)|\,, \tag{32}$$

where the parameter α' is defined as follows:

$$\alpha' \triangleq \exp((T-t_m^*)\mu(A+BK)) + \frac{\|BK\|}{\mu(A+BK)}\times \left(\frac{\|BK\|}{\|A\|}+1\right)\left(1-\exp((T-t_m^*)\,\|A\|)\right)\times \left(1-\exp((T-t_m^*)\mu(A+BK))\right). \tag{33}$$

It is worth to note that comparing the parameters α and α', introduced in (13) and (33), respectively, it holds that $\alpha' \leq \alpha$, which is because $t_m^* \leq T_{\text{off}}^{\text{cr}}$ and $\mu(A+BK) < 0$, by assumption. According to this observation, Equation (32) can be written as:

$$|x(T)| \leq \alpha\,|x(t_m^*)|\,. \tag{34}$$

The value of the Lyapunov function at $t = T$, can be estimated as follows:

$$V(T) = x(T)^T P x(T) \leq \|U\|^2 |x(T)|^2 , \tag{35}$$

which then according to (34), can be further bounded:

$$V(T) \leq \alpha^2 \|U\|^2 |x(t_m^*)|^2 . \tag{36}$$

Besides, let us define the parameter γ to be:

$$\gamma \triangleq -\frac{(1-\sigma)(\|Q\|-1)}{\|U\|^2} , \tag{37}$$

where we note that $\gamma < 0$, based on the assumption of this theorem. Then, we can rewrite (18) as in:

$$V(t_m^*) < \exp(\gamma t_m^*) V(0) . \tag{38}$$

We note that as $\gamma < 0$ and $t_m^* \leq T_{\text{off}}^{\text{cr}}$, we obtain that $\exp(\gamma T_{\text{off}}^{\text{cr}}) V(0) \leq \exp(\gamma t_m^*) V(0)$, based on this inequality, we can impose the following bound on (38):

$$V(t_m^*) < \exp(\gamma T_{\text{off}}^{\text{cr}}) V(0) \leq \exp(\gamma t_m^*) V(0) . \tag{39}$$

Now, along the same reasoning for (35), we note that $V(t_m^*) \leq \|U\|^2 |x(t_m^*)|^2$. A conservative bound can be imposed as follows:

$$V(t_m^*) \leq \|U\|^2 |x(t_m^*)|^2 < \exp(\gamma T_{\text{off}}^{\text{cr}}) V(0) . \tag{40}$$

Applying bound (40) on (36), we obtain:

$$V(T) < \alpha^2 \exp(\gamma T_{\text{off}}^{\text{cr}}) V(0) . \tag{41}$$

Hence, according to (41), the following holds:

$$\alpha^2 \exp(\gamma T_{\text{off}}^{\text{cr}}) < 1 \Longleftrightarrow V(T) < V(0) .$$

Therefore, a sufficient condition for maintaining the asymptotic stability is given in the following:

$$\alpha^2 \exp(\gamma T_{\text{off}}^{\text{cr}}) < 1 . \tag{42}$$

Now, we recall the definition of parameter γ, presented in (37). Also, we note that $\|U\|^2 = \|P\|$, plus given that $\exp$ is a monotonically increasing function, we can rewrite (42) in the form of (12). This, hence, completes the proof. ■

Remark 4.3: The result provided in the Theorem 4.1 can be interpreted as a feasibility problem. So, in other words, for a given system in the form (1a), one has to find proper desing parameters K, P, Q, and $\sigma \in (0,1)$ such that the following constraints would be satisfied:

$$(A+BK)\text{: Hurwitz} , \tag{43a}$$

$$(A+BK)^T P + P(A+BK) = -Q , \tag{43b}$$

$$\frac{(1-\sigma) T_{\text{off}}^{\text{cr}} (\|Q\|-1)}{2} > \|P\| \ln(\alpha) , \tag{43c}$$

$$\mu(A+BK) < 0 . \tag{43d}$$

We note that, e.g., if $T_{\text{off}}^{\text{cr}} = T$, i.e., the jammer is not malicious at all, then $\alpha = 1$ and so the constraint (43c) holds for free. The same will be true for $T_{\text{off}}^{\text{cr}} \approx T$. Note additionally, that more relaxed sufficient conditions for stability can be obtained by imposing $V(knT) \leq V((n-1)T)$ for some $k > 1$ and all $n \in \mathbb{N}$.

V. Simulation

In Section III, we have developed a triggering time-sequence and in Section IV proved that under some sufficient conditions, the system under attack is asymptotically stable. In this section, we shall show the validity of these theoretical results on an academic example.

Let us consider the following system:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1.5 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} 0 \\ 0.1 \end{bmatrix} u , \tag{44}$$

where $u \in \mathbb{R}$. We note that, for this system, (A, B) is a controllable pair. In addition, it is an open-loop unstable system, provided that eigenvalues of A have positive real-part. We pick the control gain:

$$K = \begin{bmatrix} -1 & 1.5 \end{bmatrix} ,$$

which renders the matrix $A + BK$ Hurwitz. Then, we consider the matrix:

$$Q = \begin{bmatrix} \frac{1}{2} & \frac{1}{4} \\ \frac{1}{4} & \frac{3}{2} \end{bmatrix} .$$

We note that $Q = Q^T \succ 0$, and that $\|Q\| > 1$. Given these matrices, Lyapunov equation (3) gives us:

$$P = \begin{bmatrix} 1.135 & -0.25 \\ -0.25 & 1.353 \end{bmatrix} .$$

We consider the jammer, imposing signal $u_{\text{jmd}}(t)$, where $T = 1$ and $T_{\text{off}}^{\text{cr}} = 0.4$.

We then refer to the Theorem 4.1. One can compute that: $\alpha = 1.075$, $\|P\| = 1.5166$ and $\|Q\| = 1.559$. Thus, the condition (12) would be translated into:

$$0.118(1-\sigma) > 0.1098 \Longrightarrow \sigma < 0.0182 .$$

It infers that the allowable range for the design parameter is $\sigma \in (0, 0.0182)$. To realize, at this point, all the assumptions of this theorem are satisfied, therefore, we expect that the triggering time-sequence (10) render the system asymptotically stable.

The temporal evolution of the states is shown in Figure 2. We can see that the control policy, along with triggering time-sequence has counteracted the effect of jamming attacks.

In order to further demonstrate the triggering time-sequence, we have drawn the temporal evolution of $|e(t)|^2$ and $\frac{\sigma(\|Q\|-1)}{\|PBK\|^2} |x(t)|^2$ in Figure 3. For the sake of clarity, we have zoomed on the first four periods. According to this figure, we note, e.g., that in the time-interval $t \in \left(T_{\text{off}}^{\text{cr}}, T\right)$, where the communication is not feasible, the error grows in an unbounded fashion. This effect, however, is compensated for in the next period by triggering more often.

The other interesting observation out of our simulation is explained here. While preserving matrices P and Q, for $T_{\text{off}}^{\text{cr}} \leq 0.394$, there is no feasible σ. This is to note

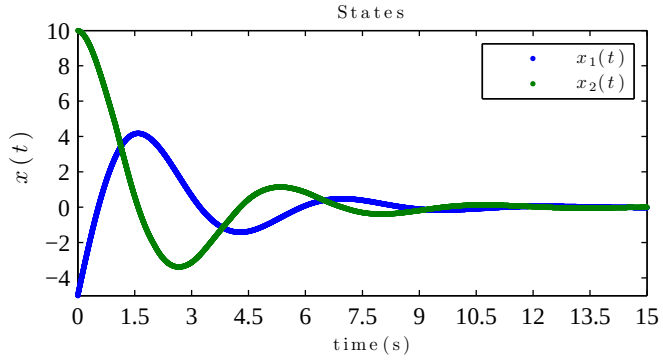

Fig. 2. Temporal evolution of the states

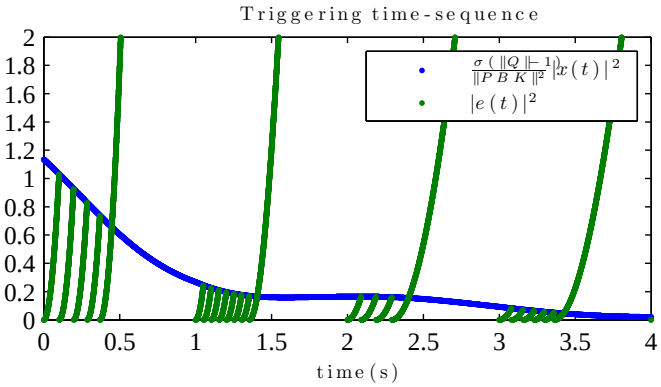

Fig. 3. Temporal evolution of the triggering condition, zoomed over the first four periods

that for these *more malicious* attackers, we cannot have a feasible controller. A solution would be to tune matrices P and Q which has not been studied in this simulation.

VI. Conclusions and Future Work

We have considered a plant-jammer-operator setup, where the control communication channel (from the operator to the plant) is corrupted by a periodic jammer. For the benefit of maintaining less communication, we have adapted an event-triggering time-sequence to restrict communications when necessary. We have then shown, theoretically and in simulation, that this triggering time-sequence is capable of counteracting the jammer attack and also rendering the system asymptotically stable under some conditions.

As is explained in the manuscript, we assume the jammer has been identified to the extent that it is periodic and its characteristic parameters are known by the operator. We are currently working on extending our triggering strategy on two fronts: (i) allow for more events so that learning and identification of the jammer is possible, and (ii) exploiting the controllability properties of the linear system to beat a wider class of periodic jammers. In the future we would like to consider more malicious jammer classes.

References

[1] N. Adams. Workshop on future directions in cyber-physical systems security. Technical report, workshop organized by Department of Homeland Security (DHS), 2010.

[2] T. Alpcan and T. Basar. *Network Security: A Decision And Game Theoretic Approach*. Cambridge University Press, 2011.

[3] S. Amin, A. Cardenas, and S. S. Sastry. Safe and secure networked control systems under denial-of-service attacks. In *Hybrid Systems: Computation and Control*, pages 31–45, 2009.

[4] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa. On the performance of IEEE 802.11 under jamming. In *Proceedings of IEEE Infocom. 08*, pages 1265 –1274, 2008.

[5] S. Bhattacharya and T. Basar. Differential game-theoretic approach to a spatial jamming problem. In *Proceedings of 14th International Symposium on Dynamic Games and Applications*, Banff, Canada, June 2010.

[6] S. Bhattacharya and T. Basar. Graph-theoretic approach for connectivity maintenance in mobile networks in the presence of a jammer. In *IEEE Conf. on Decision and Control*, Atlanta, USA, December 2010.

[7] E. Byres and J. Lowe. The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Congress, VDE Association for Electrical Electronics and Information Technologies*, 2004.

[8] 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 in Cyber-physical Systems Security*. DHS, July 2009.

[9] B. DeBruhl and P. Tague. Digital filter design for jamming mitigation in 802.15.4 communication. In *Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN), 2011*, pages 1 –6, 2011.

[10] H. Fawzi, P. Tabuada, and S. Diggavi. Secure state-estimation for dynamical systems under active adversaries. In *Proceedings of 49th Annual Allerton Conference on Communication, Control, and Computing*, 2011.

[11] A. G. Fragkiadakis, V. A. Siris, and N. Petroulakis. Anomaly-based intrusion detection algorithms for wireless networks. In *WWIC*, pages 192–203, 2010.

[12] A. Gupta, C. Langbort, and T. Basar. Optimal control in the presence of an intelligient jammer with limited actions. In *IEEE Conf. on Decision and Control*, pages 1096–1101, Atlanta, USA, December 2010.

[13] H. K. Khalil. *Nonlinear Systems*. Prentice Hall, 3 edition, 2002.

[14] C. V. Loan. The sensitivity of the matrix exponential. *SIAM Journal of Numerical Analysis*, 14(6):971–981, 1977.

[15] M. Mazo, A. Anta, and P. Tabuada. An iss self-triggered implementation of linear controllers. *Automatica*, 46(8):1310 – 1314, 2010.

[16] F. Pasqualetti, A. Bicchi, and F. Bullo. Consensus computation in unreliable networks: A system theoretic approach. *IEEE Transactions on Automatic Control*, to appear, 2011.

[17] F. Pasqualetti, R. Carli, and F. Bullo. Distributed estimation and false data detection with application to power networks. *Automatica*. submitted.

[18] R.A. Poisel. *Modern Communication Jamming Principles and Techniques*. Artech, 2004.

[19] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu. A survey of game theory as applied to network security. In *Proceedings of the 43rd Hawaii International Conference on System Sciences*, pages 1–10, Hawaii, USA, 2010.

[20] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry. Foundations of control and estimation over lossy networks. *Proceddings of IEEE Special Issue on Technology of Networked Control Systems*, 95(1):163–187, 2007.

[21] 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*, pages 1350–1362, June 2008.

[22] P. Tabuada. Event-triggered real-time scheduling of stabilizing control tasks. *IEEE Transactions on Automatic Control*, 52(9):1680–1685, 2007.

[23] G. Theodorakopoulos and J. S. Baras. Game theoretic modeling of malicious users in collaborative networks. *IEEE Journal on Selected Areas in Communications*, 7:1317–1327, 2008.

[24] D. Thuente and M. Acharya. Intelligent jamming in wireless networks with applications to 802.11b and other networks. In *Milcom*, 2006.

[25] X. Wang and M. Lemmon. Self-triggered feedback control systems with finite-gain l2 stability. *TAC*, 54(3):452 – 467, 2009.

[26] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, MobiHoc '05, pages 46–57, 2005.

[27] M. Zhu and S. Martínez. Attack-resilient distributed formation control via online adaptation. In *IEEE Conf. on Decision and Control*, Orlando, USA, December 2011.