IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 23, 2022, accepted March 22, 2022, date of publication April 4, 2022, date of current version April 18, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3164424

On the Stability of Cyber-Physical Control Systems With Sensor Multiplicative Attacks

LUIS FRANCISCO CÓMBITA[1], (Member, IEEE), NICANOR QUIJANO[2], (Senior Member, IEEE), AND ÁLVARO A. CÁRDENAS [3], (Member, IEEE)

[1]Facultad de Ingeniería, Universidad Distrital Francisco José de Caldas, Bogotá 110231, Colombia
[2]Departamento de Ingeniería Eléctrica y Electrónica, Universidad de Los Andes, Bogotá 111711, Colombia
[3]Department of Electrical and Computer Engineering, University of California at Santa Cruz, Santa Cruz, CA 95064, USA

Corresponding author: Luis Francisco Cómbita (lfcombita@udistrital.edu.co)

This work was supported in part by the Comisión de Estudios (015 de 2014) funded by the Universidad Distrital Francisco José de Caldas, in part by the Convocatoria 727 Doctorados Nacionales 2015 by Colciencias, and in part by the Air Force Office of Scientific Research under Award FA9550-19-1-0014.

ABSTRACT To understand the impact of cyber-attacks to sensors in control systems, we present a stability analysis of a wide range of systems in this paper. Based on Lyapunov stability analysis, we formulate an optimization problem with constraints in the form of a set of linear matrix inequalities to find conservative bounds of stability related to the attacks, which can be analyzed simultaneously or one at the time. When considering the attacks one at the time, with the proposed formulation, we can find the most vulnerable output in the system, which can help the designer (i.e., the defender) to understand how to make the system more secure in case of multiplicative attacks on sensors. We show the effectiveness of our analysis with simulations based on the three tanks benchmark system.

INDEX TERMS Stability, cyber-attacks, industrial cyber-physical systems, safety, vulnerability analysis.

I. INTRODUCTION

Cyber-physical control systems are control systems of physical systems in which sensors, actuators, and controllers are working on a network through a communication infrastructure. These systems have some advantages as reduced system wiring, low installation and maintenance costs, and increased flexibility and adaption capability [1]. Cyber-attacks on control systems have been received attention from both the information technology community, and most recently, the control community, given that once the attacker accomplishes the goal of hacking the network, the system needs to be able to react (or, at least, that is what is expected). In fact, from the control systems community, there are some very recent surveys in cyber-physical systems (CPS) security [2]–[5].

Cyber-attack detection is a subject that has received great interest recently, from two points of view: i) information security; and ii) secure control (see [2], [3], [6] and related references therein). Information security point of view focuses on IT-related aspects, such as access control, authentication, and message integrity. From the point of view of secure control methods, the focus lies on the physical part of the CPSs and use control systems techniques. Some strategies in this field include Bayesian detection with binary hypothesis, weighted least squares approaches, χ^2-detectors based on Kalman filters, and quasi-fault detection and isolation (FDI) techniques.

Those detection strategies deal with two main kinds of attacks: denial of service (DoS), and false data injection, or deception, attacks. Many efforts have been done towards the detection of deception attacks such as cover, replay, and zero-dynamics attacks [7]. Also, very closely related to detection, there have been many works showing the design of optimal stealthy deception attacks that exploit the weakness of systems. It is commonly accepted, that cybersecurity techniques are more mature than secure control but an interesting approach to explore is the simultaneous use of tools from the two above-mentioned approaches, e.g., a better security strategy could include encryption as well as a mitigation mechanism.

Over the last few years, the problem of secure state estimation, i.e., the capability of reconstructing the state even when the CPS of interest is under deception attacks, has gained considerable attention [8]–[10]. These works assume

The associate editor coordinating the review of this manuscript and approving it for publication was Min Wang.

that there are an unknown but bounded number of false-data injection on the outputs sensors. In these works, the authors give a characterization of the maximum number of attacks that can be detected and corrected in order to reconstruct the state of the system. In [8] the authors also give the conditions under which the state cannot be reconstructed. For this work, the authors assume that the set of attacked nodes remain unchanged over time i.e., the set of measurements and/or control inputs under attack are time-invariant. This last assumption is relaxed in [10], where the set of attacked nodes can change over time. The practical implementation of these approaches is reinforced in [10] with the inclusion of a Kalman filter. The aforementioned works show that the state reconstruction can be done successfully although a number of sensors are under attack. A recent survey on this subject is presented in [11].

Some features are examined for securing industrial control systems. In [12] and the references therein, the authors show that controllability, observability and operability are the most important features to analyze the security of an industrial control system. However, stability analysis are very critical in the evaluation of the safety of a control system. Some attacks could be focused on modifying the control system behavior, up to make the system unstable. Stability is perhaps the most important property of control systems, since it allows the system to have a desired performance regarding robustness, resilience, and security. However, the stability implications of cyber-attacks have not received as much attention as expected, being such an important characteristic. Most of the efforts have been directed to power systems applications, e.g., works dealing with transient stability [13], or attacks effects in isolated power systems [14]. Something more general has been done related to stability implications of denial of service (DoS) attacks, and some other attacks types in [7]. Mainly, the synthesis of new resilient controllers based on a series of techniques guarantees stability as part of the process, but not many authors have been interested in what happens to legacy cyber-physical control systems under attacks. However, in a recent work [15], the authors define some metrics to quantify the cyber-resilience level based on the design, structure, stability, and performance under the attack of a given CPS. The metrics provide reference points to evaluate whether the system is better prepared or not to face the adversaries. Therefore, it is possible to quantify the ability to recover from an adversary using its mathematical model based on actuators saturation. The evaluation of the security in an industrial control system includes vulnerability analysis to false data injection attacks, identification of potential attacks, and the development of mechanisms that increase the difficulty to launch such an attack and to reduce and limit their effects [16].

Some recent work on the design of resilient controllers includes careful stability analysis together with the respective design of the control law. In [17] the stochastic finite-time stability criteria for a networked closed-loop control system is analyzed with the utilization of a mode-dependent piecewise Lyapunov-Krasovskii functional. In there, a finite-time control law is exposed while special attention is put in guaranteeing that, for a given fixed-time period, the system trajectories are expected to avoid exceeding a given physical threshold. Another networked control strategy is investigated in [18]. In this work, the Lyapunov and convex optimization theories are utilized to develop a class of discrete-time Takagi-Sugeno fuzzy networked singularly perturbed systems via an observer-based technique. An attack-resilient adaptive control law for networked control systems is explored in [19]. The control law in this work focuses on a design that ensures the stability and boundedness of the Markovian jumped systems with time-varying and time-invariant attacks. Additive and multiplicative attacks on both sensors and actuators are considered in this work. A common feature is to include stability analysis within the design technique [17]–[19]. However, to the best of our knowledge, no works are focused on finding controllers vulnerabilities produced by attacks on sensors on control systems, and hence, quantification of the vulnerability level of sensors on an industrial control system to face false data injection attacks is an interesting gap that we investigate in this work.

In the present work, we consider two kinds of false data injection attacks on sensors of legacy cyber-physical control systems: i) additive attacks, which could be considered as external inputs; and ii) multiplicative attacks, which could be modeled as changes on the constant gain of the sensors. The effect on the tracking closed-loop control systems stability of these two types of attacks is then analyzed and the vulnerability level of each sensor is quantified. We also use the attack detection, isolation, and mitigation mechanisms described in [20] to see if the considered attacks can be mitigated, finding that once the attacker succeeds in making the system unstable, secure state estimation and, therefore, the mitigation of the sensor attack cannot be achieved. We use some tools from robust control theory to formulate two equivalent optimization problems with LMI constraints, which allows us to find a conservative limit on the gain of each sensor of the system to determine which of the system outputs is more vulnerable to multiplicative attacks. Hence, the contribution of our work is twofold: i) we propose the formulation of an optimization problem to find bounds on multiplicative attacks on sensors that guarantee the system remains stable even if a sensor attack is acting on the control system; and ii) the stability analysis formulation that gives comparative information on the vulnerability levels of existing sensors in a control system, which allows the definition of more demanding attacks to test mitigation mechanisms of attacks on sensors.

The paper is organized as follows. Section II shows the general setup of an already functional closed-loop control system, which might be subject to cyber-attacks. Section III shows how the system model including attacks on sensors, and whether or not those attacks affect the system dynamics. Section IV shows the classic Lyapunov approach for the stability of discrete-time systems and, then, we show

the condition for which we can find bounds on the attacks acting on the system with the purpose of making it unstable. In Section V, the three tanks benchmark system is used to show the effects of the attacks on system stability and its mitigation, when possible. Finally, in Section VI we draw some conclusions.

II. EXISTING SYSTEM SETUP

We consider a physical system that works with a digital controller in a closed-loop manner through a network, i.e., an existing cyber-physical control system, as the one depicted in Figure 1. The controller allows the system to maintain a specific behavior, where normally the system is able to follow a reference input and to maintain specific characteristics in the transient response. Since the real system is considered to be, in general, nonlinear, it has a behavior modeled as

$$\begin{aligned} \dot{\mathbf{x}}(t) &= \mathbf{f}(\mathbf{x}(t), \quad \mathbf{u}(t), t), \\ \mathbf{y}(t) &= \mathbf{g}(\mathbf{x}(t), \quad \mathbf{u}(t), t), \end{aligned} \tag{1}$$

where $\mathbf{x}(t) \in \mathbb{R}^n$, $\mathbf{u}(t) \in \mathbb{R}^m$, and $\mathbf{y}(t) \in \mathbb{R}^p$ are the system state, input, and output, respectively. The vector functions $\mathbf{f}(\cdot)$ and $\mathbf{g}(\cdot)$ are, in general, nonlinear functions that relate the system state and inputs with the state dynamics and the system outputs, respectively. Since the closed-loop system works with a digital controller, we consider that the controller is designed with the more straightforward approximation, i.e., a discrete-time linear approximation of the system, which can be expressed as

$$\begin{aligned} \mathbf{x}[k+1] &= \mathbf{A}\,\mathbf{x}[k] + \mathbf{B}\,\tilde{\mathbf{u}}[k], \\ \mathbf{y}[k] &= \mathbf{C}\,\mathbf{x}[k], \end{aligned} \tag{2}$$

where $\mathbf{x}[k] \in \mathbb{R}^n$, $\tilde{\mathbf{u}}[k] \in \mathbb{R}^m$, and $\mathbf{y}[k] \in \mathbb{R}^p$ are the discrete-time system state, input, and output, respectively. Notice that the system input is not $\mathbf{u}[k]$ but $\tilde{\mathbf{u}}[k]$, which represents $\mathbf{u}[k]$ after passing through the network. $\mathbf{A} \in \mathbb{R}^{n\times n}$, $\mathbf{B} \in \mathbb{R}^{n\times m}$ and $\mathbf{C} \in \mathbb{R}^{p\times n}$ are the dynamic, input, and output matrices of the system. This kind of system model defined by (2) can be obtained from either, discretizing the linearization of the system around an equilibrium point or, learning the discrete-time model from input-output data, using an adequate sampling time, T_s, according to the closed-loop system dynamical behavior [21].

The controller that works with the system is considered to be a tracking control with state feedback, i.e., a servo system [22], represented as

$$\begin{aligned} \mathbf{v}[k+1] &= T_s\left(\mathbf{y}^r[k] - \tilde{\mathbf{y}}[k]\right) + \mathbf{v}[k], \\ \mathbf{u}[k] &= -\mathbf{K}_I\,\mathbf{v}[k] - \mathbf{K}_S\,\hat{\mathbf{x}}[k], \end{aligned} \tag{3}$$

where $\mathbf{y}^r[k] \in \mathbb{R}^p$ is the system reference input (the one the system is desired to follow), $\tilde{\mathbf{y}}[k]$ represents $\mathbf{y}[k]$ after passing through the network and $\hat{\mathbf{x}}[k]$ is the estimated state. Notice that the first equation in (3) is the integrator state equation (and, in this case, it is considered as an interior variable of the controller in Figure 1), where $\mathbf{v}[k] \in \mathbb{R}^p$ is a discrete-time approximation of the error integral, with the error defined as

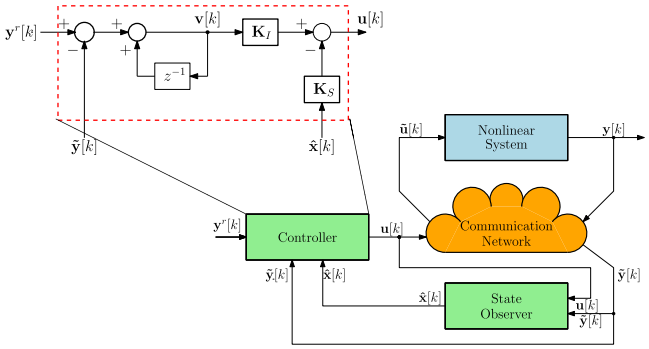

FIGURE 1. Block diagram of a cyber-physical control system.

$\mathbf{e}[k] = \mathbf{y}^r[k] - \mathbf{y}[k]$. The control signal $\mathbf{u}[k]$ is obtained as a linear combination of the states, through the state feedback gain $\mathbf{K}_S \in \mathbb{R}^{m\times n}$, and a linear combination of the error integral, through the integral gain $\mathbf{K}_I \in \mathbb{R}^{m\times p}$.

As usual, we assume that not all the system states are available for implementing the part of the controller related to state feedback. In order to estimate system states, we use a full-order current observer [21], [23], with the following dynamics

$$\begin{aligned} \bar{\mathbf{x}}[k] &= \mathbf{A}\,\hat{\mathbf{x}}[k-1] + \mathbf{B}\,\mathbf{u}[k-1], \\ \hat{\mathbf{x}}[k] &= \bar{\mathbf{x}}[k] + \mathbf{L}\,(\tilde{\mathbf{y}}[k] - \mathbf{C}\,\bar{\mathbf{x}}[k]), \end{aligned} \tag{4}$$

where $\bar{\mathbf{x}}[k]$ is the predicted estimate based on a model prediction from the previous time estimate, which is corrected by the measurement of the output becoming $\hat{\mathbf{x}}[k]$, and $\mathbf{L} \in \mathbb{R}^{n\times p}$ is the observer gain that guarantees $\mathbf{A} - \mathbf{L}\,\mathbf{C}\,\mathbf{A}$ is Hurwitz, when $(\mathbf{A},\ \mathbf{C}\,\mathbf{A})$ is observable.

Since the system and the controller are coupled by a network, the control signal received by the system is not $\mathbf{u}[k]$ but $\tilde{\mathbf{u}}[k]$, and the output signal received by the controller is not $\mathbf{y}[k]$ but $\tilde{\mathbf{y}}[k]$, where

$$\tilde{\mathbf{u}}[k] = \sum_{i=0}^{q} \delta[\tau_k - i]\,\mathbf{u}[k-i], \tag{5}$$

and

$$\tilde{\mathbf{y}}[k] = \sum_{i=0}^{q} \delta[\tau_k - i]\,\mathbf{y}[k-i]. \tag{6}$$

The Kronecker delta function $\delta[\tau_k - i]$ is used to represent the random communication delays and stochastic data missing. The time delay τ_k is a random variable considered to be an integer multiple of the sampling time, T_s, introduced to describe the possibility of data missing as well as the size of the delay at time instant k. For the ideal case, there is no communication delay, i.e., $\tau_k = 0$, then $\delta[0-i] = 1$ only for $i = 0$, and hence $\tilde{\mathbf{u}}[k] = \mathbf{u}[k]$. For a communication delay greater than zero ($1 \leq i \leq q$), only a term of the summation is equal to 1, hence $\tilde{\mathbf{u}}[k] = \mathbf{u}[k-i]$. In the case that the delay produces a timeout error $q = -1$, there is no terms on the summation, and $\tilde{\mathbf{u}}[k] = \mathbf{0}$, case where there is a lost data in the transmission through the network [24].

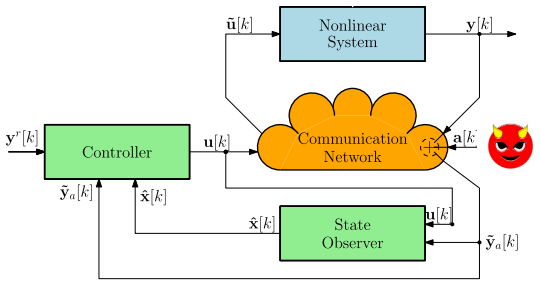

FIGURE 2. closed-loop control system with sensor attack.

It should be emphasized that the system, controller, and observer described in this section are supposed to be properly designed and fully functional, because our focus is on the attacks definition and the analysis of their impact in terms of stability.

III. ATTACKED SYSTEM

Let us consider an attack on the system like the one depicted in Figure 2, with two different possibilities of false data injection attacks on sensors [7]: an additive one and a multiplicative one, in order to study the stability of the attacked system and to conclude regarding which one would be more harmful.

A. ADDITIVE ATTACK

We first consider the closed-loop system working with a controller and an observer, described by

$$\begin{aligned}
\mathbf{x}[k+1] &= \mathbf{A}\,\mathbf{x}[k] + \mathbf{B}\,\tilde{\mathbf{u}}[k], && \text{(7a)}\\
\mathbf{y}[k] &= \mathbf{C}\,\mathbf{x}[k], && \text{(7b)}\\
\tilde{\mathbf{y}}_a[k] &= \tilde{\mathbf{y}}[k] + \mathbf{F}_a\,\mathbf{a}[k], && \text{(7c)}\\
\bar{\mathbf{x}}[k] &= \mathbf{A}\,\hat{\mathbf{x}}[k-1] + \mathbf{B}\,\mathbf{u}[k-1], && \text{(7d)}\\
\hat{\mathbf{x}}[k] &= \bar{\mathbf{x}}[k] + \mathbf{L}\,(\tilde{\mathbf{y}}_a[k] - \mathbf{C}\,\bar{\mathbf{x}}[k]), && \text{(7e)}\\
\mathbf{v}[k+1] &= \mathbf{y}^r[k] - \tilde{\mathbf{y}}_a[k] + \mathbf{v}[k], && \text{(7f)}\\
\mathbf{u}[k] &= -\mathbf{K}_I\,\mathbf{v}[k] - \mathbf{K}_S\,\hat{\mathbf{x}}[k], && \text{(7g)}
\end{aligned}$$

where $\mathbf{a}[k] \in \mathbb{R}^p$ represents external attack signals in each of the outputs, and $\mathbf{F}_a \in \mathbb{R}^{p\times p}$ is a matrix that indicates how the attacks signals affect each output.

Let us assume that the network has no perceptible effects on the signals whatsoever, that is $\tilde{\mathbf{u}}[k] = \mathbf{u}[k]$, $\tilde{\mathbf{y}}[k] = \mathbf{y}[k]$ and $\tilde{\mathbf{y}}_a[k] = \mathbf{y}_a[k]$. Therefore, the state equation for the control loop can be obtained from the system defined by (7a) with the control law in (7f)-(7g) and the attacked output in (7c), defining an extended state vector composed by the state variables and the integrator variables. That is

$$\begin{bmatrix}\mathbf{x}[k+1]\\ \mathbf{v}[k+1]\end{bmatrix} = \begin{bmatrix}\mathbf{A}-\mathbf{B}\,\mathbf{K}_S & -\mathbf{B}\,\mathbf{K}_I\\ -\mathbf{C}\mathbf{I} & \end{bmatrix}\begin{bmatrix}\mathbf{x}[k]\\ \mathbf{v}[k]\end{bmatrix} + \begin{bmatrix}0\\ \mathbf{I}\end{bmatrix}\mathbf{y}^r[k] + \begin{bmatrix}0\\ -\mathbf{F}_a\end{bmatrix}\mathbf{a}[k]. \quad (8)$$

Notice that the dynamic matrix of the equation has no terms related with the attack. In fact, the attack signal acts as an external input. Therefore, it is clear that this kind of attack does not affect the stability of the control loop, since the dynamic matrix remains the same as when there is no attack considered.

Let us consider the state equation of the observer loop that can be obtained from the system defined in (7a), with the observer in (7d)-(7e) and the attacked output in (7c). It can be written as

$$\hat{\mathbf{x}}[k] = (\mathbf{A} - \mathbf{L}\,\mathbf{C}\,\mathbf{A})\,\hat{\mathbf{x}}[k-1] + (\mathbf{B} - \mathbf{L}\,\mathbf{C}\,\mathbf{B})\,\mathbf{u}[k-1] + \mathbf{L}\,\mathbf{y}[k] + \mathbf{L}\,\mathbf{F}_a\,\mathbf{a}[k]. \quad (9)$$

Notice, again, that the dynamic matrix of the equation has no terms related with the attack and it acts as an external input. That is, $\mathbf{a}[k]$ does not affects the stability of the observer loop.

We can conclude from the prior analysis that additive attacks, where the attack signal is external, do not affect the stability of neither the control nor the observer loops and, therefore, do not affect the overall system stability.

B. MULTIPLICATIVE ATTACK

Let us consider the closed-loop control system of the previous section, disturbed with a sensor attack proportional to the state vector. That is, the same set in (7a)-(7g), but instead of (7c), we have

$$\tilde{\mathbf{y}}_a[k] = \mathbf{C}_m\,\mathbf{x}[k] + \mathbf{C}_a\,\mathbf{x}[k], \quad (10)$$

where $\tilde{\mathbf{y}}_a[k] \in \mathbb{R}^p$ represents a multiplicative attack on the output signal, of a tracking feedback control system, modifying its value in a proportion determined by $\mathbf{C}_a$ (after passing through the network). The structure for $\mathbf{C}_m$ corresponds to consider each output associated with a single measured state variable. That is, let us consider sensor gains k_i, for $i = 1, 2, \cdots, p$, for a system with p outputs, each of them related to an output. Then, without loss of generality, we consider that the sensors are related to the first p state variables (which can be easily arranged with an order modification of the state variables, through a basic transformation). Therefore, the structure for $\mathbf{C}_m$ can be written as

$$\mathbf{C}_m = \left[\text{diag}[k_1, k_2, \cdots, k_p]\ \mathbf{0}_{p\times(n-p)}\right].$$

$\mathbf{C}_a$ can be considered to have in some time window a similar structure. That is

$$\mathbf{C}_a = \left[\text{diag}[\alpha_1, \alpha_2, \cdots, \alpha_p]\ \mathbf{0}_{p\times(n-p)}\right],$$

where α_i is the constant value that represents the attack on the i^{th} output. Notice that for stability analysis purposes all α_i could be different than zero. In this case, the stability ranges will be more restrictive than considering only some of them different than zero, or even just one of them different than zero. With the previous structure for $\mathbf{C}_{a_i}$, it is easy to see that the attack on the i^{th} output consists in modifying the measurement by the i^{th} sensor in a proportional fashion. That is

$$\tilde{y}_i^a = k_i\,x_i + \alpha_i\,x_i. \quad (11)$$

Now, let us show how this kind of attack affects the stability of the control and observer loops. In order to do that, we consider, as in the previous case, the network has no perceptible effects on the signals whatsoever, i.e., $\tilde{\mathbf{u}}[k] = \mathbf{u}[k]$, $\tilde{\mathbf{y}}[k] = \mathbf{y}[k]$, and $\tilde{\mathbf{y}_a}[k] = \mathbf{y}_a[k]$.

For the control loop, the state equation can be obtained in the same way as we have obtained (8), but with the attack described as in (10). Then, the state equation for the control loop can be written as

$$\begin{bmatrix}\mathbf{x}[k+1]\\ \mathbf{v}[k+1]\end{bmatrix} = \begin{bmatrix}\mathbf{A}-\mathbf{B}_c\mathbf{K}_1 & -\mathbf{B}_c\mathbf{K}_2\\ -\mathbf{C}_m-\mathbf{C}_a & \mathbf{I}\end{bmatrix}\begin{bmatrix}\mathbf{x}[k]\\ \mathbf{v}[k]\end{bmatrix} + \begin{bmatrix}0\\ \mathbf{I}\end{bmatrix}\mathbf{y}^r[k]. \tag{12}$$

Notice that different from the additive case, the value of $\mathbf{C}_a$ affects the dynamic matrix of the system and, therefore, the stability of the control loop.

For the observer loop, the state equation can be obtained as we have obtained (9), but with the attack described as in (10). Then, the state equation for the observer loop can be written as

$$\begin{aligned}\hat{\mathbf{x}}[k] = {} & [\mathbf{A}-\mathbf{L}(\mathbf{C}_m+\mathbf{C}_a)\mathbf{A}]\,\hat{\mathbf{x}}[k-1]\\ & +[\mathbf{B}_c \;\; -\mathbf{L}(\mathbf{C}_m+\mathbf{C}_a)\mathbf{B}_c]\,\mathbf{u}[k-1]+\mathbf{L}\,\tilde{\mathbf{y}}_a[k],\end{aligned} \tag{13}$$

where, again, the value of $\mathbf{C}_a$ affects the system dynamic matrix and the stability of the observer loop.

After analyzing the stability effects of additive and multiplicative attacks, we can conclude that an attack as an external input does not affect system stability, whereas an attack proportional to the state may destabilize the system. Then, some questions rise in order to find ways of increase system safety, such as: what are the attack values the system can handle? or, what is the most vulnerable state? In the next section we propose a method to answer those questions.

IV. STABILITY ANALYSIS

In the previous section, we have showed that additive attacks do not affect the system stability, since the attack values do not affect the dynamic matrix of neither the control nor the observer loops. Also, we have showed that multiplicative attacks do modify the dynamic matrix of both the control and the observer loops, therefore, it can modify the stability of the closed-loop system. In this section, we use Lyapunov's second method for discrete-time systems and, with a parameterization of the attack, we come up with a way of finding conservative bounds on the attacks values to guarantee closed-loop asymptotic stability of the system.

A. QUADRATIC LYAPUNOV STABILITY FOR DISCRETE-TIME SYSTEMS

We start with a very well know result that establishes the conditions for the existence of a Lyapunov function for a discrete-time system, associated with the system state, and the asymptotic stability of the equilibrium point, shown in Theorem 1 [22].

Theorem 1: Consider a system of the form

$$\mathbf{x}[k+1] = \mathbf{A}\,\mathbf{x}[k].$$

Suppose there exists a scalar function $V(\mathbf{x}) > 0$, continuous in $\mathbf{x}$ such that

1) $V(\mathbf{x}) > 0$ *for* $\mathbf{x} \neq 0$.
2) $V(\mathbf{0}) = 0$.
3) $V(\infty) \to \infty$ *as* $||\mathbf{x}|| \to \infty$.
4) $\Delta V(\mathbf{x}) < 0$ *for* $\mathbf{x} \neq 0$, *where*

$$\Delta V(\mathbf{x}[k]) = V(\mathbf{x}[k+1]) - V(\mathbf{x}[k]).$$

Then, the equilibrium state $\mathbf{x}^* = \mathbf{0}$ is asymptotically stable in the large and $V(\mathbf{x})$ is a Lyapunov function.

Let us consider the following Lyapunov function candidate,

$$V(\mathbf{x}[k]) = \mathbf{x}^\top[k]\,\mathbf{P}\,\mathbf{x}[k], \tag{14}$$

where $\mathbf{P}$ is a positive definite and symmetric Hermitian matrix. Then

$$\begin{aligned}\Delta V(\mathbf{x}[k]) &= V(\mathbf{x}[k+1]) - V(\mathbf{x}[k])\\ &= \mathbf{x}^\top[k+1]\,\mathbf{P}\,\mathbf{x}[k+1] - \mathbf{x}^\top[k]\,\mathbf{P}\,\mathbf{x}[k]\\ &= (\mathbf{A}\,\mathbf{x}[k])^\top\,\mathbf{P}\,\mathbf{A}\,\mathbf{x}[k] - \mathbf{x}^\top[k]\,\mathbf{P}\,\mathbf{x}[k]\\ &= \mathbf{x}^\top[k]\,\mathbf{A}^\top\,\mathbf{P}\,\mathbf{A}\,\mathbf{x}[k] - \mathbf{x}^\top[k]\,\mathbf{P}\,\mathbf{x}[k]\\ &= \mathbf{x}^\top[k](\mathbf{A}^\top\,\mathbf{P}\,\mathbf{A}-\mathbf{P})\,\mathbf{x}[k].\end{aligned}$$

For asymptotic stability we require that $\Delta V(\mathbf{x}[k]) < 0$. Therefore,

$$\Delta V(\mathbf{x}[k]) = \mathbf{x}^\top[k](\mathbf{A}^\top\,\mathbf{P}\,\mathbf{A}-\mathbf{P})\,\mathbf{x}[k] < 0. \tag{15}$$

For this equation to be satisfied, we need to solve the following linear matrix inequality (LMI)

$$\mathbf{A}^\top\,\mathbf{P}\,\mathbf{A} - \mathbf{P} < 0. \tag{16}$$

B. QUADRATIC LYAPUNOV STABILITY FOR THE ATTACKED SYSTEM

We need to check the stability for both, the dynamic matrix from the discrete-time closed-loop system and the observer. In order to do that, we use Lyapunov theory, which for this kind of system establishes that the LMI in (16) should be satisfied. For the tracking feedback closed-loop system, from (12) we can see that

$$\bar{\mathbf{A}} = \begin{bmatrix}\mathbf{A}-\mathbf{B}_c\mathbf{K}_1 & -\mathbf{B}_c\mathbf{K}_2\\ -\mathbf{C}_m-\mathbf{C}_a & \mathbf{I}\end{bmatrix},$$

and, for the observer, from (13) we can identify

$$\bar{\mathbf{A}} = \mathbf{A} - \mathbf{L}(\mathbf{C}_m+\mathbf{C}_a)\mathbf{A},$$

each of them designed to be stable for $\mathbf{C}_a = \mathbf{0}$.

Before introducing the main result of this work, let us introduce a lemma that will help to prove our result [25].

Lemma 1: Let $\mathbf{S}$ and $\mathbf{Z}$ be $q \times q$ symmetric positive-semidefinite matrices and $\mathbf{Y}$ a $q \times q$ symmetric negative-semidefinite matrix. Suppose further that

$$(\mathbf{w}^\top\,\mathbf{Y}\,\mathbf{w})^2 - 4\mathbf{w}^\top\,\mathbf{S}\,\mathbf{w}\,\mathbf{w}^\top\,\mathbf{Z}\,\mathbf{w} > 0, \tag{17}$$

for all $\mathbf{w} \neq \mathbf{0} \in \mathcal{R}^q$. *Then* $\varepsilon^2 \mathbf{S} + \varepsilon \mathbf{Y} + \mathbf{Z} < \mathbf{0}$, *for some* $\varepsilon > 0$.

Theorem 2 (General Stability): Let us assume that the system is described by

$$\mathbf{x}[k+1] = \bar{\mathbf{A}}\,\mathbf{x}[k], \tag{18}$$

where $\bar{\mathbf{A}} = \bar{\mathbf{A}}_n + \Delta\bar{\mathbf{A}}$ *and the matrix* $\Delta\bar{\mathbf{A}}$ *is decomposed as a bounded norm uncertainty, i.e.,*

$$\Delta\bar{\mathbf{A}} = \gamma\,\mathbf{D}\,\mathbf{F}\,\mathbf{E}. \tag{19}$$

$\mathbf{F}$ *represents the real unknown parameters, in this case the attacks, that satisfies* $\mathbf{F}^\top\mathbf{F} \leq 1$ *and,* $\mathbf{D}$ *and* $\mathbf{E}$ *represent how the unknown values affect* $\bar{\mathbf{A}}$.

The equilibrium state of the system in (18) *is stable if and only if there exist a symmetric positive definite matrix* $\mathbf{P}$ *and positive scalars* $\alpha > 0$ *and* $\varepsilon > 0$ *such that*

$$\begin{aligned} &\min \quad \alpha \\ &\textit{subject to} \quad \begin{bmatrix} -\mathbf{P} & \bar{\mathbf{A}}_n^\top\mathbf{P} & \mathbf{0} & \mathbf{E}^\top \\ \mathbf{P}\bar{\mathbf{A}}_n & -\mathbf{P} & \mathbf{D}^\top\mathbf{P} & \mathbf{0} \\ \mathbf{0} & \mathbf{PD} & -\varepsilon\mathbf{I} & \mathbf{0} \\ \mathbf{E} & \mathbf{0} & \mathbf{0} & -\alpha\mathbf{I} \end{bmatrix} < \mathbf{0}, \end{aligned} \tag{20}$$

or, equivalently, if and only if there exist a symmetric positive definite matrix $\mathbf{P}$ *and positive scalars* $\beta > 0$ *and* $\varepsilon > 0$ *such that*

$$\begin{aligned} &\max \quad \beta \\ &\textit{subject to} \quad \beta > 0, \ \begin{bmatrix} -\mathbf{P} + \beta\,\mathbf{E}^\top\mathbf{E} & \bar{\mathbf{A}}_n^\top\mathbf{P} & \mathbf{0} \\ \mathbf{P}\bar{\mathbf{A}}_n & -\mathbf{P} & \mathbf{D}^\top\mathbf{P} \\ \mathbf{0} & \mathbf{PD} & -\varepsilon\mathbf{I} \end{bmatrix} < \mathbf{0}. \end{aligned} \tag{21}$$

Proof: Using the Schur complement [26], (16) can be written as

$$\begin{bmatrix} -\mathbf{P} & \bar{\mathbf{A}}^\top\mathbf{P} \\ \mathbf{P}\bar{\mathbf{A}} & -\mathbf{P} \end{bmatrix} < \mathbf{0}. \tag{22}$$

By hypothesis, we will consider $\bar{\mathbf{A}}$ as a matrix with a bounded nominal uncertainty, that is $\bar{\mathbf{A}} = \bar{\mathbf{A}}_n + \Delta\bar{\mathbf{A}}$, this representation is the more general one. For the controller loop, we will have that we must have

$$\bar{\mathbf{A}}_n = \begin{bmatrix} \mathbf{A} - \mathbf{B}_c\mathbf{K}_1 & -\mathbf{B}_c\mathbf{K}_2 \\ -\mathbf{C}_m & \mathbf{I} \end{bmatrix}, \tag{23}$$

with

$$\Delta\bar{\mathbf{A}} = \begin{bmatrix} \mathbf{0}_{n\times n} & \mathbf{0}_{n\times m} \\ -\mathbf{C}_a & \mathbf{0}_{m\times m} \end{bmatrix}. \tag{24}$$

For the observer loop, we will have that

$$\bar{\mathbf{A}}_n = \mathbf{A} - \mathbf{L}\,\mathbf{C}_m\,\mathbf{A}, \tag{25}$$

with

$$\Delta\bar{\mathbf{A}} = -\mathbf{L}\,\mathbf{C}_a\,\mathbf{A}. \tag{26}$$

Then,

$$\begin{bmatrix} -\mathbf{P} & (\bar{\mathbf{A}}_n + \Delta\bar{\mathbf{A}})^\top\mathbf{P} \\ \mathbf{P}(\bar{\mathbf{A}}_n + \Delta\bar{\mathbf{A}}) & -\mathbf{P} \end{bmatrix} < \mathbf{0}.$$

By (19), this corresponds to

$$\begin{bmatrix} -\mathbf{P} & (\bar{\mathbf{A}}_n + \gamma\,\mathbf{D}\,\mathbf{F}\,\mathbf{E})^\top\mathbf{P} \\ \mathbf{P}(\bar{\mathbf{A}}_n + \gamma\,\mathbf{D}\,\mathbf{F}\,\mathbf{E}) & -\mathbf{P} \end{bmatrix} < \mathbf{0}.$$

Equivalently

$$\begin{bmatrix} -\mathbf{P} & \bar{\mathbf{A}}_n^\top\mathbf{P} \\ \mathbf{P}\bar{\mathbf{A}}_n & -\mathbf{P} \end{bmatrix} + \begin{bmatrix} \mathbf{0} & \gamma\,\mathbf{E}^\top\mathbf{F}^\top\mathbf{D}^\top\mathbf{P} \\ \gamma\,\mathbf{P}\mathbf{D}\mathbf{F}\mathbf{E} & \mathbf{0} \end{bmatrix} < \mathbf{0},$$

which can also be written in quadratic form as

$$\mathbf{X}^\top\begin{bmatrix} -\mathbf{P} & \bar{\mathbf{A}}_n^\top\mathbf{P} \\ \mathbf{P}\bar{\mathbf{A}}_n & -\mathbf{P} \end{bmatrix}\mathbf{X} + \mathbf{X}^\top\begin{bmatrix} \mathbf{0} & \gamma\mathbf{E}^\top\mathbf{F}^\top\mathbf{D}^\top\mathbf{P} \\ \gamma\mathbf{PDFE} & \mathbf{0} \end{bmatrix}\mathbf{X} < 0,$$

for all $\mathbf{X} \neq \mathbf{0}$. Since we know that $\mathbf{F}^\top\mathbf{F} \leq 1$, we can write

$$\begin{aligned} &\mathbf{X}^\top\begin{bmatrix} -\mathbf{P} & \bar{\mathbf{A}}_n^\top\mathbf{P} \\ \mathbf{P}\bar{\mathbf{A}}_n & -\mathbf{P} \end{bmatrix}\mathbf{X} \\ &\quad < -\max\left\{\mathbf{X}^\top\begin{bmatrix} \mathbf{0} & \gamma\,\mathbf{E}^\top\mathbf{F}^\top\mathbf{D}^\top\mathbf{P} \\ \gamma\,\mathbf{P}\mathbf{D}\mathbf{F}\mathbf{E} & \mathbf{0} \end{bmatrix}\mathbf{X}:\ \mathbf{F}^\top\mathbf{F} \leq 1\right\}, \end{aligned}$$

which left hand side is negative. Then, squaring on both sides of the inequality, we have

$$\begin{aligned} &\left(\mathbf{X}^\top\begin{bmatrix} -\mathbf{P} & \bar{\mathbf{A}}_n^\top\mathbf{P} \\ \mathbf{P}\bar{\mathbf{A}}_n & -\mathbf{P} \end{bmatrix}\mathbf{X}\right)^2 \\ &\quad > \left(\max\left\{\mathbf{X}^\top\begin{bmatrix} \mathbf{0} & \gamma\,\mathbf{E}^\top\mathbf{F}^\top\mathbf{D}^\top\mathbf{P} \\ \gamma\,\mathbf{P}\mathbf{D}\mathbf{F}\mathbf{E} & \mathbf{0} \end{bmatrix}\mathbf{X}:\ \mathbf{F}^\top\mathbf{F} \leq 1\right\}\right)^2. \end{aligned} \tag{27}$$

In order to rewrite the right hand side of (27), we express $\mathbf{X} = \begin{bmatrix}\mathbf{x}^\top & \mathbf{y}^\top\end{bmatrix}^\top$, obtaining

$$\begin{aligned} &\left(\begin{bmatrix}\mathbf{x}^\top & \mathbf{y}^\top\end{bmatrix}\begin{bmatrix} \mathbf{0} & \gamma\mathbf{E}^\top\mathbf{F}^\top\mathbf{D}^\top\mathbf{P} \\ \gamma\mathbf{PDFE} & \mathbf{0} \end{bmatrix}\begin{bmatrix}\mathbf{x} \\ \mathbf{y}\end{bmatrix}\right)^2 \\ &\qquad = 4\left(\gamma\mathbf{y}^\top\mathbf{PDFEx}\right)^2. \end{aligned} \tag{28}$$

Using the triangle inequality, we have

$$4\ \gamma^2\ \left(\mathbf{y}^\top\mathbf{P}\,\mathbf{D}\,\mathbf{F}\,\mathbf{E}\,\mathbf{x}\right)^2 \leq 4\,\mathbf{y}^\top\mathbf{P}\,\mathbf{D}\,\mathbf{D}^\top\mathbf{P}\,\mathbf{y}\,\gamma^2\,\mathbf{x}^\top\mathbf{E}^\top\mathbf{E}\,\mathbf{x}, \tag{29}$$

which can be rewritten as

$$\begin{aligned} 4\ \gamma^2\ \left(\mathbf{y}^\top\mathbf{PDFEx}\right)^2 &\leq 4\mathbf{X}^\top\begin{bmatrix}\gamma^2\mathbf{E}^\top\mathbf{E} & \mathbf{0} \\ \mathbf{0} & \mathbf{0}\end{bmatrix} \\ &\quad \times \mathbf{X}\mathbf{X}^\top\begin{bmatrix}\mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{PDD}^\top\mathbf{P}\end{bmatrix}\mathbf{X}, \end{aligned} \tag{30}$$

which implies that the right hand side is the maximum value that we are looking for. Therefore, we can rewrite (27) as

$$\begin{aligned} &\left(\mathbf{X}^\top\begin{bmatrix} -\mathbf{P} & \bar{\mathbf{A}}_n^\top\mathbf{P} \\ \mathbf{P}\bar{\mathbf{A}}_n & -\mathbf{P} \end{bmatrix}\mathbf{X}\right)^2 + -4\,\mathbf{X}^\top\begin{bmatrix}\gamma^2\mathbf{E}^\top\mathbf{E} & \mathbf{0} \\ \mathbf{0} & \mathbf{0}\end{bmatrix} \\ &\qquad \times \mathbf{X}\mathbf{X}^\top\begin{bmatrix}\mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{PDD}^\top\mathbf{P}\end{bmatrix}\mathbf{X} > 0. \end{aligned} \tag{31}$$

Using Lemma 1,

$$\varepsilon\begin{bmatrix}\gamma^2\mathbf{E}^\top\mathbf{E} & \mathbf{0} \\ \mathbf{0} & \mathbf{0}\end{bmatrix} + \begin{bmatrix} -\mathbf{P} & \bar{\mathbf{A}}_n^\top\mathbf{P} \\ \mathbf{P}\bar{\mathbf{A}}_n & -\mathbf{P} \end{bmatrix} + \frac{1}{\varepsilon}\begin{bmatrix}\mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{PDD}^\top\mathbf{P}\end{bmatrix} < 0.$$

Adding up the matrices, we have

$$\begin{bmatrix} -\mathbf{P} + \varepsilon\,\gamma^2\,\mathbf{E}^\top\,\mathbf{E} & \bar{\mathbf{A}}_n^\top\,\mathbf{P} \\ \mathbf{P}\,\bar{\mathbf{A}}_n & -\mathbf{P} + \varepsilon^{-1}\,\mathbf{P}\,\mathbf{D}\,\mathbf{D}^\top\,\mathbf{P} \end{bmatrix} < \mathbf{0}, \quad (32)$$

which needs to be solved for ϵ, γ and $\mathbf{P}$ and, therefore, it is not an LMI. Finally, applying the Schur complement to each of the principal diagonal elements and defining $\alpha^{-1} = \varepsilon\,\gamma^2$, the problem of finding the upper limit for the attack in order the complete closed-loop system (controller together with observer) remains stable can be formulated as (20). If we only apply the Schur complement to the term $-\mathbf{P} + \varepsilon^{-1}\,\mathbf{P}\,\mathbf{D}\,\mathbf{D}^\top\,\mathbf{P}$ in (32), the problem can be formulated as (21), with $\beta = \varepsilon\,\gamma^2$. □

Notice that the previous result can be applied not only to systems with controllers as the ones defined in (3), but also controllers in state-space representation. Therefore, the formulation proposed can be used with a wide range of systems.

Now, how can we use the results obtained in this section? Solving (20) or, equivalently, (21) for one attack simultaneously, we can find the most vulnerable variable of the system and, depending on the stability range of the attack value in such output, we can decide if it is necessary to reinforce the safety characteristics of the system. That is, if an attacker could easily instabilize the system, some actions are needed, like using some kind of encryption for the data. Also, this result could give us information about the hardest combination of attacks the system could handle, before going unstable, and the most restrictive stability range derived from such situation. In the following section we illustrate particularly the first situation.

V. NUMERICAL RESULTS

In order to see the implications on the closed-loop system stability of the false data injection attacks considered in Section III, we are going to simulate additive and multiplicative attacks on the original system, and on the system with the mitigation mechanism similar to the ones proposed in [27] and [20], in order to verify the severity of the attacks.

Let us consider the three tanks benchmark system [28]. The system modeling, parameters, operation point, and linearized model are the same as the ones utilized in [20], and for the reader's convenience are included next. The nonlinear dynamics of this system are obtained using first-principles, which are based on the use of physical laws to describe the dynamic evolution of a system. In this specific case, a balance of mass is used to obtain the differential equations that are the model of the system [28], given by

$$\begin{aligned} S\frac{d}{dt}L_1(t) &= Q_1(t) - q_{13}(t), \\ S\frac{d}{dt}L_2(t) &= Q_2(t) + q_{32}(t) - q_{20}(t), \\ S\frac{d}{dt}L_3(t) &= q_{13}(t) - q_{32}(t), \end{aligned} \quad (33)$$

TABLE 1. Parameter values of the three tank system.

Parameter	Symbol	Value
Tank cross section area	S	0.0154 m^2
Pipe cross section area	S_n	$5 \times 10^{-5}\mathrm{m}^2$
Outflow coefficient	$\mu_{13} = \mu_{32}$	0.5
Outflow coefficient	μ_{20}	0.6
Maximum flow rate	$Q_{i\,max}\ i \in [1,2]$	$1.5 \times 10^{-4}\mathrm{m}^3/\mathrm{s}$
Maximum level	$L_{j\,max}\ j \in [1,2,3]$	0.62 m

where the parameter description and values are shown in Table 1, and

$$\begin{aligned} q_{13}(t) &= \mu_{13}\,S_n\ \mathrm{sgn}[L_1(t) - L_3(t)]\sqrt{2g|L_1(t) - L_3(t)|}, \\ q_{32}(t) &= \mu_{32}\,S_n\ \mathrm{sgn}[L_3(t) - L_2(t)]\sqrt{2g|L_3(t) - L_2(t)|}, \\ q_{20}(t) &= \mu_{20}\,S_n\,\sqrt{2gL_2(t)}, \end{aligned} \quad (34)$$

where g is the gravity acceleration, $|\cdot|$ represents the absolute value, and $\mathrm{sgn}[\cdot]$ represents the sign of the argument.

The schematic diagram of the system is shown in Fig. 3. The goal of this control system is to track the liquid level of two tanks ($L_1(t)$ and $L_2(t)$) in concordance with the two set-points settled. For this case, we consider the system has three coupled tanks, with a level sensor for tanks 1 and 2 (i.e., two outputs), and two valves to regulate the intake flow in tanks 1 and 2 (i.e. two inputs). However, the state variables are the levels of the three tanks (i.e., there is no measurements in one of the three tanks).

The operation point of the system is obtained fixing the nominal intake flow as $u_1 = 3.5 \times 10^{-5}$ m^3/s and $u_2 = 3.75 \times 10^{-5}$ m^3/s. Therefore, the operation point for the state variables of the system would be $h_1 = 0.4$ m, $h_2 = 0.2$ m, and $h_3 = 0.3$ m.

In order to be able of using the stability analysis, a linear discrete-time model for the system is required. This linear model is obtained using input-output data. The data is used to estimate a discrete-time incremental linear state-space model, which is an approximation of the physical nonlinear system near the operation point. The discrete-time space state model (2) is obtained using a sampling time $T_s = 1$ s as in [29], together with subspace identification techniques [30] and a similarity transformation. Therefore, the parameters of the model are given by

$$\mathbf{A} = \begin{bmatrix} 0.9899 & 0.0005 & 0.0098 \\ 0.0004 & 0.9804 & 0.0095 \\ 0.0108 & 0.0107 & 0.9784 \end{bmatrix},$$

$$\mathbf{B} = \begin{bmatrix} 60.1584 & 0.1660 \\ -0.3848 & 60.1895 \\ 0.4138 & 0.1935 \end{bmatrix},$$

and

$$\mathbf{C} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

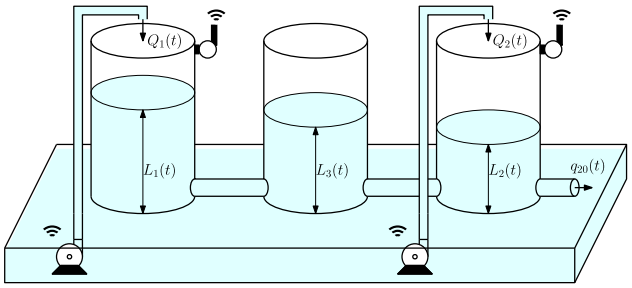

FIGURE 3. Schematic diagram of three tanks system.

The proposed control for this system given in [29] is a discrete-time controller as in (7f)-(7g), and feedback gains given by

$$\mathbf{K}_S = \begin{bmatrix} 21.6 & 3 & -5 \\ 2.9 & 19 & -4 \end{bmatrix} \times 10^{-4},$$

and

$$\mathbf{K}_I = \begin{bmatrix} -0.95 & -0.32 \\ -0.30 & -0.91 \end{bmatrix} \times 10^{-4}.$$

In order to implement the control law, we design a full order current observer as in (7d)-(7e), with

$$\mathbf{L} = \begin{bmatrix} 0.9995 & 0.0005 \\ 0.0005 & 0.9995 \\ 45.0167 & 42.5017 \end{bmatrix}.$$

The behavior of the closed-loop system is shown in Figure 4.

In order to show some interesting numerical results, we found through simulation that the stability limits for multiplicative attacks on input 1 is 0.553, whereas for output 2 is 0.735. Since the behavior attacking each output is quite similar, we will show attacks on output 2 (since the range of attacks is a little larger), to illustrate the effect of the attacks and how to use the results presented in this work.

Notice the attack signal is not random. What we have done is to sweep over a range of attack values that would cause a big impact on the system, for both the additive and multiplicative attacks. The selection of the attack signal is done taking into account the effect that this signal can cause on the system. Additive attacks are effectively external inputs whereas multiplicative attacks are changes in the model output matrix of the system.

A. ADDITIVE ATTACKS

As we have mentioned before, we are going to show the effects of an additive attack on one of the sensors, in this case on output 2. For that, we set $\mathbf{a}[k] = \begin{bmatrix} a_1[k] & a_2[k] \end{bmatrix}^\top$. Since we are only considering an attack on output 2, $a_1[k] = \mathbf{0}$, while

$$a_2[k] = \begin{cases} 0, & t < t_1, \\ f_i f_{s_1}, & t_1 \le k \le t_1 + 20, \\ f_i, & t_1 + 21 \le k \le t_2 - 21, \\ f_i f_{s_2}, & t_2 - 20 \le k \le t_2, \\ 0, & t > t_2, \end{cases} \tag{35}$$

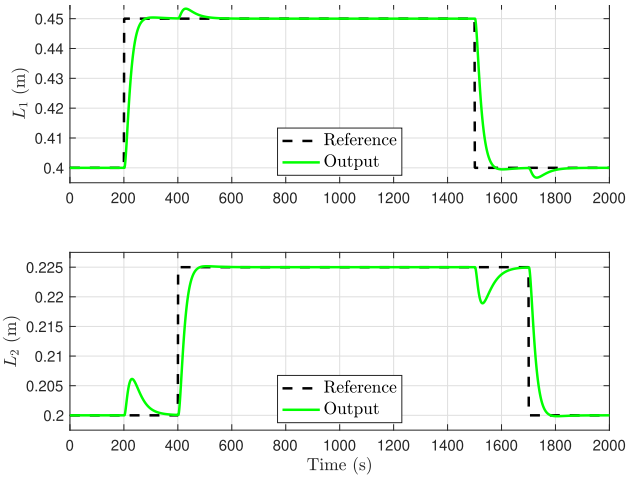

FIGURE 4. Response of the closed-loop control system without attacks.

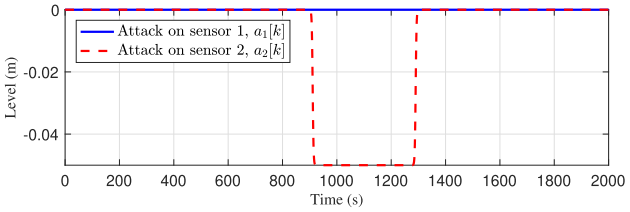

FIGURE 5. Example of additive attacks: $a_1[k]$ is an attack of magnitude 0 on sensor L_1 and $a_2[k]$ is an attack of magnitude -0.05 on sensor L_2, as in (35).

where f_{s_1} and f_{s_2} are functions to soften the initial and final portions of the attacks, as

$$f_{s_1} = \frac{1 + \tanh\left[(0.1(k - t_1) - 1)\pi\right]}{2} \tag{36}$$

and

$$f_{s_2} = \frac{1 - \tanh\left[(0.1(k - (t_2 - 20)) - 1)\pi\right]}{2}, \tag{37}$$

$t_1 = 900$s and $t_2 = 1300$s are the initial and final times of the attack, f_i is the function that shapes the i^{th} attack itself, in this case a pulse (between t_1 and t_2) of amplitude a, see Figure 5 for an example of attack signals with $a = -0.05$.

In Figure 6 we can see the effect of the attacks defined by (35) for different values of a. There, we can notice that, no matter the sign or the magnitude of the additive attack, the shape of the attack effect on the outputs is the same and it never compromises system stability, as it was shown in the analysis in Subsection III-A. Also, it is important to mention that there can be attack magnitudes that will take out the variables from its feasible values, and that can cause malfunction of the closed-loop system. However, that is not an implication related with stability.

B. MULTIPLICATIVE ATTACKS

In this case, for k when there is no attack, $\mathbf{C}_a = 0$. Notice that we do not consider attacks that last the complete simulation time. That is, for the sake of comparison, we will see the

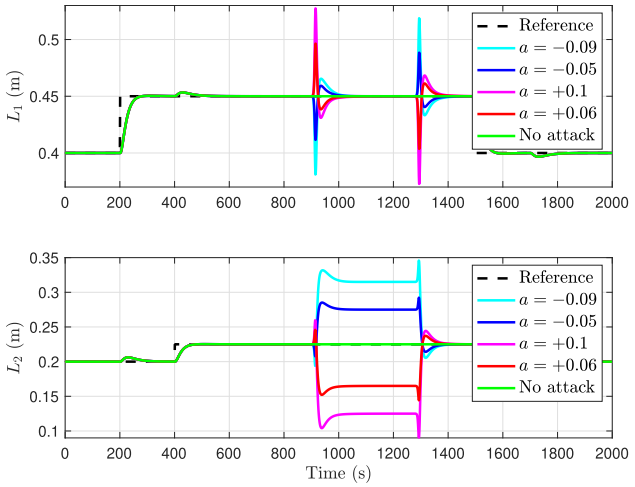

FIGURE 6. Response of the closed-loop control system with additive attacks of magnitude a.

implications of having a multiplicative attack on output 2 during the same time interval as the additive attack. Therefore,

$$\mathbf{C}_a = \begin{bmatrix} 0 & 0 \\ 0 & b \end{bmatrix}, \tag{38}$$

between t_1 and t_2.

Now, we are going to use Theorem 2 to find the stability value interval for b. We have to analyze two systems to find such interval, the controller loop and the observer loop.

Let us first consider the controller loop, with $\bar{\mathbf{A}}_n$ as in (23) and, $\mathbf{C}_a$ defined as in (24) and parameterized as in (19). That is,

$$\Delta\bar{\mathbf{A}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & b & 0 & 0 & 0 \end{bmatrix} = \underbrace{\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ -1 \end{bmatrix}}_{\mathbf{D}} \underbrace{\frac{b}{\sqrt{\gamma}}}_{\mathbf{F}} \underbrace{\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \end{bmatrix}}_{\mathbf{E}}.$$

Therefore, solving (21), we find that $b \leq 0.7871$. For solving (21), we use the Matlab® Robust Control Toolbox, as in the following code.

Notice that `Anb` $= \bar{\mathbf{A}}_n$ defined as in (23) and `a` $= \beta$ from (21).

Now, considering the observer loop, with $\bar{\mathbf{A}}_n$ as in (25) and, $\mathbf{C}_a$ defined as in (26) and parameterized as in (19), we have

$$\mathbf{\Delta}\,\bar{\mathbf{A}} = -\mathbf{L}\,\mathbf{C}_a\,\mathbf{A} = \underbrace{-\mathbf{L}(:,2)}_{\mathbf{D}} \underbrace{\frac{b}{\sqrt{\gamma}}}_{\mathbf{F}} \underbrace{\mathbf{A}(2,:)}_{\mathbf{E}},$$

where the notation $\mathbf{A}(2,:)$ represents the second row of $\mathbf{A}$, and $\mathbf{L}(:,2)$ represents the second column of $\mathbf{L}$. Solving (21) we find that $b \leq 0.5189$. Therefore, given the separation principle [22], [23], we can guarantee the stability of the system if both loops (controller and observer) are stable. That is, the system is going to be stable for attacks with $b \leq 0.5189$. Equivalent results were found solving (20). Notice that, as we mentioned before, using simulation, we find $b = 0.735$ for

```
setlmis([])
a = lmivar(1, [1,1]); % scalar
e = lmivar(1, [1,1]); % scalar
P = lmivar(1, [size(Anb,1),1]); % P ...
    symetric 5x5

lmiterm([1 1 1 a],-1,1) % -a < 0 % 1st ...
    constraint

% 2nd constraint
lmiterm([2 1 1 P],-1,1)
lmiterm([2 1 1 a],E',E)
lmiterm([2 2 1 P],1,Anb)
lmiterm([2 2 2 P],-1,1)
lmiterm([2 3 2 P],D',1)
lmiterm([2 3 3 e],-1,1)

LMIs = getlmis;

c = mat2dec(LMIs,-1,0,zeros(size(Ab,1),...
    size(Ab,1)));

options = [1e-5,0,0,0,0];
[copt,xopt] = mincx(LMIs,c,options);

a = dec2mat(LMIs, xopt, a)
e = dec2mat(LMIs, xopt, e)
P = dec2mat(LMIs, xopt, P)

gamma = sqrt(a/e) % the limit on b
```

critically stable system; a higher value than the one obtained solving (21), as expected, since the values obtained from that approach are more restrictive.

Notice that we could do the same analysis for the stability of the system with attacks on output 1, modifying accordingly $\mathbf{C}_a$, $\mathbf{\Delta}\bar{\mathbf{A}}$ for both, the controller and the observer loop. Solving (21), for the controller loop, we find that the system is stable for attacks up to 0.7909, and, for the observer loop, the system becomes unstable for attacks greater that 0.4989; and we could conclude that attacks on output 1 greater that 0.4989 will make the system unstable. Notice that, as we mentioned before, using simulation, we find the attack value for critically stable system as 0.553, a less restrictive value than the one found solving (21). However, it is worth to mention that the stability limits found solving either (20) or (21), even though being more restrictive, are consistent with the stability limits found by simulation. That is, we can find the most vulnerable output to multiplicative attacks solving (20) or (21), for the controller and the observer loops, for each output at a time, in a more efficient way than finding it through simulation (which is very time consuming).

In Figure 7 we can see the effect of the attacks defined in (10) for different values of b, where we can notice different system behavior depending on the sign and magnitude of the attack. For instance, for negative attacks, the larger the attack the larger the response peak time and the overshoot remains approximately the same. On the other hand, for positive attacks, the larger the attack magnitude the larger the overshoot up to achieving an unstable system (see Figure 10). The former was expected and, it can be explained from the fact that, as we mentioned before, the $\mathbf{C}_a$ matrix become part of the augmented dynamic matrix of the system $\bar{\mathbf{A}}$; therefore,

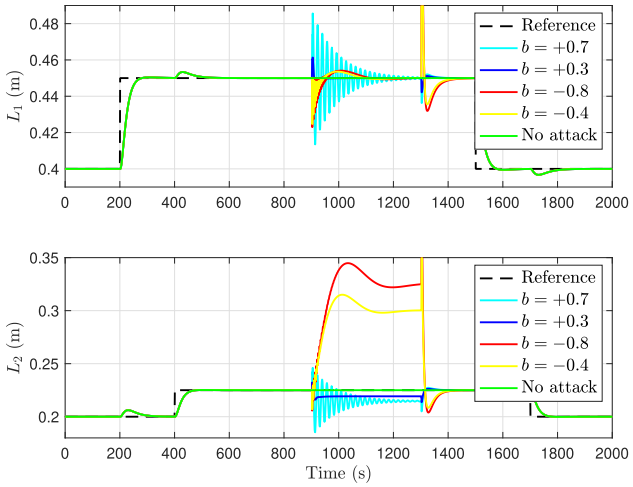

FIGURE 7. Response of the closed-loop control system with multiplicative attacks of magnitude b.

changes in $\mathbf{C}_a$ move the system poles, modifying the system transient response.

Now, in order to see how severe these attacks might be, we decide to mitigate them, if possible.

C. MITIGATION PROCESS

The mitigation process used here is similar to the one proposed in [27] and [31], using a bank of UIOs, and reconfiguring the control signal as in [20]. Below, we describe how to design the UIOs and how to reconstruct the outputs without the effect of the attack.

The j^{th} UIO is designed for a system with a state description as

$$\mathbf{x}[k+1] = \mathbf{A}\,\mathbf{x}[k] + \mathbf{B}\,\tilde{\mathbf{u}}[k] + \mathbf{E}^j\,d^j[k], \tag{39}$$

where vector signal $d^j[k] \in \mathbb{R}$ are disturbances, that in this case represent the effect of the sensor attacks in the state variables, considered different for each UIO; the matrix $\mathbf{E}^j \in \mathbb{R}^{n\times 1}$ represents how the disturbances affect the system. Then, the j^{th} UIO is described using the following state-space equation

$$\begin{aligned}\mathbf{z}^j[k+1] &= \mathbf{F}^j\,\mathbf{z}^j[k] + \mathbf{T}^j\,\mathbf{B}\,\mathbf{u}[k] + \mathbf{K}^j\tilde{\mathbf{y}}_a^j[k],\\ \hat{\mathbf{x}}^j[k+1] &= \mathbf{z}^j[k+1] + \mathbf{H}^j\tilde{\mathbf{y}}_a^j[k+1],\end{aligned} \tag{40}$$

where $\mathbf{z}^j[k] \in \mathbb{R}^n$ is the dynamic (first) approximation of the estimated state vector, $\hat{\mathbf{x}}^j[k] \in \mathbb{R}^n$ is the estimated state vector, which corresponds to the UIO that does not uses the information of the j^{th} output for the estimation process, i.e., $\mathbf{y}_a^j[k]$ is the output vector $\mathbf{y}_a[k]$ where the j^{th} component is eliminated. $\mathbf{F}^j \in \mathbb{R}^{n\times n}$, $\mathbf{T}^j \in \mathbb{R}^{n\times n}$, $\mathbf{K}^j \in \mathbb{R}^{n\times(p-1)}$ and $\mathbf{H}^j \in \mathbb{R}^{n\times(p-1)}$ are design matrices such that the estimated state of the UIO, $\hat{\mathbf{x}}^j[k]$, converges to $\mathbf{x}[k]$ without the attack effect, i.e., $\mathbf{F}_a = \mathbf{0}$, for additive attacks, or $\mathbf{F}_a = \mathbf{0}$, for multiplicative attacks. The j^{th} UIO described by (40).

The design of the j^{th} UIO consists in holding the following equivalences

$$(\mathbf{I} - \mathbf{H}^j\mathbf{C}^j)\,\mathbf{E}^j = \mathbf{0} \tag{41}$$

$$\mathbf{A}_1^j = (\mathbf{I} - \mathbf{H}^j\mathbf{C}^j)\mathbf{A} \tag{42}$$

$$\mathbf{F}^j = \mathbf{A}_1^j - \mathbf{K}_1^j\mathbf{C}^j, \tag{43}$$

$$\mathbf{T}^j = \mathbf{I} - \mathbf{H}^j\mathbf{C}^j, \tag{44}$$

$$\mathbf{K}_2^j = \mathbf{F}^j\mathbf{H}^j, \tag{45}$$

if that is possible, the estimation error will converge to zero and the UIO will estimate the system state.

Attack detection and isolation processes are done as in [20]. Once the attack is detected, the attacked sensor signal is recalculated as

$$\tilde{\mathbf{y}}_r^j[k] = \tilde{\mathbf{y}}^j[k] - \mathbf{m}^j[k]\,\mathbf{a}^j[k], \tag{46}$$

where $\tilde{\mathbf{y}}_r^j[k]$ is the reconstruction of $\mathbf{y}[k]$ without the effect of the attack, where $\mathbf{a}^j[k]$ is a binary signal that indicates whether or not there is an attack on the j^{th} sensor, and

$$\mathbf{m}^j[k] = \mathbf{C}_m^j(\hat{\mathbf{x}}^j[k] - \hat{\mathbf{x}}^i[k]), \qquad i \neq j, \tag{47}$$

where $\mathbf{C}_m^j$ is the j^{th} row of the $\mathbf{C}_m$ matrix, $\hat{\mathbf{x}}^j[k]$ is a state estimation insensitive to disturbances on j^{th} sensor and $\hat{\mathbf{x}}^i[k]$ is a state estimation sensitive to disturbances on all but the i^{th} sensor.

For the case of the three tanks benchmark system, we start with the design of UIOs bank. For UIO1 we have

$$\mathbf{E}^1 = \begin{bmatrix}10^{-4} & 1 & 10^{-4}\end{bmatrix}^\top,$$

in order to decouple the influence of sensor 1 in the system state, to be able to estimate the state only with sensor 2 information. After the decoupling transformation is done on the system, the transformed resulting system turns out to have only one observable mode. Therefore, only one of the close loop UIO1 mode can be located, and we chose to locate it at $p_d = 0.001$. Given that the non observable modes of the UIO are located at 0.9957 and 0.9707, the closed-loops poles of UIO1 will be located at 0.9957, 0.9707 and 0.0010.

Doing something similar for UIO2, we have

$$\mathbf{E}^2 = \begin{bmatrix}1 & 10^{-4} & 10^{-4}\end{bmatrix}^\top.$$

Similar to the case of UIO1, after performing the decoupling transformation, we found again only one observable mode for the resulting system. That mode will be located at $p_d = 0.001$. The remaining non observable modes are located at 0.9667 and 0.9890, since they are inside the unit circle (they are stable) the UIO can be designed. The modes of UIO2 will be located at 0.9667, 0.9890 and 0.0010.

Attack detection and isolation processes are done as mentioned in the previous section. Figures 8 and 9 show the result of mitigate the attacks effects shown in Figures 6 and 7. There, we can see that the attack effect on the system has been reduced. Interestingly enough, for the mitigation of both kinds of attacks we get sort of pulse responses in both sensors; obviously, for positive multiplicative attacks we can

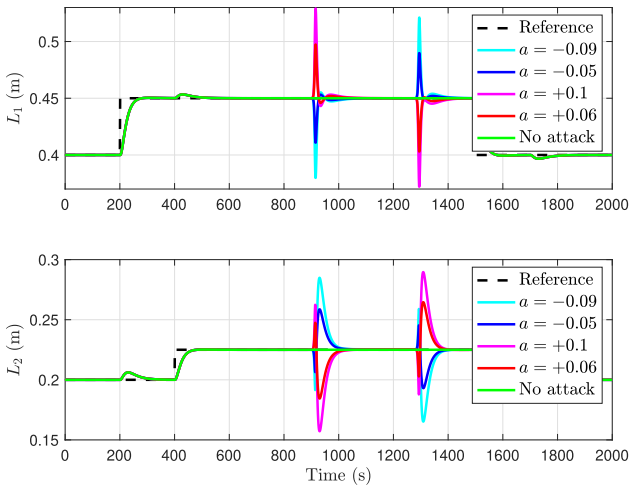

FIGURE 8. Response of the closed-loop control system with mitigated additive attacks of magnitude a.

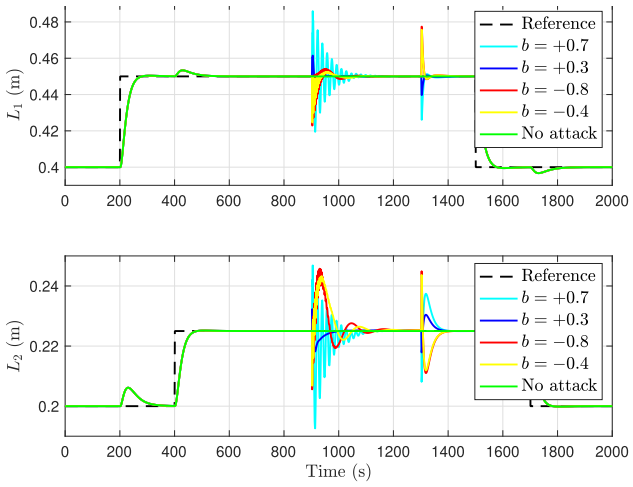

FIGURE 9. Response of the closed-loop control system with mitigated multiplicative attacks of magnitude b.

notice longer oscillations (since it is affecting directly system stability). Also, we can notice that the effect on the non attacked sensor is shorter than for the attacked one, whereas for the additive attacks the mitigated effect lasts almost the same in both sensors, only the magnitude of the overshoot is depending on the magnitude of the attack.

Finally, we show in Figure 10 an attack with magnitude bigger than the stability limit (specifically $b = 0.8$), where we can see classic unstable behavior for the attacked system without mitigation, where there are increasing oscillations up to the system collapses. Notice that, in this case, the mitigation of the attack diminish slightly the oscillations amplitude, allowing the system to work for a little bit longer, but ending up collapsing. In any case, we can see that both kinds of attacks can be mitigated, but in the case of multiplicative attacks the mitigation is only possible when the attack magnitude is inside the range that allows the system to keep stability. All program codes to easily replicate the above numerical results are included as supplementary material of this paper.

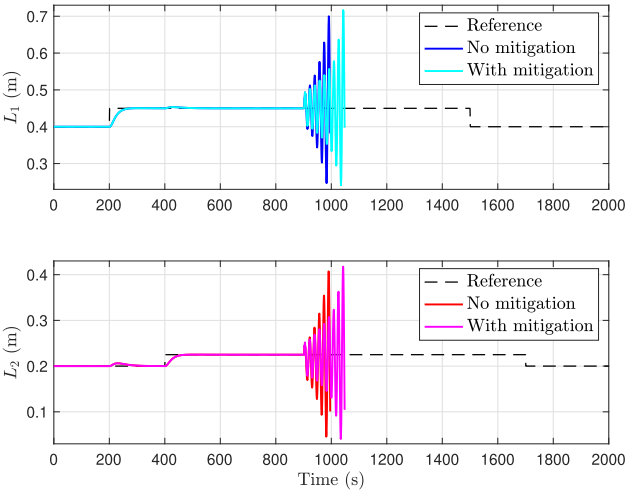

FIGURE 10. Response of the closed-loop control system with multiplicative attack of magnitude $b = 0.8$ with and without mitigation.

VI. CONCLUSION

In this paper, we show that multiplicative attacks, which are very simple, can affect directly the system stability. We use an LMI formulation to calculate a conservative value for the stability bounds. In this sense, we have utilized tools from the robust control to quantify the maximum attack on each sensor, before the system becomes unstable and collapses. If we use the stability bounds of the attack on one output at the time, we can find which output is more vulnerable to attacks, allowing the engineer in charge of the system to decide whether or not a sensor needs redundancy to enhance its resilience to cyber-attacks. Although the method produces conservative values for the maximum attack on each sensor, this result is novel and useful because it allows us to compare the vulnerability of each sensor compared with the other ones in the system. Also, in the simulations, we have shown that this kind of attacks can be mitigated with previous approaches introduced in the literature, but once the attack is big enough to make the system unstable, the system cannot be recovered and the attack cannot be mitigated.

The proposed stability analysis can be used for attacks affecting the system simultaneously, at different times, and in as many outputs as desired. As expected, the more aggressive the scenario the more restrictive the bounds to be found. Also, when analyzing simultaneous attacks, it will be unclear the information about the vulnerability, that we have emphasized in the numerical results shown.

Future work can be addressed on different fronts. The results presented in this work can be extended into the case in which measurement noise is included or, perhaps, to include nonlinear models. Also, it is important to design strategies to defend the most vulnerable system outputs, to avoid the attacker having access to sensor information and being able to perform multiplicative attacks.

APPENDIX A PROOF OF LEMMA 1

Proof (of Lemma 1): Let us start noticing that (17) holds for all $\mathbf{w}$ and that the unit ball in $\mathbb{R}^q$ is compact. Since the left

side of (17) is continuous in $\mathbf{w}$, we can write

$$0 < \eta_1 \triangleq \min \left\{ (\mathbf{w}^\top \mathbf{Y}\, \mathbf{w})^2 - 4\mathbf{w}^\top \mathbf{S}\, \mathbf{w}\, \mathbf{w}^\top \mathbf{Z}\, \mathbf{w} : \; ||\mathbf{w}|| = 1 \right\}.$$

Let η_2 be a positive scalar such that

$$\eta_2^2 + \eta_2 \left(\lambda_{\max}[\mathbf{S}] + \lambda_{\max}[\mathbf{Z}]\right) < \eta_1/8.$$

Since $\lambda_{\max}[\mathbf{S}] + \lambda_{\max}[\mathbf{Z}] \geq 0$, the left hand side of the inequality vanishes for $\eta_2 = 0$ and has a non-negative slope. Therefore, we can conclude that such η_2 exists. Let us define symmetric positive definite matrices

$$\bar{\mathbf{S}} \triangleq \mathbf{S} + \eta_2 \mathbf{I} \quad \textit{and} \quad \bar{\mathbf{Z}} \triangleq \mathbf{Z} + \eta_2 \mathbf{I}.$$

Now, let us show that

$$(\mathbf{w}^\top \mathbf{Y}\, \mathbf{w})^2 - 4\mathbf{w}^\top \mathbf{S}\, \mathbf{w}\, \mathbf{w}^\top \mathbf{Z}\, \mathbf{w} > \mathbf{0} \tag{48}$$

for all $\mathbf{w} \neq \mathbf{0} \in \mathbb{R}^q$.

From the definitions of η_1, $\bar{\mathbf{S}}$ and $\bar{\mathbf{Z}}$, we have

$$\begin{aligned} \eta_1 ||\mathbf{w}||^4 \leq\; & (\mathbf{w}^\top \mathbf{Y}\, \mathbf{w})^2 - 4\mathbf{w}^\top \mathbf{S}\, \mathbf{w}\, \mathbf{w}^\top \mathbf{Z}\, \mathbf{w} \\ =\; & (\mathbf{w}^\top \mathbf{Y}\, \mathbf{w})^2 - 4\mathbf{w}^\top (\mathbf{S} - \eta_2 \mathbf{I})\, \mathbf{w}\, \mathbf{w}^\top (\mathbf{Z} - \eta_2 \mathbf{I})\, \mathbf{w} \\ =\; & (\mathbf{w}^\top \mathbf{Y}\, \mathbf{w})^2 - 4\mathbf{w}^\top \bar{\mathbf{S}}\, \mathbf{w}\, \mathbf{w}^\top \bar{\mathbf{Z}}\, \mathbf{w} \\ & + 4\,\eta_2\, ||\mathbf{w}||^2 (\mathbf{w}^\top \bar{\mathbf{S}}\, \mathbf{w} + \mathbf{w}^\top \bar{\mathbf{Z}}\, \mathbf{w}) + -4\,\eta_2^2\, ||\mathbf{w}||^4, \end{aligned} \tag{49}$$

for all $\mathbf{w} \neq \mathbf{0} \in \mathbb{R}^q$. Using the definition of η_2

$$\begin{aligned} & 4\,\eta_2\, ||\mathbf{w}||^2 (\mathbf{w}^\top \bar{\mathbf{S}}\, \mathbf{w} + \mathbf{w}^\top \bar{\mathbf{Z}}\, \mathbf{w}) \qquad (50) \\ & = 4\,\eta_2\, ||\mathbf{w}||^2 (\mathbf{w}^\top \mathbf{S}\, \mathbf{w} + \mathbf{w}^\top \mathbf{Z}\, \mathbf{w} + 2\,\eta_2\, ||\mathbf{w}||^2) \\ & \leq 4\,\eta_2\, ||\mathbf{w}||^4 \left(\lambda_{\max}[\mathbf{S}] + \lambda_{\max}[\mathbf{Z}] + \eta_2\right) \\ & = 4\,||\mathbf{w}||^4 \left(\eta_2^2 + \eta_2 \left(\lambda_{\max}[\mathbf{S}] + \lambda_{\max}[\mathbf{Z}]\right)\right) \\ & < \frac{\eta_1}{2}\, ||\mathbf{w}||^4. \qquad (51) \end{aligned}$$

From (49) and (51), we conclude that

$$(\mathbf{w}^\top \mathbf{Y}\, \mathbf{w})^2 - 4\mathbf{w}^\top \bar{\mathbf{S}}\, \mathbf{w}\, \mathbf{w}^\top \bar{\mathbf{Z}}\, \mathbf{w} + \frac{\eta_1}{2}\, ||\mathbf{w}||^4 \geq \eta_1\, ||\mathbf{w}||^4.$$

Therefore, (48) holds.

From Theorems (12.5) and (13.1) in [32], we can conclude that $\varepsilon^2 \bar{\mathbf{S}} + \varepsilon\, \mathbf{Y} + \bar{\mathbf{Z}} < \mathbf{0}$ for some $\varepsilon > 0$. As a result, for any $\mathbf{w} \neq 0 \in \mathbb{R}^q$

$$\begin{aligned} 0 >\; & \mathbf{w}^\top (\varepsilon^2 \bar{\mathbf{S}} + \varepsilon\, \mathbf{Y} + \bar{\mathbf{Z}})\, \mathbf{w} \\ =\; & \mathbf{w}^\top (\varepsilon^2 \mathbf{S} + \varepsilon\, \mathbf{Y} + \mathbf{Z})\, \mathbf{w} + 2\,\eta_2\, ||\mathbf{w}||^2 \\ >\; & \mathbf{w}^\top (\varepsilon^2 \mathbf{S} + \varepsilon\, \mathbf{Y} + \mathbf{Z})\, \mathbf{w}. \end{aligned}$$

□

REFERENCES

[1] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proc. 47th Design Autom. Conf.*, 2010, pp. 731–736.

[2] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annu. Rev. Control*, vol. 47, pp. 394–411, Jan. 2019.

[3] D. Ding, Q.-L. Han, Y. Xiang, C. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, Jan. 2018.

[4] Y. Z. Lun, A. D'Innocenzo, F. Smarra, I. Malavolta, and M. D. Di Benedetto, "State of the art of cyber-physical systems security: An automatic control perspective," *J. Syst. Softw.*, vol. 149, pp. 174–216, Mar. 2019.

[5] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo, "Bibliographical review on cyber attacks from a control oriented perspective," *Annu. Rev. Control*, vol. 48, pp. 103–128, Jan. 2019.

[6] M. Kordestani and M. Saif, "Observer-based attack detection and mitigation for cyberphysical systems: A review," *IEEE Syst., Man, Cybern. Mag.*, vol. 7, no. 2, pp. 35–60, Apr. 2021.

[7] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, Jan. 2015.

[8] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.

[9] Y. Mo and B. Sinopoli, "Secure estimation in the presence of integrity attacks," *IEEE Trans. Autom. Control*, vol. 60, no. 4, pp. 1145–1151, Apr. 2015.

[10] Y. H. Chang, Q. Hu, and C. J. Tomlin, "Secure estimation based Kalman filter for cyber–physical systems against sensor attacks," *Automatica*, vol. 95, pp. 399–412, Sep. 2018.

[11] D. Ding, Q.-L. Han, X. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 1, pp. 176–190, Jan. 2021.

[12] M. Krotofil, K. Kursawe, and D. Gollmann, "Securing industrial control systems," in *Security and Privacy Trends in the Industrial Internet of Things*. Cham, Switzerland: Springer, 2019, pp. 3–27.

[13] A. Farraj, E. Hammad, and D. Kundur, "On the impact of cyber attacks on data integrity in storage-based transient stability control," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3322–3333, Dec. 2017.

[14] M. Sahabuddin, B. Dutta, and M. Hassan, "Impact of cyber-attack on isolated power system," in *Proc. 3rd Int. Conf. Electr. Eng. Inf. Commun. Technol. (ICEEICT)*, Sep. 2016, pp. 1–4.

[15] M. Segovia, J. Rubio-Hernan, A. R. Cavalli, and J. Garcia-Alfaro, "Cyber-resilience evaluation of cyber-physical systems," in *Proc. IEEE 19th Int. Symp. Netw. Comput. Appl. (NCA)*, Nov. 2020, pp. 1–8.

[16] M. Wolf and D. Serpanos, "False data injection attacks," in *Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems*. Cham, Switzerland: Springer, 2020, pp. 73–83.

[17] W. Qi, Y. Hou, G. Zong, and C. K. Ahn, "Finite-time event-triggered control for semi-Markovian switching cyber-physical systems with FDI attacks and applications," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 68, no. 6, pp. 2665–2674, Jun. 2021.

[18] J. Wang, C. Yang, J. Xia, Z.-G. Wu, and H. Shen, "Observer-based sliding mode control for networked fuzzy singularly perturbed systems under weighted try-once-discard protocol," *IEEE Trans. Fuzzy Syst.*, early access, Mar. 31, 2021, doi: 10.1109/TFUZZ.2021.3070125.

[19] H. He, W. Qi, Z. Liu, and M. Wang, "Adaptive attack-resilient control for Markov jump system with additive attacks," *Nonlinear Dyn.*, vol. 103, no. 2, pp. 1585–1598, Jan. 2021.

[20] L. F. Combita, A. Cardenas, and N. Quijano, "Mitigating sensor attacks against industrial control systems," *IEEE Access*, vol. 7, pp. 92444–92455, 2019.

[21] G. F. Franklin, M. L. Workman, and D. Powell, *Digital Control of Dynamic Systems*, 3rd ed. Boston, MA, USA: Addison-Wesley, 1997.

[22] K. Ogata, *Discrete-Time Control Systems*. Upper Saddle River, NJ, USA: Prentice-Hall, 1987.

[23] C. L. Phillips and H. T. Nagle, *Digital Control System Analysis and Design*, 3rd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 1995.

[24] X. He, Z. Wang, and D. Zhou, "Robust fault detection for networked systems with communication delay and data missing," *Automatica*, vol. 45, no. 11, pp. 634–639, 2009.

[25] I. R. Petersen and C. V. Hollot, "A Riccati equation approach to the stabilization of uncertain linear systems," *Automatica*, vol. 22, no. 4, pp. 397–411, Jul. 1986.

[26] S. Boyd, L. E. Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory* (Studies in Applied Mathematics). Philadelphia, PA, USA: SIAM, Jun. 1994, vol. 15.

[27] L. F. Cómbita, A. A. Cárdenas, and N. Quijano, "Mitigation of sensor attacks on legacy industrial control systems," in *Proc. IEEE 3rd Colombian Conf. Autom. Control (CCAC)*, Oct. 2017, pp. 1–6.

[28] *Laboratory Setup: Three-Tank System DTS200*, Amira, Duisburg, Germany, 2002.

[29] H. Noura, D. Theilliol, J.-C. Ponsart, and A. Chamseddine, *Fault-Tolerant Control Systems: Design and Practical Applications*. Dordrecht, The Netherlands: Springer, 2009.
[30] P. Van Overschee and B. De Moor, *Subspace Identification for Linear Systems: Theory, Implementation, Applications*. New York, NY, USA: Springer, 1996.
[31] L. F. Combita, J. A. Giraldo, A. A. Cardenas, and N. Quijano, "DDDAS for attack detection and isolation of control systems," in *Handbook of Dynamic Data Driven Applications Systems*. Cham, Switzerland: Springer, 2018, pp. 407–422.
[32] I. Gohberg, P. Lancaster, and L. Rodman, *Matrix Polynomials*. Philadelphia, PA, USA: SIAM, 2009.

LUIS FRANCISCO CÓMBITA (Member, IEEE) received the B.S. degree in electronics engineering from Universidad Distrital Francisco José de Caldas, Bogotá, Colombia, in 1992, and the M.S. and Ph.D. degrees in electrical engineering from the Universidad de los Andes, Bogotá, in 2002 and 2021, respectively. He joined the Engineering Faculty, Universidad Distrital Francisco José de Caldas, as an Auxiliar Professor, in 1997, where he is currently an Assistant Professor. His current research interests include cyber-physical systems security, modeling and simulation of dynamical systems, and industrial control systems.

NICANOR QUIJANO (Senior Member, IEEE) received the B.S. degree in electronics engineering from Pontificia Universidad Javeriana, Bogotá, Colombia, in 1999, and the M.S. and Ph.D. degrees in electrical and computer engineering from The Ohio State University, Columbus, OH, USA, in 2002 and 2006, respectively. He joined the Electrical and Electronics Engineering Department, Universidad de los Andes (UAndes), Bogotá, as an Assistant Professor, in 2007, where he is currently a Full Professor and the Director of the Research Group in Control and Automation Systems. His current research interests include hierarchical and distributed optimization methods using bio-inspired and game-theoretical techniques for dynamic resource allocation problems, especially those in energy, water, and transportation.

ÁLVARO A. CÁRDENAS (Member, IEEE) received the B.S. degree from the Universidad de Los Andes, Colombia, and the M.S. and Ph.D. degrees from the University of Maryland, College Park. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, University of California at Santa Cruz, Santa Cruz. His research interests include cyber-physical systems and the IoT security and privacy, network intrusion detection, and wireless networks.