Computing and Artificial Intelligence 2023; 1(1): 409.
Original Research Article

Advanced nonlinear fuzzy observer and robust control design for systems subject to cyber-physical attacks

Souad Bezzaoucha Rebai

Department of Electrical, Computer Engineering and Automation, EIGSI La Rochelle, MIA Lab., La Rochelle 17041, France; souad.bezzaoucha@eigsi.fr

ARTICLE INFO

Received: 18 October 2023
Accepted: 20 December 2023
Available online: 29 December 2023

doi: 10.59400/cai.v1i1.409

ABSTRACT: In the following contribution, the control design of CPSs (Cyber Physical Systems) usually consists of an observer to estimate the state of the physical system and a controller to compute the control commands based on the state estimation studied. Our objective is to design control methods that are robust against attacks in the model, attenuating their effect and ensuring at the same time a reliable state and attack estimation allowing their detection and isolation while maintaining the system stability, integrity, and performance. The considered approach is based on the Lyapunov theory and LMI resolution approach in order to deduce the observers-controller gains. A robust output H_∞ control and quadratic stabilization for nonlinear systems subject to actuator and sensor data deception attacks (cyber-physical-attacks) is proposed. The detection & identification issues are also reconsidered since the system states and the malicious signals will be reconstructed via a Polytopic-based T-S (Takagi-Sugeno) observer. An innovative design method where the attacked system is presented as an uncertain one subject to external disturbances is developed. A robust polytopic state feedback stabilizing controller based on a polytopic observer with disturbances attenuation for the resulting uncertain system is considered. To illustrate our proposed approach, we present a numerical example. An algorithm based on a robust polytopic controller ensuring asymptotic stability despite data deception attacks and external perturbations attenuation guaranteed by the H_∞ norm will be given. Indeed, a PDC (Parallel Distributed Compensation) controller coupled with a polytopic observer to estimate the unmeasurable state variables and actuator/sensor attack signals will be designed for nonlinear systems subjected to data deception attacks.

KEYWORDS: polytopic fuzzy representation; cyber-physical-systems; state and attack reconstruction; robust stabilizing control; disturbances attenuation

1. Introduction

In recent years, many scholars have presented reliable control strategies against various cyberattacks, such as false data injection attacks, time-delay switch attacks, and denial-of-service attacks. Indeed, since there are numerous physical sensors, complex interaction mechanisms, and massive signals, the security of cyber-physical systems (CPSs) is inevitably threatened. In order to tackle these threats, we need advances in detection, feedback control, and estimation with built-in resilience to cyber-attacks, to maintain system integrity and reliability at all times, by providing uninterrupted, equipment-safe, and controlled operation.

The development of control and estimation algorithms resistant to faults and failures is a longstanding challenge. In fault detection and isolation, the goal is to identify one or more components that have malfunctioned within a system. Conventionally, this involves comparing sensor measurements with a model and generating what is known as a residual signal. The resulting signal is subsequently examined to ascertain the occurrence of a fault. One of the interesting approaches, based on both model-based, nonlinear modeling, robust control, and state and unknown parameters estimation, isolation, and reconstruction is the so-called polytopic one. This approach is the one to be considered in the following contribution.

This class of systems can indeed represent numerous nonlinear systems. Furthermore, it shows in the technical development similarities with the well-studied linear models where it extends existing results established for linear systems into the nonlinear domain.

2. Literature review

Cyber-Physical security extends beyond the scope of cyber-security, offering an additional layer of defense. As an extension of the previous contribution[1], where an event-based approach was considered; in the following paper, a robust control design is developed by applying a fuzzy robust control and attack resilient estimation algorithm for nonlinear system stabilization. Indeed, neutralizing attacks through resilient estimation and control enhances the system's ability to withstand damage and sustain operation, even in the presence of adversarial threats. The domain of cyber-security and resilience encompasses various stages, including detection (discerning if an attack has occurred), isolation (identifying the elements under attack, such as sensors, actuators, or control nodes), identification/estimation, and resilience[2].

In order to tackle this threat, we need advances in detection, feedback control, and estimation with built-in resilience to cyber-attacks, to maintain system integrity and reliability at all times, by providing uninterrupted, equipment-safe, and controlled operation[2,3].

Numerous approaches for detecting attacks found in the literature rely on classical fault detection techniques[4–9]. Viewed from a physical process standpoint, cyber-attacks can be perceived as stealthy and malicious disturbances. Addressing cyber-physical attacks requires surpassing traditional methods derived from fault diagnosis such that novel techniques become imperative to handle attacks that appear in mathematical models. Consequently, to overcome the conservative mathematical conditions, there is a growing interest in merging advanced nonlinear approaches with conventional control theory-based techniques; this method is gaining a lot of interest as a promising approach and interesting solution.

Applying robust control and attack-resilient estimation algorithms seems to be of great interest in recent research. Indeed, Zhu et al.[10] considered an L2 state estimation issue for a class of discrete time-invariant systems subjected to both randomly occurring switching topologies and deception attacks over wireless sensor networks. Lu et al.[11] tried to compensate DoS attacks and save network bandwidth resources by combining event triggered mechanisms and the Lyapunov function method. Zhu and Basar[12] proposed a set of coupled optimality criteria for a holistic robust and resilient design for cyber physical systems with an application to power systems. A model-based approach coupled with deep neural network was also proposed by Moazeni and Khazaei[13] where a cyberattack detection procedure was applied on the tank's level measurements of a water distribution system.

Developing control and estimation algorithms resilient against faults and failures is a well-established challenge. In fault detection and isolation, the goal is to identify if one or more components of a system have failed. Conventionally, this involves comparing sensor measurements with an analytical model of the system and generating a residual signal. This residual signal is then analyzed in order to determine if a fault has occurred.

Nevertheless, in these algorithms, typically, there is one residual signal per failure mode. In certain problem formulations, the number of failure modes can be extensive, making it impractical to generate and analyze a residual signal for each possible failure mode[13]. For instance, in a study by Bezzaoucha Rebai[14], a novel detection criterion based on state residuals, utilizing real-time observed state data, was applied to an intelligent transportation system. To expedite detection, an adaptive detection threshold was introduced to replace the pre-existing computed threshold.

One of the interesting approaches, based on both model-based, nonlinear modeling, robust control, and state and unknown parameters estimation, isolation, and reconstruction is the so-called polytopic one. This approach is the one to be considered in the following contribution.

To address challenges introduced by various nonlinearities, such as time-varying parameters, saturation, hysteresis, and sine and cosine functions, among others, the concept behind Fuzzy Takagi-Sugeno Polytopic models is to extend the well-established linear results/approaches into the nonlinear domain. The polypotic Takagi-Sugeno approach was already applied for state and stealthy attack estimation[1,14–16]. In the present contribution, as a natural extension of research work, the robust control side will be considered.

Impact and contribution

The present article addresses the stability, estimation, and control aspects of cyber-physical systems subject to false-data injection attacks from a pure automation and control point of view. The proposed approach is based on the so-called Model-based Attack Detection Identification and Isolation strategy, which incorporates a system model in the processes of detecting, isolating, and identifying.

In the following paper, the control design of CPSs computing the control commands based on the state estimation is studied. Our objective is to design control methods that are robust against attacks in the model, attenuating their effect and ensuring at the same time a reliable state and attack estimation allowing their detection and isolation while maintaining the system stability, integrity, and performance. The considered approach is based on the Lyapunov theory and LMI resolution approach in order to deduce the observers-controller gains. A robust output H_∞ control and quadratic stabilization for nonlinear systems subject to actuator and sensor data deception attacks (cyber-physical-attacks) is proposed. The detection & identification issues are also reconsidered since the system states and the malicious signals will be reconstructed via a Polytopic-based T-S (Takagi-Sugeno) observer. An innovative design method where the attacked system is presented as an uncertain one subject to external disturbances is developed. A robust polytopic state feedback stabilizing controller based on a polytopic observer with disturbances attenuation for the resulting uncertain system is considered.

The paper is organized as follows: After a brief introduction with a short literature review of related works and impact and contribution sections, presented in section 1; the Polytopic representation is applied to the malicious attacks, the system modeling with the actuator and sensor data deception attacks, followed by the uncertain system representation are then detailed respectively in section 2, i.e., Materials and Methods. Section 3 is about the main Results of the following paper, presenting the robust output

H∞ observe-based T-S controller. Sections 4 and 5 are about the approach illustration through a numerical example, discussion, and conclusion.

3. Materials and methods

The design of control and estimation algorithms resilient to faults and failures is an important challenge in control engineering. In prior works, Teixeira et al.[19] and Oudghiri et al.[20] delved into fault detection and identification, focusing on detecting component failures by comparing measured output signals with expected ones. In our current study, our objective goes beyond mere detection; we aim to not only identify attacks but crucially to estimate them. This estimation is used for fault/attack-tolerant control design that is robust and stable. Without effective detection and estimation strategies, attacks can lead to undesirable consequences, potentially harming the physical plant.

We focus in this paper on deception attacks or false-data injection attacks. In control systems, various types of detectors can be developed to defend against such malicious attacks. Here, we aim to adapt the approach developed by Bezzaoucha et al.[16] to achieve an exact and simultaneous reconstruction of both the system state and the time-varying attack signal.

In our scenario, we assume that the attacker manipulates the gains of the sensors and/or actuators in the control system, constituting the injection of false information from sensors or controllers. Mathematically, explicit equations for both sensor and actuator signal attacks are derived, representing time-varying multiplicative faults/attacks. The Polytopic T-S approach is then employed to achieve real-time reconstruction of these signals.

3.1. Polytopic modeling of attacked systems

Let us consider the nonlinear system described by Equation (1), wherein the vector of time-varying parameters is denoted as $\theta(t)$, $\theta(t) \in \mathbb{R}^n$ is defined by $\theta(t) = \begin{pmatrix} \theta^u(t) \\ \theta^y(t) \end{pmatrix}$ where $\theta^u(t) \in \mathbb{R}^{n_{\theta_u}}$ and $\theta^y(t) \in \mathbb{R}^{n_{\theta_y}}$ correspond respectively to the actuator and sensor attacks ($n = n_{\theta_u} + n_{\theta_y}$). Denoting $x(t) \in \mathbb{R}^{n_x}$, $y(t) \in \mathbb{R}^m$ and $u(t) \in \mathbb{R}^{n_u}$ as the system state, output, and control, respectively. The nonlinear system is characterized by a Polytopic representation with r sub-models. This representation can be readily obtained using the Sector Nonlinearity Transformation (SNT). The formulation of System (1) is as follows:

$$\begin{cases} \dot{x}(t) & = & \sum_{i=1}^{r} \mu_i\left(x(t)\right)\left(A_i x(t) + \mathcal{B}_i u(t)\right) \\ y(t) & = & C(t)x(t) \end{cases} \tag{1}$$

with the time-varying matrices $B_i(t)$ and $C(t)$ defined by follow:

$$\begin{cases} B_i(t) = B_i + \sum_{j=1}^{n_{\theta_u}} \theta_j^u(t)\overline{B}_{ij} \\ C(t) = \left(I_m + F(t)\right)C \end{cases} \tag{2}$$

s.t. B_i, $\overline{B}_{ij}$ are constant matrices and $\theta_j^u(t)$ time-varying unknown parameters corresponding to the multiplicative actuator attacks. $F(t) = diag(\theta^y(t)) \in \mathbb{R}^{m \times m}$ is defined by:

$$F(t) = \sum_{j=1}^{n_{\theta_y}} \theta_j^y(t) F_j \tag{3}$$

$diag(\theta^y(t))$ corresponds to a diagonal matrix with the terms $\theta_j^y(t)$ (sensor attacks) on its diagonal with $n_{\theta_y} = m$ and F_j matrices of dimension $\mathbb{R}^{m\times m}$ and where the element of coordinate (i, i) is equal to 1 and 0 elsewhere, i.e.,

$$F_j = \begin{pmatrix} 1 & 0 & 0 \\ \vdots & 1 & \vdots \\ 0 & \dots & 1 \end{pmatrix} \tag{4}$$

3.2. Polytopic representation of malicious attacks

The actuator data deception, or false data injection are modeled thanks to the time-varying parameters $\theta_j^u(t)$. These attacks are of course unknown but bounded $\theta_j^u(t) \in \left[\theta_j^{2^u}, \theta_j^{1^u}\right]$, with supposed known limits. From the SNT transformation, the $\theta_j^u(t)$ are rewritten as:

$$\theta_j^u(t) = \tilde{\mu}_j^1\left(\theta_j^u(t)\right)\theta_j^{1^u} + \tilde{\mu}_j^2\left(\theta_j^u(t)\right)\theta_j^{2^u} \tag{5}$$

with

$$\begin{aligned} \tilde{\mu}_j^1\left(\theta_j^u(t)\right) &= \frac{\theta_j^u(t) - \theta_j^{2^u}}{\theta_j^{1u} - \theta_j^{2u}} \\ \tilde{\mu}_j^2\left(\theta_j^u(t)\right) &= \frac{\theta_j^{1^u} - \theta_j^u(t)}{\theta_j^{1u} - \theta_j^{2u}} \\ \tilde{\mu}_j^1\left(\theta_j^u(t)\right) + \tilde{\mu}_j^2\left(\theta_j^u(t)\right) &= 1,\ \forall t \end{aligned} \tag{6}$$

In a similar manner $\theta_j^y(t)$ is expressed as:

$$\theta_j^y(t) = \bar{\mu}_j^1\left(\theta_j^y(t)\right)\theta_j^{1^y} + \bar{\mu}_j^2\left(\theta_j^y(t)\right)\theta_j^{2^y} \tag{7}$$

with

$$\begin{aligned} \tilde{\mu}_j^1\left(\theta_j^y(t)\right) &= \frac{\theta_j^y(t) - \theta_j^{2^y}}{\theta_j^{1^y} - \theta_j^{2y}} \\ \tilde{\mu}_j^2\left(\theta_j^y(t)\right) &= \frac{\theta_j^{1^y} - \theta_j^y(t)}{\theta_j^{1^y} - \theta_j^{2y}} \\ \tilde{\mu}_j^1\left(\theta_j^u(t)\right) + \tilde{\mu}_j^2\left(\theta_j^u(t)\right) &= 1,\ \forall t \end{aligned} \tag{8}$$

Replacing (5) and (7) in (2), we obtain:

$$\begin{cases} B_i(t) = B_i + \displaystyle\sum_{j=1}^{n_{\theta_u}} \sum_{k=1}^{2} \tilde{\mu}_j^k\left(\theta_j(t)\right)\theta_j^{k^u}\overline{B}_{ij} \\ C(t) = \left(I + \displaystyle\sum_{j=1}^{n_{\theta_y}} \sum_{k=1}^{2} \bar{\mu}_j^k\left(\theta_j^y(t)\right)\theta_j^{k^y} F_j\right) C \end{cases} \tag{9}$$

3.3. Polytopic representation of physical plant subjected to data deception attacks

To ensure uniform weighting functions, and to express $C(t)$ as a straightforward polytopic matrix, we leverage the convex sum property of $\tilde{\mu}_j\left(\theta_j^u(t)\right)$ and $\overline{\mu}_j\left(\theta_j^y(t)\right)$ of each parameter $\theta_j^u(t)$ and $\theta_j^y(t)$. Consequently, Equation (9) is reformulated as:

$$\begin{aligned} B_i(t) &= B_i + \sum_{j:1}^{2^{n_{\theta_u}}} \tilde{\mu}_j\big(\theta^u(t)\big)\bar{B}_{i_j} \\ C(t) &= \left(I + \sum_{j=1}^{2^{n_{\theta^y}}} \bar{\mu}j^{(\theta^y(t))\bar{F}_J} \right) C \end{aligned} \qquad (10)$$

with

$$\begin{cases} \widetilde{\mu_J}\big(\theta^u(t)\big) = \prod_{k=1}^{n_{\theta_u}} \tilde{\mu}_k^{\sigma_j^k}\left(\theta_k^u(t)\right) \\ \overline{\mathcal{B}}_{ij} = \sum_{k=1}^{n_{\theta_u}} \theta_k^{u\sigma_j^k}\,\overline{B}_{ik} \end{cases} \qquad (11)$$

and

$$\begin{cases} \overline{\mu_j}\big(\theta^y(t)\big) = \prod_{k=1}^{n_{\theta_y}} \overline{\mu}_k^{\sigma_j^k}\left(\theta_k^y(t)\right) \\ \overline{F}_j = \sum_{k=1}^{n_{\theta_y}} \theta_k^{y\sigma_j^k}\,F_j \end{cases} \qquad (12)$$

where the global weighting functions $\widetilde{\mu_J}\big(\theta^u(t)\big)$ and $\overline{\mu_j}\big(\theta^y(t)\big)$ satisfy the convex sum property where indices are expressed by:

$$j{=}2n\theta u{-}1\sigma j1{+}2n\theta u{-}2\sigma j2{+}\ldots{+}20\sigma jn\theta u{-}(21{+}22{+}\ldots{+}2n\theta u{-}1) \qquad (13)$$

for the actuator, and for the sensor.

$$j = 2^{n_{\theta y}-1}\sigma_j^1 + 2^{n_{\theta y}-2}\sigma_j^2 + \cdots + 2^0\sigma_j^{n_{\theta y}} - (2^1 + 2^2 + \cdots + 2^{n_{\theta y}-1}) \qquad (14)$$

Finally, using Equations (10), the nonlinear LPV system (1) becomes:

$$\begin{cases} \dot{x}(t) &= \sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}} \mu_i\left(x(t)\right)\widetilde{\mu_J}\big(\theta^u(t)\big)\left(A_i x(t) + \mathcal{B}_{ij}u(t)\right) \\ y(t) &= \sum_{k=1}^{2^{n_{\theta_y}}} \overline{\mu_k}\left(\theta^y(t)\right)\tilde{C}_k x(t) \end{cases} \qquad (15)$$

$$\begin{aligned} \mathcal{B}_{ij} &= B_i + \overline{\mathcal{B}}_{ij} \\ \tilde{C}_k &= C + \overline{F}_k C \end{aligned} \qquad (16)$$

3.4. Uncertain system representation

Utilizing Equation (15), we formulate a state and actuator/sensor data deception observer. Employing an $\mathcal{L}_2$ attenuation approach, our objective is to minimize the impact of attacks on both the state and the estimation error of malicious inputs.

The considered observer is described by:

$$\begin{cases} \dot{\hat{x}}(t) = \sum_{i=1}^{r} \sum_{j=1}^{2^{n_{\theta_u}}} \mu_i(\hat{x}(t))\tilde{\mu_J}\left(\widehat{\theta^u}(t)\right) \\ \qquad \left(A_i x(t) + \mathcal{B}_{ij}u(t) + L_{ij}(y(t) - \hat{y}(t))\right) \\ \dot{\widehat{\theta^u}}(t) = \sum_{i=1}^{r} \sum_{j=1}^{2^{n_{\theta_u}}} \mu_i(\hat{x}(t))\tilde{\mu_J}\left(\widehat{\theta^u}(t)\right) \\ \qquad \left(K_{ij}^u(y(t) - \hat{y}(t)) - \alpha_{ij}^u \hat{\theta}^u(t)\right) \\ \dot{\widehat{\theta^y}}(t) = \sum_{i=1}^{r} \sum_{k=1}^{2^{n_{\theta_y}}} \mu_i\,(\hat{x}(t))\overline{\mu_k}\left(\widehat{\theta^y}(t)\right) \\ \qquad \left(K_{ik}^y(y(t) - \hat{y}(t)) - \alpha_{ik}^y \widehat{\theta^y}(t)\right) \\ \hat{y}(t) = \sum_{k=1}^{2^{n_{\theta_y}}} \overline{\mu_k}\left(\widehat{\theta^y}(t)\right) \tilde{C}_k \hat{x}(t) \end{cases} \tag{17}$$

where $L_{ij} \in \mathbb{R}^{n_x \times m}$, $K_{ij}^u \in \mathbb{R}^{n \times m}$, $\alpha_{ij}^u \in \mathbb{R}^{n \times n}$, $K_{ik}^y \in \mathbb{R}^{m \times m}$ and $\alpha_{ik}^y \in \mathbb{R}^{m \times m}$ are the observer gains to be calculated, ensuring at the same time the state and attacks estimation (convergence to zero of the estimation errors) and robust control constraints (to be developed in details in the following section). Let's establish the errors in state and data deception estimation as follows: $e_x(t)$, $e_{\theta^u}(t)$ and $e_{\theta^y}(t)$ as:

$$\begin{gathered} e_x(t) = x(t) - \hat{x}(t) \\ e_{\theta^u}(t) = \theta^u(t) - \hat{\theta}^u(t) \\ e_{\theta^y}(t) = \theta^y(t) - \hat{\theta}^y(t) \end{gathered} \tag{18}$$

The system Equation (15) are reformulated to facilitate the computation of the dynamics of estimation errors. The modified representation is as follows:

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^{r} \sum_{j=1}^{2^{n_{\theta_u}}} [\,\mu_i(\hat{x}(t))\tilde{\mu_J}\left(\widehat{\theta^u}(t)\right)\left(A_i x(t) + \mathcal{B}_{ij}u(t)\right) + \\ \qquad \delta_{ij}(t)\left(A_i x(t) + \mathcal{B}_{ij}u(t)\right)] \\ y(t) = \sum_{k=1}^{2^{n_{\theta_y}}} \left[\overline{\mu_k}\left(\widehat{\theta^y}(t)\right)\tilde{C}_k x(t) + \overline{\delta_k}(t)\tilde{C}_k x(t)\right] \end{cases} \tag{19}$$

with $\delta_{ij}(t)$ and $\overline{\delta_k}(t)$ are defined by the following equations:

$$\delta_{ij}(t) = \mu_i(x(t))\tilde{\mu_J}(\theta^u(t)) - \mu_i(\hat{x}(t))\tilde{\mu_J}\left(\widehat{\theta^u}(t)\right) \tag{20}$$

$$\overline{\delta_k}(t) = \overline{\mu_k}(\theta^y(t)) - \overline{\mu_k}\left(\widehat{\theta^y}(t)\right) \tag{21}$$

and satisfying:

$$-1 \le \delta_{ij}(t) \le 1, -1 \le \overline{\delta_k}(t) \le 1 \tag{22}$$

Let us define now:

$$\varDelta A(t) = \sum_{i=1}^{r} \sum_{j=1}^{2^{n_{\theta u}}} \delta\, ij(t) A_i = \mathcal{A}\varSigma(t) E_A \tag{23}$$

$$\varDelta B(t) = \sum_{i=1}^{r} \sum_{j=1}^{2^{n_{\theta u}}} \delta_{ij}\,(t) \mathcal{B}_{ij} = \mathcal{B}\varSigma(t) E_B \tag{24}$$

$$\varDelta C(t) = \sum_{k=1}^{2^{n_{\theta y}}} \overline{\delta_k}\,(t) \tilde{C}_k = \mathcal{C}\bar{\varSigma}(t) E_C \tag{25}$$

with

$$\mathcal{A} = \begin{bmatrix} A_1 & \dots & A_1 & \dots & A_r & \dots & A_r \\ & \underbrace{}_{2^{n_{\theta u}}times} & & & & \underbrace{}_{2^{n_{\theta u}}times} & \end{bmatrix} \tag{26}$$

$$\mathcal{B} = [\mathcal{B}_{11} \quad \dots \quad \mathcal{B}_{r2^n}] \tag{27}$$

$$\sum(t) = diag(\delta_{11}(t), \dots, \delta_{r2^n}(t)) \tag{28}$$

$$\bar{\varSigma}(t) = diag\left(\bar{\delta}_2(t), \cdots, \overline{\delta_{2^{n_{\theta y}}}}(t)\right) \tag{29}$$

$$\begin{gathered} E_A = [I_{n_x} \quad \dots \quad I_{n_x}]^T,\ E_B = [I_{n_u} \quad \dots \quad I_{n_u}]^T \\ E_C = \left[I_{2^{n_{\theta y}}} \quad \dots \quad I_{2^{n_{\theta y}}}\right]^T = [I_{2^m} \quad \dots \quad I_{2^m}]^T \end{gathered} \tag{30}$$

Thanks to (22) and definitions (29), we have:

$$\varSigma^T(t)\varSigma(t) \leq I, \quad \bar{\varSigma}^T(t)\bar{\varSigma}(t) \leq I \tag{31}$$

Using the above definitions (23)–(30), system (19) is then written as an uncertain system given by:

$$\begin{cases} \dot{x}(t) = \displaystyle\sum_{i=1}^{r} \sum_{j=1}^{2^{n_{\theta u}}} \mu_i\left(\hat{x}(t)\right)\widetilde{\mu_J}\left(\widehat{\theta^u}(t)\right) \\ \qquad \left(\left(A_i + \varDelta A(t)\right)x(t) + \left(\mathcal{B}_{ij} + \varDelta B(t)\right)u(t)\right) \\ y(t) = \displaystyle\sum_{k=1}^{2^{n_{\theta y}}} \overline{\mu_k}\left(\widehat{\theta^y}(t)\right)\left(\tilde{C}_k + \varDelta C(t)\right)x(t) \end{cases} \tag{32}$$

4. Results: Robust polytopic H_∞ T-S control

Herein, we shall propose an algorithm in order to calculate the considered observer and controller gains ensuring the fulfillment of the following conditions:

- The system described by Equation (32) attains asymptotic stability despite data deception attacks.
- External perturbations attenuation guaranteed by the H_∞ norm. In other words, the goal is to find an observer Equation (17) and a Parallel Distributed Compensation (PDC) controller Equation (33) for a given scalar $\gamma > 0$ s.t. attenuation condition Equation (40) is met. The resulting conditions to be solved will be detailed in Lemma II.

For the nonlinear system subjected to data deception attacks Equation (1), employing the polytopic observer to estimate the unmeasurable state variables and actuator/sensor attack signals, as detailed in Equation (17); we define the PDC (Parallel Distributed Compensation) controller as follows:

$$u(t) = -\sum_{l=1}^{r} h_l\left(\hat{x}(t)\right)\Omega_l \hat{x}(t) \tag{33}$$

Let us first express the estimation errors dynamics. From Equations (32) and (18), the estimation errors dynamics are then given by:

$$\begin{cases} \dot{e}_x(t) = \displaystyle\sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}\sum_{k=1}^{2^{n_{\theta_y}}}\sum_{l=1}^{r} \\ \quad \mu_i\left(\hat{x}(t)\right)\widetilde{\mu_j}\left(\widehat{\theta^u}(t)\right)\overline{\mu_k}\left(\widehat{\theta^y}(t)\right)\mu_l\left(\hat{x}(t)\right) \\ \quad \left(\left(A_i - L_{ij}\tilde{C}_k + \Delta B(t)\Omega_l\right)e_x(t)\right. \\ \quad \left. + \left(\Delta A(t) - \Delta B(t)\Omega_l - L_{ij}\Delta C(t)\right)x(t)\right) \\ \dot{e}_{\theta^u}(t) = \displaystyle\sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}\sum_{k=1}^{2^{n_{\theta_y}}} \mu_i\left(\hat{x}(t)\right)\widetilde{\mu_j}\left(\widehat{\theta^u}(t)\right)\overline{\mu_k}\left(\widehat{\theta^y}(t)\right) \\ \quad \left(-K_{ij}^u\tilde{C}_k e_x(t) - \alpha_{ij}^u e_{\theta^u}(t)\right. \\ \quad \left. - K_{ij}^u \Delta C(t)x(t) + \alpha_{ij}^u\theta^u(t) + \dot{\theta}^u(t)\right) \\ \dot{e}_{\theta^y}(t) = \displaystyle\sum_{i=1}^{r}\sum_{k=1}^{2^{n_{\theta_y}}} \mu_i\left(\hat{x}(t)\right)\overline{\mu_k}\left(\widehat{\theta^y}(t)\right) \\ \quad \left(-K_{ik}^y\tilde{C}_k e_x(t) - \alpha_{ik}^y e_{\theta^y}(t)\right. \\ \quad \left. - K_{ik}^y \Delta C(t)x(t) + \alpha_{ik}^y\theta^y(t) + \dot{\theta}^y(t)\right) \end{cases} \tag{34}$$

By Equations (32), (17) and (34), the following uncertain system with bounded external disturbances is obtained:

$$\begin{aligned} \dot{x}_a(t) = & \sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}\sum_{k=1}^{2^{n_{\theta_y}}}\sum_{l=1}^{r} \\ & \mu_i\left(\hat{x}(t)\right)\widetilde{\mu_j}\left(\widehat{\theta^u}(t)\right)\overline{\mu_k}\left(\widehat{\theta^y}(t)\right)\mu_l\left(\hat{x}(t)\right) \\ & \left(\Phi_{ijkl}x_a(t) + \Psi_{ijk}\omega(t)\right) \end{aligned} \tag{35}$$

where $x_a(t) = \begin{pmatrix} x(t) & e_x(t) & e_\theta^u(t) & e_\theta^y(t) \end{pmatrix}^T$ is the extended state vector and $\omega(t) = (\theta^u(t) \quad \dot{\theta}^u(t) \quad \theta^y(t) \quad \dot{\theta}^y(t))^T$ the exogenous input (attack signals and their derivatives), supposed unknown but bounded. Matrices Φ_{ijkl} and Ψ_{ijk} are defined as follows:

$$\Phi_{ijk} = \begin{pmatrix} \Phi_{ijkl}^1 & \left(\mathcal{B}_{ij} + \Delta B(t)\right)\Omega_l & 0 & 0 \\ \Delta A(t) - \Delta B(t)\Omega_l - L_{ij}\Delta C(t) & A_i - L_{ij}\tilde{C}_k + \Delta B(t)\Omega_l & -K_{ij}^u\tilde{C}_k & 0 \\ -K_{ij}^u\Delta C(t) & -K_{ij}C & -\alpha_{ij}^u & 0 \\ -K_{ik}^y\Delta C(t) & -K_{ik}^y\tilde{C}_k & 0 & -\alpha_{ik}^y \end{pmatrix} \tag{36}$$

with $\Phi_{ijkl}^1 = A_i - \mathcal{B}_{ij}\Omega_l + \Delta A(t) - \Delta B(t)\Omega_l$ and

$$\Psi_{ijk} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \alpha_{ij}^{u} & I & 0 & 0 \\ 0 & 0 & \alpha_{ik}^{y} & I \end{pmatrix} \tag{37}$$

From Equation (35) and the nominal system output (without sensor data deception attack, i.e. $y_n(t) = Cx(t)$), the resulting closed-loop system becomes:

$$\begin{pmatrix} \dot{x}_a(t) \\ y_n(t) \end{pmatrix} = \sum_{i=1}^{r} \sum_{j=1}^{2^{n_{\theta_u}}} \sum_{k=1}^{2^{n_{\theta_y}}} \sum_{l=1}^{r} \mu_i(\hat{x}(t))\widetilde{\mu_j}\left(\widehat{\theta^u}(t)\right)\overline{\mu_k}\left(\widehat{\theta^y}(t)\right)\mu_l(\hat{x}(t)) \begin{pmatrix} \Phi_{ijkl} & \Psi_{ijk} \\ \overline{C} & 0 \end{pmatrix}\begin{pmatrix} x_a(t) \\ \omega(t) \end{pmatrix} \tag{38}$$

s.t.

$$y_n(t) = Cx(t) = (C \quad 0 \quad 0 \quad 0)x_a(t) = \overline{C}x_a(t) \tag{39}$$

Let us remember the following definition and lemmas:

Definition 1. For a positive scalar γ, the system Equation (38) is said to be stable with desired H_∞ attenuation level γ if it is exponentially stable with:

$$\int_{\infty}^{0}\{\left(y_n^T(t)\right)_\infty\left(y_n(t)\right)_\infty - \gamma^2\omega^T(t)\omega(t)\}dt < 0 \tag{40}$$

Lemma I. From the Lyapunov theory, the system (18) is stable with an H_∞ disturbance attenuation γ if there exists a positive symmetric matrix $P = P^T > 0$ s.t.

$$\begin{bmatrix} \Phi_{ijkl}^T P + P\Phi_{ijkl} & P\Psi_{ijk} & \overline{C}^T \\ * & -\gamma^2 I & 0 \\ * & * & -I \end{bmatrix} < 0 \; i,l = 1,\dots,r, j = 1,\dots,2^{n_{\theta_u}}, k = 1,\dots,2^{n_{\theta_y}} \tag{41}$$

In order to relax conditions given in Lemma I, the following formulation is given:

Lemma II. For a given positive scalar γ, if there exist matrices P, Z_{ijkl}, where $P = P^T > 0$ and $Z_{ljki} = Z_{ijkl}^T$, $i \neq k$, $i,l = 1,\dots,r, j = 1,\dots,2^{n_{\theta_u}}, k = 1,\dots,2^{n_{\theta_y}}$ fulfilling the matrix inequalities (42)-(43)-(44), then, the controller Equation (33) makes the H_∞ norm of polytopic system Equation (38) under attenuation level γ.

$$\begin{bmatrix} \Phi_{ijki}^T P + P\Phi_{ijki} & P\Psi_{ijk} \\ * & -\gamma^2 I \end{bmatrix} < Z_{ijki}; i,l = 1,\dots,r, j = 1,\dots,2^{n_{\theta_u}}, k = 1,\dots,2^{n_{\theta_y}} \tag{42}$$

$$\begin{bmatrix} (*)^T P + P\left(\Phi_{ijkl} + \Phi_{ljki}\right) & 2P\Psi_{ijk} \\ * & 2\Psi_{ijk}^T P \end{bmatrix} < Z_{ijkl} + Z_{ljki}; i \neq l, j = 1,\dots,2^{n_{\theta_u}}, k = 1,\dots,2^{n_{\theta_y}} \tag{43}$$

$$\begin{bmatrix} Z_{1jk1} & \cdots & Z_{1jkr} & \overline{C}^T \\ \vdots & \ddots & \vdots & \vdots \\ Z_{rjk1} & \cdots & Z_{rjkr} & \overline{C}^T \\ \overline{C} & \cdots & \overline{C} & -I \end{bmatrix}_{j=1,\dots,2^{n_{\theta_u}}, k=1,\dots,2^{n_{\theta_y}}} < 0 \tag{44}$$

Lemma III: Consider two matrices X and Y with appropriate dimensions, a time-varying matrice

$\Delta(t)$ and a positive scalar ε. The following property is verified:

$$X^T\Delta^T(t)Y + Y^T\Delta(t)X \leq \varepsilon X^T X + \varepsilon^{-1}Y^T Y \tag{45}$$

for $\Delta^T(t)\Delta(t) \leq I$.

Replacing Φ_{ijkl} and Ψ_{ijk} by their expressions, the obtained constraints can be easily solved using convex optimization tools and/or the use of a dedicated resolution tool for bilinear constraints like the PenBMI Matlab toolbox. In the study by Kocvara and Stingl[21,22] we can find some examples.

Calculation details

In the following, a detailed calculation procedure is given in order to solve the matrix inequalities (41–43). For simplicity reasons, let us consider the case where the system is subject to a single actuator attack (i.e., $y(t) = Cx(t)$ and $n_{\theta_y} = 1$). The obtained uncertain system with bounded external disturbances is given by:

$$\dot{x}_a(t) = \sum_{i=1}^{r}\sum_{j=1}^{2}\sum_{k=1}^{r} h_i(\hat{x})\mu_j\left(\widehat{a^u}\right)h_k(\hat{x})\left(\Phi_{ijk}x_a(t) + \Psi_{ij}\omega(t)\right) \tag{46}$$

s.t. $x_a(t) = (x(t) \quad e_x(t) \quad e_{a^u}(t))^T$ and $\omega(t) = (a^u(t) \quad \dot{a^u}(t))^T$. Matrices Φ_{ijk} and Ψ_{ij} are defined as follows:

$$\Phi_{ijk} = \begin{pmatrix} \Phi_{ijk}^1 & \left(\mathcal{B}_{ij} + \Delta B(t)\right)\Omega_k & 0 \\ \Delta A(t) - \Delta B(t)\Omega_k & A_i - L_{ij}C & 0 \\ 0 & -K_{ij}C & -\alpha_{ij}^u \end{pmatrix} \tag{47}$$

with $\Phi_{ijk}^1 = A_i - \mathcal{B}_{ij}\Omega_k + \Delta A(t) - \Delta B(t)\Omega_k$ and

$$\Psi_{ij} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ \alpha_{ij}^u & I \end{pmatrix} \tag{48}$$

Let us now detail the stability condition given by Lemma 1 for this system, i.e.,

$$\begin{bmatrix} \Phi_{ijk}^T P + P\Phi_{ijk} & P\Psi_{ij} & \overline{C}^T \\ * & -\gamma^2 I & 0 \\ * & * & -I \end{bmatrix}_{i,k=1,\ldots,r,j=1,2} < 0 \tag{49}$$

In order to solve this constraint, each term will be replaced by its expression and then we will separate the constant and the time-varying terms. The last one, based on the convex sum property, will be bounded; this will allow to solve the matrix inequalities using the tools mentioned above.

Based on definitions, Equations (47) and (48), and considering the matrix P as a diagonal one (i.e., $P = \begin{pmatrix} P_1 & 0 & 0 \\ 0 & P_2 & 0 \\ 0 & 0 & P_3 \end{pmatrix}$, where P_1, P_2 and P_3 are positive symmetric matrix), the constraint Equation (49) is rewritten as:

$$Qijk+Qkt+QkTt<0, i,k=1,\ldots,r,j=1,2 \tag{50}$$

where Q_{ijk} is given by:

$$Q_{ijk} = \begin{pmatrix} Q_{ijk}^{1} & P_1\mathcal{B}_{ij}\Omega_k & 0 & 0 & 0 & C \\ * & Q_{ij}^{2} & -C^T K_{ij}^T P_3 & 0 & 0 & 0 \\ * & * & -2\alpha_{ij}P_3 & P_3\alpha_{ij} & P_3 & 0 \\ * & * & * & -\gamma^2 I & 0 & 0 \\ * & * & * & * & -\gamma^2 I & 0 \\ * & * & * & * & * & -I \end{pmatrix} \tag{51}$$

with $Q_{ijk}^1 = P_1A_i - P_1\mathcal{B}_{ij}\Omega_k + A_i^TP_1 - \Omega_k^T\mathcal{B}_{ij}^TP_1$ and $Q_{ij}^2 = P_2A_i - P_2L_{ij}C + A_2^TP_2 - C^TL_{ij}^TP_2$ Based on Equations (23), (24) and (25), $\mathcal{Q}_k(t)$ is rewritten as:

$$\begin{aligned} \mathcal{Q}_k(t) = (\mathcal{A}^TP_1 \quad \mathcal{A}^TP_2 \quad 0 \quad 0 \quad 0 \quad 0)^T\Sigma(t)(E_A \quad 0 \quad 0 \quad 0 \quad 0 \quad 0) \\ +(\mathcal{B}^TP_1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0)^T\Sigma(t)(-E_B\Sigma_k \quad -E_B\Sigma_k \quad 0 \quad 0 \quad 0 \quad 0) \\ +(0 \quad \mathcal{B}^TP_2 \quad 0 \quad 0 \quad 0 \quad 0)^T\Sigma(t)(-E_B\Sigma_k \quad 0 \quad 0 \quad 0 \quad 0 \quad 0) \end{aligned} \tag{52}$$

Based on property (31) and lemma 3, $\mathcal{Q}_k(t) + \mathcal{Q}_k^T(t)$ is bounded as the following:

$$\mathcal{Q}_k(t) + \mathcal{Q}_k^T(t) < \begin{pmatrix} \mathcal{Q}_1 & \mathcal{Q}_3 & 0 & 0 & 0 & 0 \\ \mathcal{Q}_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{53}$$

with $\mathcal{Q}_1 = \varepsilon_{A1}^{-1}P_1\mathcal{A}\mathcal{A}^TP_1 + \varepsilon_{A1}E_A^TE_A + \varepsilon_{B1}^{-1}P_1\mathcal{B}\mathcal{B}^TP_1 + \varepsilon_{B1}\Omega_k^TE_B^TE_B\Omega_k + \varepsilon_{A2}E_A^TE_A + \varepsilon_{B1}^{-1}P_1\mathcal{B}\mathcal{B}^TP_1 + \varepsilon_{B2}\Omega_k^TE_B^TE_B\Omega_k$, $\mathcal{Q}_2 = \varepsilon_{A2}^{-1}P_2\mathcal{A}\mathcal{A}^TP_2 + \varepsilon_{B2}^{-1}P_2\mathcal{B}\mathcal{B}^TP_2$, and $\mathcal{Q}_3 = \varepsilon_{B1}\Omega_k^TE_B^TE_B\Omega_k$. Applying now Schur's complement with adequate change of variables, constraints (41), (42) and (43) will be easily solved using the tools (PenBMI) presented above.

5. Discussion: Numerical simulation

In the subsequent sections, the presented approach is employed on a fundamental model of a biological wastewater treatment plant. The mathematical model is defined by two state variables, $x_1(t)$ and $x_2(t)$, corresponding to the biomass and substrate concentrations, respectively. The input $u(t)$ signifies the dwell time in the treatment plant, while the measured output is the biomass concentration ($y(t) = x_1(t)$).

5.1. LPV representation of the process

As a preliminary step, we express the nonlinear system Equations (54) in a polytopic form. As presented by Zhou and Khargonekar[18], and with specific assumptions in place, certain simplifications allow us to represent the nonlinear model as follows:

$$\begin{cases} \dot{x}_1(t) = \dfrac{ax_1(t)x_2(t)}{x_2(t)+b} - x_1(t)u(t) \\ \\ \dot{x}_2(t) = -\dfrac{cax_1(t)x_2(t)}{x_2(t)+b} + \big(d - x_2(t)\big)u(t) \end{cases} \tag{54}$$

where a, b, c and d are known parameters. Let us define:

$$\rho_1(t) = -u(t), \quad \rho_2(t) = \frac{ax_1(t)}{x_2(t)+b} \tag{55}$$

From Equations (54) and (55), the quasi-LPV system Equation (56) is deduced:

$$\dot{x}(t) = \begin{pmatrix} \rho_{1(t)} & \rho_2(t) \\ o & -c\rho_2(t) + \rho_1(t) \end{pmatrix} x(t) + \begin{pmatrix} 0 \\ d \end{pmatrix} u(t) \tag{56}$$

Given that a Linear Parameter-Varying (LPV) representation is derived within a compact set of the state space, we can determine the maximum and minimum values of the terms $\rho_1(t)$ and $\rho_2(t)$ based on knowledge of the domain of variation of $u(t)$, Specifically, $\rho_1(t) \in [-1, -0.2]$ and $\rho_2(t) \in [0.004,15]$. By applying the convex polytopic transformation, two partitions are defined for each premise variable:

$$\begin{cases} \rho_1(t) = \varrho_{11}(\rho_1)\rho_1^2 + \varrho_{12}(\rho_1)\rho_1^1 \\ \rho_2(t) = \varrho_{21}(\rho_2)\rho_2^2 + \varrho_{22}(\rho_2)\rho_2^1 \end{cases} \tag{57}$$

with

$$\begin{gathered} \varrho_{11}(\rho_1) = \frac{\rho_1(t) - \rho_1^2}{\rho_1^1 - \rho_1^2}, \ \varrho_{12}(\rho_1) = \frac{\rho_1^1 - \rho_1(t)}{\rho_1^1 - \rho_1^2} \\ \varrho_{21}(\rho_2) = \frac{\rho_2(t) - \rho_2^2}{\rho_2^1 - \rho_2^2}, \ \varrho_{22}(\rho_2) = \frac{\rho_2^1 - \rho_2(t)}{\rho_2^1 - \rho_2^2} \end{gathered} \tag{58}$$

where the scalars ρ_1^1, ρ_1^2, ρ_2^1 and ρ_2^2 are defined as

$$\begin{gathered} \rho_1^1 = \max_u \rho_1(t), \ \rho_1^2 = \min_u \rho_1(t) \\ \rho_2^1 = \max_x \rho_2(t), \ \rho_2^2 = \min_x \rho_2(t) \end{gathered} \tag{59}$$

The sub-models are characterized by the sets (A_i, B_i, C) with $i = 1,2,3,4$. Utilizing the definitions of ρ_1 and ρ_2, all the B_i matrices are set to $B = [0 \quad d]^T$. The output matrix $C = [1 \quad 0]$ and the matrices A_i are expressed as:

$$A_1 = \begin{pmatrix} \rho_1^1 & \rho_2^1 \\ 0 & -c\rho_2^1 + \rho_1^1 \end{pmatrix}, \ A_2 = \begin{pmatrix} \rho_1^1 & \rho_2^2 \\ 0 & -c\rho_2^2 + \rho_1^1 \end{pmatrix}$$

$$A_3 = \begin{pmatrix} \rho_1^2 & \rho_2^1 \\ 0 & -c\rho_2^1 + \rho_1^2 \end{pmatrix}, \ A_4 = \begin{pmatrix} \rho_1^2 & \rho_2^2 \\ 0 & -c\rho_2^2 + \rho_1^2 \end{pmatrix}$$

The weighting functions $\mu_i(t)$ are defined by the following equations:

$$\begin{gathered} \mu_{1(t)} = g_{11}\big(\rho_1(t)\big)g_{21}\big(\rho_2(t)\big) \big| \mu_{2(t)} = g_{11}\big(\rho_1(t)\big)g_{22}\big(\rho_2(t)\big) \\ \mu_{3(t)} = g_{12}\big(\rho_1(t)\big)g_{21}\big(\rho_2(t)\big) \big| \mu_{4(t)} = g_{12}\big(\rho_1(t)\big)g_{22}\big(\rho_2(t)\big) \end{gathered} \tag{60}$$

5.2. Date deception attacks representation on the actuator/sensor

Two categories of data deception attacks are considered, specifically attacks targeting actuators and sensors. Mathematically, these attacks are assumed to be modeled as bounded multiplicative actuator and sensor time-varying faults.

In the considered example, it is presumed that the parameter d is susceptible to hacking. This actuator attack is represented by $d(t)$, such that:

$$d(t) = d + \Delta d(t) \tag{61}$$

It can alternatively be expressed as:

$$d(t) = d + \theta^u(t)\overline{d}, \quad \theta^u(t) \in \left[\theta^{u2}, \theta^{u1}\right] \tag{62}$$

with $d = 2.5$, $\overline{d} = 2.1$ and $\theta^{u2} = -0.1958, \theta^{u1} = 0.1979$. Parameters a, b, c have been identified and set to $a = 0.5$, $b = 0.07$ and $c = 0.7$. Regarding the actuator attack, the polytopic representation of the input matrix B is subsequently expressed through two sub-models, as follows:

$$B_1 = B + \theta^{u1}\overline{B}, \quad B_2 = B + \theta^{u2}\overline{B} \tag{63}$$

where is defined by $\overline{B} := [0 \quad \overline{d}]^T$. The weighting functions $\widetilde{\mu_j}(\theta^u(t))$ are defined as given in Equations (6) and (11).

Now, in the case of a sensor attack, we assume that a bounded multiplicative sensor fault $\theta^y(t)$ influences the output $y(t)$, such that:

$$y(t) = \left(1 + \theta^y(t)\right)x_1(t) \tag{64}$$

As previously explained, $\theta^y(t)$ can also be written as:

$$\theta^y(t) = \overline{\mu}_1{}^1\left(\theta^y(t)\right)\theta^{y1} + \overline{\mu}_1^2\left(\theta^y(t)\right)\theta^{y2},\ \theta^y(t) \in \left[\theta^{y2}, \theta^{y1}\right] \tag{65}$$

with $\theta^{y2} = 0.125, \theta^{y1} = 0.625$, $\overline{\mu}_1{}^1\left(\theta^y(t)\right)$ and $\overline{\mu}_1^2\left(\theta^y(t)\right)$ are defined by Equations (8) and (12). The polytopic form of the output is then given by:

$$y(t) = \sum_{k=1}^{2} \overline{\mu}_k\left(\theta^y(t)\right)\tilde{C}_k x(t) \tag{66}$$

with $\tilde{C}_1 = (1 + \theta^{y2} \quad 0)$, $\tilde{C}_2 = (1 + \theta^{y1} \quad 0)$.

5.3. Simulation results

In the given example, incorporating both actuator and sensor attacks and applying the proposed approach by solving Theorem 1, a simultaneous state and attacks observer is formulated. The initial conditions for the system are taken as $x(0) = (0.1 \quad 1.5)$, and for its observer $\hat{x}(0) = (0.09 \quad 2.3)$. For both attacks, the initial conditions are set to zero, i.e $\hat{\theta}^u(0) = 0$ and $\hat{\theta}^y(0) = 0$.

The state vector, its estimate, and the data deception attack along with their estimates are illustrated in **Figures 1** and **2**, respectively. The plots demonstrate the efficacy of the proposed observer; both system states and the time-varying multiplicative actuator/sensor attacks are accurately estimated, ensuring system stability and attenuating the effects of attacks.

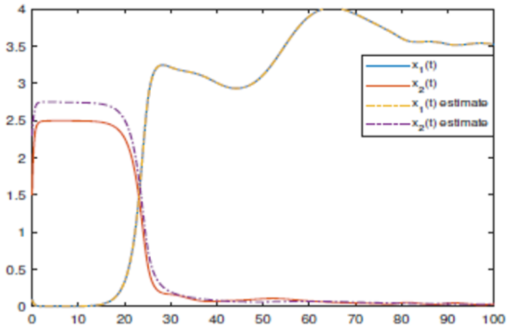

Figure 1. System states and their estimates.

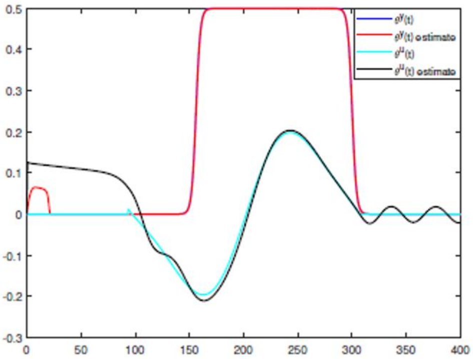

Figure 2. Data deception attacks and their estimates.

6. Conclusion

In the presented contribution, a robust control and quadratic stabilization for nonlinear systems subject to actuator and sensor data deception attacks (cyber-physical-attacks) has been proposed. A new design method based on the rewritten of the attacked system as an uncertain one subject to external disturbances was detailed. Robust polytopic state feedback stabilizing controller based on polytopic observer with disturbance attenuation for the obtained uncertain system was applied. The considered approach gives both controller and observer gain on a single step design and presents less conservative stability conditions than usual approaches. The obtained results are promising and as perspective research work would be on a concrete system (cyber-physical-plant) application.

Conflict of interest

The author declares no conflict of interest.

References

1. Bezzaoucha Rebai S. *A Cyber-Security Contribution to Estimation and Event-Based Control Scheduling Co-Design for Polytopic and T-S Fuzzy Models Using a Lyapunov Approach*. Springer Nature; 2022.
2. Wang R, Sun Q, Ma D, Hu X. Line impedance cooperative stability region identification method for grid-tied inverters under weak grids. *IEEE Transactions on Smart Grid* 2020; 11(4): 2856–2866.
3. Housh M, Kadosh N, Haddad J. Detecting and localizing cyber-physical attacks in water distribution systems without records of labeled attacks. *Sensors* 2022; 22(16): 6035. doi: 10.3390/s22166035
4. Taheri M, Khorasani K, Shames I, Meskin N. Cyber attack and machine induced fault detection and isolation methodologies for cyber-physical systems. *arXiv* 2009; arXiv:2009.06196. doi: 10.48550/arXiv.2009.06196
5. Ye L, Zhu F, Zhang J. Sensor attack detection and isolation based on sliding mode observer for cyber-physical systems. *International Journal of Adaptive Control and Signal Processing* 2020; 34(4): 469–483.
6. Zhang X, Zhu F. Observer-based sensor attack diagnosis for cyber-physical systems via zonotope theory. *Asian Journal of Control* 2020.
7. Karimipour H, Leung H. Relaxation based anomaly detection in cyber-physical systems using ensemble Kalman filter. *IET Cyber-Physical Systems: Theory & Applications* 2019; 5(1): 49–58.
8. Li Q, Bu B, Zhao J. A novel hierarchical situation awarness model for CBTC using SVD entropy and GRU with PRD algorithms. *IEEE Access* 2021.
9. Lukens JM, Passian A, Yoginath S, et al. Bayesian estimation of oscillator parameters: Toward anomaly detection and cyber-physical system security. *Sensors* 2022; 22(16): 6112. doi: 10.3390/s22166112
10. Zhu F, Liu X, Wen J, et al. Distributed robust filtering for wireless sensor networks with markov switching topologies and deception attacks. *Sensors* 2020; 20(7): 1948. doi: 10.3390/s20071948
11. Lu W, Yin X, Fu Y, et al. Observer-based event-triggered predictive control for networked control systems under dos attacks. *Sensors* 2020; 20(23): 6866. doi: 10.3390/s20236866
12. Zhu Q, Basar T. Robust and resilient control design for cyber-physical systems with an application to power systems. In: Proceedings of the 50th IEEE Conference on Decision and Control and European Control

Conference (CDC-ECC); 12–15 December 2011; Orlando, FL, USA.

13. Moazeni F, Khazaei J. Detection of random false data injection cyberattacks in smart water systems using optimized deep neural networks. *Energies* 2022; 15(13): 4832. doi: 10.3390/en15134832
14. Bezzaoucha Rebai S. A cyber-security contribution: Estimation and event-based control scheduling co-design for polytopic & t-s models. In: Proceedings of the 2021 International Conference on Fuzzy Theory and Its Applications (Ifuzzy 2021); 5–8 October 2021; Taitung, Taiwan.
15. Bezzaoucha Rebai S, Voos H. Simultaneous State and False-Data Injection Attacks Reconstruction for NonLinear Systems: An LPV Approach. In: Proceedings of the 2019 3rd International Conference on Automation, Control and Robots; 11–13 October 2019; Prague, Czech Republic.
16. Bezzaoucha S, Marx B, Maquin D, Ragot J. Nonlinear joint state and parameter estimation: Application to a wastewater treatment plant. *Control Engineering Practice* 2013; 21(10): 1377–1385.
17. Blanke M, Kinnaert M, Lunze J, Staroswiecki M. *Diagnosis and Fault-Tolerant Control*. Springer-Verlag; 2003.
18. Zhou K, Khargonekar P. Robust stabilization of linear systems with norm-bounded time-varying uncertainty Control. *Systems and Control Letters* 1988; 10(1): 17–20.
19. Teixeira A, Pérez D, Sandberg H, Johansson K. Attack models and scenarios for networked control systems. In: Proceedings of the 1st International Conference on High Confidence Networked Systems; 17–18 April 2012; Beijing, China.
20. Oudghiri M, Chadli M, El Hajjaji A. One step procedure for robust output fuzzy control. In: Proceedings of the 2007 Mediterranean Conference on Control & Automation; 27–29 June 2007; Athens, Greece. pp. 1–6. doi: 10.1109/MED.2007.4433964
21. Kocvara M, Stingl M. PENNON—A code for convex nonlinear and semidefinite programming. *Optimization Methods and Software* 2003; 18(3): 317–333.
22. Kocvara M, Stingl M. PENBMI, Version 2.0, 2004. Available online: www.penopt.com for a free developer version (accessed on 2 June 2023).