Simultaneous State and False-Data Injection Attacks Reconstruction for NonLinear Systems: an LPV Approach

Souad BEZZAOUCHA REBAI*
Automatic Control Research Group-SnT
University of Luxembourg
29 Av J.F Kennedy L-1855, Luxembourg
phone: (+352) 46 66 44-57 75
souad.bezzaoucha@uni.lu

Holger VOOS
Automatic Control Research Group-SnT
University of Luxembourg
29 Av J.F Kennedy L-1855, Luxembourg
phone: (+352) 46 66 44 -58 10
holger.voos@uni.lu

ABSTRACT

The present contribution addresses simultaneous state and actuator/sensor false-data injection attacks reconstruction for nonlinear systems. The considered actuator/sensor attacks are modeled as time-varying parameters with a multiplicative effect on the actuator input signal and the sensor output signal, respectively. Based on the sector non-linearity approach and the convex polytopic transformation, the nonlinear model is written in a Linear Parameter-Varying (LPV) form, then an observer allowing both state and attack reconstruction is designed by solving an $\mathcal{LMI}$ optimization problem.

Sensors and actuators

CCS Concepts

•Computer systems organization → Embedded and cyber-physical systems;

Keywords

Observer design; State and attack reconstruction; LPV systems; $\mathcal{LMI}$ optimization problem.

1. INTRODUCTION

The isolation and reconstruction of Cyber-attacks, as well as the design of attack-resilient control are currently the focus of many industrial and academic research projects. Indeed, due to the connectivity of modern physical systems, they are more and more subject to malicious intrusions and attacks. In addition to the classical IT approach in order to cope with cyber-attacks, a pure control approach can also be applied. Different approaches have been investigated, as for instance we can cite [14], [5], [1] and [12]. In this case, the attacks can be modeled as an adversary signals (i.e. like disturbances, unknown inputs, faults,...) introduced via the the internal network by hackers and affecting the sensors and/or actuators data [13], [17]. The control signal is then designed in order to detect, identify and possibly counteract malicious cyber-attacks by triggering the activation of adaptive, attack-tolerant control laws [9], [5], [15].

Even if a considerable amount of results are available in the linear framework, it is well established that the linearity assumption is only valid around an operating point; consequently, the natural nonlinear behaviors of the system inevitably affect the performances of the control laws or supervision modules designed with the system linearity assumption. In order to enhance the system performances, it is necessary to take into account the nonlinear behaviors of the system from the modeling task to the control or diagnosis implementation. This can result in complex models to be dealt with, requiring heavy mathematical tools. That is why, a common strategy to deal with complex problems would be to divide them into smaller and simpler one (also known *divide & conquer*). Based on this idea, the so-called Polytopic representation, also known as multiple-models approach or Takagi-Sugeno (T-S) model is of an unquestionable interest. Indeed, substituting the non-linear parts by locally valid set of linear sub models will lead to a simple enough system, easily understood and more convenient to study [18].

The complexity of nonlinear systems leads to consider some specific and conservative assumptions in order to be able to establish some results. One major reason would be the diversity of their nonlinearities, that does not allow to have a generic and unique representation; Indeed, often we have to deal with complex study case which imply to use a different tool for each of them. That is why, the polytopic writing represents an interesting alternative for the nonlinear framework, thanks to a unique writing, that allows us to represent a large category of nonlinearties. A unified representation of the system, including the model nonlinearities, as well as the control constraints and observer design is obtained. Another key point of this representation, is that we can, thanks to some mathematical manipulation, transpose some well-known results of the linear framework to the nonlinear one.

For nonlinear systems, only few contributions that are dealing with the state and attack reconstruction problem can be found [10], [8] and [11]. Indeed, as it was developed in previous contribution [4], this approach provides an alternative and attractive path to deal with complex nonlinear systems and to obtain an equivalent representation by bounding

*Corresponding author

ACM ISBN 978-1-4503-7288-6/19/10…15.00
DOI: https://doi.org/10.1145/3365265.3365280

the parameters and using the well known sector nonlinearity transformation (SNT).

1.1 Contributions and Outline

In this contribution, we propose to use previously developed approach, applied for joint state and time-varying parameters estimation of Takagi-Sugeno models in order to reconstruct the state and cyber-attack signals for nonlinear LPV systems.
Indeed, based on [2] and [3], we will use the proposed decomposition and the proposed strategy in the case of false-data injection attacks on actuators and sensors. The considered actuator/sensor attacks are modeled as time-varying parameters with multiplicative effect on the actuator input signal and sensor output signal, respectively. Based on the sector non-linearity writing, and using the convex property, the nonlinear model will be presented in a Linear Parameter-Varying (LPV) form, then an observer allowing both state and attack reconstruction is designed by solving a $\mathcal{LMI}$ optimization problem.
In the following contribution, the problem of secure state estimation for nonlinear systems, i.e. state reconstruction in the presence of faults and attacks is considered. Based on the decomposition developed in [2] and [3], the special case of false-data injection attacks on actuators and sensors is considered by modeling them as time-varying parameters with multiplicative effect on the actuator input signal and sensor output signal, respectively.
The present contribution is organized as follows. After a brief introduction and a short overview of related works in section I, the problem statement is detailed in section II by the presentation of the Polytopic modeling of time-varying nonlinear systems and time-varying parameters (malicious attacks) with a LPV model of physical plant under data deception attacks. In section III the main result/contribution of this work is given in terms of a general theorem for the observer design strategy. In section IV, an illustrative example is developed. From a basic nonlinear model of a biological waste-water treatment plant, the proposed approach is applied and illustrated with simulations. Conclusion will be given in the last section.

2. PROBLEM STATEMENT

The problem of state reconstruction in the presence of faults and attacks, also denoted as secure state estimation, has recently attracted considerable attention from the control community. The problem of reconstructing the state under actuator/sensor attacks is closely related to fault-detection and fault-tolerant state reconstruction. Based on the approach presented in previous works [2], [3] and adapted to the cyber-security problem, we address the design of observers that can accurately reconstruct the state and attacks of a cyber-physical system under physical faults and actuator/sensor attacks.
For that, we propose a simultaneous state and time-varying (attacks) observers for nonlinear systems in the presence of corrupted inputs and measurements, more specifically, the so-called false-data injection attacks. In the spirit of a Luenberger observer, a state and attacks reconstruction algorithm is proposed based on the $\mathcal{LMI}$ approach and convex optimization problem.

2.1 False-Data Injection Attacks on Actuators/Sensors

Faults and failures resilient control and estimation algorithms design represent a common problem in control engineering. In [6] and [19] for example, the authors investigated the fault-detection and identification problem where the objective is to detect if one or more of the components of a system has failed based on the residual signals obtained by comparing the measured output signal and the measured ones. In the present work, our aim is not only to detect the attacks, but more importantly, to estimate them in order to design afterwords a robust and stable fault/attack tolerant control. Indeed, in the absence of appropriate detection and estimation strategies, attacks may lead to unwanted consequences, such as damaging the physical plant.
In this paper, we focus on the attacks that aim at compromising the integrity of the system, often referred to as deception attacks or false-data injection attacks. In control systems, in order to defend against these malicious attacks, different types of detectors may be developed [17], [7]. Among existing results in the literature, the most commonly used approach is to design a state estimator, and detect the attack based on the estimation residue, i.e., the difference between the measurement data and the estimator output. However, even if residual gives good results for the fault/attack detection, only few approaches give an estimation or exact reconstruction, online, of the attack signal. For this reason, we would like to adapt the previously developed approach in [2], [3] in order to obtain an exact and simultaneous reconstruction of the state and the time-varying attack signal.
In the current paper, we assume that the attacker modifies the gain/s of the sensor and/or the actuator of the control system, which represent the injection of false information from sensors or controllers. Mathematically speaking, explicit equations of both sensor and actuator signal attacks are derived and represented as time-varying multiplicative actuator/sensor faults/attacks. The Polytopic T-S approach is then used to reconstruct these signals in real-time.
In this section, we assume that a malicious third party wants to compromise the integrity of the system. The attacker is assumed to have the following capabilities:

- It knows the system model, i.e. we assume that the hacker knows the system model and matrices.
- It can control the readings of the sensors and the actuators, i.e. modifies their values.
- The intrusions are represented as time-varying multiplicative actuator/sensor faults/attacks. The attacks signal are, of course, unknown, but bounded. Their min and max values are supposed to be known. Indeed, this assumption is not that conservative since we suppose that if the boundaries are exceeded the attacks effect will be too obvious and easily detectable. Meaning, the hacker should respect the min and max values to a certain extend if he/she wants to remain undetectable.

2.2 Polytopic Modeling of Time-Varying Nonlinear Systems

Let us consider the nonlinear system represented by equation (1) where the time-varying parameters vector $\theta(t)$, $\theta(t) \in \mathbb{R}^n$

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 ($n = n_{\theta_u} + n_{\theta_y}$). $x(t) \in \mathbb{R}^{n_x}$, $y(t) \in \mathbb{R}^m$ and $u(t) \in \mathbb{R}^{n_u}$ correspond respectively to the system state, output and control. The nonlinear system is modeled thanks to a Polytopic representation with r sub-models. This representation may be obtained in a straightforward way by applying the Sector Nonlinearity Transformation (SNT). The interested readers can refer to [2] and [16] for more calculation details.
System (1) is defined by:

$$\begin{cases} \dot{x}(t) &= \sum_{i=1}^{r} \mu_i(x(t))(A_i x(t) + B_i(t)u(t)) \\ y(t) &= C(t)x(t) \end{cases} \quad (1)$$

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

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

s.t. B_i, $\overline{B}_{ij}$ are constant matrices with appropriate dimensions and $\theta_j^u(t)$ time-varying unknown parameters and correspond to the multiplicative actuator attacks.
The matrix $F(t) \in \mathbb{R}^{m \times m}$ is defined by:

$$F(t) = \text{diag}(\theta^y(t)) \quad (3)$$

s.t. $\text{diag}(\theta^y(t))$ corresponds to a diagonal matrix with the terms $\theta_j^y(t)$ (sensor attacks) on its diagonal. $F(t)$ may be expressed as

$$F(t) = \sum_{j=1}^{n_{\theta_y}} \theta_j^y(t) F_j \quad (4)$$

with $n_{\theta_y} = m$, F_j are matrices of dimension $\mathbb{R}^{m \times m}$ and where the element of coordinate (i, i) is equal to 1 and 0 elsewhere. The coordinate i corresponds to the number of the attacked sensor. The terms $\theta_j^y(t)$ are time-varying unknown parameters and represent the multiplicative sensor attacks.

2.3 Polytopic Modeling of Time-Varying Parameters (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 $\theta_j^u(t) \in [\theta_j^{2u}, \theta_j^{1u}]$, with supposed known limits. Applying the SNT transformation, each parameter $\theta_j^u(t)$ can always be expressed as:

$$\theta_j^u(t) = \widetilde{\mu}_j^1(\theta_j^u(t))\theta_j^{1u} + \widetilde{\mu}_j^2(\theta_j^u(t))\theta_j^{2u} \quad (5)$$

with

$$\begin{cases} \widetilde{\mu}_j^1(\theta_j^u(t)) &= \dfrac{\theta_j^u(t) - \theta_j^{2u}}{\theta_j^{1u} - \theta_j^{2u}} \\ \widetilde{\mu}_j^2(\theta_j^u(t)) &= \dfrac{\theta_j^{1u} - \theta_j(t)}{\theta_j^{1u} - \theta_j^{2u}} \end{cases} \quad (6)$$

$$\widetilde{\mu}_j^1(\theta_j^u(t)) + \widetilde{\mu}_j^2(\theta_j^u(t)) = 1, \ \forall t$$

Based on the same reflexion, the sensor data deception, or false data injection are modeled thanks to the time-varying parameters $\theta_j^y(t)$, such that:

$$\theta_j^y(t) = \overline{\mu}_j^1(\theta_j^y(t))\theta_j^{1y} + \overline{\mu}_j^2(\theta_j^y(t))\theta_j^{2y} \quad (7)$$

with

$$\begin{cases} \overline{\mu}_j^1(\theta_j^y(t)) &= \dfrac{\theta_j^y(t) - \theta_j^{2y}}{\theta_j^{1y} - \theta_j^{2y}} \\ \overline{\mu}_j^2(\theta_j^y(t)) &= \dfrac{\theta_j^{1y} - \theta_j(t)}{\theta_j^{1y} - \theta_j^{2y}} \end{cases} \quad (8)$$

$$\overline{\mu}_j^1(\theta_j^y(t)) + \overline{\mu}_j^2(\theta_j^y(t)) = 1, \ \forall t$$

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

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

2.4 LPV Model of Physical Plant Under Data Deception Attacks

In order to have the same weighting functions for all the time-varying matrices $B_i(t)$, and write $C(t)$ as a simple polytopic matrix, exploiting the convex sum property of the weighting functions $\widetilde{\mu}_j(\theta_j^u(t))$ and $\overline{\mu}_j(\theta_j^y(t))$ of each parameter $\theta_j^u(t)$ and $\theta_j^y(t)$ (see [2] for calculation details), (9) is written as:

$$\begin{cases} B_i(t) &= \sum_{j=1}^{n_{\theta_u}} \left[\left[(\widetilde{\mu}_j^1(\theta_j^u(t))\theta_j^{1u} + \widetilde{\mu}_j^2(\theta_j^u(t))\theta_j^{2u})\overline{B}_{ij} \right] \right] \times \\ & \qquad \left[\prod_{\substack{k=1 \\ k \neq j}}^{n_{\theta_u}} \sum_{m=1}^{2} \widetilde{\mu}_k^m(\theta_k^u(t)) \right] + B_i \\ &= B_i + \sum_{j=1}^{2^{n_{\theta_u}}} \widetilde{\mu_j}(\theta^u(t))\overline{\mathcal{B}}_{ij} \\ C(t) &= \left(I + \sum_{j=1}^{2^{n_{\theta_y}}} \overline{\mu_j}(\theta^y(t))\overline{F}_j \right) C \end{cases} \quad (10)$$

with

$$\begin{cases} \widetilde{\mu_j}(\theta^u(t)) = \prod_{k=1}^{n_{\theta_u}} \widetilde{\mu}_k^{\sigma_j^k}(\theta_k^u(t)) \\ \overline{\mathcal{B}}_{ij} = \sum_{k=1}^{n_{\theta_u}} \theta_k^{u\sigma_j^k} \overline{B}_{ik} \end{cases} \quad (11)$$

and

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

where the global weighting functions $\widetilde{\mu_j}(\theta^u(t))$ and $\overline{\mu_j}(\theta^y(t))$ satisfy the convex sum property. The index σ_j^k is either equal to 1 or 2 and indicates which partition of the k^{th} parameter ($\widetilde{\mu_k}^1$ or $\widetilde{\mu_k}^2$, i.e. $\overline{\mu_k}^1$ or $\overline{\mu_k}^2$) is involved in the j^{th} sub-model.

The relation between the sub-model number j and the σ_j^k indices is given by the following equation:

$$j=2^{n_{\theta_u}-1}\sigma_j^1+2^{n_{\theta_u}-2}\sigma_j^2+\ldots+2^0\sigma_j^{n_{\theta_u}}-(2^1+2^2+\ldots+2^{n_{\theta_u}-1}) \tag{13}$$

for the actuator, and

$$j=2^{n_{\theta_y}-1}\sigma_j^1+2^{n_{\theta_y}-2}\sigma_j^2+\ldots+2^0\sigma_j^{n_{\theta_y}}-(2^1+2^2+\ldots+2^{n_{\theta_y}-1}) \tag{14}$$

for the sensor.
Finally, using equations (10), the nonlinear LPV system (1) becomes:

$$\left\{\begin{array}{rcl} \dot{x}(t) & = & \displaystyle\sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}\mu_i(x(t))\widetilde{\mu_j}(\theta^u(t))(A_ix(t)+\mathcal{B}_{ij}u(t)) \\ y(t) & = & \displaystyle\sum_{k=1}^{2^{n_{\theta_y}}}\overline{\mu_k}(\theta^y(t))\widetilde{C}_kx(t) \end{array}\right. \tag{15}$$

$$\begin{array}{l} \mathcal{B}_{ij}=B_i+\overline{\mathcal{B}}_{ij} \\ \widetilde{C}_k=C+\overline{F}_kC \end{array} \tag{16}$$

3. MAIN RESULT: OBSERVER DESIGN

From the system equations (15), a state and actuator/sensor data deception observer is designed. An $\mathcal{L}_2$ attenuation approach is applied in order to minimize the attacks effect on the state and malicious input estimation error.
The state and actuator/sensor data deception observer is given by the following equations:

$$\left\{\begin{array}{l} \dot{\hat{x}}(t)=\displaystyle\sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}\mu_i(\hat{x}(t))\widetilde{\mu_j}(\hat{\theta^u}(t)) \\ \qquad (A_ix(t)+\mathcal{B}_{ij}u(t)+L_{ij}(y(t)-\hat{y}(t))) \\ \dot{\hat{\theta^u}}(t)=\displaystyle\sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}\mu_i(\hat{x}(t))\widetilde{\mu_j}(\hat{\theta^u}(t)) \\ \qquad (K_{ij}^u(y(t)-\hat{y}(t))-\alpha_{ij}^u\hat{\theta^u}(t)) \\ \dot{\hat{\theta^y}}(t)=\displaystyle\sum_{i=1}^{r}\sum_{k=1}^{2^{n_{\theta_y}}}\mu_i(\hat{x}(t))\overline{\mu_k}(\hat{\theta^y}(t)) \\ \qquad (K_{ik}^y(y(t)-\hat{y}(t))-\alpha_{ik}^y\hat{\theta^y}(t)) \\ \hat{y}(t)=\displaystyle\sum_{k=1}^{2^{n_{\theta_y}}}\overline{\mu_k}(\hat{\theta^y}(t))\widetilde{C}_k\hat{x}(t) \end{array}\right. \tag{17}$$

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 obtained by solving $\mathcal{LMI}$ constraints s.t. the estimated state and malicious input parameters converge to the real system state and attacks (i.e. the estimation errors for both state and malicious input parameters converge to zero).
Let us define the state and data deception estimation errors $e_x(t)$, $e_{\theta^u}(t)$ and $e_{\theta^y}(t)$ as:

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

Based on the convex sum property of the weighting functions, from the results presented in [2] and in order to be able to calculate the estimation errors dynamics, the system equations (15) are rewritten as follows:

$$\left\{\begin{array}{l} \dot{x}(t)=\displaystyle\sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}[\mu_i(\hat{x}(t))\widetilde{\mu_j}(\hat{\theta^u}(t))(A_ix(t)+\mathcal{B}_{ij}u(t))+ \\ \qquad\qquad \delta_{ij}(t)(A_ix(t)+\mathcal{B}_{ij}u(t))] \\ y(t)=\displaystyle\sum_{k=1}^{2^{n_{\theta_y}}}\left[\overline{\mu_k}(\hat{\theta^y}(t))\widetilde{C}_kx(t)+\overline{\delta_k}(t)\widetilde{C}_kx(t)\right] \end{array}\right. \tag{19}$$

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

$$\delta_{ij}(t)=\mu_i(x(t))\widetilde{\mu_j}(\theta^u(t))-\mu_i(\hat{x}(t))\widetilde{\mu_j}(\hat{\theta^u}(t)) \tag{20}$$

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

and satisfy the inequalities:

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

Representation (19) allows to deduce the state and data deception estimation errors dynamics in a straightforward way, since the state and output are written now only depending on the weighting functions of the estimate $\mu_i(\hat{x}(t))$, $\widetilde{\mu_j}(\hat{\theta^u}(t))$ and $\overline{\mu_k}(\hat{\theta^y}(t))$.
Let us define now:

$$\Delta A(t)=\sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}\delta ij(t)A_i=\mathcal{A}\Sigma(t)E_A \tag{23}$$

$$\Delta B(t)=\sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}\delta_{ij}(t)\mathcal{B}_{ij}=\mathcal{B}\Sigma(t)E_B \tag{24}$$

$$\Delta C(t)=\sum_{k=1}^{2^{n_{\theta_y}}}\overline{\delta_k}(t)\widetilde{C}_k=\mathcal{C}\overline{\Sigma}(t)E_C \tag{25}$$

with

$$\mathcal{A}=\left[\begin{array}{cccc} \underbrace{A_1 \quad \ldots \quad A_1}_{2^{n_{\theta_u}}\,times} & \ldots & \underbrace{A_r \quad \ldots \quad A_r}_{2^{n_{\theta_u}}\,times} \end{array}\right] \tag{26}$$

$$\mathcal{B}=\left[\begin{array}{ccc} \mathcal{B}_{11} & \ldots & \mathcal{B}_{r2^n} \end{array}\right] \tag{27}$$

$$\mathcal{C}=\left[\begin{array}{ccc} \widetilde{C}_1 & \ldots & \widetilde{C}_{2^{n_{\theta_y}}} \end{array}\right] \tag{28}$$

$$\begin{array}{l} \Sigma(t)=\mathrm{diag}(\delta_{11}(t),\ldots,\delta_{r2^n}(t)), \\ \overline{\Sigma}(t)=\mathrm{diag}(\overline{\delta_1}(t),\ldots,\overline{\delta_{2^{n_{\theta_y}}}}(t)) \end{array} \tag{29}$$

$$E_A=\left[\begin{array}{ccc} I_{n_x} & \ldots & I_{n_x} \end{array}\right]^T,\ E_B=\left[\begin{array}{ccc} I_{n_u} & \ldots & I_{n_u} \end{array}\right]^T$$

$$E_C=\left[\begin{array}{ccc} I_{2^{n_{\theta_y}}} & \ldots & I_{2^{n_{\theta_y}}} \end{array}\right]^T=\left[\begin{array}{ccc} I_{2^m} & \ldots & I_{2^m} \end{array}\right]^T \tag{30}$$

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

$$\Sigma^T(t)\Sigma(t)\leq I,\quad \overline{\Sigma}^T(t)\overline{\Sigma}(t)\leq I \tag{31}$$

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

$$\left\{\begin{array}{l} \dot{x}(t)=\displaystyle\sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}\mu_i(\hat{x}(t))\widetilde{\mu_j}(\hat{\theta^u}(t)) \\ \qquad ((A_i+\Delta A(t))x(t)+(\mathcal{B}_{ij}+\Delta B(t))u(t)) \\ y(t)=\displaystyle\sum_{k=1}^{2^{n_{\theta_y}}}\overline{\mu_k}(\hat{\theta^y}(t))(\widetilde{C}_k+\Delta C(t))x(t) \end{array}\right. \tag{32}$$

From equations (32) and (18), the estimation errors dynamics are then given by:

$$\left\{\begin{array}{l}\dot{e}_x(t)=\sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}\sum_{k=1}^{2^{n_{\theta_y}}}\mu_i(\hat{x}(t))\widetilde{\mu_j}(\hat{\theta^u}(t))\overline{\mu_k}(\hat{\theta^y}(t))\\ \qquad((A_i-L_{ij}\widetilde{C}_k)e_x(t)\\ \quad+(\Delta A(t)-L_{ij}\Delta C(t))x(t)+\Delta B(t)u(t))\\ \dot{e}_{\theta^u}(t)=\sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}\sum_{k=1}^{2^{n_{\theta_y}}}\mu_i(\hat{x}(t))\widetilde{\mu_j}(\hat{\theta^u}(t))\overline{\mu_k}(\hat{\theta^y}(t))\\ \qquad(-K^u_{ij}\widetilde{C}_k e_x(t)-\alpha^u_{ij}e_{\theta^u}(t)\\ \qquad-K^u_{ij}\Delta C(t)x(t)+\alpha^u_{ij}\theta^u(t)+\dot{\theta^u}(t))\\ \dot{e}_{\theta^y}(t)=\sum_{i=1}^{r}\sum_{k=1}^{2^{n_{\theta_y}}}\mu_i(\hat{x}(t))\overline{\mu_k}(\hat{\theta^y}(t))\\ \qquad(-K^y_{ik}\widetilde{C}_k e_x(t)-\alpha^y_{ik}e_{\theta^y}(t)\\ \qquad-K^y_{ik}\Delta C(t)x(t)+\alpha^y_{ik}\theta^y(t)+\dot{\theta^y}(t))\end{array}\right. \tag{33}$$

Let us now consider the augmented vectors $e_a(t)$ and $\omega(t)$, such that:

$$e_a(t)=\begin{pmatrix}e_x(t)\\ e^u_\theta(t)\\ e^y_\theta(t)\end{pmatrix},\ \omega(t)=\begin{pmatrix}x(t)\\ \theta^u(t)\\ \theta^y(t)\\ \dot{\theta}^u(t)\\ \dot{\theta}^y(t)\\ u(t)\end{pmatrix} \tag{34}$$

From (33) and (34), it follows:

$$\dot{e}_a(t)=\sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}\sum_{k=1}^{2^{n_{\theta_y}}}\mu_i(\hat{x}(t))\widetilde{\mu_j}(\hat{\theta^u}(t))\overline{\mu_k}(\hat{\theta^y}(t))\\ (\Phi_{ijk}e_a(t)+\Psi_{ijk}(t)\omega(t)) \tag{35}$$

with

$$\Phi_{ijk}=\begin{pmatrix}A_i-L_{ij}\widetilde{C}_k & 0 & 0\\ -K^u_{ij}\widetilde{C}_k & -\alpha^u_{ij} & 0\\ -K^y_{ik}\widetilde{C}_k & 0 & -\alpha^y_{ik}\end{pmatrix}$$

$$\Psi_{ijk}(t)=\begin{pmatrix}\Delta A(t) & 0 & 0 & 0 & 0 & \Delta B(t)\\ -K^u_{ij}\Delta C(t) & \alpha^u_{ij} & 0 & I & 0 & 0\\ -K^u_{ik}\Delta C(t) & 0 & \alpha^y_{ik} & 0 & I & 0\end{pmatrix} \tag{36}$$

Considering (35), the objective would be to design a simultaneous state and attacks observer with a minimal $\mathcal{L}_2$ gain of the transfer from $\omega(t)$ to $e_a(t)$. The computation of the gains is detailed in the next theorem.

REMARK 1. *In order to apply the considered criterion, a minimal $\mathcal{L}_2$ attenuation between the augmented estimation error vector and $e_a(t)$ and external input $\omega(t)$, we assume that $\omega(t)$ is of finite energy. For the considered example (i.e. stable), knowing that the attacks do not appear all time (stealthy attacks), the assumption is satisfied.*

THEOREM 1. *There exists a state and actuator/sensor date deception attack observer (17) for a nonlinear system (1) with an $\mathcal{L}_2$ gain from $\omega(t)$ to $e_a(t)$ bounded by β ($\beta>0$) if there exists positive symmetric matrices $P_1=P_1^T>0$, $P_2=P_2^T>0$, $P_3=P_3^T>0$, positive matrices Γ_l, $l=1,\ldots,6$, matrices $\overline{\alpha}^u_{ij}$, $\overline{\alpha}^y_{ik}$, F^u_{ij}, F^y_{ik}, R_{ij} and scalars positive β, λ_A, λ_B, λ_{1C} and λ_{2C} solution of the optimization problem (37) under LMI constraints (38) and (39) (see next page)*

$$\min_{\{P_1,P_2,P_3,R_{ij},F^u_{ij},F^y_{ik},\overline{\alpha}^u_{ij},\overline{\alpha}^y_{ik},Gamma_l,\lambda_A,\lambda_B,\lambda_{1C},\lambda_{2C}\}}\beta \tag{37}$$

for $i=1,\ldots,r$, $j=1,2^{n_{\theta_u}}$ and $k=1,2^{n_{\theta_y}}$

$$\Gamma_l<\beta I \text{ for } l=1,\ldots,6 \tag{38}$$

with

$$\begin{array}{l}Q^{11}_{ijk}=P_1A_i+A_i^TP_1-R_i\widetilde{C}_j-\widetilde{C}_j^TR_i^T+I_{n_x}\\ Q^{22}_{ij}=-\overline{\alpha}^u_{ij}-\overline{\alpha}^{u\,T}_{ij}+I\\ Q^{33}_{ik}=-\overline{\alpha}^y_{ik}-\overline{\alpha}^{y\ T}_{ik}+I\\ Q^{44}=-\Gamma_1+\lambda_AE_A^TE_A\end{array} \tag{40}$$

The observer gains are given by

$$\left\{\begin{array}{l}L_{ij}=P_1^{-1}R_{ij}\\ K^u_{ij}=P_2^{-1}F^u_{ij}\\ K^y_{ik}=P_3^{-1}F^y_{ik}\\ \alpha^u_{ij}=P_2^{-1}\overline{\alpha}^u_{ij}\\ \alpha^y_{ik}=P_3^{-1}\overline{\alpha}^y_{ik}\end{array}\right. \tag{41}$$

PROOF. Let us consider the following quadratic Lyapunov function:

$$V(e_a(t))=e_a^T(t)Pe_a(t),\ P=P^T>0 \tag{42}$$

Using (35), its time derivative is given by

$$\begin{array}{l}\dot{V}(e_a(t))=\sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}\sum_{k=1}^{2^{n_{\theta_y}}}\mu_i(\hat{x}(t))\widetilde{\mu_j}(\hat{\theta^u}(t))\overline{\mu_k}(\hat{\theta^y}(t))\\ \big[e_a^T(t)((\Phi_{ij})^TP+P\Phi_{ij})e_a(t)\\ +e_a^T(t)P\Psi_i(t)\omega(t)+\omega^T(t)\Psi_i^T(t)Pe_a(t)\big]\end{array} \tag{43}$$

It is known that $e_a(t)$ asymptotically converges toward zero when $\omega(t)=0$ and that the $\mathcal{L}_2$ gain from $\omega(t)$ to $e_a(t)$ is bounded by β if the following inequality holds

$$\dot{V}(e_a(t))+e_a^T(t)e_a(t)-\omega^T(t)\Gamma\omega(t)<0 \tag{44}$$

with

$$\Gamma=\text{diag}(\Gamma_l),\ \Gamma_l<\beta\ I,\ \text{for } l=1,\ldots,6 \tag{45}$$

An appropriate choice of Γ enables to attenuate the transfer from some components of $\omega(t)$ to $e_a(t)$.
From (43), (44) becomes:

$$\sum_{i=1}^{r}\sum_{j=1}^{2^{n_{\theta_u}}}\sum_{k=1}^{2^{n_{\theta_y}}}\mu_i(\hat{x}(t))\widetilde{\mu_j}(\hat{\theta^u}(t))\overline{\mu_k}(\hat{\theta^y}(t))\begin{pmatrix}e_a(t)\\ \omega(t)\end{pmatrix}^T\\ \left(\left(\begin{array}{c|c}\Phi_{ij}^TP+P\Phi_{ij}+I & P\Psi_i(t)\\ \hline \Psi_i^T(t)P & -\Gamma\end{array}\right)\right)\begin{pmatrix}e_a(t)\\ \omega(t)\end{pmatrix}<0 \tag{46}$$

For a chosen structure of the Lyapunov matrix P (diagonal)

$$P=\text{diag}(P_1,P_2,P_3) \tag{47}$$

with a variables change as given in (41), based on decompositions (23), (24) and (25), properties (31), Schur's complement and the following lemma:

LEMMA 1. *[19] 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*

$$X^T\Delta^T(t)Y+Y^T\Delta(t)X\leq\varepsilon X^TX+\varepsilon^{-1}Y^TY \tag{48}$$

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

$$\begin{pmatrix} Q_{ijk}^{11} & -\widetilde{C}_k^T F_{ij}^{u\,T} & -\widetilde{C}_k^T F_{ik}^{y\,T} & 0 & 0 & 0 & 0 & 0 & 0 & P_1\mathcal{A} & P_1\mathcal{B} & 0 & 0 \\ * & Q_{ij}^{22} & 0 & 0 & \overline{\alpha}_{ij}^{u} & 0 & P_2 & 0 & 0 & 0 & 0 & F_{ij}^{u}\mathcal{C} & 0 \\ * & * & Q_{ik}^{33} & 0 & 0 & \overline{\alpha}_{ik}^{y} & 0 & P_3 & 0 & 0 & 0 & 0 & F_{ik}^{y}\mathcal{C} \\ * & * & * & Q^{44} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & -\Gamma_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & -\Gamma_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * & -\Gamma_4 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * & * & -\Gamma_5 & 0 & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * & * & * & -\Gamma_6 + \lambda_B E_B^T E_B & 0 & 0 & 0 & 0 \\ * & * & * & * & * & * & * & * & * & -\lambda_A I & 0 & 0 & 0 \\ * & * & * & * & * & * & * & * & * & * & -\lambda_B I & 0 & 0 \\ * & * & * & * & * & * & * & * & * & * & * & -\lambda_{1C} I & 0 \\ * & * & * & * & * & * & * & * & * & * & * & * & -\lambda_{2C} I \end{pmatrix} < 0 \quad (39)$$

following the same development as the work presented in [2], [3], the Lyapunov stability with an $\mathcal{L}_2$ transfer from $\omega(t)$ to $e_a(t)$ is obtained by solving the optimization problem (37) under the $\mathcal{LMI}$ constraints (38) and (39), which ends the proof. □

4. NUMERICAL SIMULATION

In the following, the proposed approach is applied to a basic model of a biological waste-water treatment plant. The mathematical model is represented thanks to two state variables $x_1(t)$ and $x_2(t)$, corresponding to the biomass and substrate concentration respectively, the input $u(t)$, which represents the dwell-time in the treatment plant and the measured output which is the biomass concentration ($y(t) = x_1(t)$).

4.1 LPV Representation of The Process

First step, let us write the nonlinear system equations (49) in a polytopic form. As it was developed in [3], and under specific assumptions, some simplifications can be made and the nonlinear model may be given by:

$$\begin{cases} \dot{x}_1(t) = \frac{a x_1(t) x_2(t)}{x_2(t)+b} - x_1(t)u(t) \\ \dot{x}_2(t) = -\frac{c a x_1(t) x_2(t)}{x_2(t)+b} + (d - x_2(t))u(t) \end{cases} \quad (49)$$

Where a, b, c and d are known parameters.
From the system non-linearities, applying the Sector Nonlinearity Approach with the premise variables $\rho_1(t)$ and $\rho_2(t)$ chosen as follows:

$$\rho_1(t) = -u(t), \quad \rho_2(t) = \frac{a x_1(t)}{x_2(t)+b} \quad (50)$$

From (49) and (50), the quasi-LPV system (51) is deduced:

$$\dot{x}(t) = \begin{pmatrix} \rho_1(t) & \rho_2(t) \\ 0 & -c\rho_2(t) + \rho_1(t) \end{pmatrix} x(t) + \begin{pmatrix} 0 \\ d \end{pmatrix} u(t) \quad (51)$$

Since a LPV representation is deduced in a compact set of the state space, the max and min values of the terms $\rho_1(t)$ and $\rho_2(t)$ may be calculated using the knowledge of the domain of variation of $u(t)$, i.e. $\rho_1(t) \in [-1, -0.2]$ and $\rho_2(t) \in [0.004, 15]$.
Applying the convex polytopic transformation, two partitions for each premise variable are defined:

$$\begin{cases} \rho_1(t) = \varrho_{11}(\rho_1)\rho_1^2 + \varrho_{12}(\rho_1)\rho_1^1 \\ \rho_2(t) = \varrho_{21}(\rho_2)\rho_2^2 + \varrho_{22}(\rho_2)\rho_2^1 \end{cases} \quad (52)$$

$$\begin{aligned} &\text{with} \quad \varrho_{11}(\rho_1) = \frac{\rho_1(t) - \rho_1^2}{\rho_1^1 - \rho_1^2}, \ \varrho_{12}(\rho_1) = \frac{\rho_1^1 - \rho_1(t)}{\rho_1^1 - \rho_1^2} \\ &\varrho_{21}(\rho_2) = \frac{\rho_2(t) - \rho_2^2}{\rho_2^1 - \rho_2^2}, \ \varrho_{22}(\rho_2) = \frac{\rho_2^1 - \rho_2(t)}{\rho_2^1 - \rho_2^2} \end{aligned} \quad (53)$$

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

$$\begin{aligned} \rho_1^1 &= \max_u \rho_1(t), \ \rho_1^2 = \min_u \rho_1(t) \\ \rho_2^1 &= \max_x \rho_2(t), \ \rho_2^2 = \min_x \rho_2(t) \end{aligned} \quad (54)$$

The sub-models are defined by the sets (A_i, B_i, C) with $i = 1, 2, 3, 4$. Based on ρ_1 and ρ_2 definitions, all the B_i matrices are set to $B = \begin{bmatrix} 0 & d \end{bmatrix}^T$. The output matrix $C = \begin{bmatrix} 1 & 0 \end{bmatrix}$ and the matrices A_i are given by:

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

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

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

$$\begin{aligned} &\mu_1(t) = \varrho_{11}(\rho_1(t))\varrho_{21}(\rho_2(t)), \mu_2(t) = \varrho_{11}(\rho_1(t))\varrho_{22}(\rho_2(t)) \\ &\mu_3(t) = \varrho_{12}(\rho_1(t))\varrho_{21}(\rho_2(t)), \mu_4(t) = \varrho_{12}(\rho_1(t))\varrho_{22}(\rho_2(t)) \end{aligned} \quad (55)$$

Since the polytopic representation is obtained in a compact set of the state space, maximum and minimum values that occur in $\rho_1(t)$ and $\rho_2(t)$ may be calculated using the knowledge of the domain of variation of $u(t)$: $\rho_1(t) \in [-1, -0.2]$ and $\rho_2(t) \in [0.004, 15]$.

4.2 Date Deception Attacks Representation on The Actuator/Sensor

Two types of data deception attacks are considered, i.e. attacks on actuators and sensors. It is assumed that, mathematically speaking, these attacks are modeled as bounded multiplicative actuator and sensor time-varying faults.
For the considered example, it is assumed that parameter d may be hacked. This actuator attack is represented by $d(t)$, such that:

$$d(t) = d + \Delta d(t) \quad (56)$$

It can also be written as:

$$d(t) = d + \theta^u(t)\overline{d}, \quad \theta^u(t) \in [\theta^{u2}, \theta^{u1}] \quad (57)$$

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 $c = 0.7$.

Considering the attack on the actuator, the polytopic representation of the input matrix B is then given by two submodels, such that:

$$B_1 = B + \theta^{u1}\overline{B}, \quad B_2 = B + \theta^{u2}\overline{B} \tag{58}$$

where is defined by $\overline{B} := \begin{bmatrix} 0 & \overline{d} \end{bmatrix}^T$. The weighting functions $\widetilde{\mu_j}(\theta^u(t))$ are defined as given in (6) and (11).
Now, for the sensor attack, it is assumed that a bounded multiplicative sensor fault $\theta^y(t)$ affects the output $y(t)$ such that:

$$y(t) = (1 + \theta^y(t))x_1(t) \tag{59}$$

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

$$\theta^y(t) = \overline{\mu}_1{}^1(\theta^y(t))\theta^{y1} + \overline{\mu}_1^2(\theta^y(t))\theta^{y2},\ \theta^y(t) \in [\theta^{y2}, \theta^{y1}] \tag{60}$$

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

$$y(t) = \sum_{k=1}^{2} \overline{\mu}_k(\theta^y(t))\widetilde{C}_k x(t) \tag{61}$$

with $\widetilde{C}_1 = \begin{pmatrix} 1+\theta^{y2} & 0 \end{pmatrix}$, $\widetilde{C}_2 = \begin{pmatrix} 1+\theta^{y1} & 0 \end{pmatrix}$.

4.3 Simulation Results

From the considered example, with both attacks on the actuator/sensor, applying the proposed approach by solving the theorem 1, a simultaneous state and attacks observer is designed such that the system initial conditions are taken as $x(0) = \begin{pmatrix} 0.1 & 1.5 \end{pmatrix}$ and $\hat{x}(0) = \begin{pmatrix} 0.09 & 2.3 \end{pmatrix}$ for its observer. 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 as well as the data deception attacks with their estimates are depicted in the figures 1, and 2 respectively. From the obtained plots, the efficiency of the proposed observer is highlighted; indeed, both system states and the time-varying multiplicative actuator/sensor attacks are well estimated.

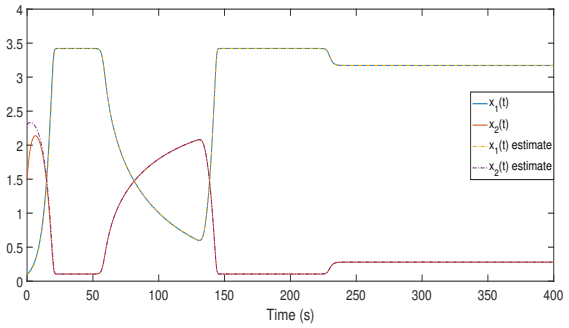

Figure 1: System states and their estimates

5. CONCLUSIONS

In the present paper, a polytopic approach was applied to cope with the system state and data deception attacks estimation. Based on previous work, both attacks on actuator and sensor are modeled as multiplicative time-varying faults and written in a convex set, based only on their min and max

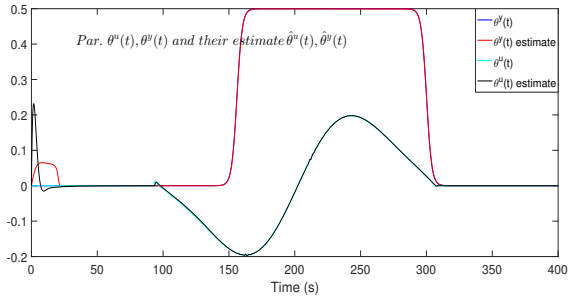

Figure 2: Data deception attacks and their estimates

bound. A simultaneous state and attack observer is designed by minimizing the $\mathcal{L}_2$ gain from the augmented input to the different estimation errors. The chosen application example is an activated sludge reactor with attacks represented by unknown time-varying parameters on the parameter d and the output. From the nonlinear equations of the system, a LPV model is derived. The proposed observer is synthesized and the obtained results illustrate its performance.

6. REFERENCES

[1] A. Barboni, F. Boem, and T. Parisini. Model-based detection of cyber-attacks in networked mpc-based control systems. In 10^{th} *IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS 2018*, Warsaw, Poland, August 2018.

[2] S. Bezzaoucha, B. Marx, D. Maquin, and J. Ragot. Nonlinear joint state and parameter estimation. Application to a wastewater treatment plant. *Control Engineering Practice.*, 21(10):1377–1385, 2013.

[3] S. Bezzaoucha, B. Marx, D. Maquin, and J. Ragot. State and multiplicative sensor fault estimation for nonlinear systems. In 2^{nd} *International Conference on Control and Fault-Tolerant Systems*, Nice, France, 2013.

[4] S. Bezzaoucha, H. Voos, and M. Darouach. *The Inverted Pendulum: From Theory to New Innovations in Control and Robotics - PART IV Robust controllers-based observers via Takagi-Sugeno or linear approaches, Chapter 12:A Survey on The Polytopic Takagi-Sugeno Approach: Application to the Inverted Pendulum*, volume ISBN: 978-1-78561-320-3. The Institution of Engineering and Technology IET-publishing, 2017.

[5] S. Bezzaoucha Rebaï, H. Voos, and M. Darouach. Attack-tolerant control and observer-based trajectory tracking for cyber-physical systems. *European Journal Control*, 2018. https://doi.org/10.1016/j.ejcon.2018.09.005.

[6] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and Fault-Tolerant Control*. Springer-Verlag, Berlin, Germany, 2003.

[7] Q. Dinh Vu, R. Tan, and D. Yau. On applying fault detectors against false data injection attacks in cyber-physical control systems. In *INFOCOM 2016 - The* 35^{th} *Annual IEEE International Conference on Computer Communications*, San Francisco, CA, USA, 2016.

[8] N. Forti, G. Battistelli, L. Chisci, and B. Sinopoli. Secure state estimation of cyber-physical systems under switching attacks. In 20^{th} *IFAC World Congress*, Toulouse, France, 2017.

[9] B. Gerard, S. Bezzaoucha Rebai, H. Voos, and M. Darouach. Cyber security and vulnerability analysis of networked control system subject to false-data injection. In *The 2018 American Control Conference*, Milwaukee, Wisconsin, USA, June 2018.

[10] Q. Hu, D. Fooladivanda, Y.-H. Chang, and C. J. Tomlin. Secure state estimation for nonlinear power systems under cyber attacks. In *American Control Conference (ACC)*, Seattle, WA, USA, 2017.

[11] Y. Li, H. Voos, L. Pan, M. Darouach, and C. Hua. Stochastic cyber-attacks estimation for nonlinear control systems based on robust h_∞ filtering technique. In 27^{th} *Chinese Control and Decision Conference (CCDC)*, 2015.

[12] M. Pajic, J. WeiBezzo, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. Pappas. Robustness of attack-resilient state estimators. In *ACM/IEEE* 4^{th} *International Conference on Cyber-Physical Systems (ICCPS)*, Berlin, Germany, April 2014.

[13] M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G. Pappas, and I. Lee. Design and implementation of attack-resilient cyberphysical systems. *IEEE Control Systems Magazine*, 37(2):66–81, April 2017.

[14] F. Pasqualetti, F. Dörfer, and F. Bullo. Cyber-physical security via geometric control: Distributed monitoring and malicious attacks. In *IEEE Conference on Decision and Control*, Hawai, USA, 2012.

[15] B. RebaiS., H. Voos, and M. Darouach. Observer-based event-triggered attack-tolerant control design for cyberphysical systems. In 14^{th} *International Workshop on Advanced Control and Diagnosis*, Bucharest, Romania, November 2017.

[16] K. Tanaka and H. Wang. *Fuzzy Control Systems Design and Analysis: A Linear Matrix Inequality Approach*. John Wiley & Sons, Inc., New York, 2001.

[17] A. Teixeira, D. Perez, H. Sandberg, and K. Johansson. Attack models and scenarios for networked control systems. . pages 55-64 .beijing, china ÂŮ april 17 - 18, 2012 . In *HiCoNS '12 Proceedings of the* 1^{st} *international conference on High Confidence Networked Systems*, Beijing, China, 2012.

[18] F. Yacef, O. Bouhali, H. Khebbache, and F. Boudjema. Takagi-sugeno model for quadrotor modelling and control using nonlinear state feedback controller. *International Journal of Control Theory and Computer Modelling*, 2(3):9–24, May 2012.

[19] K. Zhou and P. Khargonekar. Robust stabilization of linear systems with norm-bounded time-varying uncertainty. *Systems and Control Letters*, 10(1):17–20, 1988.