Contents lists available at ScienceDirect

European Journal of Control

journal homepage: www.elsevier.com/locate/ejcon

Attack-tolerant control and observer-based trajectory tracking for Cyber-Physical Systems

Souad Bezzaoucha Rebaï[a,*], Holger Voos[a], Mohamed Darouach[b]

[a] Interdisciplinary Centre for Security, Reliability and Trust (SnT), Automatic Control Research Group, University of Luxembourg, 29 Avenue J.F Kennedy, L-1855, Luxembourg
[b] Research Center for Automatic Control of Nancy (CRAN), Université de Lorraine, IUT de Longwy, 186 rue de Lorraine, Cosnes et Romain 54400, France

ARTICLE INFO

Article history:
Received 18 January 2018
Revised 7 June 2018
Accepted 1 September 2018
Available online 6 September 2018

Recommended by Dr. A Zemouche

Keywords:
Observer design
Attack/fault tolerant control
Trajectory tracking
$\mathcal{LMI}-\mathcal{BMI}$ framework
Cyber-Physical Systems
Data deception
Lyapunov theory
Stability conditions

ABSTRACT

In the present paper, a model-based fault/attack tolerant scheme is proposed to cope with cyber-threats on Cyber-Physicals Systems. A common scheme based on observers is designed and a state feedback control based on an aperiodic event-triggered framework is given with control synthesis and condition on the switching time.

Classical fault tolerant control with Bi-linear Matrix Inequality ($\mathcal{BMI}$) approaches are used to achieve novel and better security strategy based on an event-triggered control implementation. The purpose of using the event-based implementation would be to reduce (limit) the total number of transmissions to only instances when the networked control system (NCS) needs attention. Simulation results on a real-time laboratory three tank system are given to show the attack-tolerant control ability despite data deception attacks on both actuators and sensors. A detection/isolation scheme based on residual observers bank is also proposed.

1. Introduction

Due to a highest degree of connectivity in control systems during the past few years, Cyber-Physicals Systems (CPS), and especially their communication networks, are more and more subject to malicious intrusions and attacks. Thus, control-specific CPS security challenges arise from two perspectives [14]. A first perspective is given through the conventional information-security approach (IT) that can be used to prevent intrusions, but attackers can still affect the system via the physical environment. The second one is related to the control approach, where attacks can be modeled as an adversary signals (i.e., like disturbances, unknown inputs, faults,...) introduced via the internal network by hackers and affecting the sensors and/or actuators data [14,22].

In the present paper, the second approach will be investigated based on classical fault-tolerant control (FTC) approach and event-triggered control.

In fact, from a control perspective, to deal with cyber-attacks, different approaches have been investigated, as for instance [5,8,15] and [13]. In the proposed paper, an attack-tolerant control solution using observers is proposed. The idea would be to apply the well known FTC approach to security issues. A dynamic model including the dynamic behavior of the physical process under attacks is considered. If an attack is detected, a control strategy should maintain the process in a desired safe state even under the attack ("attack-tolerant" control (ATC)) via the so-called event-triggered control. In order to combine security and safety aspects, both ideas of FTC and ATC will be combined to an integrated approach and adapted to the special characteristics of CPS.

The proposed control is inspired by classical FTC and event-based control. It is based on the comparison between the difference between the physical process output (that may be hacked) and its estimate with the difference between the continuous-time and the sampled control input (obtained thanks to the event-based approach).

In the present work, in order to lower communication needs, the introduction of the event-based paradigm is well motivated. In fact, nowadays, an increasing number of applications of networked control systems demand the consideration of certain limitations on the control system design [9], like for instance energy consumption, computation power and communication resources.

In networked control systems, controllers and actuators communicate with each other through communication networks.

[*] Corresponding author.
E-mail addresses: souad.bezzaoucha@uni.lu (S. Bezzaoucha Rebaï), holger.voos@uni.lu (H. Voos), mohamed.darouach@univ-lorraine.fr (M. Darouach).

https://doi.org/10.1016/j.ejcon.2018.09.005
0947-3580/© 2018 European Control Association. Published by Elsevier Ltd. All rights reserved.

In this context, the emerging event-based sampling strategies [2] have become popular during the past two decades, due to their capability to maintain the system performance at reduced communication or computation costs. The basic rationale of the event-based action strategies is that the sensors and actuators do not update their actions until certain events happen (for instance, the difference between the current measurement and the measurement at the previous event time goes beyond a pre-specified level [12,18].

For the controller implementation, a state observer is designed as well as an asynchronous or aperiodic event-triggered framework. The event-triggered control system consists of two elements, namely, a feedback controller that computes the control inputs, and a triggering mechanism that determines when the control input has to be updated again [9].

The event-based control is mainly introduced for lowering communication needs, i.e., implementing an aperiodic controller means that sensor and control communications are limited to instances when the system needs attention, which largely reduces the total transmission burden and network traffic. The idea is to make the system broadcasts its control information only when the defined error exceeds a threshold value. Other methods do exists in order to determine/implement the triggering mechanism/condition. In [23] for example, an H_∞ output tracking control problem of the networked control systems under an adaptively adjusted event-triggered scheme with stochastic sensor faults is proposed to choose the necessary packets of sampled data to be transmitted through the networks. In [17], it is the finite-time event-triggered H_∞ control problem for Takagi–Sugeno Markov jump fuzzy systems that was investigated and aimed to reduce the communication burden.

Indeed, the presence of the event-triggers, however, has introduced new and distinct challenges for controller design, and performance evaluation; for instance, stability, optimality are more difficult to be determined theoretically compared with their periodic counterparts [18]. Here, the stability constraint is solved as a $\mathcal{BMI}$ (Bilinear Matrix Inequality) feasibility problem using the Matlab solver PENBMI [11]. The observer and controller synthesis consists in designing the adequate gains ensuring the stability of the system and the convergence of the estimation errors to an origin-centered ball.

In the following paper, a model-based fault/attack tolerant scheme is proposed to cope with cyber-threats on Cyber-Physicals Systems. A common scheme based on observers is designed and a state feedback control based on an aperiodic event-triggered framework is given with control synthesis and condition on the switching time.

The paper is organized as follows. After a short introduction of the state of art in Section 1, in Section 2, an observer-based attack-tolerant control design is considered with the presentation of an asymptotic stability criterion and an Event-triggered strategy design. An application of the proposed method is given in the next section with simulation results on a real-time laboratory three tank system are given to show the attack-tolerant control ability despite data deception attacks on both actuators and sensors. A detection/isolation scheme based on residual observers bank is also proposed. Finally, conclusion will be given in the last Section 4.

2. Observer-based attack-tolerant control design

In the following section, a modeling framework to capture different sorts of attack on control systems is considered. Unlike other IT systems where cyber-security mainly involves the protection of data-related properties and services, cyber-attacks on control systems may influence physical processes through feedback actuation. Therefore, networked control system security needs to consider threats at both the cyber and physical layers [21].

In the continuity of the contribution [5], and as an extension of the work presented in [6], a focus is given in the present work to the data deception attack/corruption due to malicious cyber attacks on both controller and sensors. In fact, since the communication network may be unreliable, the data exchanged between the plant and the controller may be altered, resulting in discrepancies in the data at the plant and controller ends, which modify the control actions and sensor measurements from their calculated or real values to the corrupted signals.

In the present contribution, based on the results presented in [6], an application to a real-time laboratory three tank system is considered. Simulation results are given to show the attack-tolerant control ability despite data deception attacks on both actuators and sensors. A detection/isolation scheme based on residual observers bank is also proposed in the following extension.

Let us consider a physical plant operation supported by a communication network through which the sensor measurements and actuator data are transmitted, which at the plant side correspond to $y_p(t)$ and $\tilde{u}(t)$, respectively with, at the controller side we denote the sensor and actuator data by $\tilde{y}(t)$ and $u(t)$, respectively.

Inspired by [20], the physical plant is then modeled in the continuous-time state-space form:

$$\begin{cases} \dot{x}_p(t) = Ax_p(t) + B\tilde{u}(t) \\ y_p(t) = Cx_p(t) \end{cases} \tag{1}$$

where $x_p(t) \in \mathbb{R}^{n_x}$ is the system state, $y_p(t) \in \mathbb{R}^{n_y}$ the system output and $\tilde{u}(t) \in \mathbb{R}^{n_u}$ the control input applied to the process. The system matrices A, B and C are constant and of appropriate dimensions.

System (1) satisfies the following assumption, i.e., the plant has no transmission to zeros at zero [20,24]:

Assumption 1. $n_u \geq n_y$ and $rank\left(\begin{bmatrix} A & B \\ C & 0 \end{bmatrix}\right) = n_x + n_y$

For the design of an attack-tolerant robust control, an observer-based state feedback controller to drive the output to a given non-zero constant set-point r is defined:

$$\begin{cases} \dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) - K_o(\tilde{y}(t) - \hat{y}(t)) \\ \hat{y}(t) = C\hat{x}(t) \\ u(t) = K_c\hat{x}(t) + K_r r \end{cases} \tag{2}$$

where $\hat{x}(t) \in \mathbb{R}^{n_x}$ is the observer state, $\hat{y}(t) \in \mathbb{R}^{n_y}$ the observer output and $r \in \mathbb{R}^{n_y}$ the constant reference signal. The observer and controller matrices, respectively, K_o and K_c are constant and of appropriate dimensions, where K_r is a feed-forward gain.

Since data deception modifies the control actions and sensor measurements from their calculated or real values $u(t)$ and $y(t)$ to the corrupted signals $\tilde{u}(t)$ and $\tilde{y}(t)$. The deception attacks are modeled as:

$$\tilde{u}(t) \triangleq u(t) + \Gamma^u a^u(t), \quad \tilde{y}(t) \triangleq y(t) + \Gamma^y a^y(t) \tag{3}$$

where the signals $a^u(t)$ and $a^y(t)$ represent the data corruption and Γ^u, Γ^y the binary incidence matrices that indicate which data channels can be accessed by the hacker (attacker).

An event-triggering strategy is chosen to be applied for the control design, s.t. the control value is maintained constant as long as the triggering condition is not satisfied and updated when the condition is satisfied. For that, we assume the input to be held constant in between the successive re-computation of the control. This is often refereed in the literature as sample-and-hold and can be formalized as [10]:

$$u(t) = u(t_k) \quad \forall t \in [t_k, t_{k+1}[, k \in \mathbb{N} \tag{4}$$

where the sequence $\{t_K\}_{k\in\mathbb{N}}$ represents the instants at which the control is re-computed.

In the proposed contribution, the so-called a co-design problem is considered, where the design of both the controller and the event-triggering rule is performed simultaneously. The design is addressed where the asymptotic stability is guaranteed by a condition in terms of $\mathcal{LMI}$.

Under the control sequence (4), the plant model and the observer structure become, respectively:

$$\begin{cases} \dot{x}_p(t) = Ax_p(t) + B\tilde{u}(t_k) \\ y_p(t) = Cx_p(t) \end{cases} \tag{5}$$

and

$$\begin{cases} \dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t_k) - K_o(\tilde{y}(t) - \hat{y}(t)) \\ \hat{y}(t) = C\hat{x}(t) \end{cases} \tag{6}$$

with the following input:

$$u(t_k) = K_c\hat{x}(t_k) + K_r r \tag{7}$$

and the corrupted input given by:

$$\tilde{u}(t_k) = u(t_k) + \Gamma^u a^u(t) \tag{8}$$

Let us define the state estimation error, $e(t) = x_p(t) - \hat{x}(t)$, its dynamics is then given by:

$$\dot{e}(t) = (A + K_oC)e(t) + B\Gamma^u a^u(t) + K_o\Gamma^y a^y(t) \tag{9}$$

For a given constant reference signal r, the error dynamics between the observer state $\hat{x}(t)$ and its equilibrium point $x_{o,\,eq}$ is given by:

$$\dot{\varepsilon}_{eq}(t) = (A + BK_c)\varepsilon_{eq}(t) + B\delta(t) - K_oCe(t) - K_o\Gamma^y a^y(t) \tag{10}$$

where $\delta(t)$ is defined as [19,20]:

$$\delta(t) = K_c(\varepsilon_{eq}(t_k) - \varepsilon_{eq}(t)) \tag{11}$$

and can be seen as a measure of the difference between the continuous-time and the sampled control input.

Remark 1. In the present contribution, as mentioned previously, the simultaneous design of the controller and observer gains K_o and K_c with the event-based condition is addressed where the asymptotic stability is guaranteed by a condition in terms of $\mathcal{BMI}$. However, regarding the feedforward gain K_r, it depends on the controller gain K_c and is defined by the following:

For the considered constant reference signal r and for an attack-free case ($a^y(t) = 0$), the equilibrium point ($x_{p,\,eq}$, $x_{o,\,eq}$) of (1) and (2) satisfies [20]:

$$\begin{cases} x_{o,eq} = x_{p,eq}, \quad (A + BK_c)x + BK_r r = 0 \\ Cx_{o,eq} = r \end{cases} \tag{12}$$

From (12) and due to Assumption 1, the Moore–Penrose pseudo inverse of $\begin{bmatrix} A & B \\ C & 0 \end{bmatrix}$ exists such that $\begin{bmatrix} A & B \\ C & 0 \end{bmatrix}\begin{bmatrix} A & B \\ C & 0 \end{bmatrix}^+ = I$ and K_r is given by [20]:

$$K_r = \begin{bmatrix} -K_c & I \end{bmatrix}\begin{bmatrix} A & B \\ C & 0 \end{bmatrix}^+ \begin{bmatrix} 0 \\ I \end{bmatrix} \tag{13}$$

The augmented system (plant and observer error dynamics) is then modeled by the following state equations:

$$\dot{\eta}(t) = A_a\eta(t) + B_a a(t) + C_a\delta(t) \tag{14}$$

where $\eta(t) = \begin{pmatrix} e(t) \\ \varepsilon_{eq}(t) \end{pmatrix}$, $a(t) = \begin{pmatrix} a^u(t) \\ a^y(t) \end{pmatrix}$ and the matrices A_a, B_a and C_a are defined by:

$$\begin{aligned} A_a &= \begin{pmatrix} A + K_oC & 0 \\ -K_oC & A + BK_c \end{pmatrix} \\ B_a &= \begin{pmatrix} B\Gamma^u & K_o\Gamma^y \\ 0 & -K_o\Gamma^y \end{pmatrix} \\ C_a &= \begin{pmatrix} 0 \\ B \end{pmatrix} \end{aligned} \tag{15}$$

Since $\delta(t)$ depends only on the observer variables, it is therefore available at each instant t and will be interpreted in the following as an input to the augmented system (14).

In this contribution, our aim is to implement an event-triggered strategy on the controller (2), i.e., that an event generator algorithm is integrated in the controller to decide whenever the control signal has to be updated. The event-triggered implementation of the feedback control thus consists in maintaining the control value constant as long as the triggering condition is not satisfied and updating its value when the condition is satisfied [5]. The triggering times t_k are then determined thanks to:

$$t_{k+1} = min\{t \geq t + T, s.t. f(\delta(t), \eta(t) \geq 0)\} \tag{16}$$

In the following, f will be chosen based on the Lyapunov stability theory ensuring an $\mathcal{L}_2$ attenuation from $\delta(t)$ to $\eta(t)$.

2.1. Asymptotic stability criterion

The observer and event-based controller synthesis consists in designing the gains K_o and K_c ensuring the stability of system (14) and the convergence of the errors $\eta(t)$ to an origin-centered ball as proposed in Theorem 1.

Theorem 1. *For some given parameter Ψ, under the event-triggered scheme (7), there exists an observer-based feedback controller (2) for the system (1) ensuring the convergence to a desired constant reference with a converging estimation error toward an origin-centered ball of radius bounded by ρ, with an $\mathcal{L}_2$ performance index matrix $\Gamma = \begin{pmatrix} \gamma_1 & 0 \\ 0 & \gamma_2 \end{pmatrix}$ from $\delta(t)$ to $\eta(t)$, if there exist matrices $P = P^T > 0$, K_o, K_c, positive scalars α and ρ, solution of the optimization problem:*

$$min_{\{P,\alpha,K_o,K_c\}}\, \rho \qquad \text{s.t.}$$

$$\begin{pmatrix} Q & I \\ I & -\rho I \end{pmatrix} < 0 \tag{17}$$

$$\alpha\Psi < \rho \tag{18}$$

with

$$Q = \begin{pmatrix} A_a^TP + PA_a + \alpha^{-1}PB_aB_a^TP & PC_a \\ C_a^TP & -\Gamma \end{pmatrix} \tag{19}$$

Proof 1. *Let us define the following Lyapunov function:*

$$V(t) = \eta^T(t)P\eta(t) \tag{20}$$

where $P = P^T > 0$. According to (14), its time derivative is given by:

$$\begin{aligned} &\dot{V}(t) = \eta^T(t)(A_a^TP + PA_a)\eta(t) + a^T(t)B_a^TP\eta(t) \\ &+\eta^T(t)PB_Aa(t) + \delta^T(t)C_a^TP\eta(t) + \eta^T(t)PC_a\delta(t) \end{aligned} \tag{21}$$

Based on the following lemma:

Lemma 1. *Consider two matrices X and Y with appropriate dimensions and α a positive scalar. The following property is verified*

$$X^TY + Y^TX \leq \alpha X^TX + \alpha^{-1}Y^TY \tag{22}$$

and the following assumption:

$$||a(t)||^2 \le \Psi,\ \Psi \ge 0 \tag{23}$$

The Lyapunov derivative is then bounded by:

$$\begin{aligned}\dot V(t) &\le \eta^T(t)(A_a^TP+PA_a)\eta(t)+\alpha\Psi+\alpha^{-1}\eta^T(t)PB_aB_a^TP\eta(t)\\ &\quad+\delta^T(t)C_aP\eta(t)+\eta^T(t)PC_a\delta(t)\end{aligned} \tag{24}$$

the $\mathcal{L}_2$ attenuation from $\delta(t)$ to $\eta(t)$ is satisfied if:

$$\dot V(t)+\eta^T(t)\eta(t)-\delta^T(t)\Gamma\delta(t)<0 \tag{25}$$

which leads to:

$$x_a^T(t)Qx_a(t)+\alpha\Psi<0 \tag{26}$$

with $x_a(t)=\begin{pmatrix}\eta(t)\\ \delta(t)\end{pmatrix}$ and $Q=\begin{pmatrix}A_a^TP+PA_a+\alpha^{-1}PB_aB_a^TP & PC_a\\ C_a^TP & -\Gamma\end{pmatrix}$.

Let us define

$$\beta=\min\{\lambda_{min}(-Q)\} \tag{27}$$

and

$$\gamma=\max\{\alpha\Psi\} \tag{28}$$

where $\lambda_{min}(M)$ and $\lambda_{max}(M)$ correspond to the smallest and largest eigenvalues of a matrix M, respectively.

Since α_1 and Ψ are both positive scalars, it follows that (26) is true for

$$Q<0 \quad \text{and} \quad ||x_a(t)||_2^2>\frac{\beta}{\gamma} \tag{29}$$

which means that, according to the Lyapunov stability theory [4,25], $x_a(t)$ is uniformly bounded and converges to an origin-centered ball of radius $\sqrt{\frac{\beta}{\gamma}}$.

In order to improve the convergence criterion, the objective is to minimize the convergence radius $\sqrt{\frac{\beta}{\gamma}}$. We have:

- γ is bounded by ρ from (28) and (18).
- From (17), with a Schur's complement, it obviously follows that:

$$(1/\rho)I<-Q \tag{30}$$

implying that all the eigenvalues of $(-Q)$ are larger than $1/\rho$. As a consequence, $1/\rho<\beta$ holds, and finally the radius of the ball is bounded by ρ.

2.2. Event-triggered strategy design

In an event-triggered implementation, the input signal of the plant $u(t)$ is not transmitted to the controller at every sampling instant, rather this is done only at the transmission times that are denoted by t_k. As mentioned previously, the event-triggered implementation of the feedback control consists in maintaining the control value constant as long as the triggering condition is not satisfied and updating its value when the condition is satisfied. The triggering times t_k are then determined based on the following strategy:

It is assumed that the input signal is transmitted only when the following condition:

$$\bar e_y^T(t)\bar e_y(t)-\gamma_1\delta^T(t)\delta(t)<0 \tag{31}$$

is not satisfied, with $\bar e_y(t)=\tilde y(t)-\hat y(t)$; i.e., when

$$\bar e_y^T(t_{k+1})\bar e_y(t_{k+1})-\gamma_1\delta^T(t_{k+1})\delta(t_{k+1})\ge 0$$

assuming that the initial values satisfy the inequality (31).

Hence, in our framework, a control input is transmitted only when the difference between the latest transmitted value and the current calculated input is sufficiently large as compared to the current value. Hence, in this setup unnecessary usage of the transmission bandwidth and data overloading are avoided [7].

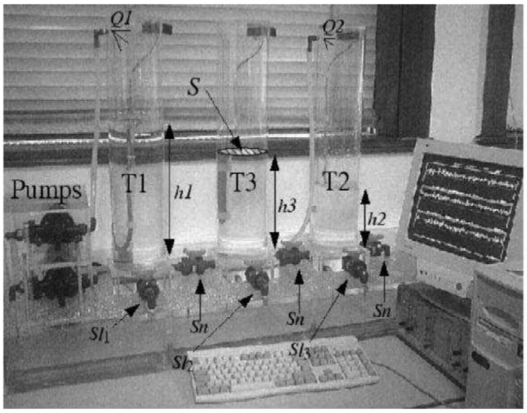

Fig. 1. Physical structure of the three-tank system.

It should be noted that condition (31) comes from the $\mathcal{L}_2$ attenuation previously used for the stability proof. Indeed, the attenuation matrix Γ from $\delta(t)$ to $\eta(t)$ may be chosen as a diagonal matrix $\Gamma=\begin{pmatrix}\gamma_1 & 0\\ 0 & \gamma_2\end{pmatrix}$ with an attenuation rate of $\sqrt{\gamma_1}$ on $e(t)$ and $\sqrt{\gamma_2}$ on $\varepsilon_{eq}(t)$.

Considering the attenuation on the state estimation error, we can write:

$$e^T(t)e(t)-\gamma_1\delta^T(t)\delta(t)<0 \tag{32}$$

which is equivalent to have:

$$||e(t)||_2^2<\gamma_1||\delta(t)||_2^2 \tag{33}$$

The updating condition is then given by:

$$||e(t)||_2^2\ge\gamma_1||\delta(t)||_2^2 \tag{34}$$

From the definition of $\bar e_y(t)$, we can write:

$$\bar e_y(t)=\tilde y(t)-\hat y(t)=e(t)+\Gamma^y a^y(t)\Rightarrow||\bar e_y(t)||_2^2\ge||e(t)||_2^2 \tag{35}$$

(34) become:

$$||\bar e_y(t)||_2^2\ge||e(t)||_2^2\ge\gamma_1||\delta(t)||_2^2 \tag{36}$$

which is equivalent to the violation of condition (31).

3. Application

In order to illustrate the efficiency of the proposed approach, simulations are conducted on a real-time laboratory three tank system. A Matlab/Simulink environment with characteristics as close as possible to the real time system is used for the simulation part. The considered AMIRA DTS200 laboratory equipment [1] consists of three interconnected cylindrical tanks. Valve positions are controlled and measured by electrical signals, which allows precise positioning.

In the conducted experiment, the process is supposed to be connected to the network for receiving the controller order and sending the sensor measurements, which makes it hackable via data deception attacks.

The experimental setup is based on a pilot three-tank system, manufactured by "AMIRA" industry (Fig. 1). The plant consists of three cylinders T_1, T_2, T_3 with cross-section S. These are connected serially with one another cylindrical pipes with a cross-section S_n. The out-flowing liquid (usually distilled water) is collected in a reservoir, which supplies the pumps 1 and 2. Here, the circle is closed. The three water levels (in m) are denoted h_1, h_2 and h_3. They are measured via piezo-resistive pressure sensors. Q_1 and

Q_2 (in V) are the flow rates of the pumps 1 and 2. The pumps are rotational-speed controlled such that a well-defined incoming mass flow corresponds to the reference input introduced by the pump controller. The fault in this study models a leakage in the third tank.

The implemented controller is the one given by Eq. (4) corresponding to the combination between the observer state feedback and event-based approach.

To model the dynamics of this multiple-input/multiple-output system, the *Torricielli* rule is used. The following model (37) is deduced from the nonlinear model using a first-order approximation around an equilibrium point.

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) \end{cases} \tag{37}$$

where $u = \begin{pmatrix} Q_1 & Q_2 \end{pmatrix}^T$ is the controlled inputs and $y = \begin{pmatrix} h_1 & h_2 & h_3 \end{pmatrix}^T$ represents the measured outputs.

The system matrices are the following:

$$A = \begin{pmatrix} -k_1 a_{10} & 0 & k_1 a_{10} \\ 0 & -k_3 a_{30} - k_2 a_{20} & k_3 a_{30} \\ k_1 a_{10} & k_3 a_{30} & -k_1 a_{10} k_3 a_{30} \end{pmatrix}, C = I_3$$

$$B = \frac{1}{S}\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

w_i, k_i and a_{i0} for $i = 1, 2, 3$ are constant parameters and the nominal values of the outflow coefficients. k_i are defined as follows:

$$k_1 = \frac{S_n\sqrt{2g}}{2S\sqrt{h_1^* - h_3^*}}, \ k_2 = \frac{S_n\sqrt{2g}}{2S\sqrt{h_2^*}}, \ k_1 = \frac{S_n\sqrt{2g}}{2S\sqrt{h_3^* - h_2^*}} \tag{38}$$

where $\{h_1^*, h_2^*, h_3^*\}$ denote an equilibrium point set and g the constant gravity.

The numerical values are given $S = 0.0154\ \text{m}^2$, $S_n = 510^{-5}\text{m}^2$, $h_{max} = 60$ cm, $a_1 = 0.4$, $a_2 = 0.3$, $a_3 = 0.2$, $h_1^* = 40$ cm, $h_2^* = 20$ cm, $h_3^* = 30$ cm

The proposed control law is applied to the three-tank system model. In order to appreciate the effect of the feedback and event-triggering parts, simulations results from a nonlinear simulator is first presented, ignoring the measurement noises and the effect of the DAC-DCA. The numerical method used to solve the integration and differential equations is based on the Euler method with a sampling period equal to $T_s = 10$ ms. This configuration (also used in previous application [3]) is retained since they correspond to the one used for the real experiments.

The considered experience corresponds to the following simulation: The system starts at the equilibrium point h_1^*, h_2^* and h_3^*, respectively, equal to 0.4 m, 0.2 m and 0.3 m, a change of reference occurs at $t = 200$ s, the new references to attain being fixed to 0.44sm, 0.22sm and 0.33 m for the three outputs. A simple second order polynomial path planing is also implemented for each output to track. Then, a sinusoidal variation of the outflow coefficients is simulated for $t \geq 200$ s.

We consider the worst case scenario, meaning both controllers and sensors may be hacked. In this case, the binary incidence matrices that indicate which data channels can be accessed by the attacker Γ^u and Γ^y are equal to the identity matrix I. The event condition rate Ψ is chosen to be equal to 0.1. Two data deception attempt are generated, on the first actuator for $t \geq 700$ s and first sensor for $400 \leq t \leq 700$ s.

Since (19) is still in a $\mathcal{BMI}$ form, a classical solution would be to linearize this constraint by applying well-known methods like the Schur's complement for example. However, the main drawback introduced by these methods is the conservatism which makes it difficult to find a feasible solution. For that, inequality (19) is solved here using some dedicated toolbox for $\mathcal{BMI}$ optimization problems.

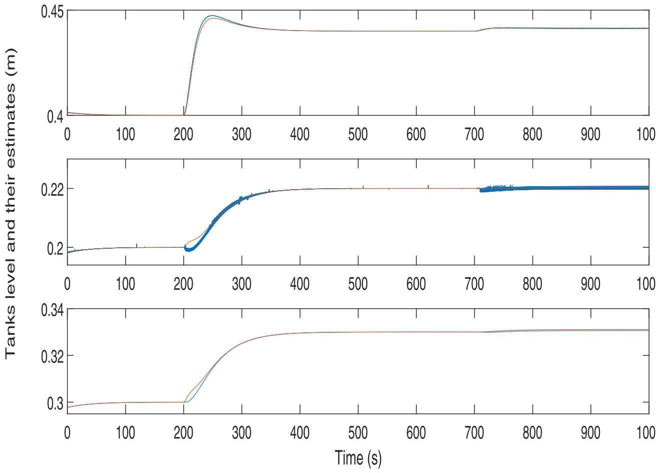

Fig. 2. Tanks level and their estimates.

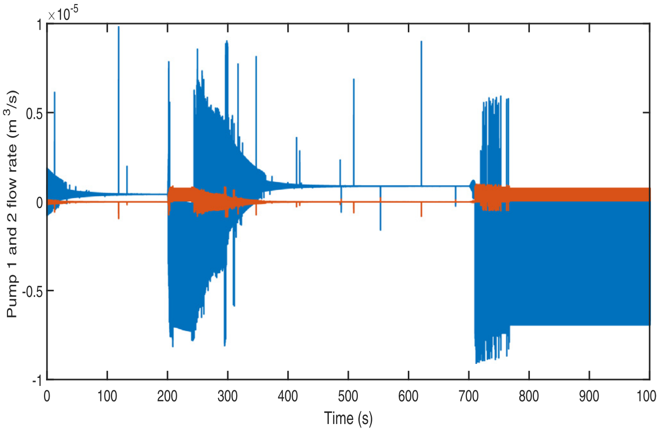

Fig. 3. Pump inputs.

For the considered example, the problem solution under the $\mathcal{BMI}$ constraint was obtained with the use of the PENBMI solver and Matlab software. In fact, PENBMI [11] is a solver for optimization problems with quadratic objective and bilinear matrix inequality constraints. The algorithm combines ideas of the exterior (penalty) and interior (barrier) methods with the Augmented Lagrangian method and is aimed at small to large-scale dense and sparse $\mathcal{LMI}$ and $\mathcal{BMI}$ problems.

$$K_c = \begin{pmatrix} -10.2938 & 0.6375 & -7.0241 \\ 0.0075 & -73.4571 & 56.8218 \end{pmatrix},$$

$$K_o = \begin{pmatrix} -0.3173 & 0.0001 & -0.0111 \\ 0.0001 & -0.3151 & 0.0001 \\ -0.0111 & 0.0001 & -0.3106 \end{pmatrix}$$

The obtained results (tanks level) are illustrated in Fig. 2, where it shows that despite of the attacks, the control is efficient as well as the estimation. The input is illustrated in Fig. 3, where the effect of the triggering control appears at each time the attack is launched.

An attack detection and isolation strategy is also performed in order to localize the data deception attacks. As for the Fault Detection and Isolation (FDI), the core element of model-based Attack Detection and Isolation (ADI) is residuals generation [16].

A first step would be the residual generation based on the full state observer designed previously. In theory, the residual signals

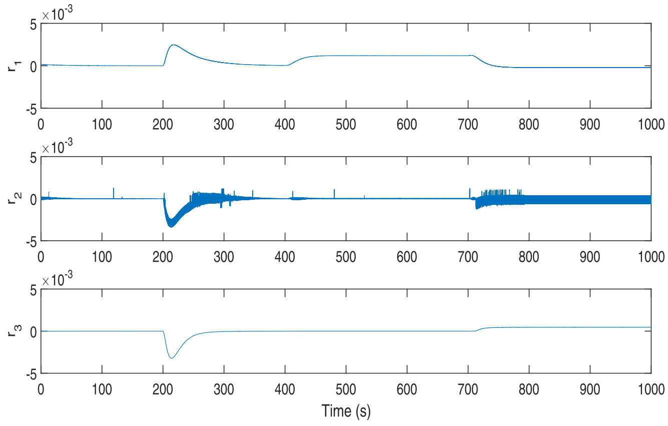

Fig. 4. Residuals.

(i.e., the output estimation error) are null (or exponentially converge to zero) under normal operating conditions of the system and it will be stated as healthy. The following Fig. 4 is then obtained.

As it is shown in Fig. 4, based on the residual shape, one can clearly see an anomaly between time slot 400 s $\leq t \leq$ 700 s and $t \geq$ 700 s. Now, for the isolation task, the so-called observer bank will be designed.

As presented in [16], one approach to fulfill the attack/fault isolation task is to design a set of structured residuals. Each residual is designed to be sensitive to a subset of attacks/fault, while remaining insensitive to the others. The design procedure consists into a setup of a bank of observers and to design the corresponding residual generators according to the considered interactions, i.e. making each residual sensitive to all but one fault.

With this bank of observers, a bank of residuals based on output estimation error is defined $r(t) = \tilde{y}(t) - \hat{y}(t)$. A fault signature localization based on the residual shape is the considered. In order to generate appropriated fault indicators, the residual signal structuring can be obtained by replacing the use of only one observer by the use of a bank of observers where each observer is driven by a partial set of the available signals [5].

In order to generate appropriated attack indicators, the residual signals obtained are depicted in Fig. 5.

From the depicted figure, for the first bank observer where the residues are obtained from a partial observer (based only on the second and third output), a clear disturbance appear at $t \geq 700$s on residues $r_{12} = \tilde{y}_{12} - \hat{y}_{12}$ and $r_{13} = \tilde{y}_{13} - \hat{y}_{13}$, which corresponds to the first actuator attack. From the second bank observer (based only on the first and third output), a two steps disturbance appears on the first residual $r_{21} = \tilde{y}_{21} - \hat{y}_{21}$, which corresponds to the first actuator attack at $t \geq 700$s and first sensor attack at $400\text{s} \leq t \leq 700$s. Finally, for the third bank observer (based only on the first and second output), both effects of the sensor and actuator attacks appear respectively at $400\text{s} \leq t \leq 700$s and $t \geq 700$s, which confirms the previously obtained figure.

4. Conclusion

In the presented paper, an attack/fault tolerant control based on event-triggered control system was presented. The observer based state feedback controller ensures the convergence to a desired constant reference with an converging estimation error toward an origin-centered ball of an optimal and bounded radius. The triggering mechanism that determines when the control input has to be updated again is deduced when the error exceeds a chosen threshold value.

The proposed design was applied to a real-time laboratory three tank system subject to data deception attempt on sensor and actuator, with satisfying control results. An attack detection/isolation design based on a structured bank of observers with convincing results was also presented.

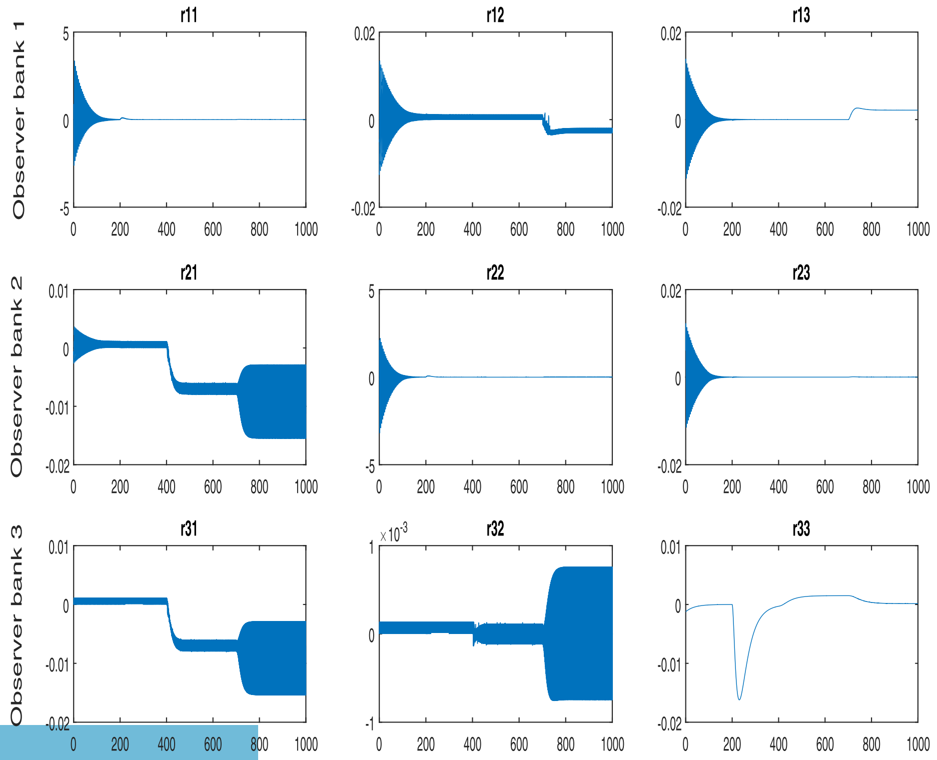

Fig. 5. Bank observer residuals.

References

[1] Amira, Three-tank system DTS200, Munich, Germany, Technical Report, 2002.

[2] K. Âström, B. Bernhardsson, Comparison of periodic and event based sampling for first-order stochastic systems, in: Proceedings of the Fourteenth World Congress of IFAC, Beijing, China, 1999.

[3] S. Bezzaoucha, D. Henry, An LMI approach for the integral sliding mode and h_∞ state feedback control problem, J. Phys.: Conf. Ser. (659–012052) (2015), doi:10.1088/1742-6596/659/1/012052.

[4] S. Bezzaoucha, B. Marx, D. Maquin, J. Ragot, State and output feedback control for Takagi–Sugeno systems with saturated actuators, Int. J. Adapt. Control Signal Process. 30 (6) (2016).

[5] S. Bezzaoucha, H. Voos, M. Darouach, A contribution to cyber-security of networked control systems: an event-based control approach, in: Proceedings of the Third International Conference on Event-Based Control, Communication and Signal Processing, Funchal, Madeira, Portugal, 2017.

[6] S. Bezzaoucha Rebaï, H. Voos, M. Darouach, Observer-based event-triggered attack-tolerant control design for cyber-physical systems, in: Proceedings of the Fourteenth International Workshop on Advanced Control and Diagnosis, Bucharest, Romania, 2017.

[7] M. Davoodi, N. Meskin, K. Khorasani, Event-triggered robust h_∞ control for linear systems, IEEE Trans. Ind. Inform. 13 (1) (2017) 298–311.

[8] H. Fawzi, P. Tabuada, S. Diggavi, Secure estimation and control for cyber-physical systems under adversarial attacks, IEEE Trans. Autom. Control 59 (4) (2014) 1454–1467.

[9] W. Heemels, K. Johansson, P. Tabuada, An introduction to event-triggered and self-triggered control, in: Proceedings of the IEEE Fifty-first Annual Conference on Decision and Control (CDC), 2012.

[10] W. Heemels, K. Johansson, P. Tabuada, Event-triggered and self-triggered control, in: J. Baillieul T. Samad (Eds.), Springer-Encyclopedia of Systems and Control, pp. 384–391. doi:10.1007/978-1-4471-5058-9-97.

[11] M. Kocvara, M. Stingl, Penbmi User's Guide (version 2.1), 2006,.

[12] M. Miskowicz, Send-on-delta concept: an event-based data reporting strategy, Sensors 6 (1) (2006) 49–63.

[13] M. Pajic, J. WeiBezzo, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, G. Pappas, Robustness of attack-resilient state estimators, in: Proceedings of the ACM/IEEE Fourth International Conference on Cyber-Physical Systems (ICCPS), Berlin, Germany, 2014.

[14] M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G. Pappas, I. Lee, Design and implementation of attack-resilient cyber-physical systems, IEEE Control Syst. Mag. 37 (2) (2017) 66–81.

[15] F. Pasqualetti, F. Dörfer, F. Bullo, Cyber-physical security via geometric control: Distributed monitoring and malicious attacks, in: Proceedings of the IEEE Conference on Decision and Control, Hawai, USA, 2012.

[16] R. Patton, J. Chen, Observer-based fault detection and isolation: robustness and applications, Control Eng. Pract. 5 (5) (1997) 671–682.

[17] H. Shen, F. Li, H. Yan, H. Karimi, H.-K. Lam, Finite-time event-triggered $\mathcal{H}_\infty$ control for t-s fuzzy Markov jump systems, IEEE Trans. Fuzzy Syst. (2018), doi:10.1109/TFUZZ.2017.2788891.

[18] D. Shi, L. Shi, T. Chen, Event-Based State Estimation: A Stochastic Perspective, Springer International Publishing, 2016.

[19] P. Tabuada, Event-triggered real time scheduling of stabilizing control tasks, IEEE Trans. Autom. Control 52 (9) (2007) 1680–1685.

[20] S. Tarbouriech, A. Seuret, J.M. Gomes da Silva Jr, D. Sbarbaro, Observer-based event-triggered control co-design for linear systems, IET Control Theory Appl. 10 (18) (2016) 2466–2473.

[21] A. Teixeira, Toward cyber-secure and resilient networked control systems, Ph.D. thesis, KTH Royal Institute of Technology, Stockholm, Sweden, 2014.

[22] A. Teixeira, D. Pérez, H. Sabdberg, K. Johansson, Attack models and scenarios for networked control systems, in: Proceedings of the First International Conference on High Confidence Networked Systems (HiCoNS), Beijing, China, 2012.

[23] H. Yan, C. Hu, H. Zhang, H. Karimi, M. Jiang, X. Liu, h_∞ output tracking control for networked systems with adaptively adjusted event-triggered scheme, IEEE Trans. Syst. Man Cybern. (2018) 1–9, doi:10.1109/TSMC.2017.2788187.

[24] P. Young, J. Willems, An approach to the linear multivariable servomechanism problem, Int. J. Control 15 (5) (1972) 961–979.

[25] K. Zhang, B. Jiang, P. Shi, A new approach to observer-based fault-tolerant controller design for Takagi–Sugeno fuzzy systems with state delay, Circuits Syst. Signal Process. 28 (5) (2009) 679–697.