Event-Based Control Approach to Cyber-Security for Complex Discrete-time Networked Systems

Eya Hassine *, Assem Thabet, Noussaiba Gasmi, Ghazi Bel Hajfrej

Posted Date: 8 May 2025

doi: 10.20944/preprints202505.0587.v1

Keywords: fault tolerant attack; cyber-physical systems; output feedback control; event-triggered mechanisms; luenberger observer; bilinear matrix inequalities; linear matrix inequalities

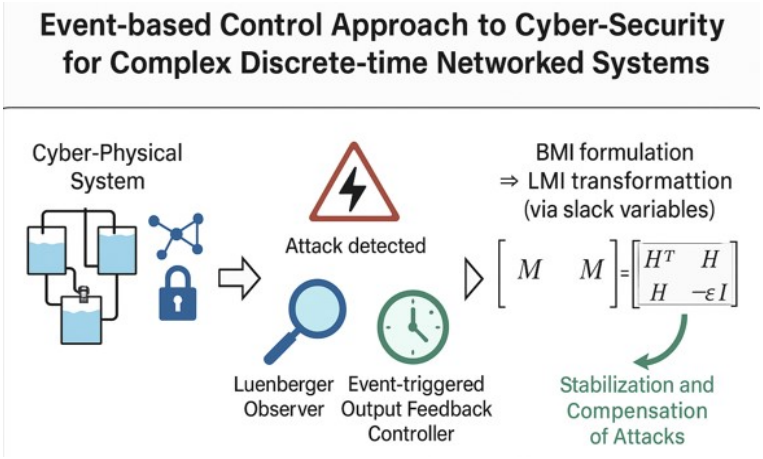
Article

Event-Based Control Approach to Cyber-Security for Complex Discrete-Time Networked Systems

Eya Hassine [1,2,*,†,‡], Assem Thabet [1,‡], Noussaiba Gasmi [2,‡] and Ghazi Bel Hajfrej [3,‡]

[1] Research Lab MACS, University of Gabes, Tunisia; ayahassine118@gmail.com; assem.thabet@yahoo.fr
[2] Laboratoire d'Informatique & Telecommunications, ECAM Louis de Broglie; noussaiba.gasmi@ecam-rennes.fr
[3] IMS Laboratory, CNRS UMR 5218, Bordeaux INP, University of Bordeaux; ghazi.bel haj frej@bordeaux-inp.fr
* Correspondence: ayahassine118@gmail.com
† Current address: Research Lab MACS, University of Gabes, Tunisia.
‡ These authors contributed equally to this work.

Abstract: This paper presents an observer-based FTA compensation strategy with ETM to enhance cybersecurity in discrete-time CPS. The proposed method leverages advanced mathematical lemmas and BMI resolution techniques to synthesize an output feedback control scheme capable of reconstructing system states and generating corrective control actions. By integrating Lyapunov theory, the approach formulates the control synthesis as an optimization problem with BMI constraints. A switching criterion dynamically adjusts control parameters, while the introduction of slack variables transforms the originally nonlinear BMI into a more tractable LMI form. This modification enhances computational efficiency and flexibility in solving the optimization problem. The effectiveness of the proposed strategy is validated through numerical simulations on a three-tank system, demonstrating its applicability in real-world CPS scenarios.



Keywords: fault tolerant attack; cyber-physical systems; output feedback control; event-triggered mechanisms; luenberger observer; bilinear matrix inequalities; linear matrix inequalities

1. Introduction

Advances in mathematics, physics, computer science, and engineering over the last twenty years have enabled the development of novel stabilization and monitoring techniques for complex systems [1–7]. This progress has significantly increased the importance and sophistication of Control-Supervision Systems, particularly in communication networks [8–10]. Given the growing need for safety and resilience, research has increasingly focused on Fault-Tolerant and FTA systems [11–14]. Ensuring resilience in FTA design is critical for maintaining operational efficiency under abnormal conditions, a necessity for modern industrial supervision systems [15,16]. Unlike conventional systems, where cyber-security primarily safeguards data, NCSs face threats from CA that manipulate physical processes via feedback mechanisms [17]. This distinction highlights the importance of integrating

control approaches to improve NCS security by analyzing the interplay between CA and control algorithms, particularly their physical impacts [18–20].

Extensive research has explored CA detection and mitigation, with particular attention to false data injection and physical attack models. These studies emphasize mathematical modeling of CA and their disruptive effects on controlled processes. Using dynamic process models and control algorithms, CAs can be effectively identified. Among the most studied attack vectors are physical intrusions, which remain key considerations in NCS security analysis [21]. For instance, numerous methodologies have been proposed to detect and assess such attacks in CPS:

- Graph-Theoretic Analysis: Using graph theory [22] to model complex system structures and pinpoint vulnerabilities in network control systems.
- Secure Set Theory: Employ maximal robustly controlled invariant sets [23] to strengthen the resilience of the system against external disturbances and uncertainties.
- Frequency-Domain Attack Analysis: Investigating the effects of CA on control inputs and outputs using frequency domain techniques [24,25].
- Distributed Consensus Control: Applying discontinuous observation-based control consensus principles to linear multi-agent systems [26] for enhanced reliability in distributed architectures.
- Event-Triggered-State Feedback: Implement consensus control via event-triggered state feedback [27] to reduce network congestion while maintaining system performance.
- Adaptive Fault-Tolerant Control: Design of controllers that depend on the state in time [28] to improve robustness against faults and dynamic uncertainties.
- Observer-Based Protocol Synthesis: Developing topology-dependent Lyapunov functions for observer-based protocols with nonlinear Lipschitz dynamics [29], ensuring stability in large-scale networked systems.
- Sampled-Data Observers: Utilizing programmable sampled-data observers [30,31] for real-time CA detection and mitigation.

While extensive research has addressed continuous-time systems, complex discrete-time systems have received comparatively limited attention in the literature [32,33]. Furthermore, existing observer-based approaches predominantly utilize state feedback mechanisms rather than output feedback strategies. To bridge these research gaps, this study introduces novel security measures employing observer-based output feedback controls specifically designed for discrete-time systems. The proposed framework simultaneously addresses both safety and security considerations through model-based attack detection using observers. By comparing estimated process outputs with actual measurements, the method identifies discrepancies and triggers appropriate corrective actions, enabling effective attack and fault detection.

The key contributions of this work include:

- Developments of an innovative Event-Triggered with output feedback control strategy for cyber-physical discrete-time systems, contrasting with conventional continuous-time approaches. The proposed method specifically resolves the technical challenges of implementing output feedback in faulty system models, advancing beyond traditional state feedback limitations.
- Significant generalization capabilities, being successfully adapted to both nonlinear Lipschitz systems and decentralized architectures. This extension substantially broadens the method's potential applications in complex networked environments.
- The introduction of supplementary decision variables enhances the convex optimization formulation, providing greater design flexibility. Through innovative slack variable techniques, the linearization of complex bilinear terms in the BMI formulation is formulated, yielding more computationally tractable solutions.
- Simulation studies validate the proposed approach's effectiveness, with results indicating strong potential for real-time implementation using digital signal processing platforms. These findings demonstrate practical feasibility for industrial applications.

The paper is organized as follows: preliminary concepts and the problem statement are presented, followed by the synthesis of an attack-tolerant controller. Numerical validation on an example is then provided, concluding with insights for future research directions.

Notation: The following notation will be used throughout this paper:

- In a matrix, the notation $(\star)$ is used for the blocks induced by symmetry.
- $\bar{Q}^T$ is the transposed matrix of $\bar{Q}$, if $\bar{Q}$ is a square matrix then the notation $\bar{Q} > 0$ ($\bar{Q} < 0$) means that $\bar{Q}$ is positive definite (negative definite).
- The set $\mathrm{Co}(x, y) = \{\lambda x + (1-\lambda)y, 0 \leq \lambda \leq 1\}$ is the convex hull of x, y.

2. Problem Statement and Preliminaries

This section outlines a modeling framework to address various types of attacks with event trigged control systems. The cyber-physical system can be represented by:

$$\begin{aligned} x_{k+1}^i &= \underline{A_i} x_k^i + \underline{B_i} \tilde{u}_k^i + \underline{F_i} \overline{f_k^i} \\ y_k^i &= \underline{C_i} x_k^i \end{aligned} \tag{1}$$

The global system is :

$$\begin{aligned} x_{k+1} &= \underline{A} x_k + \underline{B} \tilde{u}_k + \underline{F} \overline{f_k} \\ y_k &= \underline{C} x_k \end{aligned} \tag{2}$$

Where $x_k(t) \in R^{n_x}$ represent the sate vector, $y_k(t) \in R^{n_y}$ is the output vector, $\tilde{u}_k \in R^{n_u}$ is the control vector, $\overline{f_k} \in R^{n_f}$ is the unknown inputs represents the effect of faults, $\underline{A} = \mathrm{diag}\{\underline{A_i}\}, \underline{B} = \mathrm{diag}\{\underline{B_i}\}, \underline{C} = \mathrm{diag}\{\underline{C_i}\}, \underline{F} = \mathrm{diag}\{\underline{F_i}\}$ are constant matrices of appropriate dimensions.

In this particular system, our focus lies in exploring a method for detecting and identifying attacks primarily through a model designed to detect and estimate attack signals within two communication channels. The diagram in Figure 1 provides an overview of the general control/supervision structure of interconnected cyber-physical systems.

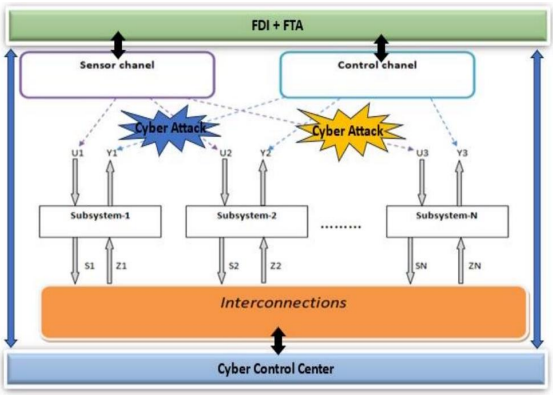


Figure 1. General diagram of the control scheme.

Cyber-attacks can simultaneously impact control and/or observation communication chains, as well as interconnection functions. The latter will be modeled in the following by: $\underline{b_{k^u}}$ and $\underline{b_{k^y}}$ which represent the data corruption / modification on the control sequences and measurements respectively. Following this, the FDI function will be executed through the synthesized observers. This will furnish the Cyber Control Center with crucial information regarding the nature and location of the cyber-attack, thereby enabling it to compute or update the command via a event-trigged strategy.

For this, the designed Luenberger observer is :

$$\begin{aligned} \hat{x}_k &= \underline{A} \hat{x}_k + \underline{B} u_k + \overline{L}(\tilde{y}_k - \hat{y}_k) \\ \hat{y}_k &= \underline{C} \hat{x}_k \end{aligned} \tag{3}$$

The control signal, by principle of output feedback, is designed with the following form:

$$u_k = \overline{K_1}\hat{y}_k + \overline{K_2}\tilde{y}_k \tag{4}$$

The faults and attacks are modeled as follows:
- $\overline{f_k}$ simulates errors modeling, faults, unknown input, disturbances.
- Since data corruption / modification can change the control sequences and measurements provided by the different sensors from their actual calculations or values u_k, y_k to corrupted signals $\tilde{u}_k$ and $\tilde{y}_k$. False attacks are modelled by:

$$\begin{aligned} \tilde{u}_k &= u_k + \underline{\Gamma^u}\overline{b_k^u} \\ \tilde{y}_k &= y_k + \underline{\Gamma^y}\overline{b_k^y} \end{aligned} \tag{5}$$

With $\overline{b_k^u}$ and $\overline{b_k^y}$ represents the pirated data. $\underline{\Gamma^u}$ and $\underline{\Gamma^y}$ are the binary impact matrices indicating which data strings can be accessed by the 'hacker'.

Now we define a new variable $\overline{\alpha_k}$, group the fault/attack signals as follows: $\overline{\alpha_k} = \begin{bmatrix} \overline{f_k} & \overline{b_k^u} & \overline{b_k^y} \end{bmatrix}^T$. This allows us to rewrite the augmented system (system + observer) as follows:

$$\begin{aligned} \eta_{k+1} &= \underline{A_\alpha}\overline{\eta_k} + \underline{B_\alpha}\overline{\alpha_k} \\ y_\alpha &= \underline{C_\alpha}\overline{\eta_k} \end{aligned} \tag{6}$$

With $\overline{\eta_k} = \begin{bmatrix} x_k \\ \hat{x}_k \end{bmatrix}, \overline{y_\alpha} = \begin{bmatrix} y_k \\ \hat{y}_k \end{bmatrix}$

$$\underline{A_\alpha} = \begin{bmatrix} \underline{A} + \underline{B}\overline{K_2}\underline{C} & \underline{B}\overline{K_1}\underline{C} \\ \overline{L}\underline{C} + \underline{B}\overline{K_2}\underline{C} & \underline{A} - \overline{L}\underline{C} + \underline{B}\overline{K_1}\underline{C} \end{bmatrix}$$

$$\underline{B_\alpha} = \begin{bmatrix} \underline{F} & \underline{B\Gamma^u} & \underline{B}\overline{K_2}\underline{\Gamma^y} \\ 0 & 0 & (\overline{L} + \underline{B}\overline{K_2})\underline{\Gamma^y} \end{bmatrix}, \underline{C_\alpha} = \begin{bmatrix} \underline{C} & 0 \\ 0 & \underline{C} \end{bmatrix}$$

Then the following lemmas are considered:
Lemma 1: [34] Given two matrices $\underline{M}, \underline{N}$, of appropriate dimensions, then the following inequality holds for any constant $\underline{\beta} > 0$

$$\underline{M}^T\underline{N} + \underline{N}^T\underline{M} \leq \underline{\beta}\underline{M}^T\underline{M} + \underline{\beta}^{-1}\underline{N}^T\underline{N} \tag{7}$$

Lemma 2: [34] Consider a nonlinear function $h : \mathbb{R}^n \to \mathbb{R}^n$, the following two items are equivalent: h is globally Lipschitz with respect to its argument, i.e.,

$$\|h(a) - h(b)\| \leq \underline{l}\|a - b\| \tag{8}$$

There exist constants h_{ij} and $\overline{h_{ij}}$ so that for all $\forall a, b \in \mathbb{R}^n$ there exist $r_i \in \mathrm{Co}(a, b), r_i \neq a, r_i \neq b$ and functions $h_{ij} : \mathbb{R}^n * \mathbb{R}^n$ satisfying the following equality:

$$h(a) - h(b) = \sum_{i,j=1}^{q,n} h_{ij}(r_i)H_{ij}(a - b) \tag{9}$$

And $\underline{h_{ij}} \leq h_{ij}(r_i) \leq \overline{h_{ij}}$ where $h_{ij}(r_i) = \frac{\partial h_i}{\partial h_j}(r_i)$ and $H_{ij} = e_q(i)e_n^T(j)$

3. FTA Control Synthesis

This section is dedicated to the development of the new FTA synthesis. The main result is given by the following Theorem:

Theorem 1: *There exists an asymptotic stable observer of the form (3) and an event-based fault-attack tolerant controller (4), with a triggering condition* $\|\overline{\alpha_k}\|^2 \leq \underline{\sigma}\|\overline{\eta_k}\|^2$, *for the system (2), if there exist positive symmetric matrices* $\overline{P} = \begin{bmatrix} \overline{P_1} & 0 \\ 0 & \overline{P_2} \end{bmatrix}$, *matrices* $R = \overline{P_2}\underline{L}$, $\overline{K_1}$, $\overline{K_2}$ *and a positive scalar* $\underline{\beta}$, *solution if the following BMI is feasible:*

$$\begin{bmatrix} \underline{A_\alpha}^T\overline{P}\underline{A_\alpha} - \overline{P} & \underline{A_\alpha}^T\overline{P}\underline{B_\alpha} & 0 \\ \star & \left(\underline{\beta}^{-1}I\right)^{-1} & 0 \\ \star & \star & \underline{B_\alpha}^T\overline{P}\underline{B_\alpha} + \underline{\sigma}\underline{\beta}I \end{bmatrix} < 0 \tag{10}$$

With: $\overline{P_2} = \underline{\mu}\overline{P_1}, \overline{L} = (\underline{\mu}\overline{P_1})^{-1}R, \overline{K_1} = \underline{B}^+\overline{P_1}^{-1}Z_1, \overline{K_2} = \underline{B}^+\overline{P_1}^{-1}Z$.

Proof

To determine the different control and observer gains, a stability analysis is based on the Lyapunov function:

$$\overline{\Delta V} = \bar{V}_{k+1} - \bar{V}_k < 0 \tag{11}$$

With $\bar{V}_k = \overline{\eta_k^T}\overline{P}\overline{\eta_k}, \bar{V}_{k+1} = \overline{\eta_{k+1}^T}\overline{P}\overline{\eta_{k+1}}$.

Now using **lemma 1** on $\overline{\Delta V}$, the latter becomes:

$$\begin{aligned} \overline{\Delta V} = \overline{\eta_k^T}\left[\underline{A_\alpha}^T\overline{P}\underline{A_\alpha} + \underline{\beta}^{-1}\underline{A_\alpha}^T\overline{P}\underline{B_\alpha}\underline{B_\alpha}^T\overline{P}\underline{A_\alpha} - \overline{P}\right]\overline{\eta_k} \\ + \overline{\alpha_k^T}\left[\underline{B_\alpha}^T\overline{P}\underline{B_\alpha} + \underline{\sigma}\underline{\beta}I\right]\overline{\alpha_k} < 0 \end{aligned} \tag{12}$$

Thus, the stability condition can be given by

$$\overline{\Delta V} < 0 \equiv \bar{Q} < 0 \tag{13}$$

We apply Schur's complement using $\|\overline{\alpha_k}\|^2 \leq \underline{\sigma}\|\overline{\eta_k}\|^2$, we obtain:

$$\bar{Q} = \begin{bmatrix} \underline{A_\alpha}^T\overline{P}\underline{A_\alpha} - \overline{P} & \underline{A_\alpha}^T\overline{P}\underline{B_\alpha} & 0 \\ \star & (\underline{\beta}^{-1}I)^{-1} & 0 \\ \star & \star & \underline{B_\alpha}^T\overline{P}\underline{B_\alpha} + \underline{\sigma}\underline{\beta}I \end{bmatrix} \tag{14}$$

Where:

- $\underline{A_\alpha}^T\overline{P}\underline{A_\alpha} - \overline{P} = \begin{bmatrix} \overline{R_{11}} & \overline{R_{12}} \\ \overline{R_{21}} & \overline{R_{22}} \end{bmatrix}$

with:

$\overline{R_{11}} = \underline{A}^T\overline{P_1}\underline{A} + \underline{A}^T\overline{P_1}\underline{B}\overline{K_2}\underline{C} + \underline{C}^T\overline{K_2}^T\underline{B}^T\overline{P_1}\underline{A} + \underline{C}^T\overline{K_2}^T\underline{B}^T\overline{P_1}\underline{B}\overline{K_2}\underline{C} + \underline{C}^T\overline{K_2}^T\underline{B}^T\overline{P_2}\underline{B}\overline{K_2}\underline{C} + \underline{C}^T\overline{K_2}^T\underline{B}^T\overline{P_2\underline{L}}\underline{C} + \underline{C}^T\overline{L}^T\overline{P_2}\underline{B}\overline{K_2}\underline{C} + \underline{C}^T\overline{L}^T\overline{P_2\underline{L}}\underline{C} - \overline{P_1}$

$\overline{R_{12}} = \underline{A}^T\overline{P_1}\underline{B}\overline{K_1}\underline{C} + \underline{C}^T\overline{K_2}^T\underline{B}^T\overline{P_1}\underline{B}\overline{K_1}\underline{C} + \underline{C}^T\overline{K_2}^T\underline{B}^T\overline{P_2}\underline{A} - \underline{C}^T\overline{K_2}^T\underline{B}^T\overline{P_2\underline{L}}\underline{C} + \underline{C}^T\overline{K_2}^T\underline{B}^T\overline{P_2}\underline{B}\overline{K_1}\underline{C} + \underline{C}^T\overline{L}^T\overline{P_2}\underline{A} - \underline{C}^T\overline{L}^T\overline{P_2\underline{L}}\underline{C} + \underline{C}^T\overline{L}^T\overline{P_2}\underline{B}\overline{K_1}\underline{C}$

$\overline{R_{21}} = \underline{C}^T\overline{K_1}^T\underline{B}^T\overline{P_1}\underline{A} + \underline{C}^T\overline{K_1}^T\underline{B}^T\overline{P_1}\underline{B}\overline{K_2}\underline{C} + \underline{A}^T\overline{P_2}\underline{B}\overline{K_2}\underline{C} + \underline{A}^T\overline{P_2\underline{L}}\underline{C} - \underline{C}^T\overline{L}^T\overline{P_2}\underline{B}\overline{K_2}\underline{C} - \underline{C}^T\overline{L}^T\overline{P_2\underline{L}}\underline{C} + \underline{C}^T\overline{K_1}^T\underline{B}^T\overline{P_2}\underline{B}\overline{K_2}\underline{C} + \underline{C}^T\overline{K_1}^T\underline{B}^T\overline{P_2\underline{L}}\underline{C}$

$\overline{R_{22}} = \underline{C}^T\overline{K_1}^T\underline{B}^T\overline{P_1}\underline{B}\overline{K_1}\underline{C} + \underline{A}^T\overline{P_2}\underline{A} - \underline{A}^T\overline{P_2\underline{L}}\underline{C} + \underline{A}^T\overline{P_2}\underline{B}\overline{K_1}\underline{C} - \underline{C}^T\overline{L}^T\overline{P_2}\underline{A} + \underline{C}^T\overline{L}^T\overline{P_2\underline{L}}\underline{C} - \underline{C}^T\overline{L}^T\overline{P_2}\underline{B}\overline{K_1}\underline{C} + \underline{C}^T\overline{K_1}^T\underline{B}^T\overline{P_2}\underline{A} - \underline{C}^T\overline{K_1}^T\underline{B}^T\overline{P_2\underline{L}}\underline{C} + \underline{C}^T\overline{K_1}^T\underline{B}^T\overline{P_2}\underline{B}\overline{K_1}\underline{C} - \overline{P_2}$

and:

- $\underline{A_\alpha}^T\overline{P}\underline{B_\alpha} = \begin{bmatrix} \overline{S_{11}} & \overline{S_{12}} & \overline{S_{13}} \\ \overline{S_{21}} & \overline{S_{22}} & \overline{S_{23}} \end{bmatrix}$

With:

$$\overline{S_{11}} = \underline{A}^T\overline{P_1}\underline{F} + \underline{C}^T\overline{K_2}^T\underline{B}^T\overline{P_1}\underline{F}$$

$$\overline{S_{12}} = \underline{A}^T\overline{P_1}\underline{B\Gamma^u} + \underline{C}^T\overline{K_2}^T\underline{B}^T\overline{P_1}\underline{B\Gamma^u}$$

$$\overline{S_{13}} = \underline{A}^T\overline{P_1}\underline{B\overline{K_2}\Gamma^y} + \underline{C}^T\overline{K_2}^T\underline{B}^T\overline{P_1}\underline{B\overline{K_2}\Gamma^y} + \underline{C}^T\overline{K_2}^T\underline{B}^T\overline{P_2L}\underline{\Gamma^y}$$
$$+ \underline{C}^T\overline{K_2}^T\underline{B}^T\overline{P_2}\underline{B\overline{K_2}\Gamma^y} + \underline{C}^T\overline{L}^T\overline{P_2L}\underline{\Gamma^y} + \underline{C}^T\overline{L}^T\overline{P_2}\underline{B\overline{K_2}\Gamma^y}$$

$$\overline{S_{21}} = \underline{C}^T\overline{K_1}^T\underline{B}^T\overline{P_1}\underline{F}, \overline{A_{22}} = \underline{C}^T\overline{K_1}^T\underline{B}^T\overline{P_1}\underline{B\Gamma^u}$$

$$\overline{S_{23}} = \underline{C}^T\overline{K_1}^T\underline{B}^T\overline{P_1}\underline{B\overline{K_2}\Gamma^y} + \underline{A}^T\overline{P_2L}\underline{\Gamma^y} + \underline{A}^T\overline{P_2}\underline{B\overline{K_2}\Gamma^y}$$
$$- \underline{C}^T\overline{L}^T\overline{P_2L}\underline{\Gamma^y} - \underline{C}^T\overline{L}^T\overline{P_2}\underline{B\overline{K_2}\Gamma^y} + \underline{C}^T\overline{K_1}^T\underline{B}^T\overline{P_2L}\underline{\Gamma^y}$$
$$+ \underline{C}^T\overline{K_1}^T\underline{B}^T\overline{P_2}\underline{B\overline{K_2}\Gamma^y}$$

$$\bullet \underline{B_\alpha}^T\overline{P}\underline{B_\alpha} = \begin{bmatrix} \underline{F}^T\overline{P_1}\underline{F} & \underline{F}^T\overline{P_1}\underline{B\Gamma^u} & \underline{F}^T\overline{P_1}\underline{B\overline{K_2}\Gamma^y} \\ \star & \underline{\Gamma^u}^T\underline{B}^T\overline{P_1}\underline{B\Gamma^u} & \underline{\Gamma^u}^T\underline{B}^T\overline{P_1}\underline{B\overline{K_2}\Gamma^y} \\ \star & \star & \overline{M_{33}} \end{bmatrix}$$

$$\overline{M_{33}} = \underline{\Gamma^y}^T\overline{K_2}^T\underline{B}^T\overline{P_1}\underline{B\overline{K_2}\Gamma^y} + \underline{\Gamma^y}^T\overline{L}^T\overline{P_2L}\underline{\Gamma^y} + \underline{\Gamma^y}^T\overline{L}^T\overline{P_2}\underline{B\overline{K_2}\Gamma^y} + \underline{\Gamma^y}^T\overline{K_2}^T\underline{B}^T\overline{P_2L}\underline{\Gamma^y}$$
$$+ \underline{\Gamma^y}\overline{K_2}^T\underline{B}^T\overline{P_2}\underline{B\overline{K_2}\Gamma^y}$$

Then, contrary to the various synthesis approaches considered in the literature and to give more degrees of freedom to the optimization problem, we propose the following form of the matrix $\overline{P}$:

$$\overline{P} = \begin{bmatrix} \overline{P_1} & 0 \\ 0 & \overline{P_2} \end{bmatrix} = \begin{bmatrix} \overline{P_1} & 0 \\ 0 & \underline{\mu}\overline{P_1} \end{bmatrix} \tag{15}$$

Where $\underline{\mu} > 0$.
The final step, let's consider the following proposed variables changes:

$$Z = \overline{P_1}\underline{B\overline{K_2}}, Z_1 = \overline{P_1}\underline{B\overline{K_1}}, X = \overline{L}^T R, Y = Z^T\overline{L}, Y_1 = Z_1^T\overline{L},$$
$$W = Z^T\underline{B\overline{K_2}}, W_1 = Z_1^T\underline{B\overline{K_1}}, W_2 = Z_1^T\underline{B\overline{K_2}}$$

Then, inequality (10) is easily obtained.

4. Event-Triggered Mechanisms

To implement Event-based control [35], it's necessary to recompute the control gains and update the signal whenever (10) nears a violation. To express this equality conveniently, we assume that the input remains constant between successive recomputation of the FTA. This practice is commonly known in the literature as 'sample and hold'.

$$u_k = u_{k_i} \forall k \in [k_i, k_{i+1}[, k \in N \tag{16}$$

Or the sequence $\{k_i\} i \in N$ represents the moment when the command is recalculated. Subsequently, we introduce the error $e_1(k)$ defined by:

$$\begin{aligned} e_1(k) &= u_{k_i} - \tilde{u}_k \\ e_1(k) &= u_k - \tilde{u}_k + u_{k_i} - u_k \\ e_1(k) &= \begin{pmatrix} 0 & \underline{\Gamma^u} & 0 \end{pmatrix} \left(\overline{\alpha_{k_i}} - \overline{\alpha_k}\right) \end{aligned} \tag{17}$$

which means that

$$\overline{\alpha_{k_i}} - \overline{\alpha_k} = \overline{C_1}^+ e_1(k) + \left(I - \overline{C_1}^+\overline{C_1}\right)\overline{w_k} \tag{18}$$

 doi:doi:10.20944/preprints202505.0587.v1

Such as: $\overline{C_1} = \begin{pmatrix} 0 & \underline{\Gamma^u} & 0 \end{pmatrix}, \overline{C_1}^+$: is the pseudo-inverse of $\overline{C_1}, \overline{w_k}$: Arbitrary vector represents the disturbances.

From equation (6), the dynamics of the system in the interval $[k_i, k_{i+1}$ [is given by:

$$\begin{aligned} \overline{\dot{\eta}_k} &= A_\alpha \overline{\eta_k} + \underline{B_\alpha} \overline{\alpha_{k_i}} \\ \overline{\dot{\eta}_k} &= \overline{A_\alpha} \overline{\eta_k} + \underline{B_\alpha} \overline{\alpha_{k_i}} + \underline{B_\alpha} (\overline{\alpha_k} - \overline{\alpha_k}) \\ \overline{\dot{\eta}_k} &= \underline{A_\alpha} \overline{\eta_k} + \underline{B_\alpha} \overline{\alpha_k} + \underline{B_\alpha} \overline{C_1}^+ e_1(k) + \underline{B_\alpha} \left(I - \overline{C_1}^+ \overline{C_1} \right) \overline{w_k} \end{aligned} \tag{19}$$

Using (13) and (19), held to:

$$J_k^T \begin{bmatrix} \bar{Q} & \overline{P} \underline{B_\alpha} \overline{C_1}^+ & \overline{P} \underline{B_\alpha} \left(I - \overline{C_1}^+ \overline{C_1} \right) \\ \star & 0 & 0 \\ \star & 0 & 0 \end{bmatrix} J_k \leq 0 \tag{20}$$

With $J_k^T = \begin{bmatrix} \overline{\eta_k} \\ e_1(k) \\ \overline{w_k} \end{bmatrix}^T$

Subsequently, the k_i trigger time can now be defined as the moment that this equality is satisfied:

$$J_{k_i}^T \Upsilon J_{k_i} = 0 \tag{21}$$

With $\Upsilon = \begin{bmatrix} \bar{Q} & \overline{P} \underline{B_\alpha} \overline{C_1}^+ & \overline{P} \underline{B_\alpha} \left(I - \overline{C_1}^+ \overline{C_1} \right) \\ * & 0 & 0 \\ * & 0 & 0 \end{bmatrix}$

5. Discussion and Comments

1. This article examines the closed-loop system dynamics, which can be extended and generalized to accommodate the case of (by adjusting the matrix dimensions):
   • Lipschitz nonlinear discrete-time systems where the basic idea is to use the DMVT on the nonlinear function [34] to transform the global nonlinear system to LPV system using **Lemma 2**. Then, if the nonlinear function verify $h(k, 0) = 0$, the dynamic matrix $\underline{A}$ becomes $\underline{\mathcal{A}}(\phi)$ where the parameter ϕ lies inside the bounded convex set of $h(k, x_k)$ variation.
   • Decentralized systems with the consideration of the nonlinear interconnection function in the synthesis of the proposed control.
2. In this work, two gains ($\overline{K_1}$ and $\overline{K_2}$) have been synthesized separately to stabilize the overall system during cyber-attacks on the two communications chains of control and observation (representing the interconnections). To reduce the complexity of the BMI to be solved, a proposal can ensure this by admitting that $\overline{K_2} = \theta \overline{K_1}$ (like the proposed form of the $\overline{P}$ matrix where $\theta > 0$). This will make it possible to linearize several expressions in the BMI while guaranteeing a more optimal solution (scalar variables to be searched instead of matrices).

6. Numerical Simulation and Results

This section presents an application on a pilot system comprising three tanks. A plant model is introduced, and the proposed control design is implemented on the system. Numerical findings are provided to demonstrate the effectiveness of the developed methodology.

The dynamic equation for the system is given as:

$$\underline{A} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \underline{B} = \begin{bmatrix} 0.0649 & 0 \\ 0 & 0.0649 \\ 0 & 0 \end{bmatrix}; \underline{C} = I_3$$

 doi:doi:10.20944/preprints202505.0587.v1

$\overline{f}_k$ simulates errors modeling, faults, unknown input, disturbances, where the weighing matrix $\underline{F}$ is defined as: $\underline{F} = \begin{bmatrix} 0 \\ 0 \\ 0.2626 \end{bmatrix}$

$\underline{\Gamma^u}$ and $\underline{\Gamma^y}$ is equal to the identity matrix I. The event condition $\underline{\sigma}$ rate was chosen to be equal to 5%. The initial conditions of the system and the observer are: $\begin{bmatrix} 0.4 & 0.2 & 0.3 \end{bmatrix}^T$ with $T_e = 0.001$ s.

By solving (10) with (15)using YALMIP®, an optimal solution is found such that the gains found are as follows:

$$\overline{L} = \begin{bmatrix} 0.19005 & 0.071893 & 0.10582 \\ 0.72594 & 0.81695 & 0.51331 \\ -0.014559 & -0.069732 & 0.017343 \end{bmatrix}$$

$$\overline{K_1} = \begin{bmatrix} -80.4016 & -6.7935 & 0.0647 \\ -6.7955 & -70.8443 & -0.0177 \end{bmatrix}$$

$$\overline{K_2} = \begin{bmatrix} -15.3423 & 0.0114 & 2.3703 \\ 0.0117 & -15.3609 & 1.1387 \end{bmatrix}$$

$$\underline{\mu} = 2.4052$$

6.1. No-Attacks Case:

First, during the implementation phase, noise was introduced into the system in the form of sinusoidal signals characterized by a random varying frequencies (between 02 and 42 Hz) and amplitudes $(\pm 0.15\% y(k))$. Now, Figures 2–4 show the evolution of the control u_k and various outputs $(y_1(k), y_2(k))$ without attacks:

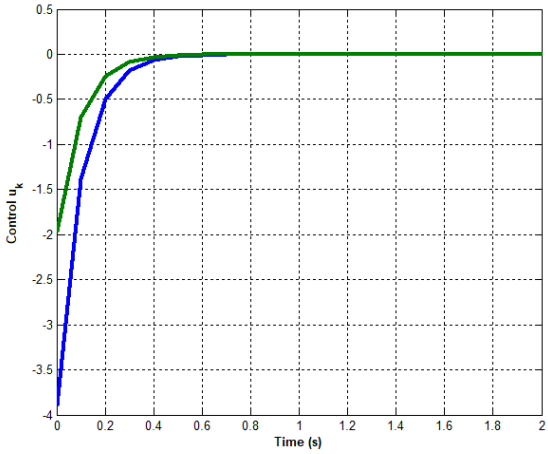


Figure 2. Evolution of the control u_k without cyber-attack.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: Posted: 8 May 2025 doi:doi:10.20944/preprints202505.0587.v1

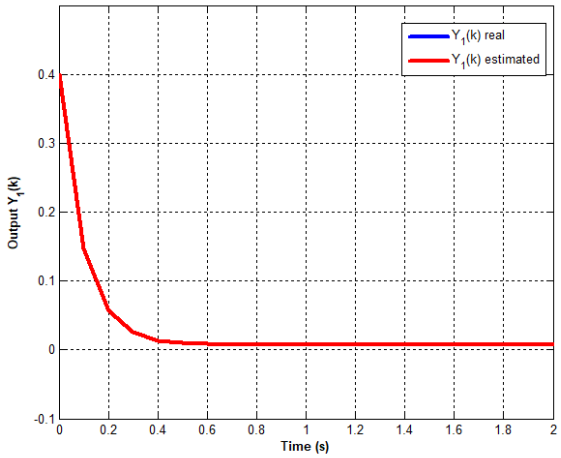


Figure 3. Evolution of the output $y_1(k)$ and its estimate without cyber-attack.

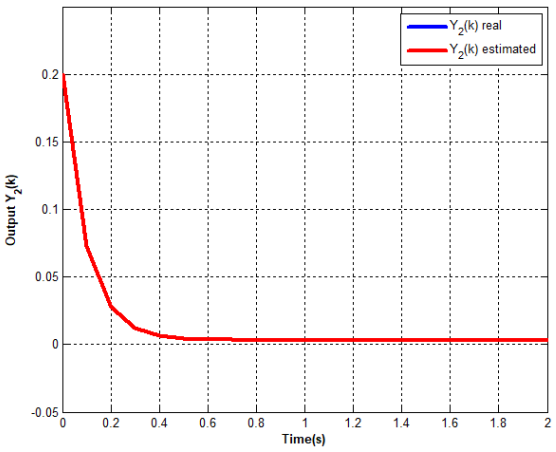


Figure 4. Evolution of the output $y_2(k)$ and its estimate without cyber-attack.

From Figures 2–4, it is clear that the proposed output feedback control ensures the stabilization despite injected disturbances. Effectively, According to Figures 3 and 4, the estimated states converge to the real ones around the equilibrium point, despite the injection of random perturbations on the system dynamics and output. This is also validated through the variation of the control signals Figure 2, which show the convergence of the control without amplitude variation and even in terms of convergence time.

Remark 3:

In the dynamics of the proposed system, the eigenvalues are on the stability limit ($\lambda_i = 1$). The output feedback control strategy (even without cyber-attacks on the control/observation chains) guarantees the overall stability of the system towards the equilibrium point despite injected disturbances such as $\lambda_i = \{0.0046; 0.0027; 0.0038\}$.

6.2. Case With Attacks

For this case, we apply the attack on the actuator chain and then on the sensor chain such as $\underline{b_k^u} = \begin{bmatrix} 0.001 & 0 \end{bmatrix}^T$ and $\underline{b_k^y} = \begin{bmatrix} 0.3 & 0 & 0 \end{bmatrix}^T$. Now, the cyber-attacks will be applied to the control chain and the sensor chain in the time interval $\begin{bmatrix} 16\,\text{s} & 26\,\text{s} \end{bmatrix}$. Figures 5–7 illustrate the evolution of the control u_k to reduce the impact of cyber-attacks on control and observer chains and the various outputs $(y_1(k), y_2(k))$ using the trigger condition ($\|\overline{\alpha_k}\|^2 \leq 0.05\|\overline{\eta_k}\|^2$).

 doi:doi:10.20944/preprints202505.0587.v1

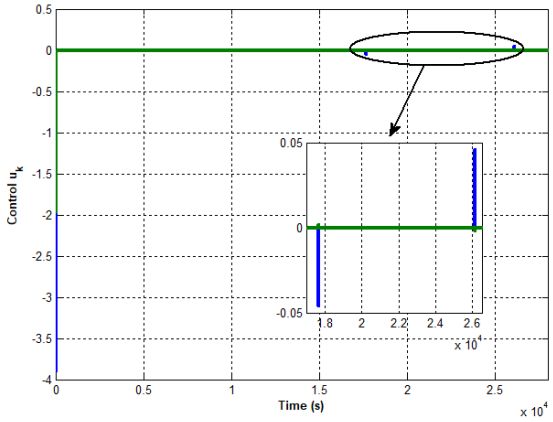


Figure 5. Evolution of the control u_k with cyber-attack.

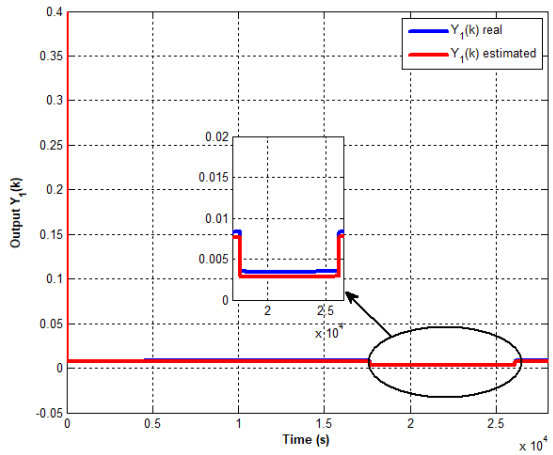


Figure 6. Evolution of the output $y_1(k)$ and its estimate with cyber-attack.

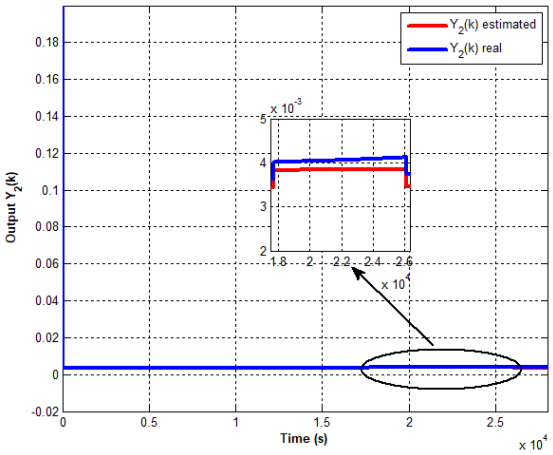


Figure 7. Evolution of the output $y_2(k)$ and its estimate with cyber-attack.

Figures 5–7 depict the progression of control and different outputs utilizing the event-triggered approach. This strategy aims to minimize the effects of attacks on sensors and actuators while ensuring the stabilization of the interconnected system around its equilibrium point. Thus, it is evident that the initial phase of attack detection and identification has been successfully achieved Figures 6 and 7. Moreover, the impact of attacks on both communication chains (control/observation) in terms of amplitude spikes and even control signal Figure 5 has been reduced through the proposed approach while avoiding a very important parameter which is the switching phenomenon in actuators.

Another point related to convergence speed/time is shown in the presented figures. Effectively, comparing the convergence times (t_c) of an approach that handles the continuous-time case [8] such that $t_c = 220$ s while the proposed discrete version converges to only 0.189 s for the same example system.

A comparison of convergence times with approaches dealing with the discrete case is as follows:

• Unamed Ground Vehicle [33] with $t_c = 1.087s$ where the proposed approach converges in 0.9824 s.

• Modular Servo System [32] with $t_c = 0.63s$ where the proposed approach converges in 0.5771 s.

7. Conclusion

This paper introduces an attack/fault-tolerant control system based on an event-triggered control framework. Through an examination of stability using the BMIs framework and the design of an observer, a feedback controller is derived to compute control inputs. The triggering mechanism for control input activation is determined based on a predefined threshold for error occurrence. A numerical validation is conducted using a three-tank system subjected to disturbances and attempts at sensor and actuator data falsification, yielding satisfactory results. Additionally, fault detection and attack isolation are facilitated through the utilization of a residual generator and observer. Future studies may explore extending the proposed synthesis methods to accommodate nonlinear output and generalizing the approach for robust schemes.

Author Contributions: Conceptualization and methodology, A.T. and E.H.; software, N.G., A.T. and G.B.H.F.; supervision and validation, A.T. and N.G.; writing original draft preparation, E.H.; writing review and editing, G.B.H.F. and E.H. All authors have read and agreed to the final version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

FTA	Fault Tolerant Attack
ETM	Event-Triggered Mechanisms
CPS	Cyber-Physical Systems
BMI	Bilinear Matrix Inequality
LMI	Linear Matrix Inequality
CA	Cyber-Attacks
NCS	Network Control Systems

References

1. Ilioudis, V.C. 'A Study of MTPA Applied to Sensorless Control of the Synchronous Reluctance Machine (SynRM)'. *Automation 2025.* , Vol. 6 (11), https://doi.org/10.3390/automation6010011.
2. Duo, W., Zhou, M., and Abusorrah, A. (2022),'A survey of cyber attacks on cyber physical systems: Recent advances and challenges', *IEEE/CAA Journal of Automatica Sinica*,Vol. 9, No. 5, p. 784-800.
3. Saif, A. W. A. (2007), ' Strong stabilisation: an LMI approach.', *International Journal of Modelling, Identification and Control* ,Vol. 2, No.1, p. 3-8.
4. M.A. Rahman et al. (2022), 'A Cloud-Based Cyber-Physical System with Industry 4.0: Remote and Digitized Additive Manufacturing', *Automation 2022*, Vol. 3(3), 400-425; https://doi.org/10.3390/automation3030021.

5. Thabet A, Frej G.B.H, Mansouri K, Chauveau E, Abdallah S.B.H. (2021), 'Estimation des defauts pour les systÃ¨mes non lineaires interconnectes : Application a un reseau Electrique.', ,*SGE21, Symposium de Genie Electrique, Nantes, France.*
6. Gupta, P., Singh, N., Mahajan, V. (2021), 'Intrusion Detection in Cyber-Physical Layer of Smart Grid Using Intelligent Loop Based Artificial Neural Network Technique', *International Journal of Engineering,* Vol. 34(5), p. 1250-1256.
7. Zou, X., Ding, H. and Li, J. (2023), 'Sliding mode speed control of permanent magnet synchronous motor based on improved reaching law',*COMPEL-The international journal for computation and mathematics in electrical and electronic engineering*, Vol. 42 No. 6, p. 1335-1348.
8. Rebai S.B., Voos H. and Darouach M. (2017), 'A contribution to Cyber-Security of Networked Control Systems: an Event-based Control Approach.', *In Proc. The 3rd International Conference on Event-Based Control, Communication and Signal Processing, Madeira, Portugal*
9. Das, D., and Savier, J. (2009), 'A Multi-Objective Method for Network Reconfiguration (TECHNICAL NOTE)', *International Journal of Engineering,* Vol. 22(4), p. 333-350.
10. Liu, Y. (2006), ' Robust adaptive control of uncertain non-linear systems with non-linear parameterisation', *International Journal of Modelling, Identification and Control* ,Vol. 1, No.2, p. 151-156.
11. Liu K., Guo H., Zhang Q., and Xia Y. (2022), 'A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges', *IEEE/CAA J. of Automatica Sinica* ,Vol. 9, No. 5, p. 784-800.
12. Dadi, L., Ethabet, H., and Aoun, M. (2024), ' Interval observer-based fault tolerant control for discrete-time switched linear system.', *International Journal of Modelling, Identification and Control* ,Vol. 44, No. 4, p. 341-349.
13. Barik, S.K., Nanda, S., Samal, P. and Senapati, R.(2024) 'Detection and localization of fault in DC microgrid using discrete Teager energy and generalized least square method', *COMPEL - The international journal for computation and mathematics in electrical and electronic engineering*, Vol. 47, No. 1, pp.227-246.
14. Neupane, S.R.; Sun, W. (2025). 'Advanced Data Classification Framework for Enhancing Cyber Security in Autonomous Vehicles'. *Automation 2025.* , Vol. 6 (1), https://doi.org/10.3390/automation601000.
15. Hassine, E., Thabet, A., Gasmi, N., Frej, G. B. H., and Thabet, H. (2023), 'Reconfiguration and Cyber-Attack Tolerant Control for Nonlinear Multi-Agent Systems', *In 2023 IEEE International Workshop on Mechatronic Systems Supervision (IW-MSS),* p. 1-6.
16. Mo Y., Weerakkody S., and Sinopoli B. (2015), 'Physical authentication of control systems designing water-marked control inputs to detect counterfeit sensor outputs',*IEEE Control Systems* p. 93-109.
17. Zhang, K., Braverman, E. and Gharesifard, B. (2023), 'Event-triggered control for discrete-time delay systems.', *Automatica,*Vol. 147, p. 110688.
18. Keshavarz, M., Doroudi, A., Kazemi, M., and Mahdian D. N. (2021),'A New Consensus-based Distributed Adaptive Control for Islanded Microgrids', *International Journal of Engineering,*Vol.34(7), p. 1725-1735.
19. Moufaddal M., Benghabrit A., and Bouhaddou I (2023), 'Towards a novel cyber physical control system framework: a deep learning driven use case.', *International Journal of Intelligent Unmanned Systems.*, Vol 16, p. 233-240.
20. Ghansah, F. A., and Lu, W. (2023), 'Cyber-physical systems and digital twins for a cognitive building in the construction industry', *Construction Innovation.*
21. Teixeira A., Shames I., Sandberg H., and Johansson K.H. (2015), 'A secure control framework for resource-limited adversaries.', *Automatica.2015,* Vol. 51, p. 135-148.
22. Pasqualetti F., Darfer F., and Bullo F.(2012), 'Cyber-physical security via geometric control: Distributed monitoring and malicious attacks.', *In IEEE Conference on Decision and Control, Hawai, USA.*
23. Rosich A., Voos H., and Darouach, M. (2014), 'Cyber-attack detection based on controlled invariant sets.', *In European Control Conference, Strasbourg, France.*
24. RSmith R.S.(2015), 'Covert misappropriation of networked control systems.', *IEEE Control Systems.*Vol. 35(1), p.82-92.
25. Asgari, S., Menhaj, M., Suratgar, A. A.,and Kazemi, M. (2021) 'A Disturbance Observer Based Fuzzy Feedforward Proportional Integral Load Frequency Control of Microgrids', *International Journal of Engineering.*, Vol. 34(7), pp.1694-1702
26. Wen G., Li Z. , Duan Z., and Chen G. (2013), 'Distributed consensus control for linear multi-agent systems with discontinuous observations.', *Int. J. Control.*Vol. 86, No. 1, p. 95-106.
27. Ding, D., Wang, Z., Ho, D. W., and Wei, G.(2016), 'Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks', *IEEE transactions on cybernetics,* Vol. 47(8), p. 1936-1947.

28. Chao D., Qi R., et Jiang B. (2022), 'Adaptive fault-tolerant control for the ascent phase of hypersonic vehicle with time-varying full state constraints', *Aerospace Science and Technology*, Vol. 131, p. 108-116.
29. Wen G., Yu W., Xia Y., Yu X., and Hu J. (2017), 'Distributed tracking of nonlinear multiagent systems under directed switching topology: An observer-based protocol.', *IEEE Trans. Syst. Man, Cybern., Syst*,Vol. 47, No. 5, p. 869-881.
30. Wan Y., Cao J., and Wen G. (2016), 'Quantized synchronization of chaotic neural networks with scheduled output feedback control.', *IIEEE Trans. Neural Netw. Learn. Syst.*
31. Wan Y., Cao J., Alsaedi A., and Hayat T. (2017), 'Distributed observer-based stabilization of nonlinear multi-agent systems with sampled-data control.', *Asian J. Control*,Vol. 19, No. 3, p. 918-928.
32. Zhao D. , Zidong W. , Ho D.W. C. Ho , Guoliang W., (2019), 'Observer-Based PID Security Control for Discrete Time-Delay Systems Under Cyber-Attacks', *IEEE Transactions on Systems, Man, and Cybernetics: Systems*,Vol. 51, p. 3926-3938.
33. Zhu Y. and Zheng W. X. (2020), 'Observer-Based Control for Cyber-Physical Systems With Periodic DoS Attacks via a Cyclic Switching Strategy',*IEEE Transactions on Automatic Control*,Vol. 65, No. 8, p. 3714-3721,
34. Thabet, A., Hassine, E., Gasmi, N., Frej, G.B.H., Boutayeb, M. (2023), 'LMI-Based Designs for Feedback Stabilization of Linear/Nonlinear Discrete-Time Systems in Reciprocal State Space: Synthesis and Experimental Validation.', *In: State Estimation and Stabilization of Nonlinear Systems: Theory and Applications. Cham: Springer Nature Switzerland*,p. 205-219.
35. Zhang, K., Braverman, E. (2023), 'Delayed impulsive stabilization of discrete-time systems: a periodic event-triggering algorithm', *International Journal of Control*,Vol. 147, p. 1-11.