Cyber-Attack Detection Strategy with Markovian Distribution Logic in Cyber-Physical Systems

Eya HASSINE, *Member, IAENG,* Assem THABET, *Member, IAENG,* Noussaiba GASMI,
and Ghazi BEL HAJ FREJ

Abstract—**This study proposes a Luenberger observer-based structure incorporating residual generation for detecting various attack strategies, including Denial-of-Service (DoS) and False Data Injection (FDI), targeting the sensors and actuators of discrete-time Cyber-Physical Systems (CPS). The proposed approach improves upon existing methods by enhancing convergence properties and increasing robustness against realistic attack scenarios. The observer design introduces additional decision variables into the synthesis constraints, resulting in less conservative conditions. Sufficient stability criteria are formulated as Linear Matrix Inequalities (LMIs), which are addressed using block-matrix decomposition and a slack variable technique. Furthermore, Markovian distribution logic is employed to simulate the behavior of attack signals, improving the realism of the threat model. The effectiveness of the proposed method is validated through a case study involving a three-tank interconnected system, with numerical comparisons demonstrating its advantages over existing approaches.**

Index Terms—**Cyber-Physical System, Markovian Stochastic Processes, Luenberger observer, Denial of Service attack(DoS), False Data Injection attack(FDI)**

I. Introduction

IN recent years, Cyber-Physical Systems (CPS) have emerged as transformative innovations in engineering, seamlessly integrating digital and physical domains to create highly interconnected and intelligent systems [1]-[2]. These systems have revolutionized various industries by leveraging advances in engineering, communication networks, and the automated control of physical processes. Their ability to support real-time monitoring and control while processing large volumes of data has fundamentally reshaped process management and system analysis. This integration has enabled the deployment of advanced control strategies and robust security mechanisms to ensure operational continuity and system integrity [3], [4], [5], [6]. Despite their immense potential, CPS face significant challenges. Their inherent complexity and reliance on open communication networks make them highly susceptible to cyber threats. The interconnected nature of CPS creates multiple entry points for malicious actors to exploit vulnerabilities, disrupt operations, compromise data integrity, and extract sensitive information [7]-[9]. Consequently, the development of resilient detection and protection mechanisms is essential to maintaining reliability and safeguarding these systems against cyber-attacks. In the field of automatic control, considerable research has focused on high-impact threats such as Denial-of-Service (DoS) and False Data Injection (FDI) attacks due to their particularly disruptive effects [10], [11]. Stochastic Markovian modeling has emerged as an effective approach in this context, providing a realistic framework to capture the probabilistic and time-varying behavior of such attacks. Furthermore, advanced detection techniques, such as observer banks and residual generation methods, are increasingly employed to monitor system performance, detect anomalies in key variables, and trigger timely alerts to mitigate or prevent intrusions [12]-[14].

The pervasive use of communication networks in CPS increases their vulnerability to cyber threats, prompting the development of various attack detection strategies to enhance system security. These include Unknown Input Observer (UIO)-based methods [15]-[16], [17], zonotope-based observer schemes [18], sliding mode observers with adaptive thresholds [19], robust adaptive sliding mode observers [20], disturbance observers for unmanned aerial vehicles (UAVs) [21], nullspace-based residual filter designs [22], centralized and distributed observers [23], and hybrid observer-based anomaly detection frameworks [24]. While many studies have addressed cyber-attack detection in CPS, relatively few have considered the simultaneous modeling of system faults within the observer synthesis framework, particularly when combined with a stochastic Markovian model that realistically captures the distribution of these attacks. Motivated by the work presented in [23], this paper introduces a detection framework based on a Luenberger-type observer. The observer synthesis is formulated using the S-procedure and block matrix decomposition, leading to sufficient stability conditions expressed as Linear Matrix Inequalities (LMIs). Although the observer structure itself may appear conventional, it provides a solid foundation for future research on resilient and robust control strategies. The insights gained from this design are expected to contribute to more advanced developments in CPS security. The feasibility of the proposed method is demonstrated through numerical simulations involving a three-tank interconnected system [25]-[26].

To highlight the main contributions of this paper, the improvements over existing methods are summarized as follows:

- The integration of stochastic Markovian modeling of cyber-attacks into the observer design, along with the explicit consideration of system faults, constitutes a

Manuscript received April 14, 2025; revised July 16, 2025.

E. HASSINE is a PhD candidate of National Engineering School of Gabes, Laboratoire de Recherche M.A.C.S, University of Gabes, Zrig 6072 Tunisia (corresponding author to provide phone: 00216-50-265-311;e-mail: ayahassine118@gmail.com).

A. THABET is an Associate Professor of Electrical Engineering Department, Laboratoire de Recherche M.A.C.S, University of Gabes, Tunisia (e-mail: assem.thabet@yahoo.fr).

N. GASMI is an Associate Professor of Automatic Engineering Department, Laboratoire d'Informatique et Télécommunications, ECAM Louis de Broglie, Campus de Ker Lann - Bruz Rennes, Bruz 35170 France (e-mail: noussaiba.gasmi@ecam-rennes.fr).

G. BEL HAJ FREJ is an Associate Professor of Automatic Engineering Department, IMS Laboratory, UMR 5218, University of Bordeaux, Talence 33400 France (e-mail: ghazi.bel-haj-frej@u-bordeaux.fr).

novel contribution that has not been extensively addressed in the existing literature.
- The proposed approach introduces additional decision variables into the convex formulation, providing increased degrees of freedom and enhanced flexibility in the observer design process.
- In contrast to many existing methods that treat faults and attacks as unknown inputs [15]-[16], [17], the proposed synthesis explicitly incorporates fault and attack dynamics within the system model.
- A simplified yet effective application of block-matrix decomposition and the S-procedure is adopted to improve the tractability and flexibility of the synthesis framework.

The remainder of this paper is organized as follows. Section 1 introduces notations and preliminary concepts. Section 2 presents the problem formulation. Section 3 details the observer synthesis procedure based on a stochastic Markovian model. Section 4 provides simulation results on a three-tank system to demonstrate the effectiveness and robustness of the proposed observer. *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 $\bar{Q}$.
- I_r represents the identity matrix of dimension r.
- Q is a square matrix then the notation $Q > 0$ $(Q < 0)$ means that Q is positive definite (negative definite).

II. Problem Formulation

Consider the following discrete-time cyber-physical system (1), where both the input and output are assumed to be transmitted remotely:

$$\begin{aligned} x_{k+1} &= Ax_k + B\tilde{u}_k + \bar{F}f_k, \\ y_k &= Cx_k + W_2 d_k^s, \end{aligned} \tag{1}$$

where the actual control input $\tilde{u}_k$ is defined as:

$$\tilde{u}_k = u_k + W_1 d_k^a, \tag{2}$$

with $x_k \in \mathbb{R}^{n_x}$ denoting the system state vector, $y_k \in \mathbb{R}^{n_y}$ the measured output, and $\tilde{u}_k \in \mathbb{R}^{n_{\tilde{u}}}$ the control input effectively received by the plant. The vector $f_k \in \mathbb{R}^{n_f}$ represents system faults, while $u_k \in \mathbb{R}^{n_u}$ is the nominal (intended) control input. Matrices A, B, C, and $\bar{F}$ are constant and of appropriate dimensions. The matrices W_1 and W_2 are coupling matrices that define the structure of actuator and sensor attacks, respectively. The vectors $d_k^a \in \mathbb{R}^r$ and $d_k^s \in \mathbb{R}^m$ represent actuator and sensor attack signals.

A Luenberger-type observer for the system in (1) is proposed as follows:

$$\begin{aligned} \hat{x}_{k+1} &= A\hat{x}_k + Bu_k + L(y_k - \hat{y}_k), \\ \hat{y}_{k+1} &= C\hat{x}_k, \end{aligned} \tag{3}$$

where $\hat{x}_k \in \mathbb{R}^{n_x}$ denotes the estimated state vector, $\hat{y}_k \in \mathbb{R}^{n_y}$ the estimated output, and $L \in \mathbb{R}^{n_x \times n_y}$ the observer gain matrix.

The estimation error is defined as $e_k = x_k - \hat{x}_k$, and its dynamics evolve according to:

$$e_{k+1} = x_{k+1} - \hat{x}_{k+1}. \tag{4}$$

Substituting (1) and (3) into (4) yields:

$$e_{k+1} = (A - LC)e_k + \bar{F}f_k + BW_1 d_k^a - LW_2 d_k^s. \tag{5}$$

To ensure that each type of cyber-attack leads to a distinct detection signature, the residual signal r_k, defined as the difference between the actual and estimated outputs, is given by:

$$\begin{aligned} r_k &= y_k - \hat{y}_k \\ &= C(x_k - \hat{x}_k) + W_2 d_k^s. \end{aligned} \tag{6}$$

Thus, the compact expressions for the estimation error and residual signals can be rewritten as:

$$\begin{aligned} e_{k+1} &= \tilde{A}e_k + \bar{F}f_k + \tilde{W}_1 d_k^a - \tilde{W}_2 d_k^s, \\ r_k &= Ce_k + W_2 d_k^s, \end{aligned} \tag{7}$$

where $\tilde{A} = A - LC$, $\tilde{W}_1 = BW_1$, and $\tilde{W}_2 = LW_2$.

III. Formulation of Attack Schemes

This section introduces the types of cyber-attacks considered in this study, each designed to compromise the integrity and performance of the target Cyber-Physical System (CPS).

A. Denial of Service (DoS) Attacks

The goal of a Denial-of-Service (DoS) attack is to disrupt the transmission of control or measurement data, typically by saturating the communication network, interfering with signal transmission, or causing packet loss. Under a DoS scenario, the actuator and sensor attack signals are modeled as follows:

$$\begin{aligned} d_k^a &= -m_k^1 u_k, \\ d_k^s &= -m_k^2 x_k, \end{aligned} \tag{8}$$

where m_k^1 and m_k^2 are discrete-time stochastic Markov processes that take values in $\{0, 1\}$ [27]. Incorporating the expressions in (8) into the system dynamics (1) results in the following modified model:

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + \bar{F}f_k - m_k^1 BW_1 u_k, \\ y_k &= Cx_k - m_k^2 W_2 x_k. \end{aligned} \tag{9}$$

B. False Data Injection (FDI) Attacks

In a False Data Injection (FDI) attack, an adversary injects falsified data into the system to deliberately mislead the controller or sensor measurements, effectively replacing legitimate values with corrupted ones. The corresponding actuator and sensor attack signals are modeled as follows:

$$\begin{aligned} d_k^a &= -m_k^1 u_k + m_k^1 s_k^a, \\ d_k^s &= -m_k^2 x_k + m_k^2 s_k^s, \end{aligned} \tag{10}$$

where s_k^a and s_k^s denote the falsified (malicious) signals introduced at the actuator and sensor levels, respectively. Substituting (10) into the original system (1) yields the updated system model:

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + \bar{F}f_k - m_k^1 BW_1 u_k + m_k^1 BW_1 s_k^a, \\ y_k &= Cx_k - m_k^2 W_2 x_k + m_k^2 W_2 s_k^s. \end{aligned} \tag{11}$$

IV. Observer Stability Analysis

To ensure the asymptotic stability of the observer system described in equation (3), the following theorem is proposed:
Theorem 1.
he observer associated with systems (1) *and* (3) *is stable if, for a scalar parameter* $\alpha > 0$*, there exist constants* $\tau_1, \tau_2, \tau_3, \delta_1 > 0$*, and matrices* $P = P^T > 0$ *and* R *of appropriate dimensions such that the following optimization problem is satisfied:*

$$\begin{bmatrix} M_1 & M_2 \\ {M_2}^T & M_3 \end{bmatrix} < 0 \tag{12}$$

where:

$$M_1 = \begin{bmatrix} -P + \tau_1 I & A^T P\tilde{W}_1 - C^T R\tilde{W}_1 & A^T P - C^T R \\ * & -\tau_1 I + \tilde{W}_1^T P\tilde{W}_1 & 0 \\ * & 0 & -P \end{bmatrix} \tag{13}$$

$$M_2 = \begin{bmatrix} -\tau_2 I & A^T P\bar{F} - C^T R\bar{F} & A^T P - C^T R \\ -\tilde{W}_1^T R^T W_2 & -\tau_2 I + \tilde{W}_1^T P\bar{F} & 0 \\ R^T W_2 & 0 & -P \end{bmatrix} \tag{14}$$

$$M_3 = \begin{bmatrix} -(\delta - \tau_3)I & -{W_2}^T R\bar{F} & W_2^T R \\ * & -(\tau_3 - \delta_1)I + \bar{F}^T P\bar{F} & 0 \\ * & * & -P \end{bmatrix} \tag{15}$$

Then, the observer gain matrix is given by $L = P^{-1}R^T$.
Proof:
Consider the following quadratic Lyapunov function:

$$V(e_k) = {e_k}^T P e_k \tag{16}$$

where $P > 0$. The variation of $V(e_k)$ along the solutions of (16) is:

$$\begin{aligned} \Delta V_k &= V(e_{k+1}) - V(e_k) \\ \Delta V_k &= {e_{k+1}}^T P e_{k+1} - {e_k}^T P e_k \end{aligned} \tag{17}$$

Replacing e_{k+1} from equation (7), gives:

$$\Delta V_k = \overline{e}_k^T \mathbb{M} \overline{e}_k \tag{18}$$

with :

$$\overline{e}_k^T = \left[e_k, d_k^a, d_k^s, f_k\right]^T \tag{19}$$

$$\mathbb{M} = \begin{bmatrix} \tilde{A}^T P\tilde{A} - P & \tilde{A}^T P\tilde{W}_1 & -\tilde{A}^T P\tilde{W}_2 & \tilde{A}^T P\bar{F} \\ \tilde{W}_1^T P\tilde{A} & \tilde{W}_1^T P\tilde{W}_1 & -\tilde{W}_1^T P\tilde{W}_2 & \tilde{W}_1^T P\bar{F} \\ -\tilde{W}_2^T P\tilde{A} & -\tilde{W}_2^T P\tilde{W}_1 & \tilde{W}_2^T P\tilde{W}_2 & -\tilde{W}_2^T P\bar{F} \\ \bar{F}^T P\tilde{A} & \bar{F}^T P\tilde{W}_1 & -\bar{F}^T P\tilde{W}_2 & \bar{F}^T P\bar{F} \end{bmatrix} \tag{20}$$

Secondly, using the notion of bloc-matrix [28] in (18), this is leads to:

$$\mathbb{M} = \begin{bmatrix} M_1 & M_2 \\ {M_2}^T & M_3 \end{bmatrix} \tag{21}$$

with:

$$M_1 = \begin{bmatrix} \tilde{A}^T P\tilde{A} - P & \tilde{A}^T P\tilde{W}_1 \\ \tilde{W}_1^T P\tilde{A} & \tilde{W}_1^T P\tilde{W}_1 \end{bmatrix} \tag{22}$$

$$M_2 = \begin{bmatrix} -\tilde{A}^T P\tilde{W}_2 & \tilde{A}^T P\bar{F} \\ -\tilde{W}_1^T P\tilde{W}_2 & \tilde{W}_1^T P\bar{F} \end{bmatrix} \tag{23}$$

$$M_3 = \begin{bmatrix} \tilde{W}_2^T P\tilde{W}_2 & -\tilde{W}_2^T P\bar{F} \\ -\bar{F}^T P\tilde{W}_2 & \bar{F}^T P\bar{F} \end{bmatrix} \tag{24}$$

The use of the block matrix notion [28] and the S-procedure technique [29] aims to facilitate the resolution of constraints by transforming them into a structured form suitable for the application of Schur's complement [30]. Specifically, the constraint $\mathbb{M} < 0$ *can be rewritten as:* $M_1 < 0$ *and* $M_1 - M_2 M^{-1} 3 M^T 2 < 0$.
However, when the diagonal elements of these matrices have singular values, the S-procedure technique ensures feasibility by introducing positive scalars $\tau_{1,2,3} > 0, \delta_1 > 0$ *into the matrix structures* $M_{1,2,3}$.
The S-procedure principal is applied, for example [31] as follows :
Consider the following Matrix inequality :

$$\begin{bmatrix} \tilde{A}^T P + P\tilde{A} & P \\ * & 0 \end{bmatrix} \tag{25}$$

Then, to avoid the problem of singularity or to introduce a parameter τ *to ensure that a term is negative, the use of the S-procedure leads to:*

$$\begin{bmatrix} \tilde{A}^T P + P\tilde{A} + \tau I & P \\ * & -\tau I \end{bmatrix} \tag{26}$$

This combination enhances numerical stability and guarantees the validity of the transformation.
Now, applying the S-procedure [31]-[29], matrices M_1,M_2,M_3 becomes:

$$M_1 = \begin{bmatrix} \tilde{A}^T P\tilde{A} - P + \tau_1 I & \tilde{A}^T P\tilde{W}_1 \\ \tilde{W}_1^T P\tilde{A} & -\tau_1 I + \tilde{W}_1^T P\tilde{W}_1 \end{bmatrix} \tag{27}$$

$$M_2 = \begin{bmatrix} -\tilde{A}^T P\tilde{W}_2 + \tau_2 I & \tilde{A}^T P\bar{F} \\ -\tilde{W}_1^T P\tilde{W}_2 & -\tau_2 I + \tilde{W}_1^T P\bar{F} \end{bmatrix} \tag{28}$$

$$M_3 = \begin{bmatrix} -(\delta_1 - \tau_3)I + \tilde{W}_2^T P\tilde{W}_2 & -\tilde{W}_2^T P\bar{F} \\ -\bar{F}^T P\tilde{W}_2 & -(\tau_3 - \delta_1)I + \bar{F}^T P\bar{F} \end{bmatrix} \tag{29}$$

Using the Schur complement lemma [30] leads to the following BMIs:

$$M_1 = \begin{bmatrix} -P + \tau_1 I & \tilde{A}^T P\tilde{W}_1 & \tilde{A}^T P \\ \tilde{W}_1^T P\tilde{A} & -\tau_1 I + \tilde{W}_1^T P\tilde{W}_1 & 0 \\ P\tilde{A} & 0 & -P \end{bmatrix} \tag{30}$$

$$M_2 = \begin{bmatrix} -\tau_2 I & \tilde{A}^T P\bar{F} & \tilde{A}^T P \\ -\tilde{W}_1^T P\tilde{W}_2 & -\tau_2 I + \tilde{W}_1^T P\bar{F} & 0 \\ P\tilde{W}_2 & 0 & -P \end{bmatrix} \tag{31}$$

$$M_3 = \begin{bmatrix} -(\delta - \tau_3)I & -\tilde{W}_2^T P\bar{F} & \tilde{W}_2^T P \\ -\bar{F}^T P\tilde{W}_2 & -(\tau_3 - \delta_1)I + \bar{F}^T P\bar{F} & 0 \\ * & 0 & -P \end{bmatrix} \tag{32}$$

Finally, considering the variable change $R = L^T P$, the LMIs (30)-(31)-(32)results given by **Theorem 1** are obtained and consequently provides the observer gain $L = P^{-1}R^T$, ensuring the asymptotic stability of the observer.

V. Simulation Results

In the field of chemical process engineering, interconnected tank systems play a crucial role. For the considered example, the system is composed of three tanks that are interconnected by means of pipes and valves [11].
The various parameters and variables of this system are as

follows:

$$x_k = \begin{bmatrix} h_k^1 \\ h_k^2 \\ h_k^3 \end{bmatrix}, \ u_k = \begin{bmatrix} Q_k^1 \\ Q_k^2 \end{bmatrix}, \ y_k = \begin{bmatrix} h_k^1 \\ h_k^2 \\ h_k^3 \end{bmatrix};$$

where $Q_k^{1,2}$ are the flow rates of the two pumps and $h_k^{1,2,3}$ are the level of liquid in each tank. The dynamic, input, output and cyber-attacks distribution matrices are:

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

$$W_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, W_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \bar{F} = \begin{bmatrix} 0 \\ 0 \\ 0.26 \end{bmatrix}, f = 1.$$

The initial conditions are: $x_k(0) = \begin{bmatrix} 0.4 & 0.2 & 0.3 \end{bmatrix}^T$, $\hat{x}_k = \begin{bmatrix} -0.32 & -0.16 & -0.24 \end{bmatrix}^T$.

Attacks signals: $s_k^a = \begin{bmatrix} 0.83 \\ 1.5 \\ -0.45 \end{bmatrix}$, $s_k^s = \begin{bmatrix} -0.2 \\ 0.65 \\ 0.85 \end{bmatrix}$.

Solving the observer synthesis problem (12) via $YALMIP^{®}$ in $MATLAB^{®}$ yields the gain matrix:

$$L = \begin{bmatrix} 0.7760 & -0.0086 & -0.0363 \\ 0.0086 & 1.0257 & -0.0014 \\ -0.0363 & -0.0014 & 0.9944 \end{bmatrix}$$

with optimization parameters $\tau_1 = 2.7$, $\tau_2 = 1.9$,$\tau_3 = 1.5$, $\delta_1 = 2$.

A. Baseline Scenario: System Behavior without Attacks

Figures 1-2 illustrate the system performance in the absence of any cyber-attacks or faults. The estimation errors converge rapidly to zero, and the residual signals remain within nominal bounds, confirming the correct functioning of the observer.

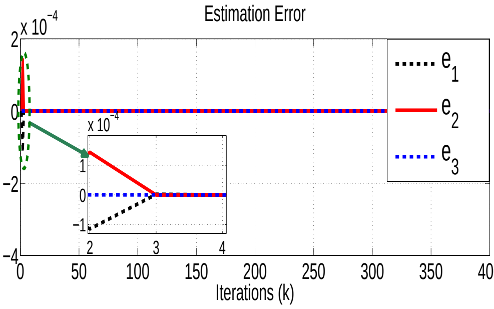

Fig. 1. Evolution of estimation errors e_i in the absence of cyber-attacks

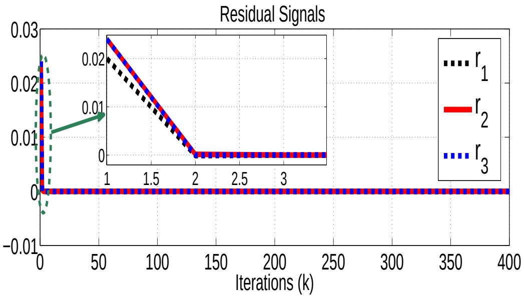

Fig. 2. Evolution of residual signals r_k in the absence of cyber-attacks

B. Sequential Attacks: Fault, DoS, and FDI

The observer's response is evaluated under sequential attacks applied over different time intervals: a system fault in the interval [400k, 600k], a DoS attack in [800k, 1000k], and an FDI attack in [1200k, 1400k]. Figures 3-4 present the corresponding estimation errors and residuals (e_k and r_k). The residuals exhibit clear responses during each attack window, enabling accurate identification of anomalies in both actuator and sensor channels.

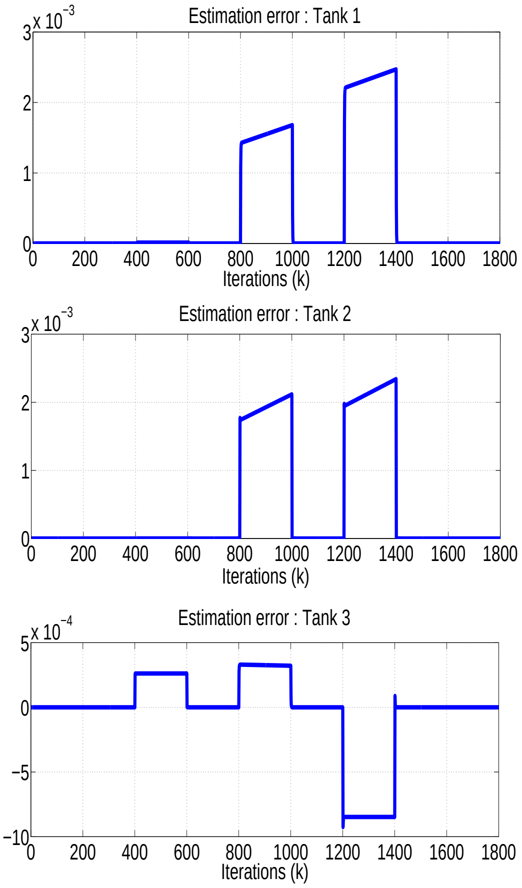

Fig. 3. Estimation errors e_k under sequential cyber-attacks.

To provide a comprehensive evaluation, an exhaustive set of attack scenarios is tested, and a corresponding signature table is constructed. Table I summarizes the observer's detection capability for various combinations of attacks on system states and control inputs, with the following notation:

- $(*)$ indicates the detection of an anomaly.
- For attack schemes in Sensor, $m_k^1 = 0$; m_k^2: random variation.
- For attack schemes in Actuator, m_k^1: random variation ; $m_k^2 = 0$.
- For combined attack schemes, both m_k^1 and m_k^2 exhibit random variation.

Table I presents the simulation results for various attack schemes and logic patterns targeting the system. It highlights the impact of each attack combination on the residuals, represented by either zero or nonzero values. These results demonstrate that the proposed observer structure reliably detects a wide range of attacks affecting different system components-states, actuators, and sensors-regardless of the attack configuration.

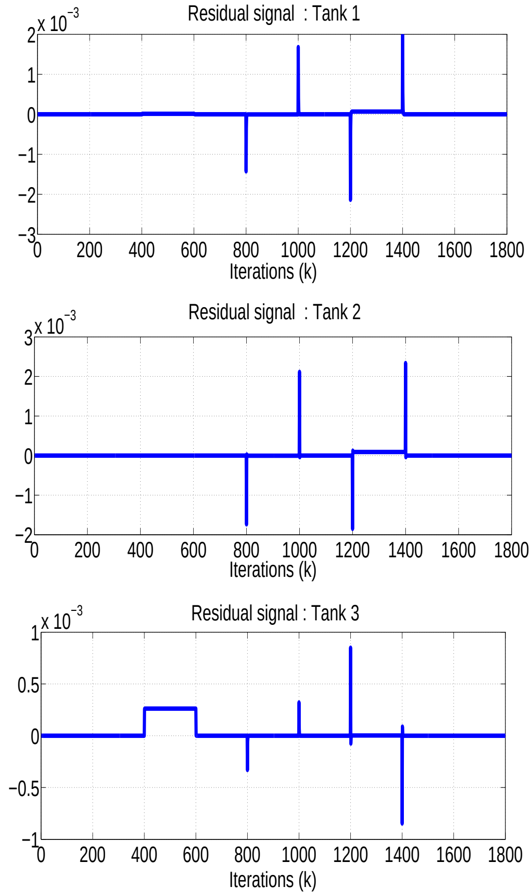

Fig. 4. Residuals signals r_k under sequential cyber-attacks.

C. Sustained DoS Attack Scenario

To evaluate long-term resilience, a permanent DoS attack is injected from k=800 onwards. Figures 5-6-7 show the behavior of state estimation, residuals and error respectively. The figures 5-6-7 clearly show that, even with a permanent DoS attack, the estimated states converge towards the real states by reducing the effects of the attacks in terms of amplitude of variation. In addition, the residuals remain responsive and the estimation error remains bounded, indicating the robustness of the observer in cyber-attack conditions.

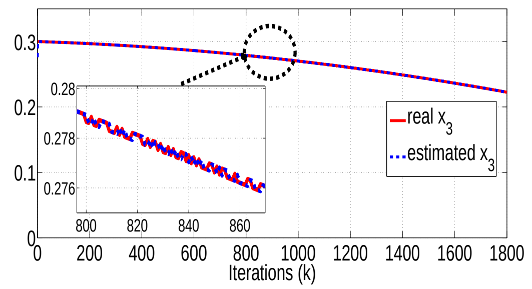

Fig. 5. State trajectories and estimation (x_3, $\hat{x}_3$) during a permanent DoS attack.

TABLE I
COMBINATIONS OF ATTACK SCHEMES WITH DIFFERENT APPLICATION LOGICS

		r_1	r_2	r_3	e_1	e_2	e_3
Sensor	x_1	*	0	0	*	0	0
	x_2	0	*	0	0	*	0
	x_3	*	0	*	0	0	*
	x_1, x_2	*	*	0	*	*	0
	x_1, x_3	*	0	*	*	0	*
	x_2, x_3	0	*	*	0	*	*
	x_1, x_2, x_3	*	*	*	*	*	*
Actuator	u_1	*	0	0	*	0	0
	u_2	0	*	0	0	*	0
	u_1, u_2	*	*	0	*	*	0
Combined	x_1, u_1	*	0	0	*	0	0
	x_2, u_1	0	*	0	0	*	0
	x_3, u_1	0	0	*	0	0	*
	x_1, x_2, u_1	*	*	0	*	*	0
	x_1, x_3, u_1	*	0	*	*	0	*
	x_2, x_3, u_1	0	*	*	0	*	*
	x_1, x_2, x_3, u_1	*	*	*	*	*	*
	x_1, u_2	*	0	0	*	0	0
	x_2, u_2	0	*	0	0	*	0
	x_3, u_2	0	0	*	0	0	*
	x_1, x_2, u_2	*	*	0	*	*	0
	x_1, x_3, u_2	*	0	*	*	0	*
	x_2, x_3, u_2	0	*	*	0	*	*
	x_1, x_2, x_3, u_2	*	*	*	*	*	*
	x_1, u_1, u_2	*	0	0	*	0	0
	x_2, u_1, u_2	0	*	0	0	*	0
	x_3, u_1, u_2	0	0	*	0	0	*
	x_1, x_2, u_1, u_2	*	*	0	*	*	0
	x_1, x_3, u_1, u_2	*	0	*	*	0	*
	x_2, x_3, u_1, u_2	0	*	*	0	*	*
	x_1, x_2, x_3, u_1, u_2	*	*	*	*	*	*

VI. Comparative Analysis and Robustness Evaluation

This section compares the proposed approach with several state-of-the-art methodologies for attack detection and mitigation in cyber-physical systems (CPS). The evaluation highlights key benefits of the proposed method, including improved resilience to attacks, faster convergence, and clearer fault signatures. Table II summarizes the main differences. While [1] provides a foundational perspective on CPS integration, it lacks considerations for attack detection and robustness. The method in [2] targets DoS attacks but does not incorporate an observer-based framework. In contrast, the proposed approach integrates a dynamic observer enabling real-time detection and mitigation of diverse attacks. The review in [3] covers multiple detection techniques but does not propose a unified mitigation strategy. The proposed method overcomes this by employing a single adaptive observer for both tasks. Although [10] presents a rigorous solution grounded in linear algebra, its computational complexity increases significantly with system size, unlike the synthesized observer, which remains scalable. Reference [16] is limited to predefined models for autonomous vehicles, whereas the proposed design accommodates nonlinear and time-varying systems. Similarly, the sensor-attack defense in [17] suffers from linearity assumptions and ambiguous fault signatures. The proposed strategy ensures distinguishable signatures even under large-scale attacks, with reduced computational load. The zonotope-based tool in [18] effectively

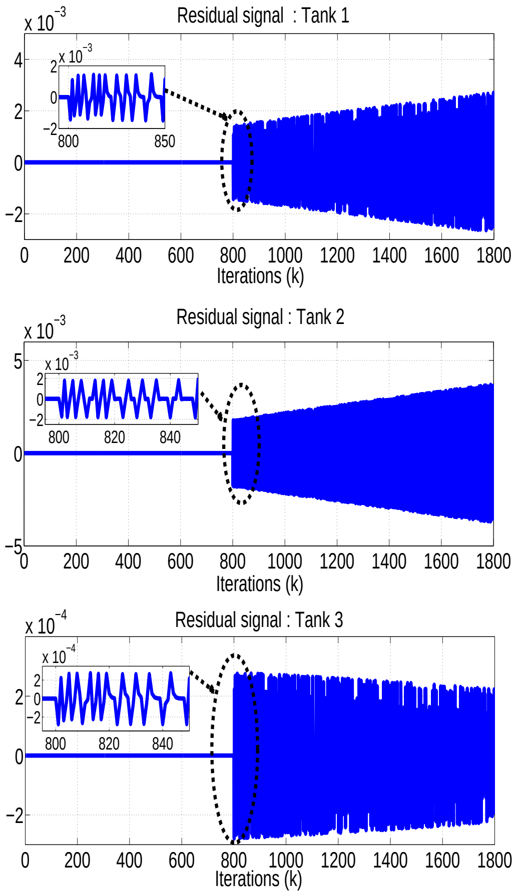

Fig. 6. Variation of Residual signals r_k under a permanent DoS attack.

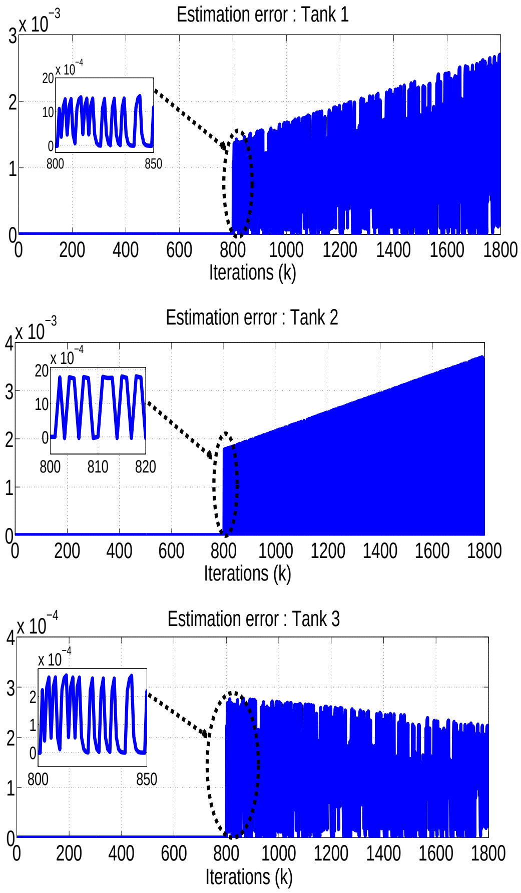

Fig. 7. Evolution of estimation errors e_k in the presence of a permanent DoS attack.

addresses uncertainties but becomes less tractable in large networks. The proposed method achieves higher efficiency and simplicity. While [11] focuses on attack-tolerant trajectory tracking, it struggles with high-dimensional dynamics, which the proposed observer handles effectively. Finally, the null-space filter approach in [22] lacks scalability, unlike the proposed framework, which is tailored for large-scale CPS with minimal computational overhead and rapid convergence. In this comparison, the proposed approach demonstrates several significant advantages. It exhibits a notably reduced convergence time, requiring only four iterations as opposed to up to fifty iterations for other methods such as [17]. Furthermore, it provides unique and clearly distinguishable attack signatures, even in complex scenarios, whereas existing methods often suffer from biased results and false detections. In addition, the proposed solution is more flexible and computationally efficient, maintaining its effectiveness for nonlinear and large-scale systems, unlike alternative strategies that rely heavily on linearity assumptions or predefined models. These aspects collectively confirm that the proposed observer-based strategy not only enhances detection and mitigation performance but also ensures superior robustness and adaptability to a wide range of cyber-attacks in CPS.

TABLE II
COMPARISON OF CONVERGENCE TIME, ATTACK TYPES, AND FAULT SIGNATURE CLARITY

Method	Convergence Time	Attack Types	Fault Signature
Proposed Method	4	DoS, FDI	Clear, Unique
[17]	50	DoS	False Signatures
[2]	N/A	DoS	N/A
[3]	N/A	Various	N/A
[10]	N/A	DoS, FDI	Moderate

To further highlight the advantages of the proposed method, Table III presents a comparative overview with respect to several state-of-the-art observer-based detection approaches. The comparison considers key criteria, including the types of cyber-attacks addressed, the inclusion of stochastic modeling (e.g., Markov chains), the ability to explicitly handle system faults, the nature of the observer structure, and the associated computational complexity. Unlike many existing approaches that either overlook stochastic behavior or treat faults as unknown disturbances, the proposed method offers a unified framework that models both faults and cyber-attacks explicitly within the system dynamics. It further employs a discrete-time stochastic model to simulate more realistic attack patterns, thereby enhancing detection robustness. While

TABLE III
COMPARISON WITH STATE-OF-THE-ART OBSERVER-BASED DETECTION METHODS

Approach	Attack Types	Observer Type	Computation Time
Proposed Method	DoS, FDI	Luenberger	Low
[1]	None	Conceptual CPS	N/A
[2]	DoS	Resilient Controller	Moderate
[3]	Various	Observer	Variable
[10]	DoS, FDI	Algebraic Detection	High
[16]	FDI	Unknown Input Observer	Moderate
[17]	Sensor Attacks	State Feedback Based	High
[18]	Sensor Attacks	Zonotope Observer	High
[22]	DoS	Null-space Filter	High

some recent studies achieve attack detection using advanced but computationally intensive observers (e.g., zonotopes or null-space filters), our method relies on a simplified Luenberger observer structure combined with Linear Matrix Inequality (LMI) formulations, resulting in a lightweight and efficient implementation. This comprehensive comparison underlines the originality of the proposed approach, which balances robustness, modeling accuracy, and implementation simplicity: three essential factors for scalable cyber-attack detection in practical Cyber-Physical Systems (CPS).

Now, to complement the previous comparison with existing approaches, this section further analyzes the performance of the proposed observer-based scheme by addressing two key aspects: (i) a direct structural comparison with the observer design from [17], and (ii) the robustness of the fault signature with respect to increasing the amplitude of cyber-attacks with a scaling parameter θ which is introduced in the DoS attack formulation as follows:

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k - \theta m_k^1 BW_1 u_k, \\ y_k &= Cx_k - \theta m_k^2 W_2 x_k. \end{aligned} \tag{33}$$

Results in Table IV confirm consistent detection signatures even with $\theta = 100$. The effectiveness of the observer remains intact across all test scenarios, establishing it as a reliable detection mechanism for resilient CPS. A targeted comparison with the observer approach proposed in [17] reveals key differences in terms of convergence performance and sensitivity to cyber-attacks. As shown in Figure 8, the proposed method enables accurate estimation of the system states within only four iterations, whereas the observer in [17] requires approximately fifty iterations to achieve a similar level of accuracy. In addition, Table V illustrates the residual and error patterns generated by the method from [17] under various DoS and FDI attack combinations. The results indicate that this approach, which does not incorporate control synthesis, yields biased and nonspecific responses, failing to clearly isolate the source of the attack. In contrast, the proposed observer not only reduces convergence time but also provides precise, discriminative signatures across different attack types, as confirmed by the results in Table I. The results discussed above clearly confirm the effectiveness and robustness of the proposed observer-based approach. In comparison with other methods such as those in [17], [1], [2], [3], and [10], the suggested method demonstrates significantly faster convergence in state estimation and higher accuracy in detecting and isolating cyber-attacks, even under conditions of increased attack intensity. These findings strongly support the suitability of the proposed architecture for secure and resilient supervision of cyber-physical systems operating in adversarial environments.

TABLE IV
COMBINATIONS OF DOS ATTACK SCHEMES WITH DIFFERENT AMPLIFICATION FACTORS

		r_1	r_2	r_3	e_1	e_2	e_3
$\theta = 2$	x_2, x_3, u_1, u_2	0	*	*	0	*	*
	x_3, u_1	0	0	*	0	0	*
$\theta = 10$	x_2, x_3, u_1, u_2	0	*	*	0	*	*
	x_3, u_1	0	0	*	0	0	*
$\theta = 100$	x_2, x_3, u_1, u_2	0	*	*	0	*	*
	x_3, u_1	0	0	*	0	0	*

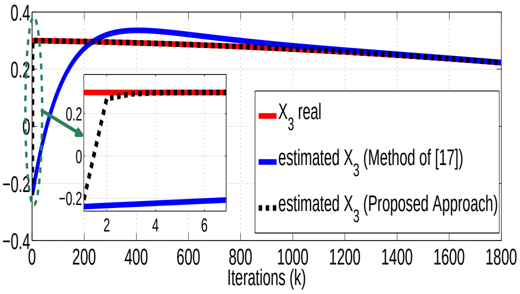

Fig. 8. Comparison of State trajectories (x_3 and their estimates $\hat{x}_3$)

TABLE V
COMBINATIONS OF ATTACK SCHEMES WITH THE METHOD FROM [17]

Method of [17]		r_1	r_2	r_3	e_1	e_2	e_3
DoS	x_1, x_2, x_3, u_1, u_2	*	0	0	*	0	0
	x_1, u_1, u_2	*	0	0	0	0	0
	x_1, x_2, x_3, u_1	*	*	*	0	0	*
FDI	x_1, x_2, x_3, u_1, u_2	*	*	*	*	*	*
	x_1, u_1, u_2	*	*	*	*	*	*
	x_1, x_2, x_3, u_1	*	*	*	*	*	*

VII. CONCLUSION

This paper presents a simplified Luenberger observer design incorporating residual generation for the detection of sensor and actuator attacks, specifically Denial of Service (DoS) and False Data Injection (FDI), in discrete-time Cyber-Physical Systems (CPS). By introducing additional decision variables into the observer synthesis constraints, the proposed method enhances convergence guarantees while accommodating more realistic and complex attack scenarios. System stability is established through Linear Matrix Inequalities (LMIs), addressed using block-matrix decomposition and the S-procedure. To emulate realistic cyber threats, the attack signals are modeled using a Markovian probabilistic framework. The effectiveness of the approach is validated through a case study involving a three-tank interconnected system, demonstrating its capacity to detect and isolate various types of cyber-attacks. Future work may focus on extending the synthesis framework to nonlinear systems and generalizing the detection scheme to achieve more robust identification and resilience in highly dynamic or uncertain environments.

AUTHOR CONTRIBUTIONS

Conceptualization and methodology, Eya Hassine and Assem Thabet; software, Eya Hassine, Assem Thabet and Ghazi Bel Haj Frej; supervision and validation, Assem Thabet and Noussaiba Gasmi; writing original draft preparation, Eya Hassine and Assem Thabet; writing review and editing, Ghazi Bel Haj Frej. and Eya Hassine. All authors have read and agreed to the final version of the manuscript.

REFERENCES

[1] Rajkumar, R., Lee, I., Sha, L., and Stankovic, J. (2010). *Cyberphysical systems: The next computing revolution*. 731–736. doi:10.1145/1837274.1837461.

[2] Yuan, Y., Zhu, Q., Sun, F., Wang, Q., and Baasar, T. (2013). Resilient control of cyber-physical systems against denial-of-service attacks. In *2013 6th International Symposium on Resilient Control Systems (ISRCS)*, 54–59. doi:10.1109/ISRCS.2013.6623750.

[3] M. Kordestani and M. Saif, ”Observer-Based Attack Detection and Mitigation for Cyberphysical Systems: A Review,” in *IEEE Systems, Man, and Cybernetics Magazine*, vol. 7, no. 2, pp. 35–60, April 2021, doi: 10.1109/MSMC.2020.3049092.

[4] W. L. Duo, M. C. Zhou, and A. Abusorrah, ”A survey of cyber attacks on cyber physical systems: Recent advances and challenges”, *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 5, pp. 784–800, May 2022. doi:10.1109/JAS.2022.105548.

[5] E. Hassine, A. Thabet, N. Gasmi, G. B. H. Frej, and H. Thabet, ”Reconfiguration and Cyber-Attack Tolerant Control for Nonlinear Multi-Agent Systems,” In *2023 IEEE International Workshop on Mechatronic Systems Supervision (IW-MSS)*, Hammamet, Tunisia, 2023, pp. 1–6, doi:10.1109/IW-MSS59200.2023.10369717.

[6] Meng Li and Libing Wu, ”Event-Triggered Adaptive Fault-Tolerant Control for Linear Multi-Agent Systems with Actuator Faults and Time Delays,” *IAENG International Journal of Applied Mathematics*, vol. 55, no. 5, pp. 1028–1034, 2025.

[7] Orojloo, H. and Azgomi, M. A. (2015). ”Evaluating the complexity and impacts of attacks on cyber-physical systems”. In *2015 CSI Symposium on Real-Time and Embedded Systems and Technologies (RTEST)*, pp. 1–8. doi:10.1109/RTEST.

[8] Bordel Sanchez, B., Alcarria, R., Robles, T., and Martín, D. (2017). ”Cyber-physical systems: Extending pervasive sensing from control theory to the internet of things”. *Pervasive and Mobile Computing*, 40. doi:10.1016/j.pmcj.2017.06.011.

[9] William R. Simpson, ”Zero Trust Philosophy versus Architecture,” *Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering 2022*, 6-8 July, 2022, London, U.K., pp. 89–94.

[10] Li, Y., Voos, H., Darouach, M., and Hua, C. (2016). ”An application of linear algebra theory in networked control systems: stochastic cyber-attacks detection approach”. *IMA Journal of Mathematical Control and Information*, 33(4), 1081–1102. doi:10.1093/imamci/dnv026.

[11] Bezzaoucha Rebai, S., Voos, H., and Darouach, M. (2018). ”Attack-tolerant control and observer-based trajectory tracking for cyber-physical systems”. *European Journal of Control*, 47. doi:10.1016/j.ejcon.2018.09.005.

[12] Shames, I., Teixeira, A., Sandberg, H., and Johansson, K. (2011). ”Distributed fault detection for interconnected second-order systems with applications to power networks”. *Automatica*, Vol. 47, No. 12, pp. 2757–2764. doi:10.1016/j.automatica.2011.09.011.

[13] Joo, Y., Qu, Z., and Namerikawa, T. (2021). ”Resilient control of cyber-physical systems using nonlinear encoding signal against system integrity attacks.” *IEEE Transactions on Automatic Control*, 66(9), 4334–4341. doi:10.1109/TAC.2020.3034195.

[14] Haoyu Wang, Xinyu Hu, Zhilian Yan, and Yebin Chen, ”Event-Driven Stabilization for Markov Jump Systems Based on Disturbance Observer,” *IAENG International Journal of Computer Science*, vol. 52, no. 5, pp. 1378–1384, 2025.

[15] M. Taheri, K. Khorasani, I. Shames, and N. Meskin, ”Cyberattack and Machine-Induced Fault Detection and Isolation Methodologies for Cyber-Physical Systems,” in *IEEE Transactions on Control Systems Technology*, vol. 32, no. 2, pp. 502–517, March 2024, doi:10.1109/TCST.2023.3324870.

[16] Mengfan Ma, Shijian Luo, Shenghui Guo, ”Unknown Input Estimation and FDI Attack Detection for Autonomous Vehicles”, in *2024 IEEE 13th Data Driven Control and Learning Systems Conference (DDCLS)*, 10.1109/DDCLS61622.2024.10606925, (pp. 1549–1554), 2024.

[17] Cambita, L. F., Quijano, N., and Cardenas, A. (2023). ”Defending State-Feedback Based Controllers Against Sensor Attacks”. *Ingenierea*, 28(2), e20094. https://doi.org/10.14483/23448393.20094.

[18] Xiangming Zhang, Fanglai Zhu, ”Observer-Based Sensor Attack Diagnosis for Cyber-Physical Systems via Zonotope Theory”. *Asian Journal of Control*, Volume 23, Issue 5, September 2021, pp. 2444–2458.

[19] Xu D., Zhu F., Zhou Z., Yan X. ”Distributed fault detection and estimation in cyber-physical systems subject to actuator faults”. *ISA Trans.*, 2020 Sep; 104:162–174. doi:10.1016/j.isatra.2019.12.002.

[20] Jian Li, Defu Yang, Qingyu Su, ”Reliable control strategy based on sliding mode observer against FDI attacks in smart grid”, *Asian Journal of Control*, 10.1002/asjc.2839, 25(2), pp. 910–920, 2022.

[21] Kunpeng Pan, Feisheng Yang, Yang Lyu, Zheng Tan, Quan Pan, ”Observer-based attack detection and security control for UAVs against attacks on desired trajectory”, *Journal of the Franklin Institute*, Vol. 361, Issue 11, 2024. doi:10.1016/j.jfranklin.2024.106920.

[22] Daniel Ossmann, ”Attack detection in cyber-physical systems via nullspace-based filter designs”, *IFAC-PapersOnLine*, Vol. 58, No. 4, 2024, pp. 526–531. doi:10.1016/j.ifacol.2024.07.272.

[23] Tan, S., Guerrero, J. M., Xie, P., Han, R., and Vasquez, J. C. (2020). ”Brief Survey on Attack Detection Methods for Cyber-Physical Systems.” *IEEE Systems Journal*, 14(4), 5329–5339. doi:10.1109/JSYST.2020.2991258.

[24] Nicholas Jeffrey, Qing Tan, Jose R. Villar, ”A hybrid methodology for anomaly detection in Cyber-Physical Systems”, *Neurocomputing*, Vol. 568, 2024. doi:10.1016/j.neucom.2023.127068.

[25] Tahir, Z., Khan, A. Q., and Asad, M. (2019). ”Attack detection and identification in cyber-physical systems: An example on a three-tank system”. In *2019 15th International Conference on Emerging Technologies (ICET)*, doi:10.1109/ICET48972.2019.8994635.

[26] Janueario, F., Cardoso, A., and Gil, P. (2019). ”A distributed multi-agent framework for resilience enhancement in cyber-physical systems”. *IEEE Access*, 7, 31342–31357. doi:10.1109/ACCESS.2019.2903629.

[27] Angel R. Guadarrama, Gloria L. Osorio-Gordillo, Rodolfo A. Vargas-Mendez, Juan Reyes-Reyes, and Carlos M. Astorga-Zaragoza, ”Cyber-Physical System Attack Detection and Isolation: A Takagi-Sugeno Approach”, *Math. Comput. Appl.*, 2025, 30(1), 12. doi:10.3390/mca30010012.

[28] Biswa Nath Datta, Chapter 2, ”A Review of some Basic Concepts and Results from Theoretical Linear Algebra”. *Numerical Methods for Linear Control Systems, Academic Press*, 2004, pp. 19–32. doi:10.1016/B978-012203590-6/50006-9.

[29] I. Polik and T. Terlaky, ”A Survey of the S-Lemma”, *SIAM Review*, Vol. 49, 2007, pp. 371–418.

[30] S. Boyd, L. E. Ghaoui, E. Ferron, and V. Balakrishnan, ”Linear Matrix Inequalities in Systems and Control Theory”. 15^{th} *ed., Philadelphia: Studies in Applied Mathematics SIAM*, 1994.

[31] V. A. Yakubovic, *As-procedure in nonlinear control theory*. Vestnik Leningrad Univ, pp. 62–77, 1971.