

Industrial Control

Countermeasures against collusive stealthy attacks in cyber-physical microgrids: A dynamic encoding approach

Zhihua Wu¹, Chen Peng^{1,*}, Engang Tian², and Yajian Zhang¹

¹ School of Mechatronic Engineering and Automation, Shanghai Key Laboratory of Power Station Automation Technology, Shanghai University, Shanghai 200444, China

² School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China

Received: 25 March 2025 / Revised: 6 May 2025 / Accepted: 8 July 2025 / Published online: 25 October 2025

Abstract Cyber-physical microgrids, as a representative industrial system, seamlessly integrate computation, communication, control, and physical devices, making it vulnerable to cyber-attacks that can trigger cascading failures and potentially lead to the collapse of the entire grid. This paper aims to develop an efficient detection framework for collusive stealthy attacks in cyber-physical microgrids. First, an \mathcal{L}_∞ unknown input observer (UIO) is deployed at the control center to monitor communication links between distributed generation units (DGUs). By treating interconnections and secondary control as unknown inputs, the observer gain is designed using only local information. Then, the vulnerability of the \mathcal{L}_∞ UIO-based monitoring unit is analyzed, and a collusive stealthy attack is devised to disrupt grid operations without alerting the \mathcal{L}_∞ UIO-based detection mechanism. To counteract the novel attack, a dynamic encoding mechanism is developed for the communication links between DGUs. This mechanism involves encoding control signals prior to transmission and subsequently decoding them at the control center. Furthermore, an in-depth analysis of the feasibility criteria for the encoding matrix has been conducted. Eventually, the efficacy of the proposed detection framework is validated through a series of simulation experiments.

Keywords Cyber-physical microgrids, Stealthy attacks, Attack detection, Unknown input observer

Citation Wu Z, Peng C, Tian E and Zhang Y. Countermeasures against collusive stealthy attacks in cyber-physical microgrids: A dynamic encoding approach. Security and Safety 2025; 4: 2025007. <https://doi.org/10.1051/sands/2025007>

1 Introduction

The evolution of industrial cyber-physical system (ICPS) marks a paradigm shift in engineering infrastructure, propelled by the synergistic integration of computational intelligence, control theory, and advanced communication paradigms [1]. Architecturally, these systems are hierarchically organized into three functional layers: the physical layer, encompassing operational entities ranging from power generation facilities to autonomous maritime systems; the application layer, which includes cyber systems such as supervisory control and data acquisition systems for information processing and decision-making; and the communication layer, which orchestrates the bidirectional flow of operational data and control directives. This interconnected architecture establishes a robust framework for seamless interaction between physical processes and cyber-based decision-making mechanisms. As a class of advanced systems, ICPS

* Corresponding author (email: c.peng@shu.edu.cn)

embodies structural complexity that necessitates interdisciplinary knowledge fusion across heterogeneous domains [2].

The integration of cutting-edge communication technologies has substantially increased the capabilities of cyber systems in achieving accurate data collection and optimizing decision-making processes, thus markedly increasing the operational efficiency of ICPS. Owing to their profound benefits, ICPS is increasingly recognized as a fundamental cornerstone in advancing critical infrastructure, fostering smart manufacturing initiatives, and driving the transition toward a green economy, among other pivotal applications. In summary, ICPS represents a key technological cornerstone of Industry 5.0, serving as an essential enabler to realize its overarching vision [3]. To date, ICPS has demonstrated extensive applicability across diverse domains, including healthcare and medical technologies, smart grid infrastructure, and intelligent transportation networks. These implementations have not only significantly enhanced quality of life but have also generated substantial economic value across multiple sectors. Among these applications, cyber-physical microgrids, as a paradigmatic example of ICPS, have garnered significant attention from both industrial and academic communities due to their capability to flexibly integrate various renewable energy sources, thereby substantially reducing carbon emissions [4].

The widespread implementation of open communication architectures in cyber-physical microgrid systems has been predominantly motivated by their operational efficiency and cost-effectiveness. Nevertheless, despite offering substantial economic benefits and enhanced deployment scalability, these public networks fundamentally expose critical infrastructure to advanced cyber vulnerabilities. Contemporary research [5–7] has documented a significant surge in cyber-security incidents targeting ICPS, with particular emphasis on cyber-physical DC microgrid, raising substantial concerns regarding societal resilience and infrastructure security [4]. When compared to their AC counterparts, DC microgrids demonstrate superior performance in power transmission efficiency while requiring lower investment in metering infrastructure and control units. This emerging threat landscape has been vividly illustrated through numerous critical infrastructure compromises of notable significance. In 2015, a sophisticated coordinated attack compromised Ukraine’s power grid, causing widespread blackouts and substantial infrastructure damage [8]. The following year witnessed the successful infiltration of a 200 MW generation facility in Kiev, resulting in its complete operational disruption [9]. More recently, in 2020, Venezuela’s national grid experienced a targeted assault on 765 trunk lines, affecting power supply across multiple regions. These consecutive security breaches highlight the imperative for implementing a defense strategy to ensure the operational continuity of cyber-physical microgrids.

Denial-of-Service (DoS) attacks primarily degrade network performance by drastically diminishing packet acceptance rates [10]. In contrast, false data injection (FDI) attacks pose a more intricate threat to data integrity through advanced manipulation techniques [11], rendering them inherently more difficult to detect. Building upon existing classical attack strategies, a variety of intelligent attack schemes have been successively proposed. For instance, in [12], an optimal DoS attack scheduling was designed to maximize the disruption of remote estimator performance. In [13], a critical data-based attack strategy combined with a stochastic energy allocation scheme was developed to degrade system performance. Beyond DoS attacks, more covert FDI attacks have also been constructed. For example, in [6], a dynamic feedback-based method was employed to design an optimal FDI attack aimed at maximizing output error. In [14], a zero-trace stealth attack was devised to compromise the operation of DC microgrids.

Currently, detection methodologies for FDI attacks can be fundamentally classified into two paradigms: analytical model-dependent solutions and data-driven learning methodologies. For instance, Euclidean distance was employed as a metric to quantify the variation in voltage signals and combined with pre-designed thresholds to detect attacks [15]. In [16], an interval observer was tailored for smart grid, capable of generating both upper and lower bounds for state estimation, and then determining whether an attack occurs based on whether the true state is within these bounds. In [17], a summation-based detector was proposed to identify FDI attacks, leveraging historical information to significantly enhance detection accuracy. Unlike the aforementioned model-based detection schemes, which rely on precise system models, the core concept of data-driven learning approaches lies in leveraging collected data to uncover underlying patterns and construct a detection model capable of distinguishing between normal and anomalous data. Specifically, in [18], a distributed support vector machine was implemented to detect stealthy FDI attacks in smart grids, employing principal component analysis for dimensionality reduction to mitigate computational complexity. In [19], a semi-supervised learning algorithm rooted in generative adversarial networks was utilized to train the model and infer the data distribution from

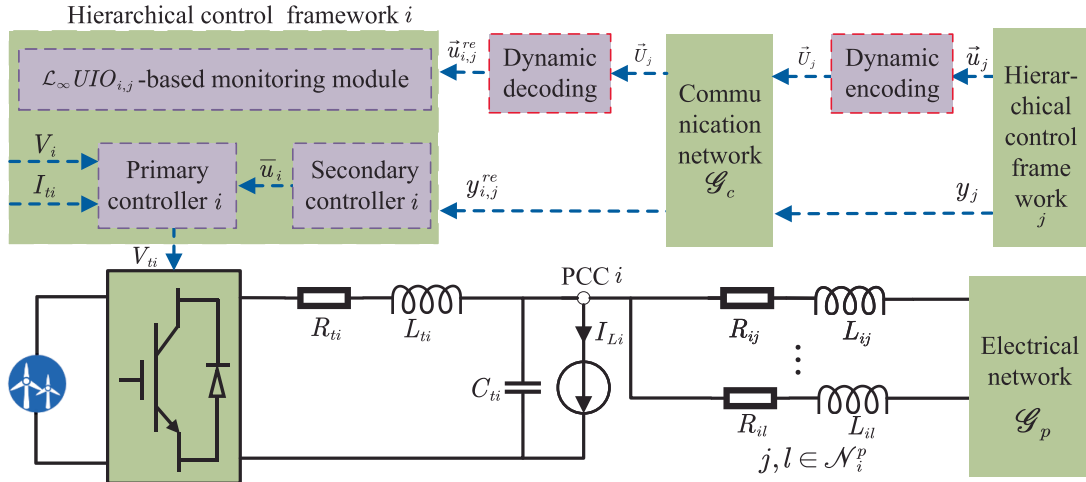


Figure 1. The overall architecture diagram of cyber-physical microgrid

samples, thereby distinguishing between attacked and normal states in the smart grid. Based on the aforementioned analysis, existing detection strategies may fail when confronted with coordinated attack tactics and struggle to adapt to the dynamic insertion or removal of subsystems.

This paper aims to construct an effective detection framework targeting collusive stealthy attacks in cyber-physical microgrids, with the following key contributions: (1) an \mathcal{L}_∞ unknown input observer (UIO) is established at the control center to monitor DGU communication links relying solely on local data; (2) systematic analysis of UIO vulnerability enables the design of collusive stealthy attacks that disrupt microgrid operations while evading detection by the \mathcal{L}_∞ UIO-based detection mechanism. Unlike conventional unobservable attacks [20], the proposed attack strategy conceals the attack signal as an unknown input and implements it in a collaborative manner; (3) dynamic encoding embedded within DGUs communication channels are proposed to expose the collusive stealthy attack, with geometric control theory deriving feasibility conditions for the encoding matrix.

2 Model of cyber-physical microgrids

This article investigates a cyber-physical microgrid encompassing M interconnected distributed generation units (DGUs), as shown in Figure 1. Each DGU is equipped with a DC voltage source, an RLC filter, a local controller, a load, and a buck converter. The physical power network of microgrids can be represented as a weighted undirected connected graph $\mathcal{G}^p = (\mathcal{V}^p, \mathcal{E}^p, \mathcal{W}^p)$. In this graph, the vertex set $\mathcal{V}^p = \{1, 2, \dots, M\}$ stands for DGUs. The edge set $\mathcal{E}^p \subseteq \mathcal{V}^p \times \mathcal{V}^p$ signifies the distribution lines that connect neighboring DGUs. The adjacency matrix $\mathcal{W}^p = [w_{ij}^p]_{M \times M}$ has nonnegative elements w_{ij}^p ($\forall (i, j) \in \mathcal{E}^p$). Let $\mathcal{N}_i^p = \{j \in \mathcal{V}^p | (i, j) \in \mathcal{E}^p\}$ denote the set of coupled neighboring units for DGU i . Moreover, the communication topology of the cyber layer, denoted as $\mathcal{G}^c = (\mathcal{V}^c, \mathcal{E}^c, \mathcal{W}^c)$, shares identical structural configuration and edge weight assignments with graph \mathcal{G}^p .

The dynamic behavior of DGU i is governed by the following differential equations derived through the systematic application of Kirchhoff's voltage and current laws:

$$\begin{aligned} \frac{dV_i(t)}{dt} &= \frac{1}{C_{ti}} I_{ti}(t) + \sum_{j \in \mathcal{N}_i^p} \frac{1}{C_{ti}} I_{ij}(t) - \frac{1}{C_{ti}} I_{Li}(t), \\ \frac{dI_{ti}(t)}{dt} &= \frac{1}{L_{ti}} V_{ti}(t) - \frac{1}{L_{ti}} V_i(t) - \frac{R_{ti}}{L_{ti}} I_{ti}(t), \end{aligned} \quad (1)$$

where $I_{ti}(t)$, L_{ti} , C_{ti} , and R_{ti} denote the current, inductance, capacitance, and resistance, respectively. $V_i(t)$ and $V_{ti}(t)$ correspond to the voltage at the i th point of common coupling (PCC) and the output voltage of the i th buck converter. As for the current flowing through the distribution line ij , modeled as

an RL network, it is represented by $I_{ij}(t)$ and satisfies:

$$\frac{dI_{ij}(t)}{dt} = -\frac{R_{ij}}{L_{ij}}I_{ij}(t) + \frac{1}{L_{ij}}V_j(t) - \frac{1}{L_{ij}}V_i(t), \quad (2)$$

where L_{ij} and R_{ij} respectively indicate the distribution line ij 's inductance and resistance. In Equation (2), the current $I_{ij}(t)$ can be approximately regarded as $\frac{V_j(t)-V_i(t)}{R_{ij}}$ when assuming the quasi-static linear approximation, with $V_j(t)$ denoting the voltage of the j th PCC.

Figure 1 depicts that each DGU is equipped with a local primary controller, ensuring the voltage $V_i(t)$ at the PCC follows the desired reference voltage $V_i^{re}(t)$. To enhance voltage tracking precision, an integral compensation component is embedded in the DGU architecture, expressed mathematically as:

$$\dot{v}_i(t) = e_i^v(t) = V_i^{re}(t) - \bar{u}_i(t) - V_i(t), \quad (3)$$

where $e_i^v(t)$ denotes the voltage tracking error, $v_i(t)$ corresponds to its integral term, and $\bar{u}_i(t)$ defines the secondary control input, aimed at achieving voltage balancing and current sharing. Thus, the augmented dynamical model for DGU i is formulated as:

$$\begin{cases} \dot{x}_i(t) = A_{ii}x_i(t) + \tilde{B}_i\tilde{u}_i(t) + \bar{B}_i\bar{u}_i(t) + \bar{B}_i\bar{u}_i(t) + \sum_{j \in \mathcal{N}_i^p} A_{ij}(x_j(t) - x_i(t)) + \xi_i^1(t), \\ y_i(t) = C_i x_i(t) + \xi_i^2(t), \end{cases} \quad (4)$$

where $x_i(t) = [V_i(t), I_{ii}(t), v_i(t)]^T \in \mathbb{R}^3$ stands for the state, $y_i(t) \in \mathbb{R}^3$ represents the measurement output, $C_i \in \mathbb{R}^{3 \times 3}$ is identity matrix, other associated matrices are derived as follows:

$$A_{ii} = \begin{bmatrix} 0 & \frac{1}{C_{ii}} & 0 \\ -\frac{1}{L_{ii}} & -\frac{R_{ii}}{L_{ii}} & 0 \\ -1 & 0 & 0 \end{bmatrix}, A_{ij} = \begin{bmatrix} \frac{1}{C_{ii}R_{ij}} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \tilde{B}_i = \begin{bmatrix} 0 \\ \frac{1}{L_{ii}} \\ 0 \end{bmatrix}, \bar{B}_i = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \bar{B}_i = \begin{bmatrix} -\frac{1}{C_{ii}} & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Furthermore, $\bar{u}_i(t) = [I_{ii}(t), V_i^{re}(t)]^T \in \mathbb{R}^2$ represents the exogenous input, while $\tilde{u}_i(t) = V_i(t) = K_i^T y_i(t) \in \mathbb{R}$ is the primary control input with $K_i \in \mathbb{R}^3$ denoting the vector of primary control gains. A consensus-based coordination protocol is implemented to synthesize the secondary control signal $\bar{u}_i(t)$, governed by

$$\dot{\bar{u}}_i(t) = [0, k_i, 0] \sum_{j \in \mathcal{N}_i^c} w_{ij}^c \left(\frac{y_i(t)}{I_{ii}^s} - \frac{y_{i,j}(t)}{I_{ij}^s} \right), \quad (5)$$

where $k_i > 0$ represents weight parameter, $I_{ii}^s > 0$ and $I_{ij}^s > 0$ represent current proportional parameters for DGU i and DGU j , $y_{i,j}(t)$ represents the output of DGU j transmitted to DGU i . Without loss of generality, assume that the disturbance $\xi_i^1(t)$, measurement noise $\xi_i^2(t)$, and $\dot{\xi}_i^2(t)$ are amplitude bounded, *i.e.*, $\|\xi_i^1(t)\|_\infty = \sup_{t \in \mathbb{R}} \|\xi_i^1(t)\| < \infty$, $\|\xi_i^2(t)\|_\infty = \sup_{t \in \mathbb{R}} \|\xi_i^2(t)\| < \infty$, and $\|\dot{\xi}_i^2(t)\|_\infty = \sup_{t \in \mathbb{R}} \|\dot{\xi}_i^2(t)\| < \infty$, where $\|\star\|_\infty$ and $\|\star\|$ represents the \mathcal{L}_∞ norm and Euclidean norm, respectively.

3 Collusive stealthy attack mechanism

In light of the vulnerabilities, large-scale characteristics, and inherent uncertainties of cyber-physical microgrids, this section presents a detection scheme based on the \mathcal{L}_∞ UIO for identifying communication link risks between DGUs. Additionally, a novel of collusive stealthy attack is proposed to bypass current defense mechanisms.

3.1 \mathcal{L}_∞ UIO-based countermeasure

As illustrated in Figure 1 and the consensus scheme Equation (5), the secondary control of DGU i requires the measured outputs transmitted from neighboring DGU j . Malicious adversaries could exploit inherent

vulnerabilities in communication channels to execute cyber intrusions, deliberately falsifying transmitted data and compromising information integrity. This adversarial manipulation directly impacts secondary control inputs, ultimately undermining system performance. In general, such attacks mainly disrupt the integrity of data through the replacement or modification of critical parameters [4]. The FDI attack between the communication link of DGU i and DGU j can be modeled as:

$$y_{i,j}^{re}(t) = y_j(t) + \chi_j(t - t_j^s) y_{i,j}^a(t), \quad (6)$$

where $y_{i,j}^{re}(t)$, t_j^s , $\chi_i(\cdot)$, and $y_{i,j}^a(t)$, denotes the actual measurement received by DGU i , the attack initiation time instant, time-delayed step function characterized by t_j^s , and attack signals, respectively.

The implementation of a distributed detection framework is essential for addressing the vulnerability of microgrids to cascading failures induced by cyber-attack propagation. This architecture facilitates concurrent monitoring of DGUs, ensuring prompt identification and containment of compromised components. Cyber-physical microgrids inherently comprise interconnected subsystems characterized by dual-layer coupling: physical layer interactions governed by power flow dynamics and cyber layer communications mediated through network protocols and control architectures [14]. To establish independent state estimation without relying on global system data, a dedicated \mathcal{L}_∞ UIO is deployed for each communication channel, effectively treating inter-subsystem connections and secondary control inputs as unknown inputs. The observer embedded in DGU i produces the state estimation $\hat{x}_{i,j}^o(t)$ of DGU j , formally expressed as:

$$\begin{cases} \dot{z}_{i,j}^o(t) = F_j^o z_{i,j}^o(t) + T_j^o \bar{B}_j \bar{u}_{i,j}^{re}(t) + K_j^o y_{i,j}^{re}(t), \\ \hat{x}_{i,j}^o(t) = z_{i,j}^o(t) + H_j^o y_{i,j}^{re}(t), \end{cases} \quad (7)$$

where $F_j^o \in \mathbb{R}^{3 \times 3}$, $T_j^o \in \mathbb{R}^{3 \times 3}$, $K_j^o \in \mathbb{R}^{3 \times 3}$, and $H_j^o \in \mathbb{R}^{3 \times 3}$ are the UIO $_{i,j}$ gain matrices, $z_{i,j}^o(t) \in \mathbb{R}^3$ is the state of UIO $_{i,j}$, $\bar{u}_{i,j}(t)$ represents the input of DGU j transmitted to DGU i . The asymptotic convergence of $\hat{x}_{i,j}^o(t)$ toward $x_j(t)$ is guaranteed under the dual conditions [21].

(1) $\text{rank}(C_j \mathbb{F}_j^o) = \text{rank}(\mathbb{F}_j^o)$, where $\mathbb{F}_j^o \bar{d}_j(t) = \bar{B}_j \bar{u}_j(t) + \sum_{k \in \mathcal{N}_j^e} A_{jk} (x_k(t) - x_j(t))$, and $\bar{d}_j(t)$ denotes the unknown inputs of the UIO $_{i,j}$.

(2) The pair (C_j, A_{jj}^o) is detectable, where $A_{jj}^o = \bar{A}_{jj} - H_j^o C_j \bar{A}_{jj}$ and $\bar{A}_{jj} = A_{jj} + \bar{B}_j K_j^T C_j$.

Then, decompose K_j^o into $K_j^o = \tilde{K}_j^o + \check{K}_j^o$ and determine the UIO $_{i,j}$ gain matrices F_j^o , T_j^o , K_j^o , and H_j^o based on the following conditions:

$$0 = H_j^o C_j \mathbb{F}_j^o - \mathbb{F}_j^o, \quad (8a)$$

$$T_j^o = I_j - H_j^o C_j, \quad (8b)$$

$$F_j^o = A_{jj}^o - \tilde{K}_j^o C_j \text{ (Hurwitz)}, \quad (8c)$$

$$\check{K}_j^o = F_j^o H_j^o. \quad (8d)$$

where $I_j \in \mathbb{R}^{3 \times 3}$ is the identity matrix. The estimation error of UIO $_{i,j}$ is defined as $e_{i,j}^o(t) = x_j(t) - \hat{x}_{i,j}^o(t)$. Combining Equations (4), (7), and (8a)–(8d), yields its dynamics:

$$\dot{e}_{i,j}^o(t) = F_j^o e_{i,j}^o(t) + T_j^o \xi_j^1(t) - H_j^o \xi_j^2(t) - \bar{K}_j^o \xi_j^2(t). \quad (9)$$

It is evident that the estimation error $e_{i,j}^o(t)$ is independent of neighboring states; however, its complete decoupling from the disturbance $\xi_j^1(t)$ and measurement noise $\xi_j^2(t)$ has not yet been achieved. To improve the robustness of the UIO $_{i,j}$, a performance output associated with $e_{i,j}^o(t)$ is defined as $z_{i,j}^o(t) = C_j e_{i,j}^o(t)$. The designed observer gain is expected to ensure that the error system described by Equation (9), with performance output $z_{i,j}^o(t)$, achieves global uniform \mathcal{L}_∞ stability with a performance index γ_j , satisfying the following conditions [22].

(1) The zero-input dynamics of the system Equation (9) (with $\xi_j^1(t) \equiv \xi_j^2(t) \equiv \dot{\xi}_j^2(t) \equiv 0$) exhibits global uniform exponential stability concerning the origin.

(2) Given an arbitrary initial condition $e_{i,j}^o(t_0) = e_{i,j_0}^o$ and bounded exogenous input $\xi_j^1(t)$, $\xi_j^2(t)$, and $\dot{\xi}_j^2(t)$, a finite bound $\delta_j(e_{i,j_0}^o, \|T_j^o \xi_j^1(\cdot)\|_\infty, \|\xi_j^2(\cdot)\|_\infty, \|H_j^o \dot{\xi}_j^2(t)\|_\infty)$ can be determined such that

$$\|e_{i,j}^o(t)\| \leq \delta_j(e_{i,j_0}^o, \|T_j^o \xi_j^1(\cdot)\|_\infty, \|\xi_j^2(\cdot)\|_\infty, \|H_j^o \dot{\xi}_j^2(t)\|_\infty), \forall t \geq t_0. \quad (10)$$

(3) Given zero initial condition $e_{i,j}^o(t_0) = 0$ and bounded exogenous input $\xi_j^1(t)$, $\xi_j^2(t)$, and $\dot{\xi}_j^2(t)$, the following holds:

$$\|z_{i,j}^o(t)\| \leq \gamma_j(\|T_j^o \xi_j^1(\cdot)\|_\infty + \|\xi_j^2(\cdot)\|_\infty + \|H_j^o \dot{\xi}_j^2(t)\|_\infty), \forall t \geq t_0. \quad (11)$$

(4) Given an arbitrary initial condition $e_{i,j}^o(t_0) = e_{i,j_0}^o$ and bounded exogenous input $\xi_j^1(t)$, $\xi_j^2(t)$, and $\dot{\xi}_j^2(t)$, the following holds:

$$\limsup_{t \rightarrow \infty} \|z_{i,j}^o(t)\| \leq \gamma_j(\|T_j^o \xi_j^1(\cdot)\|_\infty + \|\xi_j^2(\cdot)\|_\infty + \|H_j^o \dot{\xi}_j^2(t)\|_\infty). \quad (12)$$

To ensure that the UIO $_{i,j}$ achieves the desired \mathcal{L}_∞ performance, the following theorem presents the conditions that its gain needs to satisfy, along with the method for solving the observer gain.

Theorem 1. For the monitoring center of DGU i with UIO $_{i,j}$ Equation (7), providing observer gains F_j^o , T_j^o , K_j^o , and H_j^o satisfy conditions Equations (8a)–(8d), and there exist matrix $S_j^o \in \mathbb{R}^{3 \times 3}$, $P_j^o \in \mathbb{R}^{3 \times 3}$ and $P_j^o = P_j^{oT} > 0$, positive scalar $\alpha_j^o > 0$, $\nu_j^1 > 0$, and $\nu_j^2 > 0$ such that the following inequality holds:

$$\Upsilon_j^o = \begin{bmatrix} \tilde{Y}_j^o & P_j^o & -S_j^o & P_j^o \\ * & -2\alpha_j^o \nu_j^1 I_j & 0 & 0 \\ * & * & -2\alpha_j^o \nu_j^1 I_j & 0 \\ * & * & * & -2\alpha_j^o \nu_j^1 I_j \end{bmatrix} \leq 0, \quad (13)$$

$$\Psi_j^o = \begin{bmatrix} P_j^o & C_j^{oT} \\ * & \nu_j^2 I_j \end{bmatrix} \geq 0, \quad (14)$$

where $\tilde{Y}_j^o = 2\alpha_j^o P_j^o + P_j^o A_{jj}^o + A_{jj}^{oT} P_j^o - S_j^{oT} C_j^o - C_j^{oT} S_j^o$, then the estimation error dynamics Equation (9) of the UIO $_{i,j}$ is globally uniformly \mathcal{L}_∞ stable with a performance index $\gamma_j = \sqrt{\nu_j^1 \nu_j^2}$ and observer gain $\tilde{K}_j^o = P_j^{o-1} S_j^o$.

Proof: Define a Lyapunov function as follows:

$$V_j^o(t) = e_{i,j}^o(t)^T P_j^o e_{i,j}^o(t). \quad (15)$$

Let $\lambda_{\max}(P_j^o)$ and $\lambda_{\min}(P_j^o)$ denote the maximum and minimum eigenvalues of P_j^o , respectively. Then, from Equation (15), we have

$$\lambda_{\min}(P_j^o) \|e_{i,j}^o(t)\| \leq V_j^o(t) \leq \lambda_{\max}(P_j^o) \|e_{i,j}^o(t)\|. \quad (16)$$

The time derivative of $V_j^o(t)$ is given by

$$\dot{V}_j^o(t) = 2e_{i,j}^o(t)^T P_j^o (A_{jj}^o e_{i,j}^o(t) - \tilde{K}_j^o C_j^o + T_j^o \xi_j^1(t) - H_j^o \dot{\xi}_j^2(t) - \bar{K}_j^o \xi_j^2(t)). \quad (17)$$

Define $\eta_j^o(t) = [e_{i,j}^o(t)^T, \xi_j^1(t)^T T_j^{oT}, \xi_j^2(t)^T, -\dot{\xi}_j^2(t)^T H_j^{oT}]$, one obtains

$$\dot{V}_j^o(t) + 2\alpha_j^o V_j^o(t) - 2\alpha_j^o \nu_j^1 \|T_j^o \xi_j^1(t)\|^2 - 2\alpha_j^o \nu_j^1 \|\xi_j^2(t)\|^2 - 2\alpha_j^o \nu_j^1 \|H_j^o \dot{\xi}_j^2(t)\|^2 = \eta_j^o(t)^T \Omega_j^o \eta_j^o(t), \quad (18)$$

where

$$\Omega_j^o = \begin{bmatrix} \bar{\Omega}_j^o & P_j^o & -P_j^o \tilde{K}_j^o & P_j^o \\ * & -2\alpha_j^o \nu_j^1 I_j & 0 & 0 \\ * & * & -2\alpha_j^o \nu_j^1 I_j & 0 \\ * & * & * & -2\alpha_j^o \nu_j^1 I_j \end{bmatrix}, \quad (19)$$

and $\bar{\Omega}_j^o = 2\alpha_j^o P_j^o + P_j^o A_{jj}^o + A_{jj}^{oT} P_j^o - P_j^o \tilde{K}_j^o C_j^o - C_j^{oT} \tilde{K}_j^{oT} P_j^o$. Then, setting $P_j^o \tilde{K}_j^o = S_j^o$ and substituting it into Equations (18) and (19), one obtains

$$\dot{V}_j^o(t) + 2\alpha_j^o V_j^o(t) - 2\alpha_j^o \nu_j^1 \|T_j^o \xi_j^1(t)\|^2 - 2\alpha_j^o \nu_j^1 \|\xi_j^2(t)\|^2 - 2\alpha_j^o \nu_j^1 \|H_j^o \dot{\xi}_j^2(t)\|^2 = \eta_j^o(t)^T \Upsilon_j^o \eta_j^o(t). \quad (20)$$

Thus, the establishment of Equation (13) can ensure Equation (20) ≤ 0 , one obtains

$$\dot{V}_j^o(t) \leq -2\alpha_j^o(V_j^o(t) - \nu_j^1 \|T_j^o \xi_j^1(t)\|^2 - \nu_j^1 \|\xi_j^2(t)\|^2 - \nu_j^1 \|H_j^o \dot{\xi}_j^2(t)\|^2), \quad (21)$$

which implies

$$V_j^o(t) \leq e^{-2\alpha_j^o(t-t_o)} V_j^o(t_o) + \nu_j^1 (\|T_j^o \xi_j^1(t)\|_\infty^2 + \|\xi_j^2(t)\|_\infty^2 + \|H_j^o \dot{\xi}_j^2(t)\|_\infty^2). \quad (22)$$

By combining inequalities Equations (16) and (22), it can be derived that

$$\|e_{i,j}^o(t)\| \leq \sqrt{\frac{\lambda_{\max}(P_j^o)}{\lambda_{\min}(P_j^o)}} e^{-\alpha_j^o(t-t_o)} \|e_{i,j}^o(t_o)\| + \sqrt{\frac{\nu_j^1}{\lambda_{\min}(P_j^o)}} (\|T_j^o \xi_j^1(t)\|_\infty + \|\xi_j^2(t)\|_\infty + \|H_j^o \dot{\xi}_j^2(t)\|_\infty). \quad (23)$$

Thus, the zero-input dynamics of the system Equation (9) (with $\xi_j^1(t) \equiv \xi_j^2(t) \equiv \dot{\xi}_j^2(t) \equiv 0$) is global uniform exponential stability concerning the origin and condition Equation (10) is satisfied. Then, defining the following matrix

$$\Psi_j^0 = \begin{bmatrix} P_j^o & C_j^T \\ * & \nu_j^2 I_j \end{bmatrix} \quad (24)$$

and inequality Equation (14) is satisfied. By the Schur complement lemma, it can be concluded that

$$P_j^o - \nu_j^{2-1} C_j^T C_j \geq 0. \quad (25)$$

By multiplying both the left and right sides of Equation (25) by $e_{i,j}^o(t)^T$ and its transpose, respectively, we obtain

$$e_{i,j}^o(t)^T P_j^o e_{i,j}^o(t) - \nu_j^{2-1} e_{i,j}^o(t)^T C_j^T C_j e_{i,j}^o(t) \geq 0, \quad (26)$$

which implies $\|z_{i,j}^o(t)\|^2 \leq \nu_j^2 V_j^o(t)$, Combined with Equation (22), we obtain

$$\|z_{i,j}^o(t)\| \leq \sqrt{\nu_j^2 V_j^o(t_o)} e^{-\alpha_j^o(t-t_o)} + \sqrt{\nu_j^1 \nu_j^2} (\|T_j^o \xi_j^1(t)\|_\infty + \|\xi_j^2(t)\|_\infty + \|H_j^o \dot{\xi}_j^2(t)\|_\infty). \quad (27)$$

Thus, condition Equations (11) and (12) are satisfied. This completes the proof. \blacksquare

Remark 1. Based on Equations (8a)–(8d) and Theorem 1, it is evident that the gain of $\text{UIO}_{i,j}$ implemented in DGU i can be determined solely using local information, independent of global system data. This local computation capability ensures the scalability of our proposed monitoring framework. Notably, the designed observer maintains its functionality without requiring global redesign when a compromised DGU is removed or a new DGU is integrated into the microgrid system.

Under the aforementioned design structure, the detection residual is crafted as $r_{i,j}^o(t) = y_{i,j}^r - \hat{y}_{i,j}^o(t)$, where $\hat{y}_{i,j}^o(t) = C_j \hat{x}_{i,j}^o(t)$. The evaluation standard is determined by the Euclidean norm of residual $r_{i,j}^o(t)$. The detection mechanism functions according to the subsequent principle [5]:

$$\begin{cases} \|r_{i,j}^o(t)\| \leq \bar{r}_{i,j}^o(t) \Rightarrow \text{No alarm,} \\ \|r_{i,j}^o(t)\| > \bar{r}_{i,j}^o(t) \Rightarrow \text{Alarm for attacks.} \end{cases} \quad (28)$$

The detection mechanism in the control center of DGU i activates an alarm signal upon violation of the predetermined threshold boundary, indicating potential anomalies in communication link ij ; conversely, the communication link ij is considered to be functioning normally. Notably, the threshold $\bar{r}_{i,j}^o(t)$ is typically defined as $\bar{r}_{i,j}^o(t) = \bar{r}_{i,j}^{o1}(t) + \bar{r}_{i,j}^{o2}(t)$, where $\bar{r}_{i,j}^{o1}(t)$ is a small constant introduced to reduce false alarms, and $\bar{r}_{i,j}^{o2}(t)$ represents the supremum of residuals under attack-free conditions. While $\bar{r}_{i,j}^{o2}(t) = 0$ holds when the microgrid experiences no external disturbances and observer initialization matches the system's initial state, these idealized assumptions rarely apply in practice. Thus, Monte Carlo simulations are conducted considering both measurement noise, load perturbations, and randomized initial conditions to statistically determine the residual supremum $\bar{r}_{i,j}^{o2}(t)$.

3.2 Implementation and analysis of collusive stealth attack

Considering the potential scenario where adversaries possess comprehensive knowledge of DGU models, they can design sophisticated attack signals to disrupt cyber-physical microgrid operations while evading detection. This section presents a systematic framework for constructing collusive stealth attacks, where the attacker simulates system dynamics to generate malicious signals. These signals are subsequently injected into the communication channel ij , concurrently compromising both the measurement $y_j(t)$ and control input $\bar{u}_j(t)$. The measurement signal $y_j^{re}(t)$ received by the control center of DGU i is expressed as in Equation (6), while the actual input signal $\bar{u}_{i,j}^{re}(t)$ is given by $\bar{u}_{i,j}^{re}(t) = \bar{u}_j(t) + \chi_j(t - t_j^s)\bar{u}_{i,j}^a(t)$, where $y_{i,j}^a(t)$ is dynamically generated as follows:

$$\begin{cases} \dot{x}_{i,j}^a(t) = \bar{A}_{jj}x_{i,j}^a(t) + \bar{B}_j\bar{u}_{i,j}^a(t) + \mathbb{F}_j^o\bar{d}_{i,j}^a(t), \\ y_{i,j}^a(t) = C_jx_{i,j}^a(t), \end{cases} \quad (29)$$

where $\bar{u}_{i,j}^a(t) = (\bar{B}_j^T \bar{B}_j)^{-1} \bar{B}_j^T \mathbb{F}_j^o \bar{d}_{i,j}^a(t)$ represents the injected attack signal, $\bar{d}_{i,j}^a(t)$ and $\bar{d}_{i,j}^a(t)$ are arbitrary non-zero false data. For simplicity, we denote $E_j^o = (\bar{B}_j^T \bar{B}_j)^{-1} \bar{B}_j^T \mathbb{F}_j^o$. The following theorem demonstrates the stealthiness of the collusion attack strategy designed for communication link ij .

Theorem 2. For the DC microgrids Equation (4) incorporating \mathcal{L}_∞ UIO-based detection mechanisms Equations (7) and (28), the communication link ij is injected with $\bar{u}_{i,j}^a(t)$ and $y_{i,j}^a(t)$, where $\bar{u}_{i,j}^a(t) = (\bar{B}_j^T \bar{B}_j)^{-1} \bar{B}_j^T \mathbb{F}_j^o \bar{d}_{i,j}^a(t)$ and $y_{i,j}^a(t)$ are generated by Equation (29). This manipulation does not prompt an alert from the monitoring center, indicating that the collusion attack strategy is stealthy.

Proof: Considering $t < t_j^s$, the cyber-physical microgrid is free from malicious attacks and operates normally, the estimation error dynamics of the UIO $_{i,j}$ in the DGU i monitoring center is given by Equation (9). Considering $t \geq t_j^s$, the communication link ij is subjected to the aforementioned collusion attack, the dynamics of the \mathcal{L}_∞ UIO $_{i,j}$ can be expressed as follows:

$$\begin{cases} \dot{\tilde{z}}_{i,j}^o(t) = F_j^o \tilde{z}_{i,j}^o(t) + T_j^o(\bar{u}_j(t) + \bar{u}_{i,j}^a(t)) + K_j^o(y_j(t) + y_{i,j}^a(t)), \\ \dot{\tilde{x}}_{i,j}^o(t) = \tilde{z}_{i,j}^o(t) + H_j^o(y_j(t) + y_{i,j}^a(t)). \end{cases} \quad (30)$$

At this point, the detection residual can be expressed as: $\tilde{r}_{i,j}^o(t) = y_j(t) + y_{i,j}^a(t) - \hat{y}_{i,j}^o(t) = C_j \tilde{e}_{i,j}^o(t) + \xi_i^2(t)$, where $\tilde{e}_{i,j}^o(t) = x_j(t) + x_{i,j}^a(t) - \hat{x}_{i,j}^o(t)$. By integrating Equations (4), (8a)–(8d), (29), and (30), the dynamics of the estimation error can be derived:

$$\begin{aligned} \dot{\tilde{e}}_{i,j}^o(t) &= \dot{x}_j(t) + \dot{x}_{i,j}^a(t) - \dot{\hat{x}}_{i,j}^o(t) \\ &= \bar{A}_{jj}x_j(t) + \bar{B}_j(\bar{u}_j(t) + \bar{u}_{i,j}^a(t)) + \mathbb{F}_j^o\bar{d}_j(t) + \xi_i^1(t) + \bar{A}_{jj}x_{i,j}^a(t) + \bar{B}_j\bar{u}_{i,j}^a(t) + \mathbb{F}_j^o\bar{d}_{i,j}^a(t) - F_j^o\tilde{z}_{i,j}^o(t) \\ &\quad - T_j^o(\bar{u}_j(t) + \bar{u}_{i,j}^a(t)) - K_j^o(y_j(t) + y_{i,j}^a(t)) - H_j^oC_j(\bar{A}_{jj}x_{i,j}^a(t) + \bar{B}_j(\bar{u}_j(t) + \bar{u}_{i,j}^a(t)) + \mathbb{F}_j^o\bar{d}_j(t) \\ &\quad + \xi_i^1(t)) - H_j^oC_j(\bar{A}_{jj}x_{i,j}^a(t) + \bar{B}_j\bar{u}_{i,j}^a(t) + \mathbb{F}_j^o\bar{d}_{i,j}^a(t)) \\ &= \bar{A}_{jj}x_j(t) + \xi_i^1(t) + \bar{A}_{jj}x_{i,j}^a(t) + \mathbb{F}_j^o\bar{d}_{i,j}^a(t) - F_j^o(\hat{x}_{i,j}^o(t) - H_j^o(C_jx_j(t) + C_jx_{i,j}^a(t))) - K_j^o(y_j(t) \\ &\quad + y_{i,j}^a(t)) - H_j^oC_j(\bar{A}_{jj}x_{i,j}^a(t) + \xi_i^1(t)) - H_j^oC_j(\bar{A}_{jj}x_{i,j}^a(t) + \mathbb{F}_j^o\bar{d}_{i,j}^a(t)) \\ &= F_j^o\tilde{e}_{i,j}^o(t) + T_j^o\xi_i^1(t) - H_j^o\xi_i^2(t) - \bar{K}_j^o\xi_i^2(t). \end{aligned} \quad (31)$$

Evidently, the estimation error dynamics Equation (9) of the \mathcal{L}_∞ UIO $_{i,j}$ in the absence of attacks are equivalent to those Equation (31) under the collusion attack, implying that the attack does not affect the detection residuals $r_{i,j}^o(t)$, thereby maintaining stealthy. The proof is concluded. \blacksquare

Remark 2. The proposed collusive attack strategy simultaneously compromises the integrity of both $y_j(t)$ and $\bar{u}_j(t)$. As evidenced by Equation (5), the corrupted measurement $y_j^{re}(t)$ directly affects the secondary control input, consequently degrading system performance. Furthermore, Theorem 2 demonstrates that the error system dynamics remain consistent before and after the attack, indicating that the collusive attack does not induce residual anomalies. Consequently, this attack strategy can effectively disrupt system performance without triggering any alarm signals.

Compared to classical FDI attacks, the proposed collusion attack strategy exhibits enhanced destructiveness and stealthiness. Consequently, to ensure the continuous and stable operation of cyber-physical microgrids, it is imperative to devise corresponding countermeasures for timely detection of such malicious attacks.

4 Dynamic encoding detection scheme

In Theorem 2, it has been demonstrated that the proposed collusive attack is stealthy and can evade detection by the \mathcal{L}_∞ UIO-based detection module. This section will present the design of a dynamic coding-based scheme to detect the aforementioned collusive stealthy attack. The core strategy involves integrating an encoder-decoder pair into the communication link ij to limit the adversary's ability to disclose information. This ensures that the attacker cannot neutralize the system's response through the injected signals $\vec{u}_{i,j}^a(t)$ and $y_{i,j}^a(t)$. As a consequence, the compromised measurement outputs $y_{i,j}^{re}(t)$ become discernible from the normal outputs $y_j(t)$, causing the residual $r_{i,j}^o(t)$ in the detection module to surpass the threshold $\bar{r}_{i,j}^o(t)$ significantly, thereby activating an alarm.

Actually, the control center of DGU i not only utilizes $y_{i,j}^{re}(t)$ to generate the secondary control input $\vec{u}_i(t)$ but also employs $\vec{u}_{i,j}^a(t)$ to estimate $x_j(t)$, thereby monitoring anomalies in the communication link ij . As depicted in Figure 1, a pair of dynamic encoder and decoder is deployed in the communication link ij , where the input $\vec{u}_j(t)$ is encoded into $\vec{U}_j(t)$ before being transmitted over the communication network, with $\vec{U}_j(t)$ defined as follows:

$$\vec{U}_j(t) = e^{\cos(t)} \Phi_j \vec{u}_j(t), \quad (32)$$

where Φ_j is an invertible matrix of appropriate dimension. Actually, the time-varying nature of $e^{\cos(t)} \Phi_j$ renders it inherently challenging for the attacker to accurately discern the coding matrix. Consequently, when a malicious adversary initiates the injection of attack signals $\vec{u}_{i,j}^a(t)$, unaware of the dynamic encoding scheme, the compromised signal is altered as follows:

$$\vec{U}_j(t) = e^{\cos(t)} \Phi_j \vec{u}_j(t) + \vec{u}_{i,j}^a(t). \quad (33)$$

Before the input signal being transmitted into the control center, $\vec{U}_j(t)$ undergoes decoding as follows:

$$\vec{u}_{i,j}^{re}(t) = e^{-\cos(t)} \Phi_j^{-1} \vec{U}_j(t) = \vec{u}_j(t) + e^{-\cos(t)} \Phi_j^{-1} \vec{u}_{i,j}^a(t). \quad (34)$$

Evidently, the control signal of DGU i operates independently of $\vec{u}_{i,j}^{re}(t)$, ensuring that the aforementioned dynamic encoding mechanism does not interfere with the operation of the cyber-physical microgrid, thereby avoiding any degradation in system performance. On the other hand, in the absence of an attack scenario where $\vec{u}_{i,j}^a(t) \equiv 0$, the input signal is restored to

$$\vec{u}_{i,j}^{re}(t) = \vec{u}_j(t) + e^{-\cos(t)} \Phi_j^{-1} \vec{u}_{i,j}^a(t) \equiv \vec{u}_j(t). \quad (35)$$

Consequently, the aforementioned dynamic encoding mechanism does not induce false alarms even in the attack-free scenario. The following theorem presents the estimation error dynamics of the UIO $_{i,j}$ in an attack scenario when the system employs the dynamic encoding mechanism.

Theorem 3. In the DC microgrid Equation (4) equipped with the detection framework based on \mathcal{L}_∞ UIO and dynamic encoding mechanism, the estimation error dynamics of UIO $_{i,j}$ when the collusive stealthy attack is injected into communication link ij can be represented as:

$$\dot{\tilde{e}}_{i,j}^o(t) = F_j^o \tilde{e}_{i,j}^o(t) - e^{-\cos(t)} T_j^o \bar{B}_j \Phi_j^{-1} E_j^o \vec{d}_{i,j}^a(t) + T_j^o \xi_j^1(t) - H_j^o \dot{\xi}_j^2(t) - \bar{K}_j^o \xi_j^2(t). \quad (36)$$

That is, with the assistance of the dynamic encoding mechanism, the dynamics of the estimation error under collusive attacks differ from those under normal conditions, as described in Equation (36). By selecting appropriate dynamic encoding matrices, the detection residual $r_{i,j}^o(t)$ can be sufficiently amplified to exceed the predefined threshold $\bar{r}_{i,j}^o(t)$, thereby triggering an alarm.

Proof: By combining Equations (4), (8a)–(8d), (29), (30), (34), and differentiating with respect to $\tilde{e}_{i,j}^o(t) = x_j(t) + x_{i,j}^a(t) - \hat{x}_{i,j}^o(t)$, we obtain

$$\begin{aligned}
 \dot{\tilde{e}}_{i,j}^o(t) &= \dot{x}_j(t) + \dot{x}_{i,j}^a(t) - \dot{\hat{x}}_{i,j}^o(t) \\
 &= \bar{A}_{jj}x_j(t) + \bar{B}_j(\bar{u}_j(t) + \bar{u}_{i,j}^a(t)) + \mathbb{F}_j^o \bar{d}_j(t) + \xi_i^1(t) + \bar{A}_{jj}x_{i,j}^a(t) + \bar{B}_j \bar{u}_{i,j}^a(t) + \mathbb{F}_j^o \bar{d}_{i,j}^a(t) - F_j^o \tilde{z}_{i,j}^o(t) \\
 &\quad - T_j^o \bar{B}_j(\bar{u}_j(t) + e^{-\cos(t)} \Phi_j^{-1} \bar{u}_{i,j}^a(t)) - K_j^o(y_j(t) + y_{i,j}^a(t)) - H_j^o C_j(\bar{A}_{jj}x_{i,j}^a(t) + \bar{B}_j(\bar{u}_j(t) \\
 &\quad + \bar{u}_{i,j}^a(t)) + \mathbb{F}_j^o \bar{d}_j(t) + \xi_i^1(t)) - H_j^o C_j(\bar{A}_{jj}x_{i,j}^a(t) + \bar{B}_j \bar{u}_{i,j}^a(t) + \mathbb{F}_j^o \bar{d}_{i,j}^a(t)) \\
 &= \bar{A}_{jj}x_j(t) + \xi_i^1(t) + \bar{A}_{jj}x_{i,j}^a(t) + \mathbb{F}_j^o \bar{d}_{i,j}^a(t) - F_j^o(\hat{x}_{i,j}^o(t) - H_j^o(C_j x_j(t) + C_j x_{i,j}^a(t))) - K_j^o(y_j(t) + \\
 &\quad y_{i,j}^a(t)) - H_j^o C_j(\bar{A}_{jj}x_{i,j}^a(t) + \xi_i^1(t)) - e^{-\cos(t)} T_j^o \bar{B}_j \Phi_j^{-1} E_j^o \bar{d}_{i,j}^a(t) - H_j^o C_j(\bar{A}_{jj}x_{i,j}^a(t) + \mathbb{F}_j^o \bar{d}_{i,j}^a(t)) \\
 &= F_j^o \tilde{e}_{i,j}^o(t) - e^{-\cos(t)} T_j^o \bar{B}_j \Phi_j^{-1} E_j^o \bar{d}_{i,j}^a(t) + T_j^o \xi_j^1(t) - H_j^o \dot{\xi}_j^2(t) - \bar{K}_j^o \xi_j^2(t). \tag{37}
 \end{aligned}$$

It is noteworthy that Equation (37) exhibits distinct characteristics compared to Equations (9) and (31). Specifically, the implementation of the dynamic encoding scheme alters the estimation error dynamics in the presence of collusive attacks. Given the relationship $\tilde{r}_{i,j}^o(t) = C_j \tilde{e}_{i,j}^o(t) + \xi_i^2(t)$, the residual undergoes corresponding variations, thereby depriving the collusive attack of its concealment. ■

Based on the above analysis, it is evident that when the system is not under attack, the dynamic encoding mechanism does not alter the normal control signals, unlike additive watermarking schemes, which modify control signals and consequently lead to system performance degradation. However, when the system is under attack, the collusive stealth attack loses its stealthiness due to the dynamic encoding mechanism, thereby triggering an alarm. To ensure the impact of the attack signal manifests in the residual signal $\tilde{r}_{i,j}^o(t)$, the following theorem presents the feasibility conditions for the dynamic encoding matrix.

Theorem 4. Based on the deployed \mathcal{L}_∞ UIO $_{i,j}$ Equation (7) and dynamic encoding mechanism, the collusive stealthy attack Equation (29) can influence the detection residual $\tilde{r}_{i,j}^o(t)$ provided that the matrix $\mathbb{M}_{i,j}^o(s)$ possesses no non-minimum phase zero dynamics and $\text{rank}(C_j T_j^o \bar{B}_j \Phi_j^{-1} E_j^o) = \text{rank}(T_j^o \bar{B}_j \Phi_j^{-1} E_j^o)$, where

$$\mathbb{M}_{i,j}^o(s) = \begin{bmatrix} sI_j - F_j^o & T_j^o \bar{B}_j \Phi_j^{-1} E_j^o \\ C_j & 0 \end{bmatrix}. \tag{38}$$

Proof: Based on the analysis mentioned above, it can be concluded that after the implementation of the dynamic encoding mechanism, the error dynamics and detection residuals of UIO $_{i,j}$ are as follows:

$$\begin{cases} \dot{\tilde{e}}_{i,j}^o(t) = F_j^o \tilde{e}_{i,j}^o(t) - e^{-\cos(t)} T_j^o \bar{B}_j \Phi_j^{-1} E_j^o \bar{d}_{i,j}^a(t) + T_j^o \xi_j^1(t) - H_j^o \dot{\xi}_j^2(t) - \bar{K}_j^o \xi_j^2(t), \\ \tilde{r}_{i,j}^o(t) = C_j \tilde{e}_{i,j}^o(t) + \xi_i^2(t). \end{cases} \tag{39}$$

To ensure that the influence of any non-zero $\bar{d}_{i,j}^a(t)$ on $\tilde{e}_{i,j}^o(t)$ is reflected in $\tilde{r}_{i,j}^o(t)$, it is necessary to select an appropriate encoding matrix such that the Rosenbrock system matrix $\tilde{\mathbb{M}}_{i,j}^o(s)$ possesses no non-minimum phase zero dynamics and is left-invertible, where

$$\tilde{\mathbb{M}}_{i,j}^o(s) = \begin{bmatrix} sI_j - F_j^o & e^{-\cos(t)} T_j^o \bar{B}_j \Phi_j^{-1} E_j^o \\ C_j & 0 \end{bmatrix}. \tag{40}$$

Moreover, since $\text{rank}(\tilde{\mathbb{M}}_{i,j}^o(s)) = \text{rank}(\mathbb{M}_{i,j}^o(s))$, this condition is equivalent to require that the matrix $\mathbb{M}_{i,j}^o(s)$ possesses no non-minimum phase zero dynamics and is left-invertible. The left invertibility of the matrix $\mathbb{M}_{i,j}^o(s)$ is equivalent to the condition that the largest controllability subspace of system $\Sigma_{i,j}^o : (C_j, F_j^o, T_j^o \bar{B}_j \Phi_j^{-1} E_j^o)$ is contained within $\text{Ker}(C_j)$, with $\mathbb{M}_{i,j}^*(\Sigma_{i,j}^o)$ defined as zero. Furthermore, $\mathbb{M}_{i,j}^*(\Sigma_{i,j}^o)$ can be expressed as:

$$\mathbb{M}_{i,j}^*(\Sigma_{i,j}^o) = \mathbb{W}_{i,j}^*(\Sigma_{i,j}^o) \cap \mathbb{V}_{i,j}^*(\Sigma_{i,j}^o), \tag{41}$$

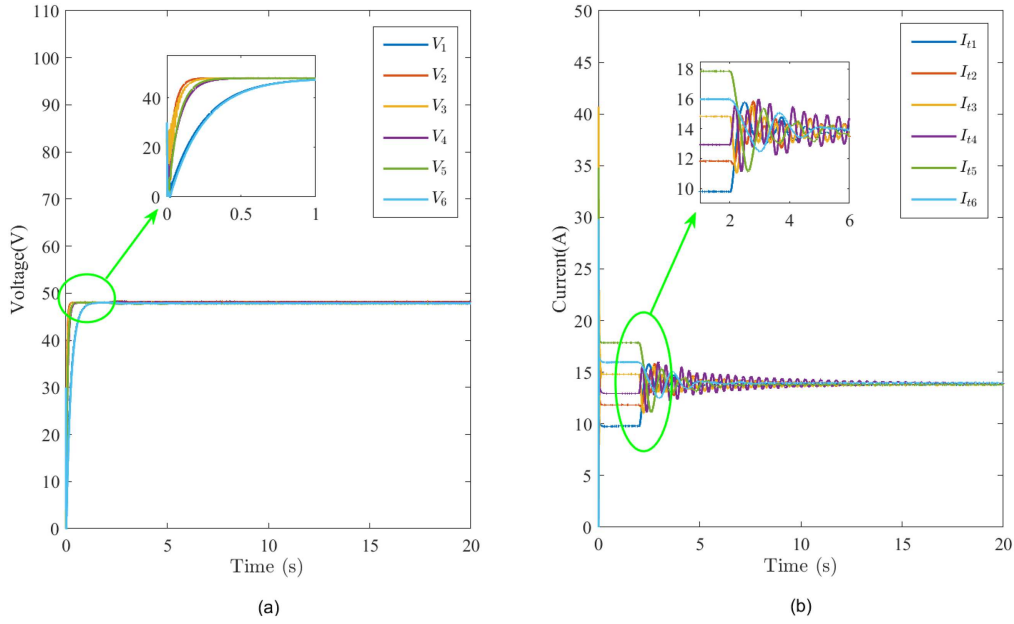


Figure 2. Simulation results under normal operating conditions. (a) and (b) correspond to the voltage at the PCC and the output current of the DGUs, respectively.

where $\mathbb{W}_{i,j}^*(\Sigma_{i,j}^o)$ represents the smallest conditioned invariant subspace encompassing $Im(T_j^o \vec{B}_j \Phi_j^{-1} E_j^o)$, and $\mathbb{V}_{i,j}^*(\Sigma_{i,j}^o)$ denotes the largest weakly unobservable subspace. The computational procedure for determining these subspaces is outlined as follows [23, 24]:

$$\mathbb{W}_{i,j}^*(\Sigma_{i,j}^o)_0 = Im(T_j^o \vec{B}_j \Phi_j^{-1} E_j^o), \quad \mathbb{W}_{i,j}^*(\Sigma_{i,j}^o)_k = \mathbb{W}_{i,j}^*(\Sigma_{i,j}^o)_{k-1} + F_j^o(\mathbb{W}_{i,j}^*(\Sigma_{i,j}^o)_{k-1} \cap Ker(C_j)), \quad (42)$$

$$\mathbb{V}_{i,j}^*(\Sigma_{i,j}^o)_0 = Ker(C_j), \quad \mathbb{V}_{i,j}^*(\Sigma_{i,j}^o)_k = \mathbb{V}_{i,j}^*(\Sigma_{i,j}^o)_0 \cap F_j^{o-1}(\mathbb{V}_{i,j}^*(\Sigma_{i,j}^o)_{k-1} + Im(T_j^o \vec{B}_j \Phi_j^{-1} E_j^o)), \quad (43)$$

where $\mathbb{W}_{i,j}^*(\Sigma_{i,j}^o)_k$ and $\mathbb{V}_{i,j}^*(\Sigma_{i,j}^o)_k$ converge to $\mathbb{W}_{i,j}^*(\Sigma_{i,j}^o)$ and $\mathbb{V}_{i,j}^*(\Sigma_{i,j}^o)$, respectively. Therefore, combining Equations (41)–(43), it can be concluded that when $\mathbb{W}_{i,j}^*(\Sigma_{i,j}^o)_0 \cap \mathbb{V}_{i,j}^*(\Sigma_{i,j}^o)_0 = 0$, then $\mathbb{M}_{i,j}^*(\Sigma_{i,j}^o) = 0$. This merely requires that $Im(T_j^o \vec{B}_j \Phi_j^{-1} E_j^o)$ does not lie in the null space of C_j , i.e., $rank(C_j T_j^o \vec{B}_j \Phi_j^{-1} E_j^o) = rank(T_j^o \vec{B}_j \Phi_j^{-1} E_j^o)$. The proof is thus completed. ■

5 Simulation results

To validate both the concealment and disruptive potential of the proposed coordinated attack strategy, along with the efficacy of the dynamic encryption-based detection mechanism, we implement a comprehensive simulation environment using the SimPowerSystems platform. The experimental setup encompasses a six DGUs microgrid configuration, with detailed electrical specifications and network topology referenced from [25].

Case 1: In this case, a simulation period of 20 s is considered, during which the cyber-physical microgrid operates without being subjected to any attacks. Initially, the six DGUs operate independently, with only the primary controller in effect. As shown in Figure 2a, the PCC voltages V_i rapidly track and stabilize at the reference values. At $t = 2$ s, the DGUs are interconnected *via* power lines, and the secondary controller is activated with current proportional parameter $I_{ti}^s = 1, \forall i \in \mathcal{V}^p$. As illustrated in Figure 2b, after a certain period of secondary controller operation, $\frac{I_{ti}}{I_{ti}^s} = \frac{I_{tj}}{I_{tj}^s}$ is achieved, demonstrating that current sharing is realized in the cyber-physical microgrid under a reliable network environment.

Case 2: In this case, the simulation period is set to 5 s. Similarly, for the first 2 s, the DGUs are considered to operate independently, and they begin to interconnect at $t = 2$ s. At $t = 3$ s, the communication link among DGUs 2–4 is subjected to the collusive stealthy attack, where $\vec{d}_{4,3}^a(t) = [0; 0.1]$ and $y_{4,3}^a(t)$ is generated by Equation (29). As shown in Figure 3, after the attack occurs, the voltage at the

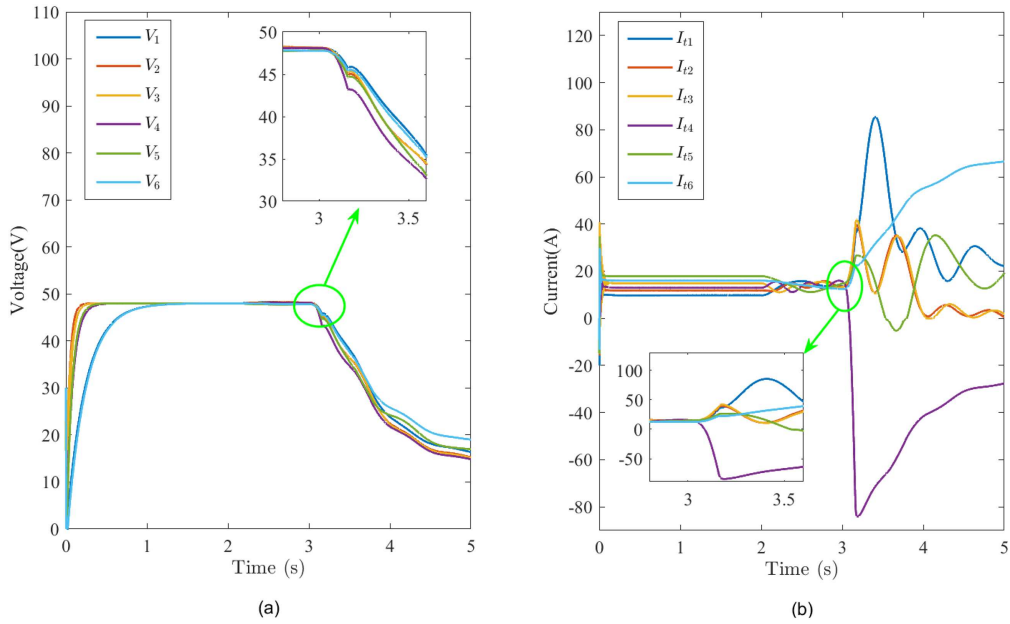


Figure 3. Simulation results under the scenario of the cyber-physical microgrid being subjected to the collusive stealthy attack. (a) and (b) correspond to the voltage at the PCC and the output current of the DGUs, respectively.

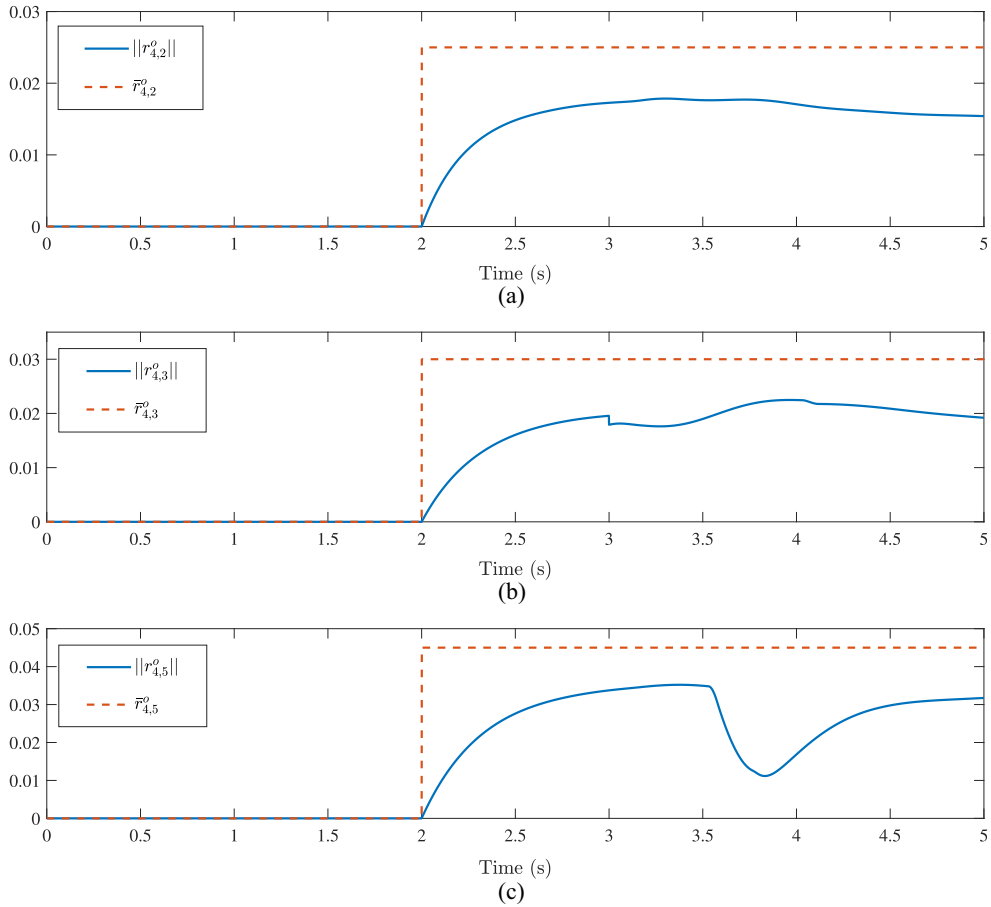


Figure 4. The detection threshold and detection residuals in the \mathcal{L}_∞ UIO-based detection module. (a), (b) and (c) present the experimental results corresponding to UIO_{4,2}, UIO_{4,3}, and UIO_{4,5}, respectively

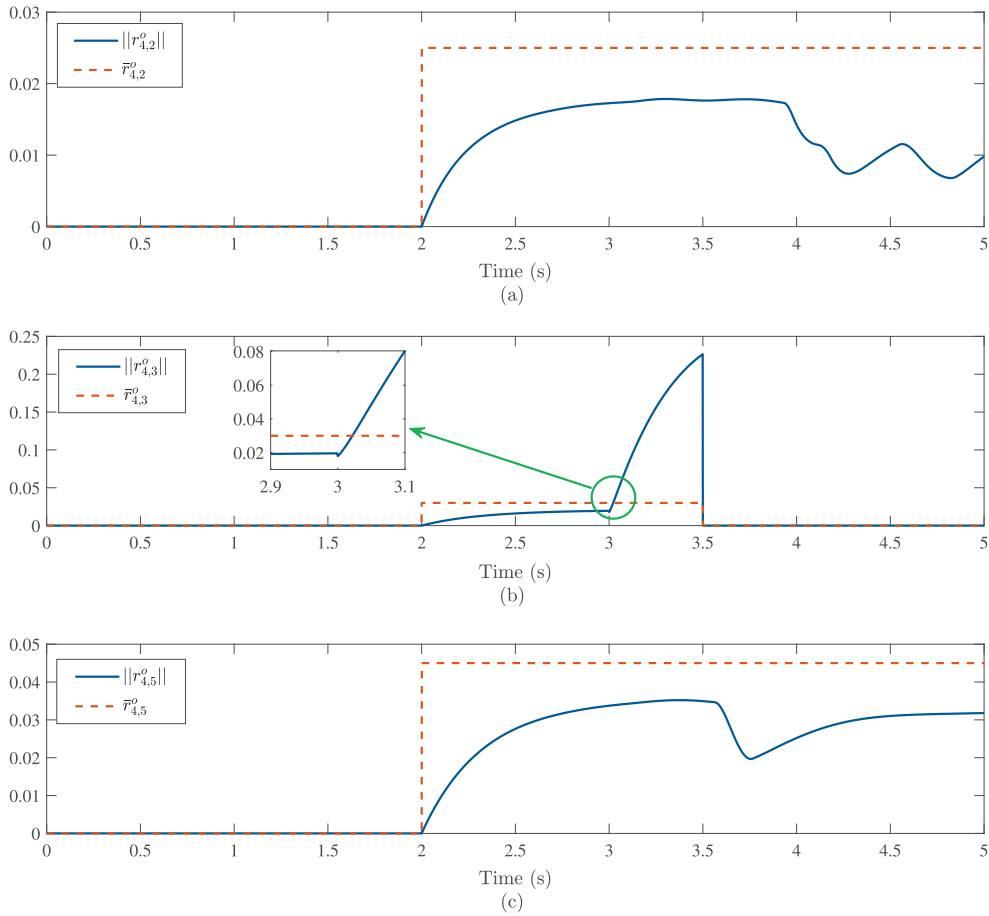


Figure 5. The detection threshold and detection residuals in the \mathcal{L}_∞ UIO-based detection module with the deployment of the dynamic encoding mechanism. (a), (b) and (c) present the experimental results corresponding to UIO_{4,2}, UIO_{4,3}, and UIO_{4,5}, respectively

PCC fails to track the reference value and diverges. The current also exhibits significant oscillations, and $\frac{I_{ti}}{I_{si}} \neq \frac{I_{tj}}{I_{sj}}$. This indicates that the negative impact of an attack on a single communication link rapidly propagates throughout the entire grid, affecting the overall system performance. Additionally, the monitoring results of UIO_{4,2}, UIO_{4,3}, and UIO_{4,5} deployed in the DGU 4 are presented in Figure 4. After the attack, none of the detection residuals show noticeable anomalies, all remaining below the threshold. This demonstrates that the collusive attack successfully evades detection while degrading system performance, posing a significant threat to the microgrid.

Case 3: In this case, similar to Case 2, the communication network is subjected to the collusive stealthy attack. However, the dynamic encoding mechanism proposed in this paper is deployed in the communication network, and $\Phi_3 = [0.001, 0.05; 0, 0.001]$ is selected based on Theorem 4. The monitoring results of UIO_{4,2}, UIO_{4,3}, and UIO_{4,5} in DGU 4 are shown in Figure 5. Before the attack occurs, all detection residuals remain below the threshold and exhibit no anomalies, indicating that the deployment of the dynamic encoding mechanism does not trigger false alarms. After the communication link among DGUs 2–4 is subjected to the collusive stealthy attack, the detection residual generated by UIO_{4,3} exhibits an abnormal increase and quickly exceeds the threshold, while other detection residuals remain unaffected. This demonstrates that the proposed detection mechanism can accurately identify the attack and precisely locate the compromised link. At $t = 3.5$ s, DGU 3 is proactively disconnected to prevent further propagation of the attack effects. The remaining detection modules require no redesign and continue to monitor the microgrid effectively, highlighting the scalability of the proposed detection framework.

6 Conclusion

This paper has proposed a dynamic encoding-based detection framework to combat collusive stealthy attacks in cyber-physical microgrids. An \mathcal{L}_∞ UIO was established at the control center to track communication link ij . The observer shows strong robustness, and its gain is calculated without needing information from neighboring DGUs. Subsequently, a collusive stealthy attack strategy has been proposed, which simultaneously compromises the integrity of input and output data, thereby disrupting grid performance, such as voltage regulation and current sharing. To counter the threat of the collusive stealthy attack, a dynamic encoding-based detection scheme has been introduced. This scheme does not degrade system performance in the absence of attacks but assists the \mathcal{L}_∞ UIO in generating anomalous detection residuals in the presence of attacks. Additionally, the feasibility conditions for the encoding matrix have been rigorously analyzed. Finally, the destructiveness of the attack and the effectiveness of the detection framework have been validated through MATLAB-based microgrid simulations. Future research could extend the proposed detection framework to cyber-physical microgrids with nonlinear loads, along with the development of data-driven detection strategies based solely on system measurements.

Acknowledgments

We would like to thank all editors and reviewers who helped to improve the paper.

Funding

This work was supported in part by the Foundation for Innovative Research Groups of the National Natural Science Foundation of China (Grant No. 62421004), and in part by the National Natural Science Foundation of China (Grant Nos. 62173218 and 62103254).

Conflicts of interest

The authors declare no conflicts of interest.

Data availability statement

The original data are available from corresponding authors upon reasonable request.

Author contribution statement

Zhihua Wu: Conceptualization, Methodology, Formal analysis, Software, Validation, Writing-review & editing. Chen Peng: Data curation, Writing-original draft, Conceptualization, Methodology, Software, Supervision. Engang Tian: Visualization, Investigation, Methodology, Supervision. Yajian Zhang: Validation, Methodology, Formal analysis, Supervision.

References

- [1] Zhang K, Shi Y, Karnouskos S, et al. Advancements in industrial cyber-physical systems: An overview and perspectives. *IEEE Trans Ind Inform* 2023; **19**: 716–29.
- [2] Chae J, Lee S, Jang J, et al. A survey and perspective on industrial cyber-physical systems (ICPS): From ICPS to AI-augmented ICPS. *IEEE Trans Ind Cyber-Phys Syst* 2023; **1**: 257–72.
- [3] Leng J, Sha W, Wang B, et al. Industry 5.0: Prospect and retrospect. *J Manuf Syst* 2022; **65**: 279–95.
- [4] Peng C, Sun H, Yang M, et al. A survey on security communication and control for smart grids under malicious cyber attacks. *IEEE Trans Syst Man Cybern: Syst* 2019; **49**: 1554–569.
- [5] Ding SX. A note on diagnosis and performance degradation detection in automatic control systems towards functional safety and cyber security. *Secur Saf* 2022; **1**: 2022004.
- [6] Gao S, Zhang H, Wang Z, et al. Optimal injection attack strategy for cyber-physical systems: A dynamic feedback approach. *Secur Saf* 2022; **1**: 2022005.
- [7] Zhu K, Wang Z, Ding D, et al. Privacy-preserving control for 2-D systems with guaranteed probability. *IEEE Trans Syst Man Cybern: Syst* 2024; **54**: 4999–5011.
- [8] Liang G, Weller SR, Zhao J, et al. The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Trans Power Syst* 2017; **32**: 3317–318.
- [9] Condliffe J. Ukraine's power grid gets hacked again, a worrying sign for infrastructure attacks. *MIT Technology Review*, 2016.
- [10] Yang H, Yu Z, Zhang Y. Event-triggered resilient consensus control of multiple unmanned systems against periodic DoS attacks based on state predictor. *Secur Saf* 2023; **2**: 2023017.
- [11] Zhang Y, Mei D, Xu Y, et al. Adaptive cooperative secure control of networked multiple unmanned systems under FDI attacks. *Secur Saf* 2023; **2**: 2023029.
- [12] Qin J, Li M, Shi L, et al. Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks. *IEEE Trans Automat Control* 2018; **63**: 1648–663.
- [13] Tian E, Fan M, Ma L, et al. Stochastic important-data-based attack power allocation against remote state estimation in sensor networks. *IEEE Trans Automat Control* 2025; **70**: 2012–019.

- [14] Liu MX, Zhao CC, Deng RL, et al. False data injection attacks and the distributed countermeasure in DC microgrids. *IEEE Trans Control Network Syst* 2022; **9**: 1962–974.
- [15] Manandhar K, Cao X, Hu F, et al. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE Trans Control Network Syst* 2014; **1**: 370–79.
- [16] Wang X, Luo X, Zhang M, et al. Detection and isolation of false data injection attacks in smart grid via unknown input interval observer. *IEEE Internet Things J* 2020; **7**: 3214–229.
- [17] Ye D, Zhang TY. Summation detector for false data-injection attack in cyber-physical systems. *IEEE Trans Cybern* 2020; **50**: 2338–345.
- [18] Esmalifalak M, Liu L, Nguyen N, et al. Detecting stealthy false data injection using machine learning in smart grid. *IEEE Syst J* 2017; **11**: 1644–652.
- [19] Farajzadeh-Zanjani M, Hallaji E, Razavi-Far R, et al. Adversarial semi-supervised learning for diagnosing faults and attacks in power grids. *IEEE Trans Smart Grid* 2021; **12**: 3468–478.
- [20] Wang X, Luo X, Zhang M, et al. Detection and isolation of false data injection attacks in smart grid via unknown input interval observer. *IEEE Internet Things J* 2020; **7**: 3214–229.
- [21] Gallo AJ, Turan MS, Boem F, et al. A distributed cyber-attack detection scheme with application to DC microgrids. *IEEE Trans Automat Control* 2020; **65**: 3800–815.
- [22] Xu B, Peng C, Zhang Y, et al. Distributed plug-and-play robust \mathcal{L}_∞ voltage control for islanded microgrids. *IEEE Trans Smart Grid* 2024; **16**: 1790–800.
- [23] Trentelman HL, Stoorvogel AA, Hautus M, et al. *Control theory for linear systems*. London: Springer, 2012.
- [24] Taheri M, Khorasani K, Shames I, et al. Cyberattack and machine-induced fault detection and isolation methodologies for cyber-physical systems. *IEEE Trans Control Syst Technol* 2023; **32**: 502–17.
- [25] Tucci M, Meng L, Guerrero JM, et al. Stable current sharing and voltage balancing in DC microgrids: A consensus-based secondary control layer. *Automatica* 2018; **95**: 1–13.



Zhihua Wu received the M.Sc. degree in operations research and cybernetics from the University of Shanghai for Science and Technology, Shanghai, China, in 2023. He is currently pursuing his Ph.D. degree in Control Science and Engineering at Shanghai University, Shanghai, China. His research interests include distributed control systems and smart grids.



Chen Peng (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in coal preparation and the Ph.D. degree in control theory and control engineering from the Chinese University of Mining Technology, Xuzhou, China, in 1996, 1999, and 2002, respectively. From November 2004 to January 2005, he was a Research Associate with the University of Hong Kong. From July 2006 to August 2007, he was a Visiting Scholar with the Queensland University of Technology, Brisbane, QLD, Australia. From July 2011 to August 2012, he was a Postdoctoral Research Fellow with Central Queensland University, Rockhampton, QLD, Australia. In 2012, he was appointed as an Eastern Scholar with the Municipal Commission of Education, Shanghai, China, and joined Shanghai University, Shanghai. His current research interests include networked control systems, distributed control systems, smart grids, and intelligent control systems.



Engang Tian (Senior Member, IEEE) received the B.Sc. degree in mathematics from Shandong Normal University, Jinan, China, in 2002, the M.Sc. degree in operations research and cybernetics from Nanjing Normal University, Nanjing, China, in 2005, and the Ph.D. degree in control theory and control engineering from Donghua University, Shanghai, China, in 2008. From 2011 to 2012, he was a Postdoctoral Research Fellow with the Hong Kong Polytechnic University. From 2015 to 2016, he was a Visiting Scholar with the Department of Information Systems and Computing, Brunel University London, Uxbridge, U.K. From 2008 to 2018, he was an associate professor and then a professor with the School of Electrical and Automation Engineering, Nanjing Normal University. In 2018, he was appointed as an Eastern Scholar by the Municipal Commission of Education, Shanghai, China, and joined the University of Shanghai for Science and Technology, Shanghai, China. He is currently a professor with the School of Optical-Electrical and

Computer Engineering, University of Shanghai for Science and Technology, Shanghai. His research interests include networked control systems, as well as nonlinear stochastic control and filtering.



Yajian Zhang received the B.Sc. and M.Sc. degrees in electrical engineering from the China University of Mining and Technology in 2013 and 2016, respectively, and the Ph.D. degree in electrical engineering from Tianjin University, Tianjin, China, in 2021. He was a Postdoctoral Research Fellow in control theory and engineering with Shanghai University, Shanghai, China. Since 2024, he has been an associate professor at Shanghai University. His current research interests include secure networked control systems, power systems, cyber-physical systems, and power grid security control.