Cyber-Threat Detection for Distributed Control against FDIA in Energy System

Ziyang Wang
State Key Laboratory of
Internet of Things for Smart City
University of Macau
Macao, China
mc45428@um.edu.mo

Shaohua Yang*
State Key Laboratory of
Internet of Things for Smart City
University of Macau
Macao, China
shaohuayang@um.edu.mo

Hongxun Hui
State Key Laboratory of
Internet of Things for Smart City
University of Macau
Macao, China
hongxunhui@um.edu.mo

Ye Chen
State Grid Jiangsu Electric Power Company
Electric Power Research Institute
Nanjing, China
joey_chenye@foxmail.com

2025 4th International Conference on Power Systems and Electrical Technology (PSET) | 979-8-3315-3728-9/25/$31.00 ©2025 IEEE | DOI: 10.1109/PSET66242.2025.11296494

***Abstract*—Distributed control has been widely applied in fields such as energy and aviation sector, and with its advantage of aggregating resources to form autonomous regions, it has evolved into a critical control technology. However, its open communication architecture exposes the distributed control system to false data injection attacks (FDIA) through multiple paths, including communication links, sensors, and controllers, leading to potential system oscillations. Therefore, there is an urgent need to detect cyber-attacks from multiple paths. To address this issue, this paper first establishes a distributed control framework for energy system, with modeling of three types of attack paths. Consequently, a reconstruction-based method is presented to identify FDIA through time-frequency masking autoencoders (TFMAE) technology. Finally, the effectiveness of detection is validated by the case studies in a simulated distributed control system, demonstrating that the detector can detect dynamic FDIA events across multiple attack paths and achieve over 95.2% precision.**

***Index Terms*—energy system, distributed control, FDIA, attack paths, anomaly detection**

I. Introduction

As a critical infrastructure in modern society, energy system encompasses the entire process from energy production, conversion, transmission, and distribution, to consumption [1]. Within the energy system, energy regulation primarily employs centralized control and distributed control approaches. Traditional energy systems primarily rely on centralized control, where a central dispatch center coordinates all decisions and operations. This approach is well-suited for systems dominated by thermal power generation [2]. With the development of renewable energy and the emergence of smart energy system, traditional centralized control struggles to adapt to their decentralized and uncertain nature. Distributed control, in contrast, disperses control functions across individual energy resources and devices. This enables each resource to make autonomous decisions and perform control actions based on its local state and information, while simultaneously coordinating with other units. Consequently, distributed control has become an integral component of modern energy system [3].

The stability of energy system relies on secure control [4]. A compromise in the control system can lead to system instability or even collapse, resulting in widespread blackouts, significant economic losses, and threats to public safety. Control systems are frequent targets for cyber-attacks. For instance, beginning in March 2019, Venezuela experienced repeated nationwide power outages, affecting most of the 23 states in the country, and causing severe issues in healthcare, industrial, and transportation services [5]. On December 23, 2015, the power grid of two western regions in Ukraine was targeted by a cyber-attack. Hackers used BlackEnergy3 malware to remotely compromise the information systems of three Ukrainian energy distribution companies, temporarily interrupting power supply to consumers and leaving approximately 230,000 consumers without electricity for 1 to 6 hours [6]. These incidents highlight the importance of cyber security in energy control systems.

Among various threats to control system, false data injection attack (FDIA) is a typical form of cyber-attack that manipulates energy system state through designed erroneous data, thereby disrupting the control process [7]. Currently, many researchers are dedicated to designing distributed control methods to counter FDIA. A distributed pulse controller targeting random FDIA has been proposed [8] to address the mean-square bounded synchronization problem in multi-agent systems under attack. An FDIA-resilient distributed controller has been proposed [9], with its convergence in distributed control system has been proven using the Laplace transform

This work is funded in part by the State Key Laboratory of Power System Operation and Control (SKLD24KM11), the Science and Technology Development Fund, Macau SAR (File no. 001/2024/SKL and 0117/2022/A3), and the Chair Professor Research Grant of University of Macau (File no. CPG2025-00023-IOTSC), and the Guangdong Basic and Applied Basic Research Foundation (File no. 2023A1515110163). (Corresponding author: *Shaohua Yang*.)

and final value theorem. [10] deploy and integrate a One-class support vector machine-based anomaly detection device in relays to accurately distinguish genuine fault data from injected false data. A novel approach combining augmented Mahalanobis distance with calibration strategies is introduced [11] to enhance out-of-distribution detection performance for text-data in power system applications. A distributed adaptive compensator has been proposed [12] to enhance the H∞ control protocol and mitigate attacks on sensors and actuators. The aforementioned control methods have achieved satisfactory defensive effects.

However, the decentralized operation of distributed control system causes abnormal information to be hidden in the local data of individual energy resources, making it difficult to monitor. In addition, compared to centralized control, distributed control involves increased risk paths across resources [8] and complex interaction behaviors [12]. These characteristics enable potential cyber-attack to gradually expand their influence without being promptly detected, thereby weakening defensive effectiveness [13]. Therefore, establishing a distributed control anomaly detection mechanism to trigger defensive measures is necessary.

This paper comprehensively considers FDIA attacks occurring on communication links, sensors, and controllers in distributed control system, applying a detector based on Temporal-Frequency Masked Autoencoders [14] for FDIA detection to perceive occurring attack behaviors.

II. Multi-location FDIA targeting distributed control energy system

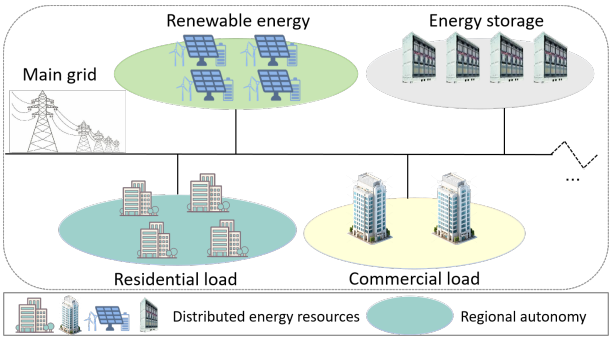

Fig. 1. Regional autonomy with distributed control

A. Distributed Control for Energy System

As shown in Fig. 1, modern energy system incorporates numerous flexible resources including solar power, wind power, energy storage system, and demand-side loads. Distributed control aggregates energy resources with similar characteristics to form autonomous regions. Within each region, local optimization of resource dispatch is achieved, thereby maximizing control fairness. Subsequently, these autonomous regions connect to the main grid to collaborate in achieving supply-demand balance.

The physical state of each energy resource participating in regulation (e.g., residential load) is obtained through data collection from the sensor. Each resource exchanges information with neighbors via a communication network. After collecting information, energy resources transmit it to the controller, which generates control signals through predefined distributed control strategies and regulates physical devices via actuators.

Based on the aforementioned energy resource coordination process, the following distributed control strategies were designed to coordinate local information and ultimately achieve global objectives:

$$\dot{\gamma}_i = s_i = -k_\gamma \sum_{j\in\mathcal{N}} a_{ij}(\gamma_i - \gamma_j) + c_i(\gamma_i - \gamma_{\text{ref}}) \tag{1}$$

where s_i represents the control input of the energy resource; γ_i represents the power state of resource i; k_γ indicates the coupling gain; $\mathcal{N}$ represents all neighbors of i; a_{ij} is an element of adjacency matrix based on the network topology, where $a_{ij} = 1$ indicates i and j are directly connected by a communication link, where $a_{ij} = 0$ indicates no communication link; γ_{ref} is the reference signal; c_i is the pinning gain, where $c_i = 0$ indicates that the node can't receive the reference signal, and $c_i = 1$ indicates that the node receives the reference signal.

For all the distributed resources in the same region, the corresponding matrix from the control protocol (1) can be shown as follows:

$$s = -k_\gamma (L + C)\gamma + k_\gamma \gamma_{\text{ref}} c \tag{2}$$

where $s = [s_1, s_2, \ldots, s_N]^T$ denotes the series of control input; L is the Laplacian matrix; C and c denote the pinning matrix and pinning vector; $\gamma = [\gamma_1, \gamma_2, \ldots, \gamma_N]^T$ denotes the power states of all resources.

B. FDIA on Distributed Control Via Different Paths

In distributed control system, FDIA achieves its goal of disrupting energy systems by injecting false data into distributed resources. As shown in Fig. 2, the control process involves multiple components, including communication links, sensor, and controller. FDIA can target these components through multiple attack paths, therefore it is necessary to model FDIA for each attack path as a prerequisite for cyber-attack detection.

Attack on communication links: Typically involves intercepting and tampering with information transmitted from neighboring nodes, making it a relatively easy attack path to implement. For nodes i and j, the FDIA for communication link $i-j$ can be modeled as:

$$\widehat{\gamma_j}(t) = \gamma_j(t) + \varepsilon_{ij}(t) \tag{3}$$

where ε_{ij} represents the injected value; $\widehat{\gamma_j}(t)$ represents the tampered information received by resource i from resource j.

Attack on sensor: this path of FDIA is achieved by tampering with measurement data. In this case, resources receive incorrect information about their status, which affects control decisions. This type of attack is modeled as follows:

$$\widehat{\gamma_i}(t) = \gamma_i(t) + \varepsilon_{ii}(t) \tag{4}$$

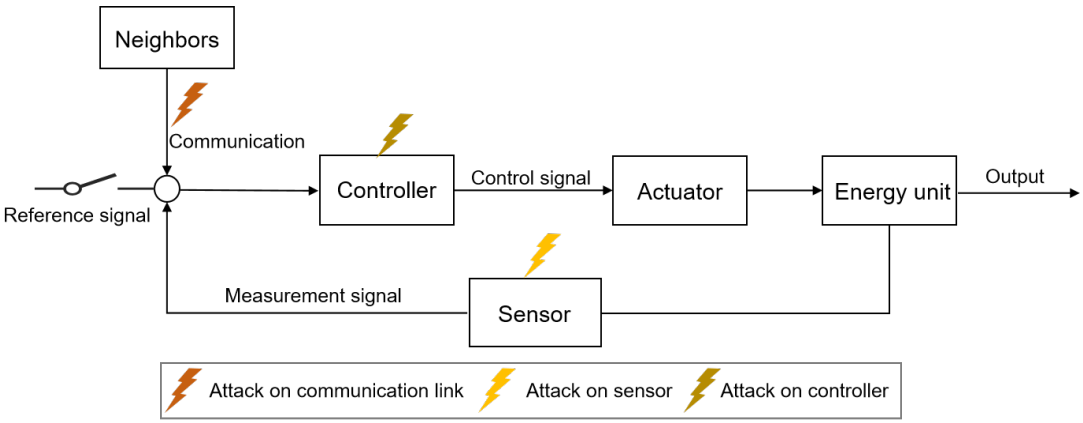

Fig. 2. Potential path for FDIA in energy resource

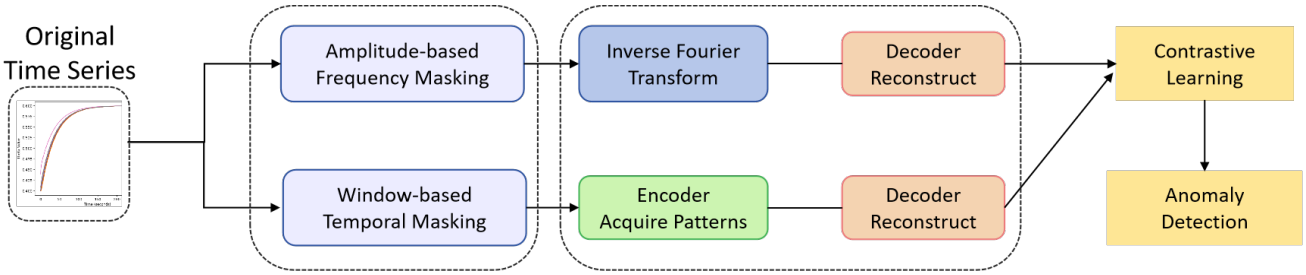

Fig. 3. The structure of TFMAE

where $\varepsilon_{ii}(t)$ represents the injected value in measurement data; $\gamma_i(t)$ is the original state of resource, while $\widehat{\gamma}_i(t)$ indicates the tampered state of resource i to participate in the control loop.

Attack on controller: this path of FDIA is achieved by tampering with the control signal from controller to actuator, misleading the control command directly. Under this type of FDIA, the compromised control can be expressed as:

$$\widehat{s}_i(t) = s_i(t) + \varepsilon_i(t) \tag{5}$$

where $s_i(t)$ is the original control input of resource i; $\varepsilon_i(t)$ is the inject value; $\widehat{s}_i(t)$ indicates the tampered control input will be sent to the actuator.

III. METHODS FOR FDIA DETECTION

In the field of time series analysis, anomaly detection is an important analytical tool that identifies abnormal parts of a sequence by analyzing whether the time series conforms to normal data distribution. In anomaly detection, reconstruction-based methods restore the complete time series from current inputs and detect anomalies by comparing the reconstructed time series with the actual series. This method applies to unsupervised learning using unlabeled training data and is suitable for detecting cyber-attack events due to the significant deviation from normal states when attacks occur. This paper applies the Temporal-Frequency Masked Autoencoder (TFMAE) [14] based on the reconstruction method to FDIA detection in distributed control of energy system.

TFMAE combines time masking and frequency masking strategies, using an autoencoder to extract normal pattern information from time series data. It identifies anomalies by comparing the differences between time-masked and frequency-masked representations. The overall structure of TFMAE is shown in Fig. 3. TFMAE mainly consists of the following three parts:

A. Temporal-Frequency Masking

For time domain masking, TFMAE employs variance coefficient analysis based on sliding window statistics to calculate data fluctuation characteristics within local time windows, masking observation values at time points with the largest fluctuation amplitudes. For frequency-domain masking, Fourier transform amplitude spectrum analysis is used to identify and mask frequency components with the weakest amplitudes. The complete time-domain signal is reconstructed via inverse Fourier transform, and the frequency domain embedding representation of the entire sequence is output.

B. Transformer-based Autoencoder

In a transformer-based [15] autoencoder, encoders and decoders have different functions depending on the input: the encoder receives unmasked time observations as input and learns the high-dimensional representation of the normal pattern in the time series, while the decoder is used for sequence reconstruction, including masked observations. In summary, the position-encoded input sequence S first passes through the self-attention layer, which can be expressed as:

$$\widetilde{S} = \text{softmax}\left(\frac{QK^{\top}}{\sqrt{d_k}}\right)V \tag{6}$$

where $\widetilde{S} \in R^{n\times d_v}$ is the output sequence matrix; $Q \in R^{n\times d_k}$, $K \in R^{n\times d_k}$, $V \in R^{n\times d_v}$ are the query, key, and value matrix, obtained from the input sequence S through linear projection [15]; d_k denotes the dimension of the key vector; d_v denotes the dimension of the value vector; $\text{softmax}(\cdot)$ is the activation function.

To ensure the stability and performance of the model, the attention mechanism undergoes the following transformation:

$$\hat{S} = LN\left(S + \widetilde{S}\right) \tag{7}$$

$$S_{\text{out}} = LN\left(\hat{S} + FFN\left(\hat{S}\right)\right) \tag{8}$$

where each layer undergoes a residual connection; $\text{LN}(\cdot)$ represents the layer normalization function; $\text{FFN}(\cdot)$ is a feed forward network consisting of two connected linear layers. $\hat{S}$ denotes the intermediate layer output obtained through residual connection. S_{out} denotes the output sequence, where the reconstructed sequence through the decoder for the frequency domain is denoted as $F \in R^{n\times D}$, and the reconstructed sequence through the decoder for the time domain is denoted as $T \in R^{n\times D}$.

C. Model Training and Anomaly Detection

Based on the sequence outputs in the frequency domain and time domain, the contrastive objective function of TFMAE is calculated as follows:

$$\Omega = D_{KL}(F,T) + D_{KL}(T,F) \tag{9}$$

where $D_{KL}(\cdot,\cdot)$ denotes the Kullback–Leibler divergence, used to measure the difference between the time domain and frequency domain representations. Similarly, for the observed sequence $\omega(t)$, the reconstructed outputs in the frequency domain and temporal domain are f and t, respectively, the anomaly score calculation in anomaly detection is as follows:

$$Score(\omega(t)) = D_{KL}(f,t) + D_{KL}(t,f) \tag{10}$$

Finally, given the threshold λ, the sequence is determined to be in an abnormal state based on the threshold, as shown below:

$$\hat{y} = \begin{cases} 1, & \text{Score}(\omega(t)) \geq \lambda \\ 0, & \text{Score}(\omega(t)) < \lambda \end{cases} \tag{11}$$

where $\hat{y} = 1$ indicates that the observed sequence is abnormal, and $\hat{y} = 0$ indicates that the observed sequence is normal.

IV. CASE STUDY

This study simulated a distributed control system comprising eight energy resources, as shown in Fig. 5, to evaluate TFMAE's capability in detecting FDIA events. According to previous research [14], [16], for data contextual anomalies caused by abnormal events, detecting anomalies achieves the purpose of perceiving events, because in reality people are more concerned with detecting events than anomalies at every moment.

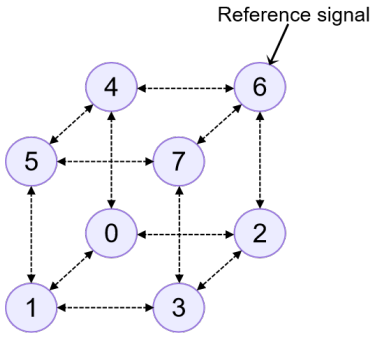

Fig. 4. The topology of test distributed system

For this simulation, 2400 data points were utilized as training data. The test set consists of three parts, each containing 300 data points, including normal and abnormal points, obtained from three different paths of dynamic FDIA event simulations. Based on the four cases mentioned above, the case study selects the same time period (t=0 to t=300) for comparison, as shown below:

Case 1: Normal operation without any FDIA events. In this case, all resources transition from a power state of 0.4 at t=0 to a regulated state with a target of 0.6. Under cyber-attack-free condition, the energy system can smoothly regulate its internal state to achieve precise regulation as shown in Fig. 5.

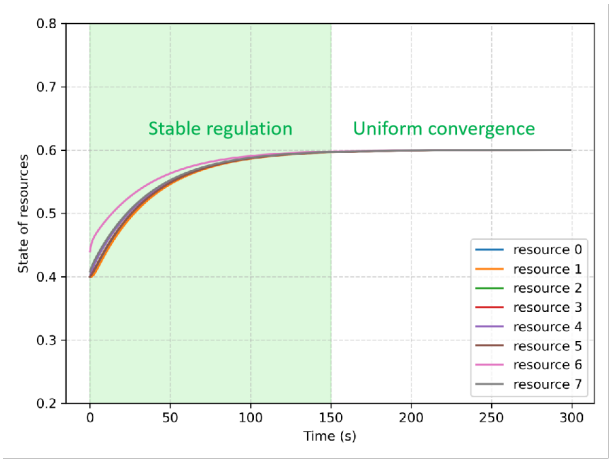

Fig. 5. Performance of distributed control without FDIA

Case 2: Anomaly operation under communication link attack. In this case, a 30-second communication attack from resource 4 to resource 0 is introduced at t=50, which can be expressed as:

$$\varepsilon_{04}(t) = 0.2\cos(t) \tag{12}$$

Case 3: Anomaly operation under sensor attack. In this case, a 30-second sensor attack to the sensor of resource 0

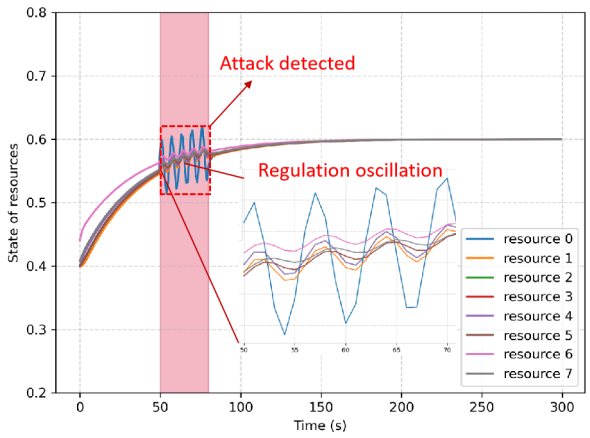

Fig. 6. Performance of control system and detector under communication attack

is introduced at t=50, which can be expressed as:

$$\varepsilon_{00}(t) = 0.2\cos(t) \tag{13}$$

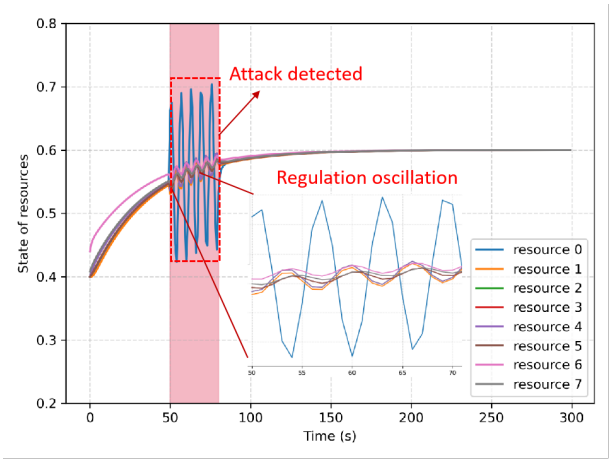

Fig. 7. Performance of control system and detector under sensor attack

Case 4: Anomaly operation under controller attack. In this case, a 30-second controller attack from controller to actuator of resource 0 is introduced at t=50, which can be expressed as:

$$\varepsilon_{0}(t) = 0.2\cos(t) \tag{14}$$

As shown in Fig. 6 to 8, dynamic attacks on resources trigger regulatory oscillations, causing the system to deviate from the convergence process. Among these, attacks on the controller cause the greatest degree of system oscillation, attacks on sensors cause the second greatest impact, and attacks on communication links cause the least impact.

Precision refers to the proportion of actual positive samples among the samples predicted as positive. Recall refers to the proportion of actual positive samples among the samples

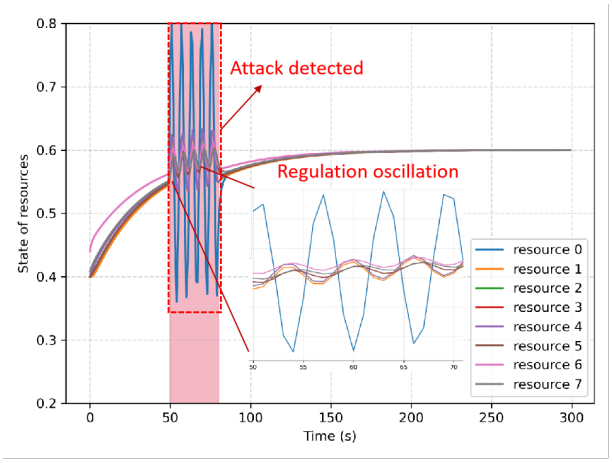

Fig. 8. Performance of control system and detector under controller attack

TABLE I
PERFORMANCE OF FDIA DETECTION IN CASES

Test Set	Metric		
	Precision	Recall	F1-score
Case2	0.952	1.000	0.976
Case3	0.976	1.000	0.988
Case4	0.985	1.000	0.992

predicted as positive, relative to the total number of positive samples in the dataset. The F1-score is the weighted average of precision and recall. As shown in Table 1, the recall indicates that TFMAE can detect attack events in all three cases. Additionally, the accuracy exceeds 95.2% for all three types of attacks, indicating that the detection model has a low false positive rate.

V. CONCLUSIONS

Cyber threats, especially FDIA, severely impact the control efficiency of distributed energy control systems and are urgent risk factors that need to be addressed. To address this challenge, we first analyzed the three attack paths of FDIA on energy resources and applied an anomaly detection framework based on TFMAE to detect FDIA. Simulation studies of dynamic attacks demonstrated that the detector achieved over 95.2% accuracy and 100% recall rate across all attack paths in the cases, with an F1 score exceeding 97.5%, confirming its ability to detect attack events while minimizing false positives. Additionally, the study found that controller attacks cause the most severe system oscillations, followed by sensor and communication link attacks, highlighting the need for path-specific protection mechanisms.

REFERENCES

[1] S. Pfenninger, A. Hawkes, and J. Keirstead, "Energy systems modeling for twenty-first century energy challenges," Renewable and sustainable energy reviews, vol. 33, pp.74-86, 2014.
[2] M. Khalid, "Smart grids and renewable energy systems: Perspectives and grid integration challenges," Energy Strategy Reviews, vol. 51, p. 101299, 2024.

[3] B.P. Koirala, E. Koliou, J. Friege, R.A. Hakvoort, and P.M. Herder, "Energetic communities for community energy: A review of key issues and trends shaping integrated community energy systems," Renewable and Sustainable Energy Reviews, vol. 56, pp. 722-744, 2016.
[4] D. Ding, Q. -L. Han, X. Ge and J. Wang, "Secure State Estimation and Control of Cyber-Physical Systems: A Survey," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 51, no. 1, pp. 176-190, 2021.
[5] J. Devanny, L. Goldoni, and B. Medeiro, "The 2019 Venezuelan Blackout and the consequences of cyber uncertainty," Revista Brasileira de Estudos de Defesa, vol. 7, no. 2, pp. 37-57, 2021.
[6] G. Liang, S. R. Weller, and J. Zhao, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," IEEE Transactions on Power Systems, vol. 32, no. 4, pp. 3317-3318, 2017.
[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," ACM Transactions on Information and System Security, vol. 14, no. 1, pp. 1-33, 2011.
[8] W. He, Z. Mo, Q.-L. Han, and F. Qian, "Secure impulsive synchronization in Lipschitz-type multi-agent systems subject to deception attacks," IEEE/CAA Journal of Automatica Sinica, vol. 7, no. 5, pp. 1326–1334, 2020.
[9] S. Yang, K. -W. Lao, Y. Chen and H. Hui, "Resilient Distributed Control Against False Data Injection Attacks for Demand Response," IEEE Transactions on Power Systems, vol. 39, no. 2, pp. 2837-2853, 2024.
[10] M. Elgamal, A. A. Eladl, B. E. Sedhom and A. Elmitwally, "Robust Overcurrent-Differential Agent-Based Relaying Scheme with a False Data Rejection Tool," Protection and Control of Modern Power Systems, vol. 10, no. 3, pp. 18-34, 2025.
[11] Y. Zhang, H. Wang, Y. Zheng, Z. Fei, H. Zhou and H. Luo, "Out-of-distribution detection for power system text data by enhanced mahalanobis distance with calibration," Protection and Control of Modern Power Systems, Early Access, 2025.
[12] H. Modares, B. Kiumarsi, and F. L. Lewis "Resilient and Robust Synchronization of Multiagent Systems Under Attacks on Sensors and Actuators," IEEE Transactions on Cybernetics, vol. 50, no. 3, pp. 1240-1250, 2020.
[13] M. Heidari Kapourchali, M. Sepehry and V. Aravinthan, "Fault Detector and Switch Placement in Cyber-Enabled Power Distribution Network," IEEE Transactions on Smart Grid, vol. 9, no. 2, pp. 980-992, 2018.
[14] Y. Fang, J. Xie, Y. Zhao, L. Chen, Y. Gao and K. Zheng, "Temporal-Frequency Masked Autoencoders for Time Series Anomaly Detection," 2024 IEEE 40th International Conference on Data Engineering (ICDE), Utrecht, Netherlands, 2024, pp. 1228-1241.
[15] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," Proceedings of NeurIPS, vol. 30, 2017.
[16] S. Tuli, G. Casale, and N. R. Jennings, "Tranad: deep transformer networks for anomaly detection in multivariate time series data," Proceedings of VLDB, pp. 1201–1214, 2022.