Cyberattack Aware Load Frequency Control in Power Systems

Shahriar Rahman Fahim[1], Rachad Atat[2], Cihat Kececi[1], Abdulrahman Takiddin[3],
Muhammad Ismail[4], Katherine R. Davis[1], and Erchin Serpedin[1]
[1]Electrical & Computer Engineering Department, Texas A&M University, College Station, TX 77843, USA;
[2]Department of Computer Science & Mathematics, Lebanese American University, Beirut, Lebanon;
[3]Department of Electrical & Computer Engineering, Florida State University, Tallahassee, FL 32310, USA;
[4]Department of Cybersecurity Education, Research and Outreach Center,
Tennessee Tech University, Cookeville, TN 38505 USA
Email: sr-fahim@tamu.edu; rachad.rachad.atat@lau.edu.lb; kececi@tamu.edu; a.takiddin@fsu.edu;
mismail@tntech.edu; katedavis@tamu.edu; eserpedin@tamu.edu

***Abstract*—The load frequency control (LFC) is crucial for stabilizing the frequency of the power grid in the intermittency of renewable energy sources. Modern LFC systems utilize open communication and automation networks that expose power systems to potential cyberattacks, which could lead to frequency instability throughout the network. Current research often treats frequency control and cybersecurity independently, which could lead to ineffective solutions and increased system instability. This paper introduces a cyber-resilient LFC strategy that improves both control performance and security. We employ reinforcement learning for adaptive frequency control and integrate it with a graph convolutional neural network to enhance control responses during a cyberattack event. Our strategy also includes a graph autoencoder-based attack detector that is trained in various scenarios and has shown more than 92% in detection rate while tested on the Iberian power system topology, which includes 486 buses. This highlights the robustness and reliability of our approach in ensuring resilience against cyberattacks within the realm of frequency control in power systems.**

***Index Terms*—Cybersecurity, false data injection attacks, frequency control, graph autoencoder, graph neural network, reinforcement learning, renewable energy sources,**

I. Introduction

The high penetration of renewable energy sources in power systems introduces significant variability and uncertainty in power generation [1]. Unfortunately, the intermittent nature of renewable sources and their rapid power fluctuations can lead to frequency deviations, thereby posing a risk to the stability and reliability of the power system. Moreover, the integration of advanced automation and communication technologies makes the modern power system more susceptible to different cyberattacks. Nevertheless, during a cyberattack, the disturbances rapidly take a cyber-physical form and compromise the normal operation of the system.

Within the context of load frequency control (LFC) systems, attackers tamper with sensor measurements to disrupt the system operation. In false data injection attacks (FDIAs), hackers can falsify power measurements by making them appear higher (i.e., additive attacks), lower (i.e., deductive attacks), or a combination of both (i.e., camouflage attacks). Thus, overlooking the potential impact of FDIAs can lead to unauthorized manipulation of the LFC system.

A. Related Works

Existing literature on cyberattacks and LFC in power systems has predominantly addressed these two aspects separately. In the case of LFC, proportional–integral–derivative (PID) controllers have been widely adopted due to their simple control structures [2]. However, these controllers do not support dynamic information sharing or adaptation to changing conditions. Recently, significant attention has been given to reinforcement learning (RL)-based LFCs, which adapt to varying grid conditions [3]. However, such approaches fail to account for cyber threats that can lead to frequency instability and struggle to respond effectively to sudden changes in demand.

The domain of cybersecurity in critical infrastructure, particularly power systems, has undergone a profound transformation in detection methodologies over the past decade, reflecting the escalating sophistication of cyber threats. Early research predominantly relied on signature-based and rule-based approaches, which demonstrated significant limitations in addressing the increasingly complex landscape of FDIAs [4], [5]. These initial strategies, while foundational, proved inadequate in detecting novel attack vectors that deviated from predefined patterns, prompting a paradigm shift toward more adaptive detection mechanisms. Statistical and machine learning techniques that introduced more nuanced anomaly detection frameworks, capable of identifying subtle deviations in system behaviors overlooked by traditional methods, were pioneered in [6] and [7].

The subsequent emergence of deep learning architectures marked a revolutionary phase in cybersecurity research, with authors in [8], [9] developing hybrid computational intelligence frameworks that demonstrated unprecedented detection accuracy rates exceeding 95%. These advanced models leveraged complex neural network architectures, including convolutional and recurrent neural networks, to process multidimensional power system data with remarkable precision. Despite these advancements, persistent challenges remain, including minimizing false positive rates, developing real-time detection capabilities, and creating adaptive learning systems that can comprehend the intricate dynamics of power infrastructure. References [10]–[12] emphasize the critical need for

interdisciplinary approaches that synergize advanced machine learning algorithms, domain-specific expertise, and contextual understanding of system vulnerabilities. The evolving research trajectory suggests a future where cyberattack detection transitions from reactive strategies to proactive, anticipatory frameworks capable of mitigating threats before they manifest, ensuring the resilience and reliability of critical energy infrastructure [13], [14].

We employ reinforcement learning for adaptive frequency control and integrate it with a graph convolutional neural network to enhance control responses during a cyberattack event. Our strategy also includes a graph autoencoder-based attack detector that is trained in various scenarios and has shown more than 92% in detection rate while tested on the Iberian power system topology, which includes 486 buses.

B. Contributions

In light of the aforementioned limitations in existing works, we propose a cyber-resilient LFC strategy that improves both control performance and security. Specifically, the contributions of this paper are summarized as follows.

- We develop a state–action–reward–state–action (SARSA)-based data-driven LFC method to minimize frequency deviations considering power system constraints.
- We develop a graph convolutional neural network (GCNN) model that predicts future load demands to improve the LFC responsiveness to cyberattacks.
- We develop a graph autoencoder (GAE)-based detector with Chebyshev filters to capture temporal and spatial grid data to enhance the FDIA detection.

This paper is organized as follows. Section II describes the frequency control problem formulation. Section III introduces the system modeling along with the data preparation. Section IV introduces the proposed cyber-resilient LFC strategy. Section V analyzes the performance of the proposed model against various attack types. Conclusions are drawn in Section VI.

II. Frequency Control Problem Formulation

The network buses, $\mathcal{N}$, are categorized into generator buses ($\mathcal{N}_G$) and load buses ($\mathcal{N}_L$). Generator buses follow dynamic differential equations, while load buses, which include frequency-sensitive loads, are governed by algebraic equations. For each bus, the dynamics of the voltage angle, η_i, and the frequency deviation, κ_i, from the nominal frequency, f_0, are determined by the net power input, P_i, as follows:

$$\dot{\eta i} = 2\pi f_0 \kappa_i, \forall i \in \mathcal{N} \quad \text{(1a)}$$

$$-\gamma_i \kappa_i - \sum_{j=1}^{n} v_i v_j B_{ij} \sin(\eta_i - \eta_j) + P_i + \rho_i = h_i \dot{\kappa i}, \forall i \in \mathcal{N}_G \quad \text{(1b)}$$

$$-\gamma_i \kappa_i - \sum_{j=1}^{n} v_i v_j Bij \sin(\eta_i - \eta_j) + P_i + \rho_i = 0, \forall i \in \mathcal{N}_L \quad \text{(1c)}$$

Here, $h_i = 2H_i > 0$ represents the inertia constant of generator i, γ_i is the frequency sensitivity coefficient (varies by bus type), v_i and B_{ij} are the voltage magnitude and susceptance at buses i and j, and ρ_i denotes the controllable power injection used for frequency regulation.

The primary goal of frequency control is to maintain the system frequency close to its nominal value, ensuring stability. From the analysis in [15], [16], the equilibrium frequency deviation in the system is expressed as:

$$\boldsymbol{\kappa} = \frac{\sum_{i=1}^{n} P_i + \sum_{i=1}^{n} \rho_i}{\sum_{i=1}^{n} \gamma_i}, \quad (2)$$

where κ represents the target frequency deviation, and ρ_i is the required value of controllable power injections to achieve the desired frequency control. As shown in Eq. (2), without active frequency control, any disturbance in power, P_i, will result in a non-zero frequency deviation ($\kappa \neq 0$). A zero frequency deviation ($\kappa = 0$) is only achievable when the sum of power disturbances and the optimal controllable power injections, $\boldsymbol{\rho}$, balance to zero. In this study, we implement power injections through two methods, namely, adjusting generator outputs to match system demand and utilizing energy storage systems, where renewable energy is stored and later released through battery storage systems to help maintain frequency control.

III. System Modeling

A. Power System Modeling

We represent the power graph via the triplet $\mathcal{G} = (\mathcal{N}, \mathcal{E}, \boldsymbol{W})$. Each node in the set $\mathcal{N}$ represents a bus, and the set of edges $\mathcal{E}$ denotes the lines interconnecting these buses, enabling power flow. The adjacency matrix $\boldsymbol{W} \in \mathbb{R}^{|\mathcal{N}| \times |\mathcal{N}|}$ models the weighted relationships between buses, with entry $\boldsymbol{W}_{ij}$ denoting the weight associated to the edge $e = (i, j)$ [17]. A graph representation of the considered system is presented in Fig. 1. In modeling the Iberian power system, we utilized a 486-bus representation to capture the network's complexity and operational characteristics accurately. This level of granularity allows for detailed analysis of power flows, voltage levels, and system stability. The undirected representation of the power system reflects the bidirectional nature of power flow in transmission lines, where electricity can flow in either direction depending on system conditions.

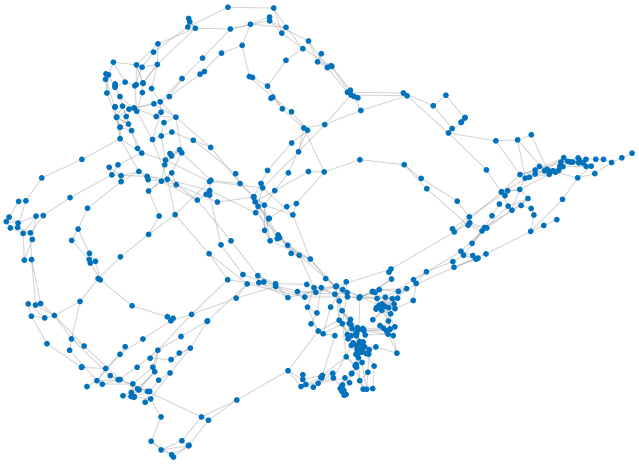

Fig. 1. Graph representation of the Iberian power system.

B. Threat Modeling

In the context of FDIAs in LFC systems, attackers target the power input variable, P, to introduce errors in power levels. These manipulations deceive the controller into adjusting the control signal, u^*, to counteract a disturbance perceived based on the falsified data. While the system appears to achieve zero frequency deviation, an actual deviation persists undetected. Over time, this concealed frequency deviation increases operational stress on the power grid, reducing efficiency and increasing the likelihood of unexpected system failures.

During an attack scenario, the equilibrium frequency deviation, as given by Eq. (2), is altered to the following expression:

$$\boldsymbol{\kappa}^*_{\text{false}} = \frac{\sum i = 1^n P_{\text{false},i} + \sum_{i=1}^{n} \rho_i^*}{\sum_{i=1}^{n} \gamma_i}, \tag{3}$$

where $P_{\text{false},i}$ denotes the falsified measurement of the actual power input P_i. This falsification leads to incorrect calculations, distorting the system's control dynamics. Next, we discuss three distinct types of manipulations on P_i to assess their impacts on the LFC system.

Let the field-measured power at bus i and timestamp t be denoted as P_i^t and the true power measurement as $P^t_{\text{true},i}$. Under normal conditions, the true power $P^t_{\text{true},i}$ should match the measured power at the control end $P^t_{\text{m},i}$, such that $V^t_{\text{true},i} = V^t_{\text{m},i}$. However, during the considered attack scenarios, these measurements are manipulated by the attackers using additive, deductive, and camouflage attack strategies. The manipulated power measurements are expressed as:

$$P^t_{\text{false},i} = P^t_{\text{true},i} + b_i \cdot \delta P_i^t, \quad b_i = \begin{cases} +1, & \text{if } i \in A_a, \\ -1, & \text{if } i \in A_d, \\ \pm 1, & \text{if } i \in A_c. \end{cases}$$

where $P^t_{\text{true},i}$ denotes the true power measurement at bus i at time t, δP_i^t represents the falsified data injected by attackers at bus i, and b_i is a variable representing the type of attack at bus i. Buses are grouped into three sets, A_a for additive attacks, A_d for deductive attacks, and A_c for camouflage attacks. During additive attacks ($i \in A_a$), power measurements are falsely increased, creating the illusion of higher demand. For deductive attacks ($i \in A_d$), power measurements are falsely decreased, leading to an underestimation of demand. For camouflage attacks ($i \in A_c$), the total number of attacked buses equals the number in either the additive or deductive sets, but buses are randomly assigned to additive ($b_i = +1$) or deductive ($b_i = -1$) categories. This randomization results in some areas experiencing over-generation and others facing under-generation, effectively masking the attack pattern and increasing detection complexity. This formulation provides a consistent and unified representation of diverse attack scenarios, enabling detailed analysis and the development of robust mitigation strategies.

Moreover, we consider two type of attack strategies, namely, random node attacks (RNAs) and vulnerable node attacks (VNAs). In RNAs, the attacker randomly selects buses in the power grid. These nodes are then manipulated by injecting falsified data into their power measurements. The goal of RNAs is to disrupt the system's operation generically. On the other hand, in VNAs, the attacker specifically targets nodes that are identified as critical or vulnerable within the power system. These vulnerable nodes are determined by analyzing various electrical and topological metrics, as discussed in [18]. By focusing on vulnerable nodes, the attacker can maximize the impact of the attack, potentially causing widespread disruptions.

C. Data Preparation

The dataset used in this study models the Iberian power system [19], comprising 486 buses and associated transmission lines, providing a detailed topology of the grid spanning Spain and Portugal. It includes active and reactive power flows as node features. Node features include active and reactive power injections, capturing the operational state of each bus. Power flow calculations were performed using MATLAB, employing the Newton-Raphson method, a robust iterative algorithm for solving nonlinear equations. The process begins with an initial guess for bus voltages and iteratively calculates mismatches in active and reactive power injections based on the grid's admittance matrix and bus data. Voltage magnitudes and angles are updated at each iteration to minimize these mismatches. Convergence is achieved when the power mismatches fall below a predefined tolerance, ensuring numerical stability. The algorithm accounts for both PQ buses (loads with specified active and reactive power) and PV buses (generators with specified active power and voltage magnitude), while maintaining slack buses to balance the overall system power. Moreover, active and reactive power flows are normalized to ensure compatibility with machine learning models and to avoid scale imbalances. Additionally, the dataset includes the system's admittance matrix, generator data, and load data, which are essential for reproducing the grid's behavior and ensuring the physical accuracy of simulations. The dataset is split into three subsets to ensure a balanced evaluation, where 70% of the data is used for training the model, 15% is allocated for validation to fine-tune the parameters, and the remaining 15% is reserved for testing to assess the model's generalization performance.

IV. Proposed Methodology

A. SARSA RL-based LFC

The considered LFC system consists of generators, renewable energy sources, battery storage systems, and loads. The proposed controller is designed as a policy network with the goal of maintaining the local frequency as close as possible to the nominal value by fine-tuning generator output and engaging the energy storage systems. At each step, the algorithm observes a state, selects an action based on the policy, and receives a reward from the environment. The action taken at a time-step influences the environment, which leads to a transition to a new state. The reward is calculated as:

$$\mathcal{R} = e^{-|\kappa^*|}, \tag{4}$$

where k^* is the frequency deviation from the nominal value.

The proposed reinforcement learning framework implements a novel Q-learning update strategy tailored to power system dynamic control. The value function evolution is

characterized by an update rule that captures the nature of power system interactions:

$$\mathcal{Q}\left(\mathcal{S}_t, \mathcal{A}_t\right) \leftarrow \mathcal{Q}\left(\mathcal{S}_t, \mathcal{A}_t\right) + \eta\left[\mathcal{R}_t + \varrho \mathcal{Q}\left(\mathcal{S}_{t+1}, \mathcal{A}_{t+1}\right) - \mathcal{Q}\left(\mathcal{S}_t, \mathcal{A}_t\right)\right], \quad (5)$$

where $\mathcal{Q}\left(\mathcal{S}_t, \mathcal{A}_t\right)$ represents the state-action value function, η denotes the adaptive learning rate, and ϱ represents the discount factor of the model.

By iteratively applying the update rule, the agent engages with the environment, leading to the convergence of the policy that maximizes cumulative rewards to a value of 1. This process effectively stabilizes the power system frequency, even under fluctuating demand and generation conditions. In the proposed control framework, an LFC controller is assigned to each conventional generator in the power system. The proportional contribution of each generator is determined by dividing its capacity by the total capacity of all generators in the system. This ratio represents the precise amount of power each generator supplies to meet the grid's demand. Importantly, distributed generators (DGs) are not directly associated with individual conventional generators. Instead, they contribute power to the grid as a whole. The total power generated by DGs is allocated among the conventional generators based on their respective proportional shares. This methodology ensures an equitable and systematic distribution of renewable energy across the grid while maintaining frequency stability. By targeting frequency control at the individual generator level, the collective action stabilizes the overall frequency of the power system.

B. GAE-Based Cyberattack Detection

Our goal is to develop a model that distinguishes between power system states with and without cyberattacks. The input sample $\boldsymbol{X}$ consists of time-series measurements of active and reactive power values $[\boldsymbol{P}_t, \boldsymbol{Q}_t] \in \mathbb{R}^{|\mathcal{N}|\times 2}$ at t timestamp. The input data is processed through graph encoder layer l_E, latent layer l_H, and graph decoder layer l_D. The objective function of the GAE-based detector is defined as

$$\min_{\{\boldsymbol{\xi}\}} \beta\left(\boldsymbol{X}, f_D\left(f_E(\boldsymbol{X})\right)\right), \quad (6)$$

where $E_G = f_E(\boldsymbol{X})$ and $D_G = f_D(\boldsymbol{X})$ represent the graph encoder and decoder function, respectively, and $\boldsymbol{\xi}$ denotes the set of training parameters. The cost function $\beta(\cdot)$ represents the mean squared error and quantifies the difference between $\boldsymbol{X}$ and the output of the composed functions $f_D\left(f_E(\boldsymbol{X})\right)$.

C. Cyberattack Aware Control Strategy

The increasing vulnerability of power systems to cyberattacks necessitates innovative defense mechanisms in LFC architectures. Current LFC systems typically rely on real-time demand measurements as critical state variables, rendering them susceptible to FDIAs. To counteract this vulnerability, the proposed approach introduces a dynamic data protection strategy that employs sophisticated GAE-based techniques to detect potential cyber intrusions. When an attack is identified, the system autonomously transitions from compromised current measurements to pre-computed demand predictions generated using GCNN. This adaptive mechanism ensures continuous frequency control by replacing potentially manipulated real-time data with reliable predictive models, thereby maintaining system reliability and operational integrity under adverse cyber threat conditions. The reinforcement learning-based algorithm iteratively refines its decision-making process, utilizing an ϵ-greedy policy to select optimal actions and minimize frequency deviations, ultimately providing a robust defense against sophisticated cyberattacks in critical power infrastructure. The pseudocode algorithm highlighting the steps within the cyberattack-aware LFC scheme is depicted in Algorithm 1.

Algorithm 1 Cyber-attack aware frequency control algorithm

Input: learning rate $\mathcal{L}$, discount factor $\mathfrak{s}$, exploration rate λ, number of episodes υ, threshold for the frequency deviation ϑ, predicted demand sequence D_P^t, binary output from the cyber-attack detection model ϕ.

Initialize: $\mathcal{Q}(\mathcal{S}, \mathcal{A})$ for all action value pairs; initial state $\mathcal{S}^0 = [D^0, G_C^0, G_{DG}^0, \kappa^{*,0}]$.

Procedure: Read binary output from the cyber attack detection model. ϕ =*1* during an attack and *0* otherwise.

```
if ϕ=1 do
    set D^t ← D_P^t
else do
    loop (for each episode)
        initialize S^t and A^t
        loop (for each step of episode)
            do take action A^t and observe R, S^{t+1}
            choose A^{t+1} based on S^{t+1} using ε-
            greedy policy algorithm
            update Q(S, A) using the formulation in (13)
            S^t ← S^{t+1}   \\ transition to next state
            A^t ← A^{t+1}
            if κ^{*,t} < |ϑ|
                break
            else
                Repeat
        end loop
    end loop
```

V. Performance Assessment

Table I highlights the model's performance under additive, deductive, and camouflage attacks, evaluated using metrics including detection rate (DR), false alarm rate (FAR), and accuracy (ACC) for the RNA and VNA cases. On average, the model achieves better performance in RNA scenarios, with an average DR of 96.12%, FAR of 10.26%, and ACC of 94.03%, compared to VNA scenarios, where the average DR is 92.34%, FAR is 14.28%, and ACC is 91.19%. Additive and deductive attacks exhibit consistently higher DR and ACC with lower FAR, as these attacks involve uniform manipulations that are easier to detect. In contrast, camouflage attacks, which mix additive and deductive manipulations, pose greater challenges due to their complexity, resulting in lower DR (i.e., 94.98% in RNA and 91.25% in VNA) and ACC (e.g., 90.28% in RNA and 88.08% in VNA), and higher FAR (e.g., 17.68% in RNA and 21.66% in VNA). The model's better performance in RNA scenarios can be attributed to the random distribution of attacks, whereas VNA targets critical nodes, making manipulations harder to detect.

The frequency control performance against additive attack is shown in Fig. 2 while comparing it with the PID con-

troller. Initially, the PID controller exhibits some fluctuations while the proposed controller demonstrates stable initiation with minimal fluctuation. The proposed controller initiates tracking of backup future load prediction data, which remains unaffected by the attack. Conversely, the PID controller starts to track falsified nominal frequency levels. This misguided response is due to its reliance on immediate input data without contextual or predictive insight that the proposed controller offers.

TABLE I. Performance of proposed model against different types of attacks and attack injection levels.

Attack type	Metric	Attack data percentage			
		RNA		VNA	
		5%	10%	5%	10%
Additive	DR	98.19	95.38	93.41	92.60
	FAR	5.92	8.87	9.93	11.95
	ACC	97.79	94.72	92.62	91.59
Deductive	DR	97.20	94.42	92.35	91.57
	FAR	7.19	10.21	11.25	13.18
	ACC	96.03	92.95	92.86	90.79
Camouflage	DR	94.98	93.25	91.25	88.47
	FAR	17.68	20.65	21.66	23.54
	ACC	90.28	88.98	88.08	87.08

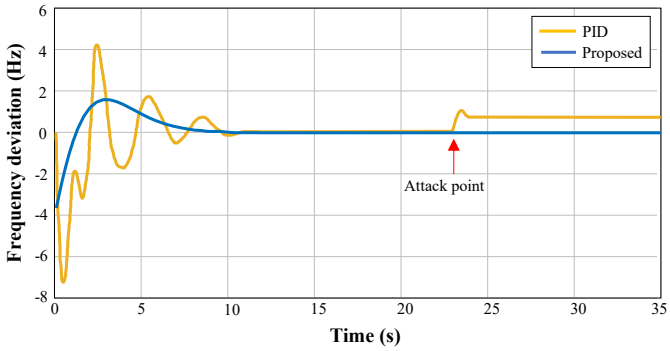

Fig. 2. Actual frequency deviation curve during additive attacks.

VI. CONCLUSIONS

This paper presented a cyber-resilient LFC strategy that exhibits superior performance against cyberattacks compared to benchmark controllers. The proposed model integrates load prediction that enhances frequency control by anticipating demand fluctuations. Specifically, we employ reinforcement learning for adaptive frequency control and integrate it with a graph convolutional neural network to enhance control responses during cyberattacks. We also employ a graph autoencoder that facilitates precise attack detection by leveraging Chebyshev filters, which efficiently capture both local and global topological patterns in the power system. These filters enable the model to aggregate operational data across the nodes while maintaining computational efficiency. The forthcoming paper will detail the implementation of SARSA reinforcement learning for LFC, alongside extensive results on control performance and future load prediction. Additionally, it will provide a comprehensive analysis of the attack detection mechanism. Future research will enhance system adaptability across various network configurations and increase its resilience against diverse threats.

ACKNOWLEDGMENT

This work is supported by NSF EPCN Awards 2220346 and 2220347.

REFERENCES

[1] Y. Liu, Y. Li, Y. Wang, X. Zhang, H. B. Gooi, and H. Xin, "Robust and resilient distributed optimal frequency control for microgrids against cyber attacks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 1, pp. 375–386, 2021.

[2] A. Kumar and S. Pan, "Design of fractional order pid controller for load frequency control system with communication delay," *ISA transactions*, vol. 129, pp. 138–149, 2022.

[3] F. Yang, D. Huang, D. Li, S. Lin, S. M. Muyeen, and H. Zhai, "Data-driven load frequency control based on multi-agent reinforcement learning with attention mechanism," *IEEE Transactions on Power Systems*, vol. 38, no. 6, pp. 5560–5569, 2023.

[4] Q. Wang, X. Cai, Y. Tang, and M. Ni, "Methods of cyber-attack identification for power systems based on bilateral cyber-physical information," *International Journal of Electrical Power & Energy Systems*, vol. 125, p. 106515, 2021.

[5] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 865–873, 2011.

[6] M. Zhang, C. Shen, N. He, S. Han, Q. Li, Q. Wang, and X. Guan, "False data injection attacks against smart gird state estimation: Construction, detection and defense," *Science China Technological Sciences*, vol. 62, no. 12, pp. 2077–2087, 2019.

[7] J. Hao, E. Kang, J. Sun, Z. Wang, Z. Meng, X. Li, and Z. Ming, "An adaptive markov strategy for defending smart grid false data injection from malicious attackers," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2398–2408, 2016.

[8] D. Xue, X. Jing, and H. Liu, "Detection of false data injection attacks in smart grid utilizing elm-based ocon framework," *IEEE Access*, vol. 7, pp. 31 762–31 773, 2019.

[9] Y. Wang, Z. Zhang, J. Ma, and Q. Jin, "Kfrnn: An effective false data injection attack detection in smart grid based on kalman filter and recurrent neural network," *IEEE Internet of Things Journal*, vol. 9, no. 9, pp. 6893–6904, 2021.

[10] Y. Li and Y. Wang, "False data injection attacks with incomplete network topology information in smart grid," *IEEE Access*, vol. 7, pp. 3656–3664, 2018.

[11] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 623–634, 2021.

[12] R. Zheng, J. Gu, Z. Jin, H. Peng, and Y. Zhu, "Load forecasting under data corruption based on anomaly detection and combined robust regression," *International Transactions on Electrical Energy Systems*, vol. 30, no. 7, p. e12103, 2020.

[13] S. Wang, S. Bi, and Y.-J. A. Zhang, "Locational detection of the false data injection attack in a smart grid: A multilabel classification approach," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8218–8227, 2020.

[14] G. Zhang, J. Li, O. Bamisile, D. Cai, W. Hu, and Q. Huang, "Spatio-temporal correlation-based false data injection attack detection using deep convolutional neural network," *IEEE Transactions on Smart Grid*, vol. 13, no. 1, pp. 750–761, 2022.

[15] E. Weitenberg, Y. Jiang, C. Zhao, E. Mallada, C. De Persis, and F. Dörfler, "Robust decentralized secondary frequency control in power systems: Merits and tradeoffs," *IEEE Transactions on Automatic Control*, vol. 64, no. 10, pp. 3967–3982, 2019.

[16] E. Weitenberg, C. De Persis, and N. Monshizadeh, "Exponential convergence under distributed averaging integral frequency control," *Automatica*, vol. 98, pp. 103–113, 2018.

[17] A. Takiddin, M. Ismail, R. Atat, and E. Serpedin, "Spatio-temporal graph-based generation and detection of adversarial false data injection evasion attacks in smart grids," *IEEE Transactions on Artificial Intelligence*, pp. 1–15, 2024.

[18] R. Atat, M. Ismail, and E. Serpedin, "Limiting the failure impact of interdependent power-communication networks via optimal partitioning," *IEEE Trans. on Smart Grid*, vol. 14, no. 1, pp. 732–745, 2022.

[19] P. M. Bento, S. J. Mariano, J. A. Pombo, and M. R. Calado, "Large-scale penetration of renewables in the iberian power system: Evolution, challenges and flexibility options," *Renewable and Sustainable Energy Reviews*, vol. 204, p. 114794, 2024.