Enhancing Cyber-Resilience of Automatic Generation Control through Moving Target Defense

Sayemul Islam*, Mohammad Zakaria Haider*, Mucun Sun†, and Mohammad Ashiqur Rahman*
*Analytics for Cyber Defense (ACyD) Lab, Florida International University, USA
†Energy Systems, Idaho National Laboratory, USA
Emails: {sisla055, mhaid010, marahman}@fiu.edu, mucun.sun@inl.gov

***Abstract*—False data injection (FDI) attacks on automatic generation control (AGC) infrastructures covertly manipulate frequency measurements, which can mislead the control loop and disrupt the system's normal operation. The falsified measurements propagate through power system dynamics, causing inter-area power oscillations, rotor angle divergence, frequency oscillations, and voltage instability. In this paper, we demonstrate that the moving target defense (MTD) strategy offers superior capability in detecting stealthy FDI attacks in state estimation compared to systems operating without MTD under similar attack conditions. To achieve this, this paper presents a unified cyber–physical framework that integrates the IEEE-39 bus system with a linearized AC state estimation-based bad data detection (BDD) technique and MTD in reference power setpoint. Traditional BDD can not accurately detect stealthy FDI attacks because the attacker knows the system dynamics and will carefully inject corrupted data that mimics system measurements. However, the attacker's lack of awareness of the controlled MTD in specific generators increases the model-measurement inconsistency and enhances the probability of attack detection, which is 32.7% in this study. MTD in reference power setpoint as controlled randomization provides a proactive defense mechanism against stealthy attacks applied to certain measurements.**

***Index Terms*—power grid, false data injection attack, moving target defense, bad data detection, state estimation**

I. Introduction

The large-scale evaluation of electric power grid from conventional control paradigms to digital and interconnected modern power grids increases structural and operational complexity [1], [2]. Consequently, modern power grids increasingly rely on automatic generation control (AGC), which coordinates distributed generator units and maintains system stability under varying generation and load conditions. AGC, acting as a secondary controller, maintains frequency and tie-line power balance between interconnected areas and ensures a secure and reliable grid operation [3], [4]. However, the cyber-physical coupling in the control loop exposes attack surfaces where attackers can exploit communication or data vulnerabilities, causing the system to deviate from its normal operating conditions. Consequently, maintaining data integrity in the secondary controller has therefore become a critical prerequisite for resilient grid performance [5]. As the scale of structural and operational complexity grows, even small data inconsistencies can spread throughout the network and intensify the impact of cyber intrusions [6].

Recent incidents have been observed as the impact of cyber-attacks that disrupt power system stability. For example, the 2022 Turkey blackout affected more than 40 provinces in Turkey due to a cyberattack on supervisory control and data acquisition (SCADA) infrastructures, causing national instability [1]. In [2], the attacker executed "SCADA hijacking" and "SCADA blackout" attacks by exploiting vulnerabilities in the communication protocols and shut down power generator units. These incidents indicate that modern grid operations face not only conventional reliability issues but also advanced cyber attacks. The coordination of AGC and AVR in WAC system facilitates SCADA to focus on enhancing system dynamics under load disturbances and communications delays. AGC adjusts reference power output based on area control error (ACE) due to frequency and tie-line power deviations. Both controllers rely on real-time data measurement in the power system dynamics. Ref. [3] and [4] provide a comprehensive analysis, including fractional-order, neural, and intelligent optimization-based AGC under load variations and renewable integration. As the SCADA network relies on protocols such as Modbus, DNP3, and IEC 60870, which can be corrupted, AGC and AVR control loop monitors every control signal entering the loop to prevent uncoordinated control actions [5]. These insights emphasize developing an integrated cyber-physical defense framework for the reliability, security, and continuity of the modern power grid.

Our study focuses on observing how stealthy FDI attacks affect AGC behavior and integrates through the generator dynamics and turbine–governor models. The main contributions of the work can be summarized as follows:

- We develop a simulation environment that linearizes state estimation with the IEEE-39 bus system and captures how false data propagates through the cyber domain, influencing the generator's mechanical and electrical behavior.
- We propose an MTD strategy that perturbs the reference power setpoint by controlled randomization into the specific generator channels. The objective is to make the system unpredictable to an attacker attempting to remain undetected.
- FDI attacks under an active MTD scenario enhance the attack detection capability compared to FDI attacks without MTD scenario under multiple attack windows and operating conditions.

979-8-3315-8138-1

The rest of the paper is organized as follows. Section II reviews the related works on MTD. The mathematical modeling of AGC dynamics, MTD, and BDD mechanisms is demonstrated in Section III. Section IV describes FDI attacks, and Section V discusses the case studies and numerical analysis of simulation outcomes. We have concluded the paper in Section VI.

II. Related Works

Recent studies have shown significant interest in enhancing resilience in AGC against cyber-physical threats such as FDI attacks and denial-of-service (DoS) attacks. Various observer-based defense mechanisms, such as directional and model-based unknown input observers (D/UIO) and adaptive and prescribed-time UIOs (PTUIOs), are proposed to isolate cyber-physical attacks within a multi-area AGC environment [6]–[8]. In particular, Ref. [8] provides a better detection mechanism by adaptively regulating thresholds and maintaining accurate state estimation within the prescribed time frame. In parallel, various data-driven schemes, including frequency analysis (FA), deep neural networks (DNNs), and modified Goertzel algorithms, demonstrate improved detection capability and reduced computational cost [9]–[11]. A reinforcement learning-based strategy, grounded in the Markov decision process, facilitates adaptive and cooperative decision-making against FDI attacks [12].

Recent development on power system state estimation (PSSE) resiliency shows robustness against FDI attacks, where controlled fluctuation has been carried out on strategic line parameters, and it enhances system resiliency by 10-20%. MTD has gained a lot of attention as an effective countermeasure against intrusion in cyber-physical systems. MTD has been applied to AGC loop and state estimation by controlled changing of branch reactances or susceptances, which increases the attack detection probability [13], [14]. Analysis studies to find the trade-off between MTD efficiency and operational cost for optimal power flow (OPF) formulations and principal angle separation metrics is presented in [15]. This study emphasizes that MTD must be designed to achieve higher security while minimizing operating costs. Another research work integrates cyber deception and game-theoretic models to dynamically adjust the attack surface and optimize defense cost [16]. Different decentralized MTD frameworks have been introduced in [17], [18] that focus on maintaining the system's scalability; however, these frameworks make the system challenging and less efficient. Noteworthy progress on distributed flexible alternating current transmission system (D-FACTS)-based coordinated control and graph-theoretic placement algorithms attracts MTD employment to enhance power system stability [19]. In Addition, different techniques, such as dynamic watermarking, sliding-mode perturbation observers (SMPO), and event-triggered control mechanisms have been introduced in AGC against coordinated attacks, like random time-delay (RTDA) and DoS events, and improve attack detection probability [20], [21].

III. Mathematical Modeling

Modern interconnected power systems can be represented as a discrete-time nonlinear dynamic system that inherently integrates secondary control loops, such as AGC, which regulates active power and frequency. The general architecture and workflow of the proposed FDI attack-resistant control system are illustrated in Fig. 1, which includes AGC control loop, MTD, and BDD state estimation.

A. AGC Dynamics

In the Automatic Generation Control (AGC) loop, variables such as mechanical power (P_b^m), electrical power output (P_b^g), reference power setpoint (P_b^{ref}), tie-line power flow between areas (P_{ij}^{tie}), area control error (ACE_i), rotor angle (δ_b), and rotor angular speed (ω_b) play active roles in maintaining power balance in an interconnected power system by regulating system frequency and tie-line power deviation [8]. Equations (1–6) illustrate a closed-loop system, where frequency and tie-line power deviation are expressed in ACE in (2) that causes imbalance between mechanical power and electrical power output during load disturbance or cyber-physical attack in certain measurements.

$$\begin{aligned}\Delta P_{ij,t+1}^{\text{tie}} = P_s\big(\Delta\delta_{\text{Area}i,t+1} - \Delta\delta_{\text{Area}j,t+1}\big) \\ + P_s\big(\Delta V_{t_{\text{Area}}i,t+1} - \Delta V_{t_{\text{Area}}j,t+1}\big)\end{aligned} \tag{1}$$

$$\begin{aligned}ACE_{i,t+1} = \left(\frac{1}{R_b} + D_b\right)\big(\omega_{b,t+1} - \omega_s\big) \\ + \sum_{\substack{i,j=1 \\ i\neq j}}^{3}\big(P_{i,t+1}^{\text{tie}} - P_{j,t+1}^{\text{tie}}\big)\end{aligned} \tag{2}$$

$$P_{b,t+1}^{\text{ref}} = P_{b,t}^{\text{ref}} + P_{b,g,t+1} - D_b\,\Delta T\,ACE_{i,t+1} \tag{3}$$

$$P_{b,t+1}^{m} = P_{b,t}^{m} + \frac{\Delta T}{T_b}\Big[\frac{1}{R_b}\big(P_{b,t+1}^{\text{ref}} - (\omega_{b,t+1} - \omega_s)\big) - P_{b,t+1}^{m}\Big] \tag{4}$$

$$\omega_{b,t+1} = \omega_{b,t} + \frac{\Delta\delta}{2H_b}\big(P_{b,t+1}^{m} - P_{b,t+1}^{g}\big) \tag{5}$$

$$\delta_{b,t+1} = \delta_{b,t} + \frac{1}{\Delta T}\big(\omega_{b,t+1} - \omega_s\big) \tag{6}$$

B. Moving Target Defense (MTD) in AGC Reference Setpoint

In classical FDI attacks, it is assumed that the attacker knows the dynamics and operating points of the system and can inject stealthy false data to be undetected by the detection techniques [19]. The proposed MTD has introduced bounded stochastic perturbations ($\Delta P_{g,t}^{\text{MTD}}$) in $P_{b,t}^{\text{ref}}$, which maintains controlled variations in system dynamics and is expected to be unknown to the attacker. Equations (7)–(9) present MTD implementations in the AGC layer, where q_t defines seven possible random deviations, ensuring maximum $d\%$ deviation by L_t.

$$P_{g,t}^{\text{MTD}} = P_{b,t}^{\text{ref}} + \Delta P_{g,t}^{\text{MTD}} \tag{7}$$

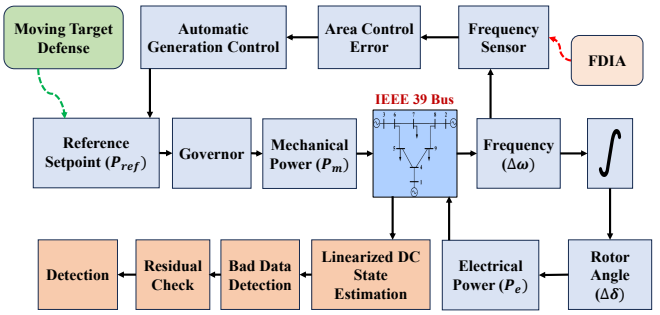


Fig. 1: Technical Overview of the MTD-enabled FDI attacks detection framework.

$$\Delta P_{g,t}^{\text{MTD}} = q_t \cdot \frac{N_{\text{levels}} - 1}{2L_t}, \quad q_t \in \{-3, -2, -1, 0, 1, 2, 3\} \tag{8}$$

$$L_t = \text{MaxDeviation} \cdot P_{g,t}^{\text{AGC}} = d \cdot P_{g,t}^{\text{AGC}} \tag{9}$$

C. Bad Data Detection (BDD) Mechanism

BDD is a fundamental component of the state estimation process in power systems, ensuring reliable control decisions [13]. In a DC or linearized AC power flow model, the measurement relationship can be illustrated as:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} \tag{10}$$

where, z is the measurement vector, H is the Jacobian measurement, and e denotes the measurement noise vector. The estimated state ($\hat{\mathbf{x}}$) during operation can be measured by the weighted least-squares (WLS) estimator:

$$\hat{\mathbf{x}} = \left(\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{z} \tag{11}$$

where R defines the measurement noise covariance matrix. The residual vector (r) is then computed, which determines how far the measured values are from expected measurements.

$$\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} \tag{12}$$

The weighted energy of residual between measured and expected values is calculated as the BDD test statistic (J).

$$J = \mathbf{r}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{r} \tag{13}$$

During normal operating conditions, J follows a chi-square distribution whose degrees of freedom depend on the number of independent measurements beyond estimated measurements. If J exceeds certain threshold limits, it indicates a potential anomaly within the system.

IV. Stealthy FDI attacks in AGC

A. Attacker's Objective and Attack Technique

The false data injected into the system's frequency measurements leads to an incorrect ACE calculation, which manipulates the control signal issued from the control center. As the attacker can inject a stealthy attack, the alteration of control signals or system states can't be detected by conventional BDD schemes. In this paper, an attack was introduced in different attack windows to observe the impact on power system dynamics. During the non-attack period, the frequency measurements remain unmodified. However, during the attack period $t_{\text{attack}} \in [t_{\text{start}}, t_{\text{end}}]$, stealthy attack vector a_i is being applied in the frequency measurement.

$$\tilde{f}_t = f_t + a_i, \quad i \in G_a \tag{14}$$

where G_a denotes the generator in which the attack has been applied. To ensure the FDI attacks remain stealthy, the attacker is constrained as follows:

$$|a_b[t]| \le \epsilon_f, \qquad \forall b \in B,\ \forall t \in T, \tag{15}$$

$$|a_b[t] - a_b[t-1]| \le \eta, \qquad \forall b \in B,\ \forall t \in T, \tag{16}$$

$$|\Delta\text{ACE}_i[t] - \Delta\text{ACE}_i[t-1]| \le \gamma, \qquad \forall i \in Z,\ \forall t \in T, \tag{17}$$

$$\omega_{\min} \le \tilde{\omega}_b[t] \le \omega_{\max}, \qquad \forall b \in B,\ \forall t \in T, \tag{18}$$

$$|\tilde{f}_t^{(i)} - \tilde{f}_t^{(j)}| \le \zeta, \qquad \forall i, j \in \mathcal{P},\ \forall t \in T. \tag{19}$$

where, ϵ_f is the noise of frequency measurement, η defines the injected attack magnitude, γ illustrates the control-loop perturbation parameter, and ζ is the unmodeled system effect.

B. Assumptions

- The attacker has sufficient knowledge of the primary control and secondary control loop (AGC) that includes system parameters and gains.
- The attacker can manipulate certain system measurements that affect the overall dynamics of the power system; however, they can not alter control signals applied to the generators.
- The attack can be continuous or time-limited depending on the attacker's strategy and available time period.

V. Case Studies and Numerical Analysis

This section presents the simulation outcomes obtained from the proposed MTD strategy, which aims to enhance the detection probability. The simulation is conducted on an IEEE 39-bus New England system, which is specifically designed for transient stability, frequency control, and cyber-physical security analysis. This bus system features 10 synchronous generators, with 7 equipped with governors, and comprises 46 transmission lines. In this study, FDI attacks were injected within three predefined attack windows: (500–700), (1100–1250), and (1400–1560) time-slots, within a total of 1800 time-slots. The control parameters used in the study are depicted in Table I, including generator time constants, AGC cycle, and MTD limits.

A. Dynamic Response Under Different Scenarios

Fig. 2(a) depicts the area control error (ACE) trajectories under four scenarios: (1) baseline (no FDI attack and no active MTD), (2) FDI attacks under no active MTD, (3) MTD-active (no FDI attack), and (4) FDI attack under active MTD scenario. The analysis focuses on generator 1 at bus 30 to provide

TABLE I: Key Simulation and Control Parameters (IEEE 39-Bus System)

Parameter	Value
Nominal frequency f_{nom}	60 Hz
Integration step ΔT	0.1 s
Simulation horizon T_{sim}	1800 s
AGC update period	60 s
Typical inertia H	4.2–6.5 (mean $\approx$ 5.5)
Typical damping D	52–76 (mean $\approx$ 63.2)
Governor time constant T_g	0.36–0.52 s
Turbine time constant T_t	1.80–2.48 s
Integral AGC gain K_I	12.6–23.4
MTD levels	7 (discrete)
Max MTD setpoint deviation d	$\pm 10\%$ of $P_{g,\text{ref}}$
MTD switch interval	5 s (hold 3–8 s)

a clear and representative explanation of the system's dynamic behavior. In the baseline scenario, ACE converges smoothly to zero as there is no cyber attack. However, ACE exhibits sharp positive excursions (approximately 0.22 - 0.25 pu) under only the FDI attack scenario and the FDI attack under the active MTD scenario, indicating that the attacker has successfully corrupted frequency measurements into the control loop during the attack window. The MTD-active (no FDI attack) scenario shows that the defense mechanism remains stable and is not affected by controlled perturbations in the reference power setpoint. Notably, the spikes in ACE are more intensified for scenario 4 than only the FDI attacks scenario, which causes the AGC to respond more strongly to these corrupted signals that affect the whole dynamics.

B. Impact on Power System Dynamics

In effect, ACE distortions propagate through the AGC control loop that cascades along the reference power setpoint, mechanical power input, and electrical power output. During FDI attacks under no active MTD scenario, reference power output in Fig. 2(b) shows oscillations approximately between 11.2–12.8 pu, which is 5–7% from the baseline conditions. However, the FDI attack under the active MTD scenario shows 2-3% higher reference setpoint variability compared to FDI attacks only. It emphasizes that MTD makes the system more sensitive to falsified measurements and baseline models, which enhances the ability of BDD to detect the abnormalities. Variations in mechanical power in Fig. 2(c) and electrical power output in Fig. 2(d) are directly related to the behavior of the reference power. The mechanical torque fluctuations in synchronous generators propagate through the electromagnetic dynamics, and the imbalance between instantaneous mechanical torque and electromagnetic torque causes corresponding variations in electrical power output, rotor angle, and terminal voltage. Fig. 3(a) illustrates that terminal voltage exhibits pronounced disturbances under only FDI attacks, while these deviations are mitigated due to the application of MTD that prevents stealthy attacks from influencing the control system and allows the excitation system to maintain a stable voltage profile.

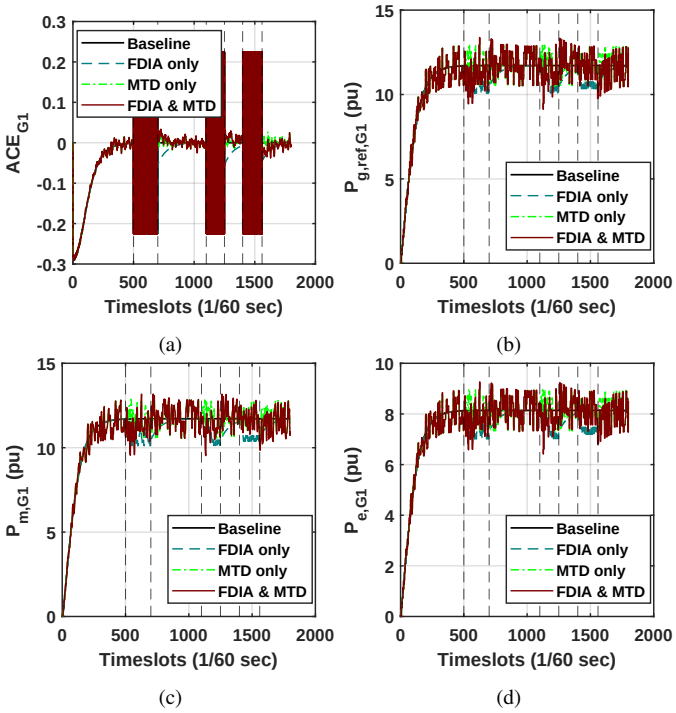
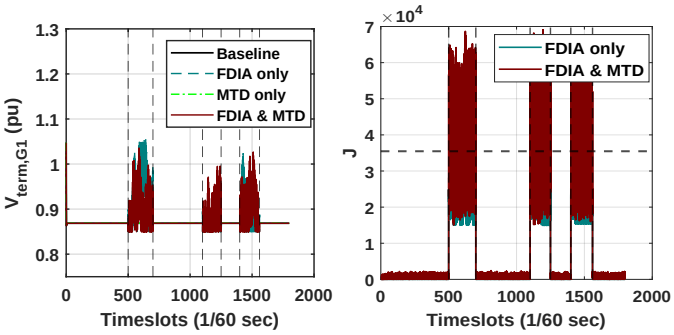


Fig. 2: Generator responses of Gen 1 at Bus 30 under four scenarios: (a) ACE trajectory, (b) AGC reference power, (c) mechanical power output, and (d) electrical power output.

C. BDD Detection Performance With and Without MTD

In FDI attacks under no MTD case, the residual energy remains low and J-statistics becomes below certain threshold limit due to stealthy FDI attacks, as shown in Fig. 3(b), while the FDI attack under MTD scenario causes inconsistencies in state-estimation residual and eventually the residual energy and J-statistic distribution increases substantially. In this study, the detection threshold has been set at the 70th percentile of baseline J-statistic distribution, corresponding to a value of 3.2×10^4. As the proposed AGC-driven framework produces non-Gaussian, time-varying residuals due to measurement corruptions and MTD perturbations, the chi-square assumption collapses in this system. The percentile-based threshold is integrated instead of the conventional chi-square bound because it reflects the true residual distribution of the system by directly being calculated from the baseline J-distribution. Fig. 4 illustrates the capability of the BDD state-estimator to detect stealthy FDI attacks. Under no MTD configuration, the FDI attacks remain hidden and lead to negligible detection in all attack windows. The FDI attack under the active MTD scenario scheme enhances the detection rate by 32.7% compared to without the MTD scenario. Although the detection rate is significant at MTD-enabled FDI attack case, the analysis reveals that active MTD does not guarantee full observability of the attacks, which detects only limited portions of attack periods.



(a) (b)

Fig. 3: (a) Terminal voltage response of Gen 1 at Bus 30 under four scenarios, and (b) J-statistic trajectories comparing FDI attacks-only scenario and the FDI attacks under no MTD scenario.

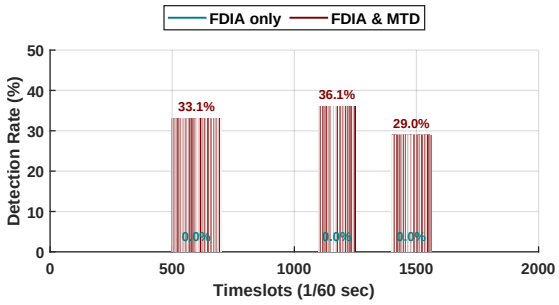


Fig. 4: Detection behavior during three attack windows for FDI attacks (a) under no active MTD and (b) under an active MTD scenario.

VI. Conclusion

AGC plays a significant role in maintaining power system stability by regulating system frequency and tie-line power deviation across interconnected areas. This work shows that stealthy FDI attacks can disrupt system dynamics while the attacker escapes detection by conventional BDD mechanisms. To address the vulnerability, we introduce MTD in reference power setpoints that break the attacker's knowledge of system dynamics and create inconsistencies during stealthy attack injection. Simulation results across multiple operating scenarios, including baseline, only FDI attacks (no active MTD), only MTD, and FDI attacks under MTD conditions, reveal that scenario 4 substantially increases the FDI attack detection rate by 32.7% compared to FDI attacks under no active MTD conditions. The percentile-based BDD threshold facilitates a clear and effective separation of stealthy FDI attacks across various scenarios. These findings establish MTD as an effective defensive layer to improve the cyber-resilience of power system operation against advanced cyber threats.

Acknowledgement

This work is supported by the Department of Energy (DOE) (Award# DE-CR0000046). Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the DOE's views.

References

[1] G. E. Mejía-Ruiz, G. Marasini, Z. Qu, S. Kundu, and S. Pushpak, "Cybersecurity challenges in power networks with distributed energy resources: A comprehensive survey," Renewable and Sustainable Energy Reviews, vol. 224, p. 116100, 2025.

[2] S. Wali, Y. A. Farrukh, I. Khan, and J. A. Hamilton, "Covert penetrations: Analyzing and defending SCADA systems from stealth and hijacking attacks," Computers and Security, p. 104449, 2025.

[3] M. M. Gulzar, D. Sibtain, M. Alqahtani, F. Alismail, and M. Khalid, "Load frequency control progress: A comprehensive review on recent development and challenges of modern power systems," Energy Strategy Reviews, vol. 57, p. 101604, 2025.

[4] P. C. Sahu, S. Mohapatra, S. K. Bhatta, G. G. Tejani, and S. J. Mousavirad, "An exclusive survey on robust controllers and novel optimization techniques for AGC of power system," Energy Reports, vol. 13, pp. 3845–3868, 2025.

[5] M. Alanazi, A. Mahmood, and M. J. M. Chowdhury, "SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues," Computers and Security, vol. 125, p. 103028, 2023.

[6] M. A. Abbasi, A. S. Khan, S. Huang, M. Z. Qadri, and L. Guo, "Securing cyber-physical systems: Attack detection and isolation in power grid AGC," International Journal of Critical Infrastructure Protection, p. 100806, 2025.

[7] X. Zhao, Z. Ma, X. Shi, and S. Zou, "Attack detection and mitigation scheme of load frequency control systems against false data injection attacks," IEEE Transactions on Industrial Informatics, vol. 20, no. 8, pp. 9952–9962, 2024.

[8] S. I. Abouzeid, Y. Chen, M. Zaery, S. M. Amrr, and E. H. Abdelhameed, "Prescribed-time mitigation of false data attacks in microgrid load frequency control," IEEE Transactions on Smart Grid, 2025.

[9] A. A. E. Elsayed, H. Khani, and H. E. Z. Farag, "A new method for stealthy false data injection attack detection using advanced feasibility areas considering spatial distribution," IEEE Transactions on Smart Grid, 2025.

[10] P. Aryan, G. L. Raja, U. Mehta, T. R. Chelliah, and U. R. Muduli, "A resilient tri-parametric fractional frequency control for cybersecurity threats amid latency," IEEE Transactions on Industry Applications, 2025.

[11] F. Mohammadi and M. Saif, "An intrusion detection and mitigation framework for automatic generation control systems," IEEE Transactions on Industrial Cyber-Physical Systems, 2024.

[12] S. Liu, L. Xi, and H. Chen, "Enhancing security in smart distribution networks: Proximal policy cooperative optimization against false data injection attacks," IEEE Transactions on Industry Applications, 2025.

[13] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and J. Chen, "Analysis of moving target defense against false data injection attacks on power grid," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2320–2335, 2019.

[14] C. Liu, J. Wu, C. Long, and D. Kundur, "Reactance perturbation for detecting and identifying FDI attacks in power system state estimation," IEEE Journal of Selected Topics in Signal Processing, vol. 12, no. 4, pp. 763–776, 2018.

[15] S. Lakshminarayana and D. K. Y. Yau, "Cost-benefit analysis of moving-target defense in power grids," IEEE Transactions on Power Systems, vol. 36, no. 2, pp. 1152–1163, 2020.

[16] Y. Zhou, G. Cheng, and S. Yu, "An SDN-enabled proactive defense framework for DDoS mitigation in IoT networks," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 5366–5380, 2021.

[17] J. Giraldo, M. El Hariri, and M. Parvania, "Decentralized moving target defense for microgrid protection against false-data injection attacks," IEEE Transactions on Smart Grid, vol. 13, no. 5, pp. 3700–3710, 2022.

[18] J. Tian, R. Tan, X. Guan, and T. Liu, "Enhanced hidden moving target defense in smart grids," IEEE Transactions on Smart Grid, vol. 10, no. 2, pp. 2208–2223, 2018.

[19] Z. Zhang, R. Deng, P. Cheng, and M.-Y. Chow, "Strategic protection against FDI attacks with moving target defense in power grids," IEEE Transactions on Control of Network Systems, vol. 9, no. 1, pp. 245–256, 2021.

[20] B. Ti, G. Li, M. Zhou, and J. Wang, "Resilience assessment and improvement for cyber-physical power systems under typhoon disasters," IEEE Transactions on Smart Grid, vol. 13, no. 1, pp. 783–794, 2021.

[21] S. Panterino and M. Fellington, "Dynamic moving target defense for mitigating targeted LLM prompt injection," Authorea Preprints, 2024.