Impact Analysis of False Data Injection Attacks on Automatic Voltage Regulators of Synchronous Generators

Mohammad Zakaria Haider*, Prabin Mali*, Mohammad Ashiqur Rahman*†and Sumit Paudyal*
*Department of Electrical and Computer Engineering, Florida International University, USA
†Knight Foundation School of Computing and Information Sciences, Florida International University, USA
mhaid010@fiu.edu, pmali004@fiu.edu, marahman@fiu.edu, spaudyal@fiu.edu

***Abstract*—Automatic Voltage Regulator (AVR) is a pivotal control within the domain of power systems engineering, specifically due to its importance in providing constant and reliable voltage. This research analyzes AVR's vulnerability to False Data Injection (FDI) attacks. With the escalating integration of the Internet of Things (IoT) and communication technologies in power grids, cybersecurity risks have emerged as a significant concern. The investigation concentrates on elucidating the impact of FDI attacks on synchronous generators equipped with AVRs, employing advanced mathematical computations to simulate scenarios involving voltage fluctuations and grid disturbances. The research presents innovative insights into the cascading repercussions of multiple compromised AVRs on terminal voltage and the destabilization of reactive power. By scrutinizing the intricate dynamics of AVRs in the context of FDI attacks, the study aims to inform the grid operator of the risks posed by cyber threats in the evolving landscape of modern energy infrastructure, thus assisting in developing more resilient and secure power systems.**

***Index Terms*—Automatic Voltage Regulator(AVR), Cyber Security, False Data Injection(FDI), Smart Grid, Voltage Instability**

NOMENCLATURE

$\mathcal{E}_{fd}$	Exciter Voltage
$\mathcal{I}_{exc}$	Exciter Current
$\mathcal{I}_{load}$	Load Current
$\mathcal{K}_A$	Amplifier Gain Constant
$\mathcal{K}_E$	Exciter Gain
$\mathcal{K}_p$	Proportional Gain
$\mathcal{K}_i$	Integral Gain
$\mathcal{K}_{exc}$	Exciter Gain
$\mathcal{Q}$	Reactive Power
$\mathcal{R}_f$	Stabilizer Feedback Variable
$\mathcal{T}_A$	Amplifier Time Constant
$\mathcal{T}_E$	Exciter Time Constant
$\mathcal{V}_t$	Terminal Voltage
$\mathcal{V}_R$	Output Voltage of Amplifier
$\mathcal{V}_{ref}$	Reference Voltage of AVR
Φ	Magnetic Flux of Rotor
θ	Power Factor

I. INTRODUCTION

A. Motivation

Automatic Voltage Regulator (AVR) is a critical component for maintaining the stability and reliability of synchronous generators within interconnected grids. This research examines the multifaceted dynamics of AVRs and their consequential impact on terminal voltage and reactive power generation. The primary objective is to elucidate the complex interactions governing the response of synchronous generators under False Data Injection (FDI) attack and to examine the broader implications of these dynamics on the stability of the associated power grid. Recently, power grids have become more innovative and efficient with the incorporation of Internet of Things (IoT) devices and information and communication technologies among different devices, making them vulnerable to cyber-attacks. A recent report found that the California Power grid has defended over a million cyber-attacks each month [1]. The ransomware attack on the Colonial Pipeline in 2021 raised a deep concern about the vulnerability of critical similar infrastructures (i.e., Power Grid) [2].

According to the Threat Intelligence Index report, the energy sector is the fourth most attacked industry in 2022, comprising 10.7% of overall cyber attacks [3]. Another ransomware named WannaCry infected four billing offices of India's West Bengal State Electricity Distribution Company, which provides service to around 0.8 million people, and caused bill payment operations to be suspended [4]. The attackers behind the epic Triton/Trisis attack that in 2017 targeted and shut down a physical safety instrumentation system in a petrochemical plant in Saudi Arabia have now been discovered by probing the networks of dozens of US and Asia-Pacific electric utilities [5]. On top of that, attacks like Stuxnet [6] and Dragonfly [7] require the attacker to have complete access to real-time data in control centers and a comprehensive understanding of the system. In [8], it has been discussed how voltage instability may occur when the power system experiences a cyber attack, resulting in widespread power outages and significant economic losses with severe social consequences. Disruptions to power grids can have serious consequences for critical infrastructure such as hospitals, emergency services, and water treatment plants, affecting the well-being of communities. Additionally, FDI attacks have the potential to diminish public trust in energy infrastructure and the institutions responsible for its regulation and security. Thus, investigating methods to uphold voltage stability in the face of cyberattacks is crucial.

AVR systems play a crucial role in maintaining voltage levels within acceptable limits in power grids. Petri net-based approach has depicted the transmission of network attacks and the control of voltage regulation in [9]. Pierrou at el. showed in [10], how voltage regulation by updating the reference points of FACTS devices can be used for Wide-Area Voltage Control (WAVC). Our motivation of this work is to explore the possibility of creating wide area voltage instability by inducing malicious data through reference voltage, which disrupts the AVR's ability to maintain the desired terminal voltage.

This research methodology involves a detailed mathematical analysis of the dynamic behavior of synchronous generators equipped with AVRs. The study uses advanced modeling techniques to simulate load fluctuations and grid disturbance scenarios, systematically varying the reference voltage to observe its cascading effects on excitation current and terminal voltage. The insights gained from this analysis will contribute to the development of optimized automatic voltage control and attack mitigation strategies that can enhance the stability and reliability of synchronous generators within interconnected power systems.

B. Related Works

The increasing use of advanced monitoring and anomaly detection faces a cybersecurity challenge in modern power grids. Adversaries can compromise measurement devices, sending malicious data to the control center and potentially causing physical damage. It is crucial to analyze cyber attack scenarios for power system safety. Studies on FDI attacks assume partial or full knowledge of the targeted system. Recent research, like [11]–[13], focuses on injecting false data into load and power transmission measurements. Chen et al. [14] demonstrated remote FDI attacks targeting Automatic Voltage Regulation (AVR) with limited knowledge of the power grid.

FDI attacks aim to manipulate measurements to misguide control actions, impacting automatic voltage regulation, load frequency control, and var voltage control [14]–[16]. In modern power systems, sensor data is transmitted to control centers for analysis by optimization and control algorithms. Lou et al. [15] introduced a reinforcement learning-based FDI attack that can bypass existing detection processes without knowing the power system topology [17].

Nevertheless, the communication lines are not secured, and the data is not encrypted in most cases, which makes these networked systems vulnerable to cyberattacks. In this paper, the FDI attack is launched on the communication line that transmits data from the power sensor to the control centers [18]. Power system operators and researchers employ sophisticated methods and tools to identify and mitigate erroneous or compromised data, which could lead to operational issues, system instability, or even cybersecurity threats. However, if the attack is stealthy enough, an attacker can bypass the BDD or other anomaly detection model within the control center, making the system unstable with malicious data.

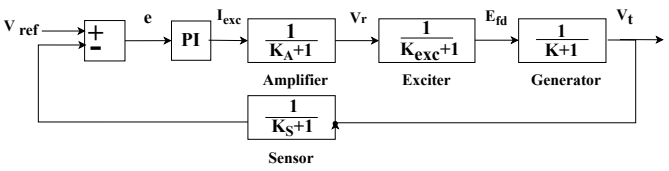

Fig. 1. Block Diagram of Automatic Voltage Regulator

C. Contribution

This study delves into a crucial yet overlooked aspect of intelligent power grid cybersecurity: specifically, the susceptibility of the communication link connecting AVR to the control center. While existing literature primarily concentrates on FDI attacks on the power grid, our research highlights the possible consequences of compromising the internal parameters of AVRs in synchronous generators. Thus, the main contributions of this paper are as follows.

- We provide a comprehensive exploration of the repercussions associated with the compromise of multiple AVRs. Our analysis elucidates the cascading effects of voltage modification, illustrating how such alterations can influence the voltage of non-generating buses. This, in turn, has the potential to trigger protective relays or cause damage to components within the associated buses, particularly over or under voltage conditions.
- Our study reveals that altering the terminal voltage exerts a more pronounced impact on the reactive power than on the real power. Through empirical evidence derived from FDI attacks on multiple AVRs, we demonstrate the oscillatory behavior of reactive power and its redistribution among non-affected buses. This redistribution phenomenon may activate protective relays, introducing a novel dimension to the potential consequences of such cyber threats.

These findings highlight the complex interactions between corrupted AVRs and the system's overall stability, advancing our understanding of cybersecurity risks within the power grid. The research's conclusions stress the need for more robust cybersecurity defenses and more attention to protecting vital parts such as AVRs to maintain the power grid's resilience against malevolent cyberattacks.

II. Control Mechanisms of AVR

The fundamental role of AVRs is to regulate the terminal voltage, $\mathcal{V}_t$ of synchronous generators through the modulation of the generator's excitation system. Fig. 1 shows the building block of AVR in the generators. In AVR, the excitation current, $\mathcal{I}_{exc}$, is continuously adjusted in response to changes in $\mathcal{V}_{ref}$ with the help of a proportional-integral control algorithm (PI). $\mathcal{I}_{exc}$ depends on the dynamic relationship of the excitation systems [19], as presented below:

$$\mathcal{T}_E \frac{d\mathcal{E}_{fd}}{dt} = -(\mathcal{K}_E + \mathcal{S}_E(\mathcal{E}_{fd}))\mathcal{E}_{fd} + \mathcal{V}_R \tag{1}$$

$$\mathcal{T}_F \frac{d\mathcal{R}_f}{dt} = -\mathcal{R}_f + \frac{\mathcal{K}_E}{\mathcal{T}_F}\mathcal{E}_{fd} \tag{2}$$

$$\mathcal{T}_A \frac{d\mathcal{V}_R}{dt} = -\mathcal{V}_R + \mathcal{K}_A\mathcal{R}_f - \frac{\mathcal{K}_A\mathcal{K}_F}{\mathcal{T}_F}\mathcal{E}_{fd} + \mathcal{K}_A(\mathcal{V}_{ref} - \mathcal{V}_t) \tag{3}$$

$$\mathcal{V}_R^{min} \leq \mathcal{V}_R \leq \mathcal{V}_R^{max} \tag{4}$$

This induced voltage is responsible for creating the terminal voltage. The basic equation describing this relationship is the generator voltage equation. This equation is typically expressed as:

$$\mathcal{V}_t = \mathcal{K}\Phi\mathcal{N} \tag{5}$$

Here, $\mathcal{K}$ is a constant that depends on the generator characteristics, and $\mathcal{N}$ is the rotational speed of the generator. Magnetic flux, Φ is related to $\mathcal{E}_{fd}$ and $\mathcal{I}_{exc}$ through the relationship $\Phi = \frac{\mathcal{E}_{fd}}{\mathcal{K}_{exc}}\mathcal{I}_{exc}$, where $\mathcal{K}_{exc}$ is a constant related to the exciter characteristics. Substituting this expression for Φ back into the generator voltage equation, we get:

$$\mathcal{V}_t = \mathcal{K}\left(\frac{\mathcal{E}_{fd}}{\mathcal{K}_{exc}}\mathcal{I}_{exc}\right)\mathcal{N} \tag{6}$$

This equation illustrates the dependence of $\mathcal{V}_t$ on $\mathcal{E}_{fd}$, $\mathcal{I}_{exc}$, and other constants $(\mathcal{K}, \mathcal{K}_{exc}, \mathcal{N})$. Combining (II)-(6), we can say $\mathcal{V}_{ref}$ serves as a setpoint for the desired terminal voltage, and any deviation triggers corrective actions through the AVR. The relationship between the reference voltage, excitation current, and terminal voltage can also be expressed as:

$$\mathcal{I}_{exc}(t) = \mathcal{K}_p e(t) + \mathcal{K}_i \int_0^t e(t)d(t) \tag{7}$$

Here, $e(t) = \mathcal{V}_{ref}(t) - \mathcal{V}_t(t)$ is the error signal representing the deviation of the terminal voltage from the reference voltage. The closed-loop control system is designed to minimize the error signal $e(t)$ by continuously adjusting the excitation current, ensuring that the terminal voltage closely follows the reference voltage under varying operational conditions. This proportional-integral control mechanism, supported by transfer functions, forms the mathematical foundation for understanding the intricate dynamics of AVRs in synchronous generators.

III. Impact of False Data Injection on AVR

Through advanced modeling techniques, this paper analyzes the impact of AVRs on terminal voltage under various operating conditions. Simulations explore scenarios of sudden load changes or disturbances in the grid, elucidating how the AVR dynamically responds to these events to stabilize the terminal voltage. The wide range of vulnerabilities and impacts of FDI attacks makes them the most challenging cyber-physical security threat in the smart grid. Unlike Denial-of-Service (DoS) attacks, FDI attacks on AVR manipulate data without necessarily interrupting system functionality. Similarly, while malware infections compromise system integrity or confidentiality, FDI attacks specifically target data integrity, distinguishing them in their objectives and methodologies.

Voltage Instability: Voltage instability poses a significant threat to the reliable operation of the power system, potentially causing equipment damage and service interruptions. This instability can lead to a loss of synchronism, disrupting the generator's ability to contribute to the overall grid operation. This condition may result in the disconnection of the generator from the grid, exacerbating power supply issues.

Reactive Power Imbalance: Beyond terminal voltage regulation, AVRs also play a crucial role in managing reactive power output from synchronous generators. Adjusting a generator's $\mathcal{V}_{ref}$ primarily influences the reactive power output by changing the terminal voltage. The relationship between reactive power, terminal voltage, and load current can be expressed through the following equation:

$$\mathcal{Q} = \mathcal{V}_t\mathcal{I}_{load}\sin\theta \tag{8}$$

Coordination of Other Control System: The interdependence of control systems within a synchronous generator is critical to power system operation. In addition to AVRs, generators are equipped with Power System Stabilizers (PSS) and Load Frequency Controllers (LFC) to address other aspects of stability and frequency control. Understanding the coordination between these control systems is paramount for optimizing overall power system performance. However, this interaction of AVR with other regulators is out of the scope of this paper.

IV. Problem Formulations

In Section II, we've presented the relationship of reference voltage $\mathcal{V}_{ref}$, with terminal voltage, $\mathcal{V}_t$ through the function of AVR. Basically, $\mathcal{V}_{ref}$ is set by the operator or control central remotely through a communication link based on system demand. That is why the vulnerability in the remote communication link between the control center and the AVR of a generator presents a critical cybersecurity concern. Adversarial interference in this communication channel allows for the injection of false commands, particularly in the control of $\mathcal{V}_{ref}$. Such malicious interventions can induce spurious adjustments to $\mathcal{V}_{ref}$, potentially triggering voltage instability in the associated bus. A compromised $\mathcal{V}_{ref}$, orchestrated through adversarial actions, introduces a destabilizing factor, potentially leading to voltage fluctuations and, in severe cases, grid instability.

V. Evaluation

To evaluate the impact of compromised AVRs, we have chosen the IEEE-39 bus system for simulation with the ePHASORSIM module of OPAL-RT in combination with MATLAB/Simulink. A model diagram for the IEEE-39 bus system has been shown in Fig. 2. We assume that the attacker can compromise the communication link of all generators and change the value up to 10%.

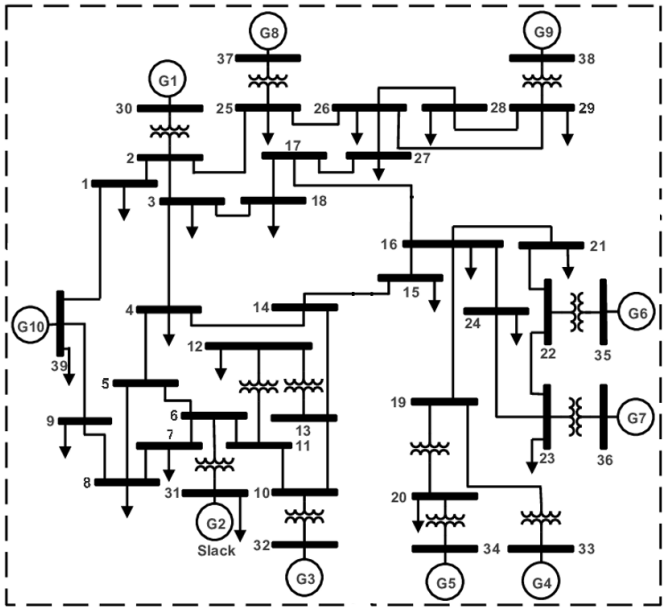

Fig. 2. IEEE 39 Bus System

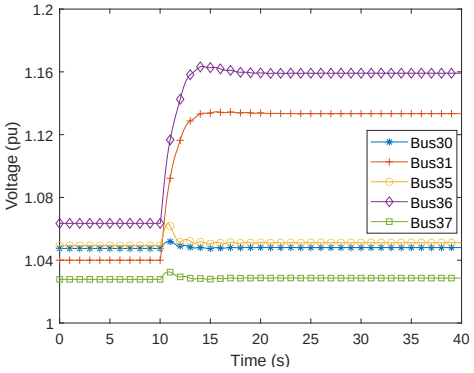

Fig. 3. Impact of Attack on Generator Buses

- Case I: We considered a vulnerability in the AVRs of the generators connected to busses 31 and 36 in this case. The attacker modifies these generators' $\mathcal{V}_{ref}$ values, affecting the terminal voltage proportionally. Fig. 3 illustrates how the unaffected generators at buses 30, 35, and 37 show oscillations at first but eventually stabilize since their $\mathcal{V}_{ref}$ are not impaired. We concentrate on impaired generators, acknowledging the influence of oscillations and protective relay activation mechanisms. As seen in Fig. 4, the attacker's manipulation of terminal voltage impacts load buses (6, 9, and 14), resulting in persistent changes in their terminal voltages. Variations in load bus voltages are caused by changes in generator terminal voltage, which can cause varied levels of variation depending on where the compromised generators are serving. Notably, this impact lasts throughout the entire duration of the strike.
- Case II: In the context of presenting our analysis, we have considered that the attacker attacked each generator

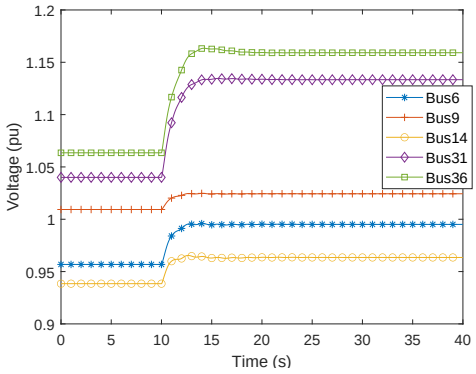

Fig. 4. Impact of Attack in Load Buses

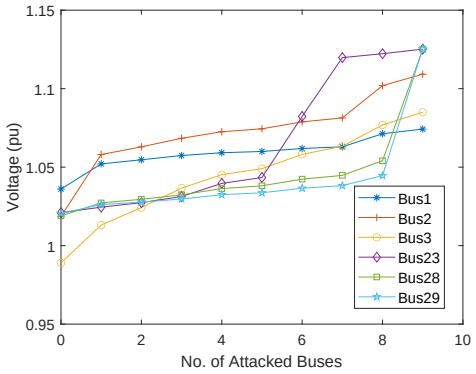

Fig. 5. Impact of Combined Attack on Load Buses

in turn, beginning with bus 30 and ending with bus 38. The voltage variation of the load buses is shown in Fig. 4, in which loads closer to the affected buses will cause a more remarkable voltage change than loads farther away. Therefore, adversaries must plan their attack on AVRs closest to the target load to target that particular load or protection device.

- Case III: As mentioned in Section II, terminal voltage has an impact on the reactive power. In this case, we have taken into account that, the attacker has changed the $\mathcal{V}_{ref}$ values of the generators connected at buses 31 and 36 which in turn change their output reactive power. In Fig. 6, we have found that to compensate for this additional reactive power supply, other generators will decrease their reactive power generation

VI. Attack Mitigation

Identification of false V_{ref} in AVRs and enhancing the robustness of the control system requires a methodical and scientifically grounded approach. An in-depth analysis of generator behavior under varying load conditions, transient disturbances, and system faults, employing mathematical modeling techniques, such as dynamic phasor analysis or state-space representation, enables the elucidation of the AVR's response to erroneous V_{ref} inputs. Exploring the intricacies of signal processing methodologies, such as digital filtering and statistical analysis, can facilitate the detection of anomalous

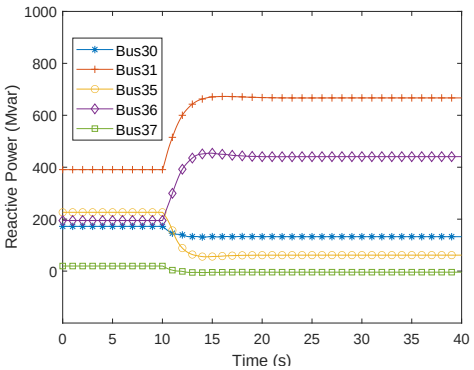

Fig. 6. Impact of Attack on Reactive Power of Generators

V_{ref}, amidst noise and operational variability. Employing advanced algorithms, including Kalman filtering or adaptive estimation techniques, may enhance the system's capability to discriminate between genuine and false V_{ref} inputs. Adaptive control-based defense mechanisms against FDI have shown in [20], [21], and two innovative approaches based on moving target defense have been discussed in [22], [23]. A machine learning-based approach similar to [24] can also be explored as an attack mitigation approach to identify injected false $\mathcal{V}_{ref}$ on AVR for increasing the robustness of the control center. Furthermore, embracing a holistic approach to system design, encompassing not only control algorithms but also hardware redundancy, system architecture resilience, and operational procedures, is essential for cultivating a robust and dependable control system.

VII. Conclusion

In conclusion, this paper has assessed the viability of FDI attacks targeting the AVR of synchronous generators to examine their impact on the associated power system. Employing advanced modeling and simulations, this research has provided insights into the intricate dynamics of AVRs and their pivotal role in maintaining power grid stability. The findings indicate that compromising the local regulators of multiple generators can induce system-wide voltage instability and reactive power oscillations, potentially triggering protective relays that force generators out of the system, leading to power outages. However, it is important to note that the attacks formulated in this study were based on a heuristic approach. Future research endeavors will prioritize the development of optimal attack vectors through formal analysis, aiming to circumvent the limitations posed by modern control systems' inadequate data and anomaly detection processes.

Acknowledgement

This work is supported by the Department of Energy (DOE) under Award# DE-CR0000024. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the DOE.

References

[1] R. Nikolewski, "California operator of electricity grid fends off millions of cyberattacks each month," 2019. https://www.sandiegouniontribune.com/business/energy-green, accessed 2023-11-01.

[2] J. Easterly, "The attack on colonial pipeline: What we've learned what we've done over the past two years," 2023. https://www.cisa.gov/news-events/news, accessed 2023-11-03.

[3] J. Gregory, "Today's biggest threats against the energy grid," 2023. https://securityintelligence.com/articles/, accessed 2023-11-02.

[4] N. Kshetri and J. Voas, "Hacking power grids: A current problem," *Computer*, vol. 50, no. 12, pp. 91–95, 2017.

[5] K. Jackson, "Analysis of ce inter-area oscillations of 1st december 2016," 2019. https://www.darkreading.com/perimeter/, accessed 2023-11-08.

[6] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *Proc. IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, pp. 4490–4494, 2011.

[7] A. Hesseldahl, "Hackers infiltrated power grids in u.s., spain," 2014. https://www.vox.com/2014/7/1/11628504/hackers-infiltrated-power-grids-in-us-spain, accessed 2014-07-01.

[8] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.

[9] R. Fu, Y. Xu, Y. Tang, and Q. Wang, "Petri net-based voltage control strategy under false data injection attack," in *Transactions of the Institute of Measurement and Control*, vol. 42, pp. 2622–2631, 2020.

[10] G. Pierrou and X. Wang, "An online network model-free wide-area voltage control method using pmus," *IEEE Transactions on Power Systems*, vol. 36, no. 5, pp. 4672–4682, 2021.

[11] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, 2011.

[12] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1731–1738, 2012.

[13] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, 2014.

[14] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2158–2169, 2019.

[15] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, 2014.

[16] S. Sridhar and G. Manimaran, "Data integrity attack and its impacts on voltage control loop in power grid," in *Proc. 2011 IEEE Power and Energy Society General Meeting*, pp. 1–6, 2011.

[17] W. Luo and L. Xiao, "Reinforcement learning based vulnerability analysis of data injection attack for smart grids," in *Proc. 2021 40th Chinese Control Conference (CCC)*, pp. 6788–6792, 2021.

[18] R. Kaur, J. Albrethsen, D. K. Yau, and S. Ghahremani, "Vulnerability assessment of false data injection attacks on optimal power flow," in *Proc. 2021 IEEE PES Innovative Smart Grid Technologies - Asia (ISGT Asia)*, pp. 1–5, 2021.

[19] P. W. Sauer, M. A. Pai, and J. H. Chow, *Synchronous Machine Control Models*, pp. 53–70. IEEE, 2017.

[20] X. Luo, R. Gao, X. Wang, and X. Wang, "An adaptive lqr-based defense strategy against false data injection attack in smart grids," in *Proc. 2022 IEEE 6th Conference on Energy Internet and Energy System Integration (EI2)*, pp. 1433–1438, 2022.

[21] Z. Xu, Q. Ma, L. Lin, Q.-G. Nie, X. Liu, D.-F. Yang, and J. Li, "A resilient defense strategy against false data injection attack in smart grid," in *Proc. 2021 40th Chinese Control Conference (CCC)*, pp. 4726–4731, 2021.

[22] W. Xu, I. M. Jaimoukha, and F. Teng, "Robust moving target defence against false data injection attacks in power grids," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 29–40, 2023.

[23] M. H. Shahriar, A. A. Khalil, M. A. Rahman, M. H. Manshaei, and D. Chen, "iattackgen: Generative synthesis of false data injection attacks in cyber-physical systems," in *Proc. 2021 IEEE Conference on Communications and Network Security (CNS)*, pp. 200–208, 2021.

[24] B. Abegaz and J. Kueber, “Smart control of automatic voltage regulators using k-means clustering,” in *Proc. 2019 14th Annual Conference System of Systems Engineering (SoSE)*, pp. 328–333, 2019.