A Remedial Action Scheme Against False Data Injection Cyberattacks Targeting ULTC Transformers in Smart Distribution Systems

Ehsan Naderi
Department of Electrical Engineering, College of Engineering and Computer Science
Arkansas State University
Jonesboro, AR, USA
enaderi@astate.edu

Arash Asrari
Department of Electrical and Computer Engineering
Purdue University Northwest
Hammond, IN, USA
aasrari@pnw.edu

Poria Fajri
Electrical and Biomedical Engineering Department
University of Nevada
Reno, NV, USA
pfajri@unr.edu

2024 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia) | 979-8-3503-5229-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICPSASIA61913.2024.10761531

***Abstract*—This paper proposes an on-line remedial action scheme (OLRAS) in order to mitigate the voltage violations caused by false data injection attacks (FDIAs) targeting under load tap changing (ULTC) transformers in smart distribution systems. The FDIA framework contains two different phases. In the attack phase, distribution system operator (DSO), being in attacker's shoe, considers cyberattack scenarios through compromising the results of volt-var optimization problem in a radial distribution grid modified with distributed energy resources (DERs) such as photovoltaic (PV) units and wind turbines (WTs). The outcome of the attack phase will be the compromised voltage profile of the distribution grid showing different rates of voltage violations. In the reaction phase, the DSO rapidly identifies a customized distribution feeder reconfiguration (CDFR) in order to update the flows of active and reactive power throughout the targeted distribution system and recover the voltage profile. The objective functions of the proposed CDFR are defined to minimize the impacts of such cyberattacks targeting ULTCs within distribution grids. This will empower DSOs to react to severe cyberattacks, bypassing the detection stage, and address the voltage violations in a timely manner. The effectiveness of the proposed OLRAS is validated on an IEEE test system.**

Keywords—customized distribution feeder reconfiguration (CDFR), false data injection attack (FDIA), on-line remedial action scheme (OLRAS), overvoltage, undervoltage, voltage violation.

I. Introduction

A. Background and Motivation

Intersection of energy infrastructure with information and communication technology (ICT) framework has transformed traditional power systems into a new generation of power grids, referred to as cyber-physical power systems (CPPSs) [1]. Although CPPSs facilitate the operation of automated systems with minimum involvement of humans in decision-making processes, a noticeable attack surface is introduced in the cyber layer of such systems through IEC 61850 standard, which is not secure [2]. Hence, adversaries can potentially penetrate into the cyber layer of power networks, compromise the recorded information, and cause a variety of operational issues such as the power outage for almost a quarter of a million end-use customers of the Ukrainian power grid in 2015 [3]. According to Edison Electric Institute (the association representing the U.S. investor-owned electric companies), millions of attacks were observed and prevented in 2020 in the U.S. electric power industry [4]. However, if a cyberattack manages to bypass the detection stage, actions will be required to remediate its impacts [5]. Therefore, remedial actions have recently been under the spotlight of researchers as an effective method to mitigate the negative impacts of cyberattacks bypassing the detection stage [6]-[7]. In this work, we concentrate on addressing voltage violations caused by false data injection attacks (FDIAs) targeting under load tap changing (ULTC) transformers within smart distribution systems. The importance of this research avenue stems from the fact that voltage profiles that are intentionally compromised can manipulate the power flow in the branches of a distribution system, consequently affecting the system efficiency. Highlighted in [8]-[9], voltage instability has been the main cause of most widespread blackouts in the history of power grids. This will necessitate proper remedial action schemes (RASs) to mitigate intended voltage violations in the forms of undervoltage/overvoltage, as a consequence of such cyberattacks.

B. A Selection of Related Works

1) Cyberattacks Targeting Voltage Profile of Power Grids

In [10], negative impacts of cyberattacks targeting voltage regulation in smart grids integrated with PV generations were studied. Investigation of FDIAs on smart inverter settings was presented in [11], where the impact of the cyberattacks on the operation of smart inverters and also the entire distribution grid was detailed. In [12], the volt-var optimization problem was approached by FDIAs injecting malicious load data into smart meters to cause abnormal voltage profile in a radial medium voltage distribution feeder. In [13], a cyberattack model was proposed to manipulate a phase-locked loop in an inverter-based energy resource. The consequences of the attack introduced in [13] were revenue losses, voltage limit violations/voltage profile

This research was supported in part by the National Science Foundation under Grant No. 2348420.

979-8-3503-5229-0/24/$31.00 ©2024 IEEE

deterioration, and system-wide power-angle instability. In [14], voltage profile in an active distribution grid was compromised via FDIAs, which led to an unacceptable voltage profile throughout the power grid as well as the uncontrolled operation of protective components.

2) Remedial Action Schemes Against FDIAs Causing Voltage Violation

In [15], a reaction mechanism was developed to counter stealthy FDIAs, that targeted tap changing commands in supervisory control and data acquisition (SCADA), pushing the power grid toward an unsecure and abnormal voltage profile. A moving target defense mechanism was introduced in [16] in order to protect a renewable-based lab-scale smart microgrid against FDIAs causing voltage unbalance in real time. A resilient control framework for multiple energy storage systems in islanded microgrids was proposed in [17] for restoring voltage profile due to a cyberattack. In [18], a framework, oriented toward voltage restoration index, was proposed to examine and remediate the stability of microgrids targeted by FDIAs. Using both disconnected generation units and load centers, a complete RAS was introduced in [19] for protecting a failed power grid against cyberattacks that targeted automatic generation control.

C. Knowledge Gap, Research Question, and Contribution of This Work

Although there have been valuable studies on RASs to mitigate the negative impacts of FDIAs targeting smart power grids (e.g., [15]-[19]), the following research question is not yet addressed in the existing literature: *How to implement a customized network reconfiguration to remediate voltage violations caused by a cyberattack targeting ULTCs within distribution systems*?

To precisely address this research question, this paper develops a two-level framework (i.e., cyberattack and the corresponding remedial action) with the following features:

1) Maximizing the rate of voltage deviation in the smart distribution system through manipulating the load data associated with smart meters (i.e., the input information of the volt-var optimization) resulting in voltage violation in both forms of overvoltage and undervoltage, and

2) Proposing an online RAS (OLRAS) to react to cyberattacks in real time via solving a customized distribution feeder reconfiguration (CDFR) with the two objective functions aiming at minimizing the voltage manipulations caused by the attack targeting ULTCs, as well as optimizing the number of switching controls to reach the goal.

II. Developed Framework and Problem Formulation

A. FDIA Targeting Under Load Tap Changing Transformer

The primary objective of volt-var optimization in distribution systems is to control different assets (e.g., ULTC transformers, capacitor banks, voltage regulators, etc.) to keep the voltage profile of the system in the normal range [20]. Generally, the problem can be written in (1)-(3).

$$\min f_{obj}(x,u) \tag{1}$$

Subject to

$$M(x,u) = 0 \tag{2}$$

$$N(x,u) \leq 0 \tag{3}$$

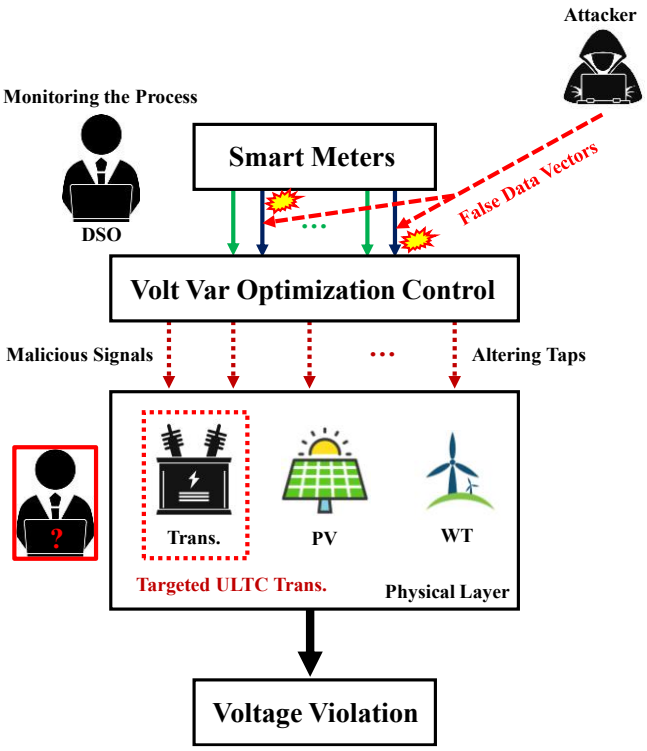

Fig. 1. The developed FDIA framework in this paper.

In (1)-(3), f_{obj} is the objective function of the problem to be minimized; x and u are, respectively, the vector of state variables or dependent variables (i.e., active power output of the generator located at slack bus, reactive power output of generators, voltage magnitude at PQ buses, and the flow of apparent power in branches) and the vector of control variables or independent variables (i.e., magnitude of generator terminal voltage, tap position of ULTC transformers, and reactive power magnitude of buses); M denotes the set of equality constraints (e.g., network active and reactive power equilibrium equations); and N shows the set of inequality constraints (e.g., control variables limits and state variable limits). The objective function of the volt-var optimization problem in this paper is the active power losses of the distribution network. Interested readers are directed to [21] for detailed information about the adopted objective function and the corresponding constraints.

The developed FDIA framework is depicted in Fig. 1. According to this figure, it can be inferred that an attacker takes advantage of the advanced metering infrastructure (AMI) to penetrate into the cyber layer of the distribution system. Then, the attacker launches an FDIA compromising the load data via injecting malicious information to the meters. The falsified data will be the input of the volt-var optimization (i.e., an important part of the distribution management system). Consequently, the results of the volt-var optimization control will be inaccurate. The outcome of the launch of FDIA will be alteration of the tap position of the ULTC transformer. Hence, the magnitude of voltage throughout the distribution system will be intentionally altered. The developed FDIA can be mathematically written in (4)-(6), where $\varphi_{i,t}$ denotes the FDIA's binary variable for ith bus; TP_t indicates the tap position of the ULTC transformer at tth time slot; Υ represents the level of data manipulation; Φ_{max} is the maximum number of compromised meters in the distribution

network; $\Delta P_{i,t}$ and $\Delta Q_{i,t}$ are, respectively, the active and reactive power manipulations for bus i at tth time interval; ξ is the threshold of data manipulation; and S_{rated} is the rated power of the distribution grid.

$$\min \Upsilon \sum_{i=1}^{N_{Bus}} \varphi_{i,t} \pm TP_t \tag{4}$$

$$\varphi_{i,t} \leq \Phi_{max} \tag{5}$$

$$\begin{bmatrix} \Delta P_{i,t} \\ \Delta Q_{i,t} \end{bmatrix} = \xi \times S_{rated} \tag{6}$$

B. Remedial Action Against FDIA Causing Voltage Violation

The expected result of the first phase of the developed framework (see Section II.A) is a compromised voltage profile in the forms of overvoltages, undervoltages, or both. This is where the significance of the second phase of the developed framework comes under the spotlight. Hence, the DSO reacts to the FDIA causing voltage violation via solving a customized distribution feeder reconfiguration (CDFR) problem with two objective functions (the number of switching and the voltage deviation index). As a result, the voltage profile of the targeted system will be improved. Decision variables of the CDFR problem are provided in (7)-(11), where DV is the vector of decision variables of the CDFR problem; $\tilde{V}$ denotes the vector of voltage magnitude after the FDIA; TS indicates the status of tie switches, which are normally open; SS is the vector of sectionalizing switches' status, which are normally closed; and d is the number of decision variables. Thus, changing the status of these switches, the DSO will be able to recognize an optimal configuration of the distribution system such that *a*) the voltage deviation of the system is minimized (see objective function (12)) and *b*) the number of switching processes, needed to achieve the optimal configuration, is minimized to limit the overall cost of the process (see objective function (13)).

$$DV = [\tilde{V}, TS, SW]^T \tag{7}$$

$$\tilde{V} = \left[\tilde{V}_1, \tilde{V}_2, \dots, \tilde{V}_{N_{Bus}}\right]^T_{1\times N_{Bus}} \tag{8}$$

$$TS = \left[TS_1, TS_2, \dots, TS_{N_{TS}}\right]^T_{1\times N_{TS}} \tag{9}$$

$$SS = \left[SS_1, SS_2, \dots, SS_{N_{TS}}\right]^T_{1\times N_{SS}} \tag{10}$$

$$d = N_{Bus} + N_{TS} + N_{SS} \tag{11}$$

The objective functions of the proposed CDFR problem (i.e., the remedial action scheme to react to the FDIA) are presented in (12)-(13), where $V_{i,t}$ is the voltage magnitude of bus i at tth time interval; $S_{s,0}$ is the initial status of the sth switch, which can be either a tie switch or a sectionalizing switch; $S_{s,t}$ is the updated status of switch s at tth time interval; N_S is the total number of switches, which will be equal to $N_{TS} + N_{SS}$; and T indicates the number of time intervals, which will be 24 in this paper for a 24-hour horizon.

$$\min \sum_{t=1}^{T} \sum_{i=1}^{N_{Bus}} \left|V_{i,t} - 1.00\right| \tag{12}$$

$$\min \sum_{t=1}^{T} \sum_{s=1}^{N_S} \left|S_{s,0} - S_{s,t}\right| \tag{13}$$

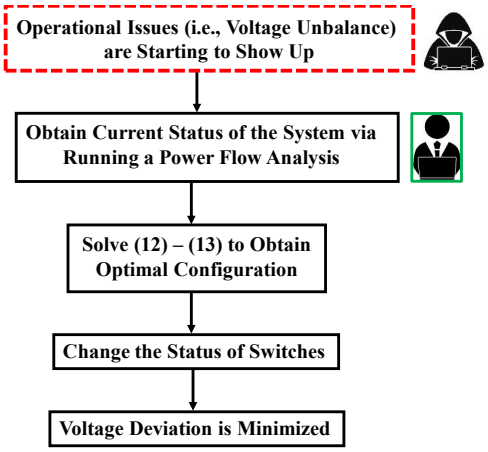

Fig. 2. Flowchart of the proposed OLRAS against FDIA causing voltage violation.

Objective functions (12)-(13) are minimized subject to satisfying a set of equality and inequality constraints. Equality constraints include distribution active and reactive power flow equilibrium and ensuring the radial structure of the network, whereas the inequality constraints consist of distribution line absolute power limit, the switching operation throughout the system, bus voltage limit, transformer current limit, and feeder current limit. Interested readers are directed to [22]-[23] for detailed information about the constraints.

To obtain a better perspective about the proposed remedial action against the developed FDIA (see Fig. 1), Fig. 2 provides a flowchart for the entire process from the DSO's standpoint.

III. Initializations, Simulation Results, and Analyses

A. Initialization

The developed FDIA and the corresponding remedial action against it were coded in MATLAB R2020b. In addition, different sections of the simulations were performed using an Intel Core i7- 13700 machine with 2.10 GHz clock frequency and 32 GB of RAM. It is noted that the power flow analysis was performed via MATPOWER 6.0 [24]. IEEE 33-bus distribution system was opted for demonstrating the negative impacts of the developed FDIAs causing voltage violations and to show the significance of the proposed remedial action scheme to mitigate the impacts of such cyberattacks. The original IEEE 33-bus system was modified to have 4 PV modules and 5 wind turbines (WTs) such that these distributed energy resources are able to supply up to 40% of the overall demand of the system. The demands of the system consist of 3,715 kW active power and 2,300 kVAR reactive power. The remaining parts of the system's information (e.g., the characteristics of the PV modules and WTs integrated into the distribution system, branches data, etc.) was extracted from [25]. The tap positions associated with the only ULTC at the substation level in the IEEE 33-bus system are in the range of [-15, 15] with the step of 0.005. There is also a limit of 5 on the number of tap alterations during each scheduling time interval (i.e., t). It is also noted that the objective functions to be minimized (12)-(13) are normalized via trapezoidal membership functions. Further, the Pareto optimal solutions are recognized via a non-dominated classification process. Interested readers are directed to [26] for detailed information about the normalization process and the Pareto classification.

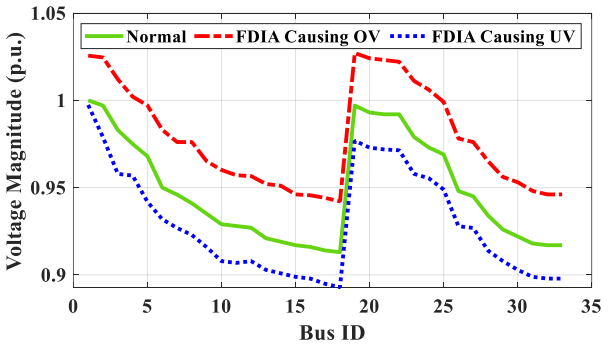

Fig. 3. Voltage profiles of the modified IEEE 33-bus test system in the normal operation and after FDIAs leading to voltage violation at the time of the attack.

TABLE I. DAILY VOLTAGE DEVIATION INDEX OF IEEE 33-BUS SYSTEM BEFORE AND AFTER THE CYBERATTACKS LEADING TO VOLTAGE VIOLATION

	Before Attack	FDIA Leading to OV[1]	FDIA Leading to UV[2]
VDI (p.u.)	25	26.61	26.64

[1] OV: Overvoltage, [2] UV: Undervoltage.

B. Obtained Simulation Results

1) FDIAs Leading to Voltage Violation

The voltage profiles of the IEEE 33-bus test system in the normal operation and after two FDIAs, one leading to overvoltage and the other one leading to undervoltage, are presented in Fig. 3. It is noted that the positive sign in objective function (4) reflects the up-warding movement of the tap position of the ULTC, consequently resulting in higher voltage profile of the distribution system or higher voltage magnitude of the system's buses. Likewise, the negative sign in the objective function (4) refers to a situation in which the tap position of the ULTC moves downward, leading to lower voltage magnitude of the buses. According to Fig. 3, one can infer that by injecting some false load data into the smart meters, the attacker was able to push the voltage profile of the distribution grid toward higher or lower voltages. This will lead to jeopardizing the voltage stability of the distribution system and deteriorating the overall efficiency of the grid.

To obtain a deeper perspective about the impacts of the FDIAs leading to voltage violations, TABLE I provides the overall voltage deviation index (VDI) of the distribution system in a 24-hour horizon before and after the FDIAs. From this table, it can be concluded that the voltage deviation of the IEEE 33-bus system almost remains constant after both attacks; however, the system shows more vulnerability to the FDIA leading to undervoltage (i.e., VDI = 26.64 p.u.) rather than overvoltage (i.e., VDI = 26.61 p.u.).

2) OLRAS to Mitigate the Impacts of FDIAs

The DSO responds to the FDIAs leading to voltage violation via concurrently minimizing objective functions (12)-(13) (i.e., the proposed CDFR problem) aiming at mitigating the affected voltage profile of the distribution system. Fig. 4 displays the Pareto-optimal frontier obtained after minimizing (12)-(13) at the same time. It is noted that the green hexagram represents the best compromise solution (BCS) between objective functions (12)-(13). In addition, TABLE II presents the obtained results for the proposed remediation. It can be inferred from TABLE II that the DSO has been able to react to both cyberattacks in real time (i.e., less than a minute), which highlights the significance of the

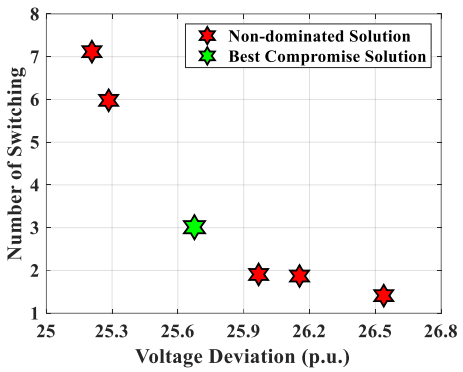

Fig. 4. Non-dominated optimal solutions obtained after minimizing (12)-(13) to react to the FDIA leading to undervoltage.

TABLE II. OBTAINED RESULTS OF THE OLRAS TO MITIGATE THE IMPACTS OF FDIAS

	Before FDIA	Overvoltage		Undervoltage	
		After FDIA	After OLRAS	After FDIA	After OLRAS
VDI (p.u.)	25	26.61	25.59	26.64	25.66
NS[1]	–	–	4	–	3
Execution Time (s)	–	36.4	44.17	35.2	44.05

[1] NS: Number of switching in the process of feeder reconfiguration.

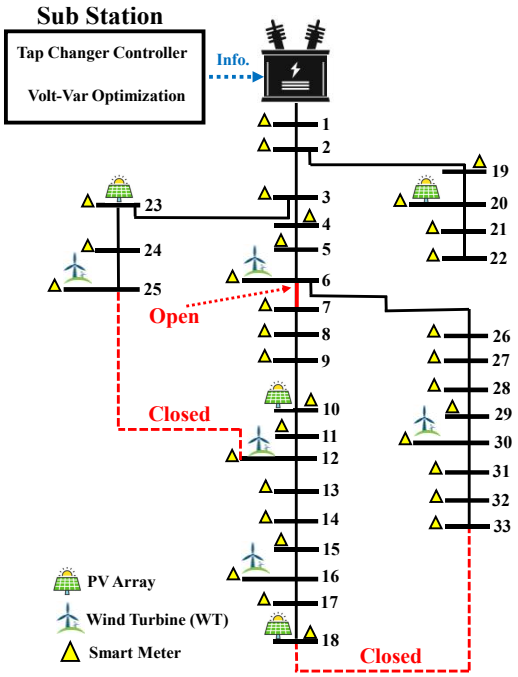

Fig. 5. Configuration of the modified IEEE 33-bus test system after the proposed CDFR to mitigate the FDIA leading to undervoltage (Network has 32 normally closed switches, 1 of which is opened after the OLRAS, and 5 normally open switches, 2 of which are closed after the OLRAS).

proposed OLRAS framework against cyberattacks causing voltage violation.

To obtain a better understanding of the new topology of switches after the proposed CDFR, mitigating the voltage violation, Fig. 5 compares the status of switches before and after solving the proposed CDFR problem as a reaction mechanism to the FDIA leading to the undervoltage scenario (see TABLE II). According to this figure, it can be gathered that after three switching actions, the DSO was able to react to the FDIA

leading to undervoltage only in 44 s, which is quite acceptable as an online reaction to cyber threats in real time.

IV. Conclusion

This paper proposed a customized distribution feeder reconfiguration (CDFR) framework within a remedial action scheme to remediate manipulated voltage violations, caused by FDIAs, targeting ULTC transformers in smart distribution systems. In order to validate the effectiveness of the proposed online remedial action scheme against FDIA, the IEEE 33-bus test distribution system was utilized and modified with PV arrays and wind turbines. Toward that end, the distribution system operator (DSO) was modeled to be in attacker's shoe to run different scenarios of cyberattacks leading to overvoltage and undervoltage through manipulation of the input information of volt-var optimization problem, resulting in subsequent alteration of the tap position of the under-load tap changing (ULTC) transformer located in the substation. Next, the DSO reacted to the FDIAs via solving a CDFR problem in a timely manner to change the configuration of the distribution system and mitigate the voltage deviation. The obtained results verified that such cyberattacks can significantly affect the efficiency of power systems; however, proper remedial actions can restore the targeted system to normal operation. Although there are other communication approaches in the literature, this paper utilized the IEC 61850 communication approach because of its simple implementation and its commonly used application in the power industry.

In the next steps of this research, we will further securitize the proposed remedial action framework, which was validated via simulations in this work, to be demonstrated through experimental validations on a lab-scale smart microgrid integrated with renewable energy resources.

References

[1] T. Huang, B. Wang, J. Ramos-Ruiz, P. Enjeti, P.R. Kumar, and L. Xie, "Detection of cyber attacks in renewable-rich microgrids using dynamic watermarking," *IEEE Power & Energy Society General Meeting (PESGM)*, Montreal, QC, Canada, 2020, pp. 1-5.

[2] V.S. Rajkumar, M. Tealane, A. Ştefanov, A. Presekal, and P. Palensky, "Cyber attacks on power system automation and protection and impact analysis," *IEEE Power and Energy Sociatey Innovative Smart Grid Technologies Europe (ISGT-Europe)*, The Hague, Netherlands, 2020, pp. 247-254.

[3] C. Liu, D. Novosel, J. Monken, "Cybersecurity and resiliency for the power grid leveraging data-driven models and analytics," *IEEE Power & Energy Society General Meeting (PESGM) 8/7 Panel Presentation*, Atalanta, GA, USA, Aug. 2019.

[4] P. J. Pizarro and T. Kuhn, "The U.S. power sector has prevented millions of cyberattacks in 2020 - That takes 24/7 commitment," Edison Electric Institute, 2020. [Online]. Available: https://www.utilitydive.com/news/the-us-power-sector-has-prevented-millions-of-cyberattacks-in-2020-that-t/587949/.

[5] R. K. Knake, "A cyberattack on the U.S. power grid," Council on Foreign Relations, 2017. [Online]. Available: https://www.cfr.org/report/cyberattack-us-power-grid.

[6] M. Basnet and M.H. Ali, "Deep-learning-powered cyber-attacks mitigation strategy in the EV charging infrastructure," *IEEE Power & Energy Society General Meeting (PESGM)*, Orlando, FL, USA, 2023, pp. 1-5.

[7] M. Dezvarei, K. Tomsovic, J.S. Sun, and S.M. Djouadi, "Exploring physical-based constraints in short-term load forecasting: a defense mechanism against cyberattack," *IEEE Power & Energy Society General Meeting (PESGM)*, Denver, CO, USA, 2022, pp. 1-5.

[8] H. Yang, Z. Wang and R.C. Qiu, "Data domain adaptation for voltage stability evaluation considering topology changes," *IEEE Trans. Power Syst.*, vol. 38, no. 3, pp. 2834 – 2844, May 2023.

[9] N. Palukuru, S. Halder nee Dey, T. Datta, and S. Paul, "Voltage stability assessment of a power system incorporating FACTS controllers using unique network equivalent," *Ain. Shams Eng. J.*, vol. 5, no. 1, pp. 103-111, Mar. 2014.

[10] N.G.A. Aysheh, T. Khattab, and A. Massoud, "Cyber-attacks against voltage profile in smart distribution grids with highly-dispersed PV generators: detection and protection," *IEEE Electric Power and Energy Conference (EPEC)*, Edmonton, AB, Canada, 2020, pp. 1-6.

[11] T.O. Olowu, S. Dharmasena, H. Jafari, and A. Sarwat, "Investigation of false data injection attacks on smart inverter settings," *IEEE CyberPELS (CyberPELS)*, Miami, FL, USA, 2020, pp. 1-6.

[12] D. Choeum and D.-H. Choi, "OLTC-induced false data injection attack on Volt/VAR optimization in distribution systems," *IEEE Access*, vol. 7, pp. 34508-34520, Mar. 2019.

[13] A. Bamigbade, Y. Dvorkin, and R. Karri, "Cyberattack on phase-locked loops in inverter-based energy resources," *IEEE Trans. Smart Grid*, Early Access, 2023, doi: 10.1109/TSG.2023.3270348.

[14] M. Ahmadzadeh, A. Abazari, and M. Ghafouri, "Detection of FDI attacks on voltage regulation of PV-integrated distribution grids using machine learning methods," *IEEE Electrical Power and Energy Conference (EPEC)*, Victoria, BC, Canada, 2022, pp. 73-78.

[15] S. Chakrabarty and B. Sikdar, "Detection of hidden transformer tap change command attacks in transmission networks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5161-5173, Nov. 2020.

[16] E. Naderi, A. Asrari, and B. Ramos, "Moving target defense strategy to protect a PV/Wind lab-scale microgrid against false data injection cyberattacks: experimental validation," *IEEE Power & Energy Society General Meeting (PESGM)*, Orlando, FL, USA, 2023, pp. 1-5.

[17] C. Deng, Y. Wang, C. Wen, Y. Xu, and P. Lin, "Distributed resilient control for energy storage systems in cyber–physical microgrids," *IEEE Trans. Ind. Inform.*, vol. 17, no. 2, pp. 1331-1341, Feb. 2021.

[18] S. Liu, Z. Hu, X. Wang, and L. Wu, "Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks," *IEEE Trans. Ind. Inform.*, vol. 15, no. 7, pp. 4066-4075, Jul. 2019.

[19] R. Tan *et al*., "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 7, pp. 1609-1624, Jul. 2017.

[20] R.R. Jha, S. Poudel, P. Sharma, A. Dubey, and K.P. Schneider, "Volt/var optimization (VVO) application on GridAPPS-D platform," *IEEE Power & Energy Society General Meeting (PESGM)*, Orlando, FL, USA, 2023, pp. 1-5.

[21] H. Mataifa, S. Krishnamurthy, and C. Kriger, "Volt/var optimization: a survey of classical and heuristic optimization methods," *IEEE Access*, vol. 10, pp. 13379-13399, Jan. 2022.

[22] A. Azizivahed *et al*., "Multi-objective dynamic distribution feeder reconfiguration in automated distribution systems," *Energy*, vol. 147, pp. 896-914, Mar. 2018.

[23] A. Azizivahed *et al*., "A hybrid evolutionary algorithm for secure multi-objective distribution feeder reconfiguration," *Energy*, vol. 138, pp. 355-373, Nov. 2017.

[24] MATPOWER Package. [Online]. Available: https://matpower.org/.

[25] A. Asrari, E. Naderi, J. Khazaei, P. Fajri, and V. Cecchi, "Modern heat and electricity incorporated networks targeted by coordinated cyberattacks for congestion and cascading outages," in *Coordinated Operation and Planning of Modern Heat and Electricity Incorporated Networks*, IEEE, Piscataway, NJ, USA, 2022.

[26] E. Naderi, L. Mirzaei, J.P. Trimble, and D.A. Cantrell, "Multi-objective optimal power flow incorporating flexible alternating current transmission systems: application of a wavelet-oriented evolutionary algorithm," *Electr. Power Compon. Syst.*, vol. 52, no. 5, pp. 766-795, 2024.