Semarak Engineering Journal

Journal homepage:
https://semarakilmu.my/index.php/sej/index
ISSN: 3036-0145

Modelling and Impact Analysis of Two-Stage Intelligent Voltage Stability Cyber Attack Method in Power Grid

Ali Taghavi[1], Mohsen Gitizadeh[1,*], Jamshid Aghaei[2], Ghassan A. Bilal[3], Mohammed K. Al-Saadi[3]

[1] Department of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz, Iran
[2] School of Engineering and Technology, Central Queensland University, Rockhampton, Queensland, Australia
[3] University of Technology-Iraq, Electromechanical Engineering Department, Baghdad, Iraq

ARTICLE INFO

Article history:
Received 12 August 2025
Received in revised form 13 January 2026
Accepted 12 February 2026
Available online 14 April 2026

Keywords:

Power systems; Cyber security; Microgrid; Voltage stability

ABSTRACT

A continuous and reliable supply of electric power is crucial for power grid consumers. However, power grids face a growing threat from cyberattacks targeting their stability and causing widespread disruption. This paper proposes a novel Two-Stage Intelligent Voltage Stability (TIVS) attack model. The TIVS model takes advantage of the knowledge of attackers of vulnerabilities of the power grid. It manipulates a variable within the Voltage Stability Index (VSI) calculation. This manipulation aims to maximize disruption to the stability of the grid while minimizing the chance of detection. The model employs a two-stage approach. In the first stage, the attacker selects the amount of manipulation. The second stage, informed by the first, allows the grid to operate for cost optimization while keeping the manipulated variable fixed. Interestingly, information from this stage feeds back into the first stage, potentially aiding further manipulation by the attacker. The effectiveness of the TIVS model is compared to a traditional False Data Injection (FDI) attack through a case study on the IEEE 24-bus test system with interconnected microgrids. The TIVS attack causes a considerable increase in the cost of power grid, demonstrating its superior disruptive capabilities.

1. Introduction

Ensuring a reliable and secure flow of electric power to consumers is the fundamental goal of the power systems [1]. To achieve this, there has been significant interest in examining the stability conditions of power grids, especially regarding voltage stability. Recently, research on voltage stability and voltage collapse has drawn more attention from researchers. This surge in research is driven by their role in triggering major blackouts, as seen in events like those that occurred in Italy, India, and the Philippines [2].

A power system is considered voltage unstable if it cannot maintain acceptable voltage levels at all buses within the grid, both under normal conditions and after disruptions [3]. Voltage instability can lead to a cascading series of events, which force the protective relays to trip components of the

* *Corresponding author.*
E-mail address: gitizadeh@sutech.ac.ir

https://doi.org/10.37934/sej.13.1.199207

grid. This can result in load shedding or even widespread blackouts [4]. Considering the significant risks posed by voltage instability, cyber attackers prioritize exploiting this vulnerability to disrupt the power systems. The rise of information and communication technologies (ICT) has revolutionized power systems. These systems have become more efficient through the implementation of computer-based control and monitoring. While the integration of advanced technologies has offered impactful advantages, it has also introduced new vulnerabilities to the power system [5].

The integrity of communications, control, and energy management systems is increasingly vulnerable to cyberattacks, which can have destructive consequences. Over the past few years, the modeling and impact analysis of various types of cyber-attacks have been investigated in literature. Xu *et al.,* [6] show the analysis of the dynamic and static effect of cyber-attacks on the power system in three key areas: economic dispatch, state estimation, and control systems. The impact of False Data Injection (FDI) attacks on reliable operations for power systems is illustrated by Liu et al., [7]. Xiang et al., [8] present a bilevel Load Redistribution (LR) attack model based on operational responsiveness. Ding *et al.,* [9] illustrated a new hybrid cyber-attack against the heating and electrical systems of IES. Gu *et al.,* [10] suggested a hybrid model incorporating both sides of the attacker and operator. The researchers examine a coordinated cyber-attack on both heat and power grids. They analyzed the potential risks and devastating consequences of this attack. Liang, Gaoqi *et al.,* [11] reviewed the impact of incorrect data on modern electronic systems. Building on this, Y. Mo *et al.,* explored how FDI attacks can manipulate energy exchange within the power grid [12]. F. Pasqualetti *et al.,* in [13] provide a comprehensive review of FDI attacks, highlighting the potential for these attacks to lead to poor decision-making in grid operation if left undetected. Finally, O. Kosut *et al.,* [14] examined cyberattacks that aim to manipulate meter readings through smart devices.

Based on open literature, there is a critical need for an intelligent model that comprehensively investigates the effects of cyber-attacks targeting voltage stability in power grids. To achieve more realistic results, this model not only simulates the behavior of the grid under attack but also incorporates models of the attacker's goals and the decision-making processes of the operator of the power grid. By modeling these attacker motivations and operator responses, the intelligent model can provide a richer understanding of potential vulnerabilities and evaluate the impact of cyberattacks on the power grid with greater accuracy.

1.1 Motivation and Aims

Power system voltage instability poses considerable risks to grid reliability and security. This paper is motivated by the need to address these risks by proposing a new cyber-attack model that leverages voltage stability vulnerabilities. Traditional cyber-attack models are susceptible to two main drawbacks. Some are easily detectable due to obvious alterations to systems. Conversely, others, due to their limited modifications, cannot cause significant damage. This work aims to develop a more sophisticated approach that exploits the attacker's knowledge of the power grid to launch intelligent attacks.

This paper has two primary aims: 1) Develop a Two-Stage Intelligent Voltage Stability Index Attack Model (TIVS), where this model will incorporate intelligence by considering both attacker goals and power grid operational behavior. 2) Optimize the TIVS Model, where the model will be designed to maximize the objective function of the attacker, which considers both maximizing the negative impact on the grid and minimizing the chance of detection.

2. Methodology

In this section, the formulation of the models and grid under study are addressed comprehensively to obtain the results. These results will be analyzed to verify the effectiveness of the proposed approach.

1.2 Proposed Power Grid Model

To analyze the effectiveness of proposed cyber-attack models, a model of the power grid itself is essential. This paper investigates the formulation of the power grid model with consideration of some technical and operation constraints to make the scenario close to a real one. The analysis is applied to a specific 24-bus IEEE test system, which included connected microgrids via a transformer on bus 6 as shown in Figure 1.

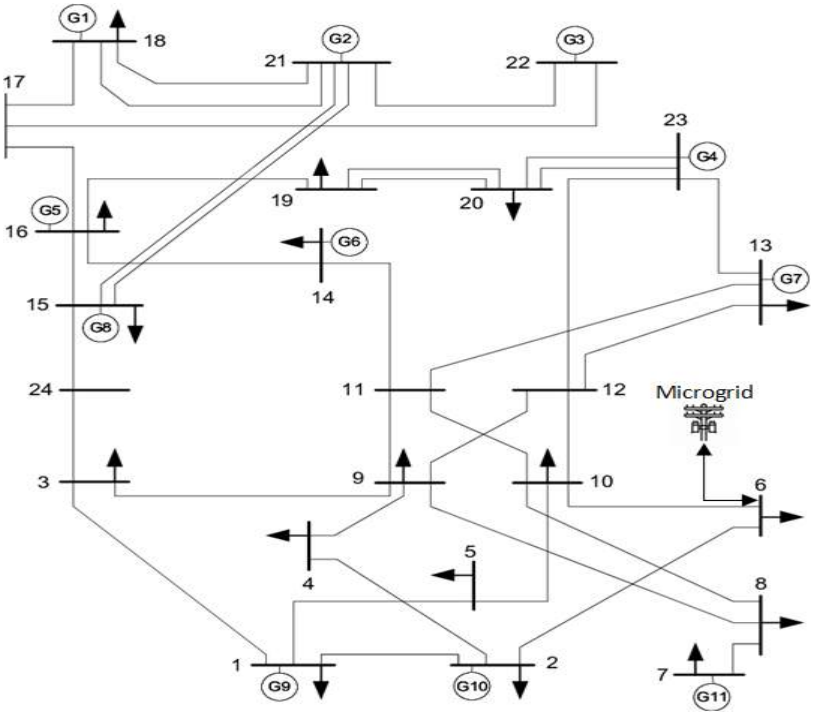

Fig. 1. 24-bus IEEE test system

Given the primary objective of evaluating a proposed attack model, this research employs a linearized power flow approach to simplify the complexity of the power grid problem [15]. The active and reactive power flowing through the lines are represented by Eqs. (1) and (2). By incorporating Eqs. (3), (4), and (5), can derive Eqs. (6) and (7). Further simplification leads to Eqs. (8) and (9).

$$P^L_{(a,t)} = V^2_{(i,t)} g_a - V_{(i,t)} V_{(j,t)} (g_a cos\delta_{(a,t)} + b_a sin\delta_{(a,t)}) \quad (1)$$

$$Q^L_{(a,t)} = -V^2_{(a,t)} (b_a + b_a 0) + V_{(i,t)} V_{(j,t)} (b_a cos\delta_{(a,t)} - g_a sin\delta_{(a,t)}) \quad (2)$$

$$\cos \delta_{a,t} \approx 1 \quad (3)$$

$$\sin \delta_{(a,t)} \approx \delta_{(a,t)} \quad (4)$$

$$V_{(i,t)} = 1 + \Delta V_{(i,t)} \quad (5)$$

$$P^L_{(a,t)} \approx (1 + 2\Delta V_{(i,t)}) g_a - (1 + \Delta V_{(i,t)} + \Delta V_{(j,t)})(g_a + b_a \delta_{(a,t)}) \quad (6)$$

$$Q^{L}_{(a,t)} \approx -(1+2\Delta V_{(i,t)})(b_i + b_{0a}) + (1+\Delta V_{(i,t)} + \Delta V_{(j,t)})(b_a - g_a \delta_{(a,t)}) \quad (7)$$

$$P^{L}_{(a,t)} = (\Delta V_{(i,t)} - \Delta V_{(j,t)}) g_a - b_a \delta_{(a,t)} \quad (8)$$

$$Q^{L}_{(a,t)} = -(1+2\Delta V_i) b_{0a} - (\Delta V_{(i,t)} - \Delta V_{(j,t)}) b_a - g_a \delta_{(a,t)} \quad (9)$$

Eqs. (10) and (11) set the maximum and minimum power output allowed for the generators within the power grid. Additionally, Eqs. (12) to (15) address different limitations: maintaining a balance between the amount of active and reactive power flowing through the grid (Eqs. 12-13). and staying within the capacity limits of the transmission lines (Eqs. 14-15).

$$P^{Gen\_Min}_{(i)} u^{Gen}_{(i,t)} \le P^{Gen}_{(i,t)} \le P^{Gen\_Max}_{(i)} u^{Gen}_{(i,t)} \quad (10)$$

$$Q^{Gen\_Min}_{(i)} u^{Gen}_{(i,t)} \le Q^{Gen}_{(i,t)} \le Q^{Gen\_Max}_{(i)} u^{Gen}_{(i,t)} \quad (11)$$

$$\sum_{i=1}^{num\_gen} P^{Gen}_{(i,t)} - \sum_{a=1}^{num\_line} P^{L}_{(a,t)} = P^{load}_{(i,t)} - P^{sheding}_{(i,t)} - P^{MG\_Trans}_{(i,t)} \quad (12)$$

$$\sum_{i=1}^{num\_gen} Q^{Gen}_{(i,t)} - \sum_{a=1}^{num\_line} Q^{L}_{(a,t)} = Q^{load}_{(i,t)} \quad (13)$$

$$P^{Line\_Min}_{(a)} \le P^{L}_{(a,t)} \le P^{Line\_Max}_{(a)} \quad (14)$$

$$Q^{Line\_Min}_{(a)} \le Q^{L}_{(a,t)} \le Q^{Line\_Max}_{(a)} \quad (15)$$

Eqs. (16) and (17) define the acceptable ranges for voltage levels and bus angles within the power grid, which are crucial for maintaining voltage stability.

$$\Delta V^{Min} \le \Delta V_{(i,t)} \le \Delta V^{Max} \quad (16)$$

$$\delta^{Min} \le \delta_{(a,t)} \le \delta^{Max} \quad (17)$$

Eq. (18) captures the total cost associated with operating the power grid. This cost incorporates several factors, such as fuel and maintenance costs for power generation (generator production costs), the costs incurred when power plants are activated or deactivated (entering and exiting costs), and the penalty associated with unmet electricity demand (Expected Energy Not Served (EENS)). The generator production costs for each power plant are calculated using a non-linear quadratic equation [16]. The following Equation details the calculation of the EENS cost, which considers the amount of active power that might be shed due to insufficient supply (Eq. 19).

$$\mathrm{Cost} = [\sum_{i=1}^{num\_gen} \sum_{t=1}^{T} \mathrm{Cost}(P^{G}_{(i.t)}) + C^{On\_gen}_{(i,t)} + C^{off\_gen}_{(i,t)}] + ENS\_\mathrm{cost} \quad (18)$$

$$ENS\_\mathrm{cost} = M \times [\sum_{i=1}^{num\_buss} \sum_{t=1}^{T} P^{Sheding}_{(i,t)}] \quad (19)$$

2.2 Attack Model

For a cyber attacker targeting a power system, success is measured by two key factors: maximizing disruption and minimizing costs. In other words, attackers achieve this mission by exploiting vulnerabilities and targeting weak points in the system while keeping their attack methods as cost-effective as possible while remaining undetected. As discussed earlier, the voltage stability of a power system becomes an attractive target for attackers because it represents a significant

vulnerability. In a power grid, voltage stability monitoring indexes are a cornerstone technique for assessing the condition of a power system. These indexes are designed to increase or decrease critical values as the system approaches instability. Several well-established voltage stability monitoring indexes exist which include the Fast Voltage Stability Index (FVSI) [17], Line stability [18], and Voltage Stability Index (VSI). VSI provides a trusted method for monitoring voltage stability within power systems [19]. As shown in Eq. (20), the VSI calculation considers the power injected into a specific bus within the grid as the main factor that affects the value of VSI. This value typically ranges between 0 and 1, providing a clear interpretation: a value closer to 0 indicates a stable system, while a value approaching 1 suggests a risk of voltage collapse.

$$VSI = \frac{2 \times S_{(i,t)} \times X_i (1 + \sin \delta_{(i,t)})}{V_{(i,t)}^2} \quad (20)$$

As mentioned in Eq. (12), Power injection into a bus can be obtained from different sources such as energy generators, grid lines, and connected microgrids power exchange. All these sources influence the voltage stability of the bus. Any malicious change in these values can lead to a significant change in VSI and cause it to increase value to critical value 1. In the proposed cyber-attack model, the attacker aims to manipulate the power grid by maximizing a VSI. This manipulation relies on influencing a variable within the system while minimizing any detectable changes to avoid getting caught. As previously discussed, the VSI can be manipulated by three methods. Notably, microgrid devices emerge as a more critical vulnerability compared to other power grid components due to their easier accessibility for attackers [20]. Leveraging this vulnerability, this paper focuses on manipulating which affects the VSI calculation to achieve our objectives. The two-stage attack model can be formulated by employing Eqs. (21) to (24), where both the operational behavior of the power grid and the attacker's objectives are taken into account when formulating the model.

First Stage

Objective function: Maximizing Eq. (20) (21)

Subject to:

$$-\beta \times P_{(i,t)}^{MG\_Trans} \leq \Delta P_{(i,t)}^{attack} \leq \beta \times P_{(i,t)}^{MG\_Trans} \quad (22)$$

Second stage

Objective function: Minimizing Eqs. (18) (23)

Subject to:

Eqs. (10)-(17) (24)

This two-stage intelligence VSI (TIVS) attack model framework aims to achieve maximum disruption (high VSI) while remaining undetected (minimal) in the first stage. This aligns with the goal of the attacker. In the second stage, the manipulated value is fixed, allowing the power grid to be operated for cost optimization, which is the operator of the grid's typical objective. Interestingly, the information from the second stage feeds back into the first stage, informing VSI calculations and potentially enabling manipulation by the attacker.

3. Results

To evaluate the effectiveness and impact of the proposed TIVS attack model, a case study on the standard 24-bus IEEE test system is presented, which incorporates interconnected microgrids.

The first stage of the TIVS model calculation leverages Particle Swarm Optimization (PSO) implemented within MATLAB 2023a. The specific parameters used for the PSO algorithm are detailed in Table. 1. The second stage, which simulates power grid operation, is calculated using GAMS software.

Table 1
PSO Hyperparameter

Tuning parameters	*value*
Inertia Weight (w)	0.9 to 0.1
Cognitive Learning Coefficient (c1)	2
Social Learning Coefficient (c2)	2
Number of particles (swarm size)	15
Maximum velocity:	$0.25 \times \beta \times P_{(i,t)}^{MG\_Trans}$
Maximum number of iterations	70

Figures 2 and 3 depict the results of the Optimal Power Flow (OPF) analysis conducted on the test power grid. It illustrates the normal operating values of some decision variables and the power grid total cost for the case study. It can be seen that some of the generators at certain hours are uncommitted due to their high operating cost and the load can be supplied by other sources. Microgrids and the main grid are able to exchange power. They can buy power during peak demand or outages, and sell excess renewable energy back when prices are high. This creates a dynamic local energy market driven by real-time electricity prices [18].

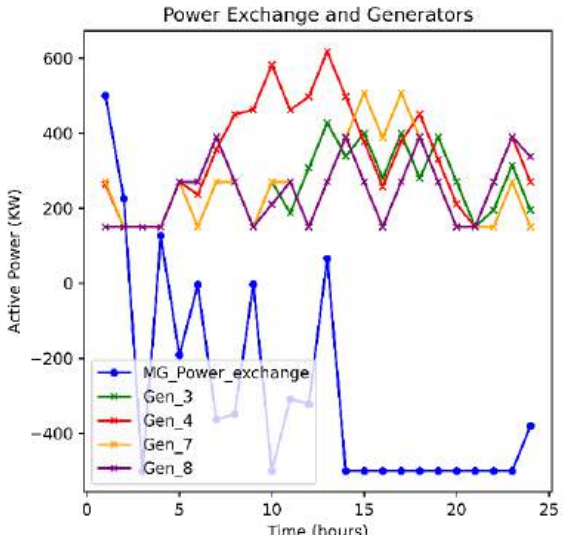

Fig. 2. Power exchange and generators' active power

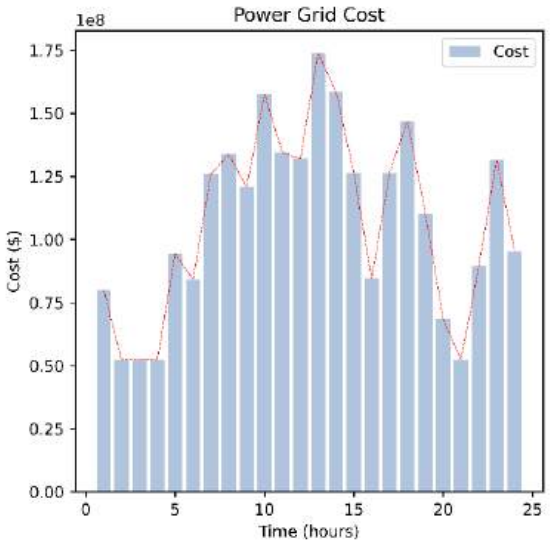

Fig. 3. Power gird cost

Figure 3 depicts the optimal magnitude of the Time-Varying TIVS attack over 24 hours. It is noteworthy that due to the model's intelligent design, the attacker strategically chooses not to

launch attacks during certain hours. This implies that the potential cost incurred by the attacker would not justify an attack at those specific times. In essence, the proposed TIVS attack model identifies critical junctures where manipulating microgrid power exchange can significantly increase costs for the power grid operator. These strategic moments are the ones chosen for launching the attack.

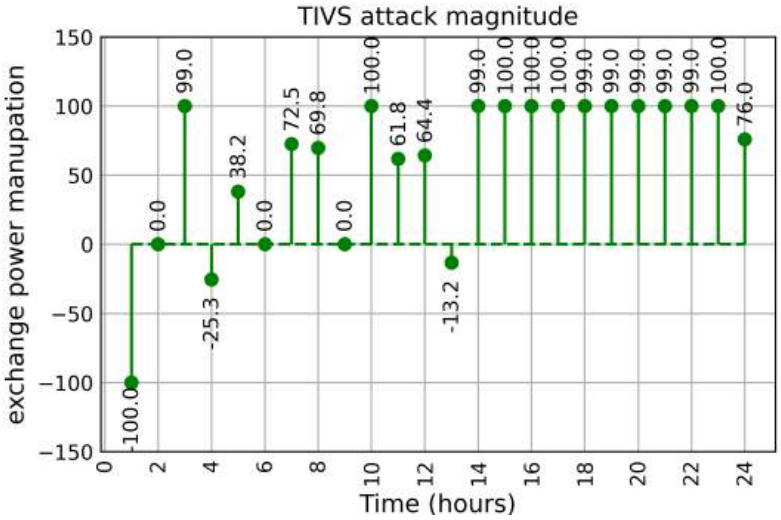

Fig. 4. TIVS attack magnitude

To assess the effectiveness of the proposed TIVS attack model on power grid performance, Figure 4 compares the results with a traditional FDI attack targeting the microgrid power exchange variable [21]. It illustrates the power grid VSI incurred over 24 hours under these two attack scenarios and normal conditions. The TIVS attack caused an 18.93% increase in VSI compared to normal conditions. This increase is 8.93% greater than that observed with a traditional FDI attack (10.00% increase).

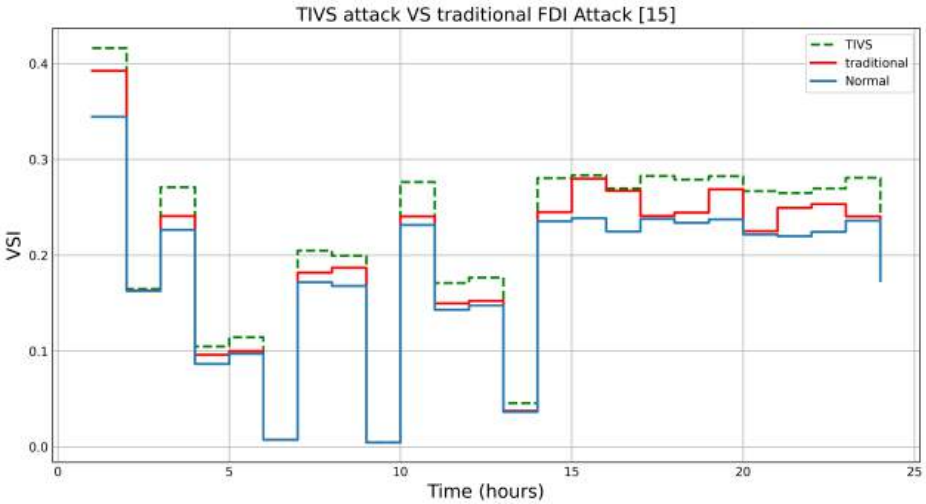

Fig. 4. TIVS attack Vs traditional FDI attack

4. Conclusions

This study investigated the potential impact of a novel TIVS attack model on power grid performance. Our research brings to light the following novel findings: 1) Two-stage attack strategy: The proposed TIVS attack model leverages a two-stage approach. In the first stage, the attacker strategically manipulates a within the VSI calculation to maximize disruption while minimizing detection. The second stage fixes the manipulated and allows the grid to operate for cost optimization. Interestingly, information from this stage feeds back into the first stage, which could potentially aid in first-stage manipulation. 2) Intelligent attack timing: The TIVS model considers the cost-benefit of attacker analysis. The model strategically chooses not to launch attacks during certain hours when the potential cost would not justify an attack. The validation results with a traditional attack demonstrated the effectiveness of the TIVS model. The case study on the IEEE 24-bus test system with interconnected microgrids showcased the impact of the TIVS attack on power grid costs. The results were obtained using PSO for the first-stage calculation in MATLAB and GAMS software for the second-stage power grid operation simulation. These findings highlight the importance of considering power grid vulnerabilities and the potential for sophisticated cyber-attacks that exploit stable conditions. Future work could propose an approach for real-time detection of intelligent cyberattacks. This approach would explore mitigation strategies to enhance power grid resilience against such attacks. Additionally, future research could investigate the effect of cyber-attacks from a microgrid perspective, exploring their potential role in improving grid resilience.

References

[1] Ghafouri, Mohsen, Minh Au, Marthe Kassouf, Mourad Debbabi, Chadi Assi, and Jun Yan. "Detection and Mitigation of Cyber Attacks on Voltage Stability Monitoring of Smart Grids." IEEE Transactions on Smart Grid 11, no. 6 (2020): 5227-38. https://doi.org/10.1109/TSG.2020.3004303.

[2] Gomes, P. "New Strategies to Improve Bulk Power System Security: Lessons Learned from Large Blackouts." In IEEE Power Engineering Society General Meeting, 2004., 1703-1708 Vol.2, 2004. https://doi.org/10.1109/PES.2004.1373163.

[3] Vittal, Vijay, James D. McCalley, Paul M. Anderson, and A. A. Fouad. Power System Control and Stability. John Wiley & Sons, 2019. https://books.google.com/books?hl=en&lr=&id=obCuDwAAQBAJ&oi=fnd&pg=PR15&dq=%5BBOOK%5D+Power+system+control+and+stability&ots=LD-wzpfJFY&sig=4Hygu60fVJJrUY599ylEig0Inc0.

[4] Ajjarapu, Venkataramana, ed. "Continuation Power Flow." In Computational Techniques for Voltage Stability Assessment and Control, 49-116. Power Electronics and Power Systems. Boston, MA: Springer US, 2007. https://doi.org/10.1007/978-0-387-32935-2_3.

[5] Tu, Haicheng, Yongxiang Xia, K. Tse Chi, and Xi Chen. "A Hybrid Cyber Attack Model for Cyber-Physical Power Systems." IEEE Access 8 (2020): 114876-83. https://doi.org/10.1109/ACCESS.2020.3003323

[6] Huang, Lei, Jian Xu, Yuanzhang Sun, Ting Cui, and Fei Dai. "Online Monitoring of Wide-Area Voltage Stability Based on Short Circuit Capacity." In Asia-Pacific Power and Energy Engineering Conference, 1-5. IEEE Computer Society, 2011. https://www.computer.org/csdl/proceedings-article/appeec/2011/05747730/12OmNx76TJF. https://doi.org/10.1109/APPEEC.2011.5747730.

[7] Liu, Lanchao, Mohammad Esmalifalak, Qifeng Ding, Valentine A. Emesih, and Zhu Han. "Detecting False Data Injection Attacks on Power Grid by Sparse Optimization." IEEE Transactions on Smart Grid 5, no. 2 (March 2014): 612-21. https://doi.org/10.1109/TSG.2013.2284438.

[8] Xiang, Yingmeng, Zhilu Ding, Yichi Zhang, and Lingfeng Wang. "Power System Reliability Evaluation Considering Load Redistribution Attacks." IEEE Transactions on Smart Grid 8, no. 2 (March 2017): 889-901. https://doi.org/10.1109/TSG.2016.2569589.

[9] Ding, Shixing, Wei Gu, Shuai Lu, Ruizhi Yu, and Lina Sheng. "Cyber-Attack against Heating System in Integrated Energy Systems: Model and Propagation Mechanism." Applied Energy 311 (April 1, 2022): 118650. https://doi.org/10.1016/j.apenergy.2022.118650.

[10] Gu, Wei, Shixing Ding, Shuai Lu, Pengfei Zhao, Dehu Zou, Yue Qiu, Ruizhi Yu, and Lina Sheng. "Coordinated Heat and Power Cyber-Attacks With Time Window Matching Strategy." IEEE Transactions on Smart Grid 14, no. 4 (July 2023): 2747-61. https://doi.org/10.1109/TSG.2023.3273710.

[11] Liang, Gaoqi, et al. "A review of false data injection attacks against modern power systems." IEEE Transactions on Smart Grid 8.4 (2016): 1630-1638.https://doi.org/10.1109/TSG.2015.2495133

[12] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in Preprints of the 1st workshop on Secure Control Systems, pp. 1-6, 2010.

[13] F. Pasqualetti, F. D¨orfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715-2729, 2013. https://doi.org/10.1109/TAC.2013.2266831

[14] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 645-658, 2011. https://doi.org/10.1109/TSG.2011.2163807

[15] Sheikh, Morteza, Jamshid Aghaei, Armin Letafat, Mohammad Rajabdorri, Taher Niknam, Miadreza Shafie-Khah, and João PS Catalão. "Security-Constrained Unit Commitment Problem with Transmission Switching Reliability and Dynamic Thermal Line Rating." IEEE Systems Journal 13, no. 4 (2019): 3933-43. https://doi.org/10.1109/JSYST.2019.2939210

[16] Nikoobakht, Ahmad, Mohammad Mardaneh, Jamshid Aghaei, Victoria Guerrero-Mestre, and Javier Contreras. "Flexible Power System Operation Accommodating Uncertain Wind Power Generation Using Transmission Topology Control: An Improved Linearised AC SCUC Model." IET Generation, Transmission & Distribution 11, no. 1 (January 5, 2017): 142-53. https://doi.org/10.1049/iet-gtd.2016.0704.

[17] Modarresi, Javad, Eskandar Gholipour, and Amin Khodabakhshian. "A Comprehensive Review of the Voltage Stability Indices." Renewable and Sustainable Energy Reviews 63 (2016): 1-12. https://doi.org/10.1016/j.rser.2016.05.010

[18] Moghavvemi, Mahmoud, and F. M. Omar. "Technique for Contingency Monitoring and Voltage Collapse Prediction." IEE Proceedings-Generation, Transmission and Distribution 145, no. 6 (1998): 634-40. https://doi.org/10.1049/ip-gtd:19982355

[19] Rana, Md Masud, Li Li, and Steven W. Su. "Cyber Attack Protection and Control of Microgrids." IEEE/CAA Journal of Automatica Sinica 5, no. 2 (March 2018): 602-9. https://doi.org/10.1109/JAS.2017.7510655.

[20] Jiang, Quanyuan, Meidong Xue, and Guangchao Geng. "Energy Management of Microgrid in Grid-Connected and Stand-Alone Modes." IEEE Transactions on Power Systems 28, no. 3 (August 2013): 3380-89. https://doi.org/10.1109/TPWRS.2013.2244104.

[21] Yuan, Yanling, Zuyi Li, and Kui Ren. "Quantitative Analysis of Load Redistribution Attacks in Power Systems." IEEE Transactions on Parallel and Distributed Systems 23, no. 9 (2012): 1731-38. https://doi.org/10.1109/TPDS.2012.58