A Over-Review Report On Risks of Cyber Security & Electrical Systems

Er. Kailash Chandra Senapati, Er. Anil Kumar Sahoo, Er. Sonali Sasmita Tripathy

* Department of Electrical Engineering, Swami Vievakananda School of Engineering & Technology, Chaitanya Prasad, Madanpur, Bhubaneswar, Khordha-752054
Email id- kailashchnadrasenapati@gmail.com
** Department of Electrical Engineering, Swami Vievakananda School of Engineering & Technology, Chaitanya Prasad, Madanpur, Bhubaneswar, Khordha-752054
Email id- anilkumar.sahoo@rediffmail.com
*** Department of Electrical Engineering, Swami Vievakananda School of Engineering & Technology, Chaitanya Prasad, Madanpur, Bhubaneswar, Khordha-752054
Email id- sonalitripathy95@gmail.com

ABSTRACT

Due to the rapid disconnection of smart devices and less integrated communication devices, electrical devices are at risk of serious cybersecurity issues. This paper reviews existing studies to reflect the impact of false data input attacks on power systems from three aspects. Firstly, the inclusion of false data can negatively affect the economic loss by increasing the operating cost of the electrical system or causing an overload of subsequent and inclusive loads. Second attackers can detect false data in the power system state estimator, which means that operators will not obtain the correct operating conditions of the system. In this case, false data entry attacks could degrade the distribution control of distributed or microcurrent generators, causing a power imbalance between supply and demand. This document fully covers potential vulnerabilities of energy systems and cyber attacks to help system operators understand the system vulnerability and take effective countermeasures.

Keywords- Cyber-security, Potential Vulnerabilities, Cyber-Attacks, Micro-Current Generators

INTRODUCTION

Due to their extensive integration of information and communication technologies, energy systems are exposed to cyber threats. By attacking the information sharing process, malicious attackers can inject fake data and cause power outages, financial losses, and system instability. False data injection (FDI) can also be used to hide existing faults in the electrical system. This will affect the operator's visibility of the faults and prevent appropriate countermeasures from being taken. For example, in 2015, Ukraine's power grid was attacked and malicious entities opened substation circuit breakers [1]. To design appropriate protective measures that improve system resilience, it is necessary to explore how FDI affects the power system. Therefore, much research has been carried out on the attack mechanism and effects of FDI. Generally, the ways in which FDI negatively affects a power system can be classified into three categories, namely, estimating system states, generating control commands, and executing control actions, as shown below: shown in Figure 1.

FDI can induce the generation of inappropriate control orders by directly targeting economic dispatch. In [2, 3], false load data is injected into the safety-constrained economic dispatch, causing line flows to exceed their overload triggering threshold, leading to line outages and even cascading failures. In [4,5,6], the economic allocation is intentionally affected to increase the operating cost or to make illegal profits in the energy markets. In [7], the potential risk of FDI attacks on economic distribution is studied when attackers do not have complete knowledge of network information. FDI can also penetrate a power system by attacking the measurement and estimation of the system state and damaging the integrity of power system state information. In [8], FDI is used as a tool to attack the supervisory control and data acquisition (SCADA) system, while in [9], fake data is injected into the phasor measurement unit (PMU) to fool the control center.

By doing so, cyber attackers can affect the operator's visibility into the true operational state of the system, preventing them from taking appropriate countermeasures. In [10, 11], FDI is used to induce arbitrary estimation errors of the state estimator, while in [12,13,14,15] FDI is applied to the estimation of the state estimator. non-linear state of the electrical system and analyze the corresponding countermeasures. . Furthermore, IEDs can modify the control input of the system, causing a deterioration in the stability of the electrical system. In [16], the input signal of a follower distributed generator is corrupted by FDI, causing disagreements between a group of distributed generators. In [17], the FDI is used to induce a synchronization problem for isolated microgrids, while the system circuit breakers are controlled to cause instability in [18], and the gains of the voltage control devices are varied to initiate a transient instability in [17]. 19].]. In [20], a malicious attack is implemented using emulated inertial control to cause system frequency instability.

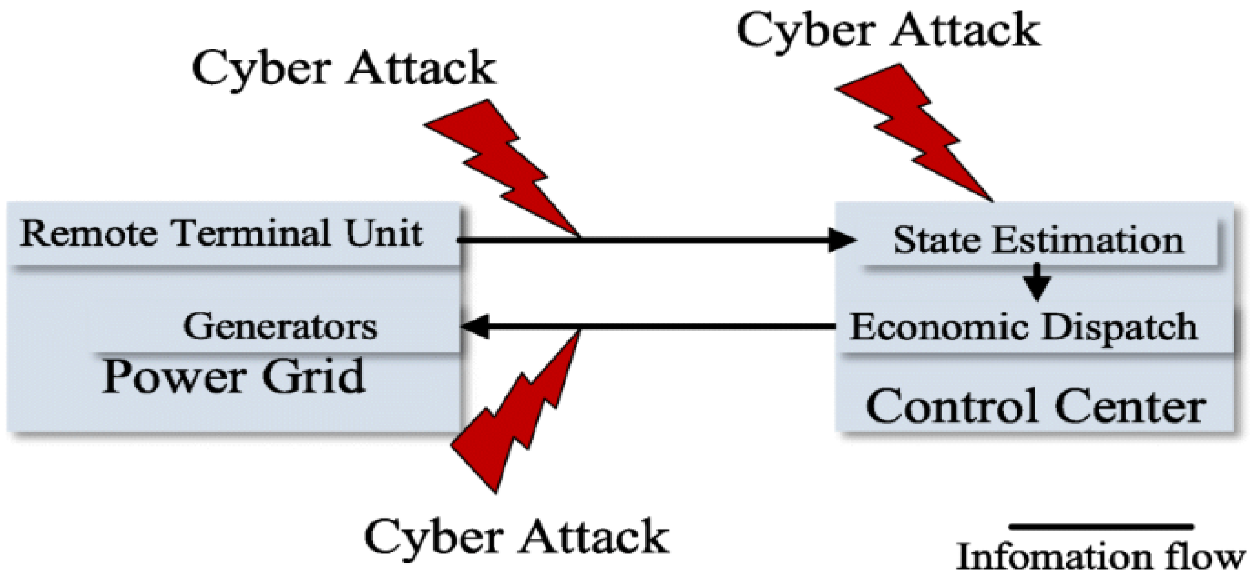


Fig-1

Currently, research on the impact of FDI is mainly based on the single instantaneous FDI model and/or the steady-state power system model; Research that considers the temporal process of an energy system is neither exhaustive nor exhaustive. Intelligent attackers can modify the injected data at each point of the attack to avoid detection or reduce power consumption during the attack process. Since real power systems are networked control systems, using the steady-state power system model is also not sufficient to analyze the FDI risk. Although the system state estimation and economic dispatch are resistant to FDI, attackers can still disrupt the secure operation of the power system by attacking the automatic generation control system. Therefore, it is very important to take into account the dynamic characteristics of foreign direct investment and the temporal characteristics of the power system to fully reveal the risk of foreign direct investment and then design effective countermeasures.

2 ATTACKS ON ECONOMIC DISTRIBUTION

In a real power system, generators are activated every 5 to 15 minutes to minimize operating costs. The load data adopted for Security Constrained Economic Dispatch (SCED) comes from short-term load forecasts that use historical and/or real-time load measurement values as input. False data that can pass Bad Data Detection (BDD) can be deliberately injected to alter SCED load information and disrupt the enforcement of flow limits.

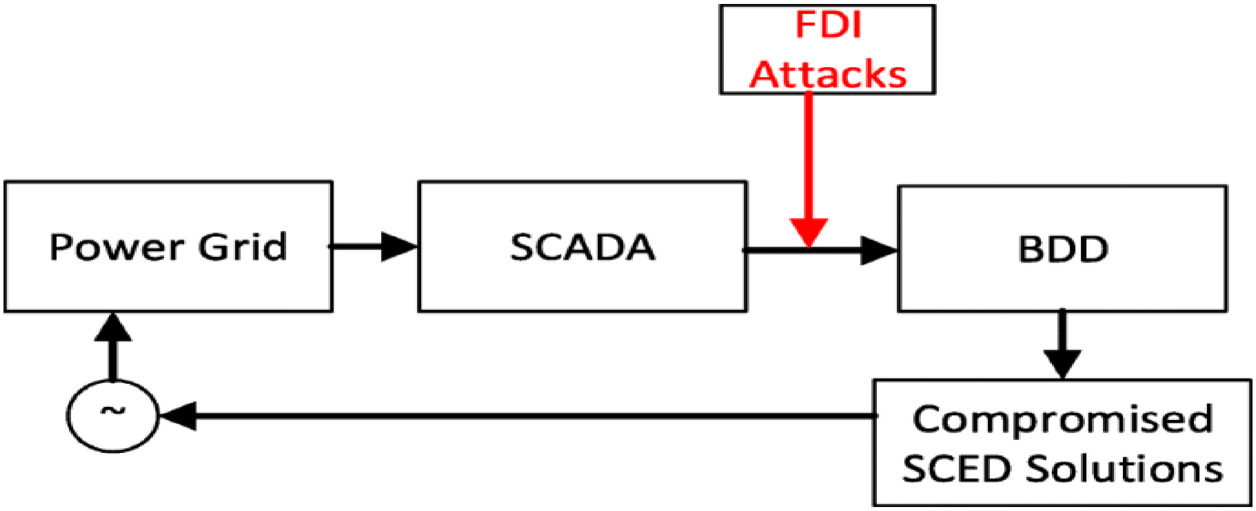


Fig-2

3-ATTACKS ON THE ESTIMATION OF THE STATE OF THE ELECTRICITY SYSTEM

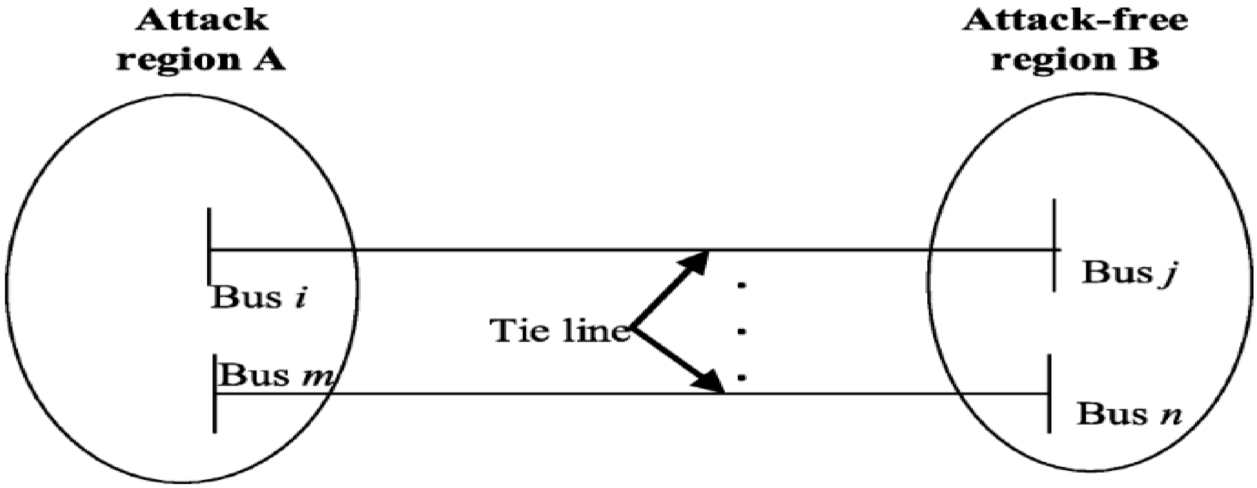
For a modern power system, many smart devices are deployed to acquire real-time data related to its operation. By leveraging this measurement data, operators can monitor the operational status of the system and take effective actions to mitigate potential risks. However, measurements must be transmitted to the control center via communications links and therefore power systems face potential cyberattacks due to the vulnerability of communication technologies. For example, a malicious agent can inject false data to trick operators into making poor decisions about the state of the system.

4-FDI ATTACK WITH INCOMPLETE NETWORK INFORMATION

It also requires attackers to have the topological information of the entire power grid as well as the line parameters. However, power grid information is sensitive and attackers will likely have a difficult time obtaining it. In addition, a modern electrical system has thousands of buses and lines. This means that attackers must manage a large amount of information about the network topology. Therefore, the assumption that attackers can acquire the estimated values from the state estimation is not practical. To build a practical attack model against state estimation, the above conditions are relaxed in [11], in which the false data injection model only requires the network information of the attack region (see Fig. 3). instead of that of the entire electrical network. . Furthermore, the attack vector in [11] does not depend directly on phase angle estimates but on line angle differences. The FDI attack model used in [11] is reformulated through the following steps:

1. Replace the measured voltages with estimates of the voltage magnitudes at the limit bars in the driving region

2. Replace the estimates of voltage magnitudes and phase angles with the corresponding measurements to determine the fluxes in the bond lines.



By doing the above, the estimated state of the system is no longer necessary in the design of the attack vector. The phase angles on the border buses in the attack region play an essential role in the implementation of the mentioned attack model. Although the PMU can access phase angle measurements, this would require the deployment of enough PMUs to provide this information, and such solutions can be difficult to scale. To successfully launch an IED attack against a power system without sufficient PMU data, it is desirable for attackers to build a more practical attack model without requiring measured phase angle values.

5-CONCLUSION

With the rapid development of smart grids and the widespread use of information and communications technologies in traditional power grids and microgrids, the energy sector is facing cyber threats. This article has conducted extensive research on the potential risks of fake data injection attacks on power systems. State-of-the-art models and methods are reviewed to explain how attackers could attack the system by injecting fake data. First, an attack vector can be constructed by solving a linear programming problem and false data is injected to significantly increase the operating cost of the power system. Economic distribution can also be negatively affected if optimal attacks against FDI are designed and an initial contingency is triggered, which consequently triggers sequential shocks. Second, an undetectable improvised explosive device (IED) attack can be designed to disrupt the power system state estimate. Such an attack can be launched using the complete/local information of the network. Third, frequency instability can be caused by the injection of false data that prevents the active power output of an inverter from following its dispatch command.

REFFERENCE:

1- Liang, G., Zhao, J., Luo, F. J., Weller, S., & Dong, Z. (2017). A review of false data injection attacks against modern power systems. IEEE Transactions on Smart Grid, 8(4), 1630–1638.
2- Che, L., Liu, X., Shuai, Z., Li, Z., & Wen, Y. (2018). Cyber cascades screening considering the impacts of false data injection attacks. IEEE Transactions on Power Apparatus and Systems, 33(6), 6545–6556.
3- Che, L., Liu, X., Li, Z., & Wen, Y. (2019). False data injection attacks induced sequential outages in power systems. IEEE Transactions on Power Apparatus and Systems, 34(2), 1513–1522.
4- Yuan, Y., Li, Z., & Ren, K. (2011). Modeling load redistribution attacks in power systems. IEEE Transactions on Smart Grid, 3(3), 382–390.
5- Liu, X., Li, Z., Shuai, Z., & Wen, Y. (2017). Cyber attacks against the economic operation of power system: A fast solution. IEEE Transactions on Smart Grid, 8(2), 1023–1025.
6- Xiang, Y., Ding, Z., Zhang, Y., & Wang, L. (2017). Power system reliability evaluation considering load redistribution attacks. IEEE Transactions on Smart Grid, 8(2), 889–901.
7- Liu, X., & Li, Z. (2014). Local load redistribution attacks in power systems with incomplete network information. IEEE Transactions on Smart Grid, 5(4), 1665–1676.
8- Zhang, Y., Wang, L., Xiang, Y., & Ten, C. (2015). Power system reliability evaluation with SCADA cybersecurity considerations. IEEE Transactions on Smart Grid, 6(4), 170–1721.
9- Zhang, Z., Gong, S., Dimitrovski, A., & Li, H. (2013). Time synchronization attack in smart grid: Impact and analysis. IEEE Transactions on Smart Grid, 4(1), 87–98.

10- Kosut, O., Jia, L., Thomas, R., & Tong, L. (2011). Malicious data attacks on the smart grid. IEEE Transactions on Smart Grid, 2(4), 645–658.

11- Liu, X., & Li, Z. (2017). False data attacks against ac state estimation with incomplete network information. IEEE Transactions on Smart Grid, 8(5), 2239–2248.

12- Zhao, J., Zhang, G., Dong, Z., & Wong, K. (2016). Foresting-aided imperfect false data injection attacks against power system nonlinear state estimation. IEEE Transactions on Smart Grid, 7(1), 6–8.

13- Zhao, J., Mili, L., & Wang, M. (2018). A generalized false data injection attacks against power system nonlinear state estimator and countermeasures. IEEE Transactions on Power Apparatus and Systems, 33(5), 4868–4877.

14- Deng, R. L., Zhuang, P., & Liang, H. (2019). False data injection attacks against state estimation in power distribution systems. IEEE Transactions on Smart Grid, 10(3), 2871–2881.

15- Bi, S., & Zhang, Y. (2014). False data injection attacks with limited susceptance information and new countermeasures in smart grid. IEEE Transactions on Smart Grid, 15(3), 1619–1628.

16- Liu, Y., Xin, H., Qu, Z., &Gan, D. (2016). An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks. IEEE Transactions on Smart Grid, 7(6), 2923–2932.

17- Abhinav, S., Modares, H., Lewis, F., Ferrese, F., &Davoudi, A. (2018). Synchrony in networked microgrids under attacks. IEEE Transactions on Smart Grid, 9(6), 6731–6741.

18- Liu, S., Mashayekh, S., Kundur, D., Zourntos, T., &Bulter-Purry, K. (2012). A smart grid vulnerability analysis framework for coordinated variable structure switching attacks, (pp. 1–6). San Diego: Proc. IEEE PES. Gen. Meeting.

19- Chen, B., Mashayekh, S., Butler-Purry, L., &Kundur, D. (2013). Impact of cyber attacks on transient stability of smart grids with voltage support devices, (pp. 1–5). Vancouver: Proc. IEEE PES Gen. Meeting.

20- Brown, H., & DeMarco, C. (2018). Risk of cyber-physical attack via load with emulated inertia control. IEEE Transactions on Smart Grid, 9(6), 5854–5866.