INTERNATIONAL JOURNAL • ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

IJIEMR Transactions, online available on 10th Apr 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 04

10.48047/IJIEMR/V12/ISSUE 04/54

Title **ANALYSIS OF FALSE DATA INJECTION ATTACKS ON OPTIMAL POWER FLOW IN POWER SYSTEMS**

Volume 12, ISSUE 04, Pages: 454-461

Paper Authors

Akula Venkata Naresh Babu, A.Vamsi Krishna, D.Divya, G.Bhargavi, A.Venkatesh,D.Rakesh Babu

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Analysis of False Data Injection Attacks on Optimal Power Flow in Power Systems

Akula Venkata Naresh Babu[1], Professor, Department of EEE,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.
A.Vamsi Krishna[2], **D.Divya**[3], **G.Bhargavi**[4], **A.Venkatesh**[5],**D.Rakesh Babu**[6]
[2,3,4,5,6] UG Students, Department of EEE,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.
[1]avnareshbabu@gmail.com,[2]vamsikrishnaakula2@gmail.com,[3]devarapallidivya91@gmail.com,[4]19BQ5A048@vvit.net,[5]venkateshannaparthy@gmail.com,
[6]rb54077@gmail.com

Abstract

A cyber-energy system develops when the degree of connectivity between information and energy increases. Communication networks are carrying an increasing amount of data, and if a cyber system malfunctions or behaves strangely, the flaw might spread over space to affect the entire system. In contemporary power systems, data of sensors is sent to the control centres across lengthy communication lines. The analysis of data is done there and used by different optimization or control methods for the planning, operation, and scheduling of power systems. These networked systems are susceptible to cyberattacks since the communication channels are not protected and the data is not secured. In this paper, the communication line carrying data from power sensors to the control centres underwent an analysis of the fake data injection (FDI) attack. The measurements of branch power flows and load demand are contained in this data, which is then further examined and used to calculate the optimal power flow (OPF). With regard to load and line flows for common test systems, a susceptibility evaluation OPF under FDI attacks has been discussed.

Keywords: Optimal power flow, Cyber attacks, False data injection, ISEA, Cyber security.

Introduction

A cyber attack is any attempt to gain unauthorized access to a computer, computing system, or computer network with the goal of doing harm. A cyber attack's objectives include changing, blocking, deleting, altering, or stealing data from a computer system as well as disrupting, destroying, or seizing control of it. Antivirus software and firewalls are no longer effective in stopping cyber threats. Cyberattack risk is always rising, and for businesses and organisations, the issue is now "when" rather than "if" an attack will

take place. Because of this, cyber security is very crucial. Cybersecurity is significant because it covers all aspects of safeguarding our data from online thieves who wish to steal it and exploit it for malicious purposes[1, 8]. They include vulnerable information in the Power Grid, sensitive data, information from the public and private sectors, personal information, personally identifiable information, intellectual property, and protected health information.

The digitalization of the contemporary electricity system has been hastened by the development of information and communication technologies. Better operational efficiency, grid flexibility, simplicity of integrating renewables, and load involvement in demand-side management have all been brought about through grid modernization[2]. Also, it has made it possible for extensive geographical monitoring and measurement, device network connectivity, and automation inside and across crucial systems.

To reduce the risk of cyber-attacks on the power grid, it is essential to employ appropriate security measures. These measures can include the use of encryption and authentication technologies, as well as implementing security protocols for all devices connected to the power grid[3-5]. Additionally, regular security assessments and testing can help to identify and address vulnerabilities in the system.

For system planning and operation, control centres in contemporary power systems heavily rely on optimum power flow (OPF) studies[6–9]. An OPF research identifies the state and control variables that, while taking into account transmission network restrictions and power balancing equations, reduce the total producing cost. OPF guarantees secure and economical system operation. By changing a few selected sensor measurements before they are transmitted to the control centers, this study creates an FDI attack to deceive the OPF algorithm[10]. The effects of FDI attacks on the OPF algorithm have been investigated using a simple 2-bus system for comprehensibility and an IEEE 14-bus system for authenticity. The document is structured as shown below. In Section II, an outline of ideal power flow is provided. Section III provides a description of the threat model. Before the article is ended in Section V, Section IV presents case studies on the IEEE 14-bus system.

Optimal Power Flow

Optimal Power Flow (OPF) is an important matter in electrical power systems. It is a mathematical optimization problem that aims to determine the optimal settings for power system control variables, such as generator output levels, transformer tap settings, and capacitor and reactor switch positions, in order to minimize the overall cost of generating and transmitting electrical power while satisfying operational constraints. The primary objective of OPF is to ensure the reliable and efficient operation of power systems by minimizing the overall cost of power generation and transmission while ensuring that the power system operates within operational constraints such as voltage limits, thermal limits, and network constraints.

Overall, the optimal power flow matter is crucial for ensuring the efficient and reliable operation of power systems, reducing operational costs, and promoting sustainable development. The OPF of power system can be calculated by using the conventional method like newton method or else by using the optimization algorithms like intellegance search evolution algorithum (ISEA) [11].

Evolutionary algorithms are a class of computational techniques inspired by the principles of natural selection and genetics. They are used to solve optimization problems that involve searching for the best solution among a large number of possible solutions. Intelligence search evolution algorithm is a type of evolutionary algorithm that is used for optimization. Intelligence search evolution algorithms use a population-based search approach, where a population of candidate solutions is evolved through successive generations. Each candidate solution is represented as a set of parameters, and the algorithm uses a fitness function to evaluate the quality of each candidate solution.

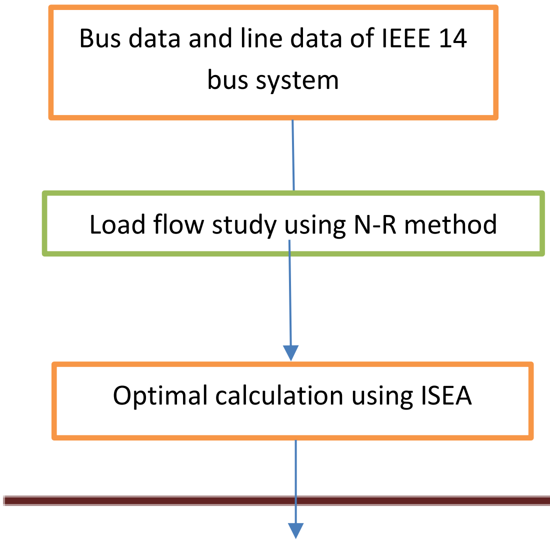
Bus data and line data of IEEE 14 bus system
Load flow study using N-R method
Optimal calculation using ISEA

Fig. 1. Flow chart of ISEA for OPF.

The cost equations and constraints are considered from ref.[11].

False Data Injection Model

The unencrypted transfer of sensor data to control centres is a recognised weakness in contemporary power systems that may be exploited by cyber-attacks. False data injection (FDI) attacks can be initiated by intruders who inject forged data into communication channels using hijacked routers to get beyond traditional bad data detectors. The branch power flows (B) and load demand (D) are two examples of manipulated data that might be used as inputs to the OPF algorithm and result in power system disturbances.

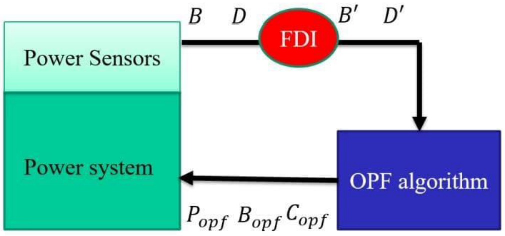

Fig. 2. Threat model of FDI attack on power system with OPF algorithum.

By sending fake data through the communication channel that transmits branch power flows and load demand to the control centre, the attacker may attempt to fabricate the load demand in the power system during an attack on the communication channel. The determined optimal operating level would be sustandard if the bogus load demand were supplied into the OPF algorithm. This would result in higher operational expenses or even load that isn't met. In order to escape detection, the attack is designed such that the system's overall load change doesn't surpass 50%, simulating typical load changes. The attacker has to be able to read and write line power flows and have access to branch parameters and cost models for generators, in order to compromise the OPF of the power system. The attacker can create an attack vector that modifies the branch MW/MVA limit or adjusts the load demand (D) in such a way that it raises the hourly cost of energy generation. The attack vector can be created in one of two ways: by modifying both the line flows and the total load, or by dispersing the line flows while maintaining the net load. The attack vector's redistribution pushes the more expensive generator to meet the load demand, increasing operational costs.

Results

FDI attacks can have a significant impact on the performance of the OPF algorithm and the overall power system. By falsifying inputs, the algorithm may be misled to operate the system at a suboptimal level, resulting in higher electricity generation costs. The total cost of power generation before and after the attack has been compared in order to assess the effect of FDI attacks on the system. If the attack results in a higher cost, it indicates that the system is operating at a suboptimal level. Additionally, ensure that the FDI attack does not push the system beyond its safe operating limits. Therefore, the effect of FDI attacks on the power flow limits of individual branch has been monitored which determine the maximum amount of power that can be transmitted through each line. If the attack causes the branch power flow limits to be exceeded, it can lead to system instability and potential power outages.

In order to visualise the effects of an FDI on the OPF solutions and system performance, a case study utilising an IEEE 14 bus system is explored. According to ISEA algorithm calculations, the IEEE 14 bus system performs at its best under typical circumstances. According to Fig. 3, the IEEE 14 bus system has 20 lines, 4 load buses, 4 generator buses, and 1 slack bus.

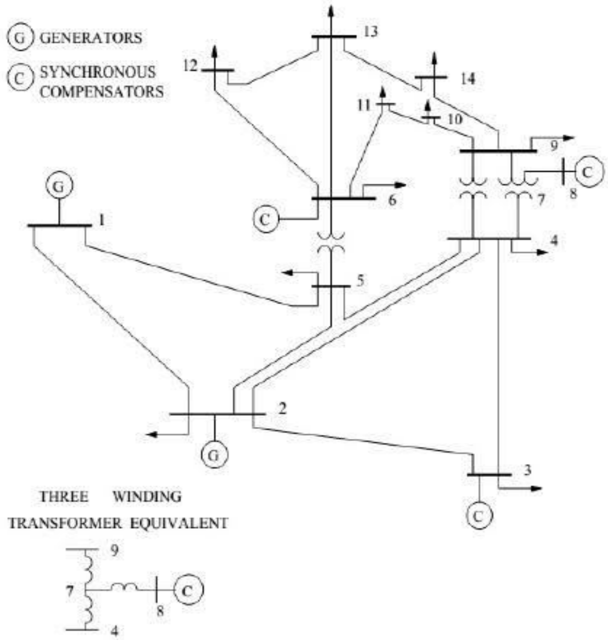

Fig. 3. IEEE 14 bus system diagram

Case 1: Base Case

The base case is the initial case in which there is no cyber attack on the system. In the base case with the help of line data and bus data, by using the ISEA algorithum the OPF results are calculated.

The Table1 consists voltage magnitude in per unit and phase angle for all the 14 buses are shown for the normal condition (base case). The Table2 shows the power flows in the different line of the IEEE 14 bus system under normal condition. The Table3 shows the OPF results and it consists of generation of each individual generator as well as total generation, total losses and total cost of generation per hour.

Table 1: Bus voltages of IEEE 14 bus system.

Bus no	Voltage magnitude (p.u)	Angle (rad)
1	1.0382	0.0000
2	1.0283	-1.1166
3	1.0043	-6.1591
4	1.0000	-3.9774
5	1.0047	-3.0506
6	1.0000	-3.4446
7	1.0219	-3.6881
8	1.0389	-0.3590
9	0.9876	-5.7094
10	0.9816	-5.6407
11	0.9866	-4.7050
12	0.9845	-4.5230
13	0.9790	-4.7221
14	0.9725	-6.2487

Table 2: Power Flows of IEEE 14 bus system.

Line	From	To bus	Power
number	bus		flow (MVA)
1	1	2	37.1012
2	1	5	28.1178
3	2	3	46.6787
4	2	4	31.7679
5	2	5	22.9308
6	3	4	20.2085
7	4	5	38.2183
8	4	7	24.8581
9	4	9	6.0996
10	5	6	18.0564
11	6	11	11.6344
12	6	12	8.5613
13	6	13	20.8479
14	7	8	36.0990
15	7	9	45.8105
16	9	10	6.7802
17	9	14	8.6357
18	10	11	7.9188
19	12	13	2.1267
20	13	14	8.2023

Table 3: OPF results

S.no	Parameter	Values
1	G1	64.229MW
2	G2	85.341MW
3	G3	30.129MW
4	G6	48.097MW
5	G8	35.001MW
6	Total generation	262.796MW
7	Total losses	3.796MW
8	Generation cost	888.627 $/h

Case 2: False Data Injection with respect to Buses

There will be load present on every bus. In this case, the load at bus 2 is changed because as compared to load at all the buses the load at bus 2 is high so the 5% load at bus 2 is changed i.e from 94.2MW to 98.5MW. The OPF results under this condition are given in Table 4,5 and 6.

Table 4: Bus Voltage of IEEE 14 bus system under FDI

Bus no	Voltage magnitude (p.u)	Angle (rad)
1	1.0642	0.0000
2	1.0525	-1.2381
3	1.0168	-6.4580
4	1.0242	-4.1058
5	1.0327	-3.2312
6	0.9970	-3.7799
7	1.0358	-3.6959
8	1.0543	-0.0572
9	1.0048	-5.8482
10	0.9954	-5.8221
11	0.9923	-4.9790
12	0.9829	-4.8353
13	0.9790	-5.0408
14	0.9744	-6.6345

Table 5: Power Flows of IEEE 14 bus system under FDI condition.

Line number	From bus	To bus	Power flow (MVA)
1	1	2	43.5392
2	1	5	30.4073
3	2	3	51.7469
4	2	4	33.1743
5	2	5	23.4498
6	3	4	23.2278
7	4	5	41.5497
8	4	7	21.3138
9	4	9	6.9897
10	5	6	6.9375
11	6	11	9.6540
12	6	12	8.0999
13	6	13	19.2501
14	7	8	40.5097
15	7	9	46.3729
16	9	10	10.5213
17	9	14	11.2123
18	10	11	7.1196
19	12	13	1.7238
20	13	14	6.9609

Table 6: OPF results under FDI condition.

S.no	parameter	Values
1	G1	73.169MW
2	G2	86.150MW
3	G3	25.339MW
4	G6	43.445MW
5	G8	39.343MW
6	Total generation	267.445MW
7	Total losses	4.145MW
8	Generation cost	913.110 $/h

By comparing the OPF results under FDI attack on bus data condition with the base case results, it has been observed that the cost of generation is increase i.e under normal condition the cost of generation is 888.627 $/h but under attack scenario it changed to 913.110 $/h. the generation on each individual generator are also changed the losses in the system are increased from 3.796MW to 4.145MW. If they go over the thresholds that might overload the lines and the buses, the power flows and voltages of the buses are also altered.

Case 3: False Data Injection with respect to Lines.

Not only w.r.t bus, the FDI attack can be done in the lines also. The OPF results for FDI attack on line data has been analyzed. In this, It has been considered the line 12-13 and the resistance of line 12-13 is changed to 5% i.e from 0.22092 to 0.209874 and the results are given in Table 7,8 and 9.

Table 7: Bus Voltage of IEEE 14 bus system under FDI

Bus no	Voltage magnitude (p.u)	angle(rad)
1	1.0937	0.0000
2	1.0656	-0.8092
3	1.0197	-5.0637
4	1.0356	-3.7814
5	1.0380	-2.9516
6	1.0443	-4.6516
7	0.9865	-3.8078
8	0.9958	-0.7472
9	0.9825	-5.7586
10	0.9853	-5.8541
11	1.0104	-5.3637
12	1.0255	-5.6066
13	1.0170	-5.6782
14	0.9784	-6.8318

Table 8: Power Flows of IEEE 14 bus system under FDI.

Line number	From bus	To bus	Power flow (MW)
1	1	2	54.0029
2	1	5	35.7271
3	2	3	46.3620
4	2	4	35.3157
5	2	5	27.4391
6	3	4	16.0300
7	4	5	34.5495
8	4	7	0.4289
9	4	9	7.9031
10	5	6	36.5556
11	6	11	17.1401
12	6	12	9.3833
13	6	13	23.5404
14	7	8	30.1075
15	7	9	30.2671
16	9	10	3.5349
17	9	14	6.1834
18	10	11	12.5329
19	12	13	3.0376
20	13	14	11.4100

Table 9:OPF results under FDI.

S.no	parameter	Values
1	G1	71.694MW
2	G2	87.634MW
3	G3	35.521MW
4	G6	38.903MW
5	G8	29.775MW
6	Total generation	263.527MW
7	Total losses	4.527MW
8	Generation cost	898.809 $/h

`In this case also the cost of generation and the total losses on the system are increased which are calculated based on the data change w.r.t lines. The cost of generation is changed from 888.627 $/h to 898.809 $/h and also losses are increased by 0.731MW. Due to this attack, the power flows and the voltage magnitudes also increased which increases the losses in the system.

Conclusion

The operation of the power system can be significantly impacted by FDI attacks on the Optimal Power Flow algorithm. By using line data and load data as two attack channels, the study looked at the impact on the power system under FDI assaults. The study assessed how FDI assaults affected OPF using the IEEE 14-bus system. The study's findings demonstrate that the OPF algorithm causes the system to operate below optimally when subjected to FDI assaults.

Attacks like this can make energy generation more expensive overall or force the company to take expensive and disruptive corrective measures like load shedding or breaker tripping.

References

[1] A. Ameli, A. Kirakosyan, K. A. Saleh, and E. F. El-Saadany, "Vulnerabilities of line current differential relays to cyber-attacks,"IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp.1–5, 2019.

[2] Y. Wu, B. Chen, J. Weng, Z. Wei, X. Li, B. Qiu, and N. Liu, "False load attack to smart meters by synchronously switching power circuits", IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 2641–2649, 2019.

[3] H. Zhang, B. Liu, and H. Wu, "Net load redistribution attacks on nodal voltage magnitude estimation in ac distribution networks", in 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), pp. 46– 50, 2020.

[4] Du Z, Chen J, Zhang Y, et al."Multi-objective routing optimization for electric power communication network considering business importance",3rd Asia energy and electrical engineering symposium (AEEES). IEEE; p.p 959–63,

2021.

[5] Li B, Lu C, Qi B, et al. 1."Risk and traffic based service routing optimization for electric power communication network",Int J Electr Power Energy Syst vol.137,2022.

[6] Zhu W, Milanovi JV, Weiskopf D, "Assessment of the robustness of cyber-physical systems using small- worldness of weighted complex networks", Int J Electr Power Energy Syst vol.125,2021.

[7] Xun J, Xiao Y, Lu W,"Reliability assessment of regional integrated energy system based on complex network theory", Electric Power Constr. Vol.41,no.4,pp.1-9,2020.

[8] Pan K, Teixeira A., Cvetkovic M., & Palensky P. "Cyber risk analysis of combined data attacks against power system state estimation". IEEE Transactions on Smart Grid, 10(3), 3044–3056,2019.

[9] A. Murray, M. Kyesswa, P. Schmurr, H. C Akmak, and V. Hagenmeyer, "On grid partitioning in ac optimal power flow," IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe),pp. 524–528, 2020

[10] J. Liu, H. Zhang, W. Qiao, and L. Qu, "DC optimal power flow-based models for simulation and mitigation of overload cascading failures," North American Power Symposium (NAPS),pp. 1–5, 2019.

[11] A V Naresh Babu, T Ramana, S Sivanagaraju "Analysis of optimal power flow problem based on two stage initialization algorithm" International Journal of Electrical Power & Energy Systems 55,p.p 91-99, 2014.