2021 IEEE PES Innovative Smart Grid Technologies - Asia (ISGT Asia) | 978-1-6654-3339-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISGTASIA49270.2021.9715641

Vulnerability Assessment of False Data Injection Attacks on Optimal Power Flow

Rajvir Kaur, Justin Albrethsen, David K.Y. Yau, and Shahram Ghahremani
Singapore University of Technology and Design, Singapore
rajvirsidhu8@gmail.com, {justin_albrethsen, david_yau, shahram_ghahremani} @sutd.edu.sg

***Abstract*—In modern power systems, sensor data is transmitted over long communication lines to the control centers. There, data is analysed and utilized by various optimization or control algorithms for power system planning, operation, and scheduling. The communication lines are not secured and the data is not encrypted, which makes these networked systems vulnerable to cyber-attacks. In this paper, the false data injection (FDI) attack is launched on the communication line transmitting power sensor data to the control centers. This data carries the measurements of load demand, and branch power flows, which is further analysed and input to the optimal power flow (OPF) algorithm. The attack vectors are designed to manipulate the line power flows. We present a vulnerability assessment of FDI attacks against OPF using case studies of IEEE 2-bus and 37-bus power systems.**

***Index Terms*—OPF, Smart Grid, FDI Attack, Cyber Security**

I. Introduction

The advancement in information and communication technologies (ICT) has accelerated the digitization of the modern power system. Modernization of the grid has resulted in higher operational efficiencies, grid resilience, ease of renewable integration, and load participation in demand-side management [1]. Moreover, it has enabled monitoring and measurement in widespread geographical areas, network connectivity among devices, and automation within and between key systems [2]. However, networked devices and the bidirectional flow of data has made the modern grid vulnerable to cyber-attacks.

Recent literature has shown the feasibility of false data injection (FDI) attacks in modern power systems [3]. FDI attacks can compromise a system's integrity by injecting forged data into monitoring or control loops. Tan et. al. [4] modelled a stealthy FDI attack on sensor measurements for automatic generation control (AGC), resulting in frequency excursions. These excursions then may cause unmet load, generator tripping, or equipment damage in the system. Another case study investigates vulnerability in line current differential relays, whose operation is dependent on communication infrastructure and the global positioning system [5]. In this case, a coordinated FDI attack may cause unintentional tripping of the relays.

Modern power systems rely on distributed smart meters to calculate consumers' energy consumption. According to Wu et al., [6] these smart meters can be compromised, assuming physical access. This attack will corrupt the integrity of measured energy consumption from smart meters. Accurate state estimation is a critical component in maintaining stable and continuous operation of a power system. Typically, a bad data detector is implemented in power systems to remove erroneous meter readings due to meter/sensor failures [7]. Yuan et. al. [8] have modelled FDI attacks on state estimation, which changes the load redistribution in the power system. Another study [9] has shown FDI attacks that introduce net load redistribution in an AC distribution system, causing violations in nodal voltage estimations.

Control centers in modern power systems extensively use optimal power flow (OPF) studies for system planning and operation. An OPF study determines the control variables and state variables that minimizes the overall generating cost, while respecting transmission network constraints and power balance equations [10]. OPF ensures that system operation is both economic and secure. In this paper, an FDI attack is formulated to mislead the OPF algorithm, by modifying targeted sensor measurements before they reach the control centers. We investigate the impact of FDI attacks on the OPF algorithm using a simple 2-bus system, for intelligibility, and an IEEE 37-bus system, for authenticity.

The paper is organized as follow. An overview of optimal power flow is presented in Section II. The threat model is described in Section III. Case studies on a 2-bus system and an IEEE 37-bus system are presented in Section IV, before the paper is concluded in Section V.

II. Optimal Power Flow

Classically, OPF is formulated for symmetrical three-phase AC systems (AC-OPF) as a non-linear and non-convex optimization problem. AC-OPF is subjected to constraints that are both continuous (voltages, angles, and current flows) and discrete (tap transformers settings and shunt devices) [11]. Solving AC-OPF may be computationally expensive, especially when implemented for large-scale power systems. As such, various modeling approaches are proposed in literature to simplify AC-OPF problem formulation. This includes iterative approximations of non-linearities, and convex relaxations of the non-linear equations [12]. However, DC-OPF is usually implemented in practice, which is a linearized version of AC-OPF with a good trade-off between accuracy and computational efficiency [13].

This research was supported in part by the National Research Foundation, Singapore, and the Energy Market Authority, under its Energy Programme (EP award no. NRF2017EWT-EP003-061), and in part by the SUTD-ZJU IDEA Programme (award no. 201805).

978-1-6654-4407-1/21/$31.00 © 2021 IEEE

We use PowerWorld Simulator [14] to study OPF. PowerWorld Simulator is an interactive industry-grade simulation platform, designed to simulate and perform power flow analysis for high voltage power systems consisting of up to 250,000 buses. PowerWorld Simulator implements a "primal linear programming" (LP) solution algorithm for solving OPF, which is an iterative algorithm.

The original non-linear optimization problem (NP) is defined as:

$$
\begin{aligned}
&\min : y(x) \\
&s.t. : \begin{cases} f_i(x) < b_i & \forall i = 1, 2, \ldots, m \\ l_j < x_j < u_j & \forall j = 1, 2, \ldots, n \end{cases}
\end{aligned}
$$

The linear problem is then formulated by linearizing NP around a feasible point x_k

$$
\begin{aligned}
&\min : \ y - y(x_k) = \sum_j c_j(\Delta x_j^+ - \Delta x_j^-) \\
&s.t. : \begin{cases} f_i(x_k) + \sum_j a_{ij}(\Delta x_j^+ - \Delta x_j^-) < b_i & \forall i \\ l_j - x_{jk} < \Delta x_j^+ - \Delta x_j^- < u_j - x_{jk} & \forall j \\ x_j - x_{jk} = \Delta x_j^+ - \Delta x_j^- & \forall j \\ c_j = \frac{\partial y(x_k)}{\partial x_j}, \quad a_{ij} = \frac{\partial f_i(x_k)}{\partial x_j} & \forall i, j \end{cases}
\end{aligned}
$$

Δx_j^+ and Δx_j^- represents the positive and negative incremental changes in x. The solutions of Δx_j^+ and Δx_j^- are used to update x, then linearization around the new x is implemented. The iteration stops when Δx_j^+ and Δx_j^- are below given tolerances. Here, the bounds are required to ensure convergence. The bounds will be reduced when an infeasible solution is located, then the problem will be resolved.

In this paper, the minimization of overall generation cost is considered as an objective function for the OPF study that is subjected to various constraints as described in Table I. The OPF process can be further examined in Figure 1.

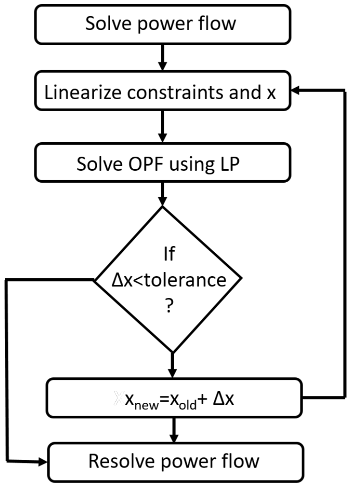


Fig. 1. **Flowchart showing the steps to solve OPF problem in PowerWorld Simulator**

III. Threat Model

In modern power systems, unencrypted sensor data is transmitted to control centers for optimization and control. These communication lines are vulnerable to cyber-attacks, where an attacker may use compromised routers to inject forged data. A strategically designed attack may inject false data into communication channels, while bypassing conventional bad data detectors. Seen in Figure 2, FDI attacks are launched on the communication line transmitting power sensor data to the control centers. This data includes measurements of load demand (D) and branch power flows (B), which are altered (D' and B') and input to the OPF algorithm.

OPF is responsible for determining the best operating level for the power plant under present load conditions and branch limits. Operating level refers to the scheduled power generation in generators P_{opf}, power flow in branch's B_{opf}, and cost of electricity generation C_{opf}. The OPF solution reroutes the power in lines, and resets the generators' scheduled power set points for the next interval. This ensures economical operation of the power plant while meeting the load demand and constraints of the power system operation.

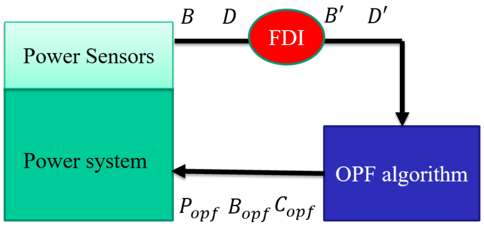


Fig. 2. **Threat model of FDI attack on power system to misguide OPF algorithm**

The attack on the communication channel attempts to falsify load demand in the power system. If the false load demand is fed to the OPF algorithm, the calculated optimal operating level would be a suboptimal solution, leading to increased operational costs or even load being unmet. To resemble natural load fluctuations and remain undetected, the attack is designed such that the total load change in the system will not be more than 50%. To compromise the OPF of power system the attacker should have access to read and write line power flows and should have knowledge of branch parameters and cost model of generators. The attacker can design a attack vector which change the load demand (ΔD) in such a way that the hourly cost of electricity generation increases or cause branch MW/MVA limit violations.The attack vector are designed in two ways i.e. the line flows are redistributed keeping the net load unchanged. Secondly, the line flows as well as net load are changed. The redistribution caused by the attack vector force the generator with higher cost to supply the load demand. The attack vector is such a value of ΔD which cause the change in branch power flow (ΔB) with an objective function given as follow:

$$
\text{Max}_{\Delta \text{D}} \sum_{g=1}^{N_g} C_{opf} P_{opf} + \sum_{b=1}^{N_b} B_b; \qquad \text{s.t.} \quad \sum_{d=1}^{N_d} \frac{\Delta D_d}{D_d} \leq 0.5
$$

TABLE I
CONSTRAINTS AND CONTROL VARIABLES IN OPF PROBLEM FORMULATION IN POWERWORLD SIMULATOR

	Constraints	Type		Control Variables
1	Bus real (MW) and reactive (MVAR) power balance	=	1	Generator power output
2	Branch power transfer capability (MVA and MW) limits	=,≤	2	Load dispatch
3	Generator real (MW) and reactive (MVAR) limits	≤	3	Phase shifting transformer tap change
4	Generator voltage setpoint	=	4	Generator cost model (piece-wise linear)
5	Area/Superarea real power (MW) exchange	=		
6	Interface real power (MW) limits	=,≤		

IV. RESULTS AND DISCUSSION

Next we examine the impact of FDI attacks designed to mislead the OPF algorithm. When inputs are falsified, the OPF algorithm may lead the system to operate at a suboptimal level. This can be observed by looking at the overall cost of electricity generation, before and after the attack. We also must ensure operations are within safe limits, so we monitor the impact of FDI attack on the branch power flow limits. The final consideration is the amount of unmet load after an attack.

We simulate two types of power systems, an IEEE 2-bus, and 37-bus system using PowerWorld Simulator. Both are used to analyze the impact of FDI attacks targeting OPF. The 2-bus system is used for simpler illustration, and the 37-bus system for a realistic system. In our simulations, we use the system operating cost, branch congestion, and unmet load to quantify the attack impact. Branch congestion refers to branch power flows exceeding branch limits.

A. Case Scenario: IEEE 2-Bus System

A case study using a simple 2-bus system is examined to visualize the impact of an FDI attack on the OPF solution, and system performance. The 2-bus system parameters are given in Table II and the system configuration is shown in Figure 3. Under normal conditions the system operates at optimal levels, as calculated by the preexisting OPF solution. The hourly cost of electricity generation is found to be 1560 $/h. Generators 1 and 2 are generating 25MW and 15MW to meet the total load demand of 40MW at bus 1 and 2. There is no congestion observed in the branch connecting bus 1 and 2.

Once the FDI attack is launched, we capture the performance of the system in terms of operating cost (C), branch power flow (B), and amount of unmet load. Table III shows the performance of the IEEE 2-bus system under different attack scenarios. The FDI attacks fools the system into wrongly estimating the load demand, which is input to the OPF algorithm. Consequently, the operating levels determined by the OPF (P_{opf}, B_{opf}, and C_{opf}) will mislead the system operation. After the attack, the system either operates at higher hourly generation cost, or branch limits are violated, causing load to be unmet. We see higher costs in attack scenarios 1, 2, 3, 5, and 8, in scenarios 4 and 6 we see branch limit violations and unmet load.

Figure 4 shows scenario 1, where C increases from 1560$/h to 1580$/h due to the FDI attack, but is otherwise safe. This shows how FDI attacks on OPF can harm the efficiency of power generation and cause a utility to waste money. Figure 5 shows scenario 6, which has lower cost following an attack, but the branch limit is violated. This violation can harm the physical equipment or may trip the breaker and disrupt operations. This scenario shows how FDI attacks against OPF can cause more serious harm related to safety, equipment damage, or operational disruption.

It is interesting to note that in scenario 6, the system will have unmet load even though it is capable of generating an additional 8MW. Even though the maximum combined generation capacity is 48MW, the system cannot meet a load demand of 40MW due to inefficient generator scheduling and branch limits. Instead, the system has 2MW load that cannot be met, because the FDI attack causes the OPF to generate an inefficient distribution. Thus, the FDI attack not only leads to economic loss to the utility but also endangers the continuity of the power system. This 2-bus system allows for easy visualization of FDI attack impacts, in the following subsection, we will examine FDI attack impacts on a realistic IEEE 37-bus system.

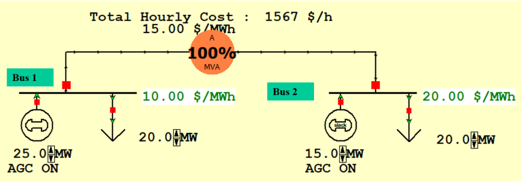


Fig. 3. **IEEE 2-bus system**

TABLE II
CASE:2-BUS SYSTEM PARAMETERS

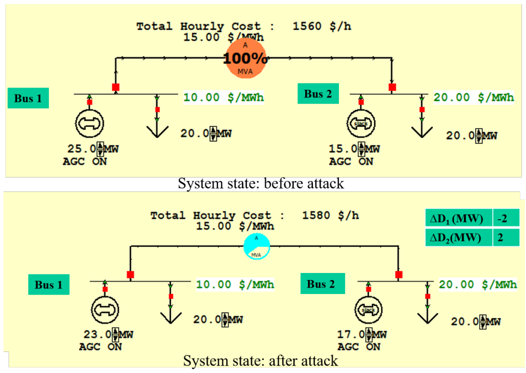
Generator	**1**	**2**
P_{max} (MW)	30	18
P_{min} (MW)	0	0
C ($\MWh)	10	20
Load	**1**	**2**
D (MW)	20	20
Branch	**12**	
MVA limit	5	

B. Case Scenario: IEEE 37-Bus System

The configuration of our IEEE 37-bus system is shown in Figure 6, with parameters borrowed from an existing case study [15]. This system is organized into 3 areas, where each area may be operated by a separate utility, and share power

TABLE III
PERFORMANCE OF THE 2-BUS SYSTEM UNDER VARIOUS FDI ATTACK SCENARIOS

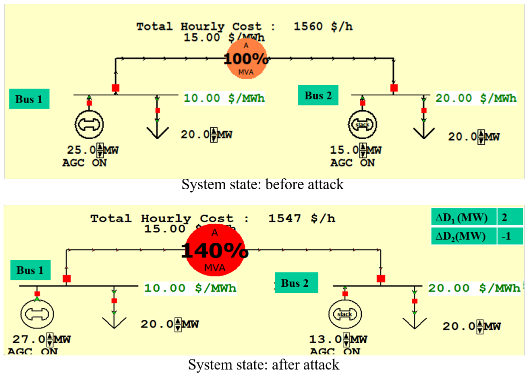
		Attack Scenario							
		1	2	3	4	5	6	7	8
Attack	ΔD_1 (MW)	-2	-4	-10	10	-1	2	0	0
	ΔD_2 (MW)	2	4	10	-10	2	-1	5	-5
False state estimation	D_1' (MW)	18	16	10	30	19	22	20	15
	D_2' (MW)	22	24	30	10	22	19	25	20
OPF results	P_{opf1} (MW)	23	21	15	30	24	27	25	20
	P_{opf2} (MW)	17	18	18	10	16	14	20	15
	B_{opf} (%)	100	120	240	0	120	100	100	100
	C_{opf} (\$/hr)	1580	1590	1590	1510	1597	1567	1667	1517
	Unmet Load (MW)	0	1	7	0	0	0	0	0
Measurements after attack	B (%)	60	40	40	200	80	140	100	0
	C (\$/hr)	1580	1590	1590	1510	1577	1547	1567	1617
	Unmet Load (MW)	0	0	0	5	0	2	0	0



System state: before attack

System state: after attack

Fig. 4. **System states before and after attack when 2-bus system is subjected attack scenario 1**



System state: before attack

System state: after attack

Fig. 5. **System states before and after the attack when 2-bus system subjected to attack scenario 6**

through tielines. The impact of different attack scenarios are analysed and tabulated in Table IV and V. The attack scenarios are designed to force the most expensive generator on bus 48 to supply the load demand. The attack scenario 1-2 are designed by manipulating the line flow and keeping the net load unchanged. Whereas, in 3-5 the line flow as well as net load is manipulated. Similar to the 2-bus system, FDI attacks on our 37-bus system result in either increased hourly generation cost, in scenarios 1 and 2, or branch congestion, in scenarios 3, 4, and 5. Of the two impacts, branch congestion is more harmful as it can cause disruptive remedial actions such as load shedding or tripping breakers.

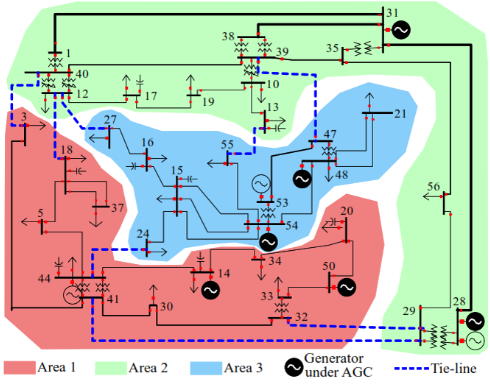


Fig. 6. **IEEE 37-bus system**

V. CONCLUSION

We examine the impact of FDI attacks on the power system OPF algorithm. The attack vector are designed in two ways i.e. the line flows are redistributed keeping the net load unchanged and the line flows as well as net load are changed. An IEEE 2-bus and 37-bus system are used to evaluate the impact of FDI attacks on OPF. Under FDI attack, the OPF algorithm leads the system to a suboptimal operating level. For both a simple 2-bus system, and a realistic 37-bus system, attacks can increase the overall cost of electricity generation, or push power flow in branches past their limits to cause disruptive remedial actions. These remedial actions include load shedding, or trip breakers, which may be very disruptive and costly for the utility. Since these attacks may be harmful, we encourage future work to form mitigation techniques to defend against them.

TABLE IV
PERFORMANCE OF THE IEEE 37-BUS MEASURED AFTER FDI ATTACK TARGETED ON OPF

			Attack Scenario			
	Normal Case		1		2	
Generator	$P(MW)$	$C(\$/hr)$	$P(MW)$	$C(\$/hr)$	$P(MW)$	$C(\$/hr)$
14	34.7	1256.06	35	1266.49	35	1265.17
28	90	2319.66	53.4	1369.99	50	1282.14
28	91.3	2319.07	3.4	83.96	8.9	220.46
31	88.6	2349.74	212	5806.55	209.4	5730.92
44	150	4335	150	4335	150	4335
48	52.1	1473.84	88.6	2530.79	102	2920.34
50	80	2010.74	80	2010.74	80	2010.74
53	140	2790.59	126.6	2482.53	140	2790.59
54	110	2486.75	87.3	1931.37	61.1	1317.26
Total	836.7	21341.45	836.3	21817.42	836.4	21872.62
Congestion	nil		nil		nil	

TABLE V
PERFORMANCE OF THE IEEE 37-BUS MEASURED AFTER FDI ATTACK TARGETED ON OPF

			Attack Scenario					
	Normal case		3		4		5	
Generator	$C(\$/hr)$	$P(MW)$	$C(\$/hr)$	$P(MW)$	$C(\$/hr)$	$P(MW)$	$C(\$/hr)$	$P(MW)$
14	1266.87	35	1266.87	35	1266.87	35	1266.87	35
28	2067.15	127.2	2428.5	147.9	2425.42	147.8	2422.8	147.6
28	0	0	0	0	0	0	0	0
31	3776.08	141	4226	157.1	3662.92	137	3117.58	117
44	4335	150	4335	150	4335	150	4335	150
48	1471.38	52	1471.38	52	1471.38	52	1471.38	52
50	2000.11	80	2000.11	80	2000.11	80	2000.11	80
53	2790.59	140	2790.59	140	2790.59	140	2790.59	140
54	2486.75	110	2486.75	110	2486.75	110	2486.75	110
Total	20193.93	835.2	21005.2	872	20439.04	851.8	19891.08	831.6
Congestion	nil		101%		106%		110%	

REFERENCES

[1] A. Khattak, S. Mahmud, and G. Khan, "The power to deliver: Trends in smart grid solutions," *IEEE Power and Energy Magazine*, vol. 10, no. 4, pp. 56–64, 2012.

[2] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, "Protecting smart grid automation systems against cyberattacks," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 782–795, 2011.

[3] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2017.

[4] R. Tan, H. H. Nguyen, E. Y. S. Foo, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1609–1624, 2017.

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

[6] 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.

[7] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—attacks, impacts, and defense: A survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411–423, 2017.

[8] 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.

[9] 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)*, 2020, pp. 46–50.

[10] J. Zhu, *Optimal Power Flow*, 2015, pp. 297–364.

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

[12] K. Y. Lee and M. A. El-Sharkawi, *Genetic Algorithms for Solving Optimal Power Flow Problems*, 2008, pp. 471–500.

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

[14] "PowerWorld Simulator help files." [Online]. Available: https://www.powerworld.com/knowledge-base/powerworld-simulator-help-files

[15] A. R. Al-Roomi, "Power Flow Test Systems Repository," Halifax, Nova Scotia, Canada, 2015. [Online]. Available: https://al-roomi.org/power-flow