

Bi-level Modelling of False Data Injection Attacks on Security Constrained Optimal Power Flow

Kush Khanna,^{*}Bijaya Ketan Panigrahi,
and Anupam Joshi,[†]

Abstract

Conventional power system was originally designed to provide efficient and reliable power. With the integration of information technology and advanced metering infrastructure, the power grid has become smart. The smart meters have allowed the system operators to continuously monitor the power system in real time and take necessary action to avoid system failures. These advancements have also made power grid prone to cyber-threats. Malicious actor, with access to the smart meters can modify the sensor measurements to disrupt the operation of power system. In order to make the power system resilient to such cyber-attacks, it is important to study all the possible outcomes of cyber-intrusions. In this paper, we present an attack on security constrained optimum power flow. We show with the help of case studies, how an attacker by injecting false data in load measurement sensors, force system operator to change the dispatch and hence making the power system $N - 1$ in-compliant. The attack is modeled as a bi-level optimization problem, aiming to find the minimum set of sensors required to launch the attack. From the system operator's perspective, the critical lines and critical generators are identified which are vulnerable to false data injection (FDI) attack. IEEE 14 bus and 30 bus test systems are used to test the vulnerability of the power system against FDI attacks.

Index Terms: Cyber security, false data injection, power system optimization, smart grid.

Nomenclature

^{*}K. Khanna and B. K. Panigrahi are with the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi, India e-mail: (kushkhanna06@gmail.com, bkpanigrahi@ee.iitd.ac.in).

[†]Anupam Joshi is with the Computer Science and Electrical Engineering Department, University of Maryland Baltimore County, Baltimore MD 21250, USA (email: joshi@umbc.edu).

- \mathbf{a} Injected attack vector.
- \mathbf{c} Estimated error injected in the state variable by the attacker.
- \mathbf{D} Bus-Load incidence matrix.
- \mathbf{e} Meter error.
- \mathbf{F}^N Flows considering dispatch \mathbf{P}'_g and actual load \mathbf{P}_D .
- $\mathbf{F}^{N-1(cg)}$ Flows considering dispatch \mathbf{P}'^{cg}_g , actual load \mathbf{P}_D and cg^{th} generator outage.
- $\mathbf{F}^{N-1(cl)}$ Flows considering dispatch \mathbf{P}'_g , actual load \mathbf{P}_D and cl^{th} line outage.
- \mathbf{G}^{cg} Bus-Generator incidence matrix considering cg^{th} generator outage.
- \mathbf{G} Bus-Generator incidence matrix.
- \mathbf{H} Measurement Jacobian matrix $[m \times n]$.
- \mathbf{P}_D Real power demand vector $N_{bus} \times 1$.
- \mathbf{P}'^{cg}_g Real power generation vector considering cg^{th} generator outage.
- \mathbf{P}'_g Generator dispatch vector considering corrupted load measurements.
- $\mathbf{P}_g, \mathbf{R}_g^{cg}$ Dispatch variables for the inner level optimization problem.
- \mathbf{R}'^{cg}_g Real power generation ramp vector considering cg^{th} generator outage.
- \mathbf{R}'_g Generator ramp vector considering corrupted load measurements.
- \mathbf{S}^{cl} Shift factor matrix considering cl^{th} line outage.
- \mathbf{S} Shifting factor matrix.
- \mathbf{x} State vector $n \times 1$.
- \mathbf{z}_{true} True measurement vector $n \times 1$.
- ΔF_l Change in the flow measurement of l^{th} branch.
- ΔP_{Dd} Change in the load measurement of d^{th} bus.
- ϵ Fraction of allowable load change.
- $\overline{F}_l/\underline{F}_l$ Maximum/Minimum flow limit of the branch l .
- $\underline{P}_{gi}/\overline{P}_{gi}$ Minimum/Maximum generation limits of generator at i^{th} bus.

B_{gen} Count for lines violating the limits for one generator contingency.

B_{line} Count for lines violating the limits for one line contingency.

$C_{gi}(P_{gi})$ Cost of generator on i^{th} bus.

FL_l $FL_l = 1$ indicating $\Delta F_l \neq 0$.

$h(x)$ Measurement function $[h_1(x_1, x_2, \dots, x_n), \dots, h_m(x_1, x_2, \dots, x_n)]^T$.

L_d $L_d = 1$ indicating $\Delta P_{Dd} \neq 0$.

N_D Set of all the buses where load is connected.

N_L Set of all the branches of the network.

N_{bus} Number of bus in the network.

r Fraction of allowable generation change during generator contingency.

1 Introduction

Communication technologies and automation are incorporated for enabling device to device communication in order to make power grid a smarter grid. These valuable additions to the conventional power grid not only makes the grid more robust and reliable but also introduces new cyber related risks and vulnerabilities into power grid. Attackers can exploit these vulnerabilities for motives like terrorism, warfare and profit. Adversary on gaining access to the power system by hacking SCADA (Supervisory Control and Data Acquisition) communication line can cause various cyber-attacks, therefore, the security of the smart grid against such risks is of utmost importance. Building a completely secure and hacker proof system is practically impossible, however, securing key components of the power system can increase the cost of such attacks. These key components can be identified by analysing all the possible impacts of the cyber-attacks on the power system so that appropriate actions can be taken in order to ensure that the sensors and devices are secured and the data collected is accurate.

Recent work in the area of smart grid and cyber-physical systems have addressed the vulnerability of power system under various cyber-threats. State estimation constitutes the crux of all the power system studies including optimal power flow, contingency analysis and security analysis [1]. Studies reveals that an attacker can inject calculated false data into the meters without being detected by the system operator to make the

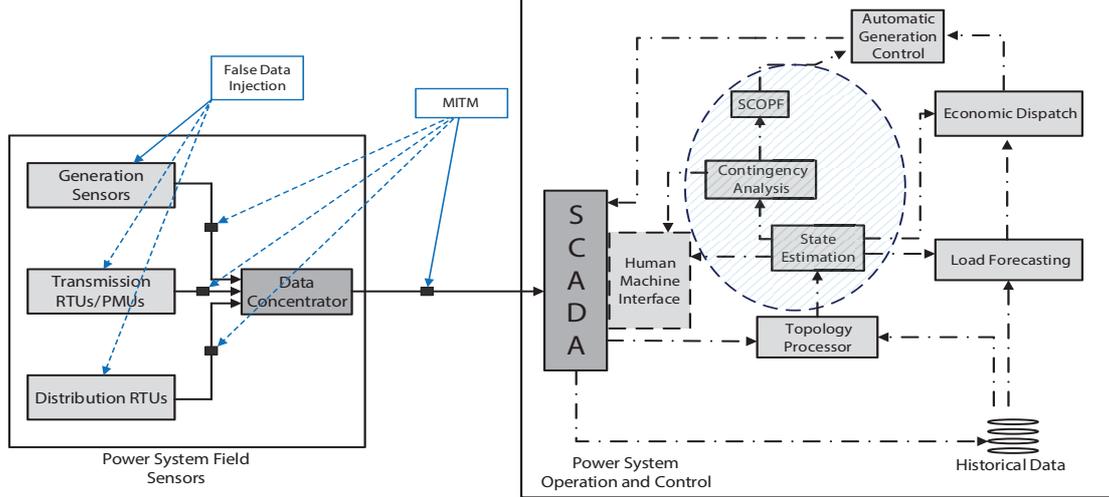


Figure 1: Security threats in smart grid.

state estimation results erroneous [2–4]. Fig. 1 shows security threats affecting operation and control of power system. False data injection and man in the middle attacks (MITM) compromises the field sensor data received by the SCADA system resulting in flawed operation of the power system. False data injection attacks were further elaborated in [5–10]. The vulnerability assessment of AC state estimation in the advent of false data injection attacks are explained in [11]. In [12] the impact of delayed and immediate load redistribution attack on power system is presented. Cyber attack aimed for overloading a transmission line is explained in [13]. In [14,15] financial impacts of false data injection attacks were presented. Data integrity attack with the motive of financial misconduct by faking higher energy export to the grid is presented in [16].

The defence techniques against FDI attacks can be broadly classified into two categories; protection based defence and detection based defence. The defence techniques presented in the literature mostly focus of protecting critical sensors [17,18] to alleviate certain FDI attacks. Furthermore, only the protected measurement sensors are trusted and hence the redundancy of the measurements is decreased affecting state estimation. The detection based approach on the other hand [19–23] analyses the raw measurements and able to detect the ones which does not follow distribution of historical measurements. Furthermore, as explained in [23], the detection technique only works when attacker causes significant change in the measurements.

In order to give reliable power supply, power system must be able to withstand line outage, loss of generator and transformer without affecting the operation. Nowadays, power systems are considered to be $N - 1$ compliant, which is a security criterion specifying that system must able to withstand loss of one component [24]. Current research in the area of cyber-physical systems and smart grid, focus on analysing the impact of

cyber-attacks on the operation and control of power system. If an attacker injects false data into the meters and succeeds in making a line or generator trip, it will not cause cascading failure immediately as power system is designed to withstand a loss of component. However, if an attack is designed intelligently considering security aspects of the power system by injecting malicious attack vector causing power system to be $N - 1$ in-compliant, it can cause serious repercussions.

In [12, 25], the attack on security constrained economic dispatch is presented with the motive of maximising the operation cost by including the load shedding cost in the model. The proposed method finds the meters required to force the power system to an uneconomic state of operation by restricting the maximum attacking cost (number of meters required to launch the attack). The protection strategy, as presented is to secure the measurement sensors (depending on the attacking cost considered) to alleviate the possibilities of such attacks. However, from the system security standpoint, in this paper, an attack model is proposed aiming to cause flawed security constrained optimal power flow (SCOPF) (encircled in Fig. 1), a program which a system operator runs to calculate the generator dispatch considering all security limits. The attack is modelled as a bi-level optimization problem. Inner level finds the economic dispatch considering $N - 1$ security constraints with compromised load measurements. The outer level finds the minimum number of measurements to be attacked in order to make the new dispatch $N - 1$ in-complaint. The attack vector ensures that at least one line or generator will be tripped if a targeted line/generator is attacked and taken out of service maliciously. From the system operator viewpoint, the identification of such critical lines is of utmost importance to secure the system against the attack on SCOPF. The contributions of this paper are twofold,

1. We present for the first time, how an attacker by injecting false data in certain measurements can launch the attack forcing power system to operate at a state in which loss of single component (generator or line) can cause multiple line outages.
2. Using a bi-level optimization, we present the minimum set of meters required to launch such attack. The critical lines and generators are identified for IEEE 14 and 30 bus systems. The information can be used to secure the minimum set of meters so that such attacks can be avoided.

The rest of the paper is organised as follows, section II gives the brief overview of security constrained optimal power flow and false data injection attacks. Attack model is explained in section III. Case study and results are discussed in section IV. Conclusions and future scope is presented in section V.

2 Brief Overview on False Data Injection Attacks

False data injection attacks can be launched by injecting malicious data into certain measurements to deceive the system operator by erroneous estimated state. Depending upon the target of the false data injection attack and the attacking resources of the attacker, the attacks can be broadly classified into 1) Observable attacks, where attacker injects random error in the accessible meters to make the state estimation result erroneous and 2) Stealthy attacks, where the attack vector is formulated intelligently by considering network topology and parameters and is unobservable to the system operator.

Considering DC state estimation, as explained by Liu et.al. [2], if $\mathbf{z}_{true} = h(\hat{\mathbf{x}}) + \mathbf{e}$ passes the residual test ($\|\mathbf{z}_{true} - h(\hat{\mathbf{x}})\| \leq \tau$), the injected attack vector bypasses the bad data detection if the attack vector is the linear combination of column vector of \mathbf{H} i.e. $\mathbf{a} = \mathbf{H}\mathbf{c}$. This can be mathematically proved as,

$$\begin{aligned} \|\mathbf{z}_{true} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + \mathbf{c})\| &= \|\mathbf{z}_{true} - \mathbf{H}\hat{\mathbf{x}} + \mathbf{a} - \mathbf{H}\mathbf{c}\| \\ &= \|\mathbf{z}_{true} - \mathbf{H}\hat{\mathbf{x}}\| \leq \tau \end{aligned} \quad (1)$$

In load redistribution attacks, attacker injects false data to the load meters such that the net change in the system load remains zero. Load is redistributed in the network to cause the intended change in the estimated states [25]. False data injection can also be launched if the attacker has incomplete or limited network knowledge as explained in [26]. Furthermore, the following key assumptions were also proposed in [26, 27] which makes false data injection attacks more reasonable by limiting the attacking resources of the attacker.

1. The generator measurement cannot be altered.
2. Zero injection buses cannot be attacked.
3. Depending on the accessibility, all flow meters and load meters can be attacked.

If intelligently crafted the impacts of the false data injection attacks are manifold. Malicious data injected in field sensors directly affects operation and control of entire power system. In this paper we are exploring the impacts of such attacks if integrity of SCOPF and contingency analysis are targeted.

3 Attack Model

Optimal Power Flow (OPF) solution gives system operator an optimal active and reactive power dispatch for the given steady state loading conditions [28]. For operating the power

system efficiently, system operator needs to confirm the robustness of the power system under various contingencies. Security Constrained Optimal Power Flow is an extension of conventional OPF subjected to the security constraints.

Adversary with access to load sensors and flow measurements can launch a stealthy attack by modifying the sensor measurements intelligently. With the change in the load pattern, the generator dispatch is fine-tuned to obtain the new optimal operating point. The attacker here deceives system operator with modified load measurements, thereby causing in-accurate scheduling of generators. It is assumed that the adversary by hacking the communication network compromises the generation dispatch process by injecting well-crafted malicious data in the load measurement sensors [13]. Attack model is formulated by considering DC power flow equations, therefore, resistances of the transmission lines are neglected, all the bus voltages are assumed to be 1.0 p.u., shunt elements of the lines and transformer taps are neglected. A fully measured power system is assumed throughout the paper.

3.1 Considering Line Contingencies only

The attack is modelled as a bi-level optimization problem. In the outer level, the minimum number of meters required to launch the attack are calculated with ΔPD as the variable as given in (2) whereas, **L1** denotes the outer level.

$$(\mathbf{L1}) \quad \min_{\Delta P_D} \left\{ \sum_{\forall d \in N_D} L_d + 2 \sum_{\forall l \in N_L} FL_l \right\} \quad (2)$$

subject to,

$$L_d = \begin{cases} 1 & \Delta P_{Dd} \neq 0, \\ 0 & \Delta P_{Dd} = 0 \end{cases} \quad \forall d \in N_D \quad (3)$$

$$FL_l = \begin{cases} 1 & \Delta F_l \neq 0, \\ 0 & \Delta F_l = 0 \end{cases} \quad \forall l \in N_L \quad (4)$$

$$-\epsilon P_{Dd} \leq \Delta P_{Dd} \leq \epsilon P_{Dd} \quad \forall d \in N_D \quad (5)$$

$$\sum_{\forall d \in N_D} \Delta P_{Dd} = 0 \quad (6)$$

$$\Delta F = S \cdot D \cdot \Delta P_D \quad (7)$$

$$F^N = S \cdot (G \cdot P'_g - D \cdot P_D) \quad (8)$$

$$\underline{F}_l \leq F_l^N \leq \overline{F}_l \quad \forall l \in N_L \quad (9)$$

$$\mathbf{F}^{N-1(cl)} = \mathbf{S}^{cl} \cdot (\mathbf{G} \cdot \mathbf{P}'_g - \mathbf{D} \cdot \mathbf{P}_D) \quad \forall cl \in N_L \quad (10)$$

$$B_{line} = \sum_{\forall l, cl \in N_L} \begin{cases} B_{cl}^l = 1 & \overline{F}_l - |F_l^{N-1(cl)}| < 0 \\ B_{cl}^l = 0 & \overline{F}_l - |F_l^{N-1(cl)}| \geq 0 \end{cases} \quad (11)$$

$$B_{line} > 0 \quad (12)$$

The optimization problem (2) is solved subjected to the constraints (3)-(12). The number of load meters and flow meters to be attacked based on change in the load measurement vector $\Delta \mathbf{P}_D$ is formulated in (3) and (4) respectively. Here N_D and N_L denotes set of load buses and lines in the network. The constraint (5) ensures the change in the load meter is confined within the limits $\pm \epsilon P_{Dd}$, here, ϵ is the percentage load change in the load meters without making system operator suspicious. Constraint (6) ensures that the net change in the system load remains zero, i.e., load is redistributed, as a non-zero value imply a increase or decrease in the load, which must trigger frequency control exposing the attack to the system operator.

The changes in the flow meter reading $\Delta \mathbf{F}$ for the change in $\Delta \mathbf{P}_D$ is calculated from (7). For system without line contingency, the line flows with perturbed load measurements are obtained using (8). The line flow limits for changed load measurements, without considering line contingencies are checked using (9). Here \mathbf{S} , \mathbf{G} and \mathbf{D} denotes shift factor matrix, bus-generator incidence matrix and bus-load incidence matrix. The constraint (9) ensures that even after the attack, the line flows are still within the limits for the system without contingency. For each line contingency cl , the line flows for perturbed load measurements are calculated from (10). In order to ensure that the new dispatch is not $N-1$ complaint, (11) counts the number of lines where the power flow is above limits considering each line outage. This count must be greater than zero in order to launch the attack as given is constraint (12).

$$\text{(L2)} \quad \{\mathbf{P}'_g\} = \arg\{\min_{\mathbf{P}_g} \sum_{\forall i \in N_G} C_{gi}(P_{gi})\} \quad (13)$$

subject to,

$$\underline{P}_{gi} \leq P_{gi} \leq \overline{P}_{gi} \quad (14)$$

$$\mathbf{F} = \mathbf{S} \cdot [\mathbf{G} \cdot \mathbf{P}_g - \mathbf{D} \cdot (\mathbf{P}_D + \Delta \mathbf{P}_D)] \quad (15)$$

$$\begin{aligned} \mathbf{F}^{cl} = & \mathbf{S}^{cl} \cdot [\mathbf{G} \cdot \mathbf{P}_g \\ & - \mathbf{D} \cdot (\mathbf{P}_D + \Delta \mathbf{P}_D)] \quad \forall cl \in N_L \end{aligned} \quad (16)$$

$$\underline{F}_l \leq F_l \leq \overline{F}_l \quad \forall l \in N_L \quad (17)$$

$$\underline{F}_l \leq F_l^{cl} \leq \overline{F}_l \quad \forall l, cl \in N_L \quad (18)$$

$$\sum_{\forall i \in N_G} P_{gi} - \sum_{\forall d \in N_D} (P_{Dd} + \Delta P_{Dd}) = 0 \quad (19)$$

The inner level optimization problem **L2** is solved to obtain the new dispatch \mathbf{P}'_g for perturbed load measurements $(\mathbf{P}_D + \Delta \mathbf{P}_D)$ subjected to constraints (14)-(19). The security constrained optimal power flow is formulated in the inner loop considering the line contingencies only. The constraint (14) limits generation between \underline{P}_{gi} and \overline{P}_{gi} . The power flows without considering line flows are obtained using (15). Similarly, for contingency cl , the line flows are obtained using (16). The constraints (17) and (18) limits the line flows as per the line limits, while (19) maintains generation and load balance.

After solving (2), we get an attack vector with the required change in the load measurements $\Delta \mathbf{P}_D$ and line flows $\Delta \mathbf{F}$, along with minimum number of meters required to successfully launch this attack (as the attack vector here is function of measurement function, since, $\Delta \mathbf{F}$ is calculated by using \mathbf{S} , \mathbf{D} and $\Delta \mathbf{P}_D$, the attack bypasses the bad data detection and hence can be termed as a ‘successful attack’).

3.2 Considering both Line and Generator Contingencies

To consider both line and generator contingencies, the attack model is modified. The objective function (2) is solved subjected to (3)-(9) and (20)-(22).

$$\begin{aligned} \mathbf{F}^{N-1(cg)} = & \mathbf{S} \cdot [\mathbf{G}^{cg} \cdot (\mathbf{P}'_g{}^{cg} + \mathbf{R}'_g{}^{cg}) \\ & - \mathbf{D} \cdot \mathbf{P}_D] \quad \forall cg \in N_G \end{aligned} \quad (20)$$

$$B_{gen} = \sum_{\substack{\forall cg \in N_G \\ \forall l \in N_L}} \begin{cases} B_{cg}^l = 1 & \overline{F}_l - |F_l^{N-1(cg)}| > 0 \\ B_{cg}^l = 0 & \overline{F}_l - |F_l^{N-1(cg)}| \leq 0 \end{cases} \quad (21)$$

$$B_{line} + B_{gen} > 0 \quad (22)$$

For each generator contingency cg , the line flows are obtained using (20). Total number of lines exceeding the line flow limits for all generator contingencies is calculated from (21). The constraint (22) ensures atleast one line must exceed the limit under line

or generator contingency for perturbed load measurements.

$$\text{(L2)} \quad \{\mathbf{P}'_g, \mathbf{R}'_g\} = \text{arg}\{\min_{\mathbf{P}_g, \mathbf{R}_g} \sum_{\forall i \in N_G} C_{gi}(P_{gi})\} \quad (23)$$

subject to (14)-(19),

$$\begin{aligned} \mathbf{F}^{cg} = & \mathbf{S} \cdot [\mathbf{G}^{cg} \cdot (\mathbf{P}_g^{cg} + \mathbf{R}_g^{cg}) \\ & - \mathbf{D} \cdot (\mathbf{P}_D + \Delta \mathbf{P}_D)] \quad \forall cg \in N_G \end{aligned} \quad (24)$$

$$\underline{F}_l \leq F_l^{cg} \leq \overline{F}_l \quad \forall l \in N_L, cg \in N_G \quad (25)$$

$$\sum_{\forall i \in N_G} (P_{gi}^{cg} + R_{gi}^{cg}) - \sum_{\forall d \in N_D} (P_{Dd} + \Delta P_{Dd}) = 0 \quad (26)$$

$$\underline{P}_{gi} \leq P_{gi}^{cg} + R_{gi}^{cg} \overline{P}_{gi} \quad \forall i \in N_G, i \neq cg \quad (27)$$

$$-r \cdot \overline{P}_{gi} \leq R_{gi} \leq r \cdot \overline{P}_{gi} \quad \forall i \in N_G \quad (28)$$

$$P_{g(i==cg)}^{cg} = 0, R_{g(i==cg)}^{cg} = 0 \quad (29)$$

The modified inner level objective function when considering both generator and line contingencies is given in (23), is minimised subjected to (14)-(19) and (24)-(29). Power flows for the generator contingency cg are calculated in (24). \mathbf{R}_g^{cg} is the vector for generator ramp value under generator contingency cg .

The constraint (25) limits the power flow in the transmission line for the contingency cg within the specified transmission line limits. When considering the outage of cg^{th} generator, the remaining generator must ramp up to meet the load demand. The total generation including the ramp must be within the the generation limits as specified in (26). The constraint (27) ensures the generation and load balance after contingency. The ramp up value of the remaining generators after contingency cg must be in the limits specified in constraint (28). In this paper the ramp up/down value is limited to the 25% of each generator capacity i.e. $r = 0.25$.

4 Results and Discussion

The proposed attack model is tested using IEEE 14 bus and 30 bus test systems. The minimum meters required to launch the attack by considering first; only line contingencies and second; both line and generator contingencies are obtained. The line limits considered for the IEEE test systems are given in Appendix. The outer level of the bi-level optimisation is solved using meta-heuristic technique and the inner level is solved using

quadrature programming. The maximum of 10% (ϵ) load change in the load sensors is considered to be spoofed by the attacker for all the test systems. To explain the attack and understand the consequences, attack is simulated for a sample 3 bus system which is explained along with IEEE 14 and 30 bus test results in this section.

4.1 Sample 3 bus system

Three bus system comprising of two generators and three transmission lines as shown in Fig. 2. The transmission line 1-2, 2-3 and 1-3 are having reactance 0.08 p.u., 0.06 p.u. and 0.12 p.u. respectively. The limits for the lines 1-2, 2-3 and 1-3 are 500 MW, 300 MW and 300 MW respectively. The generation cost data used for the 3 bus system is given in Appendix. Without attack, the generator dispatch and line flows for the system is shown in Fig. 2(a). Now considering an attack scenario, where attacker gets access to the smart sensors measuring power flows and load for each transmission line and load bus. The attacker by injecting the false data in the load and power flow measurement, deceive the system operator by an uneconomic power system operation as shown in Fig. 2, thereby, causing the operator to change the dispatch for the perturbed load measurements.

The malicious data injected in the power flow and load measurement is shown in Fig. 2(a). The load measurements at Bus 1, Bus 2 and Bus 3 are changed to 165 MW, 441.05 MW and 243.95 MW of spoofed meter readings respectively. The change in flow measurements are 141.01 MW (spoofed meter reading) and 143.99 MW (spoofed meter reading) for line 1-2 and line 1-3 respectively. The system operator runs security constrained optimal power flow to get economic operating state of the power system.

The new optimal generator dispatch for changed load measurements are 465 MW and 385 MW for generator 1 and 2 respectively. Under the normal operating condition (without contingency), the system is within limits as shown in Table 1. However, if a coordinated attack is launched and line 1-2 is tripped by the attacker, these new dispatches cause line 1-3 to be overloaded as shown in Fig. 2(b) with a power flow of 315 MW (actual flow) on a line with maximum capacity of 300 MW, causing cascaded tripping of lines.

Table 1: Generator dispatch, load and line flows before and after attack for a 3 bus system

		Pre-Attack	Attack	SCOPF (Attack)	N-1
P_g	G1	450 MW	-	465 MW	-
	G2	400 MW	-	385 MW	-
P_D	P_{D1}	150 MW	165 MW	150 MW	-
	P_{D2}	450 MW	441.05 MW	450 MW	-
	P_{D3}	250 MW	243.95 MW	250 MW	-
F	F_{1-2}	150 MW	141.01 MW	160.38 MW	out
	F_{2-3}	100 MW	100 MW	95.38 MW	65 MW
	F_{1-3}	150 MW	143.99 MW	154.62 MW	315 MW

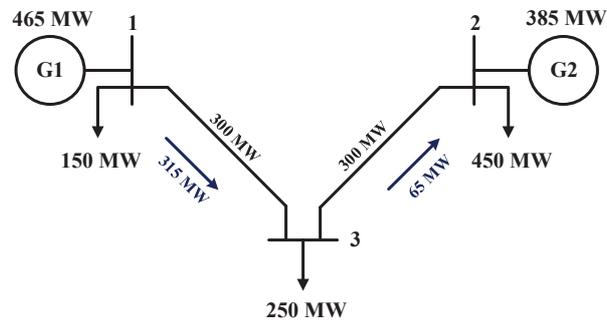
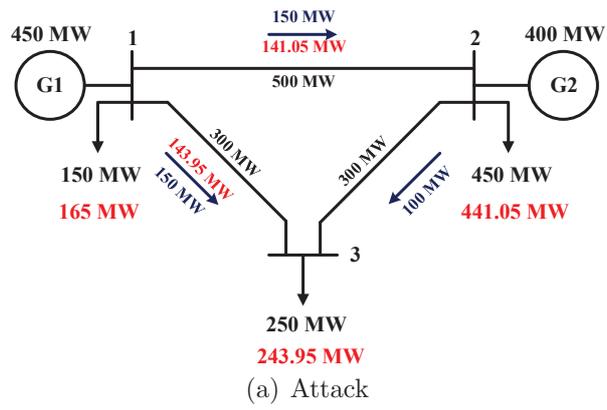


Figure 2: Three bus system.

Attacker requires access to minimum of seven meters to launch the attack if a fully measured system is considered. In the defence, system operator identifies line 1-2 as critical line must be protected to assure the security of the system.

4.2 IEEE 14 and 30 bus system

A fully measured IEEE 14 bus and 30 bus systems are considered with 14 real power injection measurements and 40 to and fro real power flow measurements for IEEE 14 bus system; and 30 real power injection measurements and 82 to and fro real power flow measurements for IEEE 30 bus system. The line limits considered are given in appendix. Line, load and generator data is taken from [29]. For IEEE 14 bus system, considering line contingencies only (LC), the attack vector for the change in load measurements is given in Table 2. The change in line flows are shown in Table 3. The number of meters required to launch the attack considering only the line contingencies for the 14 bus system are ten for load measurements and eighteen for flow measurements. As shown in Fig. 3, the critical lines are 1-2 and 1-5. Attacker if succeeds in tripping line 1-2 (event ‘1’), the flow in line 1-5 (event ‘1+’) becomes 90.1 MW (limit is 90 MW) and henceforth line 1-5 also trips (since the maximum allowable change in the load is 10% for all the load buses and the attacker tries to find the attack vector with minimum possible meters, therefore, from the system operator perspective, pessimistic scenario is considered for identifying all the possible vulnerabilities in the system. Hence, flow just above the limit is assumed to cause the line tripping).

Table 2: Attack Vector for Load Measurements in IEEE 14 Bus System (LC-Line Contingency Only; GLC-Both Generator and Line Contingency)

Bus	ΔPD (MW)		Bus	ΔPD (MW)	
	LC	GLC		LC	GLC
1	0	0	8	0	0
2	-1.559	0	9	1.417	-1.951
3	3.051	0	10	-0.899	0.095
4	-1.389	1.659	11	0	0
5	0.095	0.666	12	-0.359	0
6	1.118	-0.701	13	-1.104	0
7	0	0	14	-0.372	0.229

If both generator and line contingencies (GLC) are considered, the attack vector is shown in Table 2 and Table 3. Six load measurements and sixteen flow measurements are required to launch the attack of IEEE 14 bus system. Tripping of line 1-2 results in the tripping of line 1-5, which disconnects generator at bus 1 from the system (event ‘2’). To compensate for the loss of generator at bus 1, the remaining generators ramp up as per the dispatch schedule (post contingency). As generator at bus 1 was generating 90 MW

Table 3: Attack Vector for Power Flow Measurements in IEEE 14 Bus System (LC-Line Contingency Only; GLC-Both Generator and Line Contingency)

Line	ΔF (MW)		Line	ΔF (MW)	
	LC	GLC		LC	GLC
1-2	0	0	6-11	0	-0.140
1-5	0	0	6-12	-0.417	0
2-3	1.446	0	6-13	-0.907	0
2-4	0	0	7-8	0	0
2-5	0	0	7-9	0	-0.934
3-4	-1.604	0	9-10	-0.883	0.235
4-5	0	0	9-14	-0.511	0.247
4-7	0	-0.934	10-11	0	0.140
4-9	0	-0.536	12-13	-0.058	0
5-6	-0.223	-0.859	13-14	0.139	0

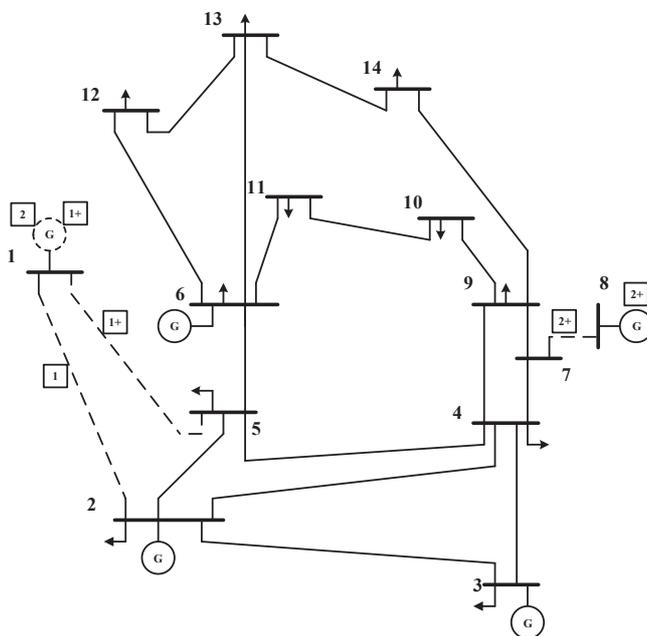


Figure 3: Critical lines and sequence of events (post-attack). ‘1’/‘2’ is target event and ‘1+’/‘2+’ are events post occurrence of ‘1’/‘2’

of power before being disconnected by co-ordinated attack on line 1-2, the generation at bus 8, is limited by the physical limit of line 7-8 which is considered to be 60 MW in this study. This opens-up a another vulnerability in the event of attack on line 7-8 which can disconnect generator at bus 8 (shown as event ‘2+’ in Fig. 3).

The study reveals that for IEEE 14 bus system, line 1-2, 1-5 and 7-8; generator at bus 1 and bus 8 are the most critical lines and generators considering the attack on SCOPF. As the change in the meters caused by the attacker is significantly less ($\approx 1\%$), therefore, the attack will not be detected by the existing detection methods [19–23] and hence protecting these critical measurements alleviates the attack on SCOPF.

Similarly, for IEEE 30 bus system, considering line contingencies only, the attack vector for load and power flow measurements are given in Table 4 and Table 5 respectively. As shown in the table, 18 load and 38 power flow measurements are required to launch the attack. If both generator and line contingencies are considered, the number of measurements required to launch the attack for this case are 13 and 38 for load and power flow measurements respectively.

Table 4: Attack Vector for Load Measurements in IEEE 30 Bus System (LC-Line Contingency Only; GLC-Both Generator and Line Contingency)

Bus	ΔPD (MW)		Bus	ΔPD (MW)	
	LC	GLC		LC	GLC
1	0	0	16	0.064	-0.254
2	0.358	-0.219	17	0.183	0
3	-0.129	-0.068	18	0.087	0
4	0.371	-0.221	19	-0.187	0.131
5	1.128	0.517	20	-0.102	0.166
6	0	0	21	0	0.316
7	-2.035	-0.567	22	0	0
8	0	0	23	-0.269	0
9	0	0	24	0.126	-0.492
10	-0.189	0.421	25	0	0
11	0	0	26	-0.128	0
12	0.532	0.107	27	0	0
13	0	0	28	0	0
14	0.480	0	29	0.041	0
15	-0.340	0.153	30	0	0

For both the cases in IEEE 30 bus system, the critical lines identified are line 1-2 and line 1-3. Tripping either of the line causes tripping of the other and hence, it becomes necessary for the system operator to secure the measurements of these line to avoid such attacks. Moreover, it is worth noting that unlike IEEE 14 bus cases tripping of line 1-2 and 1-3 does not make system vulnerable as the remaining line remain in the limits even if the generator connected at bus 1 is taken out. However, considering different line limits,

Table 5: Attack Vector for Power Flow Measurements in IEEE 30 Bus System (LC-Line Contingency Only; GLC-Both Generator and Line Contingency)

Line	ΔF (MW)		Line	ΔF (MW)	
	LC	GLC		LC	GLC
1-2	0	0	15-18	-0.115	0.136
1-3	0	0	18-19	-0.202	0.136
2-4	0	0	19-20	0	0
3-4	0	0	10-20	-0.087	0.161
2-5	0	0	10-17	0.337	-0.170
2-6	-0.238	0	10-21	0	0
4-6	-0.649	0	10-22	0	-0.050
5-7	-1.091	-0.358	21-22	0	-0.316
6-7	-0.944	-0.209	15-23	-0.225	-0.126
6-8	0	0	22-24	0	-0.367
6-9	0	0.230	23-24	0.044	-0.126
6-10	0	0.132	24-25	-0.080	0
9-11	0	0	25-26	-0.128	0
9-10	0	0.230	25-27	0.048	0
4-12	0.241	0.186	28-27	0	0
12-13	0	0	27-29	0	0
12-14	0.119	0	27-30	0	0
12-15	-0.320	0.127	29-30	0	0
12-16	-0.090	-0.084	8-28	0	0
14-15	-0.361	0.036	6-28	0	0
16-17	-0.154	0.170			

diverse results can be obtained.

The results obtained for IEEE 14 and 30 bus system shows how an attacker can cause a system wide cascaded tipping by modelling a false data injection attack on security constrained optimal power flow. In order to see the wider impact of these attacks, a pessimistic approach is considered with lower line limits and it is assumed that the attacker can attack all the load and flow measurements, this also helps in deciding the best protection strategy for the system operator by identifying the critical set of sensors required to be protected. The study exposes the vulnerabilities of the power system in the advent of false data injection attacks on load and flow sensors. It is worth noting that fully measured power system is considered and therefore the number of meters required to launch the attack are more. In practice the number of measurement sensors in the network are lot less and are just sufficient enough to assure observability of the system. Hence the meters required in practical cases would be far less.

5 Conclusion and Future Scope

The recent research in the area of cyber-physical systems reveals that cyber-attacks in smart grid can cause serious repercussions. In order to completely secure the power grid, it is important to study all the impacts of cyber-threats. In this paper, we have presented an attack on security constrained optimal power flow. We have seen how an adversary can modify the load measurements causing the system operator to inaccurately re-dispatch the generators and thus making the power system $N - 1$ in-compliant. By modelling the attack as a bi-level optimization problem, minimum number of the meters required by an attacker to launch the attack are obtained for IEEE 14 bus and 30 bus test systems. Furthermore, knowledge of these set of meters can be helpful of the system operator in securing the minimum set of meters to alleviate the possibility of the attack. In future work we will further analyse the impacts of cyber-attacks on electric vehicles and distribution side of power system. In addition our research on detection of false data injection attacks is ongoing.

6 Appendices

6.1 Generator data for three bus system

The generator cost data for the three bus example is given in Table 6 where, a_i , b_i and c_i are quadratic, linear and constant cost coefficients for each generator i .

Table 6: Generator Cost Data for 3 Bus System

Bus	a_i	b_i	c_i
1	0.00142	7.20	510
2	0.00194	7.85	310

6.2 Line limits for IEEE test systems

The line limits used for IEEE 14 bus and 30 bus system is given in Table 7 and Table 8 respectively.

Table 7: IEEE 14 Bus Line Limits

Line	Limit (MW)	Line	Limit (MW)
1-2	140	6-11	50
1-5	90	6-12	60
2-3	60	6-13	60
2-4	90	7-8	60
2-5	75	7-9	60
3-4	90	9-10	60
4-5	70	9-14	50
4-7	80	10-11	40
4-9	60	12-13	40
5-6	70	13-14	40

References

- [1] Abur A, Exposito AG. Power system state estimation: theory and implementation. CRC Press; 2004.
- [2] Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security (TISSEC). 2011;14(1):13.
- [3] Qin Z, Li Q, Chuah MC. Unidentifiable attacks in electric power systems. In: Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems. IEEE Computer Society; 2012. p. 193–202.
- [4] Kosut O, Jia L, Thomas RJ, Tong L. Malicious data attacks on the smart grid. Smart Grid, IEEE Transactions on. 2011;2(4):645–658.
- [5] Mo Y, Kim THJ, Brancik K, Dickinson D, Lee H, Perrig A, et al. Cyber-Physical Security of a Smart Grid Infrastructure. Proceedings of the IEEE. 2012 Jan;100(1):195–209.

Table 8: IEEE 30 Bus Line Limits

Line	Limit (MW)	Line	Limit (MW)
1-2	150	15-18	32
1-3	150	18-19	32
2-4	80	19-20	50
3-4	150	10-20	50
2-5	150	10-17	50
2-6	80	10-21	50
4-6	100	10-22	50
5-7	85	21-22	50
6-7	150	15-23	32
6-8	50	22-24	32
6-9	80	23-24	32
6-10	50	24-25	32
9-11	80	25-26	32
9-10	80	25-27	32
4-12	80	28-27	80
12-13	80	27-29	32
12-14	50	27-30	32
12-15	50	29-30	32
12-16	50	8-28	50
14-15	32	6-28	50
16-17	32	-	-

- [6] Valenzuela J, Wang J, Bissinger N. Real-time intrusion detection in power system operations. *Power Systems, IEEE Transactions on*. 2013;28(2):1052–1062.
- [7] Mohsenian-Rad AH, Leon-Garcia A. Distributed Internet-Based Load Altering Attacks Against Smart Power Grids. *IEEE Transactions on Smart Grid*. 2011 Dec;2(4):667–674.
- [8] Dan G, Sandberg H. Stealth Attacks and Protection Schemes for State Estimators in Power Systems. In: *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*; 2010. p. 214–219.
- [9] Giani A, Bitar E, Garcia M, McQueen M, Khargonekar P, Poolla K. Smart grid data integrity attacks. *Smart Grid, IEEE Transactions on*. 2013;4(3):1244–1253.
- [10] Kosut O, Jia L, Thomas RJ, Tong L. Limiting false data attacks on power system state estimation. In: *Information Sciences and Systems (CISS), 2010 44th Annual Conference on*; 2010. p. 1–6.
- [11] Hug G, Giampapa JA. Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks. *IEEE Transactions on Smart Grid*. 2012 Sept;3(3):1362–1370.

- [12] Yuan Y, Li Z, Ren K. Quantitative analysis of load redistribution attacks in power systems. *Parallel and Distributed Systems, IEEE Transactions on*. 2012;23(9):1731–1738.
- [13] Liu X, Li Z. Trilevel Modeling of Cyber Attacks on Transmission Lines. *IEEE Transactions on Smart Grid*. 2015;PP(99):1–1.
- [14] Xie L, Mo Y, Sinopoli B. False data injection attacks in electricity markets. In: *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE; 2010. p. 226–231.
- [15] Khanna K, Panigrahi BK, Joshi A. Bid Modification Attack in Smart Grid for Monetary Benefits. In: *Nanoelectronic and Information Systems (iNIS), 2016 IEEE International Symposium on*. IEEE; 2016. p. 224–229.
- [16] Khanna K, Panigrahi BK, Joshi A. Data integrity attack in smart grid: optimised attack to gain momentary economic profit. *IET Generation, Transmission & Distribution*. 2016;10(16):4032–4039.
- [17] Yang Q, Yang J, Yu W, An D, Zhang N, Zhao W. On false data-injection attacks against power system state estimation: Modeling and countermeasures. *Parallel and Distributed Systems, IEEE Transactions on*. 2014;25(3):717–729.
- [18] Bobba RB, Rogers KM, Wang Q, Khurana H, Nahrstedt K, Overbye TJ. Detecting false data injection attacks on dc state estimation. In: *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*. vol. 2010; 2010. .
- [19] Liu L, Esmalifalak M, Ding Q, Emesih VA, Han Z. Detecting false data injection attacks on power grid by sparse optimization. *IEEE Trans Smart Grid*. 2014;5(2):612–621.
- [20] Li S, Ylmaz Y, Wang X. Quickest Detection of False Data Injection Attack in Wide-Area Smart Grids. *IEEE Trans on Smart Grid*. 2015 Nov;6(6):2725–2735.
- [21] Huang Y, Tang J, Cheng Y, Li H, Campbell KA, Han Z. Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis. *IEEE Syst J*. 2016 June;10(2):532–543.
- [22] Liu X, Zhu P, Zhang Y, Chen K. A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure. *IEEE Trans on Smart Grid*. 2015 Sept;6(5):2435–2443.

- [23] Chaojun G, Jirutitijaroen P, Motani M. Detecting False Data Injection Attacks in AC State Estimation. *IEEE Trans Smart Grid*. 2015;6(5):2476–2483.
- [24] Yumbla PEO, Ramirez JM, Coello CAC. Optimal power flow subject to security constraints solved with a particle swarm optimizer. *Power Systems, IEEE Transactions on*. 2008;23(1):33–40.
- [25] Yuan Y, Li Z, Ren K. Modeling load redistribution attacks in power systems. *Smart Grid, IEEE Transactions on*. 2011;2(2):382–390.
- [26] Liu X, Li Z. Local load redistribution attacks in power systems with incomplete network information. *Smart Grid, IEEE Transactions on*. 2014;5(4):1665–1676.
- [27] Khanna K, Panigrahi BK, Joshi A. Feasibility and mitigation of false data injection attacks in smart grid. In: *Power Systems (ICPS), 2016 IEEE 6th International Conference on*. IEEE; 2016. p. 1–6.
- [28] Alsac O, Stott B. Optimal load flow with steady-state security. *Power Apparatus and Systems, IEEE Transactions on*. 1974;(3):745–751.
- [29] Power Systems Test Case Archive;. Available from: <http://www2.ee.washington.edu/research/pstca/>.