Data Integrity Attack in Smart Grid: Optimized Attack to Gain Momentary Economic Profit

Kush Khanna*, Bijaya Ketan Panigrahi*and Anupam Joshi†

Abstract

The cyber-physical security of power grid has gained more attention in the research community due to integration of information and communication technologies. Smart meters are vulnerable to cyber-threats and if the security of these meters are compromised then the consequence can be devastating. It is necessary to study all the possible impacts that cyber-attacks may have on the power grid in order to make the grid immune to such intrusions. With more and more renewable energy and information technology integration, electricity companies must make sure that they are not paying for spoofed electricity. In this paper, we are proposing a new attack through which a private actor injects false data into multiple meters to deceive the system operator with new modified system state to gain momentary profit by projecting higher energy export than actual. Assuming real power injection measurement to be secured at all the generator buses, the attack is simulated for IEEE 14 bus and IEEE 30 bus system. From the system operator's perspective, the most vulnerable buses are obtained and ranked based on the severity and minimum set of meters required to launch an attack.

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

Nomenclature

$\boldsymbol{\delta}_{\boldsymbol{N}_i^{pri}}$ Load angle vector for the primary attacking region.

$\boldsymbol{\delta}$ Column matrix for angles in radians.

*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).

$\boldsymbol{B_{N_i^{pri}}}$ Bus susceptance matrix for the primary attacking region.

$\boldsymbol{B}$ Bus admittance matrix of the network.

$\boldsymbol{P_D^{N_i pri}}$ Real power demand vector of the primary attacking region.

$\boldsymbol{P_{N_i^{pri}}}$ Power injection vector for the primary attacking region.

Δf Net changes in the line flows in the attacking region.

ϕ Null set.

a Attack Vector.

BB_i^{pri} Set of boundary buses for the attacking region N_i^{pri}.

BB_i^{ext} Set of the boundary buses for the extended attacking region.

c Estimated error injected in the state variable by the attacker.

e Measurement error.

$F_g(P_{Gg})$ Cost of the generator at bus g.

H $[h_{ij}]_{m\times n}$.

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

i Bus at which DG is placed.

N_G Set of generator buses.

N_i^{adj} Set of all the adjoining buses of the primary region N_i^{pri}.

N_i^{pri} Set of buses in primary attacking region for the bus i.

N_{Bi} Set of all buses directly connected to bus i.

N_{Bj} Set of all the buses directly connected to bus j.

N_{ik}^{ext} Set of all the buses in the extended attacking region considering k^{th} subset of power set $\mathcal{P}(N_i^{adj})$.

p Total number of subsets of the power set $\mathcal{P}(N_i^{adj})$.

P_D Column matrix for the power demand.

P_G Column matrix for the power generation.

P_{Gg} Power generation at bus g.

P_{Gg}^{max} Maximum generation specified for the generator at the bus g.

P_{Gg}^{min} Minimum generation specified for the generator at the bus g.

x State variable vector ($n \times 1$).

z True measurement vector ($m \times 1$).

z_a Measurement vector with false data injected.

1 Introduction

Modern power system with integrated communication technologies has improved reliability and efficiency of electrical energy. In addition, smart grid has enabled Advanced Metering Infrastructure (AMI) and Demand Response which provides better transparency and also offers incentives to end users by asking them to reduce the consumption in return [1]. This complex web of communication infrastructure has also opened up new possibilities of cyber threats. The communication medium is prone to cyber intrusion and in order to mitigate the cyber threats it is important to first know all the possible consequences of these attacks.

To launch an attack, attacker must either know the set of critical meters in advance, or the attack vector must be formulated such that the perturbed measurements bypasses the bad data estimation. An attack can also be launched by randomly changing enough sets of measurements which results in erroneous state estimation [2]. In former scenario, attacker must have knowledge of the network topology to form attack vector. Attacker injects the malicious data to obtain the desired change in states which further reflects a possible but compromised operating snapshot of the power system to the system operator. However, in latter scenario, attacker must have access to sufficient number of meters to launch the attack and moreover some of these meters must be critical meters to cause change in estimated states.

In the emerging decentralized power markets of the developing countries like India, the system operator is not involved in day ahead market. Sellers and buyers submit their bids to power exchange. Power exchange generate the aggregated supply-demand curve to obtain the Market Clearing Price (MCP). The schedules at this instant of market clearing are forwarded to the system operator which performs the security analysis and report back to power exchange in case of congestion. In case of congestion, power exchange clears the market after performing the market splitting mechanism [3]. This process continues until the congestion is cleared. Once the congestion is cleared, power exchange provides the

schedules to buyers and the sellers. A private actor, if hacks into power exchange server and compromises the confidentiality of the seller and buyer information, can launch a data integrity attack by modifying the dispatch schedules to gain the momentary profit, thereby creating a new power theft scenario in which Distributed Generators (DGs) can project higher energy export to the grid than actual. Even if the attacker does not have access to the critical bid information about the loads and dispatch, attack can still be launched with smaller changes in the appropriate meters without getting detected which is explained in this paper by considering IEEE 14 bus and IEEE 30 bus system.

In this paper we are exploring the economic impacts of false data injection attacks on the power grid. We are explaining for the first time that how an adversary, a private actor who owns a small distributed generation and supplies excess power to grid, can modify measurement to launch an attack aiming to maximize its profit. From the attacker's perspective, the suitable attack vector for maximizing the spoofed energy export by distributed generation for launching the attack is found by considering minimum set of meters to be hacked. From the system operator's perspective it is a planning problem, the most vulnerable buses based on the severity of the attack are found and if a distributed generation is placed at such location aiming for either loss minimization or to handle the ever increasing energy demands, the meters at these locations must be secured to avoid cyber-threats. A more serious version of this attack can be formulated if the attacker hacks into the power exchange server and modifies the dispatch schedules.

The research in the area of cyber-physical systems are focused primarily on the modelling of different attacks and finding ways to make a power grid resilient and immune to cyber-threats. Taxonomy of cyber-attacks for smart grid is proposed in [4]. Liu et al. [5] demonstrated false data injection attacks. Attacker with complete knowledge of network topology and parameter information can modify the estimated states by injecting a planned error vector in the meters. It is also realized that attack cannot be detected by residue test if error vector Δz is a function of Jacobian H and desired change in state variable Δx. In [6], malicious data attacks were further explained. Attacks were categorized as strong attacks regime and weak attack regime. Adversary with access to critical meters causes a strong attack which is undetectable. In weak attacks adversary alters the adequate meters to make the state estimation result erroneous. Although the weak attack can be detected but the detection is rather imperfect due to presence of measurement errors. Load redistribution attacks and load increased attacks were first proposed by Qin et al. [2] where attacker modifies load meter data at load buses such that the net change in load on the system is zero. Local load redistribution attack based on incomplete network information is presented by Liu et al. [7]. It is observed that an adversary, short of complete network information can still launch an attack without being detected. In [8] vulnerability of AC state estimation is presented against the false data

injection attacks. False data injection attacks on electricity markets are described in [9]. In [10], optimal attacking region is determined based on reduced network knowledge using mixed linear integer programming (MILP). Communication line failure, denial of service (DoS) and man in the middle (MITM) attack using real time digital simulator (RTDS) and Phasor Measurement Units (PMU) is presented in [11]. The impact of aurora attack is demonstrated in [12]. Closeness centrality measures is used to rank the N-X generator outages. It is observed that an attacker can model aurora-like attack with reduced network information.

In recent years many methods are proposed to lessen the chances of false data injection attacks. In [13–17], false data injection attacks are alleviated by securing critical measurements. This defence mechanism is only suited if the protected meters remain secure all the time. If the adversary breach the security of such meters then state estimation will again be erroneous. Extended Distributed State Estimation (EDSE) based method is presented to detect data integrity attacks in smart grids [18]. In [19], authors proposed detection based methods to identify the attacks. Kullback-Leibler Distance (KLD) is proposed to detect the false data injection attacks by comparing probability distribution of measurement variation for historical data and current time step. The proposed method fails to detect the attack on some state variables. State summation strategy for detecting false data injection attacks is described in [20]. In [21] spatial-temporal correlation based scheme is proposed for detecting false data injection attacks.

The above literature emphasize on the physical impacts of various cyber-threats on the transmission network, however, this paper presents a possibility of a financial misconduct, an attacker can cause by injecting false data in the measurement sensors. The salient contributions of this paper are,

- Finding all possible attacking regions based on the assumptions discussed in Section II.
- Modelling an attack which is confined to a small attacking region to maximize the generation at a particular bus (attacker's perspective).
- Obtaining and ranking the most vulnerable buses for launching the attack based on the maximum generation obtained and minimum number of meters required to launch an attack (system operator's perspective).

The attacking locations considered in this paper are not based on any optimal distributed generation placement strategy, but is rather more generalized in order to see the larger impact of such attacks on entire power system. All the load buses (PQ buses) are considered as possible location for considering a DG based on the viability of the attacking region. It is worth noting that here DG is assumed to be a competitive player in

electricity market, therefore, in all the different attack scenarios presented in the paper, DG is assumed to be directly connected to transmission network [22]. An adversary on faking the meter readings by showing more energy export to the grid can obtain a short term economic profit.

The rest of the paper is organized as follows. In section II, proposed attacking model is discussed and the formulation of optimal attacking region and attack parameters with all the assumptions are presented. IEEE 14 bus and IEEE 30 bus test cases are described in section III. Section IV presents the results and discussion. Existing methods and their limitations to detect these attacks are explained in section V. Finally the concluding remarks and the future scope is presented in section VI.

2 Proposed Work

In recent research on cyber security issues in smart grids, the impacts of various cyber events have been analysed in [2, 5–7, 10]. Economic impacts of the false data injection attacks by spoofed electricity export are presented in this paper. In this work we show that how an attacker who is selling power to the grid can gain momentary profit by injecting false data to the meters. For this work we have taken following assumptions:

1. All the meters at the PV (generator buses) buses are assumed secure as these meters can be physically secured or crosschecked by the power plant operator. Attacking these requires overcoming physical barriers and potentially inside help.

2. All the flow meters in the attacking region can be attacked.

3. All the meters at PQ (load) buses in the attacking region can be attacked.

4. Attacker has full knowledge of the network topology and parameters in the attacking region [12].

5. Attacker has limited access to the meters in the network, as launching a coordinated attack by attacking all the meters at same time is impractical.

These assumptions are sufficient to cause the attack. However, more serious attack can be crafted if we are allowed in addition to assume that the attacker has access to day-ahead bidding information.

Based on the above assumptions, firstly, all possible attacking regions are specified for a given network and later a minimum set of meters are found to launch the attack from the attacker's perspective. Attacking region and the attack model are now defined with illustrative example in this section.

2.1 Attacking Region

As per the assumption that generator buses are not attacked, the primary attacking region does not contain any generator bus. The primary attacking region N_i^{pri} is defined as,

$$N_i^{pri} = \{N_{Bi} \cup \{i\} : N_i^{pri} \cap N_G = \phi\} \tag{1}$$

[Figure 1 about here.]

Primary attacking region for a simple six bus system is shown in Fig. 1. It can be easily deduced that being a generator bus, bus 1 and bus 4 cannot be in a attacking region. Similarly bus 2 and bus 5 are directly connected to either of the generator buses or both. Therefore, the only primary attacking regions for this six bus network are $N_3^{pri} = \{2, 3, 6\}$ and $N_6^{pri} = \{3, 5, 6\}$.

If the optimization problem converges to a solution exactly same as the pre-attacked (base case) solution for the primary attacking region; the attacker fails to form an attack vector with given set of buses in the attacking region. The attacking region is then expanded and the optimization problem is again solved for increased number of buses. Extension of primary attacking region can be formulated using following equations,

$$N_i^{adj} = N_{Bj} - N_G - N_i^{pri}; \quad \forall j \in N_i^{pri} \tag{2}$$

$$N_{ik}^{ext} = N_i^{pri} \cup \{\mathcal{P}(N_i^{adj})\}_k; \quad k = 1, 2, .., p \tag{3}$$

here p is the total number of the subsets of the power set $\mathcal{P}(N_i^{adj})$ i.e. $p = 2^{|N_i^{adj}|} - 1$.

[Figure 2 about here.]

The extented attacking region of N_3^{pri} and N_6^{pri} is shown in the Fig 2. N_{B3} for $j = \{2, 3, 6\}$ is $\{\{1, 3\}, \{2, 6\}, \{3, 5\}\}$. Hence N_3^{adj} obtained from the equation (2) is $\{5\}$. Therefore the extended attacking region N_3^{ext} from equation (3) is only $\{2, 3, 5, 6\}$ as the power set has only one subset. Similarly for the primary attacking region N_6^{pri}, N_6^{ext} is also $\{2, 3, 5, 6\}$. As both the extended regions are same, therefore we have only one extended region as shown in the Fig 2.

2.2 Attack Model

Assuming the true measurement $z = h(x) + e$ passes the bad data detection, for a DC model, the malicious measurement $z_a = z + a$ will pass the bad data detection when a is

the linear combination of column vectors of H (i.e. $a = Hc$). The proof is given in [5].

After obtaining the primary attacking region, the distributed generator is considered on the i^{th} bus for the region N_i^{pri}. It is worth noting that the location for DG is fixed at i^{th} bus for the attacker and only the attacking region can be expanded as per the feasibility of the attack considering the set of buses in the attacking region. Hence, the attacker will model the attack only for the i^{th} bus to calculate the required attack vector. The impacts of various DG locations are considered only for the system operator at the planning stage in order to secure the necessary meters to alleviate these attacks. Using DC optimal power flow (DCOPF), the dispatch schedule is obtained for each generator including the distributed generation for the given loading conditions at all the buses. This will be the operating point for the power system without any attack.

An adversary can model the attack which is confined to the primary attacking region. It is assumed that attacker can inject false data in all the meters in the attacking region only. DCOPF is used to model the attack, therefore, resistances of the transmission lines, shunt elements and transformer tap settings are not considered. The voltage at each bus is fixed to 1.0 pu. Generation limits are considered for the optimum power flow and the transmission line limits are kept open as the attack is considered to cause only momentary change in the power flow but not to cause power system instability.

The initial operating state of the power system can be obtained by running the DCOPF considering an extra generator in the network at the i^{th} bus for the attacking region N_i^{pri}. With generation cost minimisation as objective, DCOPF can be formulated as,

$$\min_{P_G} \sum_{g=1}^{N_G} F_g(P_{Gg}) \tag{4}$$

The generator limit inequality constrains are given as,

$$P_{Gg}^{min} \leq P_{Gg} \leq P_{Gg}^{max} \quad \forall g \in N_G \tag{5}$$

The nodal power balance equation can be formulated as,

$$\boldsymbol{B} \cdot \boldsymbol{\delta} = \boldsymbol{P_G} - \boldsymbol{P_D} \tag{6}$$

Once the pre-attack state of the power system by solving the optimisation problem given in equation (4) is obtained, base case flows and nodal power injections at each line and buses respectively are calculated with a DG at i^{th} bus.

Let P_{Gi} be the real power generation, δ_i be the load angle in radians and P_{Di} be the

load at the i^{th} bus. As proposed earlier in [7], in order to make sure that the attack remain local i.e. the impact of perturbed measurements is not reflected outside the attacking region, change in the load angle for the boundary buses is kept equal to the change in the load angle of the buses in the non-attacking region. In order to gain momentary profit, attacker solves an optimization problem to maximize the power injection at the i^{th} bus of the attacking region N_i^{pri}.

$$\max_{\boldsymbol{P_D^{N_i pri}}, P_{Gi}} \Big\{ \sum_{l=1, l\neq i}^{|N_i^{pri}|} -B_{il}(\delta_l - \delta_i) \Big\} \tag{7}$$

subjected to,

$$\delta_m = \delta_m^{pre-attack}; \quad \forall m \in (N_{bus} - N_i^{pri}) \cup BB_i^{pri}, m \neq i \tag{8}$$

$$P_{Gm} = P_{Gm}^{pre-attack}; \quad \forall m \in N_G, m \neq i \tag{9}$$

$$P_{Dm} = P_{Dm}^{pre-attack}; \quad \forall m \in (N_{bus} - N_i^{pri}) \tag{10}$$

$$P_{Gi}^{pre-attack} \leq P_{Gi} \leq 1.5(P_{Gi}^{pre-attack}) \tag{11}$$

$$0.5(P_{Dm}^{pre-attack}) \leq P_{Dm} \leq 1.5(P_{Dm}^{pre-attack}); \quad \forall m \in N_i^{pri} \tag{12}$$

$$\pi/2 \leq \delta_m \leq \pi/2; \quad \forall m \in (N_i^{pri} - BB_i^{pri}) \tag{13}$$

$$\boldsymbol{P_{N_i^{pri}}} = \boldsymbol{B_{N_i^{pri}}} \cdot \boldsymbol{\delta_{N_i^{pri}}} \tag{14}$$

The attack vectors are obtained by solving equations (7-14). The decision variables used for the optimization problem here are generation at i^{th} bus P_{Gi} and all the loads in the attacking region within the range specified in equations (11-12). Equations (8-10) represents the constraints for the non-attacking region, all the loads and the generation is fixed to the previously obtained value through DCOPF. Load angles for the boundary buses are fixed to the initial values to make sure that there is no change in the line flows in the non-attacking region.

The constraints for the attacking region are given in equations (11)-(14). The distributed generation is allowed to increase to a maximum of 1.5 times of its pre-attacked value, while the lower bound is fixed at the pre-attacked value. Similarly the load at all the load buses in the attacking region N_i^{pri} is allowed to vary from 0.5 to 1.5 times of the pre-attacked value, in order to deceive the operator cleverly without raising suspicions, however, if the attacker has access to the critical bid information, the limits in (11) and (12) can be further relaxed. Load angles for the non-boundary buses are allowed to vary from $-\pi/2$ to $+\pi/2$.

After solving this optimization problem, the new loads and load angles for the attacking region are obtained. Let the net change in the angles, power generation and the demand be $\Delta\delta$, ΔP_G and ΔP_D respectively. The net changes in the line flows in the attacking region is given by,

$$\Delta f_{mn} = \frac{1}{x_{mn}}(\Delta\delta_m - \Delta\delta_n) \quad \forall m, n \in N_i^{pri} \tag{15}$$

where x_{mn} is the reactance of the line connecting bus m and n.

[Figure 3 about here.]

An attack considering distributed generation at bus 3 is shown in the Fig 3. The meters in which the false data is injected are also shown. To make sure that the attack bypasses the bad data detection algorithm, all the meters (power injection and power flow) in the attacking region are injected with the false data. If for the primary attacking region, the angles and the power injections converge to the same pre-attacked value, the region is expanded as given by equation (2-3). The equations for modelling an attack remains more or less same. The changes are, we use N_{ik}^{ext} instead of N_i^{pri} and BB_i^{ext} is place of BB_i^{pri}. Here BB_i^{ext} is a set of boundary buses for the extended attacking region N_{ik}^{ext}. The distributed generation is then placed on each non boundary bus $(N_{ik}^{ext} - BB_i^{ext})$ and optimization problem is solved for each case.

For the six bus system shown in the Fig 2, the extended region N_{ik}^{ext} is $\{2, 3, 5, 6\}$ with the non-boundary buses $\{3, 6\}$. Meters required for launching the attack for both locations can be found by first placing distributed generation on the 3^{rd} bus. Pre-attacked values are obtained from DCOPF and then equation (7) is solved. The attack vector is obtained and the steps are repeated for obtaining the attack vector corresponding to 6^{th} bus. The buses are then ranked as per the vulnerability to cyber-attacks and its consequence based on the maximum generation obtained after solving the optimization problem.

The maximum change in the generation(ΔP) obtained at the i^{th} bus is $P_G^{(i)} - P_G^{pre-attack(i)}$. Therefore the profit obtained by hacking the meters is MCP (or the price of costliest generation for the 15 minute window as per the Indian market) times ΔP for the attack with full knowledge of the day ahead bidding. As the price is constant and not related to the attack model, therefore, profit can be considered as directly proportional to ΔP or the maximum value of the P_G at the i^{ith} bus after attack.

3 Test Systems

3.1 IEEE 14 bus

The primary attacking regions for IEEE 14 bus system is shown in Fig 4. As shown, there are total three primary attacking regions N_9^{pri}, N_{10}^{pri} and N_{14}^{pri}. The distributed generation is considered on 9^{th}, 10^{th} and 14^{th} bus one at a time to obtain the maximum generation at that bus without affecting line flows and power injections at all the bus in the non-attacking region.

[Figure 4 about here.]

In case after solving the optimization problem the generation and the load in the attacking region remains unaltered for the primary attacking region N_i^{pri}, then the region is expanded. The extended attacking regions are,

- $\{4, 7, 9, 10, 11, 14\}$
- $\{4, 7, 9, 10, 13, 14\}$
- $\{7, 9, 10, 11, 13, 14\}$
- $\{9, 10, 11, 13, 14\}$
- $\{9, 10, 11, 12, 13, 14\}$

As the angles of the boundary buses remain fixed at the pre-attacked value, the optimization problem gives the same base case solution sometimes when only one non-boundary bus is present in the primary attacking region. Therefore, obtaining the extended attacking region, besides equations (2) and (3), it is important to make sure that the new expanded region must have at least two non-boundary buses. Hence, for each of the subset of the power set $\mathcal{P}(N_i^{adj})$,

$$|N_{ik}^{ext} - BB_i^{ext}| \geq 2 \tag{16}$$

$$|N_{ik}^{ext}| < 0.5 \cdot |N_{bus}| \tag{17}$$

The number of buses in the extended attacking region is restricted to be less than half of the number of buses in the entire system. This constraint is important to make sure that attacking region is small which results in lesser number of meters required to launch an attack. Hence, in the case of IEEE 14 bus system maximum number of buses in the extended attacking region is limited to six. Subsequently, an attack is modelled considering a distributed generation at each non-boundary bus one at a time for the extended attacking region N_{ik}^{ext}.

3.2 IEEE 30 bus

Primary attacking regions for IEEE 30 bus system is shown is Fig 5. Table 1 provides a detailed list of the attacking regions. The distributed generation is placed on each of the i^{th} bus for all the attacking regions given in the Table 1 for obtaining the attack vectors corresponding to the region N_i^{pri}.

[Figure 5 about here.]

Extended attacking regions can be obtained by using equations (2-3) and (16-17). The maximum number of buses in the extended attacking region is limited to 14 buses in this case. Total of 92 extended regions are obtained for IEEE 30 bus system.

[Table 1 about here.]

4 Results and Discussion

The attack is modelled using equations (1-17) in MATLAB. Generator cost data for IEEE 14 bus and IEEE 30 bus systems are taken from the MATPOWER v5.1 cases. The cost of the distributed generation is taken as $0.30P_G^2 + 33P_G$, which is slightly costlier than generator 2 in IEEE 14 bus and IEEE 30 bus test systems. It is assumed that the attacker does not have access to day-ahead bidding information, hence the attack is modelled with maximum error injection in the load meters limited to $\pm$ 50% of the base case solution [7]

4.1 IEEE 14 bus

4.1.1 Attacking Region N_9^{pri}

With a distributed generation considered at the 9^{th} bus, attack is modelled. The attack vectors are shown in the Table 2. For the attacking region {4,7,9,10,14}, 9^{th} bus is the only non-boundary bus, therefore, all the load angles δ are fixed to pre-attacked value $\delta^{pre-attack}$ except δ_9. The solution to the problem (7) is the attack vector with no change in the meters, hence, the region must be expanded.

[Table 2 about here.]

For the extended attacking region of $\{4, 7, 9, 10, 11, 14\}$, the non-boundary buses are 9 and 10. The generator is first placed at 9^{th} bus. The attack vector for this case is given in Table 3. The generation at the 9^{th} bus is increased to 9.50 MW. The change is the load as well as in the angle is also given in the Table 3. Similarly for the extended region $\{4, 7, 9, 10, 13, 14\}$, the maximum generation obtained at the $9th$ bus is 9.574 MW as shown in Table 4.

[Table 3 about here.]

[Table 4 about here.]

4.1.2 Attacking Region N_{10}^{pri}

The attack vector is shown in the Table 5 for the attacking region $\{9, 10, 11\}$. The generator is considered at the 10^{th} bus to calculate the pre-attacked values. The boundary buses for this region are $\{9, 11\}$. There is now change in the angles for the boundary buses. The increase in the generation obtained for the same values of flows (pre-attacked) in the non-attacking region is 9.574 MW. This is the maximum generation limit for the distributed generation, as given by equation (11).

[Table 5 about here.]

As the generator at 10^{th} bus hits its limit which was set at $1.5 \times P_G^{pre-attack}$, there is no need for expanding the attacking region.

4.1.3 Attacking Region N_{14}^{pri}

The distributed generation is considered at the 14^{th} bus and the pre-attack values of the generation and load angles are calculated. The attacking region $\{9, 13, 14\}$ consists of two boundary buses $\{9, 13\}$. The angles at the boundary buses are kept at the pre-attack values. The maximum generation obtained after solving the optimization problem is 9.574 MW, which is again the maximum limit for the generator at the 14^{th} bus. Hence, there is no need for expanding this region also. The attack vector is given in Table 6.

[Table 6 about here.]

The attacking regions are then ranked based on the maximum generation obtained and minimum meters required to launch the attack. In all the three cases the maximum generation obtained is same i.e. 9.54 MW, but the attacking region is small for placing generator at 10^{th} and 14^{th} bus. The location of distributed generation with attacking region and rank is shown in Table 7. For both N_{10}^{pri} and N_{14}^{pri} minimum of seven meters (four flow meters and three power injection meters) are required to be compromised for launching an attack.

[Table 7 about here.]

4.2 IEEE 30 bus

For IEEE 30 bus system, the pre-attacked value for the power generated by the distributed generation is 8.82 MW. As per the constraint given in equation (8), the maximum generation limit without violating the δ limits in the non-attacking region is $1.5 \times P_G$ at i^{th} bus i.e. 13.23 MW. The maximum generation obtained (actual+spoofed) for the different attacking regions in the IEEE 30 bus system is given in Table 8. The regions and the buses are then ranked based on the maximum generation obtained and minimum meters required to launch an attack. It is seen from the table that the 14^{th} gives the best suited location for launching an attack as the generation hits its maximum limit and the total number of meters required are nine. Similarly number of meters required for 16^{th}, 17^{th} and 18^{th} are seven with high change in the generation from the pre-attacked value of 8.82 MW.

[Table 8 about here.]

Although bus number 10 provides maximum generation but launching an attack may not be easy as the requirement for number of meters is very high. It may be difficult from the attacker's point to launch an attack as all the required meters may not be accessible. Moreover, 24^{th} bus is ranked lowest in terms of minimum number of meters required and also change in generation obtained is also quite low. For 26^{th} no suitable attack vector is obtained, hence this bus can be stated as the safest bus for placing the distributed generation from the defender's perspective.

5 Detection

If the meters in the attacking region are not secured, attacker can launch the attack without being detected by the system operator. As the attack is not severe enough to cause system instability, it can be detected by the method proposed in [23]. Distributed FACTS (D-FACTS) devices can be used to detect the false data injection attacks. The location of the D-FACTS devices can be decided by analysing the impacts in all possible attacking regions. In IEEE 14 bus system there are three optimal attacking regions, N_9^{ext}, N_{10}^{ext} and N_{14}^{ext}. Line $9-14$ is common in all the optimal attacking regions, therefore, if a D-FACTS device is placed at 9-14 line than the system operator can check the flow meters $P_{9,14}$ and $P_{14,9}$ by dynamically changing the line reactance by very small value $\Delta x_{9,14}$. This change is small enough to cause a slight change in the flow meters without violating the line limits and voltage limits. If the proportional change in the flows is not observed by perturbing the line reactance than it is deduced that the meters are compromised. However, the attacking region cannot be identified by this method. Similarly for the

IEEE 30 bus system the number of D-FACTS devices and their location required to detect the attack can also be obtained using similar approach. For large system this cannot be a viable option as the number of D-FACTS devices increases. Moreover, in case of more severe attack in which the attacker intends to disrupt the power grid, this method of detection is not suitable. Hence, the security of the meters is of utmost priority so that all such cyber-threats can be alleviated.

6 Conclusion

Securing the power grid against the cyber-threats has gained much importance in the recent years. With the possible outcomes like momentary economic profit or even a complete blackout has raised concerns over the security of the smart meters against cyber-events. To alleviate the possibilities of launching a cyber-event aiming to gain economic profit, in this paper all the possible locations of a distributed generation is considered to find out the impact of such attack. The locations are then ranked based to maximum profit and minimum meters required. Securing the meters in the highest ranked regions can be a possible option as of now to reduce the possibilities of the attack. Placing a Distributed FACTS device can be a viable option for alleviating these type of cyber-threats in smaller systems but for the large system the proposed methods in the literature fails to detect the attack. In future we will further explore the impacts of data integrity attacks on smart grid. Our research on detection and identification of attacked meters is ongoing.

References

[1] Barreto C, Giraldo J, Cardenas AA, Mojica-Nava E, Quijano N. Control systems for the power grid and their resiliency to attacks. IEEE Security & Privacy. 2014;(6):15–23.

[2] 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.

[3] Congestion Management;. Indian Energy Exchange. Available from: `http://www.iexindia.com/pdf/dam_appendix2.pdf`.

[4] Hu J, Pota HR, Guo S. Taxonomy of attacks for agent-based smart grids. Parallel and Distributed Systems, IEEE Transactions on. 2014;25(7):1886–1895.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] Xie L, Mo Y, Sinopoli B. False Data Injection Attacks in Electricity Markets. In: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on; 2010. p. 226–231.

[10] Liu X, Bao Z, Lu D, Li Z. Modeling of Local False Data Injection Attacks With Reduced Network Information. Smart Grid, IEEE Transactions on. 2015 July;6(4):1686–1696.

[11] Liu R, Vellaithurai C, Biswas SS, Gamage TT, Srivastava AK. Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid. Smart Grid, IEEE Transactions on. 2015 Sept;6(5):2444–2453.

[12] Srivastava A, Morris T, Ernster T, Vellaithurai C, Pan S, Adhikari U. Modeling cyber-physical vulnerability of the smart grid with incomplete information. Smart Grid, IEEE Transactions on. 2013;4(1):235–244.

[13] 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.

[14] 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. .

[15] Talebi M, Li C, Qu Z. Enhanced protection against false data injection by dynamically changing information structure of microgrids. In: Sensor Array and Multichannel Signal Processing Workshop (SAM), 2012 IEEE 7th. IEEE; 2012. p. 393–396.

[16] Bi S, Zhang YJ. Defending mechanisms against false-data injection attacks in the power system state estimation. In: GLOBECOM Workshops (GC Wkshps), 2011 IEEE. IEEE; 2011. p. 1162–1167.

[17] Bhattarai S, Ge L, Yu W. A novel architecture against false data injection attacks in smart grid. In: Communications (ICC), 2012 IEEE International Conference on. IEEE; 2012. p. 907–911.

[18] Wang D, Guan X, Liu T, Gu Y, Shen C, Xu Z. Extended distributed state estimation: a detection method against tolerable false data injection attacks in smart grids. Energies. 2014;7(3):1517–1538.

[19] Chaojun G, Jirutitijaroen P, Motani M. Detecting False Data Injection Attacks in AC State Estimation. Smart Grid, IEEE Transactions on. 2015;PP(99):1–1.

[20] Li Y, Wang Y. State summation for detecting false data attack on smart grid. International Journal of Electrical Power & Energy Systems. 2014;57:156–163.

[21] Chen PY, Yang S, McCann JA, Lin J, Yang X. Detection of false data injection attacks in smart-grid systems. IEEE Communications Magazine. 2015;53(2):206–213.

[22] Ackermann T, Andersson G, Söder L. Distributed generation: a definition. Electric power systems research. 2001;57(3):195–204.

[23] Morrow KL, Heine E, Rogers KM, Bobba RB, Overbye TJ. Topology Perturbation for Detecting Malicious Data Injection. In: System Science (HICSS), 2012 45th Hawaii International Conference on; 2012. p. 2104–2113.

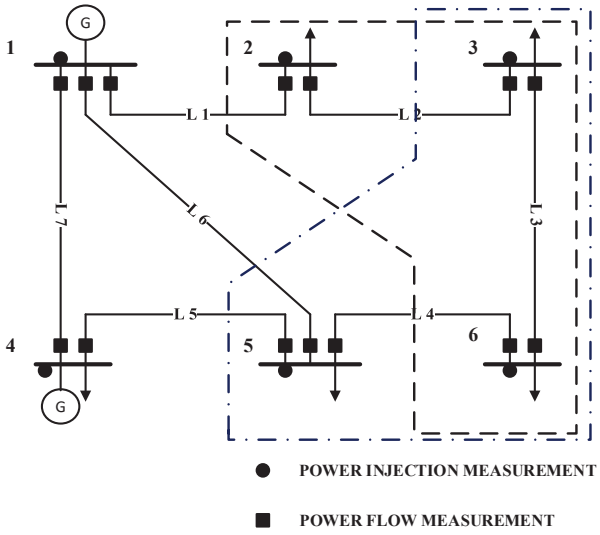

Figure 1: Six bus example with primary attacking region.

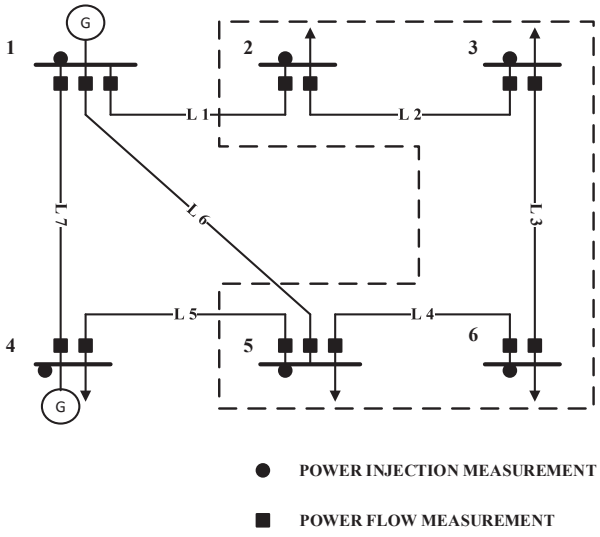

Figure 2: Extended attacking region for simple six bus system.

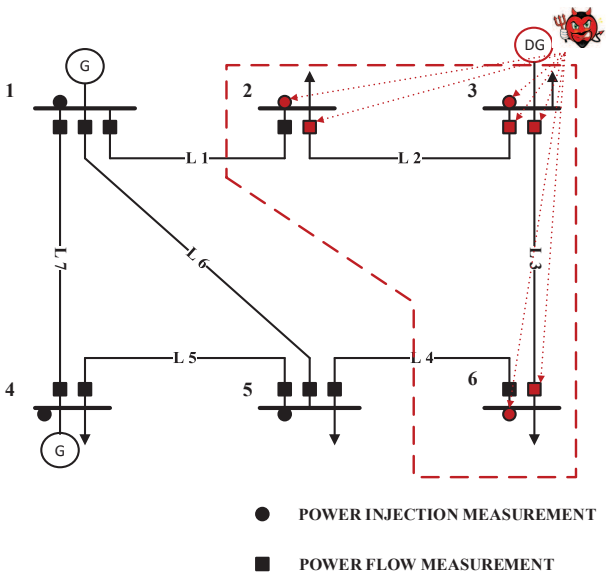

Figure 3: Attack with distributed generator considered at bus 3.

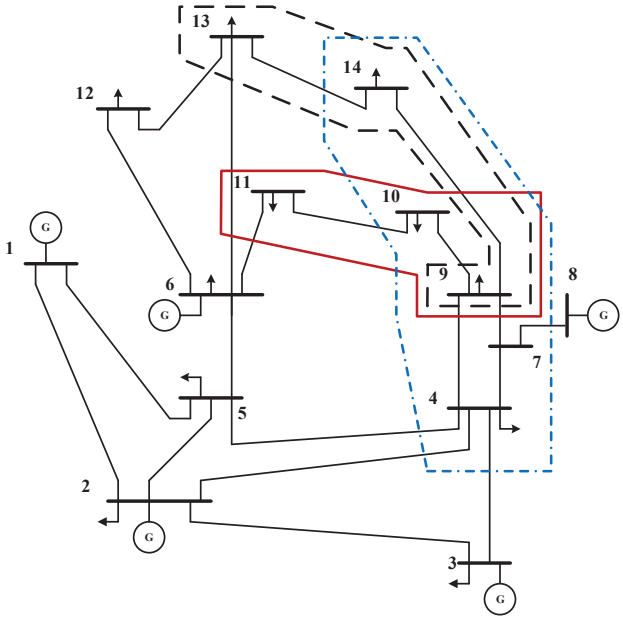

Figure 4: Primary attacking regions for IEEE 14 bus system.

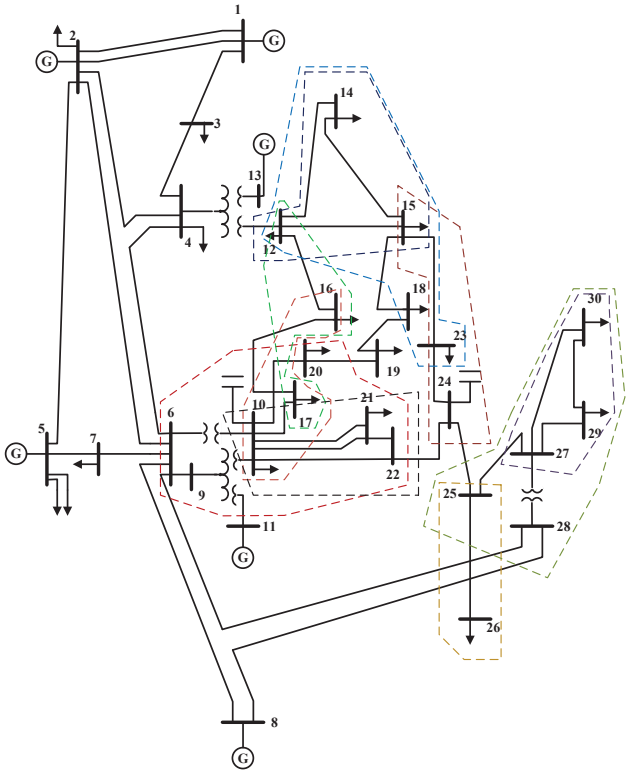

Figure 5: Primary attacking regions for IEEE 30 bus system.

Table 1: Attacking Regions for IEEE 30 Bus System

N_i^{pri}	Attacking Region
10	{6,9,10,17,20,21,22}
14	{12,14,15}
15	{12,14,15,18,23}
16	{12,16,17}
17	{10,16,17}
18	{15,18,19}
19	{18,19,20}
20	{10,19,20}
21	{10,21,22}
22	{10,21,22,24}
23	{15,23,24}
24	{22,23,24,25}
25	{24,25,26,27}
26	{25,26}
27	{25,27,28,29,30}
29	{27,29,30}
30	{27,29,30}

Table 2: Attack Vector for N_9^{pri}

Bus	Pre Attack		Post Attack		$\Delta\delta$ (Deg)
	P_D(MW)	P_G(MW)	P_D(MW)	P_G(MW)	
4	47.8	0	47.8	0	0.0
7	0.0	0	0.0	0	0.0
9	29.5	6.38	29.5	6.38	0.0
10	9.0	0	9.0	0	0.0
14	14.9	0	14.9	0	0.0

Table 3: Attack Vector for $\{4, 7, 9, 10, 11, 14\}$

Bus	Pre Attack		Post Attack		$\Delta\delta$ (Deg)
	P_D(MW)	P_G(MW)	P_D(MW)	P_G(MW)	
4	47.8	0	47.8	0	0.0
7	0.0	0	0.0	0	0.0
9	29.5	6.38	29.5	9.50	0.0
10	9.0	0	13.5	0	-0.151
11	3.5	0	2.12	0	0.0
14	14.9	0	14.9	0	0.0

Table 4: Attack Vector for $\{4, 7, 9, 10, 13, 14\}$

Bus	Pre Attack		Post Attack		$\Delta\delta$ (Deg)
	P_D(MW)	P_G(MW)	P_D(MW)	P_G(MW)	
4	47.8	0	47.8	0	0.0
7	0.0	0	0.0	0	0.0
9	29.5	6.38	28.49	9.574	0.0
10	9.0	0	13.5	0	0.0
13	13.5	0	10.24	0	0.0
14	14.9	0	22.35	0	-0.649

Table 5: Attack Vector for N_{10}^{pri}

Bus	Pre Attack		Post Attack		$\Delta\delta$ (Deg)
	P_D(MW)	P_G(MW)	P_D(MW)	P_G(MW)	
9	29.5	0	33.477	0	0.0
10	9.0	6.38	6.463	9.57	0.192
11	3.5	0	5.25	0	0.0

Table 6: Attack Vector for N_{14}^{pri}

Bus	Pre Attack		Post Attack		$\Delta\delta$ (Deg)
	P_D(MW)	P_G(MW)	P_D(MW)	P_G(MW)	
9	29.5	0	34.59	0	0.0
13	13.5	0	17.45	0	0.0
14	14.9	6.38	9.045	9.574	0.788

Table 7: Attack Locations and Ranking for IEEE 14 Bus System

Bus	P_G(MW)	Attacking Region	Rank	
			Gen.(Actual+Spoofed)	Meters
9	9.574	{4,7,9,10,13,14}	1	2
10	9.574	{9,10,11}		1
14	9.574	{9,13,14}		

Table 8: Attack Locations and Ranking for IEEE 30 Bus System

Bus	P_G(MW)	Attacking Region	Rank	
			Gen.(Actual+Spoofed)	Meters
10	13.23	{6,9,10,17,20,21,22,24}	1	6
14	13.23	{12,14,15}		3
15	13.23	{12,14,15,18,23}		5
16	12.77	{12,16,17}	3	1
17	12.99	{10,16,17}	2	
18	12.62	{15,18,19}	4	
19	10.49	{18,19,20}	9	
20	12.12	{10,19,20}	6	
21	12.23	{10,21,22,24}	5	4
22	11.02	{10,21,22,24}	7	4
23	12.62	{15,23,24}	4	1
24	10.24	{12,14,15,18,21,22,23,24,25}	10	7
25	10.57	{24,25,26,27}	8	4
26	8.82	-	-	-
27	11.02	{25,27,28,29,30}	7	5
29	12.23	{27,29,30}	5	2
30	10.02	{27,29,30}	11	