# Feasibility and Mitigation of False Data Injection Attacks in Smart Grid

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

*Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi 110016, India
†Computer Science and Electrical Engineering Department, University of Maryland Baltimore County,
Baltimore MD 21250, USA
Emails: *kushkhanna06@gmail.com,*bkpanigrahi@ee.iitd.ac.in,†joshi@umbc.edu

*Abstract*—**The power grid is evolving rapidly. With the addition of micro-grids and renewable energy resources, and increasing automation in decision-making enabled by sensors, the grid has become very complex. Research in the area of smart grids shows that the grid is vulnerable to cyber-attacks. In particular, recent studies reveals how false data injection could lead to variety of problems in the smart grid operation. A well-crafted attack can pass the bad data detection systems during state estimation and affect the operation and control of the power grid. In this paper, we build on prior efforts in this space to describe how false data injection attacks can be alleviated using conventional techniques by protecting certain critical sensors in the power system. The feasibility of false data injection attacks with incomplete network knowledge is explained in this paper considering IEEE 14 bus test system. The assumptions for defining the attacking region are also validated with the help of different case studies. This paper depicts the importance of securing the power grid against cyber-attacks.**

*Index Terms*—**Cyber security, false data injection, power systems, smart grids, state estimation.**

## I. Introduction

Conventional power grid is evolving into smart grid for increased robustness and reliability with addition of smart meters and two way communication between Remote Terminal Units(RTUs), Intelligent Electronic Devices(IEDs), Phasor Measurement Units(PMUs) and control centres to permit increased automation in decision making. Unfortunately, this increase in automation opens up new avenues of attacks by malicious actors. The communication channel is prone to malicious attacks which can cause mal-operation of various control devices. It can also affect state estimation algorithms in the control centres which gives estimated values of the state variables. The state estimator requires line flows, real and reactive power injection and voltage measurements for estimating the states, and these measurements can be subverted by an attacker as described in recent research in this space.

An attacker can inject false or bad data in any number of meters to launch a successful breach in the smart grid to affect the entire power system. For an $n$ bus system, the total number of states variables need to be estimated is $2n-1$. For estimating 2n-1 state variable at least $2n-1$ measurements are required [1]. Bad data detection is a vital part of state estimator. Measurement may have errors due to accuracy of the meters and communication medium. Bad data is broadly

classified as single bad datum and multiple bad data. The measurements are spread out in entire power system and they do not have any pattern. The error in a measurement can affect the state estimation not only due to the incorrect values but also due to their location [2].

Meters can be classified into (a) Critical meters: If these meters are removed the entire system becomes unobservable, and (b) Redundant meters: These are not so critical but can be used to identify the bad data in the other meters [3]. If an attacker perturb the measurements of sufficient number of meters so that the removal of such meters by bad data detection results in unobservable system, then the attack is said to be perfect. But to launch a perfect attack the attacker must have the knowledge of the entire power system.

Kim et al [4] described a new attack in which attacker can alter the values of a meter and frame the meters which are providing accurate values as the cause of bad data. The authors demonstrated that altering some critical meter measurement can perturb the state estimation. False data injection attacks were discussed by Liu et al [5], who described a new technique to show how an attacker can create attack vectors without being detected by bad data detection techniques given in [6]–[8], can alter the outcomes of state estimation.

Malicious data attacks were further elaborated by Kosut et al [9]. The attacks described were divided into two sub categories, i.e. strong attack regime and weak attack regime. In the strong attack regime the attacker has access to and alters adequate number of meters to cause a perfect attack which is undetectable. Here the adversary has control over the critical meters, therefore the removal of such meters will cause the system to become unobservable. While in weak attack the adversary does not have enough access to enough critical meters to launch an unobservable attack. However, the attack is sufficient to make the state estimation results erroneous.

Weak attack can be detected but due to the existence of the measurement errors the detection is imperfect. Qin et al [10] brought the focus towards unidentifiable attacks. Load redistribution attacks and load increase attacks were introduced. In load redistribution attack, the adversary modifies the load data on the load bus (PQ bus) such that the total demand in the whole system remains unaltered. The operator here can detect bad data in the system but is unable to identify the source of bad data. However, in the load increase attack, the

adversary picks up the load bus randomly and modifies the load data and keeping other bus data unchanged. As such, the attacker confuses the control room operator who is unable to judge whether the load on certain bus has increased or the flow meters are source of bad data. In [11], attack model using full AC power flow equation is presented. It is also observed that unobservable attack using full AC power flow equations can also be launched using limited network knowledge.

Local load redistribution attacks were discussed by Liu et al [12]. They stress on the idea that to launch a unidentifiable attack, requirement of complete network information is no longer a necessary condition. An attack can also be launched with limited network information. The economic impacts of data integrity attacks on market operations were presented in [13]. The detection of these attacks based on AC state estimation and probability distribution of errors is elaborated. The method proposed [14] was based on the fact that when false data is injected, the probability distribution of the measurement errors deviates from the historical data. In [15], mitigating false data injection attacks by protecting a set of sensor measurements is proposed.

In this paper, we build on prior efforts in this space and describe the possibilities of false data injection attacks and preventing such attacks by securing some critical measurements in the power system. The operator can use the network topology information to detect certain false data injection attacks without using separate algorithms for attack detection. It is also shown in this paper that in some cases adversary with incomplete network knowledge can still not launch unobservable attack as mentioned in the earlier research, although in some cases the attack can be unobservable too. These cases are explained in detail is this paper considering IEEE 14 bus test cases.

This paper is divided into five sections. Section I focus on the prior research works in area of smart grid and cyber-attacks. False data injection attacks are explained in section II. Attack model and malicious data detection technique is discussed in section III. Section IV presents various attack scenarios on IEEE 14 bus with simulations and discussion. Conclusions and future scope of this research is given in section V.

## II. FALSE DATA INJECTION ATTACKS

False data injection attacks can be studied by considering two scenarios, (a) where attacker randomly finds the attack vector and injects the malicious measurements to perturb the estimated states and (b) where attacker finds the attack vector and injects malicious data to specific meters to perturb specific state variables with specific errors. In the former scenario there are high chances for attack to be detected by the bad data algorithms. Later scenario on the other hand is far more serious as attacker has enough information about the network topology to cause pre-determined changes on the state variables. Moreover, detection of malicious data attacks is more difficult if attacker has compromised the critical meters.

For monitoring the grid measurements for power injection, voltages and frequency are taken on specified locations. These measurements are available to the independent system operator (ISO) who computes the state variables and carry out power system security analysis. Depending on the type of the meter attacked, the false data injection attacks can be given different names. In load change attacks and load redistribution attacks attacker modifies load meter measurement to launch a cyber-attack on smart grid.

1) Load Change Attack: The attacker modifies the readings of the accessible load meters to get required errors in the estimated state variables. The perturbations in the load meter readings can be both positive and negative depending on the desired amount error attacker wants to inject in state variables. Load change attack may reflect increase or decrease in total connected load on power system, however, the attacker makes sure that the total change is not high enough to get attention of ISO [16].

2) Load Redistribution Attack: In load redistribution attack, attacker redistributes the load on the buses by injecting the malicious data in accessible load meters keeping the total load on the system same. Again the change in the load meter readings is small and it is 10% to 40% of the actual connected load on the bus.

However, it is worth noting that all the load change attacks, if well-crafted and intended to be unobservable by state estimation algorithms are also load redistribution attacks as in order to balance the load and generation, the other loads in the attacking region have to be redistributed.

A 6 bus example is shown in Fig. 1. The attacker has access to meters at bus 2, 3 and 6. To launch a successful false data injection attack, attacker hacks in the accessible meters (shown in red) such that the change in the targeted state variables do not affect the line flows outside the attacking region.



○   **POWER INJECTION MEASUREMENT**
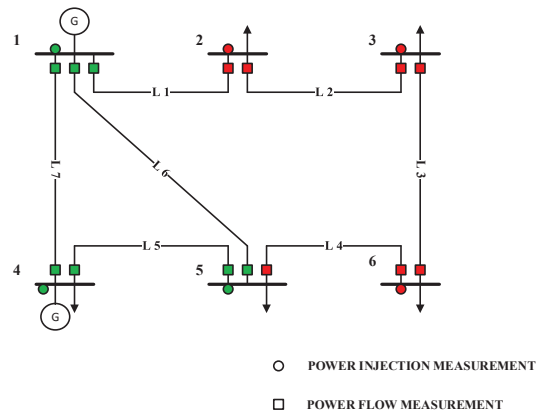
□   **POWER FLOW MEASUREMENT**

Fig. 1. Six bus example

This can be achieved by making sure that the change in the voltages and angles of the boundary buses i.e. bus 2 and 6 in this case, have same incremental change as that of all the buses in non-attacking region. The complete attacking region

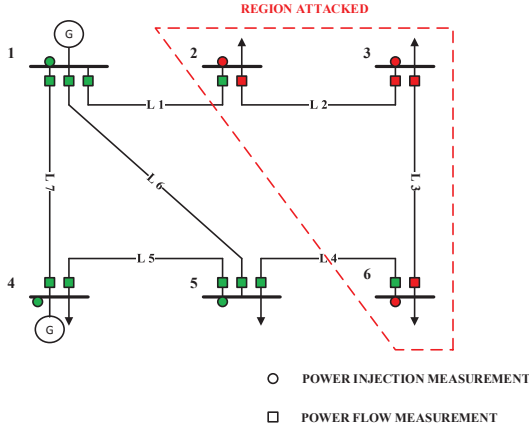with meters compromised (shown in red) is shown in Fig. 2.



Fig. 2. False data injection attack with limited network knowledge

## III. PROPOSED WORK

### A. Observable and Unobservable Attacks

As pointed out earlier by Liu et al.in [5], a false data injection attack in the measurement $z_{attack} = z + a$ will pass the normalized residue test if $a = Hc$, where $a$ is an attack vector $H$ is measurement Jacobian and $c$ is the error in the estimated state variables due to false data injection. The proof of this relation is given in [5]. As mentioned in [11], the adversary can launch a unobservable attack with limited network information if the voltages and angles of the boundary buses and of the buses in the external region are kept at same pre-attack value.

To model a false data injection attack, let us assume that the adversary has knowledge of the attacking region with set of buses $N_A$. Let $N_B$ be the set of the boundary buses in the attacking region. Let the bus admittance matrix for the attacking region $N_A$ without considering tie lines (lines connecting attacking region to the external or unknown region) be $Y_{bus}^A$. In order to make sure that angle and voltage of the boundary buses and external buses remains unchanged, all the external and boundary buses are assumed to be reference buses with voltages and angles specified to pre-attack values [11]. This assumption also ensures that there will be no power exchange between attacking and non-attacking region after the attack.

Newton-Raphson load flow equations are used to model the attack. Depending on the type of the buses in the attacking region, number of the states to be calculated is determined. If the attacking region has $N_G$ generator (PV) buses then the number of states to be calculated are $N_A - N_G - N_B$ for voltages and $N_A - N_B$ for angles. The size of the Jacobian will be $(2N_A - N_G - 2N_B) \times (2N_A - N_G - 2N_B)$. The mismatch vector,

$$\begin{bmatrix} \Delta P \\ \Delta Q \end{bmatrix} = \begin{bmatrix} P^{spec} - P^{cal} \\ Q^{spec} - Q^{cal} \end{bmatrix} \quad (1)$$

$P^{spec}$ and $Q^{spec}$ are the new specified values for real and reactive power injection after the attack.

$$P^{spec} = P_{pre-attack}^{spec} + p$$
$$Q^{spec} = Q_{pre-attack}^{spec} + q \quad (2)$$

Here $p$ and $q$ are the false data injected in load sensor measurements in the attacking region. $P^{cal}$ and $Q^{cal}$ can be calculated from the following equations,

$$P_i^{cal} = Real\{V_i^* \sum_{k=1, k \neq i}^{N_A} V_k Y_{ik}^A\} \quad \forall i \in (N_A - N_B) \quad (3)$$

$$Q_i^{cal} = -Imag\{V_i^* \sum_{k=1, k \neq i}^{N_A} V_k Y_{ik}^A\} \quad \forall i \in (N_A - N_B - N_G) \quad (4)$$

The correction vector can be determined by solving the nonlinear equation (5) iteratively.

$$\begin{bmatrix} \Delta P \\ \Delta Q \end{bmatrix} = \begin{bmatrix} J_1 & J_2 \\ J_3 & J_4 \end{bmatrix} \begin{bmatrix} \Delta \delta \\ \Delta V \end{bmatrix} \quad (5)$$

Here $J_1, J_2, J_3$ and $J_4$ are $[\partial P/\partial \delta]$, $[\partial P/\partial V]$, $[\partial Q/\partial \delta]$ and $[\partial Q/\partial V]$ respectively.

Once the post-attack values of load angles and voltages corresponding to the load change at any PQ bus in the attacking region are calculated, the new flows can be calculated from equations (6-7).

$$P_{mn} = V_{Am}^2(g_{sm} + g_{mn}) - V_m V_n(g_{mn} \cos \theta_{mn} + b_{mn} \sin \theta_{mn}) \quad \forall m, n \in N_A \quad (6)$$

$$Q_{mn} = -V_{Am}^2(b_{sm} + b_{mn}) - V_m V_n(g_{mn} \sin \theta_{mn} - b_{mn} \cos \theta_{mn}) \quad \forall m, n \in N_A \quad (7)$$

If the attack vector is well-crafted this attack cannot be detected by using conventional bad data algorithm. However, in some cases the attack formulated can still be observed if the attacking region has a PV bus or a zero injection bus and this is explained with the help of different cases in the paper.

### B. Power Mismatch based Attack Detection

After estimating the states based on the measurements available (perturbed or secured), real and reactive power injections are calculated at each bus. As it is quite impractical considering that an attacker can get the full network knowledge with current state of the power system and has access to all the sensors in the power system, securing some critical measurement can be of great help in detecting cyber-attacks.

Firstly, changing the sensor measurements corresponding to power generated at the generator bus can be very difficult for the attacker as it can be manually verified by the power plant operator. Secondly, the system operator knows the entire topology of the power system. As the name suggest zero injection bus means net injection at these buses are zero.

Therefore, any false injection at these buses can alarm the system operator about the abnormality in the system.

Hence in order to launch an unobservable false data injection attack, the attacking region must be defined such that,

1) Zero injection bus must not be present in the attacking region (necessary condition).
2) Generator bus should be avoided in the attacking region. If PV bus is present then there must be a load connected on the same bus.

We propose two indices Generator Mismatch Index (GMI) and Zero Injection Mismatch Index (ZIMI) to detect the attack. The calculated power is compared with the measured powers to calculate $GMI$ and $ZIMI$. If GMI and ZIMI are above thresholds $\alpha$ and $\beta$ then alarm is raised to alert the system operator that cyber-attack is detected.

1) Generator Mismatch Index (GMI): It is a ratio of mismatch in power injections to the measured power injections for all the generator buses $N_G$. The mismatch can be both negative and positive depending of the attack vector used to inject errors in the state variables therefore absolute value of ratio is taken as GMI. A threshold $\alpha$ is used to detect the attacks. The value of $\alpha$ is taken equal to the percentage meter error.

$$GMI = abs\left(\frac{S_{cal}^i - S_{inj}^i}{S_{inj}^i}\right) \quad \forall i \in N_G \qquad (8)$$

Here, $S_{cal}^i$ and $S_{inj}^i$ are estimated and measured real power injection at the generator bus $i$.

2) Zero injection bus index (ZIMI): It is a ratio of power mismatch at zero injection bus to the base MVA. Similar to GMI, ZIMI is also an absolute value. A threshold $\beta$ is also equal to percentage meter error. $N_Z$ is the set of zero injection buses.

$$ZIMI = abs\left(\frac{S_{cal}^i - S_{inj}^i}{S_{base}}\right) \quad \forall i \in N_Z \qquad (9)$$

Here, $S_{base}$ is the base MVA of the system.

## IV. SIMULATIONS AND DISCUSSION

The attack is modelled by using equations (1-8) in MATLAB. For estimating the states, real and reactive power flow measurements, real and reactive power injection measurements and voltage measurements are considered. The deviation is considered to be 1% for all the measurements. To estimate the state for each measurement set, meter errors are considered to follow Normalized Gaussian distribution. To get higher accuracy 1000 Monte Carlo runs are conducted to estimate the states.

### A. Case 1

The region attacked is shown in the Fig. 3. $N_A$ is the set of the buses in the region attacked i.e. $\{1, 2, 3, 4, 5, 6, 7, 9\}$ and $N_B$ is the set of the boundary buses i.e. $\{6, 7, 9\}$. The load sensor measurement at the bus 4 are hacked and an error of 20.2 MW is injected in the sensor. The value of GMI and ZIMI indices are given in Table I. The changed estimated states and

TABLE I
GMI AND ZIMI INDICES FOR IEEE 14 BUS SYSTEM

| Bus No. | GMI | | | | | ZIMI |
|---------|------|------|------|------|---|--------|
|  | 1 | 2 | 3 | 6 | 8 | 7 |
| Case 1 | < 1% | < 1% | < 1% | < 1% | - | 0.0952 |
| Case 2 | - | - | - | - | - | 0.0160 |
| Case 3 | - | - | - | - | - | - |

the power injections are shown in Table II. The change in $P_{inj}$ and $Q_{inj}$ for the generator buses 2 and 5 can be incorporated in the load measurement sensor. Buses 6, 7 and 9 being the boundary buses, therefore, there is no change in the voltages and angles of these buses after the attack. GMI for bus 1 is below the threshold $\alpha$ but ZIMI for bus 7 is 0.0952 which is above threshold $\beta$. Hence the attack is detected by the system operator.
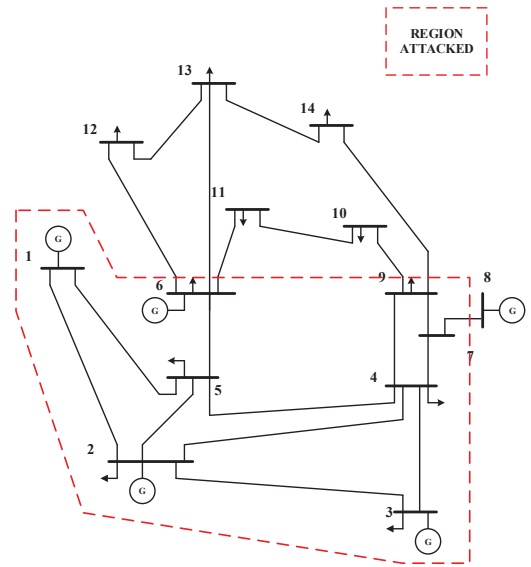


Fig. 3. Case 1

### B. Case 2

For the case shown in Fig. 4, $N_A$ is $\{4, 7, 9, 10, 12, 13, 14\}$ and set of boundary buses $N_B$ is $\{4, 7, 10, 12, 13\}$. Here, error $\Delta P$ and $\Delta Q$ of 6.8 MW and -2.5 MVAr respectively is injected on bus 14. GMI and ZIMI values for this case is given in Table I. The post-attack values of the states and power injections are given in Table II. As the generator bus is not present in the attacking region therefor GMI is not evaluated. ZIMI for bus 7 is 0.016 which is above the threshold $\beta$. Hence, false data injection attack for this case can also be detected using ZIMI index.

### C. Case 3

An attacking region considered is shown in Fig. 5. Here $N_A$ is $\{9, 10, 11, 12, 13, 14\}$. Set of boundary buses $N_B$ is $\{9, 11, 12, 13\}$. Zero injection buses and the generator buses are not present in the region attacked. All the buses in $N_A$

TABLE II
STATES AND POWER INJECTIONS FOR DIFFERENT CASES OF IEEE 14 BUS SYSTEM

| Bus | True Values Base Case | | | | Estimated Values | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Case 1 | | | | Case 2 | | | | Case 3 | | | |
| | V | $\delta$ | $P_{inj}$ | $Q_{inj}$ | V | $\delta$ | $P_{inj}$ | $Q_{inj}$ | V | $\delta$ | $P_{inj}$ | $Q_{inj}$ | V | $\delta$ | $P_{inj}$ | $Q_{inj}$ |
| 1 | 1.060 | 0 | 2.324 | -0.169 | **1.060** | **-0.0164** | **2.324** | **-0.174** | 1.060 | 0.0000 | 2.324 | -0.169 | 1.060 | 0.0000 | 2.324 | -0.169 |
| 2 | 1.045 | -0.0869 | 0.183 | 0.297 | **1.045** | **-0.1035** | **0.183** | **0.290** | 1.045 | -0.0869 | 0.183 | 0.297 | 1.045 | -0.0869 | 0.183 | 0.297 |
| 3 | 1.010 | -0.2220 | -0.942 | 0.044 | **1.010** | **-0.2392** | **-0.942** | **0.041** | 1.010 | -0.2220 | -0.942 | 0.044 | 1.010 | -0.2220 | -0.942 | 0.044 |
| 4 | 1.019 | -0.1802 | -0.478 | 0.039 | **1.019** | **-0.1983** | **-0.680** | **0.052** | 1.019 | -0.1802 | -0.475 | 0.039 | 1.019 | -0.1802 | -0.478 | 0.039 |
| 5 | 1.020 | -0.1533 | -0.076 | -0.016 | **1.021** | **-0.1689** | **-0.076** | **-0.016** | 1.020 | -0.1533 | -0.076 | -0.016 | 1.020 | -0.1533 | -0.076 | -0.016 |
| 6 | 1.070 | -0.2482 | -0.112 | 0.047 | **1.070** | **-0.2482** | **-0.040** | **0.037** | 1.070 | -0.2482 | -0.112 | 0.047 | 1.070 | -0.2482 | -0.112 | 0.047 |
| 7 | 1.062 | -0.2333 | 0.000 | 0.000 | **1.062** | **-0.2333** | **0.095** | **-0.006** | 1.062 | -0.2333 | 0.016 | -0.001 | 1.062 | -0.2333 | 0.000 | 0.000 |
| 8 | 1.090 | -0.2333 | 0.000 | 0.174 | 1.090 | -0.2333 | 0.000 | 0.174 | 1.090 | -0.2333 | 0.000 | 0.174 | 1.090 | -0.2333 | 0.000 | 0.174 |
| 9 | 1.056 | -0.2609 | -0.295 | -0.166 | **1.056** | **-0.2609** | **-0.259** | **-0.169** | 1.056 | -0.2625 | -0.295 | -0.166 | 1.056 | -0.2609 | -0.255 | -0.178 |
| 10 | 1.051 | -0.2636 | -0.090 | -0.058 | 1.051 | -0.2636 | -0.090 | -0.058 | **1.051** | **-0.2636** | **-0.072** | **-0.066** | 1.051 | -0.2636 | -0.090 | -0.058 |
| 11 | 1.057 | -0.2582 | -0.035 | -0.018 | 1.057 | -0.2582 | -0.035 | -0.018 | 1.057 | -0.2582 | -0.035 | -0.018 | 1.057 | -0.2582 | -0.035 | -0.018 |
| 12 | 1.055 | -0.2632 | -0.061 | -0.016 | 1.055 | -0.2632 | -0.061 | -0.016 | **1.055** | **-0.2632** | **-0.061** | **-0.016** | 1.055 | -0.2632 | -0.061 | -0.016 |
| 13 | 1.050 | -0.2646 | -0.135 | -0.058 | 1.050 | -0.2646 | -0.135 | -0.058 | **1.050** | **-0.2646** | **-0.103** | **-0.069** | 1.050 | -0.2646 | -0.105 | -0.068 |
| 14 | 1.036 | -0.2799 | -0.149 | -0.050 | 1.036 | -0.2799 | -0.149 | -0.050 | **1.034** | **-0.2920** | **-0.217** | **-0.025** | 1.034 | -0.2911 | -0.217 | -0.025 |

are load buses and hence load meters at all the buses can be attacked. The malicious attack vector added to the load measurement sensor of bus 14 with $\Delta P$ and $\Delta Q$ equals to 6.8 MW and -2.5 MVAr respectively. As the zero injection buses and the generator buses are not present the attack is perfectly unobservable to the system operator.
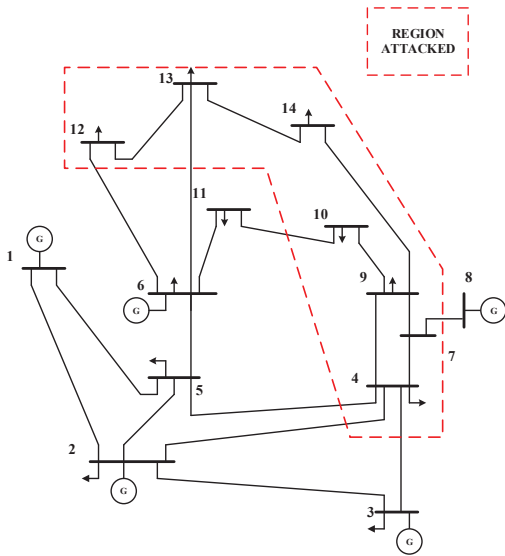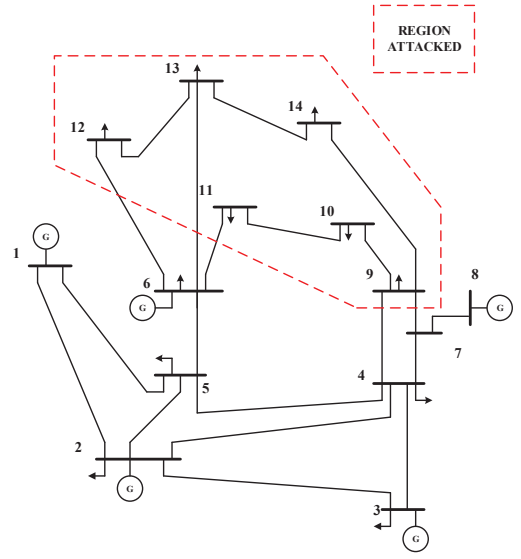


Fig. 4. Case 2



Fig. 5. Case 3

Newton-Raphson load flow equation considering limited network information can still be observable if the attacking region contains a generator bus without a load or a zero injection bus, therefore to launch a stealthy false data injection attack, the attacking region must contain only load buses. This work can be extended to identify the hacked meters to eliminate all possible threats to the power system.

## V. CONCLUSION AND FUTURE SCOPE

Automation of power systems resulted in better operation and control of electrical power system. Added communication capabilities to RTUs and IEDs makes power grid more robust. However, increased complexity and remote access has made smart grid liable to cyber-attacks. This paper presents impacts of cyber-attacks on power system. From small change in estimated states to line tripping, this work reveals the vulnerability of smart grid to cyber-attacks. This work also reveals that a false data injection attack modelled using full

## REFERENCES

[1] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation.* CRC Press, 2004.
[2] F. C. Schweppe, "Power system static-state estimation, part i,ii,iii," *Power Apparatus and Systems, IEEE Transactions on*, no. 1, pp. 120–135, 1970.
[3] A. Gomez-Exposito and A. Abur, "Generalized observability analysis and measurement classification," *Power Systems, IEEE Transactions on*, vol. 13, no. 3, pp. 1090–1095, Aug 1998.
[4] J. Kim, L. Tong, and R. J. Thomas, "Data framing attack on state estimation," *Selected Areas in Communications, IEEE Journal on*, vol. 32, no. 7, pp. 1460–1470, 2014.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[6] T. Van Cutsem and M. Ribbens-Pavella, "Bad data identification methods in power system state estimation-acomparative study," *IEEE Transactions on PowerApparatus and Systems*, vol. 104, no. 11, 1985.

[7] A. S. Costa, T. Pizza, and A. Mandel, "Qualitative methods to solve qualitative problems in power system state estimation," *IEEE Transactions on Power Systems*, vol. 5, no. 3, 1990.

[8] F. F. Wu and W.-H. E. Liu, "Detection of topology errors by state estimation," *Power Systems, IEEE Transactions on*, vol. 4, no. 1, pp. 176–183, 1989.

[9] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 645–658, 2011.

[10] Z. Qin, Q. Li, and M.-C. Chuah, "Unidentifiable attacks in electric power systems," in *Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems*. IEEE Computer Society, 2012, pp. 193–202.

[11] K. Davis, K. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, Nov 2012, pp. 342–347.

[12] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *Smart Grid, IEEE Transactions on*, vol. 5, no. 4, pp. 1665–1676, 2014.

[13] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 659–666, 2011.

[14] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *Smart Grid, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[15] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, vol. 2010, 2010.

[16] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *Smart Grid, IEEE Transactions on*, vol. 2, no. 2, pp. 382–390, 2011.