RESEARCH ARTICLE OPEN ACCESS

Simulation Of Smart Grid Security And Vulnerability Analysis Using Pmu State Estimation

[1]Mr.Mihir K Patel, [2]Ms. Palak Patel,
[1]IEEE Member, Ph.D. Scholar, Electrical Department University of Technology Jaipur, Rajasthan, India
[2]PG Scholar, M.Eng. Engineering Systems & Computing, School of Engineering, University of Guelph, Ontario, Canada

ABSTRACT
The electricity demands are increased rapidly with low power losses and low energy costs. To minimize the power loss and achieve load demand with that developing new energy sources based on Renewable energy sources are necessary to think. The controlling and achievement of about goals is difficult in the normal power grid, so smart grid development is increased in the recent few years. While the biggest issues related to SG is security. The vulnerability of SG against cyber-attacks is discussed in this paper. The Bad data injection, False Data injection, and cyber-attacks are the most focusing challenges reviewed in this paper. The PMU state estimation is one promising solution for SG security. So we have shown the SG security analysis for the IEEE 14-bus system using Matlab-Simulink. The simulation results show that PMU provides protection against cyber-physical attacks as well as reliable and secure operation of S.G.

Keywords: SG, PMU, BDD, State Estimation (SE), FDI,etc.

Date of Submission: 11-04-2020 Date of Acceptance: 27-04-2020

I. INTRODUCTION

In electrical grid network the only key objective is to maintain the balance between load demand and power generation. Smart grid provides two way communication between power supplier and consumer through digital control. SG infrastructures includes Information communication control, Automation, Computers and information control. The smart grid provides control over power supply as per the demand variation quickly through new technology and digital control. The smart grid concept provides new technology development, dependability, availableness, and new opportunities for electricity market. The key benefits of development of SG over power grid are explained below.

The advantages related to the Smart Grid include:-

- Reliable and low cost power transmission
- Fast response and quick restoration during abnormal conditions
- New technology development helps in reduction of operation and management costing
- The peak demand of electricity is also reduced which helps for low electricity rates to consumer
- Power demand achieved using integration of renewable energy sources
- Data security and management is done easily
- Load balance achieved between demand and generation

The outline of the paper is as follows. Section II discuss the literature review for the problem identification and our motivations on developing the methods for SG security. The challenges and key research objectives are also explained in this section. In Section III, the analytic vulnerability assessment with different control methods are discussed. The benefits and drawbacks of different control methods are explained w.r.t to Phasor Measurement Unit (PMU) state estimation. The co-simulation platform for SG security is explained in Section IV, including how the power system and communication network are modeled. Section V shows the Matlab simulation and results for IEEE 14-bus system SG security with the help of PMU state estimation. We also provide a discussion on simulation results. The conclusion remarks are in Section VI.

II. CHALLENGES AND RESEARCH OBJECTIVES FOR S.G SECURITY

Literature Review:-

Anurag Srivastava, Thomas Morris,Timothy Ernster, , Ceeman Vellaithurai, , Shengyi Pan, and Uttam Adhikari [1] shows the cyber-attacks modelling using Vulnerability analysis of Data and information control in grid network. The proposed Vulnerability analysis of electric grid has been analyzed with graph theory based approach. In this control topology the gird network utilizing the different concepts like feasibility, communication control, detection of threat which is implemented and verified for IEEE 14 bus system by the authors in this paper [1].

James Ranjith Kumar R. and Biplab Sikdar [2] presents simplified non calculative false/bad data detection using AC State Estimation technique. The proposed AC State estimation system calculates the data of Voltage magnitudes and Node power injection through SCADA. In this paper the authors tested proposed control methods for IEEE 118 bus system in which FDI injected around 1% to 10 % magnitude variation. The controlling of Power flow and voltage magnitude is done in proposed system [2].

Kaikai Pan, Andr´e Teixeira, Claudio David L´opez and Peter Palensky [3] Provides implementation of PMU State estimation technique with optimal power flow control for optimization point of view. The Grid Network parameters are measured and compared with the Data measured during the Bad data injection and PMU SE gives the variation and error signal from iteration calculation proposed in this paper [3].

Jingyao Fan, Youssef Khazbak, Jue Tiany, Ting Liu and Guohong Cao [4] shows that in today's grid network the data measurement and control is done through SCADA network. In S.G network when attacker do FDI on smart meters which creates problems on meters technology. The existing technology will meet consider the costing of smart metering in S.G. The main objective of the authors in this paper is how to done the selection of most critical meters to protect them against cyber-attack. The algorithm developed by the authors is based on heuristic based solutions. In the proposed controlling in this paper will provides two main concepts:-

1. Identification of the meter which will be targeted by the attacker in FDI as cyber-attacks.

2. Identify the damage which will be caused by the attack on the meter.

HADIS KARIMIPOUR, AND VENKATA DINAVAHI [5] this paper represents the overview of smart meter security against cyber-attacks and FDI. The vulnerability analysis will plays an important role for smart grid. In this paper the authors shows that the solution for FDI and cyber-attack threat is state estimation. The authors represents the markov chain theory and Euclidean distance metric for state estimation controlling.

In this paper the proposed robust state estimation used trusted historical data of bus network and calculate the bad data as FDI attack values in S.G. The proposed robust state estimation algorithm is built with the help of fine gained parallel programming technique.

Challenges:-

Smart grid infrastructure is facing number of threats for security concern including cyber-attacks, FDI, terrorism, natural disasters, etc. The failure of SG due to any of above threats creates multiple issues in power grid like failure of equipment, power cut-off, blackout, information network disturbance or failures, cascaded tripping etc. Different Security threats and challenges of smart grid have been presented in Pan, and Uttam Adhikari [1], James Ranjith Kumar R. and Biplab Sikdar [2], Abdulrahaman Okino Otuoze, Mohd Wazir Mustafaa, Raja Masood Larik [5]. These threats and challenges have focused researcher towards study and research about privacy and security of smart grid by different techniques.

SG security challenges considered in terms of authentication, authorization, and privacy of technologies depending on security levels of SG. From the technical point of view, threat of security is concerned with fault or breakdown of generation, transmission, distribution, and substation; due to natural of non-natural cause such as failure of equipment, commanding operation due to false data injection. Now a days time has come where people are very much concern with the security concept of grid network because in recent scenario and in nearby future development of smart grid is increased. Normal and healthy operation of smart grid is much concern topic against uncertain problems and cyber-attack on grid network. For security concern there is a need of approach in which we can identify the cyber-attacks that is seeking to damage grid network and provide controlling to prevent collapse & problems occurs due to cyber-attacks [4].

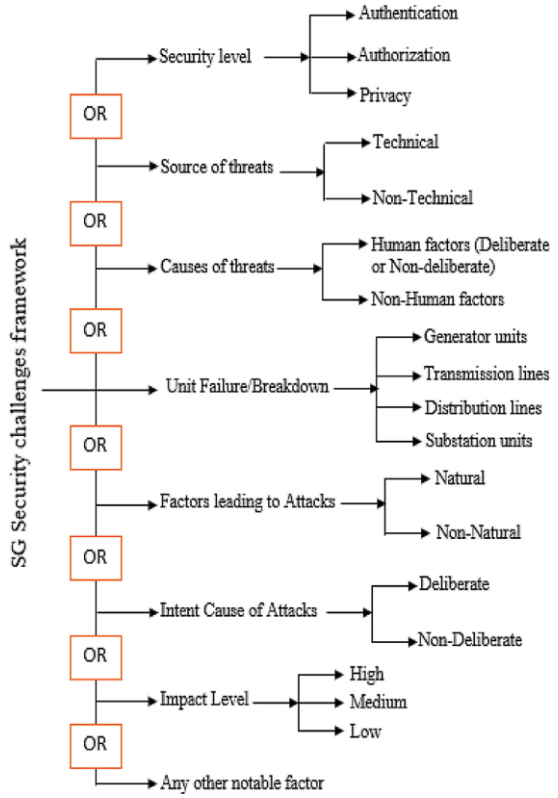

Fig. 1. Framework for identifying smart grid security threats and challenges [5]

Research Objectives: -

As discussed earlier, reliable and efficient electricity supply to consumer depends on interconnectivity and interdependency of the SG infrastructures with data control through SCADA. Therefore, well-articulated security objectives are mainly considered for ensuring an efficient and reliable operation of smart grid. These objectives include all possible expansion & improvement plans for future grids development. Here in this paper main objectives are: -

- Detection of False Data Injection (FDI) in SG infrastructures and provides security through PMU State Estimation.
- Integration of renewable energy unit for electricity supply as DG unit in SG as DG unit is also of utmost priority since it can be used for increasing the security requirements between electricity generation and demands.

Implementing the Security for smart grid against FDI provides efficient and reliable operation of smart grid. The data security and authentication objective is achieved using Security of SG.

Smart grid Architecture: -

The SG has been the best solution in replacement of conventional electrical grid network to minimize the power loss and improve system parameters like effectiveness, security, privacy, reliability, stability, efficiency and to achieve the balancing for increasing load demand [7]. The main features of SG include safe and secure operation, self-healing capability, improved power quality, fast response, energy management, Distributed Generation (D.G) unit integration, etc. The fig.2 shown below shows the architecture of smart grid with power flow management including different types of networks WAN (Wide Area Network), HAN (Home Area Network) and NAN (Neighborhood Area Network). Firstly the HAN type network manages the consumer power demands and smart devices (including smart meters, smart sensors, etc.) operations [7]. HAN is first layer network while NAN which is known as Filed Area Network (FAN) is considered as the second layer SG and SMI belongs to multiple HAN networks. NAN network helps for two way communication between the distribution system and field electrical components like meters, sensors and measurement devices. In that system, the data from multiple HAN networks are combined for service and metering information and it will transmit to the data collector with NAN to WAN network configuration. The third and last layer is WAN which serves as a backbone of communication for the network to gateways [7].

Fig.2 Architecture of Smart grid (SG) with power flow indication [7]

III. METHODOLOGY OF S.G SECURITY

In this paper we will develop IEEE-14 bus system network using MATLAB-Simulink and measure load flow analysis including load demand, line data, generation data, line outage factors, etc. After Cyber-attack, the line data becomes unbalanced and line outage problem occurred. To mitigate this, we will implement the PMU state estimation that provides an estimate of Smart grid Network in Data Attack Condition. The proposed State Estimation uses measurements collected by the Remote Terminals of Substations in Grid and provides data to SCADA base DCS Control system. The estimated state information will be processed by optimal power flow and Contingency analysis to calculate the necessary steps for safety and reliability of system. If the fault condition is not removed or it affects other bus system than proposed approach will remove that faulty part using C.B operations in the Smart grid and provides balancing and security in the system.

Fig.3- Closed Loop control system for Smart grid Security [3]

The proposed controlling of PMU State Estimation as shown in Fig.1 the data attackers can attack from various points like A1- Remote terminal unit, A2- Communication Network, A3- SCADA master. The Data measurements under suck type of attacks are presented as following steps:-

1. Bad Data Injection: - In this type the attacker tries to inject false or bad data in the grid network, state estimation provides data changes from K to K+a, where K is Bad data Attack vector.
2. Vulnerability Analysis:- The Vulnerability Analysis calculate how many measurements need to be manipulated by the attacker to keep Stealth against Bad Data Detection (BDD).
3. PMU State Estimation: - In the PMU State Estimation Method the Node power injections and Line power flows are calculated from DCS system and Voltage Magnitudes and Angles from Phasor measurement Unit (PMU) for detection of bad data attacks.
4. Iteration Calculation of SE: - In Calculation of SE the iteration steps are repeated until the values of State Variables converge to specified tolerance limits. In this grid network by assuming voltage magnitudes are near to specified limits and difference of voltage angles in line are very small then the equation may be linear and can be solved with better accuracy. If that condition is not satisfied then it indicates that bad data is present in the system [3].

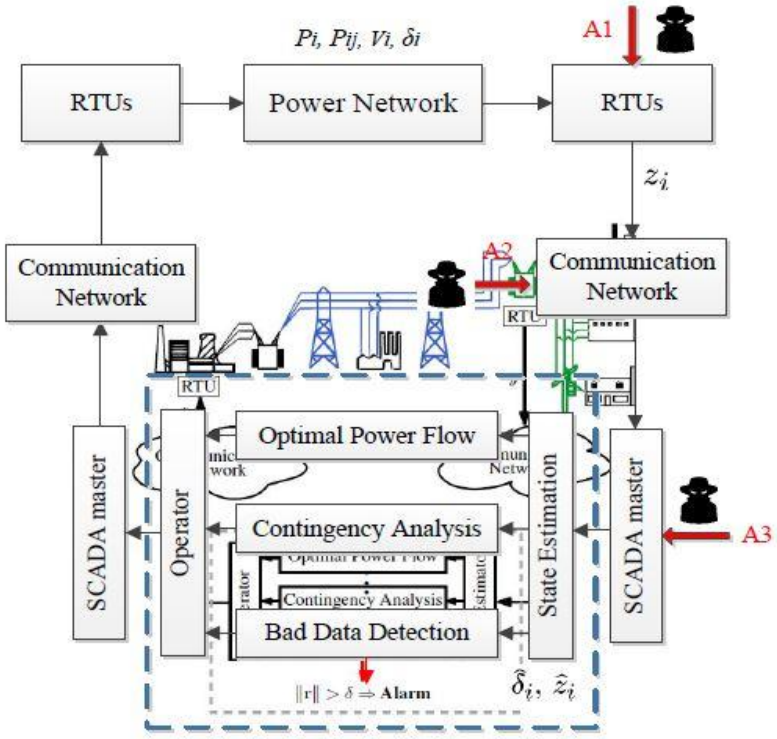

Fig.3- Energy Management System [1]

Classification of Cyber-attacks:-

1. Component Wise: - Field Components like RTU are attacked through remote access.

2. Protocol Wise: - Using the communication protocols available in the public domain, an intruder can reverse engineer data acquisition protocols and exploit them.

3. Topology Wise: - Network Topology Vulnerability is exploited. Example: - Attacks on SG Portion/Parts.

State Estimation and Bad Data Detection: -

As shown in fig.2 the Remote Terminal Units (RTU) transmit the data of node power injections, line power flows, bus and line voltage magnitudes to Supervisory Control and Data Acquisition (SCADA) controlled Digital Control System (DCS) centre for Energy Management System (EMS). The different type of network topologies are used for this. In power grid PMU will measured the voltage and current phase angles for state estimation calculations. The measured signal from PMU transmitted through filter and amplifier for amplification of signal. The measured quantities are used for EMS system to identify in which state power system is operated. The use of power balance equation is not suitable because of its nonlinearity in nature, which focus for the use of Gauss-Newton method for state estimation which is known as A.C state estimation.

For example we consider z to be the m dimensional vector for all the calculations in SE and function f(x) to be considered as nonlinear function used for variable x measurement in PMU during state estimating. This x will representing the voltage magnitudes and angles of node, which dimensional size n is assumed to be less than the m measurements in SE. From this we can say that making system an over determined the necessary condition is n<m.

The measured quantities have noise signal in the measurements we used following equation for state variables calculation:-

$$z = f(x) + e \qquad (1)$$

Where,
e= noise signal present in measured quantity
This calculations and measurements is nothing but the set of power balance equations which is nonlinear in nature. Due to which the state estimation calculations steps are usually iterative. For example at the i^{th} iteration, the state correction vector is written as below

$$\Delta x^i = \left(H^T(x^i)R^{-1}H(x^i)\right) \backslash H^T(x^i)R^{-1}\left(z - f(x^i)\right) \qquad (2)$$

Where,

H (X^i) = Jacobian matrix for the function f(X^i) and R=measurement covariance matrix.

Using the state correction vector, the values of the state variables for the next iteration can be updated as

$$X^{i+1} = X^i + \Delta X^i \quad (3)$$

This calculation method of iteration will be repeated up to the state variables values converge to the reasonable tolerance limit. For linearization in the power model calculations we are assumed that the measured voltage magnitudes are closer to the rated values and difference of voltage angles in a line are extremely small. This technique is simple for iterative solution and it is known as DC state estimation.

S.G Security Concern:-

For SG, a big challenge is to provide enhancements and improved capabilities compared to the normal power grid. These vulnerabilities will allow the network access and it will loss the data security and integrity of transmitted data to the service provider. The following vulnerabilities are the most serious in SG:

1) Customer security: *Smart meters collect information and data of usage, and transfer it to the consumer, utility companies and service provider.* This data includes consumers' personal information and consumers' activities such as devices being used when the home is vacant.

2) Greater number of intelligent devices: The SG has several intelligent devices that are used to manage load demand and generation. These intelligent devices may act as attack entry points into the network. Moreover, the massiveness of the SG network makes network monitoring and management extremely difficult.

3) Physical security: Unlike the traditional power system, SG network includes many components and most of them are out of the utility's premises. This fact increases the number of insecure physical locations and makes them vulnerable to physical access.

4) The lifetime of power systems: Since power systems coexist with the relatively short-lived IT Systems, it is inevitable that outdated Equipments are still in service. This equipment might act as weak security points and might be incompatible with the current power system devices.

5) Implicit trust between traditional power devices: Device-to-device communication in control systems is vulnerable to data spoofing where the state of one device affects the actions of others. For instance, a device sending a false state makes other devices behave in an unwanted way.

6) Different Team's backgrounds: Inefficient and unorganized communication between teams might Cause a lot of bad decisions leading to much vulnerability.

7) Using Internet Protocol (IP) and commercial off the- shelf hardware and software: Using IP standards, SG offers a big advantage as it provides compatibility between the various components. However, devices using IP are inherently vulnerable to many IP-based network attacks such as IP spoofing, Tear Drop, Denial of Service, and others.

8) More stakeholders: Having many stakeholders might give rise to a very dangerous kind of attack: insider attacks.

IV. SG SECURITY SIMULATION PLATFORM

Co-Simulation Task

The co-simulation task includes combination of Dig SILENT Power Factory, communication network using OMNeT++ and Matlab. The co-simulation helps for real-time analysis of cyber-attacks. Dig SILENT Power Factory provides power system operation, OMNeT++ used for the communication network and Matlab used for EMS algorithm and control methods. All that three things are used in combination for power grid operations as shown in fig. 4 below.

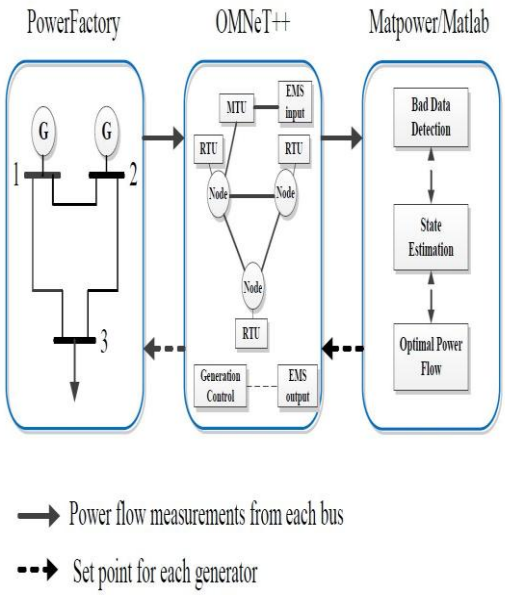

Figure 4: Co-simulation diagram [1]

DIgSILENT Power Factory: - It is used for power system operation and analysis. Load flow analysis and IEEE bus network can easily design in DIgSILENT Power Factory. There are multiple

number of power system operation control tools are available in it. Communication with Matlab of Power factor is done through OMNeT++.

OMNeT++:- it is used for communication network or platform for power factor and Matlab simulator. The script and data exchange is enabled with Power Factory and Matlab over TCP/IP sockets and run the OMNeT in real-time. The communication between RTU and EMS is done through LAN (Local Area Network) in OMNeT++.

Matlab Simulator: - The Matpower simulator is used for EMS algorithm design and simulation in Matlab. It will provides state estimation and Bad data detection. The State Estimation module uses the latest measurements from data pool to create a snapshot of estimated power flow.

V. SIMULATION AND RESULT DISCUSSION

We have consider IEEE 14-bus system as shown in fig.5 below. In which we are define the cyber physical attack effect on router-4 and router-1. The cyber-attack effects creates measurement variation in Bus-1 and Bus-2 active power flows. The changes in active power flow variation and generation are shown in fig.6 and 7. The Router-1 and Router-4 related with both generators are considered for cyber-attack analysis.

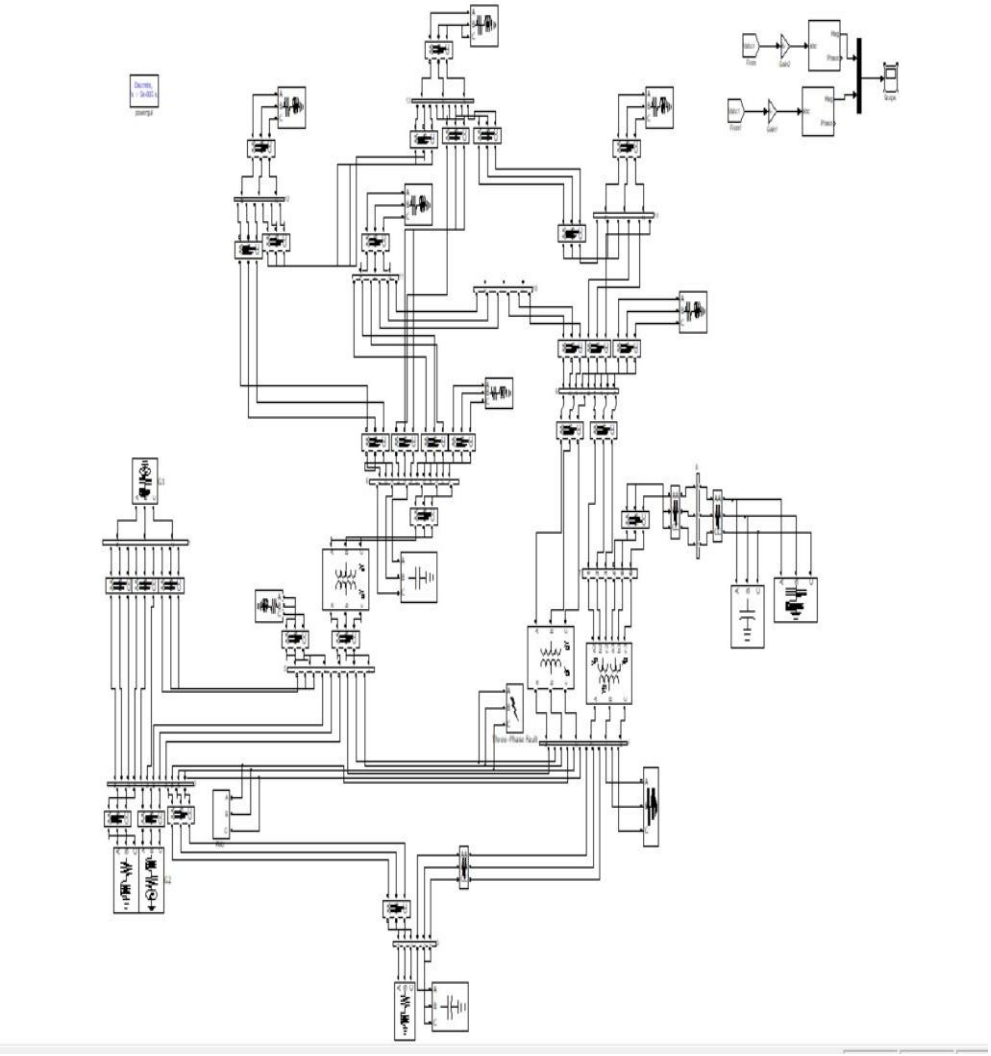

Figure 5: IEEE 14-bus system

(Here there are two generators in this system. Bus-1 with generator-1 which is considered as slack bus, while bus-2 is connected with generator-2)

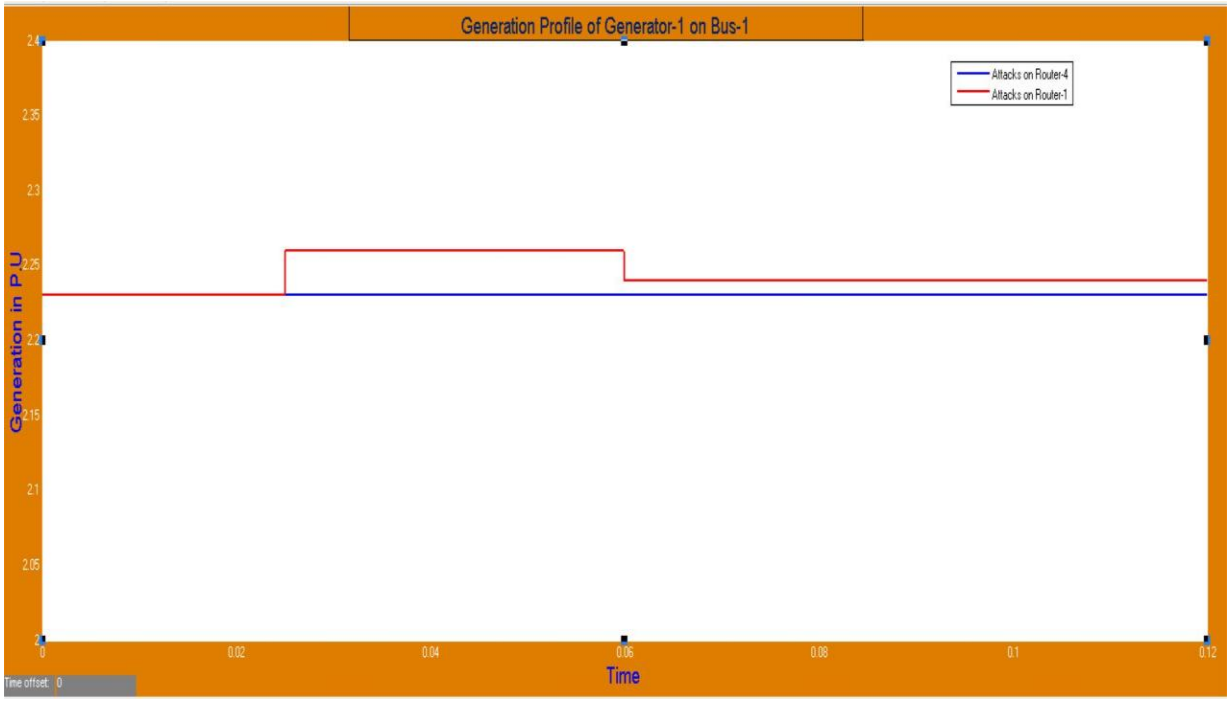

Figure 6: Generation profile variation on both the buses connected with both generator during attack on router-1 and router-4

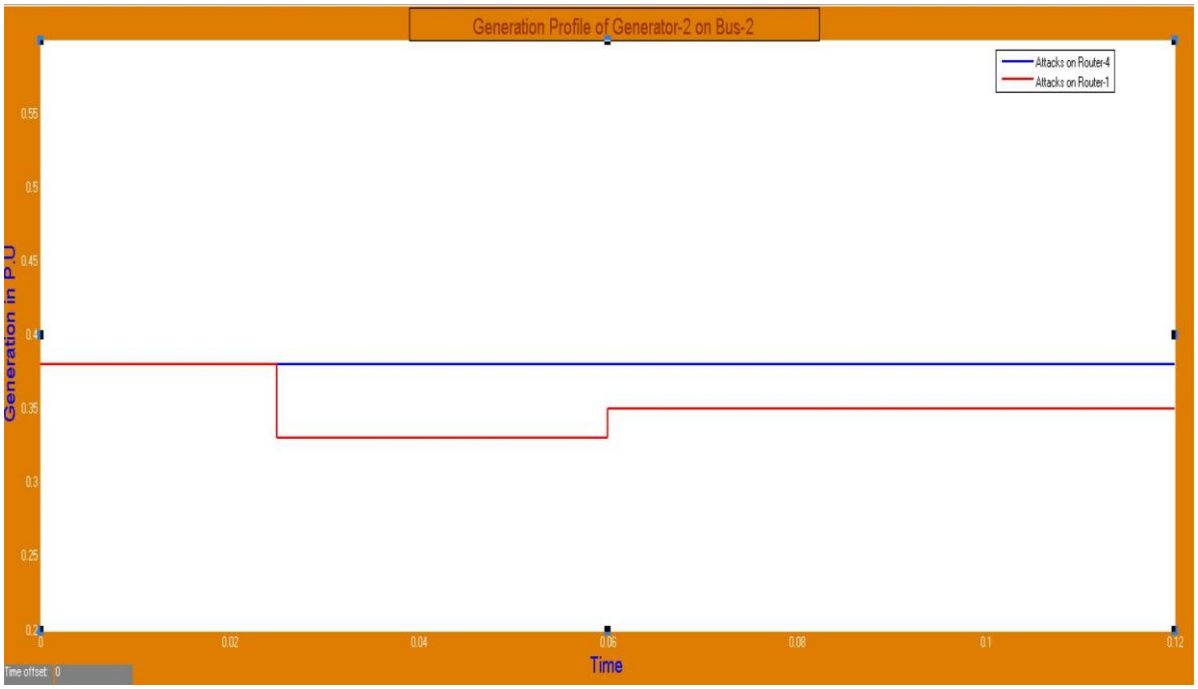

Figure 7: Attack impact on Generation profile of generator-1 and 2. Before the attack occurrence, the system is operating under the optimal power flow status giving the loads. In these two cases, the same number of measurements are corrupted.

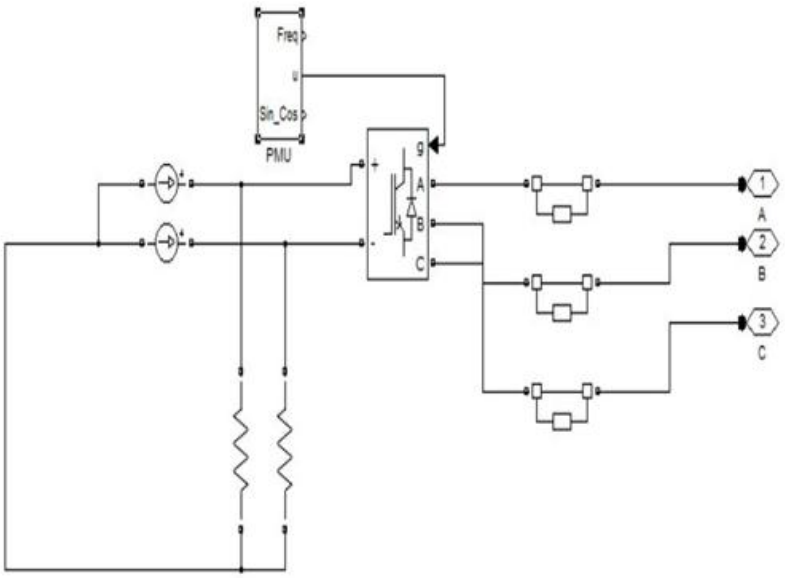

Figure-8 Controlling subsystem for SG system against attack

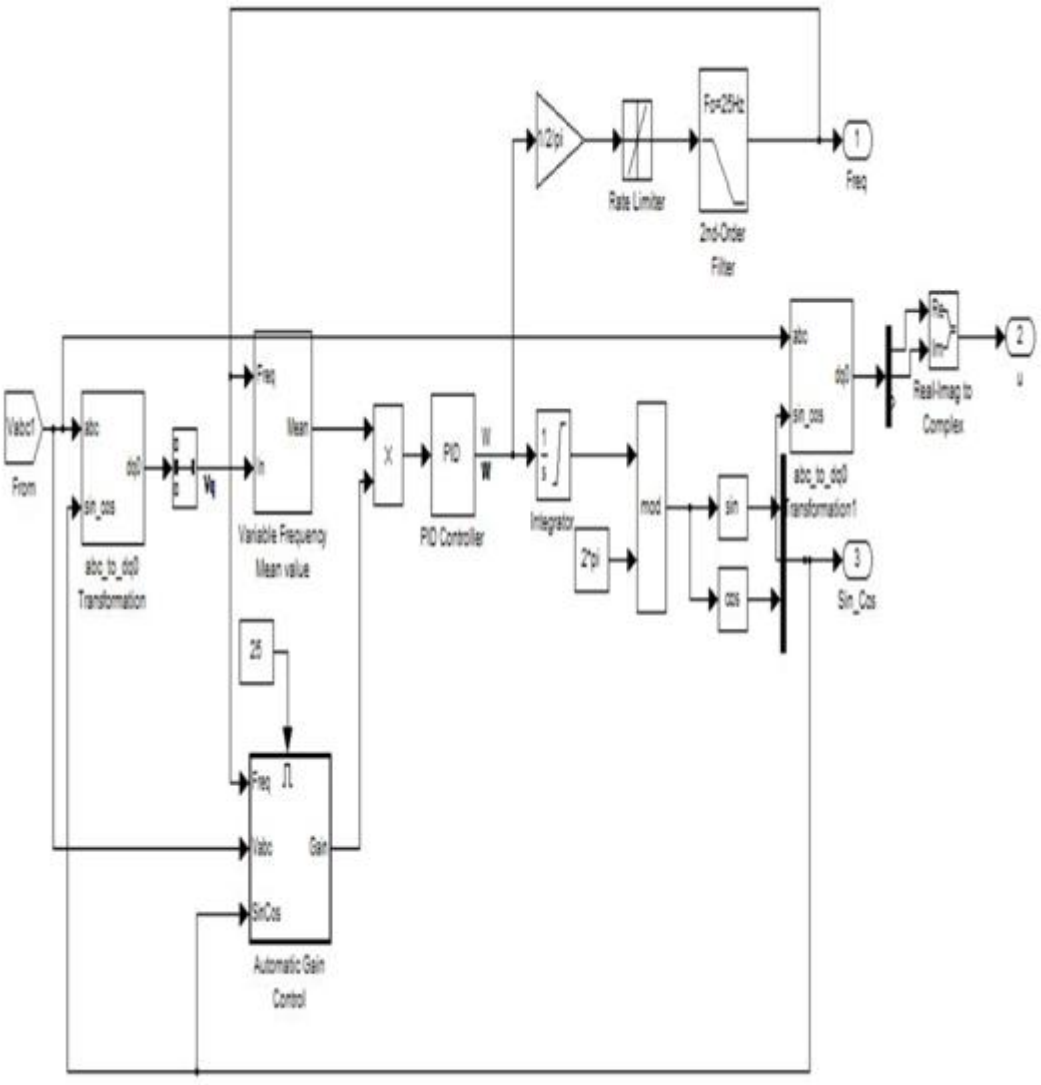

Figure-9 PMU state estimation subsystem

As shown in fig.6 above we can say that when the router-1 is attacked, the generation profile of generator-1 and generator-2 will change from its set point as shown in fig.6. In the proposed system during attack the generation of generator-2 red line has decreased which is try to compensate by the generation of generator-1. During the generation profile change the signal for EMS is sends for every 30 seconds. From the simulation results we can say that the impact of attack will remain almost same during initial time duration due to magnitude variation and corrupted measurements. Later on when router-4 is attacked, there is no attack impact on generation profile as shown in fig.6 blue line. The attacker can change the magnitudes of line flow and power flow measurements related to router-1 on bus 2, 3 and 4, which has the major impact on the generation profiles of these two generators. While the travelling packets in router- and it is backbone router there is no difference in measurements. For the case that Router 1 is attacked, the active power flows on the lines close to the generators are shown in Figure 7. The power flows get changed after re-dispatch according to the corrupted set points. Such physical impact can be utilized by the attacker to cause line overflows.

The PMU state estimation controlling is implemented in the proposed IEEE 14- bus system as shown in fig.8. The voltage magnitude measured from bus-1 and bus-2 affected due to attack is given as a feedback in PMU calculation. The phasor calculation of voltage and current magnitude has been calculated for PI controller tuning to reduce the deviation level. The park transformation and vector calculations system are shown in fig.9. The control vector is given as triggering pulses for IGBT switching operation. Which control the three phase C.B operation for protection against cyber-attack in smart grid. After the successful implementation of PMU state estimation the improvement is active power flow changes in bus-1 and bus-2 is shown in fig.10 below. We can done this analysis at different bus and node power injection points analysis in future work.

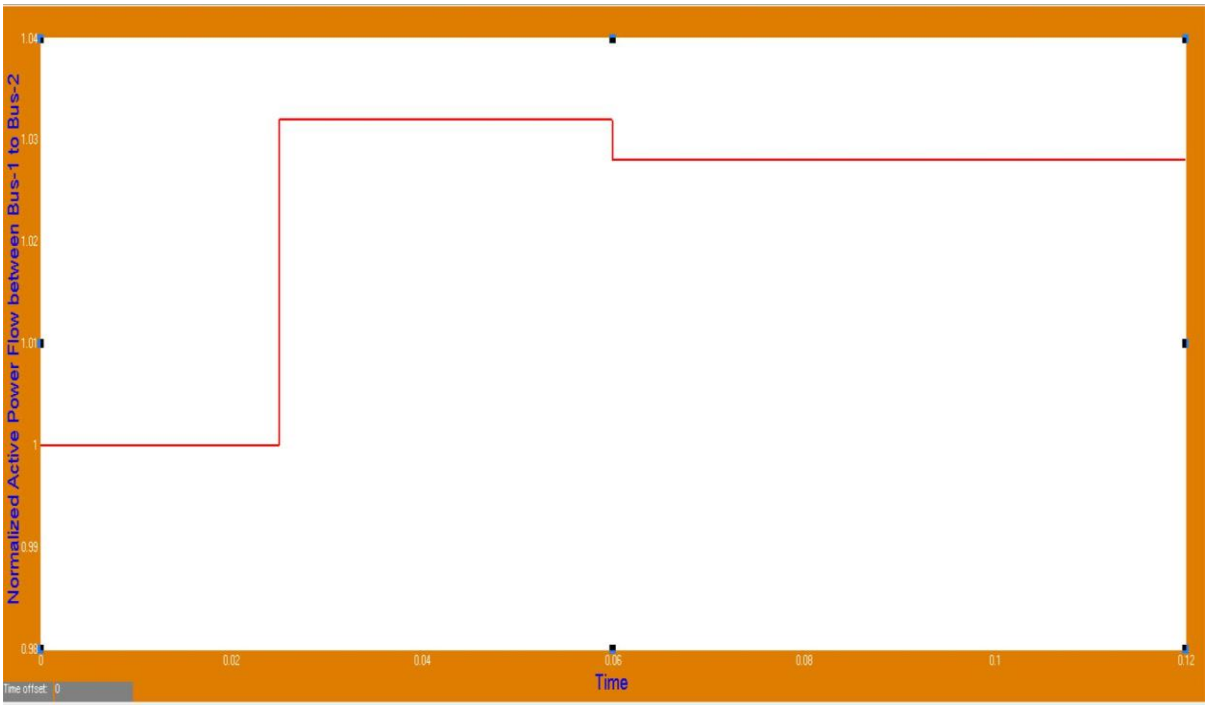

Figure-10 Normalized active power flow at bus-1 and bus-2 after PMU state estimation used

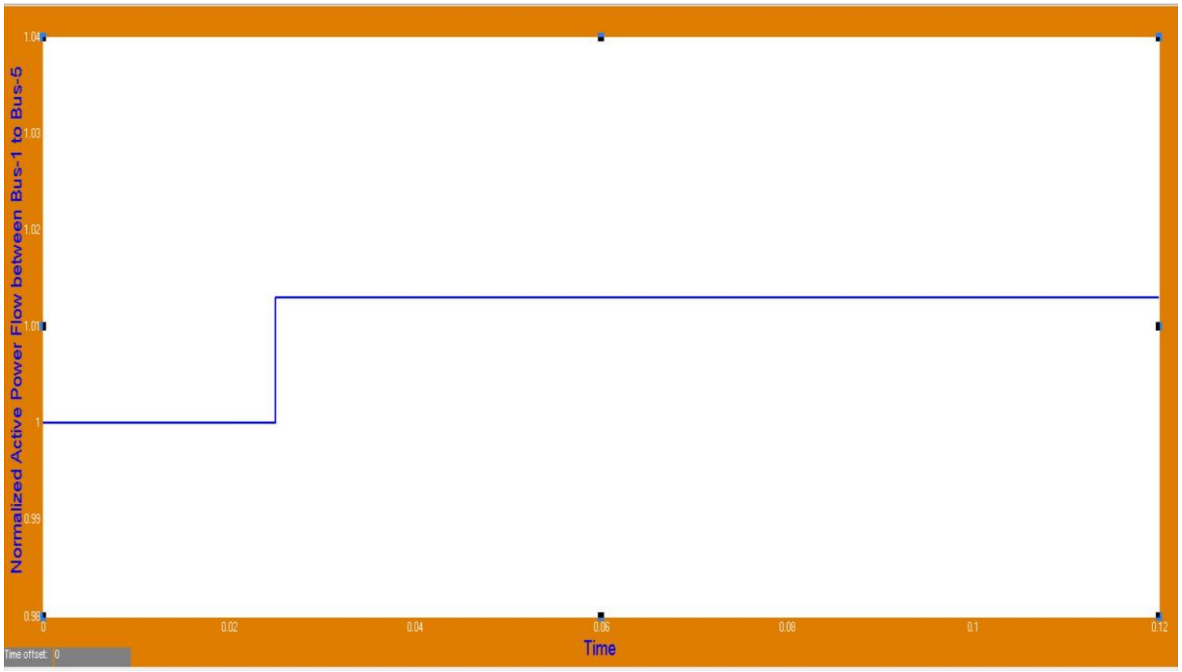

Figure-11 Attack impact of attacks on active power flows in the lines of bus 1 to 5

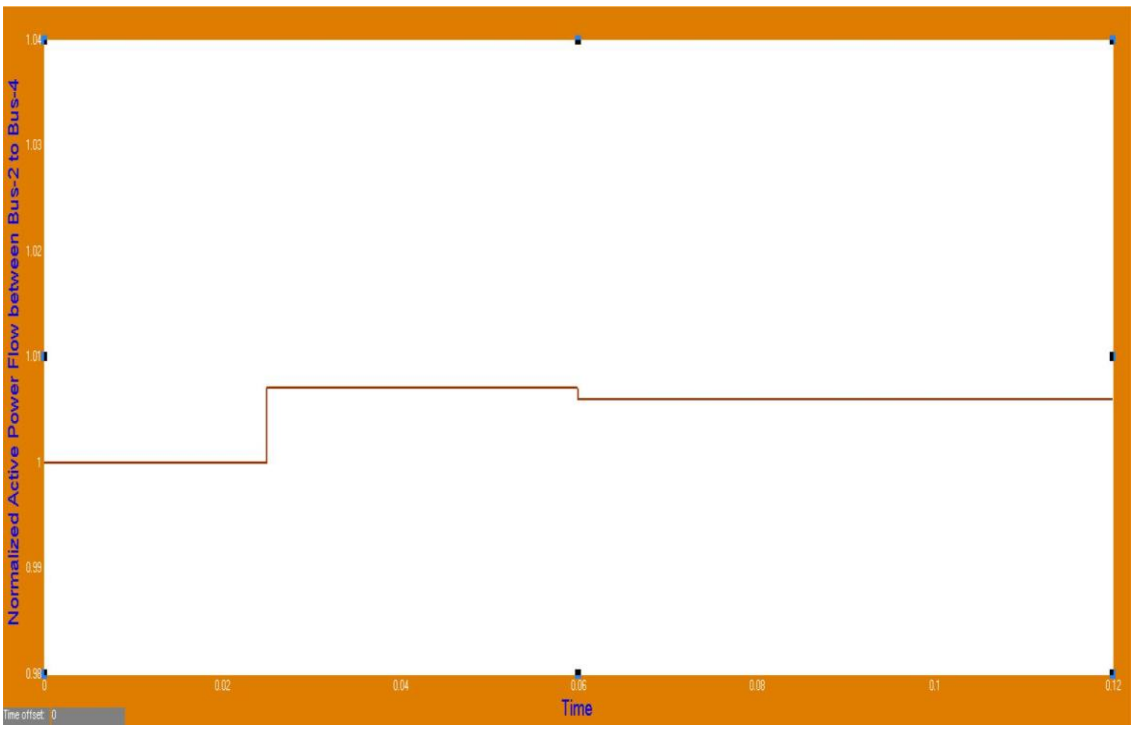

Figure-12 Attack impact of attacks on active power flows in the lines of bus 2 to 4

VI. CONCLUSION

As discussed in this paper we can say that the cyber-attack in SG has several effects on grid parameters magnitudes variation. The review on SG architecture, SG security and vulnerability analysis are discussed. The role of state estimation for SG security also represented, for validation the simulation has been carried out for IEEE 14-bus system. The simulation results shows the impact of cyber-attacks on generation profiles and active power flow of bus-1 and bus-2. The successful implementation of PMU is also implemented with discussion and improvement in active power flow is shown in simulation results.

REFERENCES

[1]. Anurag Srivastava, Thomas Morris,Timothy Ernster, , Ceeman Vellaithurai, , Shengyi Pan, and Uttam Adhikari, "Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information", IEEE TRANSACTIONS ON SMART GRID, VOL. 4, NO. 1, MARCH 2013.

[2]. James Ranjith Kumar R. and Biplab Sikdar, "Efficient Detection of False Data Injection Attacks on AC State Estimation in Smart Grids", 2017 IEEE Conference on Communications and Network Security (CNS): International Workshop on Cyber-Physical Systems Security (CPS-Sec), 978-1-5386-0683-2017 IEEE.

[3]. Kaikai Pan, Andr´e Teixeira, Claudio David L´opez and Peter Palensky, "Co-simulation for Cyber Security Analysis: Data Attacks against Energy Management System", SmartGridComm 2017 - 23 26 October, Dresden - ISBN 978-1-5386-4055-5, 978-1-5386-4055-2017 IEEE.

[4]. Abhinav Verma, "Power Grid Security Analysis: An Optimization Approach", Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, COLUMBIA UNIVERSITY 2009.

[5]. Abdulrahaman Okino Otuoze, Mohd Wazir Mustafaa, Raja Masood Larik, "Smart grids security challenges: Classification by sources of threats", Journal of Electrical Systems and Information Technology 5 (2018) 468–483, science Direct, 2018 Production and hosting by Elsevier B.V. on behalf of Electronics Research Institute (ERI).

[6]. K. Pan, A. M. H. Teixeira, M. Cvetkovic, and P. Palensky, "Combined data integrity and availability attacks on state estimation in cyberphysical power grids," in Proc. IEEE Int. Conf. Smart Grid Communications (SmartGridComm), Nov. 2016, pp. 271–277.

[7]. M. Stifter, J. H. Kazmi, F. Andr´en, and T. Strasser, "Co-simulation of power systems, communication and controls," in MSCPES, 2014 Workshop on, 2014, pp. 1–6.

[8]. M. Wei and W. Wang, "Greenbench: A benchmark for observing power grid vulnerability under data-centric threats," in INFOCOM, 2014 Proceedings IEEE, 2014, pp. 2625–2633.

[9]. M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of scada control systems (tasscs)," in Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES, 2011, pp. 1–7.

[10]. M. Findrik, P. Smith, J. H. Kazmi, M. Faschang, and F. Kupzog, "Towards secure and resilient networked power distribution grids: Process and tool adoption," in Smart Grid Communications (Smart Grid Comm), 2016 IEEE International Conference on, 2016, pp. 435–440.

[11]. H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in First Workshop on Secure Control Systems (SCS), Stockholm, 2010.

[12]. Tejaskumar Bhatt, Dr. Chetan Kotwal, Dr.Nirbhaykumar Chaubey, "Survey on Smart Grid: Threats, Vulnerabilities and Security Protocol" International Journal of Electronics, Electrical and Computational System, IJEECS, ISSN 2348-117X, Volume 6, Issue 9, September 2017.

[13]. H. Karimipour, A. Dehghantanha, R.M. Parizi, R. Choo, H. Leung, "A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-scale Smart Grids", IEEE Access, May. 2019.

[14]. E. Modiri, A. Azmoodeh, A. Dehghantanha, H. Karimipour, "Fuzzy Pattern Tree for Edge Attack Detection and Categorization", Elsevier Journal of Systems Architecture, pp. 1-15, Jan. 2018.

[15]. Chen, X., Yu, W., Griffith, D., Golmie, N. and Xu, G. (2014)On Cascading Failures and Countermeasures Based on Energy Storage in the Smart Grid. In: Proceedings of the 2014 Conference on Research in Adaptive and Convergent Systems, ACM, pp. 291–296.

[16]. Yang, Q., Yang, J., Yu, W., An, D., Zhang, N. and Zhao, W. (2014) On false data-injection attacks against power system state estimation: modeling and countermeasures. IEEE Transactions on Parallel Distributed Systems (TPDS), 25 (3), 717–729, doi: 10.1109/TPDS.2013.92.

[17]. Lin, J., Yu, W., Yang, X., Xu, G. and Zhao, W. (2012) On False Data Injection Attacks Against Distributed Energy Routing in Smart Grid. In: Proceedings of 2012 IEEE/ACM 3rd International Conference on Cyber-Physical Systems (ICCPS), IEEE, pp. 183–192.

[18]. Pasqualetti, F., Carli, R. and Bullo, F. (2011) A Distributed Method for State Estimation and False Data Detection in Power Networks. In: Proceedings of Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on, October 2011, pp. 469–474.

[19]. Kim, J., Tong, L. and Thomas, R.J. (2015) Subspace methods for data attack on state

estimation: a data driven approach. IEEE Transactions on Signal Processing, 63 (5), 1102–1114.

[20]. Yang, J., Yu, R., Liu, Y., Xie, S. and Zhang, Y. (2015) A Two-Stage Attacking Scheme for Low-Sparsity Unobservable Attacks in Smart Grid. In: Proceedings of IEEE International Conference on Communications (ICC), June 2015, pp. 7210–7215.

[21]. Liu, X., Bao, Z., Lu, D. and Li, Z. (2015) Modeling of local false data injection attacks with reduced network information. IEEE Transactions on Smart Grid, 6 (4), 1686–1696.

[22]. Berthier, R. and Sanders, W. (2011) Specification-Based Intrusion Detection for Advanced Metering Infrastructures. In: Proceedings of 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing (PRDC), December 2011, pp. 184–193.

[23]. Baig, Z. (2011) On the Use of Pattern Matching for Rapid Anomaly Detection in Smart Grid Infrastructures. In: Proceedings of 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), October 2011, pp. 214–219.

[24]. Manandhar, K., Cao, X., Hu, F. and Liu, Y. (2014) Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Transactions on Control of Network Systems, 1 (4), 370–379.

[25]. Huang, Y., Tang, J., Cheng, Y., Li, H., Campbell, K.A. and Han, Z. (2016) Real-time detection of false data injection in smart grid networks: an adaptive CUSUM method and analysis. IEEE Systems Journal, 10 (2), 532–543.

Mr.Mihir K Patel,etal. "Simulation Of Smart Grid Security And Vulnerability Analysis Using Pmu State Estimation." *International Journal of Engineering Research and Applications (IJERA*), vol.10 (04), 2020, pp 50-62.