SIMULATION OF SMART GRID SECURITY AGAINST CYBER-ATTACKS USING PMU STATE ESTIMATION

[1]Mrs. Payal Shah
[1]P.G. Scholar,
Electrical Department
LD College of Engineering
Ahmedabad, Gujarat, India.
E-mail Id- shahpayal13@gmail.com

[2]Dr. V. J. Upadhyay
[2]Associate Professor,
Electrical Department
LD College of Engineering
Ahmedabad, Gujarat, India.
E-mail Id- vju1974@gmail.com

Abstract— Nations across the world face the challenge of increasing power production while reducing the carbon emission. They need to minimize power loss and downtime, harness alternative power sources, and so on. The numerous challenges facing them have one solution – smart grids. In this paper we shows that smart grids bring improvements in cost and performance but at another side the security of the power grids becomes more complex and risky. The biggest challenge in SG is to assess the vulnerability of a cyber-physical power system to data attacks. The Bad data injection, False Data injection, and cyber-attacks are most focusing challenges reviewed in this paper. The PMU state estimation is one of promising solution for SG security. So we have shown the SG security analysis for IEEE 14-bus system using Matlab-Simulink. The simulation results shows that PMU provide protection against cyber-physical attacks as well as reliable and secure operation of S.G.

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

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:

- More economical transmission of electricity to consumers
- Quicker restoration of electricity when power disturbances occurs
- Reduced operations and management prices for utilities, and ultimately lower power prices for customers
- Reduced peak demand, which can conjointly facilitate lower electricity rates
- Increased integration of large-scale renewable energy systems
- Better integration of customer-owner power generation systems, together with renewable energy systems
- Improved security

"A smart grid is an electricity network with digital technology use to supply electricity to consumers via two-way digital communication. This system allows for monitoring, analysis, control and communication within the supply chain to improve efficiency, reduce energy consumption and cost, and maximize the transparency and reliability of the energy supply chain.'' Smart grid was introduced with the aim of overcoming the weaknesses of conventional electrical grids by using smart net meters. In electrical grid network the only key objective is to maintain the balance between load demand and power generation. Nations across the world face the challenge of increasing power production while reducing the carbon footprint. They need to minimize power loss and downtime, harness alternative power sources, and so on. The numerous

challenges facing them have alternative solution – i. e. smart grids.

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 concepts of discovery, access, feasibility, communication speed and detection threat. Real time simulations for modified IEEE 14 bus test case system and graph theory analysis for IEEE 118 bus system have been presented [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 and provides test the quality of the data even before the execution of the state estimation algorithm. The proposed method has been tested in the IEEE 118 bus system where false data with a magnitude ranging from 1% to 10 % is injected in four pairs of line power flows and one voltage measurement [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 on kalman filter which is implemented on the massively parallel architecture of graphic processing unit with the help of fine gained parallel programming technique.

Research Objectives: -

- To study the importance of smart grid development & security issues.
- Detection of False Data Injection (FDI) in SG infrastructures and provides security through PMU State Estimation.
- Implementing the Security for grid against FDI provides efficient and reliable operation.
- Implementation of IEEE-14 bus system using PMU State Estimation for SG Security against cyber-attacks and later on implement the proposed system for IEEE-30 bus system also. And authentication objective is achieved using Security of SG.

III. PROPOSED WORK AND VULNERABILITY ASSEMENT

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].

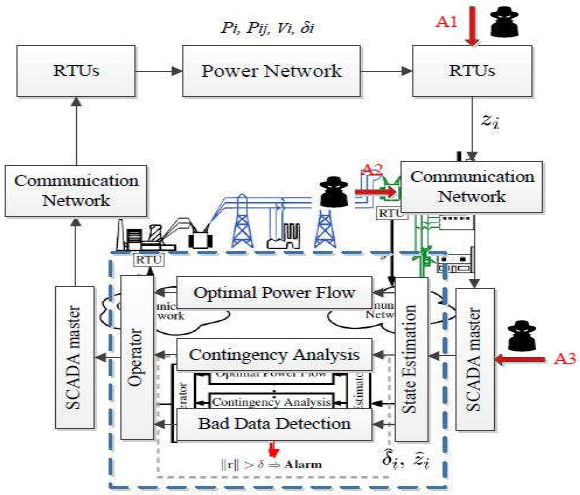

Fig.3- Energy Management System [1]

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 power balance equations are nonlinear, therefore the Gauss-Newton method is typically used for estimating the system states and this method is termed as AC State estimation.

Let consider z be the m dimensional vector that contains all the measured values and f(x) be the nonlinear function that maps the state variables x to the quantities that are measured through PMU. In the power system state estimation calculations, x represents the magnitudes and angles of node voltages and its dimensional size n is less than that of the measurements. It means n<m for making the system an over-determined.

As the measurements have noise, the mapping of the state variables to the measured values can be written as

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

Where e is the noise that is added to the true quantity. This mapping is nothing but the set of power balance equations and it is nonlinear in nature. Hence the process of estimating the states is usually iterative. At the ith iteration, the state correction vector is written as

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

Where H (X^i) is the Jacobian matrix for the function f(X^i) and R is the measurement covariance matrix. Using the state

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

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

This iteration process is repeated until the values of the state variables converge to a reasonable tolerance limit. In this power system model, by assuming that the voltage magnitudes are close to rated value and the difference of voltage angles in a line are extremely small, the equations may be linearized and can be solved fairly simply but with a trade-off in terms of the accuracy. Such a technique is popularly known as DC state estimation.

Phasor measurement unit

A **phasor measurement unit** (PMU) is a device used to estimate the magnitude and phase angle of an electrical phasor quantity (such as voltage or current) in the electricity grid using a common time source for synchronization. Time synchronization is usually provided by GPS and allows synchronized real-time measurements of multiple remote points on the grid. PMUs are capable of capturing samples from a waveform in quick succession and reconstructing the phasor quantity, made up of an angle measurement and a magnitude measurement. The resulting measurement is known as a **synchro phasor**. These time synchronized measurements are important because if the grid's supply and demand are not perfectly matched, frequency imbalances can cause stress on the grid, which is a potential cause for power outages. PMUs can also be used to measure the frequency in the power grid. A typical commercial PMU can report measurements with very high temporal resolution in the order of 30-60 measurements per second. This helps engineers in analyzing dynamic events in the grid which is not possible with traditional SCADA measurements that generate one measurement every 2 or 4 seconds. Therefore, PMUs equip utilities with enhanced monitoring and control capabilities and are considered to be one of the most important measuring devices in the future of power systems. A PMU can be a dedicated device, or the PMU function can be incorporated into a protective relay or other device.

IV. SIMULATION AND RESULT DISCUSSION

WEIGHTED LEAST SQUARE STATE ESTIMATION AND ANN BASED STATE ESTIMATION

Given the network and the required bus data, the true bus voltages and line flows are determined by Conventional Load Flow using Newton Raphson method. Given the meter placement, type and accuracies, a set of meter readings is simulated by adding errors from a random number generator, which generates a number based on Gaussian density function with the mean value and standard deviation specified. Using the simulated measurements, the best estimates of bus voltages and phase angles are calculated using the PMU State Estimator.

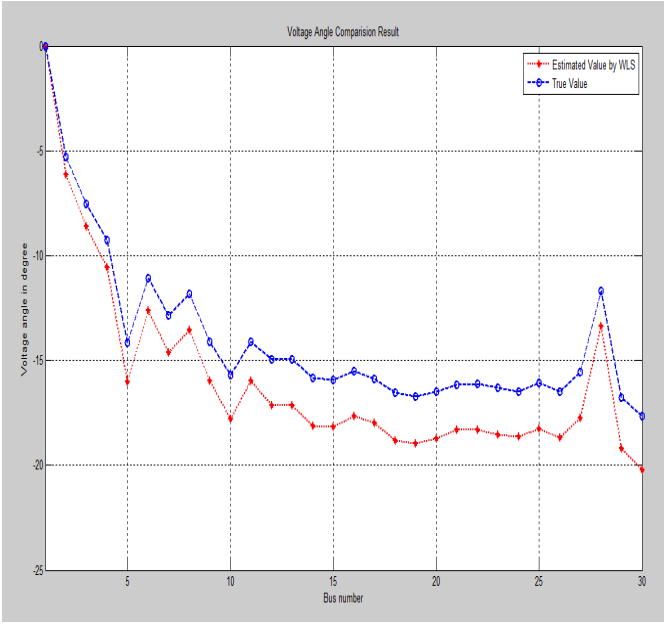

Fig.4- Voltage Angle Comparison with WLS estimation for IEEE 30 bus system

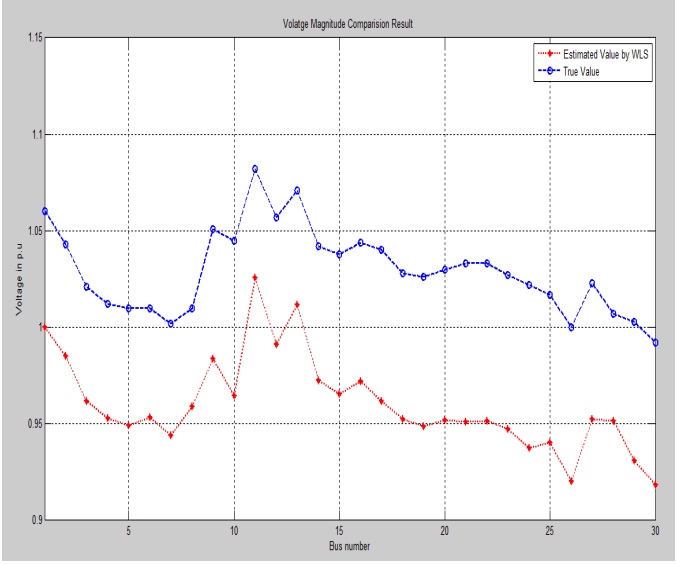

Fig 5- Voltage Magnitude Comparison with WLS estimation for IEEE 30 bus system

RESULTS OF IEEE 30 BUS SYSTEM WITH GM SE

GM estimation

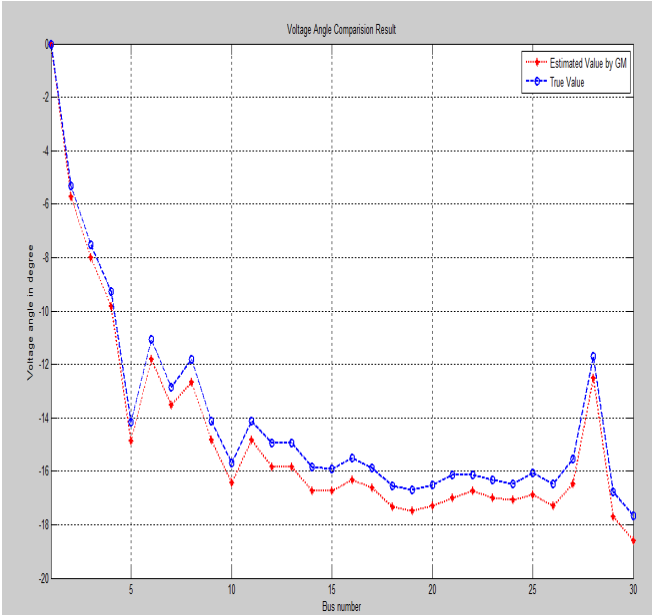

Fig 6- Voltage Angle Comparison with GM state estimation for IEEE 30 bus system

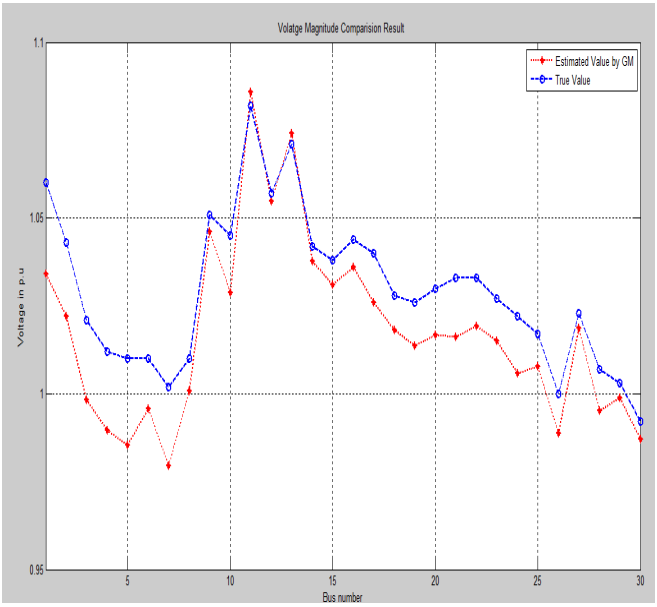

Fig.7- Voltage Magnitude Comparison with GM state estimation for IEEE 30 bus system

RESULTS OF IEEE 30 BUS SYSTEM WITH PMU SE

PMU estimation

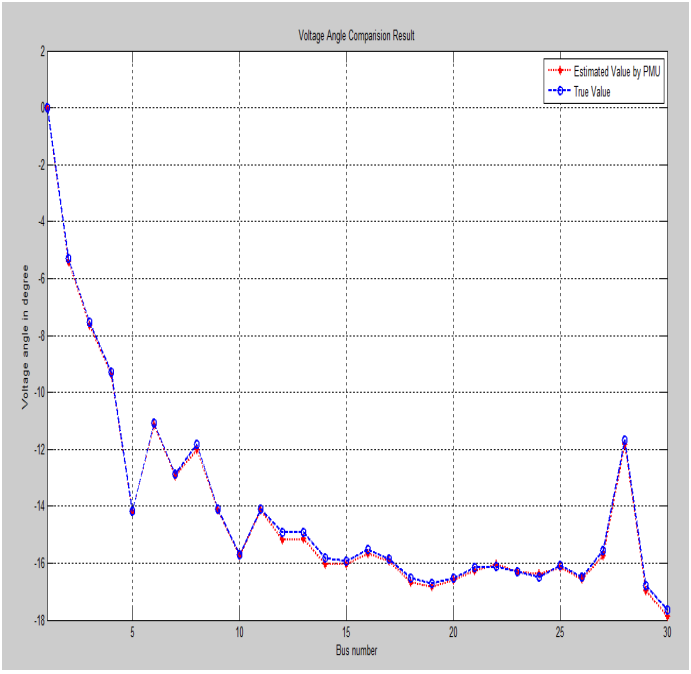

Fig.8- Voltage Angle Comparison with PMU state estimation for IEEE 30 bus system

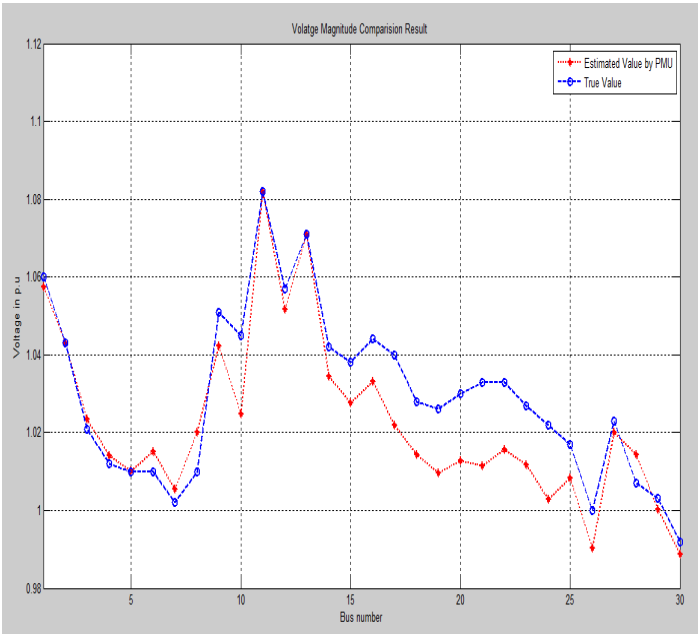

Fig.9- Voltage Magnitude Comparison with PMU state estimation for IEEE 30 bus system

COMPARISON OF CONVENTIONAL SE METHODS

As shown in the above simulation results of conventional state estimation methods including GM, WLS, and PMU, we can say that PMU State estimation techniques provides accurate results for Voltage magnitude and angle variation among all

other techniques of SE. Using the simulated measurements, the best estimates of bus voltages and phase angles are calculated using the PMU Estimator. The percentage error in the estimates with respect to the true values are determined. This is done for IEEE 30 bus system. The comparison of above methods are shown in results below.

Comparison

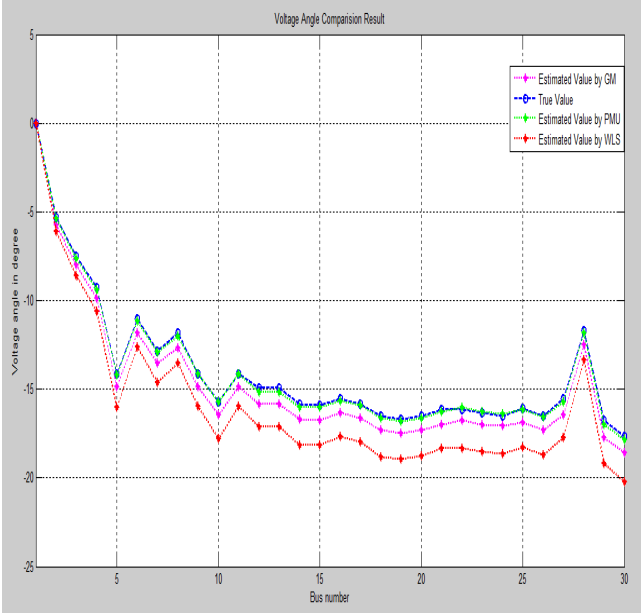

Fig.10- Voltage Angle Comparison of different S.E techniques w.r.t to True value for IEEE 30 bus system

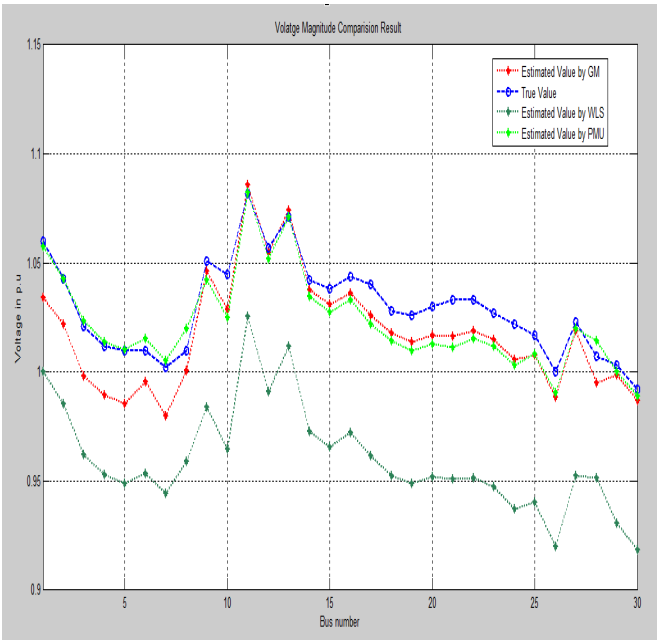

Fig.11- Voltage magnitude Comparison of different S.E techniques w.r.t to True value for IEEE 30 bus system

FDI detection through PMU SE

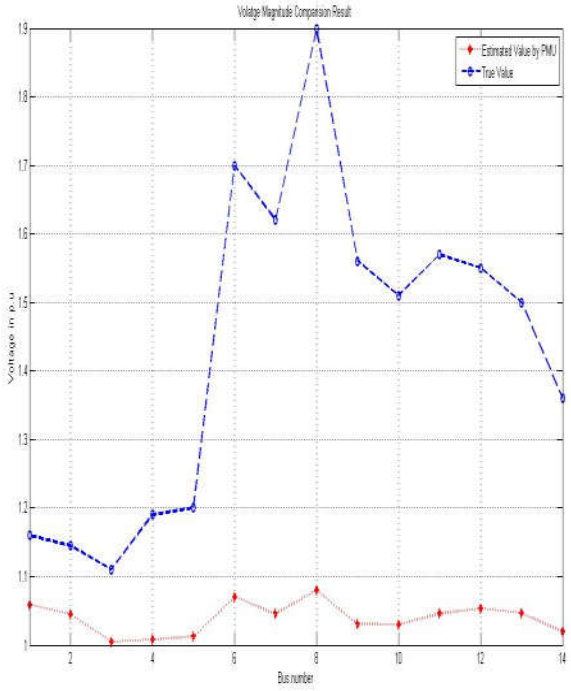

Fig.12- Voltage Magnitude Change

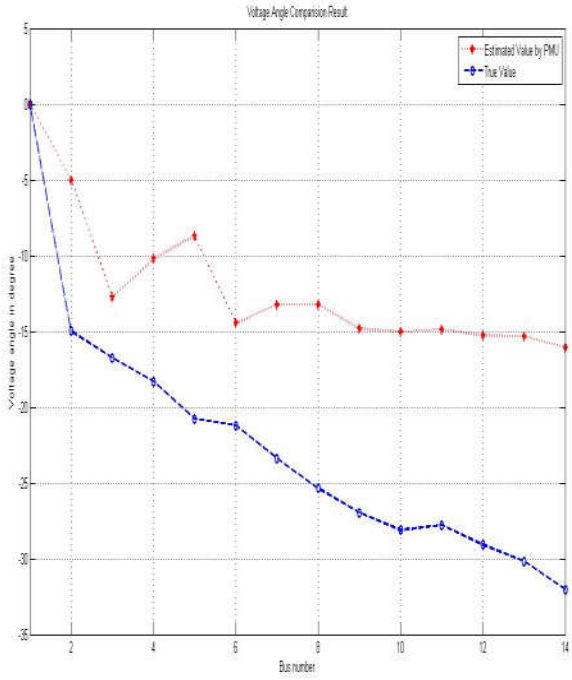

Fig.13- Voltage Angle Change

V. 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