International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 1, Jan-Feb 2021

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

IMPACT OF CYBER-ATTACK ON POWER SYSTEM STABILITY RISK ASSESSMENT

Ketchiozo Wandji*, Ali Aliwi**

*(Electrical Engineering, Morgan State University, and MD, USA
Email: Ketchiozo.Wandji@morgan.edu)

** (Electrical Engineering, Morgan State University, and MD, USA
Email : alali2@morgan.edu)

----------**********----------

Abstract:

Along with new smart grid technology, many challenges show up on the surface. Among them, cybersecurity is one of the most sophisticated challenges where correlative threats from malicious cyber-attacks on the electric grids continue to grow in frequency at power system cybersecurity technologies developed to protect networks from breaking into phasor measurements unit (PMU). PMU is uniquely designed to monitor and control real-time variable data like the voltage, phase angle, current, active, and reactive power on the wide power grid to continue delivering reliable energy to support economic security. Traditionally, PMU used State Estimation (S.E.) algorithms to consider real-time data from Remote Terminal measured in the power system to improve control and protection. The PMU is deployed through the system based on the topological observability theory using graph theorem analysis. The collected state estimation real-time data would then be transferred to Phasor Data Concentrators (PDC)s systems over Internet Protocol (IP) network infrastructure. Thus, some cybersecurity vulnerabilities existed. Within the context of this paper, the researcher has used a what-if analysis technique to identify threats and hazards. The impact of S.E. cyber-attacks on power system stability is investigated via simulations of different scenarios on the attack of the collected real-time data, to assess the risk on power system stability. A correct selection and consideration of the case study and the results analyzed, collectively yield the desired effect of the research methodology. Besides, this also determines the outcome of the research and helps achieve the research goals and objectives. The Power System Analysis Toolbox (PSAT) in MATLAB environment is used for data analysis and simulation. Finally, this research study describes the research findings and conclusions. It provides practical recommendations that not only aid in a deeper understanding of the research but also aids in further research in the future.

Keywords — **Power Flow, Cyber Security, State Estimation, False Data Injection, Voltage Stability.**

----------**********----------

I. INTRODUCTION

A cyber-physical systems (CPS) attack can lead to a loss of control in nuclear reactors, gas turbines, the power grid, transportation networks, and other critical infrastructure, placing the nation's security, economy, and public safety at risk. Electricity is critical to sustaining and enhancing living standards in North America and around the world. The reliability of electricity infrastructures is a vital need among many consumers. Enhancing the efficiency of energy generation or producing more energy are strategies that can enhance consumption. The smart grid refers to a contemporary power system that utilizes ICT to offer sustainable, reliable, and

efficient energy. The smart system enables energy and information to flow in a bidirectional manner in distribution and transmission systems. These systems enable real-time monitoring, enhancing situational awareness while guaranteeing the continual flow of power to consumers. In power systems operations, real-time feedback is fundamental. Nonetheless, these systems are prone to cyber-attacks. Scholars have previously examined data spoofing, Man-in-the-Middle, physical damage, packet analysis, malicious code injection, deniability of service, and PMU vulnerabilities and attacks. These attacks have varying impacts on networks. Researchers have also classified these attacks into fabrication, modification, and interruption classes. These classes of attacks have varying impacts on the network. There is a need for further research to determine the effects of each attack. In this thesis, the focus is to examine attacks documented previously and security vulnerability assessment. The strategy is to offer information on possible attacks, including measures to counter such attacks. The paper also provides security vulnerability testing focusing on side-channel attacks and traffic analysis. Despite the presence of documented attacks, minimal research has been conducted in this area. Therefore, this paper adds to the PMU network security, particularly documented attacks retrieved from existing literature. The thesis exposes side-channel and traffic analysis attacks while providing risk assessment. The thesis' primary goal is to ascertain security vulnerabilities to develop possible countermeasures.

II. System Overview

At the voltage stability limit, the Jacobian matrix of power flow equations are singular. Ensuring a continuous power flow resolves this problem. Based on a load scenario, the continuous power flow provides solutions for load flow. Notably, it comprises the correction and prediction stages. The tangent predictor estimates the next solution for a specific pattern of load increase from a known base solution. In the correction stage, the Newton-Raphson technique aids in determining the exact solution. The conventional power flow employees this technique. Consequently, a new prediction comes up to provide a specific load increase through the new tangent vector. The corrector stage follows, and the process is continuous up to the critical point. At the critical point, the tangent vector is 0. The insertion of a load parameter reformulates the first power flow in continuation load flow.
Injected powers can be written for the k bus of an n-bus system as follows:

$$P_k = \sum_{l=1}^{N} |V_k||V_l|\,|Y_{kl}|cos\,(\delta_k - \delta_l - \theta_{kl})$$

$$Q_k = \sum_{l=1}^{N} |V_k||V_l|\,|Y_{kl}|\,sin(\delta_k - \delta_l - \theta_{kl})$$

$$P_k = PG_k + PD_k$$
$$Q_k = QG_k + QD_k$$

D and G subscripts indicate load and generation demand, respectively. A load parameter $\boldsymbol{\lambda}$ is inserted into demand powers $\boldsymbol{PDk}$ and $\boldsymbol{QDk}$ simulate a load change.

$$PD_k = PG\,(1 + \lambda\,)$$
$$QD_k = QG(1 + \lambda\,)$$

III. Power Flow Solutions

Power flow refers to the energy transportation rate in transmission lines. The analytic solving of the power flow problem is a challenge. Therefore, iterative solutions on computer systems prove effective. Henceforth, this section reviews two solution methods, namely the Newton-Raphson and the Gauss iteration (Gauss-Seidel iterative) methods.
Studying power flow provides an understanding of the magnitude of information for every power system bus and the voltage angle. Thus, this sheds

light on voltage conditions and generator and load power. In this process, one can analytically determine the generator reactive power output and the reactive and real power flow. Experts apply a range of numerical methods to come up with a solution because this problem is nonlinear.

Solutions to power flow issues start by determining the unknown and known variables. Significantly, these variables rely on the form of the bus. A Load Bus is that which has no connected generators. Conversely, a Generator Bus is that which has at least one connected generator. One selected arbitrary bus with a generator, called the Stack Bus, was the exception.

In resolving power flow problems, there is the basic assumption that at every Load Bus, the reactive power demand, and the real power demand (PD) at every Load Bus (QD). That is why "Load Buses" are termed as "PQ-Buses." Additionally, there is the assumption that the "voltage magnitude |V|" and the power generated (PG) are known for generator buses. Furthermore, the assumption for the "Slack Bus" is that the "voltage phase (θ)" and "voltage magnitude |V|" are familiar. Although it is possible to contrive a solvable system in which the Slack Bus has fixed vars (Q) and fixed angle (θ), selecting the biggest generator to function as the Slack Bus enhances the regulation of V and θ. Significantly, the reference phase angle is also integral in setting the system frequency (F). The fact is that Theta is the "constant" aspect of the time-varying quantity. Therefore, the Slack Machine plays a fundamental part in the regulation of system frequency. The process occurs in real-time while providing power flow calculations. Thus, the "voltage angle and magnitude" are known for each Load Bus and should be solved. Regarding the Slack Bus, no variables should be solved. There are unknowns in a system comprising R generators and N buses. Resolving this requires an equation that does not incorporate new unknown variables. The power balance equation is one of the possible equations to use in this case. The equation can be provided for reactive and real power for every bus. Hence, this equation is as follows:

$P_k = \sum_{l=1}^{N} |V_k||V_l|\,|Y_{kl}| cos\,(\delta_k - \delta_l - \theta_{kl})$

A breakdown of this equation is as follows

P_k -net power injected at bus k ,

$|V_l|$ –Voltage magnitude

δ_l - Angle of ith bus

$|Y_{kl}|$ -Magnitude of the bus admittance matrix ($YBUS$).

θ_{kl} -angle of YBUS corresponding to the kth row and lth column

The following is the power balance equation

$$Q_k = \sum_{l=1}^{N} |V_k||V_l|\,|Y_{kl}|\, sin(\delta_k - \delta_l - \theta_{kl})$$

Q_k - Net reactive power injected at bus k.

$$\text{Vol}\begin{bmatrix}\Delta\theta \\ \Delta|V|\end{bmatrix} = -J^{-1}\begin{bmatrix}\Delta P \\ \Delta Q\end{bmatrix}$$

and J is a matrix of partial derivatives known as a Jacobian

$$\text{J} = \begin{bmatrix}\frac{\partial \text{P}}{\partial \theta} & \frac{\partial \text{P}}{\partial |\text{V}|} \\ \frac{\partial \text{Q}}{\partial \theta} & \frac{\partial \text{Q}}{\partial |\text{V}|}\end{bmatrix}$$

The linearized system of equations is solved to determine the next guess (m + 1) of voltage magnitude and angles based on:

$$\theta^{m+1} = \theta^m + \Delta\theta$$
$$|V|^{m+1} = |V|^m + \Delta|V|$$

The process is continuous until it meets the stopping condition. The role of root finding routines is to evaluate every step to determine whether the current outcome is good. The tests conducted in this process are termed as stopping tests or termination conditions. The tests are represented as follows:

Residual size $|f(x)| < \epsilon$

Increment size $|x_{new} - x_{old}| < \epsilon$

Number of iterations: $ITCount > ITMAX$; IT is the iteration

The residual size is a vital choice because at the solution, the residual is zero. Nonetheless, this is a bad choice since the residual can be minutes despite iterate being far from the actual solution. The increment size is an excellent choice due to quadratic convergence nature of Newton's model. In this process, the increment excellently approximates the true error. The third stopping criterion is applied after the iteration numbers surpass the maximum. Hence, this is a safety indicator to determine the iteration's capacity to terminate infinitely. The following is an outline of the power flow problem solutions include an attack.

- Guess all the unknown angles and magnitudes. In most cases, scholars begin with a "flat start" by setting all voltage magnitudes at 1.0 p.u., and voltage angles at 0. Practically, utilizing the biggest generator as the Slack Bus promotes the regulation of θ and V.
- The most recent voltage magnitude and angle values should be used to resolve the power balance.
- The system should be linearized around recent voltage magnitude and angel values.
- Calculate changes in voltage magnitude and angle
- Provide an update of the voltage angle and magnitude
- Monitor stopping conditions and terminate when met.

IV. PMU PLACEMENT

This study used optimal placement of Phasor Measurement Units (PMUs) for the purpose of power system observability using topology based formulated algorithms. The optimal PMU placement problem is formulated to minimize the number of PMUs installation subject to full network observability. The used observability rules are as follows:

- For PMU installed buses, voltage phasor and current phasor of all its incident branches are known. These are called as direct measurements
- If voltage and current phasors at one end of a branch are known, then voltage phasor at the other end of the branch can be obtained. These are called pseudo measurements.
- If voltage phasors of both ends of a branch are known, then the current phasor of this branch can be obtained directly. These measurements are also called pseudo measurements
- For a zero-injection bus i in a N-bus system we have:

$$\sum_{j=1}^{N} Y_{ij} V_j$$

where, Yij is the $ijth$ element of admittance matrix of the system and Vj is the voltage phasor of jth buse.

Therefore, if there is a zero-injection bus without PMU whose incident branches current phasors are all known but one, then the current phasor of the unknown one could be obtainable using KCL equations.

Based on topology based formulated algorithms, PMUs will be located at Bus 6, Bus 12, Bus 22, Bus 25, and Bus 30.

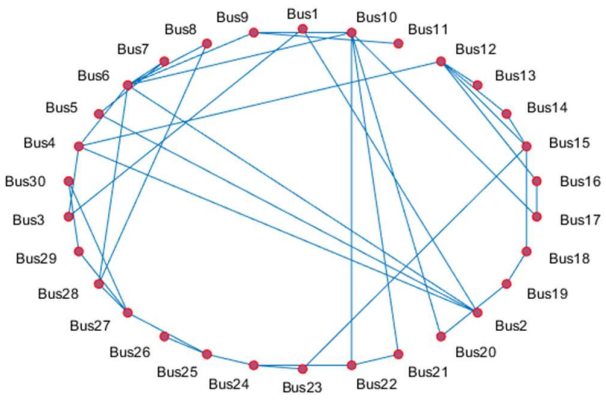


Figure 1: Graph Representation Network

V. Data Spoofing Attacks

The hacker can inject malicious software into the system, contributing to malicious tendencies in the network. In spoofing attacks, the system can send illegitimate messages to various devices and components in the synchrophasor system. Attackers may spoof GPS signals, contributing to bad-time synchronization. The outcome is an impact on redundant time synchronization schemes, making it difficult to detect errors. In systems experiencing data spoofing, the system acknowledges false data as opposed to the real data. That is why data spoofing attackers are dangerous to the reliability and stability of smart grids. The outcome is a malfunction of instability in the system, depending on the nature of information injected by the attacker. Hence, this reveals the need to develop preventive measures to safeguard smart grids, which are increasingly at risk of any of the above attacks. In contemporary society, technology has enhanced energy efficiency while compromising existing systems.

VI. False Data Injection Attacks

In the linear model, the attacker fools the control centre mainly by keeping the measurement residual unchanged, although the attacker has injected bad data into meters [1].

This is the targeted "false data injection attack," where the attacker focuses on finding an attack vector with the capacity to input a precise error into specific state variables. On the other hand, the "random false data injection attacks" involve the hacker aiming to locate attack vectors as far as the outcome is a wrong estimate of the state variables. Both attacks have the capacity to damage the power systems significantly. Nonetheless, random false data injection is more comfortable to execute. Regarding the "false data injection attacks," a possible attack scenario has been developed to enhance the understanding of ways in which the attacker can develop attack vectors to penetrate the existing poor measurement detection strategies.

Denoting a as the vector of malicious data, which is injected into the original measurement data z, therefore, the measurement vector is polluted as $z_{bad} = z + a$ after attack.

Denoting c as the deviation vector of the estimated state variable before and after the attack, the estimated state variable vector after attack can be represented as

$$\boldsymbol{x_{bad} = x + c}$$

$$\boldsymbol{\hat{x}_{bad} = (H^T W H)^{-1} H^T H_{zbad} = (H^T W H)^{-1} H^T H(z + a)}$$

$$\boldsymbol{\hat{x}_{bad} = \hat{x} + (H^T W H)^{-1} H^T W a = \hat{x} + c}$$

The target of the attacker is to find the vector of malicious data which keeps the measurement residual unchanged before and after attack.$\hat{x}_{bad} = \hat{x} + c$, then:

$$\boldsymbol{\|z_{bad} - H\hat{x}_{bad}\| = \|z + a - H(\hat{x} + H^T W H)^{-1} H^T W a\|}$$

VII. Voltage-Loading Parameter (V-λ) Curve

The (V-λ) curve proves useful in analysis processes involving power flow solutions to monitor the impacts of the system voltage on the system due to an increase in power transfer. A range of load flow solutions produces this curve for various load levels that are distributed uniformly. In this process, the power factor remains constant. Moreover, the generator rating increases the generated active power proportionally. It is fundamental to determine the given load's critical point. The fact is that it can contribute to the system's voltage collapse. Different researchers have utilized various load flow analysis to propose voltage stability indexes. The objective of these scholars is to assess the voltage stability limits. Nonetheless, when applying the Jacobian model alongside the Newton-Raphson method, the outcome is singular at the critical point. Additionally, a divergence is evident for load flow solutions near the critical limit. Thus, the continuous load flow eliminates these disadvantages.

The load bus makes it easy to draw the P-V curve as shown in figure (1), permitting the calculation of maximum transmissible power. Every transfer power value is corresponding to the voltage value at the bus until V-Vcrit. Any further decline in power at this point contributes to the bus voltage deterioration. The uppermost section of the curve reveals acceptable operations, while the lower side indicates unstable operations. Ensuring that the bus voltage is away from the critical voltage by an upper value decreases the voltage collapse risk. Therefore, the (V-λ) curve is fundamental in determining the collapse margin, contingencies, and the system's critical operating voltage.

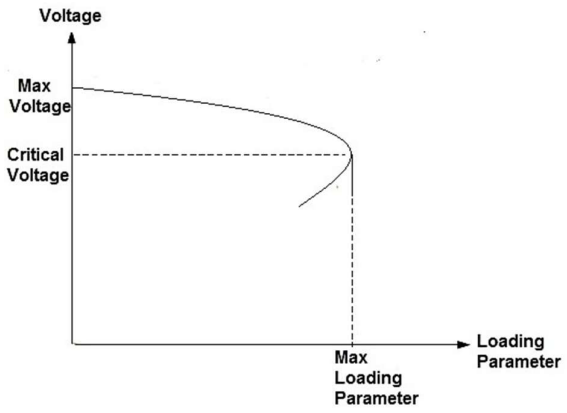


Figure 1: P-V Curve

VIII. Experimental Results and Discussion

The test system is IEEE 30 bus, Figure 2. It consists of 6 generator-buses (bus no. 1,2,13,22,23 and 27), 24 load-buses (bus no. 2,4,5,6,7,8,9,10,11,12,14,15,16,17,18,19,20,21,24,25,26,28,29, and 30) and 41 transmission lines. The total system demand is 9750.25 MW. The base power for all scenarios is 100 MVA. The following scenarios were carried out on the case study. The simulation studies were carried out PSAT/ MATLAB. The bus data and line data of the 30-bus test system are taken from Power Systems test case archive at IEEE.

- **Steady State Case**

The λ-V curves are obtained with base case load demand of standard IEEE 30 bus system under steady state condition for comparison purposes. Figures (3) shows the λ-V curves respectively for bus 1, thru bus 30, we notice that the loading parameter for nominated buses is reached to 15 p.u. and the voltage magnitudes for same buses lies between (0.55 to 1.01) p.u.

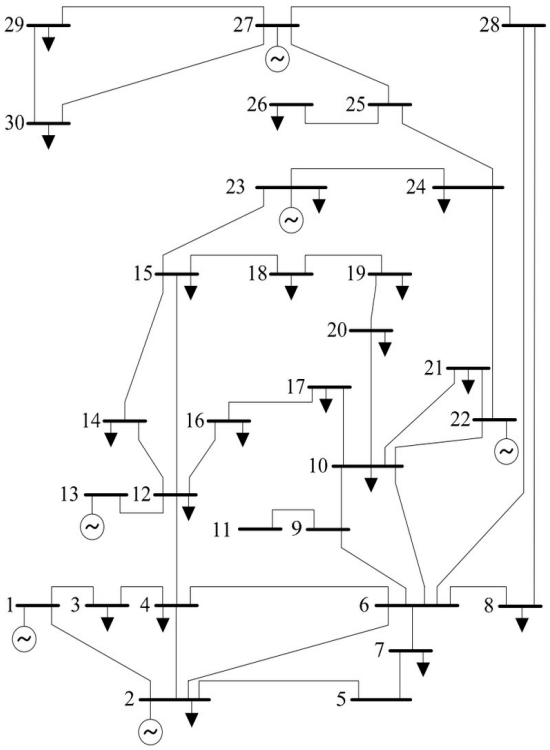
- **limited Attack Case**

there are five PMU deployed along the 30-bus system located at Bus 6, Bus 12, Bus 22, Bus 25, and Bus 30. The malicious gained access to control two PMUs, both located at bus 6 and bus 25, respectively. After injecting errors along with power flow calculation algorithm to manipulate the real time demand, we notice that the loading parameter for nominated buses is dropped compared to steady state case from 15p.u to 13p.u, the voltage profiles reduced, and the stability of the system has been impacted because transfer capability reduced.
Figures (4) shows the λ-V curves respectively for bus 1, thru bus 30.

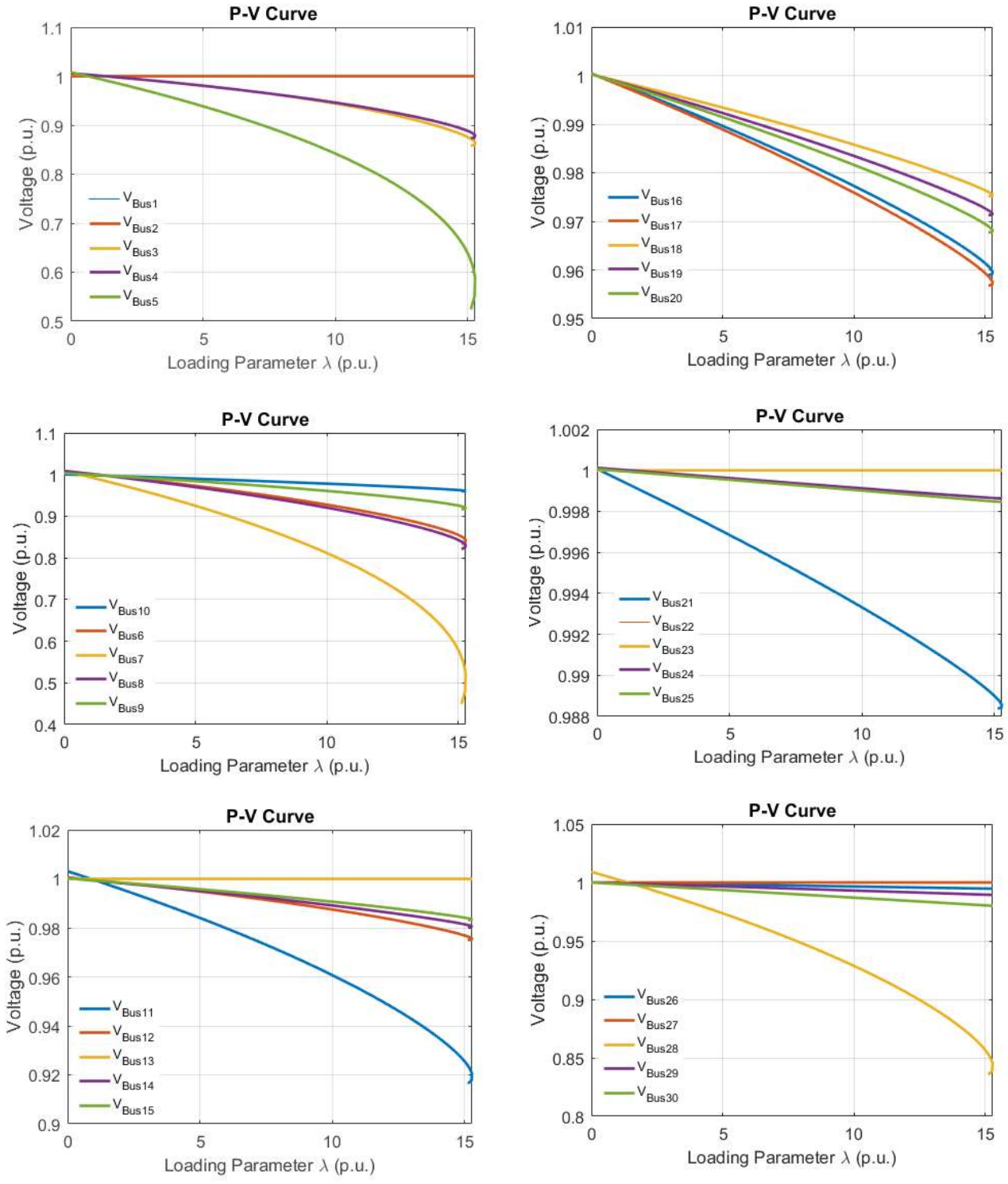
- **Advance Attack Case**

there are five PMU deployed along the 30-bus system located at Bus 6, Bus 12, Bus 22, Bus 25, and Bus 30. The malicious gained access to control three PMUs, both located at bus 12, bus 22 and bus 30, respectively. After injecting errors along with power flow calculation algorithm to manipulate the real time demand, we notice that the loading parameter for nominated buses is dropped compared to both case studies to be 8p.u. the voltage profiles reduced, and the stability of the system has been impacted as shown in figures (5).

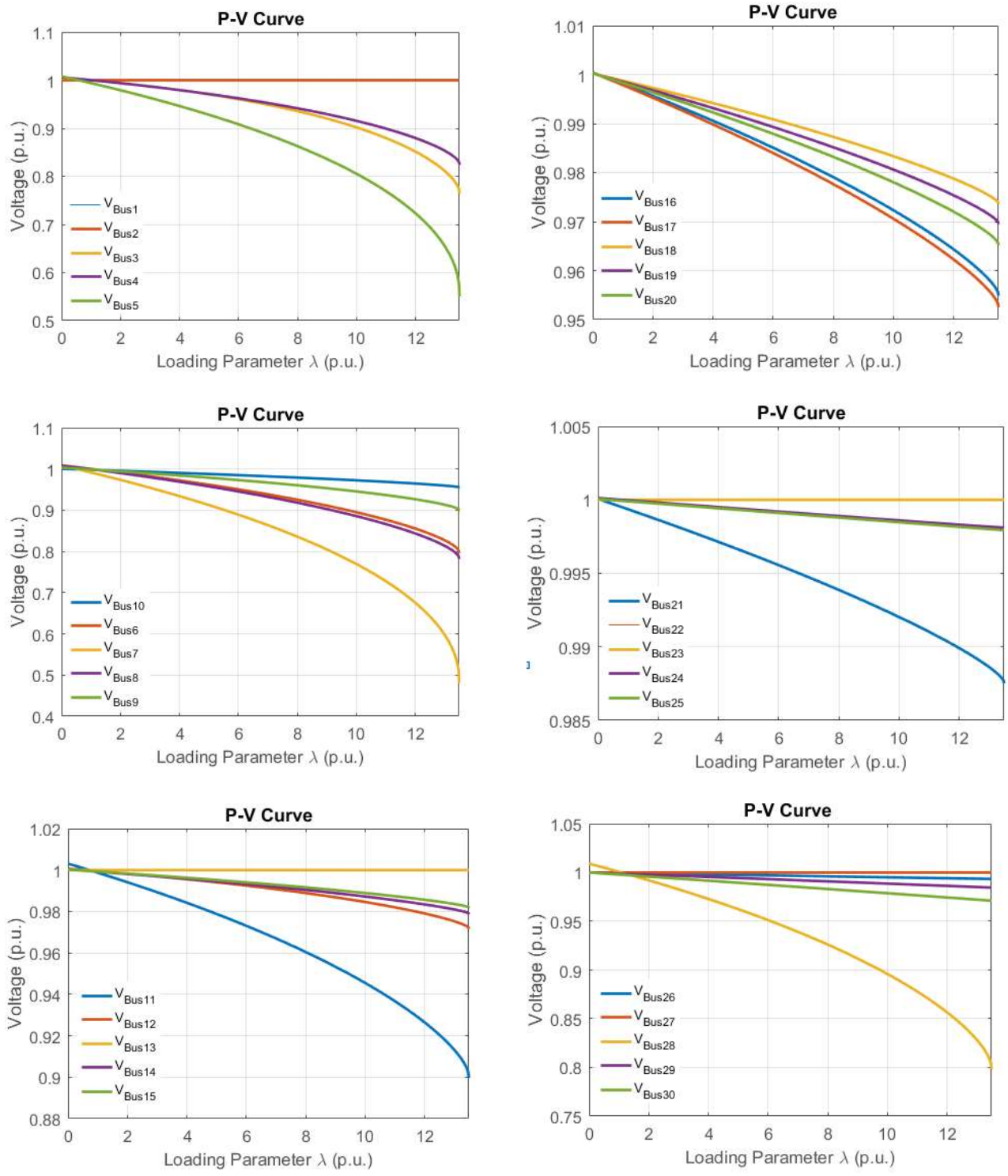
In the bulk interconnected power systems, the stability of the power systems remains a critical issue globally. The reason is that it becomes challenging to secure power system operations. Some of the recent blackouts that have been experienced globally depict the issue of secure operations. Voltage collapse is a critical issue in complex power grits. Voltage collapse refers to an occurrence in which the events that accompany instability in voltage contribute a significant drop in unacceptable voltage in a substantial section of the power system. In case the drop is catastrophic, a stability loss is experienced in bulk interconnected power systems, contributing to blackouts. Thus, in this case if the real time demand increased the voltage dropped will drop more and then cause voltage collapse.



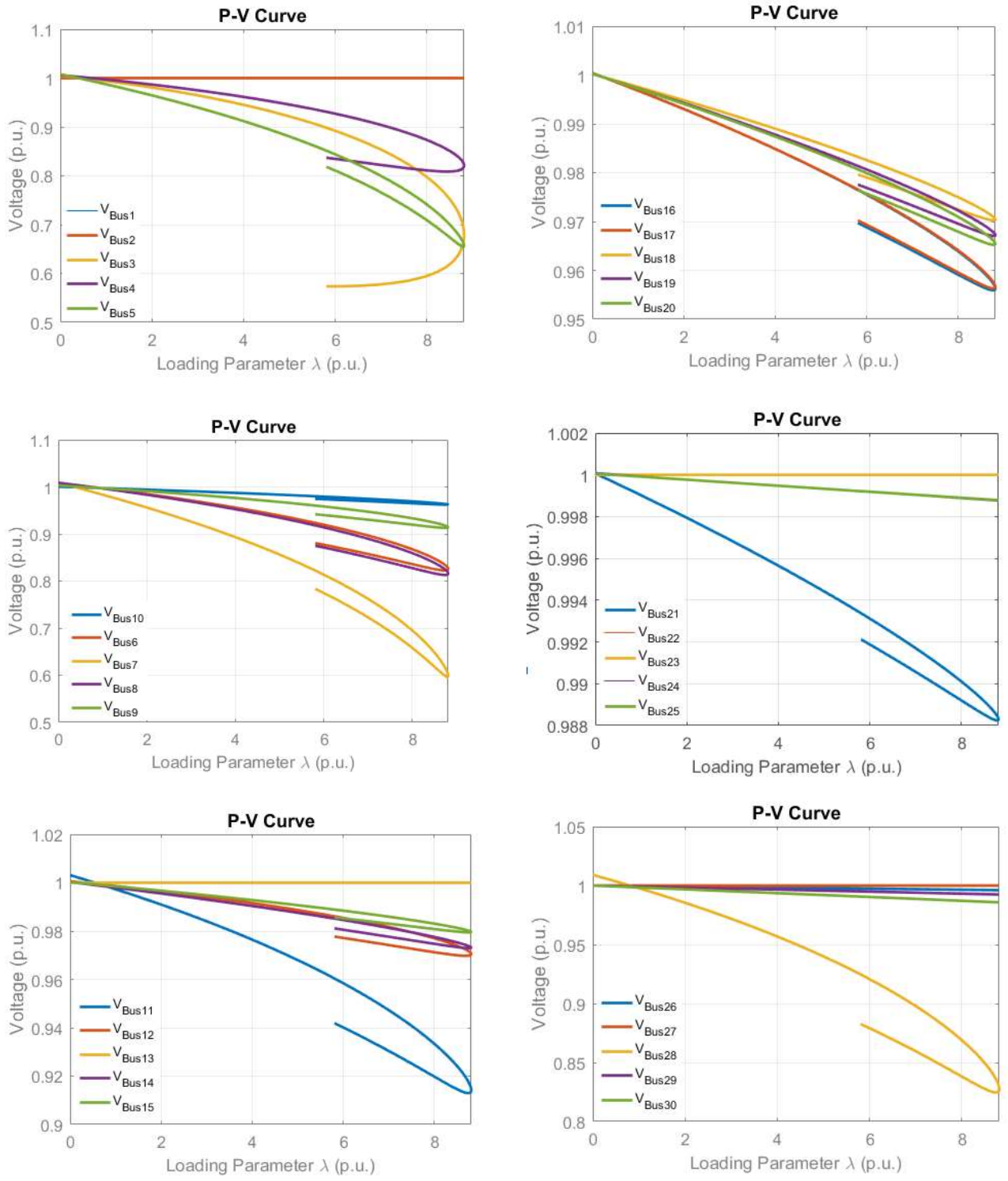
Figures 2: IEEE 30 bus



Figures 3: Voltage Profile Steady State Case



Figures 4: Voltage Profile under limited attack case



Figures 5: Voltage Profile under Advance attack case

IX. CONCLUSION

In this paper we investigated the implications of this vulnerability through presenting and analysing a class of attacks, called false data injection attacks, against state estimation in electric power systems. Under the assumption that the attacker can inject random acceptable errors extracted from historical data by manipulate the measurements of meters at physically protected locations, such attacks can introduce arbitrary errors into certain state variables without being detected by existing techniques. We considered an attack scenario, where the attacker is constrained to some specific PMUs, we showed that the attacker can systematically and efficiently construct attack vectors in this scenario, which can not only change the results of state estimation, but also modify the results in a predicted way. We also extended false data injection attacks to generalized false data injection attacks and used both theoretical analysis and simulation to show that an attacker can gain more impact than false data injection attacks by launching generalized false data injection attacks and performed risk assessment and show the real impact on power system security.

X. REFERENCES

[1] Jiongcong CHEN "Impact analysis of false data injection attacks on power system static security assessment" J. Mod. Power Syst. Clean Energy (2016) 4(3):496–505 DOI 10.1007/s40565-016-0223-6

[2] Vao Liu and Peng Ning, Michael k. Reiter "False Data Injection Attacks against State Estimation in Electric
Power Grids", In ACM Transactions on Information and System Security, Vol. 14, No. 1, Article 13, Publication date: May 2011.

[3] Kai Sun, "An Online Dynamic Security Assessment Scheme Using Phasor Measurements and Decision Trees" DOI: 10.1109/TPWRS.2007.908476 · Source: IEEE Xplore.

[4] Pankaj Sahu "Phasor Measurement Units Optimal Placement and Performance Limits for Fault Localization"
DOI: 10.1109/CERA.2017.8343356, Oct 2017

[5] Jinsub Kim and Lang Tong, "On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures" IEEE journal on selected areas in communications, vol. 31, no. 7, July 2013

[6] Dongchan Lee, Deepa Kundur., "Cyber Attack Detection in PMU Measurements via the Expectation-Maximization Algorithm", GlobalSIP14-Signal and Information Processing for Energy Exchange and Intelligent Trading

[7] Surender Kumar, "Cyber Security Threats in Synchrophasor System in WAMS," International Journal of Computer Applications (0975 – 8887) Volume 115 – No. 8, April 2015

