Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4081 - 4093
Received 25 April 2021; Accepted 08 May 2021.

Smart Hybrid Grid Infrastructure Stability Assessment and Remote Health Monitoring due to Growing Potential Risk of Cyber Threats

Ayan Banik[1*], Anubrata Sengupta[2], Sayan Ghosh[3], Rounak Das[4], Meenakshi Gupta[5], Nivedita Singh[6]

[1]Department of Electrical Engineering, National Institute of Technical Teachers' Training & Research, Kolkata

[2]School of Illumination Science Engineering and Design, Jadavpur University, Kolkata

[3,4]Cooch Behar Government Engineering College, Kochbehar

[5]School of Engineering and technology, Sushant University (Erstwhile Ansal University), Gurugram

[6]Department of Electrical Engineering,Shri Rawatpura Sarkar University, Raipur

*ayanbanik97@yahoo.com

ABSTRACT

Grid Infrastructure serves as one of the most crucial and sophisticated linkages between different dimensions of the Power System. With the increasing popularity of grid-tied new renewable energy systems and DERs, there is a growing challenge to integrate it without much disturbing system frequency and stability parameters. In recent time grid has been witnessed several unknown threats, both physical and internal. The most common and potential danger is the risk of cybersecurity issues, as a comprehensive data breach may lead to a substantial unwanted crisis that has not been encounter never before. Most countries worldwide follow one grid policy, so any instability due to cyber-attacks may cause considerable damages economically, morally and socially. Electric Power system cyber protection solutions designed to defend networks from breaking into phasor measurements unit (PMU). PMU is specifically developed to remotely monitor and regulate real-time variable data on the power grid, such as voltage, phase angle, current, active, and reactive power, to maintain reliable energy delivery and industrial security. PMU has traditionally employed for State Estimation algorithms to include real-time data from Remote Terminals monitored in the power system to enhance control and protection. The PMU is disseminated across the system utilising graph theorem analysis and topological observability theory. The acquired state estimate real-time data would then be sent through the Internet Protocol (IP) network architecture to Phasor Data Concentrators (PDC) systems. As a result, various cybersecurity flaws occurred. The researchers in this work have attempted to utilised a what-if analysis methodology to identify dangers and hazards. The influence of S.E. cyber-attacks on power system stability is explored using simulations of several scenarios, including the attack of real-time data to determine the danger to power system stability. The intended impact of the research approach is achieved by the proper selection and examination of the case study and the data assessed jointly. Besides, this also determines the outcome of the research and helps achieve the research goals and objectives. The Power System Analysis Toolbox (PSAT) in the MATLAB environment has been used for data analysis and simulation. It provides practical recommendations that aid in a deeper understanding of the research and aids in further research in this domain.

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

Introduction

With more incredible technological advancement, the need of the hour is to safeguard the science behind it and restricts its use among limited individuals or organizations. Any cutting-edge technologies that can be found free open access poses a direct or indirect threat to humanity in

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4081 - 4093
Received 25 April 2021; Accepted 08 May 2021.

several ways because technology is neither good nor bad, but it depends on the person intention. Recently, an important case study was presented by a renowned international think tank which explains that the present-day problem that we human worldwide are acutely facing is due to because of unregulated access to previous inventions and, in turn, somewhere failure of humanity.

A cyber-physical systems (CPS) assault may cause nuclear reactors, gas turbines, the electricity grid, transportation networks, and other vital infrastructure to lose control, jeopardising the nation's security, economy, and public safety. Electricity is critical to sustaining and enhancing living standards in India and around the world. The reliability of electricity infrastructures is a vital need among many consumers. Improving the efficiency of energy generation or producing more energy are strategies that can enhance consumption. The smart grid refers to a modern power system that utilizes ICT to offer sustainable, reliable, and efficient energy. The intelligent system enables energy and information to flow in a bidirectional manner in distribution and transmission systems. These systems allow 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 effects 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 reported attacks retrieved from existing literature. The thesis exposes side-channel and traffic analysis attacks while providing risk assessment. The manuscript's primary goal is to ascertain security vulnerabilities to develop possible countermeasures.

Literature Review

The authors have done an intensive literature survey to understand and explore the domain and outline important and notable outcomes. [1] s. Gray (2016) has investigated all possible cybersecurity incidents in the last 5 years and potential threats in power systems defending the grid, which give us a clear understanding. R. V. Yohanandhan et al. In (2020), have formulated a review on modeling, simulation, and analysis with cyber security applications and assess cyber-physical power system[2]. Z. Su et al. (2018) has presented a compensation method-based assessment of cyber contingency for cyber-physical power systems [3]. In (2020), M. Ni et al. Has listed and performed a study over concept and research framework for coordinated situation awareness and active defense of cyber-physical power systems against cyber-attacks [4]. F. Li, x. Yan et al. Has explored and showcase a review of cyber-attack methods in cyber-physical power system in (2019) [5]. G. Liang et al. (2019) has come out with an all-new distributed blockchain-based data protection framework for modern power systems against cyber-attacks, which was first of kind research over ict tools and its influence over grid [6]. In (2018) G. Canbek and S. Sagiroglu have analyzed and examined the intelligent grids' strategic cyber-security perspective

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4081 - 4093
Received 25 April 2021; Accepted 08 May 2021.

[7]. Authors in their previous work have been studied remote health monitoring and fault assessment but suddenly came across that minor work has been recorded over security aspects in hybrid grid [8-10]. This has motivated the authors to shape this work finally.

SystemOverview

At the voltage stability limit, the Jacobian matrix of power flow equations is singular. Ensuring a continuous power flow resolves this problem. Based on a load scenario, the constant power flow provides solutions for load flow. Notably, it comprises the correction and prediction stages. The tangent predictor estimates the following explanation 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 employs 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 crucial moment, 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-the bus system as follows:

$$P_k=\sum_{S=1}^{N}|V_k||V_S||Y_{kS}|cos(\delta_k-\delta_S-\theta_{kS}) \quad \text{.....eq (1)}$$

$$Q_k=\sum_{S=1}^{N}|V_k||V_S||Y_{kS}|sin\,(\delta_k-\delta_S-\theta_{kS}) \quad \text{.....eq (2)}$$

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

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

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

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. This process can analytically determine the generator reactive power output and the reactive and actual 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

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4081 - 4093
Received 25 April 2021; Accepted 08 May 2021.

which has no connected generators. Conversely, a Generator Bus is that which has at least one corresponding generator. One selected arbitrary bus with a generator, called the Stack Bus, was the exception.

There is the basic assumption that at every Load Bus, the reactive power demand and the actual power demand (PD) at every Load Bus (QD) resolve power flow problems. 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 accurate power for every bus. Hence, this equation is as follows:

$$P_k=\sum^{N}|V_k||V_s||Y_{ks}|cos(\delta_k-\delta_s-\theta_{ks})$$

A breakdown of this equation is as follows

P_k-net power injected at bus k,

$|V_s|$–Voltagemagnitude

δ_S- Angle of ith bus

$|Y_{ks}|$ -Magnitudeofthebusadmittance matrix ($YBUS$).

θ_{kS}-angle of YBUS corresponding to the $k$throw and $l$thcolumn

The following is the power balance equation

$$Q_k=\sum_{S=1}^{N}|V_k||V_s||Y_{ks}|sin\ (\delta_k-\delta_s-\theta_{ks})$$

Qk - Net reactive power injected at bus k

$$\text{Vol}\begin{bmatrix}\Delta\theta\\ \Delta|V|\end{bmatrix}=-J^{-1}\begin{bmatrix}\Delta P\\ \Delta Q\end{bmatrix} \quad \text{.....eq (4)}$$

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

$$J=\begin{bmatrix}\frac{\partial P}{\partial\theta} & \frac{\partial P}{\partial|V|}\\ \frac{\partial Q}{\partial\theta} & \frac{\partial Q}{\partial|V|}\end{bmatrix} \quad \text{.....eq(5)}$$

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

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

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4081 - 4093
Received 25 April 2021; Accepted 08 May 2021.

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 asfollows:

Residual size $|f(x)| <\epsilon$; Increment size $|x_{\text{new}} - x_{\text{oSd}}| <\epsilon$; Number of iterations: $ITCount>$

The residual size is a vital choice because, at the solution, the residual is zero. Nonetheless, this is a wrong choice since the residual can be minutes despite iterate being far from the real solution. The increment size is an excellent choice due to the quadratic convergence nature of Newton's model. In this process, the increment excellently approximates the actual 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 solution, including 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 angle values.
- Calculate changes in voltage magnitude and angle
- Provide an update of the voltage angle and magnitude
- Monitor stopping conditions and terminate when met.

PMU Placement

Using topology-based defined algorithms, this research optimised Phasor Measurement Units (PMUs) location for the purpose of power system observability. Under complete network observability, the optimum PMU placement issue is posed to minimise the number of PMUs installed. The following are the observability rules in use:

- The voltage and current phasors of all incident branches of PMU-installed buses are known. Direct measurements are what they're called.
- If you know the voltage and current phasors at one end of a branch, you can get the voltage phasor at the other end of the branch. Pseudo measurements are what they're termed.
- If both ends of a branch's voltage phasors are known, the current phasor of the component may be calculated immediately. Pseudo measures are another name for these kinds of measures.
- In an N-bus system, for zero-injection bus *i*, we have:

$$\sum_{j=1}^{N} Y_{ij} V_j \quad \text{.....eq (6)}$$

Where Yij is the $ijth$ element of the admittance matrix of the system and Vj is the voltage phasor of jth bus. 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

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4081 - 4093
Received 25 April 2021; Accepted 08 May 2021.

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.

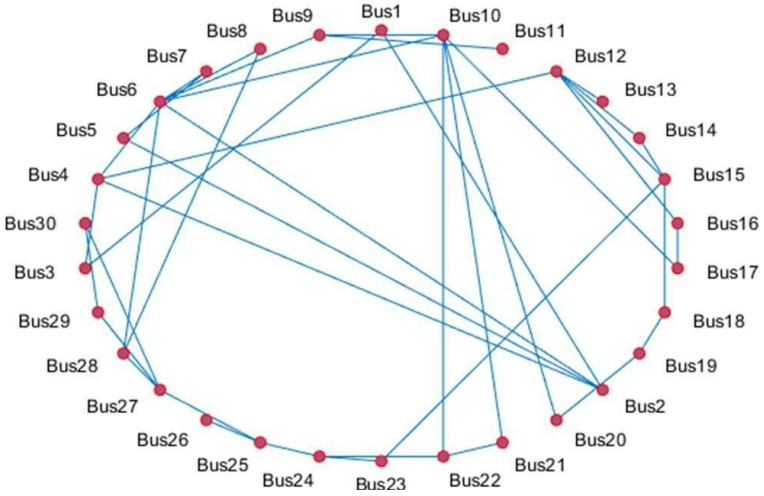

Figure 1. Graph Representation Network [3]

Data Spoofing Attacks

The hacker can inject malicious software into the system, contributing to malicious tendencies in the network. The system can send illegitimate messages to various devices and components in the synchro phasor system in spoofing attacks. 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 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.

False Data Injection Attacks

In the linear model, the attacker deceives the control centre primarily by maintaining the measurement residual while injecting inadequate data into metres. 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 establish 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.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4081 - 4093
Received 25 April 2021; Accepted 08 May 2021.

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

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

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

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

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

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

Voltage-Loading Parameter (V-Λ) Curve

The (V-λ) curve proves helpful 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 required 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 control at this point contributes to the bus voltage deterioration. The uppermost section of the curve reveals proper operations, while the lower side indicates unstable functions. 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.

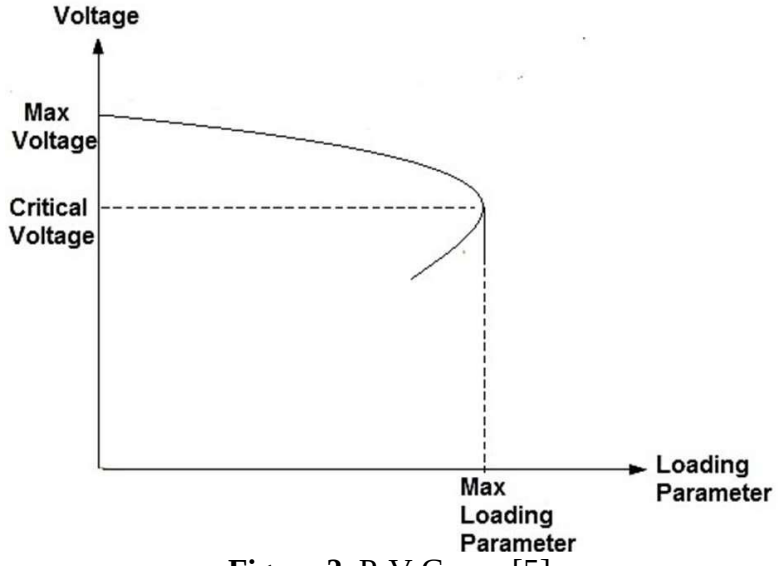

Figure 2. P-V Curve [5]

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4081 - 4093
Received 25 April 2021; Accepted 08 May 2021.

Experimental Results and Observation

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. 2,4,5,6,7,8,9,10,11,12,14,15,16,17,18,19,20,21,24,2 5,26,28,29, 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 in 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 the Power Systems test case archive at IEEE.

1. ***Steady State Case***
   The λ-V curves are obtained with base caseload demand of standard IEEE 30 bus system under steady-state condition for comparison purposes. Figures (3) show the λ-V curves respectively for bus 1 thru bus 30; it has been noticed that the loading parameter for nominated buses is reached 15 p.u. The voltage magnitudes for the same buses lie between them (0.55 to 1.01) p.u.

2. ***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 the power flow calculation algorithm to manipulate the real-time demand, we notice that the loading parameter for nominated buses is dropped compared to the 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.

3. ***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 situated at bus 12, bus 22 and bus 30, respectively. After injecting errors along with the 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 system's stability 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 functions. Voltage collapse is a critical issue in complex power grits. Voltage collapse refers to an occurrence in which the events accompanying instability in voltage contribute to 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.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4081 - 4093
Received 25 April 2021; Accepted 08 May 2021.

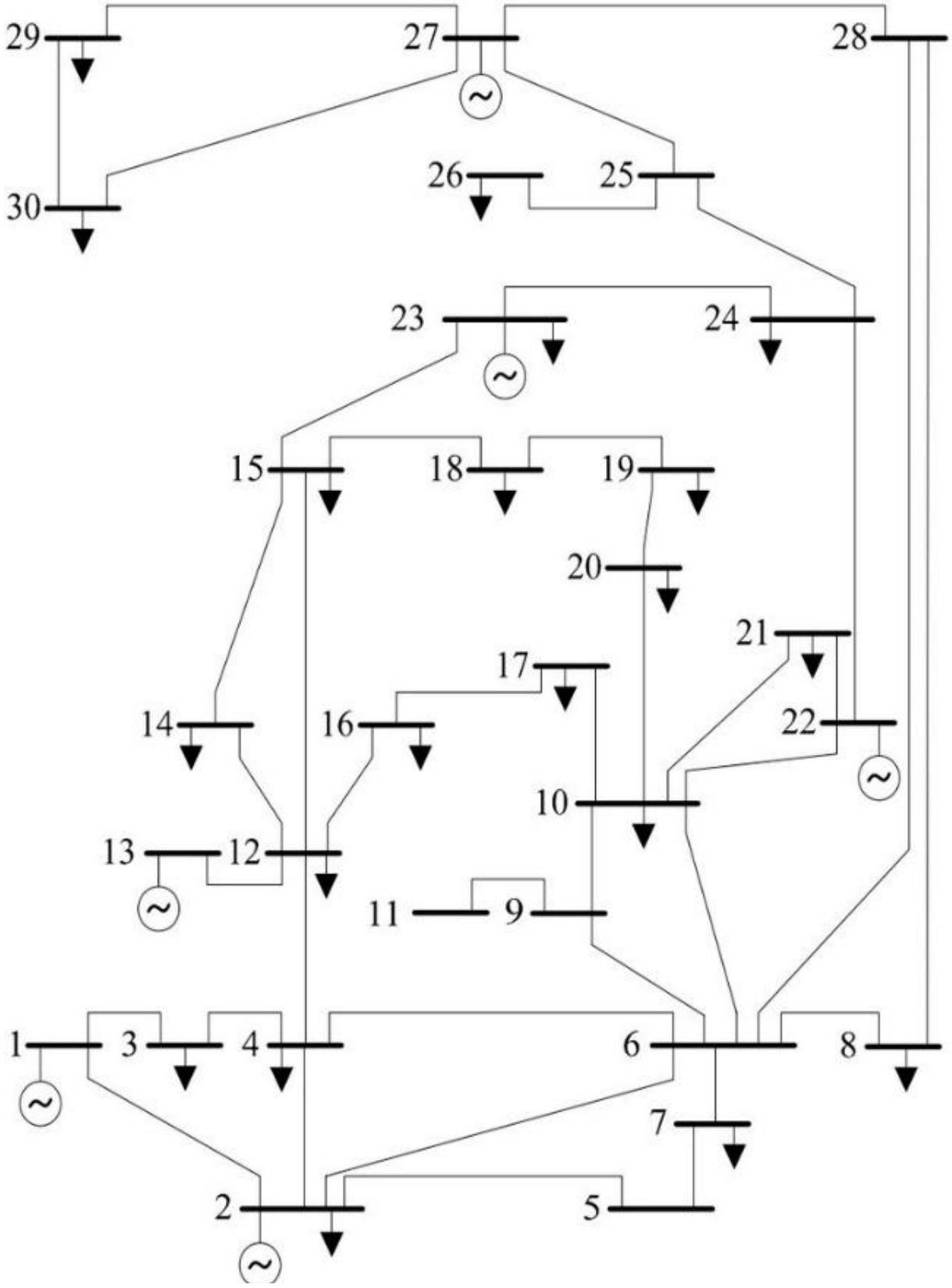

Figure 3.IEEE 30 bus [2]

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4081 - 4093
Received 25 April 2021; Accepted 08 May 2021.

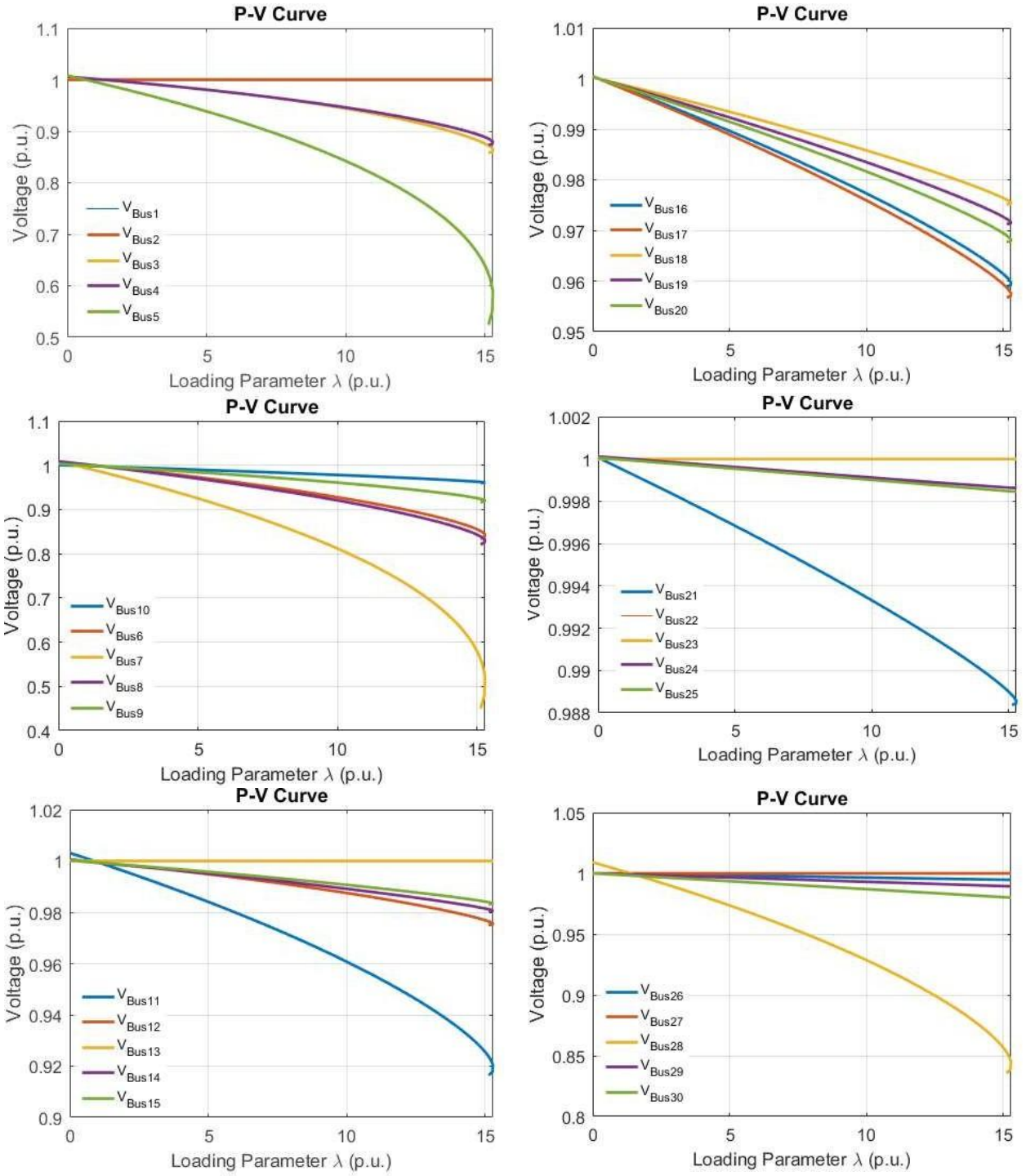

Figure 4. Voltage Profile under Steady-state case

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4081 - 4093
Received 25 April 2021; Accepted 08 May 2021.

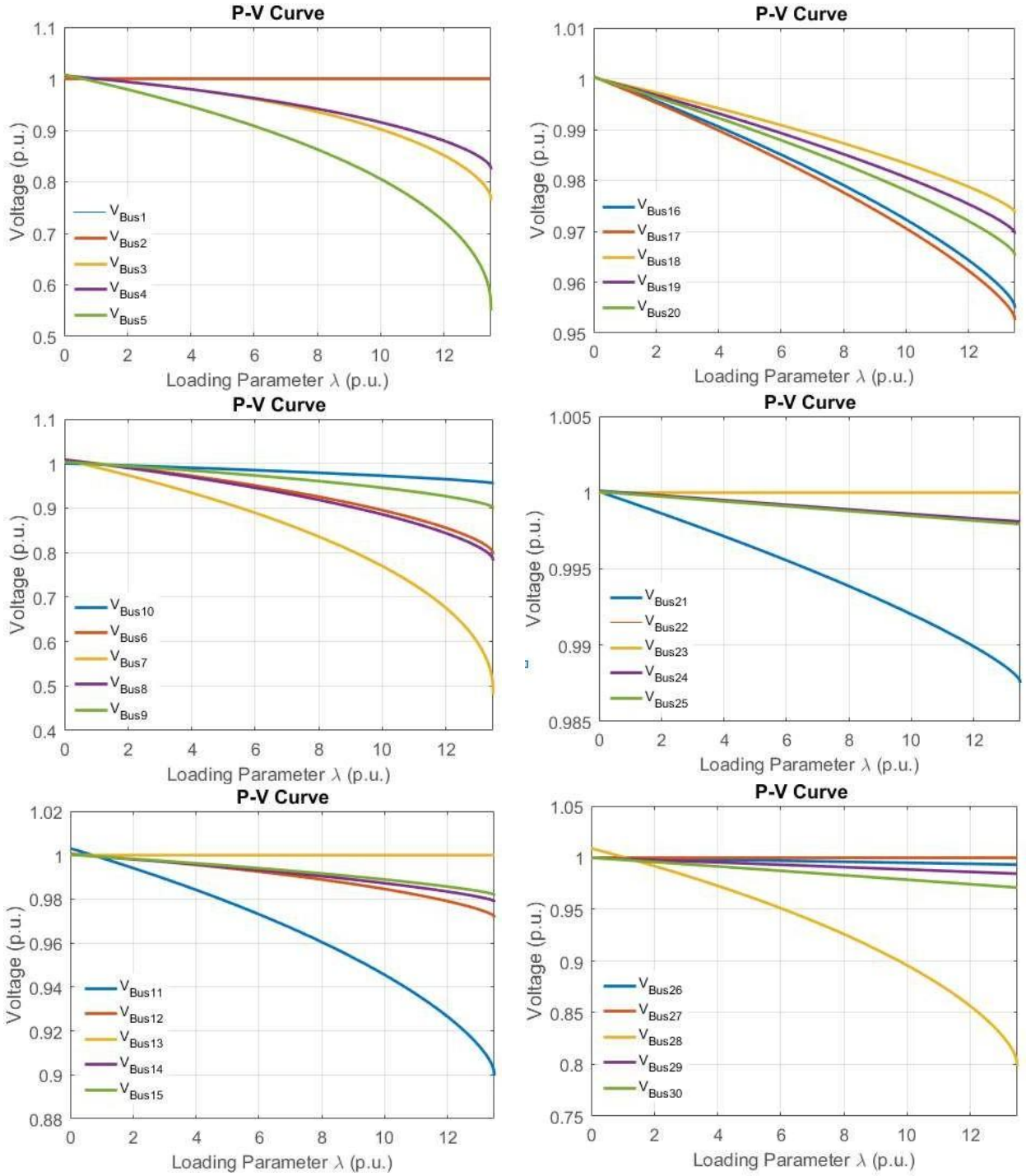

Figure 5. Voltage Profile under Limited attack case

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4081 - 4093
Received 25 April 2021; Accepted 08 May 2021.

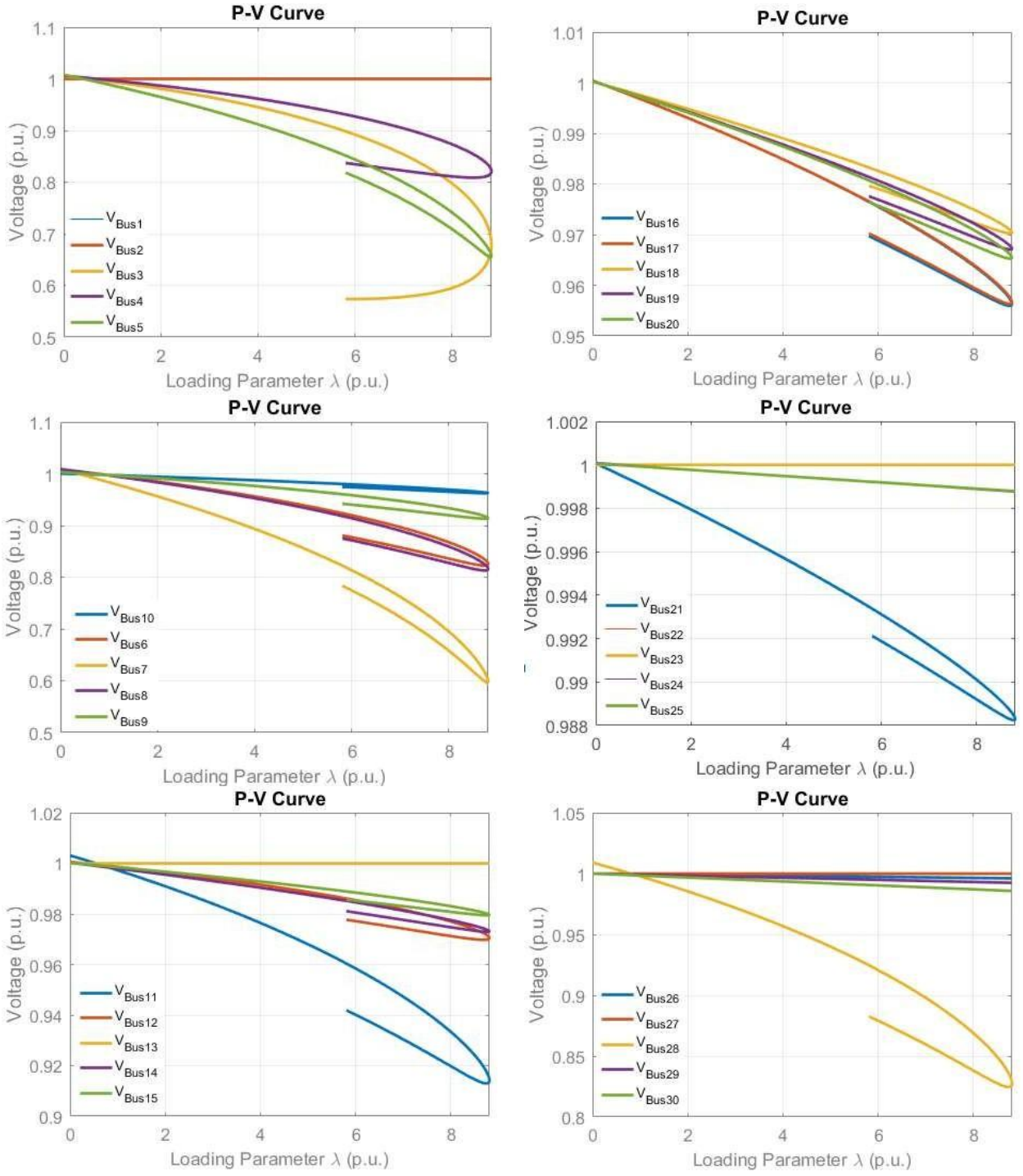

Figure 6. Voltage Profile under Advance attack case

Specific Outcome and Conclusion

The ramifications of this vulnerability were investigated in this research by describing and evaluating a class of attacks known as fake data injection attacks against state estimation in electric power systems. Such attacks may introduce arbitrary faults into particular state variables

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4081 - 4093
Received 25 April 2021; Accepted 08 May 2021.

without being detected by current procedures. The attacker can inject random acceptable mistakes retrieved from previous data by changing metres' readings at physically secured sites. We investigated an attack scenario in which the attacker is restricted to certain PMUs; we demonstrated that in this situation, the attacker might systematically and efficiently design attack vectors that can affect the findings of state estimation and predictably alter them. We further expanded false data injection attacks to generalised false data injection attacks. We utilised both theoretical analysis and simulation to demonstrate that by launching generalised false data injection attacks and doing risk assessments, an attacker may achieve a more significant effect than false data injection assaults.

References

[1] S. Gray, (2016), *"Cyber security in modern power systems defending the grid,"* IET Cyber Security in Modern Power Systems, pp. 1-9, doi: 10.1049/ic.2016.0045.

[2] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa, (2020)*"Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis with Cyber Security Applications,"* in IEEE Access, vol. 8, pp. 151019-151064.

[3] Z. Su et al., (2018)*"A Compensation Method Based Assessment of Cyber Contingency for Cyber-Physical Power Systems,"* 2018 IEEE Power & Energy Society General Meeting (PESGM), 2018, pp. 1-5, doi: 10.1109/PESGM.2018.8586445.

[4] M. Ni, M. Li, J. Li, Y. Wu and Q. Wang, (2020) *"Concept and Research Framework for Coordinated Situation Awareness and Active Defense of Cyber-Physical Power Systems against Cyber-Attacks,"* in Journal of Modern Power Systems and Clean Energy.

[5] F. Li, X. Yan, Y. Xie, Z. Sang and X. Yuan, (2019) *"A Review of Cyber-Attack Methods in Cyber-Physical Power System,"* 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP), pp. 1335-1339.

[6] G. Liang, S. R. Weller, F. Luo, J. Zhao and Z. Y. Dong, (2019) *"Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks,"* in IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 3162-3173.

[7] G. Canbek and S. Sagiroglu, (2018) *"Strategic cyber-security perspective in smart grids,"* 2018 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1-6.

[8] Das T.K., Banik A., Chattopadhyay S., Das A. (2019) Sub-harmonics Based String Fault Assessment in Solar PV Arrays. In: Chattopadhyay S., Roy T., Sengupta S., Berger-Vachon C. (eds) Modelling and Simulation in Science, Technology and Engineering Mathematics. MS-17 2017. Advances in Intelligent Systems and Computing, vol 749. Springer, Cham.

[9] T. K. Das, A. Banik, S. Chattopadhyay and A. Das, (2019), *"FFT based Classification of Solar Photo Voltaic Microgrid System,"* Second International Conference on Advanced Computational and Communication Paradigms (ICACCP), Gangtok, India, pp. 1-5.

[10] A. Banik and A. Sengupta, (2021) *"Scope, Challenges, Opportunities and Future Goal Assessment of Floating Solar Park,"* Innovations in Energy Management and Renewable Resources, Kolkata, India, pp. 1-5, https://doi.org/10.1109/IEMRE52042.2021.9386735