Engineering Research Unit
University of Moratuwa
Sri Lanka

Analysis of Cyber Attacks in Power Grids with Increasing Renewable Energy Penetration

M. A. S. P. Dayarathne
Department of Electrical Engineering
University of Moratuwa
Moratuwa, Sri Lanka
sasikadayarathna708@gmail.com

M. S. M. Jayathilaka
Department of Electrical Engineering
University of Moratuwa
Moratuwa, Sri Lanka
seranij15@gmail.com

R. M. V. A. Bandara
Department of Electrical Engineering
University of Moratuwa
Moratuwa, Sri Lanka
venuraavishka1@gmail.com

Keywords — cyber- attacks, Power system, cyber security, PSCAD

I. Introduction

With the application of advanced computer and communication technologies, traditional power systems are converting to cyber-physical power systems. [1] Several secondary systems, like SCADA (Supervisory Control and Data Acquisition), WAMS (Wide Area Monitoring System), AMI (Advanced Metering Infrastructure), and smart substations, are the main cyber-physical subsystems that could be vulnerable to cyber-attacks. [1], [3] Mathematically modeled cyber-attack types such as FDIA (False Data Injection Attack) [1], [2], [3], [4], DoS (Denial of Service) [1], [3], replay attacks, etc. can be modeled using the PSCAD power system model with the addition of renewable power source models to the system. The goal of this project is to develop a PSCAD power system model with increasing renewable power sources, simulate the different kinds of cyber-attacks mentioned above in the PSCAD power system model, collect faulty data, and develop a deep learning model to detect and act against the cyber-attacks.

II. Literature Review

To overcome the lack of labeled data and address the class imbalance, Generative Adversarial Networks (GANs) have emerged as a contemporary approach. GANs enable the reproduction of synthetic samples that maintain the distribution of original samples.[5] The scenarios include short-circuit faults, line maintenance, and various cyber-attacks like RTCI, RSC, and DI attacks. Each scenario represents a specific challenge in power grid security.[6],[7] Detailed analysis of cyber-attacks involving photovoltaic (PV) systems, such as extra reactive power compensation, PV farm inverter attacks, and linear load cutoff. These attacks simulate scenarios, where false data injection and data integrity attacks compromise power system stability.[6] Research gaps can be identified as follows.

- Only focusing on one type of attack
- Real scenarios are not simulated.
- Renewable energy penetration - less considered.

III. Materials and Methods

The study utilized software such as PSCAD and MATLAB Simulink are used to design a power system model with renewable energy sources, generate healthy data for seven transmission lines, simulate fault data injection and load alternating attack types, and collect data through simulations.

Fault data injection attack is simulated using the below model. [Fig.1] This model can generate random values for voltage, frequency, and phase angle and through the solar plant phasor measurement units these data were injected to the system communication network. Due to these types of fault data, some of diesel generators change their characteristics. Due to those changes, system instabilities occurred and by measuring wave patterns in transmission lines, fault types can be identified.

Load Alternating attack [Fig.2] model can cut off the loads in system by accessing through the solar system communication channel. The attack is directly done to breaker relay system and breakers can be controlled using the model.

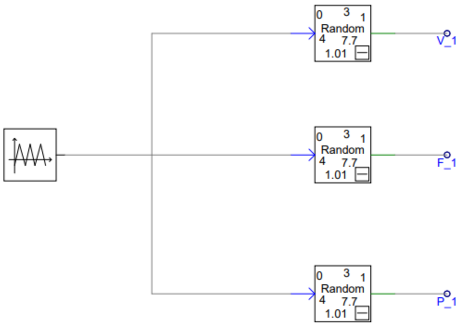

Fig. 1. Fault data injection model

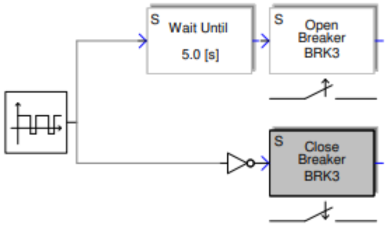

Fig. 2. Load alternating attack model

ERU Symposium 2023 - DOI 10.31705/ERU.2023.13

IV. Results and Discussion

Data was collected for healthy power system wave patterns, Fault data injection attacked system wave patterns and Load alternating attacked system wave patterns for the Instantaneous current, Instantaneous voltage, RMS voltage, Active Power, Reactive Power, and Phase angle.

A. *Healthy data wave patterns*

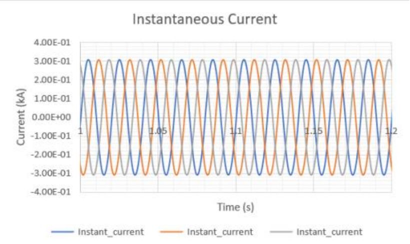

Fig. 3. Healthy data wave pattern for instantaneous current

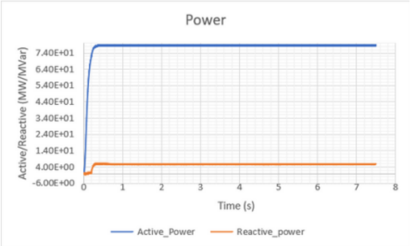

Fig. 4. Healthy data wave pattern for active and reactive power

B. *Fault data injection attack wave patterns*

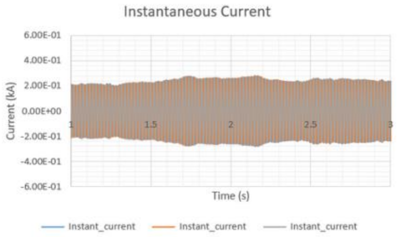

Fig. 5. Fault data injection attack wave pattern for instantaneous current

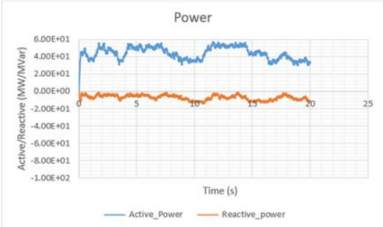

Fig. 6. Fault data injection attack wave pattern for active and reactive power

C. *Load alternating attack wave patterns*

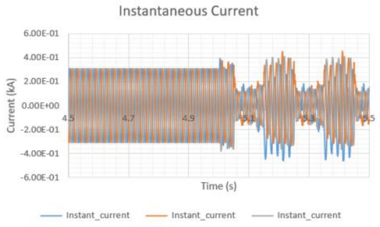

Fig. 7. Figure 1: Load alternating attack wave pattern for instantaneous current

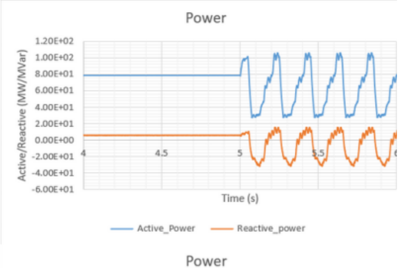

Fig. 8. Load alternating attack wave pattern for active and reactive power

V. Conclusion

Due to rapid development of cyber – physical power systems, attack detection and defense is becoming more complex day by day. Using the data collected from the power system model with and without attacks, our aim is to build a deep learning based neural network model to identify the attack type.

Future works to achieve the objectives:

- Analyze the attack patterns with common faults and improve the data set.
- Analyze the data set and feature extraction for neural network model.
- Develop the neural network model and optimize the model.

References

[1] F. Li, X. Yan, Y. Xie, Z. Sang and X. Yuan, "A Review of Cyber-Attack Methods in Cyber-Physical Power System," 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP), Xi'an, China, 2019, pp. 1335-1339, doi: 10.1109/APAP47170.2019.9225126. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] F. Almutairy, L. Scekic, R. Elmoudi and S. Wshah, "Accurate Detection of False Data Injection Attacks in Renewable Power Systems Using Deep Learning," in IEEE Access, vol. 9, pp. 135774-135789, 2021, doi:10.1109/ACCESS.2021.3117230. K. Elissa, "Title of paper if known," unpublished.

[3] D. Du et al., "A Review on Cybersecurity Analysis, Attack Detection, and Attack Defense Methods in Cyber-physical Power Systems," in Journal of Modern Power Systems and Clean Energy, vol. 11, no. 3, pp. 727-743, May 2023, doi:10.35833/MPCE.2021.000604.

[4] R. Punmiya and S. Choe, "Energy Theft Detection Using Gradient Boosting Theft Detector with Feature Engineering-Based Preprocessing," in IEEE Transactions on Smart Grid, vol. 10, no. 2, pp. 2326-2329, March 2019, doi: 10.1109/TSG.2019.2892595.

[5] M. Farajzadeh-Zanjani, E. Hallaji, R. Razavi-Far, M. Saif and M. Parvania, "Adversarial Semi-Supervised Learning for Diagnosing Faults and Attacks in Power Grids," in IEEE Transactions on Smart Grid, vol. 12, no. 4, pp. 3468-3478, July 2021, doi: 10.1109/TSG.2021.3061395.

[6] F. Li et al., "Detection and Identification of Cyber and Physical Attacks on Distribution Power Grids with PVs: An Online High-Dimensional Data-Driven Approach," in IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 10, no. 1, pp. 1282-1291, Feb. 2022, doi: 10.1109/JESTPE.2019.2943449.

[7] S. Liu, X. Feng, D. Kundur, T. Zourntos and K. L. Butler-Purry, "Switched system models for coordinated cyber-physical attack construction and simulation," 2011 IEEE First International Workshop on Smart Grid Modeling and Simulation (SGMS), Brussels, Belgium, 2011, pp. 49-54, doi: 10.1109/SGMS.2011.6089026.