Real-Time Anomaly-Driven Cyber Resilience: An Adaptive Machine Learning-Based Defense Against False Data Injection Attacks in Smart Grids

Chibozu Maambo
School of Computing, Technology and Applied Sciences
ZCAS University
Lusaka, Zambia
chibozu.maambo@gmail.com

Aaron Zimba
School of Computing, Technology and Applied Sciences
ZCAS University
Lusaka, Zambia
aaron.zimba@zcasu.edu.zm

Abstract - This work proposes a machine learning-driven adaptive framework for real-time detection and mitigation of FDIAs in critical smart grid infrastructure. The adaptive nature of the model addresses evolving False Data Injection Attacks and provides a more secure and viable method of securing critical smart grid infrastructure from the injection of false data attacks. The fast digital transformation of smart grid infrastructure has created cybersecurity vulnerabilities. Conventional detection models are challenged, and the requirement of a complex solution is required to handle evolving attacks on critical smart grid infrastructure. The technical contributions of this research include continuous update of the model based on the evolving attacks. The model can adapt without retraining from scratch. This model is therefore applicable in future implementations of smart grids, where such models can be adopted by countries who wish to implement smart cities and utility companies in developing countries.

Keywords - Machine learning, adaptive model, real-time detection, real time mitigation, false data injection attacks, critical smart grid infrastructure

I. INTRODUCTION

A. Background

Smart grids have evolved from traditional power systems into smart grids. This has largely introduced bi-directional communication, automated control and real time monitoring as advanced functionalities of smart grids. Reliability and sustainability are enhanced leading to improved efficiency. Vulnerability to malicious attacks in smart grids is due to the dependence of Information Technology. [2] Integration of cyber security components exposes the grid to various cybersecurity threats but notably False Data Injection Attacks (FDIAs).

The usage of smart grids due to Information Communication Technology dependencies has also increased the level of cyber security importance[10]. Real-time monitoring is unavoidable given the fast acceptance of renewable energy sources inside the traditional power infrastructure[11].

B. Problem Statement

Attacks targeted at critical infrastructure of the smart grid are on the increase, raising numerous inadequacies [9]. Despite smart grids enhancing efficiency in operations, they have also presented a risk due to the cyber-attacks that lie in wait. This has significantly made the grid vulnerable to FDIAs which are the most common threats to critical infrastructure of smart grids. The existing implementations are static and rely on labelled data making them non adaptive to various FDIAs. There is need to develop a machine learning driven adaptive model that addresses and responds to the detection and mitigation of FDIAs on smart grid critical infrastructure.

C. Research Aim and Objectives

The aim of the research is to develop a real-time anomaly-driven cyber resilience adaptive machine learning-based defense against false data injection attacks in smart grids. The specific objectives include:

 ISBN: 978-9982-95-500-3

- Develop a real time anomaly driven cyber resilience adaptive machine learning based defense for the detection and mitigation of FDIAs.
- Assess the FDIAs of critical smart grid infrastructure in real time.
- Evaluate the performance of the real time anomaly driven cyber resilience adaptive machine learning based defense for the detection and mitigation of FDIAs
- Assess the adaptability of the real time anomaly driven cyber resilience adaptive machine learning based defense for the detection and mitigation of FDIAs in varied smart grid conditions.

II. Literature Review

A. Search Inclusion Criteria

The literature considered under this review complied with the PRISMA guidelines for systematic reviews. Databases used in the review included IEEE Xplore, ScienceDirect, SpringerLink. The focus was only on peer-reviewed papers that were published between 2016 and 2024 were considered. Real time detection, real time mitigation and machine learning adaptive model were some of the keywords considered when filtering results. The review produced 54 relevant articles after the extensive scrutiny of the articles.

B. Search Exclusion Criteria

Papers that did not contain the availability of full text and papers that were not written in English could not be included in the search. Additionally, editorials, keynote writeups, and book chapters were not included in the search for the literature. The Nature of Smart Grids A smart grid is a complex intelligent network of electrical lines and equipment connecting buses, nodes, generators, control center, etc. [13]. While most existing techniques for protecting power grid systems were designed to ensure system reliability (i.e., against random failures), recently there have been growing concerns in smart grid initiatives on the protection against malicious cyber-attacks. The smart grid, as a cyber-physical critical infrastructure, boasts higher reliability, efficiency, and consumer-centricity in an environment of increasing power demand. Acquisition, transmission, and consumption of high-granularity real-time power system data are facilitated through the integration of communications, computing, and advanced control technologies [2].

C. Attacks on the Smart Grid

Since smart grids depend on a complex cyberspace of computers, software, and communication technologies and components are connected to an open network, this makes them vulnerable and a target to attacks. An attack from the adversary can compromise meters and inject data. False data-injection attacks can affect key functional modules in the smart grid such as energy price and energy distribution.

False data injection attacks (FDIAs) have lately been found as a major type of cyber-attacks aiming at state estimation and monitoring systems of smart grids. These cyberattacks compromise the readings of several smart grid meters in order to mislead control system operations.

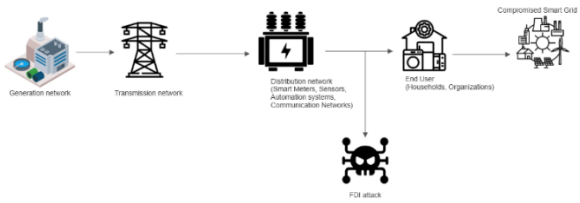

Figure 1: An Attack on The Smart Grid

D. Detection Methods Used in Smart Grid Attacks

Various research has been developed on proposing various FDI attack scenarios and developing the corresponding detection strategies. Kim et al. formulated the least effort attack strategy and proposed a protection-based defense scheme and a detection-based defense scheme [26]. Hossain et al. modelled the attack strategy using the Gaussian process and used machine learning methods for attack detection [27]. Unsal et al. developed an FDI detection mechanism by using the properties of the low dimensionality of measurements and sparsity of attacks. The equivalent measurement transformation and the largest weighted residual method were integrated for detecting the FDI attacks [28].

[40] Xiangyu et al conducted research related to the dynamic detection of false data injection attacks in the smart grid using deep learning. In this research work, the researchers proposed an approach deep learning-based framework to detect injected data measurement. This also included a time series anomaly detector that uses a convolutional neural

 ISBN: 978-9982-95-500-3

network (CNN) and a long short-term memory (LSTM) network.

[14] Yang Li et al in their study stated that traditional methods using centralized detection methods are unable to cope with the growth of the volume of data in a smart grid since these grids are becoming larger and generating more data.

Hence, studies have mainly bordered on static FDI attack detection with an assumption that attackers have a certain level of knowledge concerning the topology of the power system and can only inject a limited number of bad data points [41].

III. METHODOLOGY

A. Research Design

The research design in this work included identifying the problem, determining the objectives, assessing and evaluating the models in use.

IV. DISCUSSION

Assessing the models in use required a critical analysis of performance and constraints to check whether the models satisfied the specified objectives. This procedure ascertained whether the models could consistently solve the problem at hand in the research work.

Evaluation of the models in use was based on acceptable performance metrics. This guaranteed that the models could be tested for realistic uses and that the models generated could be enhanced as and when required.

V. CONCLUSION

This study reviewed models in use for the detection and mitigation of real time anomaly driven cyber resilience.

By combing through the literature review, the study proposes a *real time anomaly driven cyber resilience adaptive* machine learning *based defense* for *the* detection and mitigation of FDIAs.

VI. RECOMMENDATIONS

It is important for False Data Injection Attacks to be constantly monitored on the smart grid through use of a *real-time anomaly driven cyber resilience adaptive* machine learning *based defense* so that the attacks are not only detected but mitigated in real time.

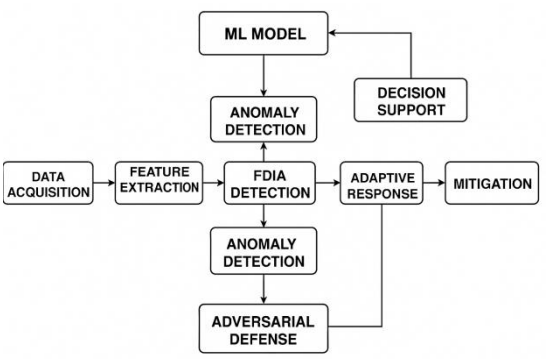

Fig 2: Technical Operations of Proposed Detection Model in a Smart Grid

References

[1] L. Xie, Y. Mo, and B. Sinopoli, 'Integrity data attacks in power market operations', IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 659–666, 2011, doi: 10.1109/TSG.2011.2161892.

[2] Y. He, G. J. Mendis, and J. Wei, 'Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism', IEEE Trans. Smart Grid, vol. 8, no. 5, pp. 2505–2516, 2017, doi: 10.1109/TSG.2017.2703842.

[3] R. K. Jha, 'Strengthening Smart Grid Cybersecurity: An In-Depth Investigation into the Fusion of Machine Learning and Natural Language Processing', no. August, 2023, doi: 10.36548/jtcsst.2023.3.005.

[4] J. Zheng et al., 'Detection to false data for smart grid', Cybersecurity, vol. 8, no. 1, 2025, doi: 10.1186/s42400-024-00326-5.

[5] T. Mazhar et al., 'Analysis of Challenges and Solutions of IoT in Smart Grids Using AI and Machine Learning Techniques : A Review', 2023.

[6] B. Paul et al., 'Heliyon Potential smart grid vulnerabilities to cyber attacks : Current threats and existing mitigation strategies', Heliyon, vol. 10, no. 19, p. e37980, 2024, doi: 10.1016/j.heliyon.2024.e37980.

 ISBN: 978-9982-95-500-3

[7] K. Alam, U. Mahmud, and A. Al Fathah, 'Cyber Attacks Detection And Mitigation Using Machine Learning In Smart Grid Systems CYBER ATTACK DETECTION AND MITIGATION USING MACHINE LEARNING IN', no. November, 2024, doi: 10.70008/jeser.v1i01.43.

[8] A. Alsirhani, N. Tariq, M. Humayun, G. Naif, and A. Hassan, 'Intrusion detection in smart grids using artificial intelligence-based ensemble modelling', Cluster Comput., vol. 9, 2025, doi: 10.1007/s10586-024-04964-9.

[9] H. T. Reda, A. Anwar, and A. Mahmood, 'Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts', Renew. Sustain. Energy Rev., vol. 163, pp. 1–24, 2022, doi: 10.1016/j.rser.2022.112423.

[10] F. Aloul, A. R. Al-ali, R. Al-dalky, and M. Al-mardini, 'Smart Grid Security : Threats , Vulnerabilities and Solutions', no. 971, 2012.

[11] D. Mukherjee, S. Chakraborty, A. Y. Abdelaziz, and A. El-Shahat, 'Deep learning-based identification of false data injection attacks on modern smart grids', Energy Reports, vol. 8, pp. 919–930, 2022, doi: 10.1016/j.egyr.2022.10.270.

[12] N. Sahani, R. Zhu, J. Cho, C. Liu, and V. Tech, 'Machine Learning-based Intrusion Detection for Smart Grid Computing : A Survey', vol. 7, no. 2, 2023, doi: 10.1145/3578366.

[13] M. Rashed, J. Kamruzzaman, I. Gondal, and S. Islam, 'False Data Detection in a Clustered Smart Grid Using Unscented Kalman Filter', IEEE Access, vol. 10, no. July, pp. 78548–78556, 2022, doi: 10.1109/ACCESS.2022.3193781.

[14] Y. Li, X. Wei, Y. Li, Z. Dong, and M. Shahidehpour, 'Detection of False Data Injection Attacks in Smart Grid: A Secure Federated Deep Learning Approach', IEEE Trans. Smart Grid, vol. 13, no. 6, pp. 4862–4872, 2022, doi: 10.1109/TSG.2022.3204796.

[15] 'False Data Injection Attacks in Smart Grid : Challenges and Solutions Research Projects'.

[16] C. Pei, Y. Xiao, W. Liang, and X. Han, 'A Deviation-Based Detection Method against False Data Injection Attacks in Smart Grid', IEEE Access, vol. 9, pp. 15499–15509, 2021, doi: 10.1109/ACCESS.2021.3051155.

[17] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, 'Achieving efficient detection against false data injection attacks in smart grid', IEEE Access, vol. 5, pp. 13787–13798, 2017, doi: 10.1109/ACCESS.2017.2728681.

[18] M. Dehghani, T. Niknam, M. Ghiasi, P. Siano, H. H. Alhelou, and A. Al-Hinai, 'Fourier singular values-based false data injection attack detection in AC smart-grids', Appl. Sci., vol. 11, no. 12, 2021, doi: 10.3390/app11125706.

[19] U. Inayat, M. F. Zia, S. Mahmood, T. Berghout, and M. Benbouzid, 'Cybersecurity Enhancement of Smart Grid: Attacks, Methods, and Prospects', Electron., vol. 11, no. 23, pp. 1–16, 2022, doi: 10.3390/electronics11233854.

[20] S. Grid, 'Real-Time Locational Detection of Stealthy False Data Injection Classification Approach', 2022.

[21] X. Lin, D. An, F. Cui, and F. Zhang, 'False data injection attack in smart grid: Attack model and reinforcement learning-based detection method', Front. Energy Res., vol. 10, no. January, pp. 1–14, 2023, doi: 10.3389/fenrg.2022.1104989.

[22] Y. Wu, Q. Wang, N. Guo, Y. Tian, F. Li, and X. Su, 'Efficient Multi-Source Self-Attention Data Fusion for FDIA Detection in Smart Grid', Symmetry (Basel)., vol. 15, no. 5, pp. 1–17, 2023, doi: 10.3390/sym15051019.

[23] H. Haider, A. Z. Ali, and A. Z. Ali, 'False Data Injection Attacks (FDIA) detection by Deep Learning Techniques in Smart Grids : survey'.

[24] J. Abudin, S. Thokchom, and R. T. Naayagi, 'applied sciences Learning-Based Approaches for Smart Grid Networks', 2024.

[25] C. Dou, D. Wu, D. Yue, B. Jin, and S. Xu, 'A Hybrid Method for False Data Injection Attack Detection in Smart Grid Based on Variational Mode Decomposition and OS-ELM', CSEE J. Power Energy Syst., vol. 8, no. 6, pp. 1697–1707, 2022, doi: 10.17775/CSEEJPES.2019.00670.

[26] J. Kim and L. Tong, 'On topology attack of a smart grid: Undetectable attacks and countermeasures', IEEE J. Sel. Areas Commun., vol. 31, no. 7, pp. 1294–1305, 2013, doi: 10.1109/JSAC.2013.130712.

[27] E. Hossain, I. Khan, F. Un-noor, S. S. Sikander, and S. H. Sunny, 'Application of Big Data and Machine Learning in Smart Grid , and Associated Security Concerns : A Review', IEEE Access, vol. 7, pp. 13960–13988, 2019, doi: 10.1109/ACCESS.2019.2894819.

[28] D. B. Unsal, T. S. Ustun, S. M. Suhail Hussain, and A. Onen, 'Enhancing cybersecurity in smart grids: False data injection and its mitigation', Energies, vol. 14, no. 9, pp. 1–36, 2021, doi: 10.3390/en14092657.

[29] A. Zibaeirad, F. Koleini, T. Wang, S. Bi, and T. Hou, 'A Comprehensive Survey on the Security of Smart Grid : Challenges , Mitigations, and Future', pp. 1–30, 2017.

[30] Z. A. Baig and A. R. Amoudi, 'An analysis of smart grid attacks and countermeasures', J. Commun., vol. 8, no. 8, pp. 473–479, 2013, doi: 10.12720/jcm.8.8.473-479.

[31] T. Mazhar et al., 'Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods', 2023.

[32] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, 'Detecting false data injection attacks on power grid by sparse optimization', IEEE Trans. Smart Grid, vol. 5, no. 2, pp. 612–621, 2014, doi: 10.1109/TSG.2013.2284438.

[33] A. O. Ajayi, B. K. Alese, S. E. Fadugba, and K. Owoeye, 'Sensing the Nation: Smart Grid ' s Risks and', no. May, pp. 151–163, 2014.

[34] A. M. Ruzbahani, 'Enhancing Smart Grids with Internet of Energy: Deep Reinforcement Learning and Convolutional Neural Network', pp. 1–8.

[35] G. Zhang, W. Gao, J. Zhu, and Y. Li, 'Detection of false data injection attacks in smart grid based on adaptive inhibition unscented Kalman filter', J. Phys. Conf. Ser., vol. 2788, no. 1, pp. 1–20, 2024, doi: 10.1088/1742-6596/2788/1/012029.

[36] S. H. Mohammed et al., 'A Review on the Evaluation of Feature Selection Using Machine Learning for Cyber-Attack Detection in Smart Grid', vol. 12, no. February, pp. 44023–44042, 2024, doi: 10.1109/ACCESS.2024.3370911.

[37] M. Irfan, A. Sadighian, A. Tanveer, S. J. Al-Naimi, and G. Oligeri, 'A survey on detection and localisation of false data injection attacks in smart grids', IET Cyber-Physical Syst. Theory Appl., no. June 2023, pp. 313–333, 2024, doi: 10.1049/cps2.12093.

8975/2015.07.005.

[42] A. Algarni, 'An Edge Computing-Based and Threat Behavior-Aware Smart Prioritization Framework for Cybersecurity Intrusion Detection and Prevention of IEDs in Smart Grids with Integration of Modified LGBM and One Class- SVM Models', IEEE Access, vol. 12, no. July, pp. 104948–104963, 2024, doi: 10.1109/ACCESS.2024.3435564.

[45] Z. Elmrabet, H. Elghazi, N. Kaabouch, and H. Elghazi, 'Cyber-Security in Smart Grid : Survey and Challenges', pp. 1–13, 2004.

[46] A. Shees, M. Tariq, and A. I. Sarwat, 'Cybersecurity in Smart Grids: Detecting False Data Injection Attacks Utilizing Supervised Machine Learning Techniques', Energies, vol. 17, no. 23, 2024, doi: 10.3390/en17235870.

[47] G. Zhang and B. Sikdar, 'A Novel Adversarial FDI Attack and Defense Mechanism for Smart Grid Demand-Response Mechanisms', IEEE Trans. Ind. Cyber-Physical Syst., vol. 2, pp. 380–390, 2024, doi: 10.1109/ticps.2024.3448380.

[48] G. Rajendran, H. V. Sathyabalu, M. Sachi, and V. Devarajan, 'Cyber Security in Smart Grid: Challenges and Solutions', Proc. 2019 2nd Int. Conf. Power Embed. Drive Control. ICPEDC 2019, vol. 5, no. November 2020, pp. 546–551, 2019, doi: 10.1109/ICPEDC47771.2019.9036484.

[38] H. Karimipour, A. L. I. Dehghantanha, and S. Member, 'A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids', IEEE Access, vol. 7, pp. 80778–80788, 2019, doi: 10.1109/ACCESS.2019.2920326.

[39] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J. P. Hubaux, Game theory meets network security and privacy, vol. 45, no. 3. 2013. doi: 10.1145/2480741.2480742.

[40] X. Niu, J. Li, J. Sun, and K. Tomsovic, 'Dynamic Detection of False Data Injection Attack in Smart Grid using Deep Learning', 2019 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. ISGT 2019, 2019, doi: 10.1109/ISGT.2019.8791598.

[41] A. Sargolzaei and H. Santana, 'Smart Grid Cyber Security : An Overview of Threats and Countermeasures', no. July 2015, 2016, doi: 10.17265/1934-

[43] F. Mohammadi, 'Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review', 2021.

[44] T. Yu et al., 'An Advanced Accurate Intrusion Detection System for Smart Grid Cybersecurity Based on Evolving Machine Learning', vol. 10, no. May, pp. 1–13, 2022, doi: 10.3389/fenrg.2022.903370.

[49] M. Irfan, A. Sadighian, A. Tanveer, S. J. Al-Naimi, and G. Oligeri, 'False Data Injection Attacks in Smart Grids: State of the Art and Way Forward', pp. 1–15, 2023.

[50] F. Wen and W. Liu, 'An Efficient Data-Driven False Data Injection Attack in Smart Grids', Int. Conf. Digit. Signal Process. DSP, vol. 2018-Novem, 2018, doi: 10.1109/ICDSP.2018.8631857.

[51] M. K. Reiter, 'False Data Injection Attacks against State Estimation in', pp. 21–32, 2009.

[52] H. Y. Tran, J. Hu, X. Yin, and H. R. Pota, 'An Efficient Privacy-Enhancing Cross-Silo Federated Learning and Applications for False Data Injection Attack Detection in Smart Grids', IEEE Trans. Inf. Forensics Secur., vol. 18, pp. 2538–2552, 2023, doi: 10.1109/TIFS.2023.3267892.