International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

ENHANCING POWER SYSTEM SECURITY THROUGH RESILIENT FREQUENCY REGULATION IN THE FACE OF HYBRID CYBER-ATTACKS

Aswin K[1], Devadharsan S[2], Guganathan M[2], Hariharan A[2], Kalaiyarasan K[2]
[1]*Department of CSE, Assistant Professor, Dhanalakshmi Srinivasan Engineering College (Autonomous), Perambalur*
[2]*Department of CSE, UG Student, Dhanalakshmi Srinivasan Engineering College (Autonomous), Perambalur*

Abstract: The growing reliance on modern communication technologies in power systems for Frequency Regulation (FR) introduces vulnerabilities to cyberattacks, posing significant threats to system stability and reliability. These attacks can disrupt the coordination among various components, such as sensors, control centers, and actuators, thereby compromising the integrity of FR analysis. In response, this article proposes a resilient solution in the form of a deep-learning-based Attack Detection and Mitigation system. By integrating advanced AI techniques, this system aims to fortify the security of FR operations within the cyber-physical framework, swiftly identifying and neutralizing cyber threats. Ultimately, this approach ensures the continuous and reliable operation of power systems, mitigating the risks posed by hybrid cyberattacks and safeguarding critical infrastructure. The proposed system represents a proactive approach to mitigating the escalating risks associated with cyberattacks targeting FR in power systems. Through its deep-learning algorithms, the system can dynamically adapt to emerging threats, enhancing the resilience of FR analysis against malicious intrusions. By bolstering security measures within the cyber-physical model, the system minimizes the potential impact of cyberattacks on power system stability and reliability. Moreover, its ability to detect and mitigate threats in real-time ensures uninterrupted operation, thereby safeguarding the functionality of power systems even amidst the evolving landscape of hybrid cyber threats. This resilient solution represents a crucial step towards fortifying power system security and maintaining essential services in the face of adversarial cyber activities.

Keywords: Attack detection and mitigation (ADM) system, Frequency Regulation(FR), hybrid power system, Renewable Energy Sources (RESs), resiliency.

1. INTRODUCTION

In the rapidly evolving landscape of modern power systems, the integration of advanced communication technologies has revolutionized the way Frequency Regulation (FR) is managed. However, with this progress comes an inherent vulnerability to cyber threats. These threats, ranging from malicious manipulation of signals to coordinated cyber attacks, pose a significant risk to the coordinated functioning of hybrid power system components. Such disruptions not only compromise the stability of the power grid but also threaten the reliability of essential services that rely on uninterrupted electricity supply. To address these critical challenges, this article proposes a cutting-edge solution: a deep-learning-based Attack Detection and Mitigation (ADM) system. By embedding resilient capabilities directly into the FR analysis within the cyber-physical model, this innovative mechanism aims to fortify the security of power systems against evolving cyber threats. Through the utilization of advanced AI techniques, including the powerful XGBOOST algorithm, the ADM system stands poised to detect and neutralize cyber threats in real-time, ensuring the continued and dependable operation of power systems in the face of dynamic and complex cyber risks

Proposed Methodology:

The proposed system represents a significant advancement in the realm of power system security, focusing specifically on bolstering the resilience of Frequency Regulation (FR) through the integration of deep-learning-based XGboost algorithm and Attack Detection and Mitigation (ADM) mechanisms. By honing in on the communication infrastructure linking sensors, control centers, and actuators within the hybrid power system, this system aims to proactively detect and counteract cyber threats that could compromise FR operations.

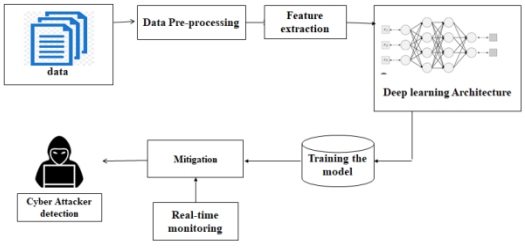

Fig -1: Architecture Diagram

Through the utilization of advanced deep-learning algorithms, the ADM system continuously analyses communication signals, swiftly identifying any aberrations indicative of potential cyberattacks such as

signal jamming, alteration, or delay. This proactive monitoring enables the system to initiate timely mitigation strategies, preserving the integrity of FR analysis and thereby ensuring the sustained stability and reliability of the power system even amidst the threat of hybrid cyber-attacks. In essence, the proposed system serves as a robust defense mechanism against the evolving landscape of cyber threats targeting power systems. By leveraging the capabilities of the XGboost algorithm and advanced deep-learning techniques, it offers a comprehensive approach to fortifying the security posture of power systems. Through its ability to promptly detect and mitigate cyber threats within the communication infrastructure, the system minimizes the potential impact of malicious interference on FR operations. Ultimately, by adopting a proactive stance towards cybersecurity, the proposed system aims to enhance the overall resilience of power systems, safeguarding against disruptions and ensuring the continuous delivery of reliable electricity to consumers.

Data Collection Module:

Data collection involves gathering relevant information from various sources within the power system, such as control centers, and communication networks. Collected data typically includes measurements of communication signals. Accurate and comprehensive data collection is crucial for identifying anomalies and potential cyber threats within the power system.

Preprocessing Module :

Preprocessing is the step where collected data is cleaned, formatted, and transformed to prepare it for analysis. Tasks in pre-processing may include removing noise, handling missing values, and standardizing data formats. Preprocessing ensures that the data is of high quality and consistency, improving the effectiveness of subsequent analysis techniques.

Deep Learning Model Training:

The deep learning model training module focuses on leveraging advanced machine learning techniques, such as deep learning using XGBoost, to develop models capable of recognizing patterns and anomalies indicative of cyber threats within the power system. Deep learning using XGboost models are trained using preprocessed data to recognize patterns and anomalies that may indicate cyber-attacks.These models learn from historical data to identify normal system behaviour and detect deviations from it.Training deep learning models is essential for developing accurate and reliable methods for identifying cyber threats in real-time.

Real-Time Monitoring Module :

Real-time monitoring involves continuously observing the operation of the power system and analysing incoming data streams. Monitoring is performed in real-time to detect anomalies or suspicious activities as they occur.Real-time monitoring allows for immediate response to potential cyber attacks, minimizing their impact on system operations.

Anomaly Detection:

Anomaly detection techniques are applied to the data to identify deviations from expected behaviour. Detected anomalies may indicate the presence of cyber-attacks or system malfunctions. Anomaly detection helps to prioritize response actions and initiate mitigation strategies to address potential threats promptly.

2. CONCLUSION

In conclusion, the proposed approach presented in this paper offers a comprehensive solution to enhance the security and resilience of Frequency Regulation (FR) in power systems against cyber threats. By leveraging deep learning models, specifically using the XGBoost algorithm, in conjunction with real-time monitoring and anomaly detection techniques, the proposed system enables proactive detection and mitigation of potential cyber-attacks targeting the communication infrastructure within the power system. The systematic workflow outlined in this paper, from data collection and preprocessing to deep learning model training and real-time monitoring, provides a robust framework for safeguarding the integrity of FR operations. Through accurate identification of anomalies and prompt response to potential threats, the proposed system ensures the continuous stability and reliability of the power grid, even in the face of dynamic and evolving cyber risks. Furthermore, the integration of advanced cybersecurity measures within the FR framework strengthens the overall security posture of power systems, safeguarding critical infrastructure and ensuring uninterrupted electricity supply to consumers. The proposed approach represents a significant step towards fortifying power system security and resilience in the increasingly interconnected and digitized energy landscape.

REFERENCES

1. R. He, H. Xie, J. Deng et al., "Reliability modeling and assessment of cyber space in cyber-physical power systems", IEEE Transactions on Smart Grid, vol. 11, no. 5, pp. 3763-3773, Sept. 2020.
2. N. Sultana, N. Chilamkurti, W. Peng and R. Alhadad, "Survey on SDN-based network access detection using machine learning methods", Peer-to-Peer Netw. Application, vol. 12, no. 2, pp. 493-501, March 2019.
3. N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, "The deep learning process on network access", by IEEE on emerging topics computational intelligence, vol. 2, no. 1, pp. 41-50, 2018.
4. S. Zuo, O. A. Beg, F. L. Lewis and A. Davoudi, "Resilient networked ac microgrids under unbounded cyber attacks", IEEE Transactions on Smart Grid, vol. 11, no. 5, pp. 3785-3794, 2020.
5. O. A. Beg, L. V. Nguyen, T. T. Johnson and A. Davoudi, "Cyber-physical anomaly detection in microgrids using time-frequency logic formalism", IEEE Access, vol. 9, pp. 20012-20021, 2021.
6. S. Sindhura, S. Phani Praveen, A. Madhuri and D. Swapna, Different Feature Selection Methods Performance Analysis for Intrusion Detection, 2022.
7. Praveen PhaniSurapaneni, Krishna MuraliThatiBala, Chawla Kumar Sunil and AnuradhaChokka, "Virtual Private Network Flow Detection in Wireless Sensor Networks Using Machine Learning Techniques", International Journal of Sensors Wireless Communications and Control, vol. 11, no. 7, 2021.
8. S. Li, K. Xue, Q. Yang and P. Hong, "PPMA: Privacy-preserving multisubset data aggregation in smart grid", IEEE Trans. Ind. Informat., vol. 14, pp. 462-471, Feb. 2018.
9. L. Che, X. Liu, Z. Shuai, Z. Li and Y. Wen, "Cyber cascades screening considering the impacts of false data injection attacks", IEEE Trans. Power Syst., vol. 33, no. 6, pp. 6545-6556, Nov. 2018.
10. XiaodanXu, Huawen Liu and Minghai. Yao, "Recent Progress of Anomaly Detection", Complexity, pp. 1-11, 2019.