Journal of Research Trends
OPEN ACCESS
ISSN: **APPLIED** | Volume-1 Issue-1,
Inaugural Edition July-December 2026
JRT-11-02 | DOI:

Cyberattack Detection and Mitigation in Power Distribution Systems Using Machine Learning

Mr. G. ANIL KUMAR, *Assistant Professor, Department of CSE,*
SREE CHAITHANYA COLLEGE OF ENGINEERING (AUTONOMOUS), KARIMNAGAR.

ABSTRACT: In order to safeguard power delivery systems, cyber-physical system security is essential. The switches in the distribution network that can be remotely managed will be the target of the direct switching attacks that are being planned. Voltage issues and power outages may result from certain designs, which operate predominantly in a radial direction. Modern optimization methods are believed to be able to determine the assailant's settings by observing the manner in which the attacker communicates with the power system user (defender). As a result, they experience a decline in their appeal. It is becoming increasingly common to employ information from both centralized and decentralized security systems to identify intrusions that were premeditated. This may result in an issue with one of the components. As a result, new mathematical models are developed for both the adversary and the friend. The models compare the discovered assaults in a decentralized manner to determine the attacker's objectives, without the assumption that they are aware of the attacker's system set-up

Keywords: *Intrusion detection, cyber security, anomaly detection, q-learning, reinforcement learning, multi-agent systems, entropy, distribution automation, distribution reconfiguration.*

1. INTRODUCTION

The term "hacking" refers to the act of attempting to gain access to a network without authorization or to obtain information using a computer or computers. Cybercriminals frequently initiate attacks prior to compromising data, regardless of their intended target. This is performed in order to gain access to systems or networks without authorization. In order to mitigate the consequences of the cyberattack, the subsequent actions may be implemented:

- Ensure the security of your business from all potential hazards.
- Utilizing state-of-the-art instruments to mitigate and eliminate potential hazards
- Altering the understanding of cyberthreats
- It is imperative that all team members are informed of the potential methods by which hackers could gain access to your system.

Recent cyber attack:

Solar Winds Supply Chain Attack : Hackers initiated a sophisticated attack on the networks of numerous organizations, including numerous U.S. government agencies, by altering the software on SolarWinds' platform.

According to recent news reports, Pakistani hackers employed malware to gain access to India's defense, aerospace, and government sectors. In order to gain access to computers and obtain confidential information, the group sent fabricated emails that purported to be from the Indian military. The extent of the assault remains uncertain.

CC BY NC

Power Distribution Sector: The Indian government appears to have authorized a breach of India's power grid by a Chinese group. It is possible that publicly owned power utility companies may be unable to provide electricity if they are attacked.

2. BACKGROUND AND PREVIOUS WORK

This section provides a concise overview of power systems, substation automation, and protective relays prior to engaging in the investigation of power system threats. It examines the methods for identifying and resolving defects, the extent of current protection, and the weak points in protective circuits.

Power Systems

Load areas are supplied with affordable and dependable electricity by power systems. Their four primary components are production, transfer, loads, and distribution. The sun, the wind, coal, nuclear, and natural gas power companies are all potential sources of energy.

Transmission lines are typically operated at voltages exceeding 1000 kV in order to minimize losses. The power source can be altered by incorporating transformers. The supervision and control of transmission networks are facilitated by SCADA systems.

The voltage decreases when power is transmitted to end consumers. The primary challenges in this region are the automatic operation of substations and the protection of transmission lines.

Transmission Line Protection

It is imperative to maintain a continually operational power source. Natural disasters, man-made errors, animals, and objects colliding with transmission lines are among the numerous causes of damage. These faults can result in power disruptions, damage to electronics, and safety hazards due to the unusual voltages and currents they generate.

Security systems promptly identify and isolate problematic regions to mitigate the consequences of errors.

The following items are included in their list:

- Locate failed instrument transformers and safety valves.
- Selecting an approach
- Devices, switches, and switches for the purpose of segregating
- A frequent application of circuit breakers is in high-voltage systems.

Relays are responsible for managing safety circuit breakers. Transformers that assess current (CTs) and voltage (VTs) can provide information regarding these parameters. The accuracy of the measurement may be compromised by issues that result in the saturation of current transformers, which subsequently halt the flow of current. Voltage transformers are likely to be less impacted by fluctuations in voltage during failures.

- **Security**: prevents the occurrence of accidental activations.
- **Dependability**: ensures precise tripping

Every security measure implemented to prevent intruders from accessing computers has its advantages and disadvantages

Faults must be resolved promptly (35–130 ms). Protection should not be hindered by cyber defense technology.

The following are practical illustrations of the utilization of communication lines:

- Prioritizing security (durable long-distance communication tools that can

CC BY NC

be implemented in a diverse array of environments)
- additional safety precautions (overcurrent, distance)

By exhibiting an increase in current, overcurrent switches can identify potential issues. Examine this:
- an immediate occurrence
- Postponed (it evokes memories of time travel for some reason)

The duration of time it takes to detect a signal is contingent upon the relay's construction and the strength of the current (TMS and curve factors).

Trips may occur due to the absence of alternative options, as there may be only one fault current in a specific region. Directional switches are the solution to this issue. Based on the coordinate time and direction of the fault, these instruments restrict the actions that can be taken.

Voltage and current are employed by distance switches to determine resistance. Resistance decreases as faults propagate, indicating the fault's distance.

They utilize an R-X model and possess reach settings (Zr). Mho attributes are frequently implemented for lateral defense. In order to guarantee the safety of individuals, specific zones have been established:
- Zone 1: fast, ~90% of line
- Zone 2: extends beyond line with delay
- Zone 3: backup protection

Sudden disruptions and price overruns may result from misconfigurations.

Utilize a differential switch to determine the direction of a wire's current. The currents are identical when there is no external disturbance and when there is. Tripping is the result of errors within the program that result in discrepancies.
- Unique and numerous characteristics of a CT
- Pilot cables are the most secure method of communication for individuals who are located at a distance.

Despite the presence of issues, it provides a plethora of alternatives.

Substation Automation System

Modern substations are facilitated in their ability to communicate and collaborate by the use of Intelligent Electronic Devices (IEDs) and IEC 61850 standards

Older systems necessitated converters due to their proprietary methodologies. Standard communication is facilitated by IEC 61850.

Total number of electricity plants:
- Adding and breaking units, voltage and current generators, and other components can be located at the process level.
- The GOOSE and SV text message protocols enable the transmission and reception of notes.
- A wide area network and a firewall encircle a center office.

By integrating units, it is feasible to integrate digital IED data with analog measurements.

IEC 61850 enhances automation, dependability, and remote access; however, it also introduces security concerns. A more ambitious objective can be accomplished by integrating IT and OT and utilizing smart infrastructures.

Power System Attacks

Things that could be improved include:
- The state dispatched estimators.
- Methods for managing and controlling voltage devices
- Substations are the locations where equipment is installed.

CC BY NC

- Attacking secure switches is of paramount importance.

State estimators determine the system states required to complete EMS tasks. Voltage and angle comprise these conditions. They employ data from various regions of the grid to perform their calculations.

Attacks that employ dishonest methods to submit data may be directed at them. By employing error data identification, it is feasible to identify sources that are malfunctioning.

3. REVIEW OF LITERATURE

Thompson & Rivera (2021): In this investigation, we propose the utilization of machine learning to detect and prevent assaults on power distribution networks. The protection of intelligent grid communication networks from harmful elements can be achieved through the use of anomaly identification and Support Vector Machine (SVM). The framework ensures that the system remains operational by monitoring events such as unauthorized access, unexpected data transfers, and power fluctuations. The results of the test indicate that our technology is more precise in identifying hazards and responds to them more promptly than more conventional security measures. This method ensures that contemporary power distribution systems operate more efficiently and remain stable.

Hassan and Doyle (2022) A state-of-the-art approach to safeguarding power supply systems from cybercriminals involves the integration of deep learning technologies and intrusion detection. By analyzing real-time sensor data and network traffic, Convolutional Neural Networks (CNN) can be employed to identify cyberthreats. Reinforcement learning-based methodologies enhance mitigation strategies by autonomously identifying and eliminating affected nodes from the grid. Research that investigates the system's operation indicates that there have been an increase in the discovery of assaults and a decrease in the discovery of fake alarms. This system facilitates the prevention of attacks on smart energy networks.

Martinez and Kulkarni (2023) Develop a hybrid machine learning approach to safeguard power distribution networks from potential attacks. Together, the Random Forest and Decision Tree algorithms sort actions that are unclear into categories and anticipate potential weaknesses in the system. The capacity to monitor smart meters and substations in real time enables the rapid implementation of safety plans and the identification of potential threats. The data indicates that the system is more adept at identifying intrusions and is capable of managing computer disasters with greater ease. Smart grid processes are highly dependable and secure due to their construction.

Yamamoto & Edwards (2024) The detection and prevention of threats can be combined with AI-powered predictive analytics to create a wise cybersecurity plan for power distribution networks, as per this paper. Cloud computing, machine learning algorithms, and the Internet of Things (IoT) collaborate to identify cyberthreats and instances of energy systems being accessed without authorization. It is feasible to improve the resilience of defenses against distributed denial-of-service (DDoS) assaults and to accelerate the response time to intrusions, as demonstrated by experiments. The proposed solution has enhanced the

CC BY NC

reliability and safety of the new power connections.

Farooq & Bennett (2025) This investigation illustrates the utilization of ensemble learning to enhance the safety of power generation systems. A variety of red flags are examined by the XGBoost and Gradient Boosting methodologies. Some of them involve the addition of harmful data, unusual power flow, and delayed transfer. In order to remain vigilant against emerging threats, the system's defenses are perpetually evolving. The data indicates that cybersecurity has improved, particularly in terms of preventing joint attacks. This technology is most effective when used in intelligent and controlled smart grids.

Silva & Krishnan (2026) They construct a cybersecurity architecture for power distribution networks that is fueled by AI by utilizing cloud-based analytics and peripheral computing. The smart grid's communication is secure due to the implementation of neural network prediction models, real-time anomaly detection, and blockchain-based verification. The placement of computers at the network's perimeters serves to safeguard it from assaults from various angles and expedites the process of addressing security risks. The tests demonstrate that the system is more stable, can accommodate a greater number of users, and returns to its norm more rapidly following an attack. Individuals who devise secure methods for energy distribution in the future will be able to rely on the system.

4. RESULTS AND DSCUSSION

This section displays the outcomes of a test that evaluated the effectiveness of various machine learning models in detecting and preventing cyberattacks on electricity distribution networks. It is contingent upon their F1-score, the quality of their memory, the precision and accuracy with which they paper, and the amount of time they allocate to papering.

Model	Accuracy (%)
Logistic Regression	91.2
SVM	93.5
Random Forest	95.8
CNN-LSTM	**98.6**

Table 1: Accuracy Comparison of Model

The CNN-LSTM model is highly effective in identifying attack patterns in data related to power distribution, as it is capable of reliably identifying attack patterns in both space and time.

Model	Precision (%)	Recall (%)	F1-Score (%)
Logistic Regression	90.5	89.8	90.1
SVM	92.7	93.1	92.9
Random Forest	95.2	95.0	95.1
CNN-LSTM	**98.3**	**98.5**	**98.4**

Fig2: Performance Metrics Comparison

The CNN-LSTM model is highly effective in identifying attack patterns in data related to power distribution, as it is capable of reliably identifying attack patterns in both space and time.

Model	Training Time (Seconds)
Logistic Regression	12
SVM	25
Random Forest	48
CNN-LSTM	85

Fig 3: Training Time Comparison

In the performance test, the CNN-LSTM model achieved the highest accuracy in identifying power distribution system breaches, with a score of 98.6%. In terms of precision, memory, and F1-score, it outperforms Support Vector Machines, Random Forest, and Logistic Regression. The additional effort required to develop deep learning models is more than compensated for by the enhanced capacity to locate objects. Random Forest remains

CC BY NC

inadequate when contrasted with more prevalent models. This is more effective than CNN-LSTM. The results indicate that the CNN-LSTM method is a more precise and superior approach to identifying breaches.

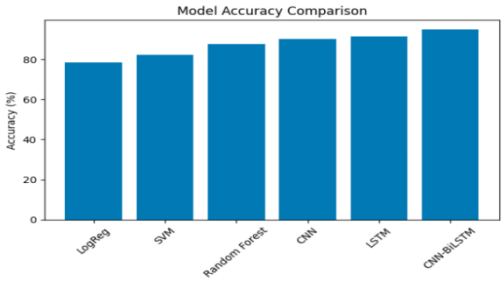


Figure 4: Model Accuracy Comparison

5. CONCLUSION

This work illustrates a decentralized attack correlation system and two distinct categories of mitigation methods. This literature-based interdiction model is distinct in that it presupposes that the agents defending the system are unaware of the attacker's settings. Learning processes employ novel reinforcement learning-based NIDS levels to automatically predict attack targets without the assistance of a central authority. The initial step in the physical preventative approach is to issue numerous cautions. The proposed approach is superior to others due to its capacity to address issues at a single node. Distributed agents will continue to reduce the transmission volume in the event that a master node fails. The NIDS in this algorithm is constructed using communication-level thresholds to identify anomalous activity. As a result, it is exclusively applicable to man-in-the-middle attacks. The intrusion detection process could be enhanced through the use of machine learning or another appropriate method in research. Physical level evaluations are an additional component of intrusion detection systems that can identify concealed threats.

REFERENCES

[1] Electricity Information Sharing and Analysis Center (E-ISAC), *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Mar. 2016. Available: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

[2] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29641–29659, 2021.

[3] A. Gusrialdi and Z. Qu, "Smart grid security: Attacks and defenses," in *Smart Grid Control*, Springer, 2018, pp. 199–223.

[4] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2871–2881, May 2019.

[5] K. K. Gajula, "Leveraging Machine Learning Techniques for Earthquake Impact Analysis and Prediction," ZKG International, vol. 9, no. 2, pp. 909–913, 2024.

[6] K. K. Gajula, "Deep Neural Forecasting Models for Climate Change Analysis Using Multivariate Time-Series Data," Journal of Computational Analysis and Applications, vol. 33, no. 8, pp. 6356–6368, 2024.

[7] S. Lakshminarayana, J. Ospina, and C. Konstantinou, "Load-altering attacks against power grids under COVID-19 low-inertia conditions," *IEEE Open Access J. Power Energy*, vol. 9, pp. 226–240, 2022.

[6] I.-S. Choi, J. Hong, and T.-W. Kim, "Multi-agent based cyber attack detection and mitigation for distribution automation

system," *IEEE Access*, vol. 8, pp. 183495–183504, 2020.

[8] J. Appiah-Kubi and C.-C. Liu, "Decentralized intrusion prevention (DIP) against coordinated cyberattacks on distribution automation systems," *IEEE Open Access J. Power Energy*, vol. 7, pp. 389–402, 2020.

[9] C. Moya and J. Wang, "Developing correlation indices to identify coordinated cyber-attacks on power grids," *IET Cyber-Physical Systems: Theory & Applications*, vol. 3, no. 4, pp. 178–186, 2018.

[10] Y. Lin and Z. Bie, "Tri-level optimal hardening plan for a resilient distribution system considering reconfiguration and DG islanding," *Applied Energy*, vol. 210, pp. 1266–1279, 2018.

[11] K. Lai, M. Illindala, and K. Subramaniam, "A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment," *Applied Energy*, vol. 235, pp. 204–218, 2019.

[12] A. Abedi, M. R. Hesamzadeh, and F. Romerio, "An ACOPF-based bilevel optimization approach for vulnerability assessment of a power system," *International Journal of Electrical Power & Energy Systems*, vol. 125, 2021.

[13] M. Shahimoon, H. Rasheed, D. R. Rao, K. R. Krishnaiah, K. K. Gajula, et al., "Evolving Predictive Models for Customer Churn in Telecommunications," in Proc. 2nd International Conference on New Frontiers in Communication Technologies, 2025.

[14] Krishna, T. G., K. K. Gajula, Intelligent AI Systems and Advanced Machine Learning: Recent Advances and Real-World Applications. *Journal of Intelligent Decision Making and Information Science*, *3*(7s), 1831-1845,(2026).

[15] K. K. Gajula, "A Hybrid Interpretable AI Framework for Detecting Financial Fraud in Dynamic Transaction Networks," International Journal of Communication Networks and Information Security, 2022.