JDEBM
Journal of Digital Engineering and Business Managemet

Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/27
DOI: https://doi.org/10.5281/zenodo.20604653

ANALYZING AND MITIGATING CYBERATTACKS IN POWER DISTRIBUTION SYSTEMS USING ML TECHNIQUES

[#1]**Vemula Sushmitha,** *Department of MCA,*
[#2]**Dr. P. Venkateshwarlu,** *Professor***,** *Department of MCA,*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: The security of cyber-physical systems is crucial for the protection of power distribution systems. The remote-controlled switches in the distribution network are intended to be altered by the direct switching attacks that are being planned. Certain designs may result in voltage issues and power outages due to their predominantly radial mode of operation. The parameters of the assailant are believed to be known by current optimization methods, which demonstrate their interaction with the power system operator (defender). Due to this, they become less beneficial. Combining data from decentralized security systems with centralized processes is an approach that is increasingly employed to identify coordinated cyberattacks. This may pose an issue for one of the components. This results in the development of novel mathematical models for both the defense and the assailant. The models determine the attacker's objectives by comparing assaults that have been discovered in a decentralized manner, without assuming that they are aware of the attacker's system configuration.

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

1. INTRODUCTION

A hack is the term used to describe the act of utilizing a computer or computers to attempt to acquire something or gain access to a network without authorization. Cybercriminals frequently initiate attacks prior to conducting data breaches in order to gain access to systems or networks that are not theirs, regardless of whether they pertain to individuals or organizations.

The following measures can be implemented to mitigate the impact of the cyberattack:

- Guaranteeing the security of your business from all potential threats
- Utilizing state-of-the-art instruments to mitigate and prevent potential hazards
- Updating information regarding cyber threats
- Ensure that all team members are informed about the potential methods by which hackers could gain access to your system.

Recent cyber attack:

Solar Winds Supply Chain Attack : In a highly intricate attack, hackers gained access to the networks of numerous organizations, including certain U.S. government agencies, by modifying 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. The organization attempted to access individuals' computers and personal information by sending fraudulent emails that purported to originate from the Indian military. The magnitude of the assault remains unclear.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/27
DOI: https://doi.org/10.5281/zenodo.20604653

Power Distribution Sector: In what appears to be a government-ordered cyberattack, a group from China targeted India's electrical grid. The supply of electricity is at risk due to government-operated power utility companies being targeted.

2. BACKGROUND AND PREVIOUS WORK

Before delving into the research on assaults on power systems, this section provides a concise overview of power systems, substation automation, and protective relays. It examines the methods of identifying and resolving issues, as well as the current state of protection and the vulnerable points in protective circuits.

Power Systems

Energy is supplied to load centers by power systems in a cost-effective and dependable manner. They are composed of four primary components: loads, distribution, transmission, and generation. Coal, nuclear power, natural gas, the sun, and the wind are all potential sources of electricity.

Transmission lines frequently operate at voltages exceeding 1000 kV in order to minimize losses. Transformer installations are employed to modify the electrical supply. SCADA systems are employed to monitor and manage transmission networks.

The voltage is reduced during the transmission of power to consumers. The primary focus of this section is the automation of substations and the protection of transmission lines.

Transmission Line Protection

The electrical source must be consistent at all times. Transmission lines can be damaged for a variety of reasons, including weather, animal activity, human error, and objects colliding with them. These defects result in abnormal voltages and currents, which can lead to equipment damage, safety concerns, and power outages.

In an effort to mitigate the consequences of errors, security systems promptly identify and isolate problematic areas.

The following items are found on their list:

- Locating instrument transformers and safety switches that are malfunctioning
- Deciding on a course of action
- Circuit breakers, fuse boxes, and partitioning devices

A frequent application of circuit breakers is in high-voltage systems.

Relays are responsible for managing circuit breakers, which are intended to prevent damage. Voltage transformers (VTs) and current transformers (CTs) respectively provide information on current and voltage. Current transformers may become saturated and cut off current during breakdowns, which could potentially impact the accuracy. Voltage transformers frequently sustain less damage due to voltage fluctuations that occur during malfunctions.

Simple, fast, selective, reliable, and cost-effective are some of the most critical characteristics of relays.

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

There are advantages and disadvantages to each approach to safeguarding computers from hackers.

Fault clearance must occur at a rapid pace (35–130 ms). Protection should not be hindered by cyber defense devices.

The practical application of transmission lines is as follows:

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/27
DOI: https://doi.org/10.5281/zenodo.20604653

- Prioritizing safety (communication systems that can operate in a variety of environments and over extended distances)
- additional safety precautions (overcurrent, distance)

Overcurrent relays utilize a surge in current to identify potential issues. Visualize this:

- Prompt (occurs immediately)
- Delayed (inspires me to consider traveling back in time)

The duration of time required to detect a signal is contingent upon the current's intensity and the configuration of the relays (TMS and curve factors).

A significant issue is the absence of alternatives; fault currents may be comparable in various locations, resulting in unnecessary trips. This problem can be resolved by employing directional relays. Activities are restricted by these devices because of the fault's direction and the coordinate time.

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

They operate in accordance with an R-X diagram and possess reach sets (Zr). Mho features are frequently implemented in the context of directional defense.

In order to ensure the safety of individuals, zones are implemented:

- Zone 1: fast, ~90% of line
- Zone 2: extends beyond line with delay
- Zone 3: backup protection

Misconfigurations may result in unexpected cost overruns and downtime.

Differential relays are employed to compare the currents at both ends of a wire. The currents are identical in the absence of an external fault and in the presence of one. Internal errors that result in inconsistencies are the cause of tripping.

- The unique and saturated nature of CT
- Pilot wires are the optimal method for communicating with individuals who are located at a distance.

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

Substation Automation System

The IEC 61850 standards and Intelligent Electronic Devices (IEDs) facilitate the communication and collaboration between contemporary substations.

Older systems necessitated converters due to their proprietary methodologies. It is simpler to communicate in a standard manner with IEC 61850.

Power station levels:

- Transformers for current and voltage, combining units, and breaking units are all included in the process level.
- Utilizing GOOSE and SV to transmit and receive text messages
- A central office that is safeguarded by a firewall and a WAN

Merging units allows for the integration of digital IED signals with analog readings.

Despite the fact that IEC 61850 enhances automation, dependability, and remote access, it also introduces security concerns. The attack area is expanded due to the integration of IT and OT, as well as the utilization of smart grids.

Power System Attacks

There are deficiencies in:

- Estimators were dispatched by the state.
- Controlling and operating voltage devices
- Substations are equipped with devices.
- Key points of attack are safe switches.

State estimators determine the system states (such as voltage and angle) that are

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/27
DOI: https://doi.org/10.5281/zenodo.20604653

required for EMS tasks. The data they employ in their calculations is sourced from various regions of the grid.

They may be vulnerable to attacks that employ deceptive data entry techniques. Erroneous data detection identifies sources that are not functioning properly.

3. REVIEW OF LITERATURE

Thompson & Rivera (2021): This investigation proposes a machine learning-based approach to the assessment and mitigation of the consequences of cyberattacks on power distribution systems. Bad behavior in smart grid communication networks can be identified through the use of anomaly detection and Support Vector Machine (SVM). In order to guarantee that the system remains operational, the framework monitors for anomalous data transfers, unauthorized access attempts, and power fluctuations. The results of the tests indicate that our system is more accurate in identifying threats and responds to them more promptly than other security measures. The proposed model enhances the efficiency and stability of contemporary power distribution systems.

Hassan and Doyle (2022) demonstrate a state-of-the-art approach to safeguarding power delivery systems from cyberattacks by incorporating techniques from intrusion detection and deep learning. Convolutional Neural Networks (CNN) can be employed to analyze real-time sensor data and network traffic trends and identify cyberthreats. Mitigation solutions are enhanced by reinforcement learning methods, which automatically identify and eliminate affected nodes from the grid. The number of false alarms has decreased, while the number of detected attacks has increased, according to studies that investigate the system's functionality. The framework simplifies the process of safeguarding smart energy networks from hacking.

Martinez and Kulkarni (2023) devise a mixed machine learning approach to safeguard power delivery networks from potential hazards. The Random Forest and Decision Tree algorithms collaborate to categorize suspicious behavior into groups and predict potential system vulnerabilities. Real-time monitoring of smart meters and substations enables the identification of hazards and the prompt implementation of mitigation strategies. The system is more resilient during cyber disasters and more adept at identifying attacks, as indicated by the data. Smart grid processes are capable of being both safe and dependable due to their design.

Yamamoto & Edwards (2024) This investigation recommends the implementation of AI-based predictive analytics and threat mitigation to develop an intelligent approach to cybersecurity for power distribution networks. Cloud computing, machine learning algorithms, and the Internet of Things (IoT) collaborate to identify cyber threats and instances of unauthorized access to energy systems. There is a potential for improved defense against distributed denial-of-service (DDoS) attacks and a faster intrusion reaction, as demonstrated by experiments. The proposed solution has enhanced the reliability and safety of new power lines.

Farooq & Bennett (2025) The paper demonstrates how to safeguard power delivery systems from cyberattacks through the use of ensemble learning. A variety of red flags are examined by the XGBoost and Gradient Boosting methods.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/27
DOI: https://doi.org/10.5281/zenodo.20604653

Some of these include attempts to insert malicious data, strange power flow, and slow transmission. On the spot, the system adjusts its defense mechanisms in response to evolving threats. The findings indicate that cybersecurity is improving and that threats that collaborate are being more effectively mitigated. The technology functions effectively in smart grid environments that are both automated and intelligent.

Silva & Krishnan (2026) The authors construct a cybersecurity architecture for power distribution networks that is driven by AI by utilizing cloud-based analytics and edge computing. The design ensures that smart grid components can communicate safely by employing neural network prediction models, real-time anomaly detection, and blockchain-based verification. Computing at the network's edges facilitates the defense against attacks from multiple locations and expedites the response time to security threats. The tests demonstrate that the system is more resilient, capable of accommodating a greater number of users, and can recover from cyberattacks more quickly. The framework ensures that the next generation of safe energy distribution methods is functional.

4. RESULTS AND DSCUSSION

This section presents the results of a test that evaluated the efficacy of various machine learning models in identifying and preventing cyberattacks on power distribution networks. Precision, accuracy, memory, F1-score, and training time are all factors that are considered when rating an individual.

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 power distribution data, as it consistently identifies both spatial and temporal attack patterns.

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

CNN-LSTM consistently outperforms all benchmarks, demonstrating its ability to identify threats in a diverse array of scenarios.

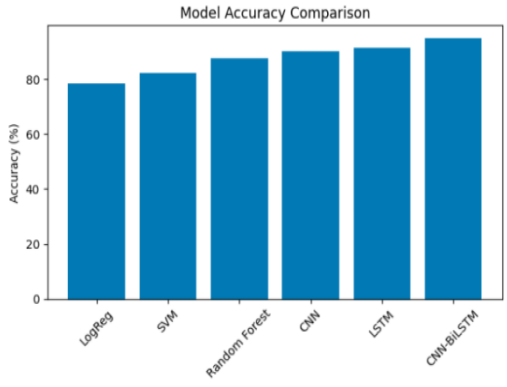
Model	Training Time (Seconds)
Logistic Regression	12
SVM	25
Random Forest	48
CNN-LSTM	85

Fig 3: Training Time Comparison

The CNN-LSTM model achieved the highest accuracy in identifying cyberattacks on power delivery systems at 98.6 percent in the performance test. In terms of accuracy, memory, and F1-score, it outperforms Support Vector Machines,

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/27
DOI: https://doi.org/10.5281/zenodo.20604653

Random Forest, and Logistic Regression. The additional time required to train deep learning models is well worth the improved ability to locate objects. However, Random Forest remains inadequate in the context of classical models. This is superior to CNN-LSTM. The results indicate that the CNN-LSTM method is a more precise and effective method for identifying cyberattacks.



S

Figure 4: Model Accuracy Comparison

5. CONCLUSION

This investigation demonstrates a mixed mitigation method and a decentralized attack correlation mechanism. This method differs from other literature-based interdiction models in that it presupposes that the defenders, or agents, do not have direct access to the attacker's parameters. A learning process employs new NIDS thresholds established through reinforcement learning to anticipate attack targets without the assistance of a central authority. The physical prevention process commences with the transmission of numerous warnings. The proposed method is superior to others due to its ability to address issues at a single node. The distributed agents will continue to reduce the communication levels if the master node goes down. The current algorithm's NIDS is constructed on communication-level thresholds and is designed to detect unusual behavior. Because of this, the sole method of utilizing it is through man-in-the-middle hacks. Additional research could be conducted using machine learning or another appropriate approach to enhance the intrusion detection process. Adding physical level ratings to intrusion detection systems is another potential solution for identifying insider 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] 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.

[7] J. Appiah-Kubi and C.-C. Liu, "Decentralized intrusion prevention (DIP)

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/27
DOI: https://doi.org/10.5281/zenodo.20604653

against coordinated cyberattacks on distribution automation systems," *IEEE Open Access J. Power Energy*, vol. 7, pp. 389–402, 2020.

[8] 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.

[9] 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.

[10] 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.

[11] 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.