Journal of Artificial Intelligence Practice (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/jaip.2025.080407
ISSN 2371-8412 Vol. 8 Num. 4

Application of Artificial Intelligence Technology in Network Security Protection of Power Enterprise

Yong Fu

Beijing Remarkables United Technology Co., Ltd., Beijing, 100192, China

Keywords: Power Information Security; Artificial Intelligence; Machine Learning; Anomaly Detection; Situational Awareness; Industrial Control System Security

Abstract: This article aims to explore how artificial intelligence (AI) technology empowers power enterprises to build a new generation of proactive, intelligent, and adaptive cybersecurity protection systems. The article first analyzes the new types of cybersecurity threats faced by power systems and their severe challenges to critical information infrastructure, and expounds on the limitations of traditional security protection methods. Furthermore, it systematically discusses the specific application paradigms of AI core technologies such as machine learning, deep learning, and natural language processing in enterprise network boundaries, production control areas (II/III zones), and wide-area environments, including intelligent threat detection, abnormal behavior analysis, security situation awareness and prediction, and automated response. Finally, this article prudently assesses the challenges faced by AI applications, such as data quality, model interpretability, adversarial attacks, and compliance, and looks forward to the future development direction of technology and business integration.

1. Introduction

The accelerated evolution of the Global Energy Interconnection and new power systems is driving the power industry into a phase of deep digital transformation. The extensive integration of technologies such as cloud computing, the Internet of Things, big data, and mobile internet not only enhances the intelligent level and operational efficiency of power grids but also drastically expands the network attack surface, making critical information infrastructure (CII) in the power sector a key target for nation-state advanced persistent threat (APT) attacks[1]. Traditional network security protection systems rely on signature-based matching and static rule sets, which are inherently reactive approaches based on known threats. These systems exhibit significant shortcomings when facing zero-day vulnerabilities, targeted attacks, insider threats, and specific industrial control system (ICS) threats. The evolution speed of attack techniques has far surpassed the update cycle of traditional security measures' defense capabilities, posing unprecedented and severe challenges to power companies[2].

Artificial intelligence (AI) technology, with its powerful pattern recognition, anomaly detection, and prediction capabilities, offers a revolutionary path for reconstructing the power network security protection paradigm. AI can perform deep mining and correlation analysis of massive, multi-source, and heterogeneous security data, constructing dynamic, adaptive security protection

mechanisms from a data-driven perspective, achieving a fundamental shift from "passive alerting" to "active prediction" and from "single-point defense" to "collaborative response." Researching the innovative application of AI technology in the network security protection of power companies is of significant strategic importance and practical value for ensuring national energy security and supporting the stable operation of the social economy[3].

This study aims to systematically construct an application framework for AI technology in the network security protection of power companies and to deeply analyze its core implementation technologies and the challenges it faces. The article will first deconstruct the security characteristics of power companies' networks and lay the theoretical foundation for AI technology. It will then propose a layered and domain-partitioned systematic application architecture and deeply elaborate on its implementation paths in key scenarios such as threat detection, behavior analysis, situational awareness, and automated response. Subsequently, it will carefully evaluate the data, model, adversarial, and management challenges faced during the application process and discuss feasible countermeasures.

2. Theoretical Foundation

2.1 Characteristics Analysis

The power enterprise network is not a homogeneous whole but is divided into logically clear and physically isolated security zones based on the protection principles of "security zoning, network specialization, horizontal isolation, and vertical authentication." Among these, the production control zone (encompassing Zone I, the real-time control zone, and Zone II, the non-control production zone) is the lifeline of core power business, operating Supervisory Control and Data Acquisition (SCADA), Energy Management Systems (EMS), Wide Area Measurement Systems (WAMS), and various Intelligent Electronic Devices (IEDs). This area commonly employs industrial standards such as IEC 61850, IEC 104, and Modbus for communication protocols. Its requirements for system availability, real-time performance, and determinacy are far higher than those for confidentiality; any minor delay or interruption can trigger significant operational accidents. The management information zone (Zones III/IV) carries traditional enterprise IT systems and has a logical connection to the internet, facing a wider variety of external threats[4].

This architectural characteristic gives rise to a unique security risk profile. Common attack behaviors in traditional IT networks, such as vulnerability scanning and brute-force cracking, can be directly transformed into damage to physical processes in the production control environment due to protocol vulnerabilities, for example, causing relay protection misoperation or generator tripping through replaying or tampering with instruction packets. Advanced Persistent Threat (APT) attackers tend to adopt a "from outside to inside" penetration strategy, first breaking through the office network (Zone IV) and gradually approaching and controlling the production system through vertical traversal. The large-scale access of distributed energy and the improvement of distribution automation make the distribution network side a new attack entry point. Distributed Denial of Service (DDoS) attacks or electricity theft against smart meters can have a widespread impact on the economic operation of the power grid. Misoperation or malicious behavior by internal personnel is more concealed and destructive in the absence of effective behavior monitoring.

2.2 Artificial Intelligence Technologies

Addressing the aforementioned complex risks requires a range of core artificial intelligence technologies, each offering unique value in understanding and analyzing data.

Machine Learning (ML) forms the cornerstone of intelligent security analysis. Supervised

learning algorithms, such as Support Vector Machines (SVM) and Random Forests, can efficiently perform tasks like malware family classification and network traffic application identification after being trained on high-quality labeled data. Unsupervised learning plays a crucial role in scenarios lacking prior labels. Clustering algorithms like K-Means and DBSCAN can automatically group massive logs and traffic data to discover potential anomaly patterns. Autoencoders establish a normal baseline of system or user behavior through reconstruction learning. Any deviation from this baseline generates a high reconstruction error, thereby identifying it as an anomalous event, which is extremely suitable for detecting unknown attacks and insider threats.

Deep Learning (DL) further enhances the ability to process high-dimensional, sequential data. Recurrent Neural Networks (RNN) and their improved variant, Long Short-Term Memory networks (LSTM), can effectively capture long-range dependencies in network traffic and system call sequences, which is essential for detecting APT attack chains that rely on multi-stage, long-cycle operations. One-dimensional Convolutional Neural Networks (1D-CNN) can be regarded as high-performance feature extractors, automatically learning discriminative features from raw network packets or system logs, reducing the reliance on manual feature engineering. Graph Neural Networks (GNN) surpass the processing capabilities of sequential data. They can abstract hosts, users, and processes in the network as nodes, and the access and communication relationships between them as edges, constructing a dynamic knowledge graph, thereby accurately identifying abnormal lateral movement paths and potential attack relationship networks[5].

2.3 Core Capabilities of AI-Empowered Cybersecurity Protection

The integrated application of these technologies ultimately refines into several core capabilities of AI-empowered cybersecurity, driving a qualitative change in the protection system.

Intelligent Threat Detection capabilities have achieved a leap from "signature matching" to "behavioral analysis." AI models no longer rely solely on signatures of known malicious code. Instead, by analyzing the behavioral patterns of entities (users, hosts, networks), even if attackers use unprecedented tools or techniques (zero-day attacks), anomalies in their behavioral patterns are sufficient to trigger alarms.

Advanced Threat Hunting capabilities have changed the previous passive mode that relied on manual queries. Security analysts can conduct in-depth trace investigations based on high-value clues output by AI, such as an unusual login time or an unconventional access to sensitive data, proactively uncovering advanced threats lurking in the network and significantly shortening the threat dwell time.

Security Situation Awareness and Prediction capabilities provide a macro-level decision-making perspective. By integrating multi-source heterogeneous data, AI can not only depict the security status of the entire network in real time but also use time-series prediction models to infer future attack trends and vulnerabilities, achieving a strategic shift from "post-incident emergency response" to "pre-incident early warning," guiding the prioritization of security resources.

Automated Response and Decision Support capabilities are the final step in building a closed-loop security system. Combined with Security Orchestration, Automation and Response (SOAR) platforms, AI systems can automatically handle low-to-medium risk security incidents with scripted playbooks (e.g., isolating devices, blocking IPs). For high-risk, complex incidents, AI provides analysts with root cause analysis and response recommendations, significantly improving emergency response efficiency and reducing personnel burden.

3. Systematic Application Architecture of AI Technology in Cybersecurity Protection for Power Enterprises

3.1 Overall Application Framework Design

The construction of an AI-driven security protection system for power enterprises requires a collaborative architecture employing layered decoupling and data fusion. This framework comprises four logical layers: The data acquisition layer achieves extensive collection and standardized pre-processing of multi-source heterogeneous data, covering network traffic, security device logs, host terminal logs, industrial control protocol traffic, and external threat intelligence. In the production control area, lightweight probes are used to collect data, ensuring no impact on business real-time performance. All data is aggregated into a security data lake after standardized processing[6].

The intelligent analysis layer undertakes the training, inference, and scheduling of AI algorithms, utilizing a distributed computing framework to process data. The machine learning platform is responsible for feature engineering, model training, and deployment, invoking different algorithms such as LSTM and GNN based on the scenario to achieve multi-dimensional security insights. The knowledge application layer transforms analysis results into concrete actions, integrating with security subsystems such as SIEM and IPS, and presents alerts and situational intelligence on the SOC visualization interface. The collaborative response layer achieves security automation through SOAR capabilities, linking pre-defined response playbooks with AI analysis results to automatically execute response actions such as blocking IPs and isolating terminals, forming a "detection-response" closed loop.

3.2 In-depth Application Analysis of Key Scenarios

In terms of intelligent threat detection and intrusion identification, AI-based NIDS demonstrates capabilities beyond traditional rule bases. It accurately learns normal communication patterns by using unsupervised learning to model industrial control protocol traffic. Any abnormal communication, such as unauthorized write instructions, unconventional time messages, or the use of abnormal function codes, is identified in real-time as a potential attack. For encrypted traffic, deep learning models extract features from message metadata, effectively identifying hidden malicious communication[7].

User and Entity Behavior Analytics (UEBA) is central to addressing internal threats. The system establishes a dynamic behavior baseline for each entity and continuously learns normal behavior patterns through clustering algorithms and time series analysis. When behavioral deviations occur, the system calculates an abnormal risk score and generates high-confidence internal threat alerts in conjunction with contextual information, accurately detecting lateral movement or compromised hosts.

Security situation awareness and prediction rely on global data fusion analysis. Graph neural networks construct network assets, users, vulnerabilities, and other entities into a dynamic knowledge graph, visually displaying potential attack paths. Combined with external threat intelligence, the system can assess the risk of specific vulnerabilities being exploited in the power industry, enabling risk-based vulnerability prioritization. By using time series forecasting models to analyze historical data, future attack trends can be predicted, enabling a shift from passive defense to proactive early warning.

In terms of automated response and security operations (SOAR), NLP technology is used for intelligent alert aggregation and noise reduction, reducing a large number of alerts to a small number of core security events. For confirmed low-to-medium risk events, SOAR playbooks

automatically complete the handling process, such as blocking malicious IPs after querying threat intelligence. For complex events, the AI system performs root cause analysis, presenting analysts with a clear attack chain graph and the handling process recommendations, enabling intelligent human-machine collaborative security operations.

This systematic application architecture embodies the concept of defense-in-depth of AI technology in power network security protection. Through the integrated application of multiple levels and technologies, it realizes comprehensive protection against known and unknown threats and significantly improves the network security protection level of power companies.

4. Application Challenges and Countermeasures Analysis

4.1 Data Level Challenges and Countermeasures

The application effect of artificial intelligence technology in the field of power network security is highly dependent on the quality and quantity of training data. Security data generated by the power enterprise production environment has significant particularities: First, the communication protocols and behavior patterns in the industrial control network are relatively fixed, and the data variance in the normal state is small, resulting in a serious imbalance in the number of normal and abnormal samples. The scarcity of abnormal samples makes it difficult for supervised learning models to obtain sufficient training. Second, due to security and reliability considerations, there are many restrictions on data collection in the production control area, and a large amount of key data only flows within the isolated network, making it difficult to obtain sufficient labeled data. In addition, the data generated by the power business system contains a large amount of noise and missing values, and the log formats of different manufacturers' equipment are inconsistent, which brings great challenges to data preprocessing.

Addressing these challenges requires a multi-dimensional strategy. Adopting a federated learning framework can realize multi-party joint modeling without aggregating raw data. Each power plant station trains local models and only uploads model parameter updates, which effectively solves the data island problem. To address sample imbalance, generative adversarial networks (GAN) can be used to generate high-quality minority class samples, or focal loss functions and other technologies can be used to improve the model's attention to minority classes. At the same time, it is necessary to establish a unified power industry security data standard, formulate standardized log formats and interface protocols, and provide a high-quality data foundation for AI model training.

4.2 Model Level Challenges and Countermeasures

The interpretability of AI models in power network security applications is extremely high. The "black box" characteristics of neural networks and other deep learning models are fundamentally contradictory to the requirement for transparency in the decision-making process in the power security field. It is difficult for operation and maintenance personnel to understand why the model judges a certain operation as abnormal. This opacity may lead to distrust of the AI system, which in turn affects its deployment in key businesses. In addition, the power network environment is dynamic, and equipment updates and system upgrades will cause changes in data distribution, resulting in concept drift, which causes the performance of offline training models to rapidly degrade.

Solving these challenges requires starting from two dimensions: model design and operation and maintenance processes. Using interpretable artificial intelligence (XAI) technology, such as LIME and SHAP, can provide post-hoc explanations of model decisions, providing feature importance rankings and decision-making basis visualization. In terms of model architecture selection, priority

can be given to models with strong inherent interpretability such as decision trees and logistic regression, or interpretable components such as attention mechanisms can be introduced into deep networks. To address the concept drift problem, it is necessary to establish a continuous learning mechanism for the model, so that the model can adapt to environmental changes through online learning or incremental learning methods, and at the same time, a strict concept drift detection mechanism should be set up to trigger model updates in a timely manner.

4.3 Environment and Adversarial Challenges and Countermeasures

The power industrial control environment places strict demands on the reliability and real-time performance of AI systems. Security detection in the production control area must be completed within milliseconds, and false positives may cause unnecessary system downtime or misoperation, resulting in significant economic losses. A more severe challenge comes from adversarial attacks, where attackers can deceive AI models with carefully constructed input samples, causing them to misjudge malicious traffic as normal behavior. Such attacks pose a serious threat to machine learning-based detection systems.

Addressing these challenges requires a defense-in-depth strategy. In production control areas with extremely high real-time requirements, model compression and knowledge distillation techniques can be used to significantly reduce computational complexity while maintaining detection accuracy, meeting millisecond-level response requirements. Establishing a multi-model collaborative detection mechanism can improve the system's robustness and reduce the risk of a single model being deceived through ensemble learning. For adversarial attacks, adversarial training techniques can be used to introduce adversarial samples during the training process to improve model robustness, while deploying auxiliary models specifically for detecting adversarial samples. Maintaining a "human-in-the-loop" mode in critical decision-making links, using AI systems as auxiliary decision-making tools rather than fully automated systems, ensures the reliability of the final decision.

4.4 Management and Compliance Challenges

The introduction of AI systems brings significant changes to the existing security management system of power companies. Traditional security operation and maintenance processes are difficult to adapt to the AI-driven automated response mode, requiring a redefinition of personnel responsibilities and disposal processes. New operation and maintenance requirements such as model version management, testing and verification, and monitoring and auditing increase management complexity. In terms of compliance, the AI decision-making process needs to meet the requirements of the Cybersecurity Law, the Data Security Law, and Level Protection 2.0 and other regulations to ensure auditability and traceability.

To this end, a comprehensive AI system governance framework needs to be established. Enterprises should develop a full lifecycle management model that covers all stages such as development, testing, deployment, monitoring and retirement. This model can continuously monitor the system, track key indicators such as accuracy and false alarm rate, and set up a performance degradation warning mechanism. In terms of compliance, this model can ensure that the decision-making process of the artificial intelligence system retains complete audit logs to meet regulatory requirements. At the same time, enterprises should also strengthen personnel training so that the security operation and maintenance team can understand and effectively use the artificial intelligence system to achieve the best efficiency of human-machine collaboration.

5. Conclusion

This study systematically explores the innovative applications of artificial intelligence technology in cybersecurity protection for power companies. By constructing a hierarchical and decoupled systematic application framework, it deeply analyzes the implementation paths of AI technology in key scenarios such as intelligent threat detection, user behavior analysis, security situation awareness, and automated response. The research shows that AI technologies such as machine learning and deep learning can effectively cope with new network threats faced by power systems, and achieve accurate identification and rapid response to known and unknown threats. Especially in the field of industrial control system security protection, behavior-based anomaly detection technology demonstrates significant advantages over traditional feature matching methods. At the same time, the study also reveals the key challenges faced in the AI application process, such as data quality, model interpretability, and adversarial attacks, and proposes corresponding strategies to address them.

References

[1] Liu Haiyan. Application and Practice of Artificial Intelligence Technology in Cybersecurity Protection of Power Enterprises [J]. Electrical Equipment and Economy, 2024, (06): 126-129.
[2] Xiang Ying, Han Xuan. Analysis of Cybersecurity Risks in the Application of Artificial Intelligence Technology in the Power Industry [J]. Information Security and Communications Privacy, 2023, (10): 67-74.
[3] Xu Bo. Application of Artificial Intelligence in Cybersecurity Situation Awareness of Power Enterprises [J]. Cybersecurity & Informatization, 2023, (06): 52-54.
[4] Liu Junhong, Zhang Qi, Wei Wenfeng, et al. Application of Artificial Intelligence in Cybersecurity Situation Awareness of Power Enterprises [J]. Cybersecurity & Informatization, 2021, (12): 126-130.
[5] Fang Xueqin, Fu Fangquan, Zhang Jiajun. Analysis of the Application of Artificial Intelligence Technology in Cybersecurity Operation and Maintenance of Power Enterprises [J]. Network Security Technology & Application, 2021, (03): 104-106.
[6] Liu Mengxu, Tu Weizheng. Discussion on the Method of Optimizing Power Communication Network Operation and Maintenance Management by Utilizing Big Data and Artificial Intelligence [J]. Information Recording Materials, 2025, 26(01): 41-43.
[7] Sun Zefeng. Research on the Application of AI in Cybersecurity Protection of Power Informationization Systems [J]. China High and New Technology, 2025, (12): 104-105+108.