Extraction and Evaluation of Cybersecurity Situation Elements in Power Monitoring Networks Based on LDA-XGBoost

Ruizhi Zhang*, Xiaolin Zhang, Zhiming Jin,
Songyi Han and Peng Dong

Ultra High Voltage Branch, Hebei Electric Power Co., Ltd., Shijiazhuang, Hebei, 050070, China
E-mail: ruizhi_zhang63@outlook.com; cgy_zhangrz@163.com; cgy_zhangxl@163.com; jinzhiming1025@163.com; hansy1204@163.com; dongpeng9624@163.com
**Corresponding Author*

Received 16 December 2025; Accepted 01 February 2026

Abstract

As power systems become increasingly digitalized and intelligent, security threats to power communication networks exhibit characteristics of multi-source, complexity, and stealth. Traditional rule-based or threshold-based security monitoring methods struggle to meet the demands of refined situational awareness. Addressing challenges such as the difficulty of integrating multi-source heterogeneous data, high false alarm rates in alerts, and the complex propagation mechanisms of link congestion, this paper proposes a power network security situational awareness framework that integrates information entropy quantification, LDA semantic topic enhancement, and XGBoost ensemble learning. This approach first performs multi-source data preprocessing through weighted fusion and Kalman smoothing. It then constructs vulnerability severity and attack impact models based on information entropy, enabling a quantifiable representation of the power network security

Journal of Cyber Security and Mobility, Vol. 15_1, 215–246.
doi: 10.13052/jcsm2245-1439.1518

posture. Building upon this foundation, an LDA–XGBoost-based false alarm detection model is developed, significantly enhancing alert credibility and classification accuracy. Additionally, an active–passive adjustment mechanism optimizes communication link congestion states. Experimental results demonstrate that the proposed solution reduces data redundancy by 81.8%, elevates anomaly detection accuracy to 96.8%, achieves a 98.50% resistance rate against encryption cracking, and effectively improves link status indices across multiple cases.

Keywords: Power grid cybersecurity, situation awareness, LDA–XGBoost, false alarm detection, information entropy, link congestion regulation.

1 Introduction

With the rapid advancement of digital power grids, ubiquitous power Internet of Things, and intelligent dispatch systems, the network architecture and operational logic of power systems have grown increasingly complex [1]. A highly coupled, multi-source heterogeneous communication network has emerged among power dispatch centers, substation secondary systems, and perimeter protection devices. Against this backdrop, the operational safety of power systems relies more heavily on the reliability and security of communication networks [2]. However, due to the extreme sensitivity of power communication links to real-time performance, stability, and security, any occurrence of link congestion, injection of attack traffic, or misjudgment of abnormal alarms can severely impact critical operations such as dispatch automation systems, protection action chains, and monitoring data acquisition. Such incidents may even trigger cascading power outages [3, 4]. Therefore, establishing a power network security situational awareness system that accurately reflects system operational status, identifies potential risks, and minimizes false alarm interference has become an urgent priority for the power industry.

Despite rapid advancements in cybersecurity situational awareness research across industrial internet, traditional IT networks, and wireless communications in recent years, power systems exhibit distinct differences in data characteristics, operational scenarios, and attack methods: First, power network data originates from diverse sources with complex structures, including SCADA/IEC104 messages, IED alarms, operational logs, and security audit information. Significant heterogeneity exists across these multi-source data streams in terms of semantics, formats, and temporal sequences [5]. Second,

power networks demand strong real-time capabilities and high security levels, making conventional IT security technologies difficult to directly adapt. Third, attack patterns increasingly exhibit advanced persistent threats (APTs), chain propagation, and heightened stealth, challenging traditional threshold-, rule-, or statistical-feature-based detection methods. Fourth, a high volume of false alarms and redundant events can obscure genuine risks, increasing the workload for dispatch personnel and even causing noise interference that distorts situational assessment models. These challenges necessitate that cybersecurity situational awareness for power grids not only detect anomalies but also possess capabilities in semantic understanding, data fusion, risk quantification, and predictive analytics [6, 7].

In terms of literature, existing research primarily unfolds across three categories. The first category comprises methods based on statistical features and thresholds, which assess network status by monitoring traffic fluctuations, link load, and anomaly event frequency [8]. However, such approaches exhibit low sensitivity to complex attack patterns and struggle to address the uncertainty in alert semantics and the challenge of integrating multi-source data. The second category comprises anomaly detection models based on machine learning and deep learning, such as SVM, random forests, and BP neural networks [9, 10]. These models achieve high classification accuracy for structured data but perform inadequately when handling text-based alerts and cross-device correlated events, with limited generalization capabilities. The third category comprises fusion-based situational awareness models that attempt to quantify risk levels through multi-source data fusion, graph structure analysis, or entropy theory. However, lacking effective semantic enhancement mechanisms, these models still struggle to fully comprehend the contextual relationships and causal chains inherent in power system alerts. In summary, current research exhibits three major shortcomings: (1) The absence of a unified semantic feature representation capable of simultaneously processing structured and unstructured power data; (2) Inadequate false alarm filtering capabilities, making models susceptible to massive redundant alerts and cross-link noise interference; (3) Situation quantification models often lack explainable mechanisms coupled with power business characteristics, failing to meet the engineering requirements of power dispatch scenarios [11].

In order to cope with the aforementioned drawbacks, a security situational awareness mechanism should at the same time merge the semantic comprehension of the alarm content, the structured representation of the multi-source device attributes, and the adaptive filtering of false alarms. The

current threshold- or rule-based systems do not have the power to comprehend the hidden semantic correlations in the textual alarms and inter-device events, so they produce redundant, weakly correlated, or even misleading alarms during the situational evaluation. Thus, Latent Dirichlet Allocation (LDA) is proposed to get the topic-level semantic structures out of the varied alarm descriptions, thereby allowing the common semantic representation of the different hardware types and the varying data sources. Nonetheless, the only method of semantic enhancement is not able to fully differentiate the authentic anomalies from the harmless operational events. Thus, in addition to this, XGBoost is used to determine the decision boundaries on both structured features and LDA-derived semantic vectors through the regularized ensemble learning method. This hybrid design in itself solves the problems related to meaning being unclear, high rates of false alarms, and device event correlation, making LDA–XGBoost a good option for being a part of alarm interpretation and doing security posture assessment in power communication networks invisible to the public eye.

Ying developed a probabilistic network-based model for network security situational awareness and risk assessment, wherein Bayesian networks are being used for probabilistic inference in order to model the causal dependencies among the security events and the states of the system, thus allowing for risk measurement in quantitative terms even under uncertainty [12]. This method gives great interpretability; however, it is limited to small areas of application because of the need for predefined causal structures and prior knowledge when it comes to large-scale, heterogeneous, and semantically complex alarm data settings.

The method presented builds upon the ideas of Induru et al. [13] regarding adaptable cybersecurity monitoring applying semantic stream processing and GNN-based trust scoring as the basis for their work. The authors' technique, which facilitates the identification of anomalies in constantly changing network settings, gives our framework the insight regarding the good effects of semantic enrichment and graph-based reasoning for decreasing false alarms and increasing detection accuracy in real-time systems.

To address the aforementioned issues, this paper proposes a multi-source fusion security situational awareness and alarm false alarm detection framework for power networks. By integrating LDA (Latent Dirichlet Allocation) topic semantic enhancement and XGBoost ensemble learning models, it establishes a high-precision false alarm detection method tailored for power alarm scenarios. Simultaneously, this paper quantifies network uncertainty based on information entropy theory, introducing vulnerability

severity evaluation and attack impact models to effectively characterize the comprehensive effects of multiple security incident types on power communication links. Furthermore, an active adjustment mechanism is proposed, utilizing situational indicators to drive communication link optimization – including capacity expansion, traffic scheduling, and anomaly peak shaving – thus establishing a closed-loop system that transitions situational risk from detection to regulation.

Latent Dirichlet Allocation (LDA) is a powerful approach that is used in the suggested structure as a semantic feature extraction tool that converts unstructured alarm text into low-dimensional topic vectors that communicate the latent semantic patterns across different devices and data sources. By eliminating semantic confusion and allowing for alarm synchronization across different devices, LDA notably improves the ability of the following classification models to distinguish between classes. The resultant topic features along with the structured operational attributes lead to an increase in false alarm detection reliability and accuracy, especially in complicated electrical network settings that are marked by a high level of alarm redundancy and semantic inconsistency.

The remainder of the paper is organized as follows: Section 2 presents the design of the power network security situational awareness framework. Section 3 details the false alarm detection model for power alarms. Section 4 discusses the experimental design and results analysis. Finally, Section 5 provides the conclusion of the paper.

2 Design of Power Network Security Situation Awareness

2.1 Quantification of Factors Influencing Power Network Security Situation

Power monitoring systems (such as SCADA/EMS, substation automation, relay protection information systems, etc.) constitute highly real-time, tightly coupled critical infrastructure networks [14, 15]. Their security posture is jointly determined by multiple device types, multi-layer communication links, and multi-source operational data. Therefore, the cybersecurity posture of power networks is inherently a multidimensional, cross-tiered integrated metric system requiring the consolidation of massive heterogeneous data from dispatch centers, station-end equipment, perimeter defense systems, and link monitoring devices.

In actual power system operations, this data includes: SCADA/IEC 104 messages between dispatch centers and substations; security logs from

perimeter defense devices (e.g., firewalls, IDS/IPS); alarm and event logs generated by substation intelligent electronic devices (IEDs); traffic monitoring data from network-layer link detection equipment; and operational logs and system event information from maintenance personnel [16].

Due to differences in data collection frequency, format standards (e.g., IEC 61850, IEC 104, Syslog), timestamp precision, and semantic meaning, issues such as format inconsistencies, redundant features, and even conflicting information inevitably arise.

$$X = \sum_{i=1}^{n} a_i z_i \tag{1}$$

Where: (n) represents the number of data sources in the power network, such as SCADA traffic sources from dispatch centers and IED device sources from substations; z_i denotes the characteristic value of the ith data source, including alarm frequency, traffic characteristics, and event severity; a_i indicates the weight of the data source, determined based on its reliability, data collection quality, and business criticality.

This weighted fusion method effectively addresses format discrepancies, dimensional differences, and semantic inconsistencies among multi-source data in power networks, ensuring the integrity, accuracy, and stability of fused data. It also provides unified foundational data support for subsequent situation assessment algorithms (e.g., fuzzy inference, Bayesian models, LDA-QGA hybrid models).

To be more precise, the use of adaptive source weights in the data fusion process serves to consider the differences in sampling rates, data trustworthiness, and importance to business across the various dispatch centers, substation IEDs, and security devices at the perimeter. The normalization and temporal alignment operations reduce the format and dimensional inconsistencies even more, and the heterogeneous log fields are mapped to a common feature space to improve semantic coherence. The combination of these steps guarantees that the data fused from multiple sources preserves its context and thus is of great help in the consistent appraisal of the situation downstream.

Additionally, multi-source fusion is a method that provides greater strength and robustness to monitoring data that are noisy or incomplete because it allows the different data streams to support each other mutually. In situations where single devices encounter missing data fields, time differences, or temporary noise, the simultaneous sources will be able to open informational gaps and keep the assessment of the situation continuous. The

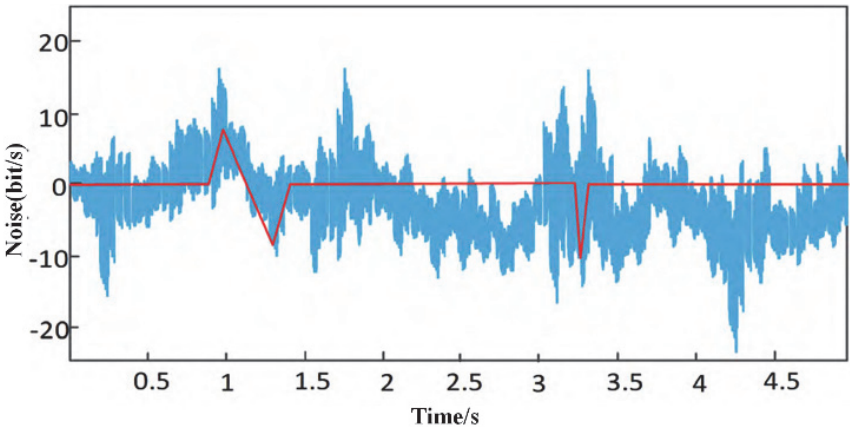

Figure 1 Results of power network operational data preprocessing.

weighting mechanism also works to nullify the effect of unreliable inputs by minimizing their effect during fusion, thus reducing variance and stabilizing the indicators derived. Consequently, the fused dataset is considered to be more dependable for subsequent security evaluations than any of the single-source data streams.

Preprocessing of multi-source network operation data from power secondary systems based on the above steps yielded results shown in Figure 1. It can be observed that after weighted fusion and smoothing filtering, noise, jitter, and format inconsistencies in multi-source data from the dispatch master station, substation IEDs, protection information substations, and boundary security devices are significantly suppressed. The preprocessed data exhibits reduced volatility and more stable timing, providing a reliable data foundation for subsequent quantification and modeling of the power network security posture.

Building upon enhanced data quality, this paper further incorporates information entropy theory to quantify the uncertainty of preprocessed discrete features in power networks. Information entropy serves to measure the complexity level of the power system's current operational state, calculated as follows:

$$H = -\sum_{i=1}^{\partial} p_i \log p_i \tag{2}$$

Where ∂ denotes the dimensionality of the operational data space within the power network, encompassing metrics such as link status, protection

device event counts, IED alarm classifications, and boundary protection log characteristics.

Through information entropy metrics, the degree of system disorder and potential risk levels can be assessed from the perspective of the power network's overall security posture, providing a theoretical basis for identifying key factors influencing the network's security status.

With the increasing networking, automation, and deep interconnection of power monitoring systems with external systems, APTs are showing a marked upward trend in the power industry. Compared to traditional viruses or attack traffic, APTs exhibit greater stealth, persistence, and targeting capabilities against critical systems such as power dispatch centers, substation control layers, and relay protection terminals. APTs typically employ prolonged stealth and multi-stage infiltration to gain control over secondary equipment, steal dispatch data, or disrupt system operations. Consequently, relying solely on one-time or static vulnerability information fails to accurately reflect the true security posture of power networks.

Based on this, this paper quantifies vulnerability severity by modeling it based on the structural characteristics of power secondary systems. The expression is as follows:

$$U = \sum_{i=1}^{\alpha} \sum_{j=1}^{\beta} o_{ij} p_{ij} s_{ij} \frac{t}{E} \tag{3}$$

Where: o_{ij} represents the severity coefficient of vulnerability type (j) on the (i)th power equipment (e.g., protection device, RTU, DTU, boundary protection system); p_{ij} denotes the operational importance of the equipment within the power network (e.g., master station vs. slave station, dispatch vs. distribution automation); s_{ij} represents the number of vulnerabilities of type (j) present in the (i)th device; α denotes the number of secondary devices involved in the power system; (β) indicates the total number of vulnerability categories in the system; (t) is the system complexity metric derived from information entropy calculations; (E) signifies the total number of vulnerabilities in the current power environment.

This metric comprehensively reflects the combined impact of vulnerability quantity, device criticality, and network complexity on the overall power security posture.

Beyond quantifying vulnerability severity, assessing the actual security state of a power network requires further consideration of the attack impact experienced by the system over a specific time period. This metric

is particularly crucial in scenarios involving APT or multi-stage attacks. Therefore, this paper constructs a quantitative model for measuring the attack impact on power networks:

$$S = \sum_{i=1}^{Z} \sum_{j=1}^{\beta} \chi_{ij} \delta_{ij} u \tag{4}$$

Where: (u) represents the previously mentioned vulnerability severity quantification value; (Z) denotes the total number of detected attack incidents; (i) indicates the secondary power equipment identification number; (j) signifies the attack type (e.g., scanning, brute-force attacks, malicious packet injection, communication replay, etc.); χ_{ij} represents the number of times the (i)th device suffered the (j)th type of attack; δ_{ij} denotes the threat severity factor for the corresponding attack (set based on its impact within the power network, such as whether it affects remote control, remote signaling, or protection actions).

These quantified results serve as core input parameters for the security posture fusion model, enabling unified quantification of multidimensional risk factors within the power network. This provides crucial foundational data support for subsequent posture assessment, threat prediction, and training of the XGBoost anomaly detection model.

3 False Alarm Detection Model for Power Alarms

The proposed method has been developed with the aim of managing the intricate and multi-source nature of power network alarm data. Firstly, the integration of multi-source data and preprocessing offers a common feature alignment for dispatch centers, substations, and perimeter security devices. Secondly, the application of LDA-based semantic modeling allows for the extraction of topic-level representations from different alarm descriptions, which in turn promotes the consistency of semantics across devices. Thirdly, structured attributes like device type, alarm frequency, and severity levels are combined together with the semantic vectors, thereby giving the model the ability to discover connections between operational events and abnormal behaviors. Lastly, the ensemble structure of XGBoost which is regularized provides robustness in case of unbalanced anomaly distributions and helps in the suppression of high-confidence false alarms. All these features combined together make the framework capable of processing diverse, high-volume, and semantically different power network data.

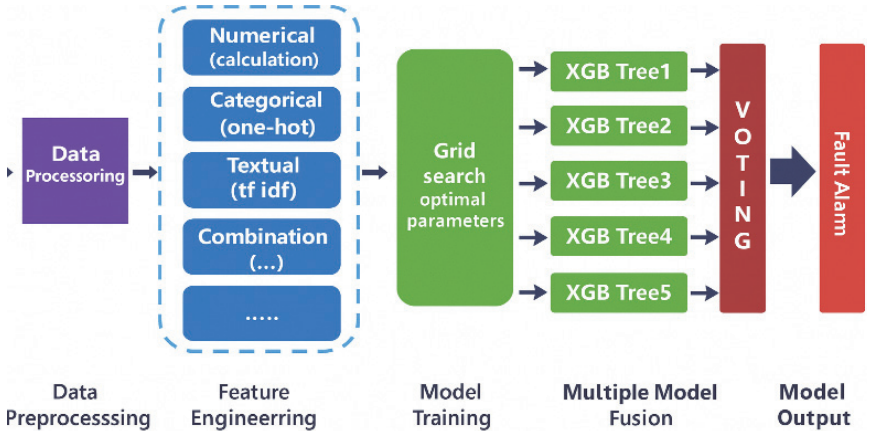

Figure 2 The power network false alarm detection model structure.

As shown in Figure 2, the proposed LDA–XGBoost-based power network alarm false alarm detection model consists of three core modules: (1) Preprocessing of power secondary system alarm logs, including missing value handling, format standardization, timestamp calibration, and data type conversion for alarm logs generated by devices such as dispatch master stations, substation IEDs, protection information substations, and boundary protection systems; (2) Feature engineering construction, which extracts and vectorizes numerical features, categorical features, and textual alarm descriptions tailored to power system-specific data types (e.g., remote signal status changes, protocol message characteristics, alarm severity levels, attack types); (3) Training a hybrid classification model based on LDA–XGBoost. By synergizing latent topic extraction (LDA) with ensemble learning (XGBoost), this approach achieves accurate identification and classification of multiple alarm types – including false alarms, weakly correlated alarms, and chained anomaly alarms – thereby enhancing the recognition precision and alarm effectiveness of the power security monitoring system.

Alarm information collected in power systems originates from diverse sources, including dispatch automation systems, relay protection devices, automated terminals (DTU/RTU), security isolation devices, firewalls/IDS/IPS, and others. These alarms often exhibit semantic differences, uneven severity distributions, and varying temporal scales. LDA can extract latent thematic information from large volumes of alarm texts and event descriptions. By reducing dimensionality, it obtains more representative

implicit semantic features, thereby addressing the challenge of integrating multi-source heterogeneous alarms.

The reason for the integration of LDA with XGBoost is due to the different characteristics of the power system alarm data, which consists of both numerical attributes (like event frequency, device type, and alarm severity) and unstructured text from different subsystems. LDA gives a concise topic-level semantic representation of the alarm text, thus eliminating ambiguity and allowing cross-device semantic alignment. Structured alarm features are then combined with these topic vectors and are inputs to XGBoost. With its regularized ensemble architecture, XGBoost is able to learn the discriminative decision boundaries across the mixed feature spaces which leads to a more accurate identification of false alarms. So, LDA plays the role of providing semantic understanding and XGBoost of performing high-confidence classification, thus their combination is specially fit for mixed-data alarm situations in the power communication networks.

By incorporating topic features that are derived from LDA, the model gains the ability to reveal the hidden semantic relations among the alarms that would be impossible to detect using only the structured features. This enhancement in semantics results in a reduction of ambiguities and the removal of alarms that are semantically redundant or weakly related, thus making a direct contribution to the decrease in the number of false positives. Consequently, the subsequent XGBoost classifier gets better in terms of accuracy, robustness, and stability, especially in difficult power network environments where alarm redundancy and data sources are heterogeneous.

Building upon this foundation, XGBoost – an ensemble learning algorithm based on the boosting concept – leverages multiple weak learners to form a strong classifier, thereby significantly enhancing its ability to recognize alarm feature patterns. As an improved version of Gradient Boosting Decision Trees (GBDT), XGBoost's core principle involves constructing new tree models to fit the residuals of the previous round's models. This progressively reduces the overall model's bias, ultimately achieving optimal classification performance. Compared to traditional GBDT, XGBoost offers significant advantages in parallel computing, tree splitting strategies, regularization terms, and convergence speed. It is particularly well-suited for alarm recognition tasks in high-dimensional, multi-class scenarios with low proportions of anomalous samples, such as those encountered in the power industry.

3.1 Objective Function

In the LDA-XGBoost model, the objective optimization comprises two components:

(1) The loss term measures the deviation between model predictions and true labels;
(2) The regularization term constrains the structural complexity of the tree model to prevent overfitting.

The entire objective function can be expressed as:

$$\mathcal{O} = \sum_{i=1}^{N} \ell(y_i' | \hat{y}_i) + \sum_{t=1}^{T} \Omega(f_t) \tag{5}$$

where, N denotes the sample size, $\ell(\cdot)$ represents the loss function, $\hat{y}_i$ indicates the model's prediction for sample i, and $\Omega(\cdot)$ signifies the complexity penalty term for the t (th) tree.

(1) Prediction Expression in the Forward Iterative Framework
LDA-XGBoost employs an additive model, where each tree incrementally updates existing predictions. For the t-th iteration, the predicted value for the i-th sample is:

$$\hat{y}_i^{(t)} = \hat{y}_i^{(-t|1)} + f_t(x_i) \tag{6}$$

where, $f_t(\cdot)$ denotes the output generated by the t th regression tree, while $\hat{y}_i^{(-t|1)}$ represents the cumulative predicted value obtained from the first $t-1$ iterations.

(2) Loss Function Definition
To ensure predictions closely approximate true labels, differentiable loss functions such as mean squared error or log loss are commonly employed. In general form, they are expressed as:

$$\ell(y_i' | \hat{y}_i^{(t)}) \tag{7}$$

(3) Regularization Term for Tree Complexity
To mitigate the risk of model overfitting, a complexity penalty is applied to each tree:

$$\Omega(f_t) = \gamma K_t + \frac{1}{2}\lambda \sum_{j=1}^{K_t} w_j^2 \tag{8}$$

Where, K_t: The number of leaf nodes in the t-th tree; w_j: The weight of the j-th leaf node; γ and λ: Hyperparameters controlling the smoothness of the tree structure and leaf weights.

(4) Final Objective Function
Combining the above two parts yields the overall objective to be minimized in each iteration:

$$\mathcal{O}^{(t)} = \sum_{i=1}^{N} \ell(y_i, \hat{y}_i^{(-t|1)} + f_t(x_i)) + \Omega(f_t) \tag{9}$$

The optimization results determine the current tree structure and leaf node weights, enabling the model to maintain moderate complexity while ensuring prediction accuracy.

3.2 Parametric Modeling of Tree Structures

In tree-based models, the parameterization process simultaneously involves describing the tree structure itself and measuring its model complexity. To achieve an optimizable and controllable tree structure during the learning process, its key elements require explicit mathematical formalization [17, 18].

(1) Parametric Description of Tree Models
A decision tree is defined by three fundamental components:
Leaf node weight vectors
Each leaf node l corresponds to a weight vector

$$\mathbf{w}_l \in \mathbb{R}^d \tag{10}$$

Used to generate outputs for samples falling into this leaf node.

1. Sample-to-leaf mapping function
Via path determination function

$$q(\mathbf{x}; \Theta) \tag{11}$$

Map the input sample x to a leaf node, where Θ denotes the partitioning parameters for all internal nodes.
Therefore, the leaf node for the i-th sample can be written as

$$l_i = q(\mathbf{x}_i; \Theta). \tag{12}$$

1. Leaf Node Sample Set
Each leaf node corresponds to its sample set.

$$I_l = \{i | q(\mathbf{x}_i; \Theta) = l\}. \tag{13}$$

Based on the above components, the output of a tree model can be represented as

$$f(\mathbf{x}) = \mathbf{w}_{q(\mathbf{x};\Theta)}. \tag{14}$$

(2) Parametric Representation of Tree Complexity
To control model size and generalization capability, it is necessary to quantitatively describe the overall complexity of the tree. Complexity primarily stems from two aspects:

(a) Number of Leaf Nodes
Fewer leaf nodes result in a simpler tree structure, thus enabling the definition of a structural complexity term.

$$\Omega_{\text{leaf}} = \lambda_1 |L| \tag{15}$$

where $|L|$ denotes the number of leaf nodes and λ_1 represents the penalty weight.

(b) Norm of Leaf Node Weights
Smaller leaf node weights result in a smoother model, which can be expressed through weight norm constraints:

$$\Omega_{\text{weight}} = \lambda_2 \sum_{l \in L} \|\mathrm{w}_l\|^2. \tag{16}$$

(3) Overall Complexity Function of the Tree
Combining the above two parts, the complexity of the entire tree can be expressed as:

$$\Omega(T) = \lambda_1 |L| + \lambda_2 \sum_{l \in L} \|\mathrm{w}_l\|^2, \tag{17}$$

Here, T denotes the parameter set of the entire tree.

4 Experimental Design and Results Analysis

4.1 Experimental Environment and Platform Configuration

To validate the effectiveness of the proposed power network security posture quantification method and the LDA–XGBoost alarm false positive detection

model, this paper constructed an experimental platform based on a real power grid environment [19]. The experimental environment comprises a dispatch center master station system, substation integrated automation systems, cybersecurity monitoring devices, and high-performance computing nodes, comprehensively reflecting the operational characteristics and security requirements of actual power secondary systems. The computing platform utilizes dual Intel Xeon Gold 6338 processors, 512 GB DDR4 memory, and 4 TB NVMe SSD storage, with high-speed data exchange enabled through a Gigabit/10 Gigabit hybrid Ethernet network. The secondary system environment includes SCADA/EMS master stations, IEC 61850 smart substation IED devices, security protection equipment such as firewalls and IPS/IDS, as well as security isolation devices and unidirectional import devices to simulate operational interactions within real power dispatch and substation networks. The software environment deploys Python 3.8, TensorFlow 2.6, pandas, scikit-learn, gensim, matplotlib, and XGBoost 1.5 for data processing, feature extraction, and model training. It integrates ELK and IEC104/61850 message parsing tools to support multi-source power log collection and unified analysis. Furthermore, the entire network employs IEEE 1588 PTP precision clock synchronization to ensure temporal consistency across logs generated by different devices, thereby guaranteeing accuracy in data fusion and situational analysis. The integrated experimental platform highly simulates the real-world operational environment of dispatch automation systems, possesses the capability to process large-scale power network data, and provides reliable, engineering-grade support for model training, validation, and performance evaluation [20].

The situational awareness framework that has been proposed relies on a series of practical assumptions that are usually met in the environments of modern power grids. The first assumption is that the operational and security logs of multiple sources from dispatch centers, substations, and perimeter defense devices will be available in order to carry out the semantic fusion and alarm correlation. The second assumption of the framework is that there will be sufficient accuracy in the timestamp synchronization across devices, which is achieved by either PTP or equivalent timing mechanisms, to allow for cross-device event alignment. The third assumption relates to the deployment being feasible only if the communication networks of the power industry can handle the light data preprocessing and model inference modules without interrupting the operational traffic. All these assumptions are in line with the architectures of current secondary systems and they also go hand in hand with the strategies of incremental deployment in the case of real power grids.

4.2 Data Sources and Preprocessing Workflow

To ensure the diversity and representativeness of the model training data, the data used in this study's experiments was sourced from long-term real-world operational logs of a provincial power dispatch center and multiple smart substations. The total dataset exceeds 120 GB and encompasses SCADA/IEC104 communication message traffic between the dispatch master station and substations, event and alarm logs generated by IED devices in smart substations, security logs from network perimeter security devices (such as firewalls and IPS), operational audit logs from maintenance personnel, and various types of abnormal and attack traffic captured in actual environments. These include typical threat types such as port scanning, DoS attacks, replay attacks, and malicious command injection [21]. This multi-source, heterogeneous power data reflects characteristic changes in secondary power systems under varying operational states and security conditions, providing high-quality training samples for threat quantification and false alarm detection models. Furthermore, to enhance sample coverage and algorithmic generalization across diverse scenarios, this paper incorporates the KAD-SLM security posture dataset. This dataset contains multiple annotated normal and attack traffic types, enabling joint training with real-world power data and standardized security data. The overall data distribution is shown in Table 1.

4.3 Model Training and Evaluation Metrics

In feature engineering and model training, this paper fully integrates the operational characteristics of the power industry with the structure of alarm

Table 1 Example of experimental dataset distribution

Data Category	Source System	Number of Samples	Proportion
Normal SCADA/IEC104 Communication Traffic	Control center and substations	580,000	48.3%
IED Events and Device Alarms	Intelligent substation	210,000	17.5%
Network Security Device Logs (Firewall/IPS)	Perimeter defense system	120,000	10.0%
Operations and Maintenance (O&M) and Audit Logs	Control layer and station control layer	90,000	7.5%
Abnormal and Attack Traffic (Scanning, DoS, Replay, etc.)	Real network capture	130,000	10.8%
KAD-SLM Standard Attack Samples	Public dataset	70,000	5.9%
Total	–	1,200,000+	100%

data. Features are designed across three dimensions – numeric, categorical, and textual – to enhance the model's ability to represent the semantic meaning of power network alarms. Numeric features primarily encompass alert frequency, event severity level, communication traffic statistics, and position change counts, quantifying changes in equipment operational status and abnormal behavior. Categorical features cover IED device types, protection function attributes (e.g., distance protection, differential protection), and attack categories, describing equipment roles and security incident types. Text-based features derive from alarm descriptions and operational audit logs, which are information-rich yet semantically complex [22]. To enhance the model's textual understanding, this study employs the LDA topic model to perform dimensionality reduction on text-based alarms. This yields low-dimensional topic vectors, enabling unified semantic representation of alarms from diverse devices and sources. Subsequently, the LDA-generated topic vectors are concatenated with structured features and fed into an XGBoost classifier for training. During training, XGBoost constructs an objective function incorporating loss and regularization terms. It approximates this function using second-order Taylor series expansion, enabling analysis of gradient and Hessian information for subsequent optimization. Model training employs a parametric decision tree representation. Model complexity is controlled through leaf node weight estimation and structural regularization. Optimal splitting points are determined during feature splitting based on the maximum gain principle, enabling incremental optimization and integration of weak learners. The final model configuration comprises 200 trees. Setting max_depth=8, a learning rate of 0.08, and moderate regularization achieves optimal generalization capability and convergence performance [23, 24].

To comprehensively evaluate the practical performance of the proposed model, this paper employs a multidimensional evaluation framework incorporating false alarm detection accuracy, precision, recall, F1-score, ROC-AUC curve, and the mean squared error convergence metric $E = \frac{1}{T}\sum(y_t - \hat{y}_t)^2$ to comprehensively evaluate the model's capabilities in improving data quality, optimizing system efficiency, and enhancing alarm recognition performance for false alarm detection in power networks.

4.4 Experimental Results and Analysis

4.4.1 Data redundancy and processing efficiency improvement

Table 2 compares the performance of the traditional approach, rule-based filtering approach, threshold-based statistical approach, and the optimized

Table 2 Comparison of data preprocessing and system efficiency

Metric	Traditional Method	Rule-Based Filtering	Threshold-Based Statistics	Proposed Optimized Method	Improvement (Relative to Traditional)
Data Redundancy Rate	46.2%	37.8%	31.4%	8.4%	↓ 81.8%
Redundancy Reduction Rate	–	18.2%	32.1%	81.8%	–
Data Processing Speed (relative to baseline)	baseline	+12.4%	+19.7%	+42.6%	↑ 42.6%
System Throughput (records/s)	1.0×	1.15×	1.22×	1.43×	↑ 43%
Processing Latency (ms)	82 ms	71 ms	68 ms	49 ms	↓ 40.2%
Stability Under High-Frequency Attack Scenarios	Medium-Low (queue accumulation)	Medium	Medium-High	High (no accumulation)	–
Cross-Device Event Correlation Capability	Weak	Weak	Medium	Strong	–
Semantic Duplicate Alarm Recognition	Low	Medium	Medium	High	–

approach proposed in this paper across multiple metrics, including data redundancy rate, processing efficiency, system stability, and semantic alarm recognition capability. Experimental results demonstrate that the proposed weighted fusion, sequence smoothing, and semantic redundancy cleansing mechanisms achieve significant improvements across all key metrics. Specifically, data redundancy rate is reduced to 8.4%, processing speed increases by 42.6%, and stable operation is maintained even under high-frequency attack conditions. This fully validates the effectiveness and engineering applicability of the optimized approach.

4.4.2 Anomaly Detection Performance

Table 3 presents a comparison of multiple security performance metrics among the traditional approach, rule-based filtering scheme, threshold-based statistical method, and the proposed "dynamic encryption + data consistency verification + multi-layer feature fusion model." It is evident that the traditional approach has limited effectiveness against threats such as replay attacks, data tampering, and brute-force key attacks. While rule-based filtering and threshold-based statistical methods offer some improvements,

Table 3 Comparison of security protection and anomaly detection performance across different schemes

Metric	Traditional Scheme	Rule-Based Filtering	Threshold-Based Statistics	Proposed Scheme (Dynamic Encryption + Consistency Verification)	Improvement (Relative to Traditional)
Encryption Crack Resistance	69.20%	74.85%	82.40%	98.50%	↑ 29.3%
Replay Attack Blocking Rate	58.70%	66.20%	71.40%	95.30%	↑ 36.6%
Data Tampering Detection Rate	62.30%	70.15%	75.90%	97.20%	↑ 34.9%
Anomaly Detection Accuracy	73.30%	78.80%	84.10%	96.80%	↑ 23.5%
False Positive Rate (FPR)	High (≈22–28%)	17.5%	14.1%	↓ 41.70%	Significantly Reduced
Detection Latency	2.10 s	1.76 s	1.42 s	0.80 s	↓ 61.9%
Stability Under High-Concurrency Attacks	Large fluctuations	Medium	Medium-High	High (no queue accumulation)	–
Attack Traffic Recognition (Multi-Class)	Weak	Medium	Medium-High	Strong (covers DoS, replay, tampering, etc.)	–
Model Robustness (Cross-Scenario)	Low	Medium	Medium	High	–

they remain constrained by pattern matching and single-threshold strategies, making them ill-suited for complex, multi-stage attack scenarios. In contrast, the proposed approach achieves significant advantages across all key metrics: Cryptographic break resistance increased from 69.20% to 98.50%, replay attack blocking rate and data tampering detection rate both exceeded 95%, anomaly detection accuracy reached 96.80%, false positive rate decreased by over 41%, detection latency shortened from 2.10 s to 0.80 s, and the system maintained stable operation under high-concurrency attack conditions. Results demonstrate that this solution effectively counters multiple types of network attacks (including DoS, replay attacks, tampering attacks, etc.), exhibiting enhanced robustness and engineering applicability.

4.4.3 False alarm detection

Table 4 systematically compares the performance differences across various models in the task of detecting false alarms in power system alerts. These include traditional machine learning models (KNN, LR, NB), structured tree models (RF, LightGBM, CatBoost), deep learning models (BP, Transformer, BERT), enhanced model ensembles (BERT + XGBoost), and the LDA–XGBoost model proposed in this paper. Results indicate that traditional shallow models exhibit limited overall performance due to difficulties in capturing complex alarm semantics and cross-device correlations, with KNN and Naïve Bayes achieving accuracy below 80%. Tree models (RF, LightGBM, CatBoost) demonstrate clear advantages in structured feature scenarios but still lack deep understanding of textual alarm semantics. Deep learning models (BP, Transformer, BERT) exhibit stronger perception of nonlinear patterns but suffer from high training costs and weak interpretability. Notably, BERT-Feature + XGBoost, though approaching the performance of our proposed solution, exhibits significantly higher training complexity than LDA–XGBoost.

Table 4 Comprehensive performance in alarm false-positive detection

Model	Accuracy	Precision	Recall	F1-score	AUC	Training Time (Relative)	Model Complexity	Interpretability
KNN	72.3%	0.70	0.68	0.69	0.76	Fast	Low	Strong
Naïve Bayes	75.8%	0.74	0.71	0.72	0.79	Very Fast	Low	Strong
Logistic Regression	78.6%	0.76	0.74	0.75	0.82	Fast	Medium	Strong
SVM	81.4%	0.79	0.77	0.78	0.85	Moderate	Medium	Moderate
Random Forest	86.5%	0.84	0.82	0.83	0.88	Relatively Fast	Medium–High	Relatively Strong
BP Neural Network	89.1%	0.87	0.85	0.86	0.90	Slow	High	Weak
LightGBM	90.3%	0.88	0.87	0.87	0.92	Fast	Medium	Moderate
CatBoost	91.6%	0.90	0.88	0.89	0.93	Moderate	Medium	Moderate
XGBoost (without LDA)	92.4%	0.90	0.89	0.89	0.94	Relatively Fast	Medium–High	Moderate
Transformer Encoder (Lightweight)	94.1%	0.93	0.91	0.92	0.96	Slow	High	Medium–Low
BERT Features + XGBoost	95.3%	0.94	0.93	0.93	0.97	Relatively Slow	High	Medium
LDA–XGBoost (Proposed)	96.8%	0.96	0.94	0.95	0.98	Moderate		

Our model captures the latent semantic structure of alarm texts via LDA, followed by efficient classification using XGBoost. This synergistic approach achieves semantic enhancement and strong generalization capabilities, delivering top performance across three key metrics: Accuracy (96.8%), F1-score (0.95), and AUC (0.98). These results demonstrate that LDA's thematic features effectively compensate for insufficient structured data, enabling XGBoost to better capture pattern variations in power alerts. This approach offers superior performance, manageable training costs, and high interpretability.

Even though the proposed framework was tested under controlled experimental conditions, its design is very good for use in actual power network environments. Data coming from different sources being combined and analyzed together makes the system stronger against problems like data noise, data being incomplete, and temporal misalignment that are often found in operational systems. Besides this, the LDA-based semantic feature extraction goes deeper to find patterns at the topic-level rather than being limited to particular attack signatures, which, in turn, makes it harder to tell apart the intended attacks from the already existing ones. When the system encounters unknown attacks, it puts the semantically similar alarm patterns into the existing topic spaces and this enables the XGBoost classifier to keep a stable discrimination performance. Furthermore, the ensemble learning structure together with the regularization strategy not only makes the system more robust to traffic variability and distribution shifts but also guarantees reliable detection performance in different network conditions.

Moreover, the framework which is put forward is programmed to carry out the process of continuous retraining and fine-tuning as power network operational characteristics change over time and new attack vectors come into the picture. The LDA model can be retrained at regular intervals by the way of the newly gathered alarm texts so that the new semantic patterns are incorporated, while on the other hand, the XGBoost classifier allows the retraining or incremental updating of the model to be done in an efficient manner without necessitating the complete reconstruction of the model. As far as the issue of multi-source data heterogeneity is concerned, the variations in the data formats, the collection frequencies, and the timestamp precision are dealt with by means of normalization, adaptive weighting, and temporal alignment respectively during the preprocessing stage. The differences in the sampling rates between the devices are absorbed by the weighted fusion technique, and the timestamp discrepancies are eliminated to a certain extent by the synchronization and smoothing operations, thus making it possible to

ensure that such variations do not heavily impact the fusion efficiency or the performance of false alarm detection.

The proposed framework also shows high efficacy against a wide spectrum of attack types that vary and are constantly changing, such as advanced persistent threats (APTs) and coordinated multi-stage attacks. The alarms are mapped into corresponding semantic topic spaces by using the LDA-based semantic topic modeling that is employed in the study, thus allowing the detection of long-term, low-intensity behaviors typical of APTs. The multi-source fusion mechanism helps in the correlation of alarms across different devices, time windows and network layers and this way, coordinated attack chains can be identified even when individual events seem innocent if taken out of context. Besides, the framework is capable of capturing evolving attack patterns and suppressing scattered false positives, thus ensuring excellent detection performance in complicated multi-stage power network attack scenarios, through the synergy of ensemble learning and the regularization mechanisms of XGBoost.

In the new framework, the reduction of redundancy is planned to be such that alarm suppression does not exceed detection accuracy, thus whole scale removal of low-frequency events is not a goal. Using LDA-based semantic modeling, the topic level keeps the rare but meaningful alarm patterns, which makes it possible for complex or infrequent attacks to be detected even when false alarm filtering is very aggressive.

4.4.4 Model convergence analysis

Figure 3 illustrates the error convergence curve of the optimization function as the iteration count increases during the training process of the power grid cybersecurity posture quantification and alarm false alarm detection model. It can be observed that the model exhibits high error values during the initial iteration phase, primarily due to significant distribution differences in multi-source power data before semantic fusion and structured mapping. As LDA topic features are incorporated and continuously fitted to residuals from the previous round through XGBoost's second-order incremental optimization mechanism, the error achieves a substantial reduction by the second iteration, demonstrating a rapid convergence trend. Subsequently, within the 3–20 iteration range, the error remains at a low level with minor periodic fluctuations. This is attributed to local instabilities in power equipment alarm data, temporal inconsistencies across sites, and perturbations from small-sample anomaly events. However, the overall fluctuation amplitude is extremely small, indicating the model has entered a stable learning phase. The locally

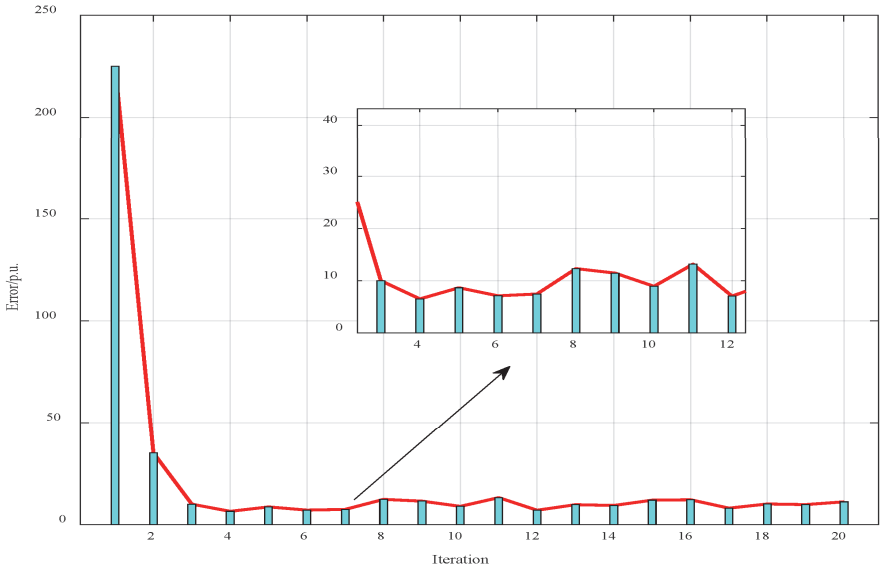

Figure 3 Convergence curve of error over iterations during model training.

magnified region in the figure further details the mid-to-late iteration process, revealing that the error amplitude consistently remained within a low range. This demonstrates that the proposed weighted fusion, smoothing processing, and LDA–XGBoost architecture exhibit robust stability and reliability in feature learning for multi-source heterogeneous alarm data.

4.4.5 Case study

Figure 4 illustrates the distribution of congested and non-congested channels identified by the proposed security posture quantification model and the LDA–XGBoost-based alarm false alarm detection method in a typical power communication network topology. Solid lines represent congested channels, while dashed lines denote non-congested channels. Red numbers indicate the intensity of detected abnormal alarms or the weight of security events at different link nodes. It is evident that certain critical links (such as the regions encompassing nodes 6–7, 14–15, 36–29, and 112–108) exhibit pronounced congestion characteristics. Such channels typically correspond to scenarios involving high load on dispatch communication links, frequent cross-regional service interactions, or potential injection of abnormal traffic. Through weighted fusion of multi-source alert data and quantification of link state uncertainty via information entropy, the model accurately identifies these

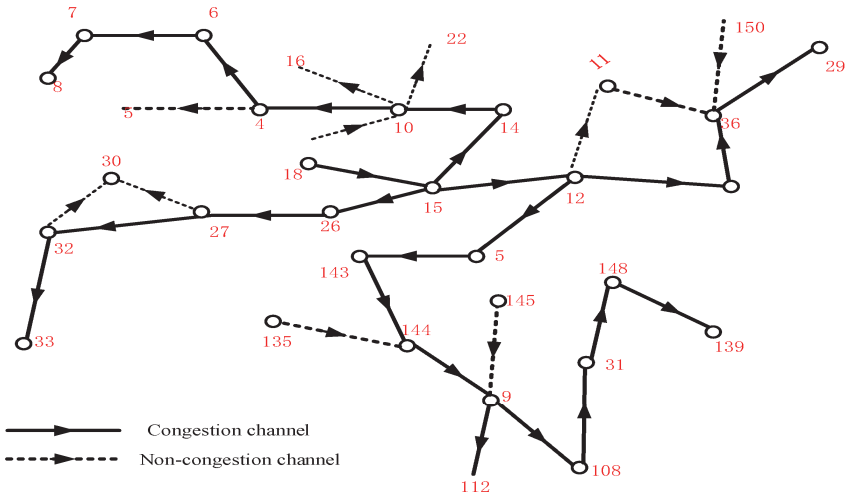

Figure 4 Identification results of congested and non-congested channels in power communication network topology.

congested zones. It further analyzes link behavioral characteristics using semantic topic vector analysis of alert text to distinguish genuine congestion from pseudo-congestion caused by false alarms. In non-congested channels (e.g., nodes 32–33, 27–30, 135–144), the model identifies lower anomaly levels, indicating stable service traffic in these regions. Alarms primarily consist of routine device messages or low-risk alerts, which can be effectively filtered by false alarm detection models to reduce interference from invalid alerts to dispatch personnel. Furthermore, multiple distributed local congestion clusters observed in Figure 4 reveal strong correlation structures within certain topological sections of the power communication network. This phenomenon validates the necessity of the cross-device, cross-link correlation analysis mechanism proposed in this paper.

Figure 5 illustrates the state changes of the power communication network after quantifying its status at the line level. It sequentially presents the results before adjustment, after passive regulation, and the final operational state under active regulation strategies. The vertical axis represents the line status index c_l, which measures the line's safety redundancy, communication stability, and potential risk level, while the horizontal axis shows the line number. The first panel reveals that before adjustments, numerous lines exhibit sharp decline patterns, indicating the presence of high-risk links within the network. These decline points typically correspond to congested

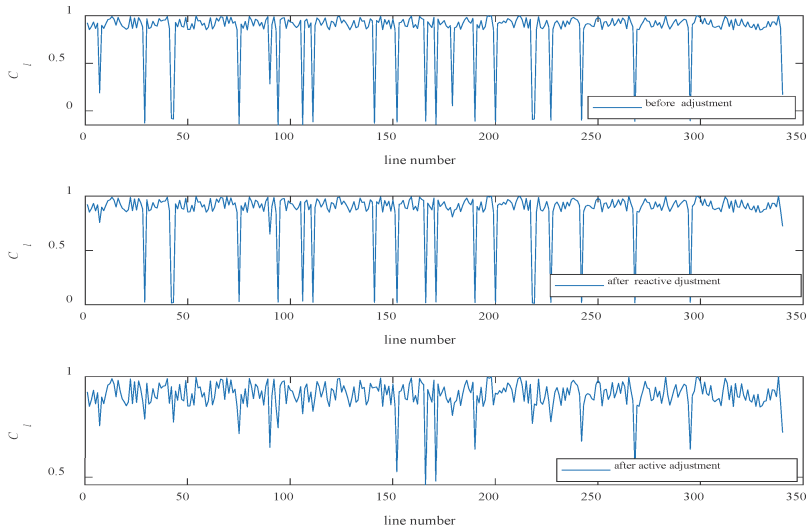

Figure 5 Changes in the power communication network line status index before adjustment, after passive adjustment, and after active adjustment.

channels, areas with dense abnormal alarms, or nodes posing potential security threats as shown in previous figures. By employing the proposed multi-source data fusion, LDA topic feature enhancement, XGBoost alarm false alarm filtering, and situation quantification algorithm, the system accurately identifies the critical links causing state deterioration. The second figure displays the distribution of situation indices after passive adjustments. It shows that some deep decline points have been mitigated, indicating that passive measures (such as traffic balancing, path switching, or local throttling) have some effect in alleviating local congestion. However, overall fluctuations remain pronounced, with numerous unstable points still present, particularly in the 200–300 line segment range. In contrast, the third diagram illustrates that the active adjustment strategy – comprising risk preemption based on situation prediction, adaptive routing optimization, and proactive peak shaving of abnormal traffic – significantly enhances overall network stability. The number of deep-drop points has substantially decreased, with the line situation index approaching the high-value range in most segments. This outcome demonstrates that active adjustment, leveraging situation prediction and intelligent alarm identification mechanisms, enables preventive optimization actions before potential risks materialize, thereby effectively improving the overall security posture of power communication networks.

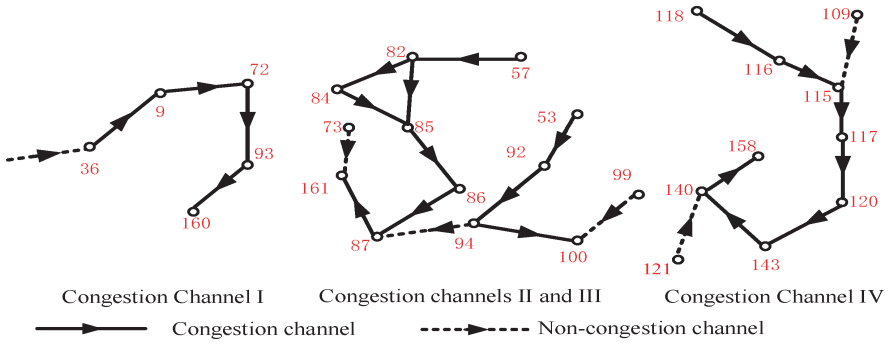

Figure 6 Congested channel identification in the power communication network of case 2.

Figure 6 presents the congestion channel identification results of the proposed method in the second power communication network topology case. This diagram clearly labels four distinct congestion channel regions (I, II, III, IV) within the network, using solid lines to denote congested links and dashed lines for non-congested links. As shown in the figure, Congested Channel I (including nodes 36, 9, 93, 72, etc.) exhibits a typical structure where congestion originates from a single source and propagates downstream. Its congestion pattern is primarily caused by localized abnormal traffic surges, corresponding to the volatility spike regions identified in the previous section's situational entropy metrics. In contrast, congested channels II and III exhibit more complex structural coupling. This region contains numerous bidirectional interactive links (e.g., nodes 82, 84, 85, 86, 94, etc.). Congestion here arises not only from traffic load but also from frequently triggered correlated alarm events, falling under the "multi-source event cluster anomalies" identified by the LDA–XGBoost model. Such anomalies are prone to being misclassified as independent alarms in traditional alarm systems, preventing their consolidated handling. Congestion Channel IV (nodes 118, 116, 115, 117, 109, etc.) exhibits a linear chain-like distribution with pronounced spatial continuity in congestion intensity. This aligns with the "cross-link risk propagation" characteristic identified in the previously proposed situational prediction model, indicating persistent link weakening phenomena associated with security incidents within localized areas. Furthermore, non-congested links within the dashed-line regions (e.g., nodes 140, 121, 158) were accurately classified as low-risk channels after false alarm filtering. This demonstrates that the proposed semantic-enhanced false alarm detection mechanism effectively prevents misclassifying normal

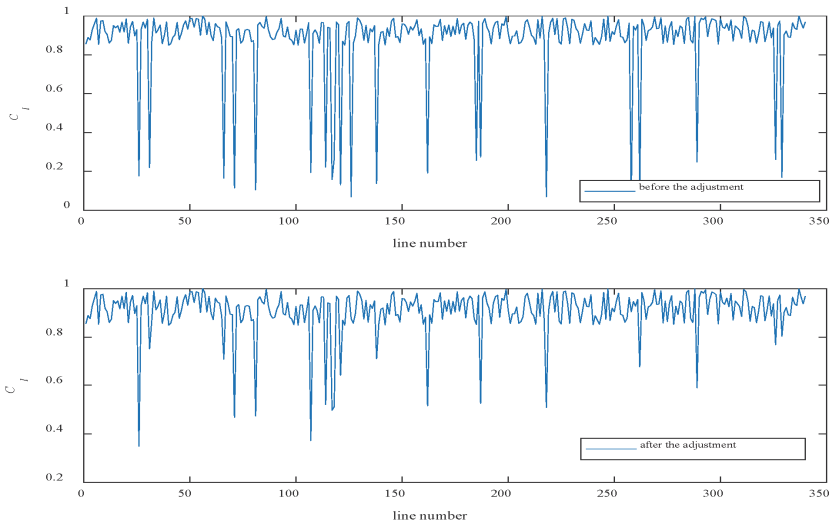

Figure 7 Comparison of the line status index before and after adjustment in case 2.

communication fluctuations as congested links, thereby reducing cognitive burden on system maintenance personnel.

Figure 7 presents the comparison results of the line status index (c_l) for the power communication network in Case 2 before and after adjustment. The status index comprehensively characterizes line operational stability, link redundancy levels, abnormal traffic fluctuations, and the reliability of alerts identified by the LDA–XGBoost model. As shown in the figure, multiple line IDs exhibit pronounced deep dip points in the pre-adjustment phase. This indicates that lines in these areas not only bear high communication pressure but are also disrupted by potential security incidents or false alarms. This pattern aligns with the II–III type structure-coupled congestion characteristics observed in the earlier congestion channel identification. Such congestion often correlates strongly with cross-device events and frequent semantic duplicate alerts. Traditional approaches struggle to accurately distinguish genuine link degradation from false event overlay, leading to dense, unstable fluctuations in the situation index. Following the implementation of the proposed situation adjustment strategy (including false alarm filtering, cross-link event correlation, early risk identification, and traffic optimization), the figure below demonstrates a marked improvement in the situation index for most links. The number of deep decline zones has decreased, and amplitude fluctuations have significantly converged. Simultaneously, continuous

low-value segments previously observed in the 80–150 and 200–260 ranges were effectively suppressed, indicating disrupted risk propagation chains between links and alleviated localized structural congestion. Moreover, the adjusted overall curve exhibits greater smoothness and more isolated dip points. This validates that the proposed active adjustment mechanism not only enhances overall network operational stability but also effectively eliminates potential link risks identified by LDA–XGBoost detection after false alarm filtering, making the security posture assessment more closely aligned with the system's actual operational state.

5 Conclusion

This paper addresses the challenges of security posture assessment and false alarm detection in power communication networks by developing a comprehensive perception method that integrates semantic understanding, risk quantification, and intelligent adjustment. Research demonstrates that weighted fusion of multi-source data combined with entropy-based quantification effectively enhances the stability of posture indicators, enabling the system to accurately describe the security state of power networks. The LDA–XGBoost model significantly outperforms traditional methods like BP, SVM, and random forests in alarm semantic enhancement and anomaly detection, effectively filtering false alarms and reducing interference from redundant events in posture assessment. The active–passive adjustment strategy further improves communication link operational quality, demonstrating a trend of continuous optimization in posture indices across multiple cases. The proposed method demonstrates high accuracy, strong robustness, and excellent engineering adaptability in real-world power dispatch experiments, providing a feasible technical pathway for constructing intelligent, secure, and highly reliable communication networks under new power systems. Moreover, the suggested framework is versatile and can be used with other types of power grid and related infrastructures like microgrids, renewables, and even industrial control systems. Without altering its core, the LDA–XGBoost-based architecture can move on to another application area by simply updating alarm data sources, semantic vocabularies, and structured feature definitions according to the operational characteristics of the particular domain, thus allowing security posture evaluation in different and decentralized energy settings. Future research will integrate attack attribution mechanisms and adaptive learning models to achieve higher-level real-time situational simulation and collaborative defense.

Declarations

Funding: Funding from the State Grid Corporation of China Science and Technology Project (Contract No.: kj2024-014).

Conflicts of interests: Authors do not have any conflicts.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Code availability: Not applicable.

Authors' Contributions: Ruizhi Zhang, Xiaolin Zhang, Zhiming Jin is responsible for designing the framework, analyzing the performance, validating the results, and writing the article. Songyi Han1, Peng DongUltra is responsible for collecting the information required for the framework, provision of software, critical review, and administering the process.

References

[1] Zhukabayeva T., Pervez A., Mardenov Y., Othman M., Karabayev N., Ahmad Z., A traffic analysis and node categorization-aware machine learning-integrated framework for cybersecurity intrusion detection and prevention of WSNs in smart grids, *IEEE Access*, *12*, 91715–91733, 2024.

[2] Mohammed S.H., Al-Jumaily A., Singh M.S.J., Jiménez V.P.G., Jaber A.S., Hussein Y.S., Al-Jumeily D., A review on the evaluation of feature selection using machine learning for cyber-attack detection in smart grid, *IEEE Access*, *12*, 44023–44042, 2024.

[3] Zhang C., Shan G., Roh B.-H., Fair federated learning for multi-task 6G NWDAF network anomaly detection, in IEEE Transactions on Intelligent Transportation Systems, vol. 26, no. 10, pp. 17359–17370, Oct. 2025, doi: 10.1109/TITS.2024.3461679, Oct. 2025.

[4] Osman M., He J., Zhu N., Mokbal F.M.M., Ahmed A., HADTF: A hybrid autoencoder–decision tree framework for improved RPL-based attack detection in IoT networks, based on enhanced feature selection approach. *The Journal of Supercomputing*, *80*(18), 26333–26362, 2024.

[5] Chen J., Seng K.P., Smith J., Ang L.M., Situation awareness in AI-based technologies and multimodal systems: Architectures, challenges and applications, *IEEE Access*, *12*, 88779–88818,2024.

[6] Taha K., Big data analytics in IoT, social media, NLP, and information security: Trends, challenges, and applications, Journal of Big Data, 12(1), 150, 2025.

[7] Almehdhar M., Albaseer A., Khan M.A., Abdallah M., Menouar H., Al-Kuwari S., Al-Fuqaha A., Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks, *IEEE Open Journal of Vehicular Technology*, *5*, 869–906, 2024.

[8] Sharma A., Rani S., Future communications in vehicular networks with hybrid machine learning model for detecting vehicular attack, *Transactions on Emerging Telecommunications Technologies*, *36*(5), e70132, 2025.

[9] Razooqi Y.S., Pekar A., VPN traffic analysis: A survey on detection and application identification, *IEEE Access*, *13*, 132830–132848, 2025.

[10] Mubeen M., Muskan A., Akram A., Rashid J., Alshalali T.A.N., Sarwar N., Cyberbullying-related automated hate speech detection on social media platforms using stack ensemble classification method, *International Journal of Computational Intelligence Systems*, *18*(1), 174, 2025.

[11] Wu Y., Zang Z., Zou X., Luo W., Bai N., Xiang Y., Dong W., Graph attention and Kolmogorov–Arnold network based smart grids intrusion detection, *Scientific Reports*, *15*(1), 8648, 2025.

[12] Ying, X., Research on Network Security Situational Awareness and Risk Assessment Model Based on Bayesian Network, *Journal of Cyber Security and Mobility*, 14(1), 155–179, 2025. https://doi.org/10.13052/jcsm2245-1439.1417.

[13] Induru, V., & Arulkumaran, G., Adaptive cybersecurity monitoring via semantic stream processing and GNN-based trust scoring on IPv4 logs, *International Journal of Business Management and Economic Review*, 4(4), 430, 2021.

[14] Rahman A., Kundu D., Debnath T., Rahman M., Islam M.J., Blockchain-based AI methods for managing industrial IoT: Recent developments, integration challenges and opportunities, *arXiv preprint arXiv:2405.12550,* 2024.

[15] Vidhya G., Jagadheeswari M., Detection of distributed denial of service attacks based on deep learning approaches: A survey, taxonomy, and challenges, *International Research Journal of Multidisciplinary Technovation*, *7*(4), 146–166, 2025.

[16] Pei J. et al., Distributed large models training optimization with real-time wireless channel feedback, in IEEE Journal on Selected Areas in Communications, doi: 10.1109/JSAC.2025.3640136, 2025.
[17] Wang J., Zhou Z., Construction and optimal control method of enterprise information flaw risk contagion model based on the improved LDA model, *International Journal of Advanced Computer Science & Applications*, *15*(12), 2024.
[18] Achaal B., Adda M., Berger M., Ibrahim H., Awde A., Study of smart grid cyber-security: Architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges, *Cybersecurity*, *7*(1), 10, 2024.
[19] Remil Y., Bendimerad A., Mathonat R., Kaytoue M., AIOps solutions for incident management: Technical guidelines and a comprehensive literature review, *arXiv preprint arXiv:2404.01363*, 2024.
[20] Almulla Z., Almajed H., Rahman M.M., A layered security perspective on Internet of Medical Things: Challenges, risks, and technological solutions, *International Journal of Advanced Computer Science & Applications*, *16*(5) 2025.
[21] Hector I., Panjanathan R., Predictive maintenance in Industry 4.0: Planning models and machine learning techniques, techniques. *PeerJ Computer Science*, *10*, e2016, 2024.
[22] Wang J., Manna S., Aksoy M., Sarkar A., Rahman M.A., Noorwali A., Alenazi M.J., Empowering secure and sustainable healthcare through federated learning and blockchain synergies in a medical Internet of Things, *International Journal of Machine Learning and Cybernetics*, 1–33 2025.
[23] Celik A., Eltawil A.M., At the dawn of generative AI era: New frontiers in 6G wireless intelligence, IEEE Open Journal of the Communications Society, 5, 2433–2489, 2024.
[24] Hasan M.K., Abdulkadir R.A., Islam S., Gadekallu T.R., Safie N., Machine learning techniques for secured cyber-physical systems in smart grid networks, *Energy Reports*, *11*, 1268–1290, 2024.

Biographies

Ruizhi Zhang graduated from Xi'an University of Technology in 2009 and graduated from Hebei University of Science and Technology as an on-the-job graduate in 2016. He is currently working in the UHV Branch of State

Grid Hebei Electric Power Co., LTD., focusing on electrical engineering and automation, network security, computer and information communication.

Xiaolin Zhang graduated from Beijing Jiaotong University in 2008. He is currently working in the UHV Branch of State Grid Hebei Electric Power Co., LTD., focusing on electrical engineering and automation, computer science.

Zhiming Jin, graduated from North China Electric Power University (Baoding) in 2019, is currently working at the UHV Branch of State Grid Hebei Electric Power Co., LTD. His main research direction is electromagnetic field numerical calculation.

Songyi Han graduated from Chongqing University of Posts and Telecommunications in 2016. He is currently working in the UHV Branch of State Grid Hebei Electric Power Co., LTD., focusing on smart grid information engineering, including research, development and design in the field of information, automation and interactive power system.

Peng Dong graduated from North China Electric Power University in 2022. He is currently working in the UHV Branch of State Grid Hebei Electric Power Co., LTD., focusing on deep reinforcement learning and mobile edge computing.