World Journal of Information Technology
Print ISSN: 2959-9903
Online ISSN: 2959-9911
DOI: https://doi.org/10.61784/wjit3092

A DYNAMIC TRUST EVALUATION METHOD FOR BOUNDARIES OF NEW POWER SYSTEMS BASED ON MULTI-MODEL PARALLEL ANALYSIS

Yang Cao, Yang Su*, Peng Zhou, XianHan She, Qian Liu, KaiMin Zheng, WeiJie Qiu
China Southern Power Grid Company Limited, Guangzhou 510000, Guangdong, China.
**Corresponding Author: Yang Su*

Abstract: Aiming at the architectural characteristics of numerous nodes and fragmented access in new power systems, as well as the technical pain points of traditional boundary trust evaluation, such as difficulty in capturing short-term anomalies, identifying medium risks, perceiving complex threats, and poor model collaboration, a dynamic trust evaluation method for power system boundaries based on multi-model parallel analysis is proposed. This method constructs a four-level architecture consisting of data collection and preprocessing, multi-model parallel analysis, model collaborative fusion, and trust level output. It collects multi-dimensional boundary data through distributed probes and performs standardization processing, realizes full-complexity risk identification relying on three parallel layers of statistical, machine learning, and deep learning models, completes the fusion of multi-model results combined with a dynamic weight adjustment strategy, and finally maps to four-level grayscale trust levels with targeted grayscale control strategies. Experiments and applications show that this method controls the trust evaluation delay within seconds, realizing real-time, accurate, and grayscale evaluation of the trust status of boundary entities, and provides reliable technical support for boundary security protection of new power systems.
Keywords: New power system; Network boundary; Dynamic trust evaluation; Multi-model parallel analysis; Risk identification; Grayscale control

1 INTRODUCTION

Driven by the "dual carbon" goals, new power systems are characterized by distributed renewable energy, energy storage units, and multi-link collaboration of "source-grid-load-storage". The in-depth integration of Internet of Things, cloud computing and other technologies endows them with architectural features of numerous nodes, wide geographical coverage and fragmented access [1]. A large number of distributed power devices are connected to the core network through public networks or virtual private networks, and are deeply interconnected with enterprise office networks and third-party service platforms. Traditional static boundary protection systems such as firewalls and intrusion detection systems can hardly adapt to the security protection requirements of new power systems.

At present, there are many technical bottlenecks in the boundary trust evaluation of new power systems: first, the ability to capture short-term anomalies is insufficient. Traditional devices rely on static rule bases and cannot analyze lightweight features in real time, making it difficult to detect short-term anomalies at the second-to-minute level; second, there are blind spots in medium-complexity risk identification. A single model cannot process multi-dimensional labeled features, resulting in low identification accuracy [2]; third, the perception of complex threat chains is missing. Traditional models cannot mine the long-term dependencies and high-dimensional anomalies of behaviors, and are ineffective against Advanced Persistent Threats (APT), zero-day attacks and other threats; fourth, the model collaboration capability is lacking. Serial analysis of a single model is difficult to balance the dual requirements of business continuity and security protection. Therefore, this paper designs a dynamic trust evaluation method based on multi-model parallel analysis to achieve full-complexity risk coverage and real-time trust evaluation, adapting to the actual needs of boundary security protection of new power systems.

2 OVERALL SYSTEM ARCHITECTURE DESIGN

The dynamic trust evaluation system for boundaries of new power systems proposed in this paper adopts a four-level architecture design. All levels work collaboratively to realize a closed-loop process from boundary data collection to trust level output. The overall system architecture includes a data collection and preprocessing subsystem, a multi-model parallel analysis subsystem, a model collaborative fusion subsystem, and a trust level output subsystem. The probe distribution, data flow and overall interaction of multi-model parallel analysis of each subsystem are shown in Figure 1.

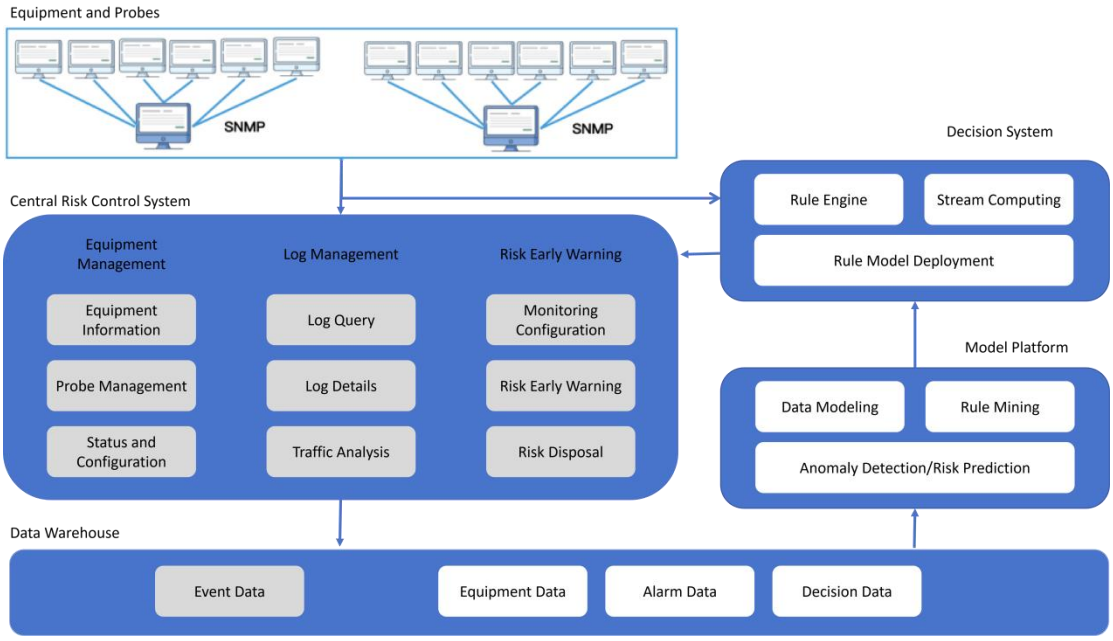

Figure 1 Architecture of Overall System

Core Functions and Interactions of Each Subsystem

1. Data collection and preprocessing subsystem: Collect multi-dimensional boundary data through distributed probes, complete data cleaning, feature extraction and normalization after encrypted transmission, form a standardized feature set, and provide input for subsequent model analysis.
2. Multi-model parallel analysis subsystem: Construct three parallel layers of statistical, machine learning and deep learning models. Each layer shares the feature set and operates independently to accurately identify short-term anomalies, medium-complexity risks and complex threat chains respectively, and output the risk confidence, risk type and threat clues of each model.
3. Model collaborative fusion subsystem: Implement a dynamic weight adjustment strategy based on business scenarios, perform weighted fusion on the output results of the three-layer models, calculate the comprehensive trust confidence, and generate trust levels and risk clue sets.
4. Trust level output subsystem: Map the comprehensive trust confidence to four-level grayscale trust levels, and output grayscale control strategies matching each level to realize the integration of "evaluation-decision-control".

The four-level architecture adopts a layered decoupling design. Each module is independently deployed and supports elastic expansion, which can be directly adapted to the existing boundary nodes of new power systems without large-scale transformation of hardware and network architecture.

3 KEY TECHNOLOGY IMPLEMENTATION

3.1 Multi-Dimensional Data Collection and Standardized Preprocessing

3.1.1 Distributed multi-dimensional data collection

Lightweight probes are deployed at key boundary nodes of new power systems (boundary protection equipment, RTU, intelligent measurement and control terminals, distributed power controllers). The probes are arranged in a distributed cluster mode, compatible with mainstream industrial and general network protocols such as SNMP, Modbus, IEC61850 and MQTT, and can automatically identify the type and version of newly online devices to realize the nearby collection of four types of multi-dimensional data [3]: first, identity credential data, including device MAC, serial number, software version, etc.; second, feature data, including access frequency, session duration, protocol type, etc.; third, environmental status data, including geographical network domain, device operating status, affiliated operation and maintenance team, etc.; fourth, historical interaction data, including historical interaction logs, historical risk scores, rule matching records, etc.

The probe has a built-in cache sub-module, which caches data locally in a circular queue when the network is interrupted, and resumes transmission in sequence after the network is restored. The collected data is pushed to the real-time message bus built based on Kafka through TLS encrypted channels. The bus divides data topics by event, device, alarm and decision types, supporting each model to subscribe to required data in parallel to ensure the security, integrity and high throughput of data transmission.

3.1.2 Data standardized preprocessing

The original collected data needs to undergo three steps of standardized processing to form a feature set adapted to multi-model analysis:

Data cleaning: Eliminate null values, data with protocol parsing errors and outliers beyond the normal range of power

system boundary interaction behaviors. Outlier judgment is based on the normal behavior baseline and business rule thresholds counted from historical data.

Feature extraction: Calculate lightweight features such as access frequency, peak-valley ratio and delay distribution based on a configurable sliding window (the window range can be flexibly adjusted according to scheduling, operation and maintenance and other business scenarios); convert device business attributes, security levels, historical trust levels and other information into numerical labels to form labeled features; slice behavior data by time step to generate behavior sequence time-series features within a specified period.

Feature normalization: Eliminate the dimensional differences of different dimensional features and provide a standardized and unified input feature set for multi-model parallel analysis.

3.2 Construction of Multi-Model Parallel Analysis System

A three-layer parallel analysis system of statistical model layer, machine learning model layer and deep learning model layer is constructed. Each layer shares the preprocessed feature set, operates independently and covers risk identification needs of different complexities respectively, realizing full-dimensional risk perception from short-term anomalies to complex threats. The specific architecture of the multi-model parallel analysis subsystem is shown in Figure 2. The multi-model fusion analysis method can effectively make up for the accuracy shortcomings of a single model in risk identification and improve the coverage and accuracy of overall detection [4].

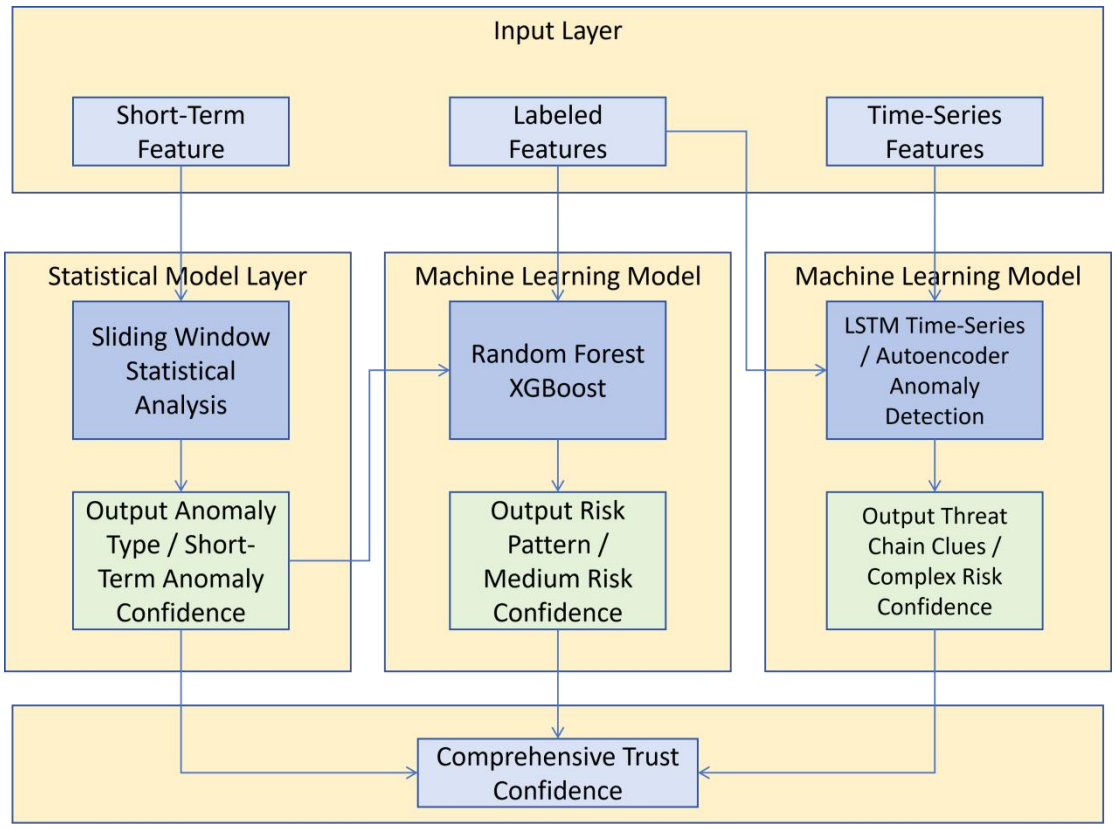

Figure 2 Architecture of the Multi-Model Parallel Analysis Subsystem

3.2.1 Statistical model layer: short-term anomaly capture

The statistical model layer focuses on capturing short-term anomalies at the second-to-minute level. It calculates lightweight features such as access frequency, peak-valley ratio and delay distribution in real time based on a sliding window, and judges whether the current features exceed the normal range combined with the normal interaction behavior baseline of power system boundaries. If it exceeds the baseline, it is marked as a short-term anomaly, and the anomaly confidence and anomaly type are output: the anomaly confidence ranges from 0 to 100 points, the higher the confidence, the more serious the anomaly degree, and the assignment is based on the degree of behavior deviation from the historical baseline; the anomaly types mainly include sudden increase in access frequency, abnormal fluctuation of delay, abnormal peak-valley ratio, etc. This layer realizes rapid perception of short-term anomalies through lightweight feature calculation and provides basic anomaly clues for subsequent risk identification.

3.2.2 Machine learning model layer: medium-complexity risk identification

The machine learning model layer targets medium-complexity risk identification, integrates algorithms such as Random Forest and XGBoost through weighted average, and completes model training using historical boundary interaction labeled data. The model input is labeled features and the short-term anomaly confidence output by the statistical model layer, which can accurately identify medium-complexity risk modes such as unauthorized protocols, abnormal device

labels, low rule matching degree, abnormal access time periods, and mismatched network domains.
The model supports online iterative optimization, adopting a mechanism combining incremental training and regular full-volume update. It continuously optimizes parameters such as node splitting threshold, weight coefficient and feature importance weight of the tree model according to the newly added boundary interaction data, ensuring that the model's ability to identify new medium-risk modes keeps pace with the times and avoiding the decline of identification accuracy caused by the evolution of risk features.

3.2.3 Deep learning model layer: complex threat chain perception

The deep learning model layer is responsible for accurate perception of complex threat chains. The LSTM time-series prediction model and autoencoder anomaly detection model are deployed in parallel to capture the long-term latent and high-dimensional linkage characteristics of complex threats respectively, and collaboratively realize the identification of complex threats such as APT and zero-day attacks [5]:
1. LSTM time-series prediction model: Analyze the long-term behavior time-series of boundary entities, predict the behavior trend in the future period, and judge that there is a long-term behavior deviation risk if the deviation between the actual behavior and the prediction result exceeds the preset threshold.
2. Autoencoder anomaly detection model: Compress and reconstruct high-dimensional behavior features, calculate the reconstruction error, and mark it as a high-dimensional feature anomaly if the error exceeds the threshold.
The two models collaborate through dynamic weight allocation. The initial weight is set according to business scenarios. During operation, if a model continuously outputs high-confidence anomalies, its weight is temporarily increased, and finally the complex risk confidence and threat chain clues are output collaboratively.

3.3 Model Collaborative Fusion Strategy Based on Dynamic Weights

The core of the model collaborative fusion subsystem is to eliminate result conflicts between models and improve the overall accuracy of trust evaluation through a dynamic weight adjustment strategy. The input of this subsystem is the risk confidence, risk type and threat clues output by the three-layer models, and the output is comprehensive trust confidence, trust level and risk clue set [6]. The core implementation strategies include:
1. Basic weight adaptation: Adjust the basic weight of each model according to different business scenarios of new power systems. For example, in the distributed device access scenario, short-term anomalies and medium risks occur frequently, so the weights of statistical models and machine learning models are increased; in the core network interconnection scenario, complex threats have a greater impact, so the weight of deep learning models is increased.
2. High-risk signal enhancement: If the risk confidence output by a model is ≥ the preset high-confidence threshold, the weight of the model is temporarily increased to ensure that high-risk signals are fully valued.
3. Abnormal result review: If the confidence difference between any two models exceeds the preset range, the manual review process is triggered immediately and pushed to the operation and maintenance and security teams. At the same time, the median value strategy is adopted to temporarily output results to avoid evaluation deviation caused by single model abnormality.
Comprehensive confidence calculation: Calculate the comprehensive trust confidence through weighted summation, and the sum of the weights of each model is 1 to realize the effective fusion of multi-model results.

3.4 Four-Level Grayscale Trust Level and Grayscale Control Strategy

The trust level output subsystem maps the comprehensive trust confidence (0-100 points) to four-level grayscale trust levels. The mapping rules are deeply adapted to the business scenarios of power systems. At the same time, targeted grayscale control strategies are matched for each level to realize hierarchical risk disposal, balancing security protection and business continuity. The subsystem takes the risk dashboard as the core visual carrier to realize multi-dimensional display and query of trust levels and risk data[7]. The division and disposal strategies of the four-level grayscale trust levels are as follows:
1. Low risk: Corresponding to a comprehensive trust confidence of 90-100 points. The behavior of boundary entities is highly consistent with the historical normal mode, without any risk clues, and no intervention measures are required.
2. Medium risk: Corresponding to a comprehensive trust confidence of 70-89 points. Only slight short-term anomalies exist, without medium risks and complex risks. The entity is included in mirror observation to continuously track behavior changes.
3. High risk: Corresponding to a comprehensive trust confidence of 50-69 points. There are medium risks or superposition of multiple short-term anomalies, without complex risks. Measures such as speed-limited access or secondary identity verification are adopted.
4. Extremely high risk: Corresponding to a comprehensive trust confidence of 0-49 points. There are complex risks or superposition of medium risks and short-term anomalies. The connection is immediately interrupted or isolated to prevent risk proliferation.
At the same time, the system synchronously outputs the risk clue set identified by each model, including anomaly types, risk modes, threat chain clues, etc. The risk dashboard supports the statistics, query and visual display of risk data by region, device type, risk level, time cycle and other dimensions, providing an intuitive risk decision-making basis for operation and maintenance and security teams.

4 APPLICATION ADVANTAGES OF THE METHOD

Based on multi-model parallel analysis and dynamic weight fusion [8], this method solves the technical pain points of traditional boundary trust evaluation of new power systems and has significant application advantages compared with existing schemes:

Strong real-time performance, adapting to the response requirements of new power systems: The statistical model layer processes data in real time based on a sliding window. The multi-model parallel architecture combined with the high throughput and low delay characteristics of the Kafka real-time message bus controls the trust evaluation delay within seconds, meeting the "second-to-subsecond" risk response requirements of new power systems and avoiding response lag caused by traditional offline analysis.

Full-dimensional coverage, realizing full-complexity risk identification: It forms a full-dimensional risk identification capability from short-term anomalies (statistical model), medium-complexity risks (machine learning model) to complex threat chains (deep learning model), making up for the shortcoming that traditional single models can only cover part of the risks, and adapting to the diversified and complex characteristics of boundary risks of new power systems.

Excellent adaptability and scalability: The model supports online iterative optimization and can be continuously updated with the evolution of boundary risk features; the probe is compatible with a variety of industrial and general protocols, adapting to boundary devices of different manufacturers and models; the system adopts a layered decoupling architecture and supports module-level expansion, such as adding new deep learning model types to meet the business expansion needs of power systems.

High compatibility and practicability, easy to deploy: It can be directly deployed on the existing boundary nodes of new power systems without large-scale transformation of existing hardware and network architecture; the trust level is directly associated with the grayscale control strategy, which can be seamlessly connected with the existing boundary risk control system to realize the closed-loop management of "evaluation-decision-control".

Compliant with safety and compliance requirements, traceable process: The whole process of data collection and transmission adopts TLS encryption to ensure data transmission security; all trust evaluation processes have complete log records, meeting the security audit and compliance requirements of power systems and avoiding the inability to define security responsibilities due to opaque evaluation processes.

5 CONCLUSION

Aiming at the actual needs of boundary security protection of new power systems, the dynamic trust evaluation method based on multi-model parallel analysis proposed in this paper realizes real-time, accurate and grayscale evaluation of the trust status of boundary entities by constructing a four-level architecture. This method relies on distributed probes and standardized preprocessing to realize efficient collection and processing of multi-dimensional boundary data, uses three-layer parallel models to complete full-complexity risk identification, realizes effective fusion of multi-model results through dynamic weight adjustment strategy, and finally realizes hierarchical risk disposal and decision support through four-level grayscale trust levels and risk dashboard visualization.

This method solves the technical pain points of traditional boundary trust evaluation such as difficulty in capturing short-term anomalies and poor model collaboration, and has the advantages of real-time performance, scalability and compatibility. It can be directly deployed on the existing boundary nodes of new power systems, providing a reliable technical solution and practical reference for network boundary security protection of new power systems.

In the future, combined with edge computing technology, part of the model analysis tasks can be sunk to edge probes to reduce the computing pressure on the central side; at the same time, a federated learning mechanism can be introduced to realize joint model training among multi-regional power systems, improve the ability to identify cross-regional complex threats, and further improve the dynamic trust evaluation system for boundaries of new power systems.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

[1] Sheng Gehao, Qian Yong, Luo Lingen, et al. Key Technologies and Application Prospects of Power Equipment Operation and Maintenance for New Power Systems. High Voltage Engineering, 2021, 47(9): 13.

[2] Cao Jinzhang, Zhu Chuanbai, Liu Bo, et al. Research and Implementation of Smart Grid Dispatching Coding System Based on Common Information Model. Automation of Electric Power Systems, 2011(2): 5.

[3] Han Ping, Zhang Han, Fang Cheng, et al. A Parallel Anomaly Detection Method for Massive Network Traffic Based on Multi-Model Fusion. Journal of Civil Aviation University of China, 2022, 40(1): 8.

[4] Zhu Yadong. Improvement of Boundary Node Identification Method in Cloud Computing Network. Computer Measurement & Control, 2017, 25(1): 167-169+172.

[5] Hu Xian, Feng Yiping, Pan Ge. Distributed LSTM Equipment Fault Prediction Based on Edge Side Autoencoder Compression//Proceedings of the 31st Chinese Process Control Conference (CPCC 2020), 2020.

[6] Chen Jianfei, Wang Rui, Zhang Fangzhe, et al. A Novel Anonymous Identity Authentication Scheme for New Power Systems Based on Ring Signature and IBE Strategy. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2026, 38(01): 93-99.

[7] Feng Shijie, Qin Yanyan, Zeng Zhixiang, et al. Research on Trusted Operation and Maintenance for Power System Network Security Based on Zero Trust Technology. Network Security Technology & Application, 2025(09): 102-105.

[8] Xiong Kaizhi, Su Jianbo, Jiang Chao, et al. Identity Authentication Technology Based on Trusted Agent Under Zero Trust Architecture in Power Industry//Journal of Information Security Research. Proceedings of 2025 Cybersecurity Innovation and Development Conference. Yalong River Basin Hydropower Development Co., Ltd.; Huawei Technologies Co., Ltd., 2025: 124-127. DOI: 10.26914/c.cnkihy.2025.017943.