A Hybrid Deep Learning Architecture for Network Security Situation Awareness and Pre-Alarm in Large-Scale Data Environments Using LSTM, Autoencoder, and GNN

Xiaoxia Wang
School of Information and Network Security, Inner Mongolia Police College, Hohhot 010000, China
E-mail: wangxx20002025@163.com

Keywords: Network security, Situation awareness, Intelligent pre-alarm, Deep learning; big data

Received: 11 October, 2025

In the large-scale data environment, network security situational awareness (NSSA) often faces the problems of poor real-time performance and low early warning accuracy. Therefore, this article proposes an intelligent early warning model that integrates multi-source heterogeneous data. This model constructs a distributed processing architecture based on Spark+Flink, which integrates a hybrid analysis mechanism of long-term memory network (LSTM), self-encoder and graph neural network (GNN) to efficiently detect abnormal behaviors and infer attack paths. At the same time, a situation scoring mechanism with dynamic weight adjustment is designed, and a time decay suppression strategy is introduced to optimize the alarm output and reduce the false alarm rate. The experiment was conducted on CICIDS2017 public data set and a real log of a provincial government cloud, and evaluated by F1-score, AUC, response delay and effective alarm compression ratio. The results show that the F1-score of this model is 0.93 on CICIDS2017, which is significantly better than the traditional method. In the real government cloud environment, the system throughput is up to 183,000 pieces/second, the average response delay is controlled within 300ms, and the number of effective alarms is reduced by over 65%. This study verifies the feasibility and superiority of the proposed model in high concurrency scenarios, and provides a practical basis for building an intelligent and extensible network security defense system.

Povzetek: Članek predstavlja inteligentni model za zgodnje zaznavanje kibernetskih groženj v velikih podatkovnih okoljih, ki z združevanjem več virov podatkov in naprednih nevronskih mrež izboljšuje natančnost, hitrost odziva ter zmanjšuje število lažnih alarmov v visoko obremenjenih sistemih.

1 Introduction

With the rapid development of information technology, the global data volume has increased exponentially. According to IDC's forecast, the total amount of global generated data will exceed 180ZB in 2025, and enterprise networks and cloud computing platforms are a large number of data sources. In this context, network security challenges become more and more complex and dynamic. Traditional protection methods based on rule matching and signature detection, such as firewall and IDS, are exposed to new attacks such as APT and zero-day attacks, and their response is delayed (Zhang et al., 2023). NSSA, as a technical paradigm to evaluate network operation, identify potential risks and predict trends, has been widely concerned by academia and industry (Zhang et al., 2021). Through multi-source information fusion, it helps security operation and maintenance personnel to master the "situation" of network security and improve their decision-making and emergency response capabilities. However, most situational awareness systems are in the stage of "post-analysis" or "passive response", lacking understanding of complex attack chains and predicting unknown threats (Yang & Zhao, 2024). In the scenario of data scale expansion, the traditional centralized architecture faces the performance bottleneck, and it is difficult to meet the real-time analysis requirements.

Introducing intelligent methods to build a network security pre-alarm model with autonomous learning and dynamic evolution ability has become the key to upgrading situational awareness technology (Luo et al., 2024). Artificial intelligence (AI), especially machine learning (ML) and deep learning (DL) technologies, provide new tools for processing large-scale security data. The model can automatically identify abnormal behaviors by learning historical attack patterns, and deduce future attacks by using time series modeling (Ma, 2025). Combined with advanced algorithms such as GNN, the system can also simulate the attacker's tactical path and find hidden actions in advance (Wei et al., 2024). If these technologies are integrated into the situational awareness system, it is expected to improve the initiative and intelligence level of the defense system. It is difficult to apply intelligent algorithm to real network environment.

On the one hand, the categories of security data are unbalanced, the normal traffic is far more than malicious samples, and the model tends to favor the majority categories, which reduces the sensitivity to rare attacks (Liu, 2020). On the other hand, the change of network environment causes concept drift, which affects the stability of the model (Zhang et al., 2022). In addition, DL models are mostly "black boxes", and the decision-making process lacks interpretability, which is unfavorable in the security field. To clarify the technical path and validation objectives of this study, the following verifiable research questions are proposed in this article:

(1) Can a hybrid model combining LSTM, autoencoder, and GNN achieve high-precision detection of abnormal behavior while maintaining preset response performance in a specified large-scale streaming environment?

(2) Can the proposed dynamic weight fusion mechanism and time decay suppression strategy significantly improve the effectiveness of alarms while ensuring that critical safety events are not missed?

(3) Compared to existing typical methods, does this model have statistically significant advantages in comprehensive detection performance indicators?

This study focuses on NSSA and intelligent pre-alarm in large-scale data environment, aiming at breaking through the limitations of existing technologies in data processing, model generalization and system practicability. A hierarchical fusion architecture framework is proposed, which integrates distributed data processing engines and various intelligent analysis models to realize end-to-end closed-loop management from log collection to risk pre-alarm. In terms of methods, the anomaly detection mechanism based on LSTM and self-encoder is mainly explored, GNN is introduced to enhance the reasoning ability of complex attack chain, and dynamic weight adjustment strategy is designed to improve the accuracy and timeliness of situation scoring. The results show that the proposed model is superior to the traditional scheme in detection accuracy. Future work will explore the feasibility of lightweight deployment on edge devices with limited resources, and further introduce external threat intelligence and federated learning mechanism to enhance the perception of unknown threats.

2 Related theory and technical basis

NSSA is not an isolated technical module, but a comprehensive system integrating information collection, analysis, risk assessment and visual decision support (Xie et al., 2020). To realize effective perception and pre-alarm for large-scale data environment, we need to rely on a series of mature basic theories and technical means (Zhang et al., 2020). These technologies cover traditional network security core methods, as well as key supporting tools in the fields of big data processing and AI.

From the theoretical framework of situational awareness, the three-level model is still widely used. This model divides situational awareness into three levels: perception, understanding and prediction (Wang & Bu, 2020). In cyberspace, this means that the system should not only collect all kinds of security events, such as login failure, abnormal outreach, port scanning, etc., but also integrate this fragmented information to identify potential attacks and infer their development direction (DeValk & Elmqvist, 2024). This logic provides a theoretical basis for building a hierarchical analysis framework. Based on this, some researchers put forward quantitative evaluation methods, such as constructing an index system to score the overall risk of the network, and often use mathematical tools such as D-S evidence theory, fuzzy comprehensive evaluation or analytic hierarchy process (AHP) to solve the uncertainty problem in multi-source information fusion (Yu et al., 2020; Lan, 2021; Cai et al., 2021).

In the big data environment, the traditional stand-alone processing mode cannot meet the real-time analysis requirements of PB-level logs and high concurrent traffic (Chen & Miao, 2021). Therefore, the distributed computing platform has become the infrastructure to support large-scale security data analysis. In the early days, Apache Hadoop provided batch processing capability, which was suitable for offline mining of historical data. With the development of streaming computing, frameworks such as Spark Streaming and Flink have gradually become the first choice for real-time security analysis because of their low latency and high throughput (Li et al., 2022). Flink, in particular, has obvious advantages in state management and precise semantic guarantee, and is more reliable when dealing with continuous network event streams. Kafka, as the mainstream message middleware, is often used to decouple data production and consumption, and realize efficient buffering and distribution of logs.

The application of ML technology makes it possible to automatically discover abnormal patterns from massive data. Supervised learning methods, such as random forest and XGBoost, are stable in the classification task of known attack types, especially suitable for labeled data sets. However, in reality, most network environments lack enough malicious samples, so unsupervised learning is more practical. Clustering algorithms (such as K-means and DBSCAN) can divide the baseline of normal behavior, and alarm will be triggered once new data deviates from the clustering center. As a deep neural network structure, self-encoder can detect abnormal input through reconstruction error, and has good performance when dealing with high-dimensional traffic characteristics. In contrast, LSTM is more suitable for modeling time series behavior, and can capture potential covert activities without relying on labels.

Simple point anomaly detection is often difficult to reveal the nature of complex attacks. APT attacks usually lurk for a long time and advance in multiple stages, so it is difficult for a single alarm to reflect the whole picture. Therefore, in recent years, GNN has been introduced into the security field to model the relationship network between entities (Ullah et al., 2024). By abstracting hosts, users, processes, services, etc. as nodes, and treating operations such as access, call and connection as edges, a dynamic evolution diagram is constructed. GNN can spread information on the graph structure, identify suspicious nodes that look normal but are in the critical path, and assist in judging whether there is lateral movement or privilege promotion (Huang et al., 2025).

The integration of threat intelligence is also extremely important. Standardized formats such as STIX/TAXII make threat information sharing between different organizations a reality. Matching external intelligence (such as malicious IP, C2 domain name and file hash) with internal monitoring data can significantly improve the detection efficiency. At the same time, combined with knowledge mapping technology, it can also realize the structural expression of attack tactics, techniques and processes (MITRE ATT&CK framework) and provide semantic support for automated response.

Although existing research has made some progress in network security situational awareness and intelligent detection, mainstream methods still have significant shortcomings in real-time processing capabilities, multi-stage attack modeling, and alarm effectiveness. Table 1 compares five representative related works in recent years.

Table 1: Comparison of existing network security situation awareness and intelligent detection models

Study (Year)	Core Technology	Dataset	Main Performance Metric	Main Limitations
Zhang et al. (2021)	LSTM + Decision Tree	NSL-KDD	F1 = 0.87	Handles only structured logs; cannot model inter-entity relationships
Yang & Zhao (2024)	Stacked Sparse Autoencoder	CICIDS2017	AUC = 0.91	No real-time processing capability; relies heavily on labeled data
Wei et al. (2024)	Random Forest + Rule Engine	Self-built enterprise traffic	Accuracy = 89%	Difficult to detect unknown attacks; unable to reason multi-stage APT
Huang et al. (2025)	GNN (Static Graph)	DARPA99	Recall = 0.82	Graph structure updates lag; unsuitable for dynamic network environments
Luo et al. (2024)	KNN + KD Tree	UNSW-NB15	F1 = 0.85	High computational complexity; throughput below 50k records/sec

The current state-of-the-art (SOTA) methods generally have the following problems: (1) Lack high concurrency real-time processing capabilities, making it difficult to cope with PB level log streams; (2) Attack modeling is isolated and often focuses on single point anomalies, making it difficult to effectively identify cross host, multi-stage APT attack chains; (3) The static alarm mechanism is prone to generating a large number of redundant alarms, which increases the burden of operation and maintenance.

The model proposed in this article addresses the aforementioned shortcomings from the following aspects. Firstly, the Spark+Flink hybrid stream batch processing architecture is adopted, which can support high-throughput real-time analysis of over 180000 events per second. Secondly, integrating LSTM with GNN to achieve joint modeling of covert and multi hop attack paths. Furthermore, introducing dynamic thresholds and time decay suppression mechanisms can significantly compress invalid alarms, thereby improving operational efficiency.

3 NSSA and prediction model based on intelligent algorithms

In the large-scale data environment, the traditional static scoring mechanism has been difficult to cope with the dynamic evolution of network threats. In order to accurately describe the overall security state and effectively predict the future trend, this article constructs a set of NSSA and prediction model integrating multi-modal intelligent algorithm. The model takes "quantification-detection-reasoning-fusion" as the main line, and completes the transformation process from original data to high-order situation output step by step.

At the level of situation quantification, scattered security incidents need to be transformed into comparable and accumulative risk values (Yu, 2024). In the field of NSSA and intelligent early warning, although the mainstream research focuses on the integration of deep learning and big data architecture, the relevant achievements from the field of control theory and nonlinear systems can also provide methodological reference. Boulkroune et al. (2017) proposed a synchronization control strategy based on output feedback, which effectively dealt with the synchronization problem of chaotic systems under input nonlinearity. The follow-up work further combines fuzzy logic with fractional calculus to realize practical fixed-time synchronization of uncertain chaotic systems (Boulkroune et al., 2025). Zouari et al. (2012) systematically studied the adaptive control of multivariable complex dynamic systems, and adopted robust neural adaptive mechanism to improve the robustness of the system. Merazka et al. (2017) designed an adaptive fuzzy controller based on high gain observer, which provided a new idea for state estimation and control of multivariable nonlinear systems. Rigatos et al.'s (2023) exploration of nonlinear optimal control also shows the potential of realizing high-performance regulation in complex dynamic systems. Although these control theory achievements are not directly oriented to network security scenarios, their technical ideas in dealing with uncertainty, nonlinearity and multivariable coupling have important enlightenment significance for building an intelligent early warning model with more robustness and adaptive ability.

In this article, the improved analytic hierarchy process (AHP) combined with entropy weight method is used for dynamic weight distribution to avoid the deviation caused by totally relying on subjective judgment. Let the index set corresponding to the i-security incident be $x_i=(x_{i1},x_{i2},\ldots,x_{in})$, including attack frequency, reputation of source IP, importance of target assets and other dimensions. By constructing the judgment matrix and calculating the feature vector, the initial weight $w_j^{(0)}$ is obtained, and then the information entropy E_j is introduced to modify it:

$$E_j=-\frac{1}{\ln m}\sum_{i=1}^{m} p_{ij}\ln p_{ij}\,,\quad p_{ij}=\frac{x_{ij}}{\sum_{k=1}^{m} x_{kj}} \tag{1}$$

Finally, the combination weight $w_j=\alpha w_j^{(0)}+(1-\alpha)w_j^{(e)}$ is obtained by combining subjective and objective factors, where $\alpha\in[0,1]$ is the adjustment coefficient. Thus, the initial risk score of a single event can be expressed as:

$$R_i=\sum_{j=1}^{n} w_j\cdot f(x_{ij}) \tag{2}$$

Here $f(\cdot)$ is a normalized function to ensure that all indicators are in the same dimension. After the scores of all events are aggregated by sliding in the time window, the situation baseline S_t of the local area is formed.

Aiming at the dynamic and nonlinear characteristics of network security time series data, this article constructs a multi-layer LSTM network structure for situation evolution trend prediction (see Figure 1). The input layer receives the network behavior feature sequence which is streamed by Kafka and preprocessed by Spark, and organizes it into a 3D tensor with a fixed window length as the model input (Wang, 2021). The hidden layer consists of two layers of stacked LSTM cells, each layer contains 128 memory cells, and the behavior dependence under a long-time span is captured through the gating mechanism (Wang & Jones, 2021). In the training process, the model uses back propagation algorithm to optimize the weight parameters along time expansion (BPTT) and learn the time evolution law of normal traffic patterns. The output layer adopts fully connected structure, which maps the final hidden state to one-dimensional output and generates the predicted value of abnormal risk score at the next moment.

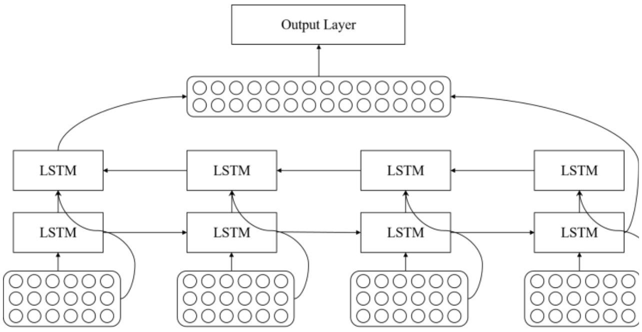

Figure 1: Multilayer LSTM network structure

The input of the model is a 42-dimensional network behavior feature sequence pretreated by Spark, which is organized as a tensor with the shape of in the form of sliding window. Each layer of LSTM contains 128 memory cells, using tanh as the state activation function and sigmoid as the gate activation function. The final output layer is mapped into one-dimensional abnormal risk score through the full connection layer, which is used for subsequent dynamic threshold judgment.

Let the input sequence be the flow characteristic vector $x_{t-T+1},\ldots,x_t$ of the past T moments, and the LSTM unit controls the information flow through the forgetting gate, the input gate and the output gate. The hidden state h_t can reflect the behavior pattern at the current moment:

$$f_t=\sigma(W_f[\mathrm{h}_{t-1},x_t]+b_f) \tag{3}$$

$$i_t=\sigma(W_i[\mathrm{h}_{t-1},x_t]+b_i) \tag{4}$$

$$\widetilde{C}_t=\tanh(W_C[\mathrm{h}_{t-1},x_t]+b_C) \tag{5}$$

$$C_t=f_t\odot C_{t-1}+i_t\odot\widetilde{C}_t \tag{6}$$

$$o_t=\sigma(W_o[\mathrm{h}_{t-1},x_t]+b_o) \tag{7}$$

$$\mathrm{h}_t=o_t\odot\tanh(C_t) \tag{8}$$

In the model training stage, the goal is to minimize the prediction error, and the loss function is defined as the mean square error:

$$\mathrm{L}=\frac{1}{N}\sum_{t=1}^{N}\Vert x_t-\hat{x}_t\Vert^2 \tag{9}$$

When the residual between the actual input and the reconstructed output exceeds the dynamic threshold τ, it is judged as abnormal behavior. The threshold is not fixed, but is adjusted adaptively according to the distribution of recent normal samples:

$$\tau=\mu_r+k\cdot\sigma_r \tag{10}$$

Where μ_r and σ_r are the historical mean and standard deviation of the reconstruction error, respectively, and k is the confidence coefficient, usually between 2 and 3.

In order to further explore the potential attack paths across hosts and processes, this article introduces GNN for context correlation analysis (see Figure 2 for its structure). The network entity is abstracted as graph $G=(V,E)$, with node $v_i\in V$ representing host or user and edge $e_{ij}\in E$ representing communication or access relationship. Each node carries a feature vector $\mathrm{h}_i^{(0)}$, which is iteratively updated by graph convolution operation:

$$\mathrm{h}_i^{(l+1)}=\sigma\left(\sum_{j\Box N(i)}\frac{1}{c_{ij}}W^{(l)}\mathrm{h}_j^{(l)}\right) \tag{11}$$

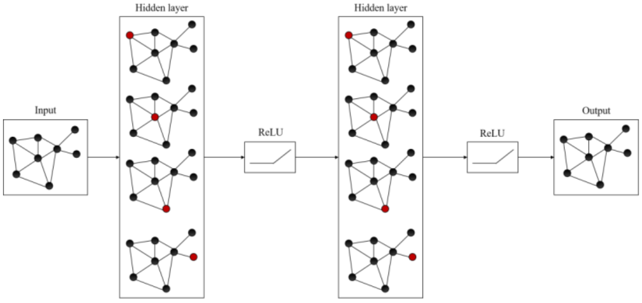

Figure 2: GNN structure

Where $N(i)$ is the neighbor set of node i and c_{ij} is the normalized coefficient, usually taking the reciprocal product of the square root of the degree. After several layers of propagation, the node embedding vector can capture the local structure information and can be used for classification tasks. For example, if an internal server frequently communicates with known malicious IP and its permission level is high, the probability of being marked as a "high-risk springboard" increases significantly.

In the model fusion stage, the Stacking integration strategy is adopted to integrate the output results of LSTM, self-encoder and GNN. The basic model outputs the abnormal probability p_1,p_2,p_3 respectively, and the meta-learner (such as logistic regression) retrains it as a new feature:

$$p_{final}=\sigma(\beta_0+\beta_1p_1+\beta_2p_2+\beta_3p_3) \tag{12}$$

This hierarchical fusion method not only retains the advantages of each sub-model, but also reduces the risk of over-fitting of a single model.

The original network traffic data is preprocessed by Kafka and Spark to form a standardized time series feature vector. The vector is sent to two modules in parallel: (1) LSTM module, which focuses on learning the normal behavior pattern of traffic in the time dimension, and detects time sequence anomalies by predicting the eigenvalues at the next moment; (2) Self-encoder module, which learns a compressed representation from the high-dimensional feature space at the current moment, and identifies point anomalies deviating from the normal baseline through reconstruction errors. The anomaly detection results of the two modules are used as the primary input and fused with the output of GNN module. GNN module uses the dynamic relationship diagram composed of hosts, users and other entities to evaluate the propagation influence and context risk of primary abnormal events in the network topology. Finally, these three complementary signals are synthesized by meta-learner through Stacking integration strategy to generate the final comprehensive risk score.

The above models do not operate in isolation, but work together under a unified framework. The situation score is continuously fed back to the detection module to adjust the sensitivity, and the graph structure evolves in real time with the new connection, forming a closed-loop optimization mechanism. Although there are still some problems such as high training cost and insufficient explanation, the overall architecture has strong expansion potential and can adapt to different scale and complexity network environments.

4 Design of intelligent pre-alarm mechanism

After the situation assessment and threat prediction are completed, how to turn the analysis results into operational pre-alarm information is the key to whether the whole system can effectively play its defense value. The traditional alarm mechanism often adopts the fixed threshold trigger mode. It is easy to produce many repeated or low-priority prompts, which makes security personnel suffer from "alarm fatigue" and even ignore real high-risk events. Based on this, this article conceives a dynamic, hierarchical and context-aware intelligent pre-alarm mechanism, hoping to reduce false positives and improve response efficiency.

The core of pre-alarm mechanism lies in establishing reasonable risk judgment logic. In this study, the comprehensive risk value R_t is defined as the final threat score at the current moment, which consists of three parts: basic anomaly score R_t^a, topological impact score R_t^g and asset association weight ω_i. The overall expression is as follows:

$$R_t=\alpha R_t^a+\beta R_t^g+\gamma\sum_{i\square A_t}\omega_i \tag{13}$$

Where A_t represents the asset set involved in the current event, α, β, γ is the adjustment parameter, which is fine-tuned according to the actual environment. The formula emphasizes not only whether the behavior itself is abnormal, but also its occurrence position and potential diffusion range, so as to avoid overreacting to small fluctuations of edge equipment.

On this basis, the warning levels are divided into four categories: Low (Green), Medium (Yellow), High (Orange), and Emergency (Red), each corresponding to different response strategies. The classification is not simply based on numerical segmentation but incorporates a dynamic threshold mechanism. Let the average value of R_t in the past 7 days be μ_R and the standard deviation be σ_R, then the thresholds at all levels will be updated with time:

$$\begin{cases} Medium{:}R_t>\mu_R+\sigma_R \\ High{:}R_t>\mu_R+2\sigma_R \\ Emergency{:}R_t>\mu_R+3\sigma_R \end{cases} \tag{14}$$

This design enables the system to adapt to the periodic changes of network activities-for example, the overall risk level naturally rises during the peak traffic hours on weekdays, and if static thresholds are still used, it will easily lead to misjudgment. After dynamic adjustment, only behaviors that significantly deviate from the normal state will be marked as high risk.

In order to avoid the alarm triggered repeatedly by the same kind of events in a short time, the system also introduces a time attenuation suppression mechanism. For continuous alarms with the same source IP and the same attack type, their effective weight decays exponentially with time:

$$W(t)=W_0\cdot e^{-\lambda(t-t_0)} \tag{15}$$

Where W_0 is the initial weight, the attenuation coefficient (0.1/h in the experiment), and t_0 is the first trigger time. When the cumulative weighted value is lower than a certain threshold, the subsequent similar events will not generate independent alarms, but only make internal records. This mechanism effectively alleviates the alarm storm problem caused by scanning attacks.

The key hyperparameters involved in this article are all determined on CICIDS2017 verification set through grid search and cross-validation: the adjustment coefficient is 0.6 to balance the expert experience and data-driven weight. All parameters are tested by A/B for two weeks before deployment in government cloud environment to confirm their stability in real business cycle.

The pre-alarm information itself has also been structured and strengthened. Each alarm not only covers basic information such as time, source and destination address, protocol type, but also includes preliminary disposal suggestions generated by knowledge map. If a host is detected to have SMB brute force cracking accompanied with signs of lateral movement, it will automatically match the technical numbers of T1110(Brute Force) and T1021(Remote Services) in MITRE ATT&CK, and it is recommended to close unnecessary shared ports and reset related account passwords. These suggestions are generated by combining rule template with semantic reasoning. Although they can't completely replace manual judgment, they can greatly shorten the response preparation time.

5 Experimental results and analysis

In order to solve the problem that the normal traffic in the security log is far more than the attack samples, this article does not adopt the over-sampling method such as SMOTE to avoid high-dimensional semantic distortion, but adopts the following strategies to alleviate it: first, only normal traffic is used to construct the reconstruction baseline in the self-encoder training, and the high reconstruction error is regarded as abnormal; Secondly, in the supervision and fine-tuning stage of LSTM and GNN, the category weight inversely proportional to frequency is applied to the minority samples; Finally, F1-score and AUC are given priority in the evaluation, so as to objectively reflect the detection ability of the model to rare attacks. On the premise of maintaining the authenticity of data distribution, the above methods effectively improve the processing performance of the model for unbalanced data.

In order to improve reproducibility, this article provides complete key configuration and process details. In the training stage, LSTM uses Adam optimizer, with a learning rate of 0.001 and 50 rounds of training. Self-encoder adopts MSE loss, with a learning rate of 0.0005 and 100 rounds of training; GNN is based on the GraphSAGE architecture, with two layers of networks, each layer has 64 dimensions, and the learning rate is 0.01. In the preprocessing step, after the original log is accessed by Kafka, the fields are standardized by Spark, and based on the sliding window segmentation, 42-dimensional features are finally extracted, including traffic rate, protocol distribution and session duration.

The experimental platform is deployed in a cluster environment consisting of six servers, each of which is equipped with a dual-channel Intel Xeon Gold 6230 processor, 128GB memory and 10GbE network interface. The operating system is CentOS 7.9, and the underlying layer manages Spark and Flink tasks through Kubernetes, and Kafka supports log stream transmission as a message bus. The experimental data covers the public data set CICIDS2017 and the real desensitization traffic of a provincial government cloud platform for two consecutive weeks, with a total amount of about 4.2TB and an average incident inflow rate of more than 150,000/sec.

The experiment evaluates the system performance from the aspects of detection accuracy, response delay, scalability and resource consumption. On CICIDS2017 data set, the average F1-score of this model is 0.93, and the standard deviation of multiple runs is less than 0.01, showing good stability. In the reasoning stage, a single Flink task manager can stably handle about 30,000 events/second, with the memory occupancy rate below 70%, and the average response delay is controlled within 300 milliseconds under the load of 200k events/second, and the deviation of repeated experiments is less than 15 milliseconds. In the training stage, it takes about 32 hours to complete the joint training of LSTM, self-encoder and GNN, and the peak GPU memory occupation is 11GB (using NVIDIA V100). When the system expands horizontally, the resource consumption increases linearly with the traffic, showing good predictability and manageability, and meeting the requirements of large-scale production environment deployment. Compared with the baseline method, this model has consistent and significant performance advantages in all indicators.

In terms of detection performance, this article compares the proposed fusion model (LSTM+Autoencoder+GNN) with four benchmark methods: Snort rule engine, random forest classifier, Isolation Forest and single LSTM model. The evaluation indexes are Accuracy, Recall, F1-score and AUC. Figure 3 shows the F1-score comparison results on CICIDS2017 data set. Traditional Snort has poor performance in the face of encrypted tunnel and low-frequency scanning attacks, and F1 is only 0.68. The model in this article reaches 0.93, especially in APT simulation scene, which is mainly due to GNN's ability to identify multi-stage behaviors.

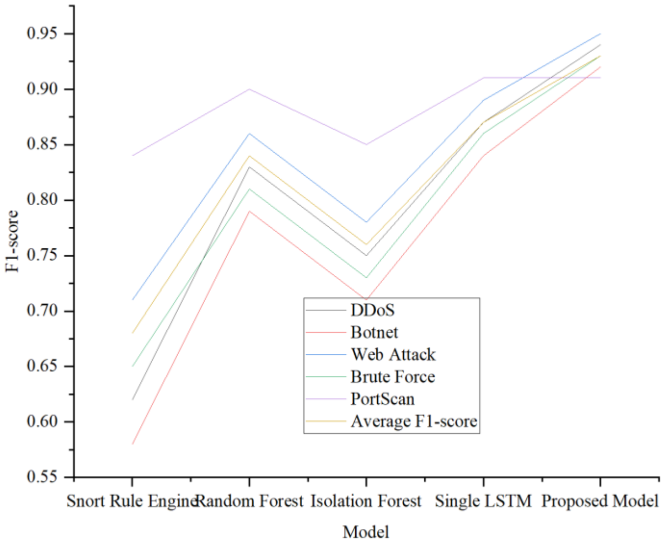

Figure 3: F1-score of Different Models on CICIDS2017

In order to systematically evaluate the contribution of each component of the model, this article designed an ablation experiment on CICIDS2017 data set. Table 2 shows the comparison results between the complete model and each ablation variant in three key indexes: F1-score, Recall and AUC.

Table 2: Comparison of ablation experiment results (CICIDS2017 Dataset)

Model Variant	F1-score	Recall	AUC
Full Model (LSTM + Autoencoder + GNN)	0.93	0.91	0.96
Remove GNN (LSTM + Autoencoder only)	0.87	0.85	0.90
Remove Autoencoder (LSTM + GNN only)	0.85	0.82	0.88
LSTM only	0.81	0.79	0.84

Figure 4 plots the average response delay of each model under different data throughput. When the input rate is increased from 50,000 to 200,000/s, the calculation cost of random forest features increases rapidly, and the delay exceeds 800ms; Isolated Forest is light, but its accuracy drops significantly; With the help of Flink's micro-batch mechanism and parallel reasoning optimization, the delay of this model is always controlled within 300ms, which meets the real-time response requirements of most security scenarios.

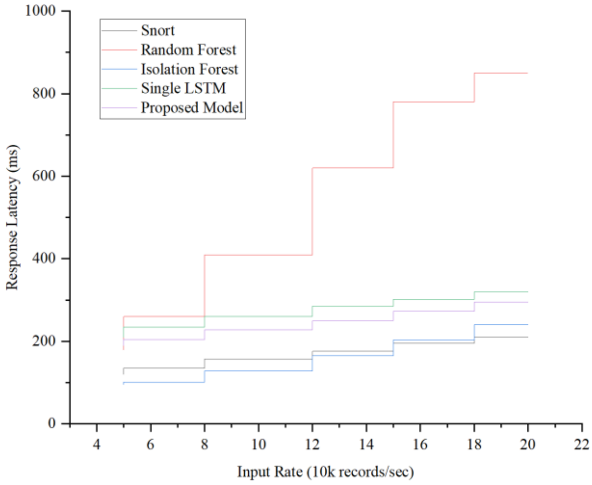

Figure 4: Response delay of each model under different throughput

In order to further verify the effectiveness of the dynamic pre-alarm mechanism, this study injected simulated attack traffic into the real government cloud environment, including slow brute force cracking, hidden DNS tunnels and lateral movement attempts. Figure 5 shows the changing trend of the number of original alarms generated by the system and the number of effective alarms after duplicate removal for 48 consecutive hours. When the attenuation suppression mechanism is not enabled, there are as many as 12,000 alarms per day, of which duplicates account for more than 65%; After it is enabled, the number of effective alarms is stable at about 1800, and there are no key events missing, which reduces the burden of operation and maintenance.

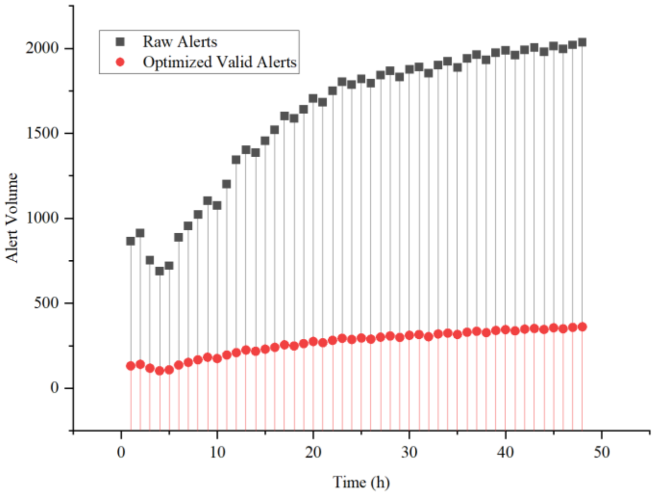

Figure 5: Changes in the number of alarms over time

Regarding the rationality of situation score, a real DDoS attack event is selected for retrospective analysis. Figure 6 shows the evolution of the comprehensive risk value of the core switch area within 3 hours before and after the attack. The score began to climb slowly from the normal level (about 35 points) and jumped to 89 points within 12 minutes after the attack was launched, triggering a "high" warning; With the continuous growth of traffic, it finally broke through 95 points and entered the "emergency" interval. The whole process is highly consistent with the actual peak flow, which shows that the model has good trend prediction ability to some extent.

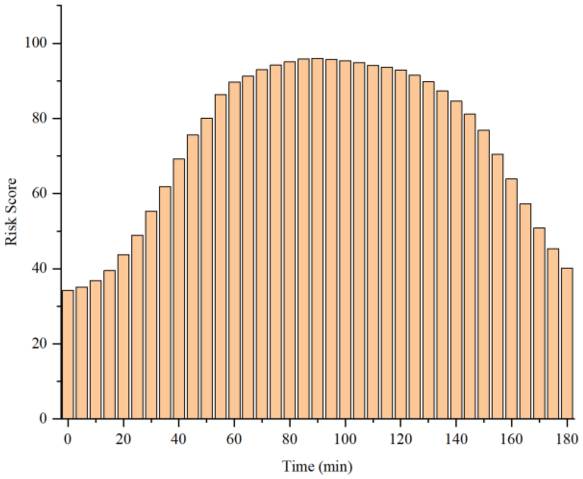

Figure 6: Changes in situation score during DDoS Attacks

In order to highlight the advantages of this model compared with traditional adaptive or fuzzy control methods, this article makes a supplementary comparative experiment on CICIDS2017 data set. Two representative methods are selected as the baseline: (1) Fuzzy Threshold System (FTS); (2) Anomaly detection framework of Model Reference Adaptive Control (MRAC). The comparison indexes include F1-score, average response delay (ms), accuracy decay rate (%/24h) in the concept drift scene and the detection rate of low-frequency APT attacks. The results are shown in Table 3.

Table 3: Performance comparison of the proposed model with classic adaptive/fuzzy methods

Method	F1-score	Average Response Delay (ms)	Daily Accuracy Decay Rate (%)	APT Detection Rate (%)
Proposed Model (LSTM+AE+GNN)	0.93	287	1.2	89.5
Fuzzy Threshold System (FTS)	0.76	320	3.8	52.1
MRAC-based Detector	0.71	410	5.6	48.7

The model in this article is significantly better than the traditional method in all indexes. Especially in the face of APT attacks with strong concealment and sparse behavior, thanks to GNN's contextual reasoning ability of attack chain, the detection rate is nearly doubled. In addition, under the concept drift caused by the dynamic change of network traffic pattern, this model is more stable in accuracy through online fine-tuning and dynamic weight mechanism. However, the classical fuzzy method still has advantages in the interpretability of rules, and this model, as a "black box" of deep learning, needs to be supplemented by an after-the-fact interpretation module in high security compliance scenarios.

Finally, test the performance of the system in scalability. By gradually increasing the number of working nodes (from 2 to 8), the change of overall processing capacity was observed. Figure 7 shows that when the cluster scale increases from 2 nodes to 6 nodes, the throughput increases approximately linearly, from 78,000 to 183,000. When it continues to increase to 8 nodes, the growth rate slows down, presumably due to the increase of metadata coordination overhead. This shows that the current architecture has good horizontal expansion ability under the medium-sized cluster.

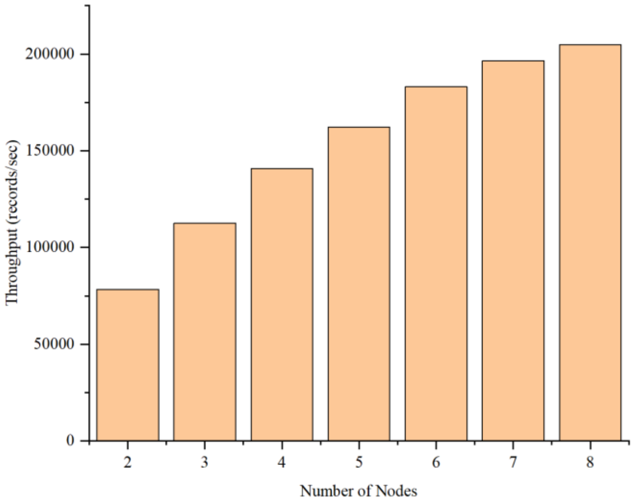

Figure 7: Relationship between cluster node number and system throughput

In addition to the routine throughput test, this article also carries out pressure verification on the system elasticity: after injecting sudden flow into Kafka, it is observed that Flink task automatically slows down due to back pressure, but no data loss occurs; When the flow rate drops, the system returns to the steady-state processing capacity within 90 seconds. In addition, Kubernetes is configured based on CPU utilization, which can automatically migrate tasks when simulating node failure to ensure service continuity.

6 Discussion

The intelligent early warning model proposed in this study is suitable for government affairs with high concurrency and high security requirements, and has good generalization ability in architecture and algorithm design, which can be extended to heterogeneous network scenarios such as IoT and key information infrastructure. This model captures the timing anomalies through LSTM, and models the dependencies between devices with GNN, thus effectively identifying complex threats such as cross-device cooperative attacks. Some challenges were also found in the experimental stage, such as slow convergence of GNN due to sparse graph structure in the initial training, or short-term false alarm triggered by legal large traffic during peak business hours, and the asset weight adjustment strategy needs to be further optimized. Nevertheless, the overall results show that the model can still maintain high stability and practicability in complex environment.

In view of the strict requirements of key infrastructure in highly sensitive areas, such as power, transportation, finance and so on, this study introduces dynamic weight adjustment and time attenuation suppression mechanism to significantly reduce alarm fatigue and improve operation and maintenance response efficiency. In terms of model interpretability, although the deep learning model is often regarded as a "black box", this article introduces gradient-based saliency map and SHAP method to explain it afterwards in the deployment stage. Taking the classification results of GNN nodes as an example, asset access frequency, source IP threat intelligence matching degree and abnormal port connection behavior, which play a leading role in high-risk judgment, can be identified by calculating the SHAP value of input features. At the same time, the visualization of the attention weight of LSTM layer shows that the model has paid high attention to the sudden increase of traffic and abnormal connection concurrency 10 minutes before DDoS attack, which proves its early warning ability. Although these explanatory means are not directly involved in training, they provide traceable decision-making basis for operation and maintenance personnel.

Aiming at the detection of zero-day attacks, the system is based on unsupervised/semi-supervised anomaly detection kernel, and uses LSTM and self-encoder to model massive normal traffic to identify unknown behaviors that deviate from known patterns. The GNN module analyzes the diffusion path and correlation of abnormal behavior in the network topology, and puts isolated events in the macro attack context to reduce the risk of omission. However, for advanced zero-day attacks whose behavior patterns are highly similar to normal traffic, the detection rate still has room for improvement. Future work will explore the feasibility of lightweight deployment on edge devices with limited resources, and further introduce external threat intelligence and federated learning mechanism to enhance the perception of unknown threats.

7 Conclusions

The challenges brought by massive logs and high-speed traffic often make traditional security tools difficult to cope with. This article tries to promote it from two aspects: engineering realization and algorithm innovation. The proposed hierarchical fusion architecture not only has the ability to handle more than 180,000 events per second, but also reduces the effective alarm by more than two thirds in real scenes, greatly reducing the pressure of operation and maintenance. In CICIDS2017 test, F1-score reached 0.93, indicating that the model has a strong ability to identify complex attacks, and its performance far exceeds that of regular systems such as Snort.

The model is not a simple technical stack, but a complete closed loop from data collection to risk pre-alarm. LSTM captures time series anomalies, GNN mines potential attack chains, and dynamic threshold and attenuation mechanism make alarms more context-sensitive. These components work together, enabling the system to detect threats and model their evolution. While the framework shows some limitations in handling zero-day attacks and concept drift, it demonstrates good overall scalability and adaptability.

Although the current architecture shows good horizontal expansion ability under medium-sized cluster, the behavior of the system under extreme network load or long-term operation scenarios still needs to be further discussed. Theoretically, thanks to Flink's stateful flow processing mechanism and Kafka's buffer decoupling design, the system has the flexibility to cope with the sudden increase of traffic. At the same time, the micro-service deployment structure also helps to maintain the stability of long-term operation. However, in a very large-scale or resource-constrained environment, coordination overhead and state consistency may become a new bottleneck, which will be an important direction for subsequent optimization.

References

[1] Boulkroune A, Hamel S, Zouari F, et al. Output-Feedback Controller Based Projective Lag-Synchronization of Uncertain Chaotic Systems in the Presence of Input Nonlinearities. Mathematical Problems in Engineering, 2017, 2017(1): 8045803. DOI: 10.1155/2017/8045803

[2] Boulkroune A, Zouari F, Boubellouta A. Adaptive fuzzy control for practical fixed-time synchronization of fractional-order chaotic systems. Journal of Vibration and Control, 2025: 10775463251320258. DOI: 10.1177/10775463251320258

[3] Cai, X., Wu, C., & Sheng, J. (2021). Spectrum situation awareness based on time-series depth networks for LTE-R communication system. IEEE Transactions on Intelligent Transportation Systems, 23(7), 8629-8640. DOI: 10.1109/TITS.2021.3083968

[4] Chen, J., & Miao, Y. (2021). Study on network security intrusion target detection method in big data environment. International Journal of Internet Protocol Technology, 14(4), 240-247. DOI: 10.1504/IJIPT.2021.118966

[5] DeValk, K., & Elmqvist, N. (2024). Riverside: A design study on visualization for situation awareness in cybersecurity. Information Visualization, 23(1), 40-66. DOI: 10.1177/14738716231118922

[6] Huang, B., Yao, H., & Wu, Q. B. (2025). Prediction and evaluation of wireless network data transmission security risk based on machine learning. Wireless Networks, 31(1), 405-416. DOI: 10.1007/s11276-024-03773-7

[7] Lan, X. (2021). Big data network security index correlation measure based on the fusion of modified two order cone programming model. International Journal of Internet Protocol Technology, 14(1), 16-22. DOI: 10.1504/ijipt.2021.113899

[8] Li, G., Hong, B., & Hu, H. (2022). Risk management of island petrochemical park: Accident early warning model based on artificial neural network. Energies, 15(9), 3278. DOI: 10.3390/en15093278

[9] Liu, D. (2020). Prediction of network security based on DS evidence theory. ETRI Journal, 42(5), 799-804. DOI: 10.4218/etrij.2019-0147

[10] Luo, X., Ma, Y., & Dang, X. (2024). Abnormal state warning system of network security management based on KD tree and KNN. Procedia Computer Science, 247, 1005-1011. DOI: 10.1016/j.procs.2024.10.121

[11] Ma, X. (2025). Research on network security situation awareness based on neural network. Procedia Computer Science, 261, 1165-1171. DOI: 10.1016/j.procs.2025.04.700

[12] Merazka L, Zouari F, Boulkroune A. High-gain observer-based adaptive fuzzy control for a class of multivariable nonlinear systems. 2017 6th International Conference on Systems and Control (ICSC). IEEE, 2017: 96-102. DOI: 10.1109/ICoSC.2017.7958728

[13] Rigatos G, Abbaszadeh M, Sari B, et al. Nonlinear optimal control for a gas compressor driven by an induction motor. Results in Control and Optimization, 2023, 11: 100226. DOI: 10.1016/j.rico.2023.100226

[14] Ullah, F., Turab, A., & Ullah, S. (2024). Enhanced network intrusion detection system for internet of things security using multimodal big data representation with transfer learning and game theory. Sensors, 24(13), 4152. DOI: 10.3390/s24134152

[15] Wang, H. (2021). Big data security management countermeasures in the prevention and control of computer network crime. Journal of Global Information Management (JGIM), 30(7), 1-16. DOI: 10.4018/JGIM.295450

[16] Wang, L., & Jones, R. (2021). Big data analytics in cyber security: network traffic and attacks. Journal of Computer Information Systems, 61(5), 410-417. DOI: 10.1080/08874417.2019.1688731

[17] Wang, Q., & Bu, S. (2020). Deep learning enhanced situation awareness for high renewable-penetrated power systems with multiple data corruptions. IET Renewable Power Generation, 14(7), 1134-1142. DOI: 10.1049/iet-rpg.2019.1015Digital Object Identifier (DOI)

[18] Wei, H., Zhao, X., & Shi, B. (2024). Research on neural networks in computer network security evaluation and prediction methods. International Journal of Knowledge-Based and Intelligent Engineering Systems, 28(3), 497-516. DOI: 10.3233/KES-23040

[19] Xie, B., Zhao, G., & Chao, M. (2020). A prediction model of cloud security situation based on evolutionary functional network. Peer-to-Peer Networking and Applications, 13(5), 1312-1326. DOI: 10.1007/s12083-020-00875-9

[20] Yang, Y., & Zhao, P. (2024). Research on dung beetle optimization based stacked sparse autoencoder for network situation element extraction. IEEE Access, 12, 24014-24026. DOI: 10.1109/ACCESS.2024.3365495

[21] Yu, Q., Ren, J., & Zhang, J. (2020). An immunology-inspired network security architecture. IEEE Wireless Communications, 27(5), 168-173. DOI: 10.1109/MWC.001.2000046

[22] Yu, Q. (2024). Network data privacy security aggregation method based on big data pattern decomposition. International Journal of Computer Applications in Technology, 74(1-2), 26-33. DOI: 10.1504/IJCAT.2024.141357

[23] Zhang, H., Kang, C., & Xiao, Y. (2021). Research on network security situation awareness based on the LSTM-DT model. Sensors, 21(14), 4788. DOI: 10.3390/s21144788

[24] Zhang, J., Feng, H., & Liu, B. (2023). Survey of technology in network security situation awareness. Sensors, 23(5), 2608. DOI: 10.3390/s23052608

[25] Zhang, R., Liu, M., & Yin, Y. (2020). Prediction algorithm for network security situation based on bp neural network optimized by sa-soa. International Journal of Performability Engineering, 16(8), 1171-1182. DOI: 10.23940/ijpe.20.08.p4.11711182

[26] Zhang, Z., Ning, H., & Shi, F. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review, 55(2), 1029-1053. DOI: 10.1007/s10462-021-09976-0

[27] Zouari F, Saad K B, Benrejeb M. Robust neural adaptive control for a class of uncertain nonlinear complex dynamical multivariable systems. International Review on Modelling and Simulations, 2012, 5(5): 2075-2103. https://www.scopus.com/pages/publications/84873265173