Research on Security Situation Assessment and Prediction Model of Network System in Deep Learning Environment

Li Xiao*, TianHeng Pan, Xiaoling Wu and YouKang Zhu

School of computer science and technology, Wuhan University of Bioengineering,
Wuhan, Hubei 430010 China
E-mail: xli00210@163.com
**Corresponding Author*

Received 06 July 2024; Accepted 13 August 2024

Abstract

With the development of the Internet, the network environment is increasingly complex, and the problem of network security is increasingly serious. Traditional passive network security technology has been unable to meet people's current security needs, in this context, network security situation awareness arises at the historic moment. NSSA technology makes the traditional passive security into active security, from the analysis of unilateral elements to the analysis of the overall security. As key technology of situation perception, security situation assessment and prediction can evaluate and predict the network security situation at the overall level, help network security managers understand the overall network security changes and take protective measures in advance when predicting the dangerous state, which has important research significance. This paper mainly studies the situation

Journal of Cyber Security and Mobility, Vol. 13_6, 1263–1282.
doi: 10.13052/jcsm2245-1439.1362

assessment and prediction technology of network security, and puts forward the improved model and algorithm, which improves accuracy of situation assessment and prediction results. Prediction accuracy reaches 97.86%, and the efficiency of the situation assessment reaches 98.22%.

Keywords: Situation assessment, situation prediction, improved algorithm, prediction model.

1 Introduction

With continuous development of computer technology, internet application has been more widely popularized [1, 2]. However, with development of network technology, structure of network system has become huge and complex, and the problem of network security has become increasingly prominent [3]. In recent years, the number of network security incidents and security vulnerabilities is increasing sharply. Cyber-attack means have become complex and diverse, and new attacks continue to appear in [4]. Large-scale DDOS attacks swept across North America, the new "worm" bitcoin ransomware WannaCry throughout the world, botnet HNS infected many Internets of things devices, nearly 100 million express company users' private information was leaked and other security incidents frequently, endangering the interests of individuals, countries and even the whole world. According to statistics, the number of security vulnerabilities included in the national information security vulnerability sharing platform increased by 47.4% in 2017 compared with 2016, reaching 15,955, and the number of vulnerabilities also reached a record high.

The first step in NSSA (Network Security Situation Awareness) is to collect data from the network, perform data fusion, and establish a NSSA model based on this. Data fusion is the collection, association, extraction, combination, and analysis of data from multiple information sources [5, 6]. Since scholars began studying situational awareness, after decades of development, situational awareness has centered around data fusion and proposed dozens of network situational awareness models. There are mainly Boyd control models, such as OODA control loop model and JDL data fusion model. Later, some scholars improved the JDL data fusion model and developed new improved models, such as the Cyber SA model proposed by Tadda et al. and the CSA research model proposed by Gong Zhenghu et al. The famous one is the Bo1yd control model (OODA model), which consists of four stages: observation, guidance, decision-making, and action, forming a control process loop. The OODA model fully demonstrates the dynamic execution process of situational awareness, and its cyclic structure and dynamic collaboration can adapt to complex cyberspace situational awareness. The JDL (Joint Directors of Laboratories) data fusion model has the widest impact. Situation awareness, as the second level fusion, receives network element data from the first level fusion downwards as the source of information for situation awareness.

In order to deal with such a severe network security problem, a variety of network security protection equipment system is installed and deployed, but these are the security measures taken in a single dimension, with targeted and limited characteristics [7, 8]. The single-function network security equipment cannot provide global network information for the administrators, and it is not easy to help the network administrators make timely and effective decisions. The security information generated by these devices will also become an "information island" with the lack of correlation analysis of security event information. If massive heterogeneous information is gathered, the valuable information will be submerged in much information. Therefore, there is an urgent need for a new defense technology to reflect the overall security situation in real time so that security managers can take adequate measures to deal with the abnormalities.

The deep integration of industrial control systems and the Internet has exposed them to many threats and attacks, which has had a serious impact on national security, economic development and social stability [9]. Therefore, situation awareness can be used to effectively monitor and control the overall operation of industrial control systems, so as to ensure the safe operation of industrial control systems. The research on situational awareness is still in its early stages, and there are still many problems that need to be improved and solved. However, with the continuous improvement of relevant technologies and research, situational awareness will definitely have greater development, and its advantages and characteristics will be utilized to provide strong guarantees for network security [10]. Situation information is mainly extracted through methods such as firewall logs, intrusion detection logs, virus logs, and network scans.

In this context, the concept of NSSA was put forward and quickly became a hot spot. The network security situation refers to the network security state and its change trend under the joint action of all the security elements in the target system. Network security status is divided into qualitative and quantitative representation methods; qualitative representation refers to using keywords such as high risk, medium risk, and low risk to indicate the level of network harm; quantitative representation refers to using numbers to measure the level of network security. Among them, the situation assessment technology and the situation prediction technology are the core content of the network security situation perception. NSSA still needs to improve its development processes, such as the rationality of the evaluation model, the effectiveness of the evaluation method, the accuracy of the prediction results, and others. This paper puts forward the improvement method and establishes a reasonable model to expand new ideas for the research of NSSA. NSSA can help network security management personnel to grasp the current network overall security changes, targeted formulation and adjust the corresponding security strategy, take active response measures to protect the security of the host and the network, make the traditional passive defense system into an active defense system, reduce the possibility of network attacks and reduce harm. Therefore, studying network security situational awareness can improve the network system's security, which is significant in its application.

2 Situational Awareness Model of Network Security

2.1 JDL Model

NSSA includes three levels: situational extraction, understanding, and security prediction, and is a complete cognitive process. Although research in this field has received considerable attention for a long time, a clear, consistent goal and system still need to be formed. New technologies are still constantly evolving. The rapid development of big data and machine learning technology has played a good role in developing NSSA technology. The neural network-based network security situational awareness technology is currently one of the most promising methods. The JDL model was first proposed in the 1990s by the US Department of Defense. On this basis, after continuous evolution and extensive use, it has become a standard model and profoundly impacted subsequent model research [11, 12].

The model mainly consists of three parts, which are information source, data fusion and human-machine interface. Data fusion is an important central part of the model. The following is the main introduction of this part:

(1) Zero-layer, data preprocessing: integrate and filter multi-source data information, and merge relevant information to achieve the purpose of streamlining data information;
(2) The first layer, object evaluation: according to the characteristics of the object, the preprocessed data is featuring extraction, clustering,

classification and other operations, so as to facilitate later higher level of data;

(3) The second layer, situation assessment: according to the constructed data set, describe the relationship between the evaluation target and the observation behavior, and integrate the data of various aspects through the intelligent algorithm to achieve the goal of evaluating the current network security situation;

(4) The third layer, threat assessment: forecast future security situation, and analyze the possible threats;

(5) The fourth layer, process evaluation: this is a process of dynamic fusion. First, the real-time and accurate prediction results are obtained, and then the whole fusion process is optimized through feedback information.

2.2 TimBass Model

Traditional security protection only relies on static detection. Passive defense is not suitable for protecting against new network threats such as advanced persistent threats and Oday attacks. From the current technology perspective, existing security defense measures cannot effectively solve network security problems. It is urgent to optimize and improve traditional security defense methods, and form a comprehensive security system that can respond to diverse and persistent threats.

The TimBass model is a network security situational awareness framework based on multi-source data fusion, and has been widely used after [13]. The data source of intrusion detection has gone through three levels of abstraction, namely data, information and knowledge. The realization of network security situational awareness also evolves layer by layer in the five hierarchical structures [14, 15].

(1) The zero-layer, data extraction: from a variety of detection tools (such as intrusion detection sensors), collect the alarm information affecting the network security situation;

(2) The first layer, security event extraction: standardize the data extracted from the upper layer, and conduct correlation processing according to the time and space attributes, remove repeated alarms, so as to extract simplified and reliable security events;

(3) The second layer, situation extraction: the comprehensive correlation analysis of the extracted security events in the first layer, to obtain the overall security situation of the network;

(4) The third layer, threat assessment: to measure the degree of damage caused by security incidents, so network administrators can take targeted defensive measures;

(5) The fourth layer, resource management: real-time monitoring and evaluation of whole NSSA system, and can dynamically display the changing trend of the security situation.

2.3 NSSA System Framework

Above classic NSSA model has laid a foundation for research, its basic theories and ideas guide the subsequent research, many scholars will gradually improve and improve it, and put forward a variety of framework [16].

Figure 1 presents the situation sequence analysis of network security. The system framework of this paper contains three layers of structure, namely, situation acquisition, situation assessment and situation prediction. The situation acquisition part first obtains the vulnerabilities of the host, the environment information of the host assets, and the alarm data generated, and obtains simplified and highly credible security event information by preprocessing the alarm data. The assessment part is core, the first security events and vulnerability information, asset environment information, on the basis of building attack knowledge base analysis of successful support, and then a single host asset as the unit, the severity of the security event itself, asset value and the successful support of security threat, and establish an evaluation model to host security situation value. Situation prediction is ultimate goal, that is, to predict network security situation at the next moment according to the historical situation information in a specific period of time, so that the security administrator can understand the current and future security state, and take security measures in advance when predicting the more dangerous security state.

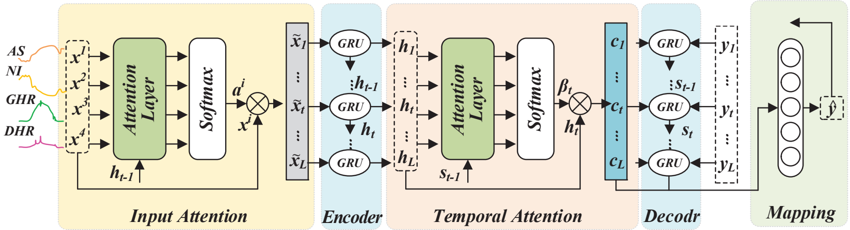


Figure 1 Serial analysis of network security situation.

3 Key Technologies of NSSA

3.1 Situation Assessment Technology

The knowledge-based reasoning method is represented by fuzzy reasoning, Bayesian networks, Markov processes, D-S evidence theory, etc., and evaluates the security situation through logical reasoning. Bayesian networks are the most commonly used method in situational assessment research, catering to situational assessment's dynamic and uncertain characteristics by introducing dynamic Bayesian networks for probabilistic inference about time. The reasoning process is becoming increasingly complex in practical applications, making applying to large-scale networks for evaluation challenging. The method based on pattern recognition establishes a situation template. It completes the division of the situation through pattern matching, mainly represented by grey correlation analysis, rough set theory, and neural networks. With the development of chips and computing technology, computing power is becoming more robust, and machine learning methods are receiving more and more attention from scholars. Based on a reasonable evaluation model, the situation data is analyzed, filtered, and integrated according to specific rules as input. A reasonable model or algorithm quantification obtains the security situation value, which describes the current network security state.

Figure 2 presents the hierarchical analysis method of situation assessment. It uses IDS alarm data, vulnerability data and network performance index data as data sources. It starts from lower level, and integrates the security data information of each layer to finally obtain the security situation of the whole system of the network. This evaluation method can be summarized as "bottom-up, first part and then whole".

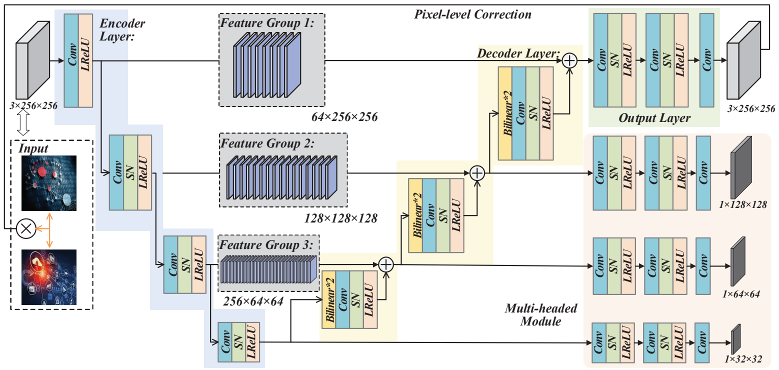


Figure 2 Hierarchical analysis method of situation assessment.

First, the attack/vulnerability layer found which attacks occurred on the host open services, and refer to the Snort user manual to statistics and analyze the severity of the attack event [17, 18]. The severity of all attacks can be classified as high, medium, and low. For example, the severity of root permission is high, and the severity of denial-of-service attack is low. Then, we combine the service importance parameter at the service layer and calculate the Services Threat Index; while the importance of services is dynamically changing, The importance of different services should be attributed to multiple levels according to the number of users, statistical access frequency and experience parameters; The host layer depends on the importance weight of the host and the data provided by the service layer, Calculate the host threat index, The importance weight of the host is often given based on the expert experience; last, The system threat index is calculated in the system layer based on the host layer data, Integrate the security state of each host to obtain the overall security situation of the network, The results are visualized graphically.

Figure 3 presents D-S evidence theory probability analysis, D-S evidence theory is a method based on knowledge reasoning, it does not need to know the prior probability and conditional probability, with the confidence function as the measurement criterion, can well represent uncertain information, is widely used to solve the uncertainty of ambiguity and randomness, meet weaker conditions than Bayesian probability theory. Identification framework represents a set of compartmentalization under all possible target regions, where each subset is called a proposition [19]. Its essence is a method to realize the logical reasoning based on the posterior probability, which

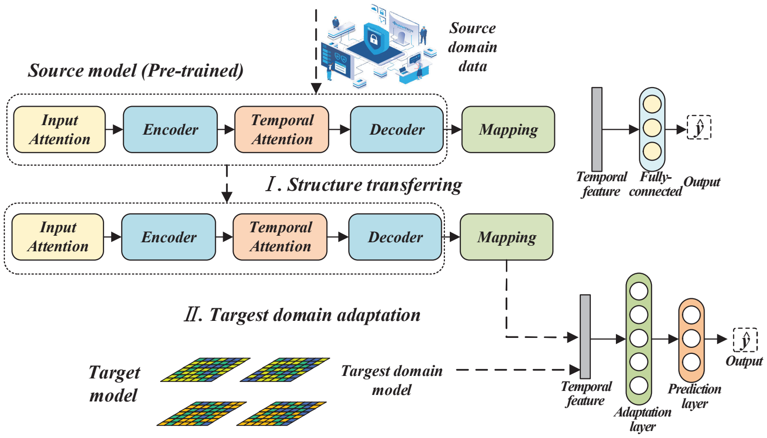


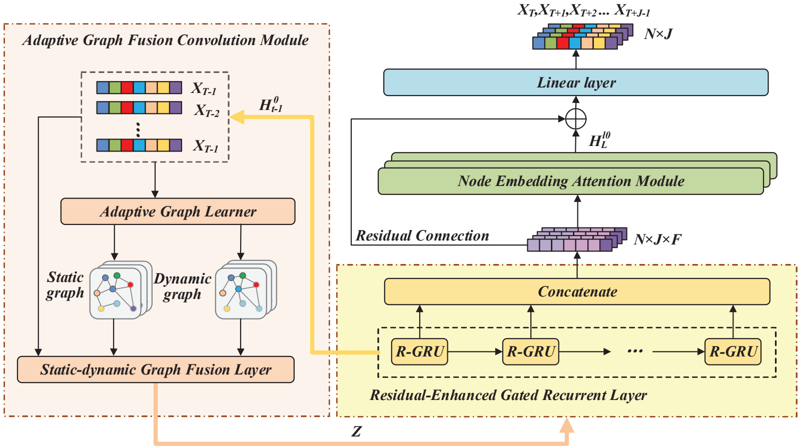
Figure 3 Probistic analysis of D-S.

can solve the reasoning process with intrinsic uncertain factors [20]. The security is often complex and variable, so it is suitable to apply the Bayesian process to the NSSA. It has the advantages of good real-time, high degree of configuration, simple and accurate, so it has been widely applied by many scholars [21, 22].

3.2 Situation Prediction Technology

The prediction method establishes a regression model by curve fitting and parameter estimation through the historical sequence data obtained from the system and digs out the law of its change over time to predict the sequence data in the future [23, 24]. Linear prediction models are used to predict linear distributed sequence data, while non-linear models are used to predict non-linear distributed sequence data [25]. The construction of non-linear prediction model usually requires based on prior knowledge and is a parameterized model, but in fact, because of dynamics and randomness of system, the determined model structure cannot accurately reflect all the key features contained in the system, so the prediction accuracy is not high [26, 27]. Although this method can realize the mapping of the construction time to the security situation value to some extent, there are problems such as accurate parameter estimation and model order in the process of model building.

Figure 4 presents prediction flow path. The prediction method does not determine mathematical model of sequence data in advance, but builds the



$X_T, X_{T+1}, X_{T+2} \dots X_{T+J-1}$
N×J
Adaptive Graph Fusion Convolution Module
X_{T-1}
X_{T-2}
X_{T-1}
H^0_{t-1}
Linear layer
H^{l0}_L
Node Embedding Attention Module
Adaptive Graph Learner
Residual Connection
N×J×F
Static graph
Dynamic graph
Concatenate
R-GRU
R-GRU
...
R-GRU
Static-dynamic Graph Fusion Layer
Residual-Enhanced Gated Recurrent Layer
Z

Figure 4 Prediction flow path.

prediction model through the learning of sample sequence data. The advantages of neural networks are their ability to perform nonlinear mapping and good self-learning and adaptation. By constantly adjusting the weights of the input training sample, the situation prediction model can be built [28, 29]. A typical neural network is radial base neural network, which is widely used and has high research value. The algorithm enhances the model's applicability by introducing kernel functions to solve the "dimension disaster" problem. Compared with the neural network algorithm, the model construction is more straightforward, and the number of parameters that need to be determined is less. At the same time, it can accurately fit the data and dig out the potential value and law in the data.

4 Experimental Results

4.1 Data Preprocessing

In order to verify the accuracy of the IFOA _ SVR situation prediction method proposed in this paper, the evaluation method is used to obtain the trend sequence value for 13 days. For one situation value per hour, there are 300 trend values. The first 270 situation values were selected to construct the training set, and the last 30 were used to construct the test set [30]. In order to prevent the impact on the prediction results due to the large original data span, these security situation values are first normalized. The normalization formula is shown in formula (1), x is the essential feature, and $\hat{x}$ is the norm result.

$$\hat{x} = \frac{x - x_{min}}{x_{max} - x_{min}} \tag{1}$$

The index calculation formula is shown as in formula (2), (3) and (4). y_i' is the predicted value, and y_i is the true value.

$$e = |y/ - y| \tag{2}$$

$$MAPE = \frac{1}{n}\sum_{i=1}^{n}\frac{|y_i' - y_i|}{y_i} \tag{3}$$

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i' - y_i)^2} \tag{4}$$

For the classification problems, the loss function is used, as shown in formula (5). L is the loss result, and p is the probability value.

$$L = -\frac{1}{N}\sum_{i=1}^{N} y_i log(p(y_i|x_i)) + (1 - y_i)log(1 - p(y_i|x_i)) \tag{5}$$

Security posture assessment indicators include various measures, such as attack detection rate (TPR), false alarm rate (FPR), and their combination, such as the area under the ROC curve (AUC) derived from formula (6) and formula (7).

$$TPR = \frac{TP}{TP + FN} \tag{6}$$

$$FPR = \frac{FP}{FP + TN} \tag{7}$$

Safety situation prediction involves time series analysis or state transfer model. Autoregressive moving average model (ARMA), as indicated in formula (8). Φ_i is the decisive factor coefficient, θ_i is the parameter values.

$$X_t = c + \sum_{i=1}^{p} \Phi_i X_{t-i} + \sum_{i=1}^{q} \theta_i e_{t-i} + e_t \tag{8}$$

Accuracy is a commonly used measure of classification model performance, which is shown in formula (9):

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \tag{9}$$

The F1 score is a comprehensive measure of precision and recall, and is calculated as shown in formula (10).

$$\mathrm{F1} = 2 \cdot \frac{\text{Precision} - \text{Recall}}{\text{Precision} + \text{Recall}} \tag{10}$$

The Precision and Recall are calculated in formula (11) and (12), respectively.

$$Precision = \frac{TP}{TP + FP} \tag{11}$$

$$Recall = \frac{TP}{TP + FN} \tag{12}$$

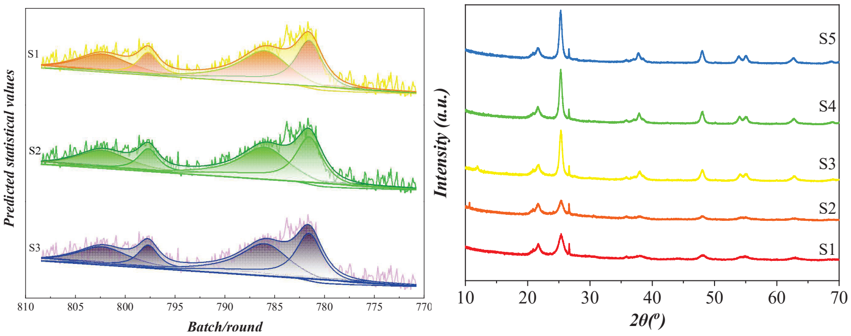


Figure 5 Results of the situation forecast indicators.

4.2 Experimental Process and Result Analysis of Situation Prediction

This section uses Python's machine learning library to implement the situation prediction method based on IFOA _ SVR, conduct experimental verification and result analysis, and prove that this method can effectively predict the situation value. The time series embedding dimension n is set to 10 to generate a dataset of the corresponding dimension. By calculating the prediction result index value of this method, the results are shown in Figure 5.

4.3 Comparison with The Results of Other Prediction Methods

In order to further illustrate that the prediction method of this paper is better than other methods, support vector regression is used to verify prediction method.

In the situation prediction experiment scheme based on FOA _ SVR, the fly population size was set to 20. Similarly, single step prediction is used to predict last situation value with the first 10 safety situation values. After iterative optimization of the Drosophila algorithm, the optimal parameter value C = 32.384625490, g = 12.327590332.

Figure 6 shows the distribution of the coefficient of determination of situation prediction. In the situation prediction, 55 experiments based on PSO _ SVR, the particle swarm size is set to 20, the maximum number of iterations is 200, and the learning factor c; the value is 1.4. The situation prediction model is constructed with a coefficient of determination of 0.829745805, the optimal parameter value C = 102.904678911, and g = 8.774037521. The comparison shows that the coefficient of determination is still lower. When the group intelligent algorithms selected parameters, each algorithm

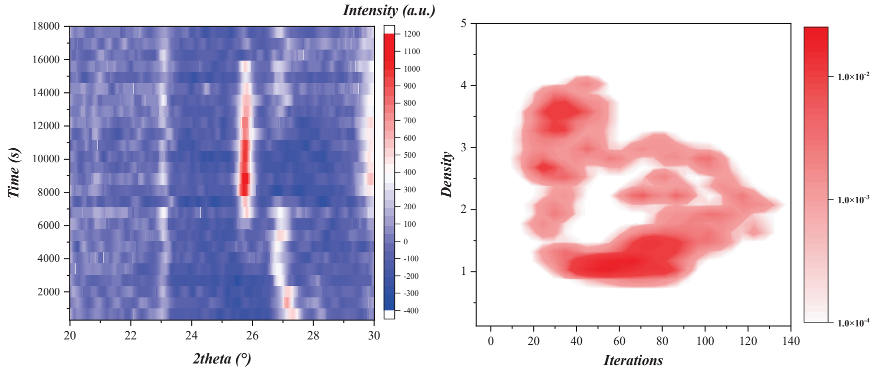


Figure 6 Distribution of coefficient of determination of situation prediction.

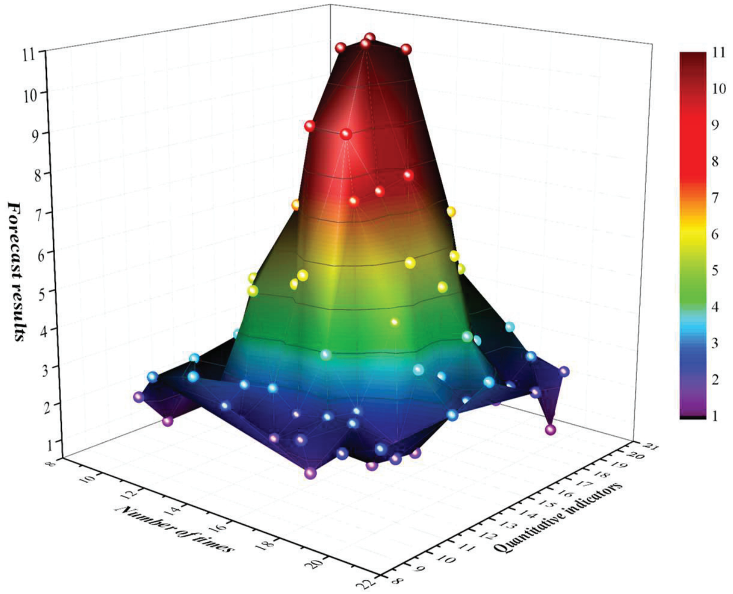


Figure 7 Situation forecast fitness curve.

underwent 200 iterations, and the coefficient of determination obtained was taken as fitness.

Figure 7 for the situation forecast fitness curve of fitness curve, as can be seen from the improvement of the fruit fly algorithm in about 70 generations, in the early iteration on the whole in the optimal state, the rise of fitness value is larger, because the dynamic search step of fruit fly optimization algorithm in the early stage of the iteration, global optimal ability, can search better value on the global, thus not easy into the local optimal. In late stage of iteration, fitness value rise is small and gradually tends to converge the stable state, because the Drosophila optimization algorithm with dynamic search step size has strong local optimization ability in the late stage of the iteration and can search more refined solutions than the current one. The Drosophila algorithm converges around 80 generations, converges slower than the improved algorithm, and achieves lower fitness values, resulting in poor final prediction accuracy. The particle swarm algorithm converges to about 45 generations. It only obtains a suboptimal result, eventually leading to low accuracy in network security situation measurement. The improved Drosophila optimization algorithm can realize global-wide optimization and local fine optimization. Compared with the Drosophila optimization algorithm and particle swarm algorithm, it has better optimization ability and gets better parameters to improve the prediction accuracy of the situation value. After obtaining the best parameters, the above three algorithms input the best parameters and the training set to train support vector regression again to build the new prediction model, which is then tested with the test set. In comparing the error values of IFOA _ SVR, FOA _ SVR, and PSO _ SVR between the prediction results and the actual results, 16 trend error values in the prediction results of IFOA _ SVR are less than FOA _ SVR and PSO _ SVR by 80%. In comparison, only four trend error values are more significant than FOA _ SVR and PSO _ SVR, further proving that, on the whole, the IFOA proposed prediction method _ SVR has better prediction results and higher accuracy.

5 Conclusion

This paper mainly studies network security situation assessment and prediction technology. Aiming at shortcomings of safety situation based on hidden model and safety situation method, the improved model and prediction algorithm are proposed, which improves accuracy of evaluation and prediction results. The main contributions are as follows:

(1) This paper introduces the development status of network security and analyzes the significance of studying NSSA. This paper introduces several typical NSSA models. Summarize the classic situation assessment and prediction methods.

(2) After collecting the small network data and comparing the experiment, the results show that evaluation has a good consistency between the situation value and the alarm event, which improves accuracy of situation assessment results and provides reasonable and reliable situation data for situation prediction.

(3) In order to predict the future safety situation value more accurately, the situation prediction method is studied. According to the problem, a safe method based on IFOA _ SVR is proposed. This paper puts the dynamic search step improvement of Drosophila optimization algorithm IFOA, balance the global optimization and local optimization ability, improve the convergence accuracy and convergence speed. Using the evaluated sequence value of historical situation, the method is compared with other prediction methods to optimize SVR parameters, and the results show that this method improves the prediction accuracy of network security situation, and has obvious advantages. The prediction accuracy reached 97.86%, and the efficiency of the situation assessment reached 98.22%.

The application prospects of deep learning in the field of network security are very broad, and its prospects are constantly growing with the improvement of big data processing capabilities and the continuous upgrading of computing power. Although deep learning faces many challenges in the field of network security, research on network security models based on deep learning remains an important direction in the foreseeable future. Future work can start from the following aspects: firstly, data collection and annotation to make up for the problem of insufficient data; The second is to enhance the robustness of deep learning models to better adapt to diverse attacks; The third is to use GPU acceleration training to improve the training speed of the model.

Funding

This study is supported by 2022 Hubei Provincial Department of Education Research Program Guidance Project, NO. B2002306.

References

[1] R. Zhang, Z. Pan, Y. Yin, and Z. Cai, “A Model of Network Security Situation Assessment Based on BPNN Optimized by SAA-SSA,”

International Journal of Digital Crime and Forensics, vol. 14, no. 2, 2022.

[2] G.-F. Yu, “A multi-objective decision method for the network security situation grade assessment under multi-source information,” *Information Fusion*, vol. 102, 2024.

[3] D. Zhao, G. Ji, and S. Zeng, “Network security situation assessment based on dual attention mechanism and HHO-ResNeXt,” *Connection Science*, vol. 35, no. 1, 2023.

[4] R. Zhang, M. Liu, Z. Pan, and Y. Yin, “Network Security Situation Assessment Based on Improved WOA-SVM,” *Ieee Access*, vol. 10, pp. 96273–96283, 2022.

[5] H. Yang, R. Zeng, G. Xu, and L. Zhang, “A network security situation assessment method based on adversarial deep learning,” *Applied Soft Computing*, vol. 102, 2021.

[6] H. Wang, D. Zhao, and X. Li, “Research on Network Security Situation Assessment and Forecasting Technology,” *Journal of Web Engineering*, vol. 19, no. 7–8, pp. 1239–1265, 2020.

[7] L. Yuan, “Prediction of network security situation awareness based on an improved model combined with neural network,” *Security and Privacy*, vol. 4, no. 6, 2021.

[8] Y. Zhu and Z. Du, “Research on the Key Technologies of Network Security-Oriented Situation Prediction,” *Scientific Programming*, vol. 2021, 2021.

[9] H. Sun, J. Wang, C. Chen, Z. Li, and J. Li, “ISSA-ELM: A Network Security Situation Prediction Model,” *Electronics*, vol. 12, no. 1, 2023.

[10] Y. Wang, Y. Yang, R. Gao, S. Li, and Y. Zhao, “A Security Situation Prediction Model for Industrial Control Network Based on EP-CMA-ES,” *Ieee Access*, vol. 11, pp. 135449–135462, 2023.

[11] D. Zhao, P. Shen, and S. Zeng, “ALSNAP: Attention-based long and short-period network security situation prediction,” *Ad Hoc Networks*, vol. 150, 2023.

[12] Y.-X. Wu and D.-M. Zhao, “Build IPSO-ABiLSTM Model for Network Security Situation Prediction,” *Journal of Information Science and Engineering*, vol. 40, no. 1, pp. 71–88, 2024.

[13] S. Duraibi and A. Mujawib Alashjaee, “Enhancing Cyberattack Detection Using Dimensionality Reduction With Hybrid Deep Learning on Internet of Things Environment,” *IEEE Access*, vol. 12, pp. 84752–84762, 2024.

[14] M. Luan, B. Wang, Y. Zhao, and F. Hu, "Anomalous Subgraph Detection in Given Expected Degree Networks With Deep Learning," *Ieee Access*, vol. 9, pp. 60052–60062, 2021.

[15] E. H. Salman, M. A. Taher, Y. I. Hammadi, O. A. Mahmood, A. Muthanna, and A. Koucheryavy, "An Anomaly Intrusion Detection for High-Density Internet of Things Wireless Communication Network Based Deep Learning Algorithms," *Sensors*, vol. 23, no. 1, 2023.

[16] K. Haciefendioglu, F. Mostofi, V. Togan, and H. B. Basaga, "CAM-K: a novel framework for automated estimating pixel area using K-Means algorithm integrated with deep learning based-CAM visualization techniques," *Neural Computing & Applications*, vol. 34, no. 20, pp. 17741–17759, 2022.

[17] L. Xiong, J. Liu, B. Song, J. Dang, F. Yang, and H. Lin, "Deep learning compound trend prediction model for hydraulic turbine time series," *International Journal of Low-Carbon Technologies*, vol. 16, no. 3, pp. 725–731, 2021.

[18] R. Dong, B. Wang, and K. Cao, "Deep Learning Driven 3D Robust Beamforming for Secure Communication of UAV Systems," *IEEE Wireless Communications Letters*, vol. 10, no. 8, pp. 1643–1647, 2021.

[19] D. Tian, Y. Han, B. Wang, T. Guan, and W. Wei, "RETRACTED: A Review of Intelligent Driving Pedestrian Detection Based on Deep Learning (Retracted Article)," *Computational Intelligence and Neuroscience*, vol. 2021, 2021.

[20] G. Nguyen, S. Dlugolinsky, V. Tran, and A. Lopez Garcia, "Deep Learning for Proactive Network Monitoring and Security Protection," *Ieee Access*, vol. 8, pp. 19696–19716, 2020.

[21] M. Hamian, K. Faez, S. Nazari, and M. Sabeti, "A novel learning approach in deep spiking neural networks with multi-objective optimization algorithms for automatic digit speech recognition," *Journal of Supercomputing*, vol. 79, no. 18, pp. 20263–20288, 2023.

[22] B. Long, Z. Chen, T. Liu, X. Wu, C. He, and L. Wang, "A Novel Medical Image Encryption Scheme Based on Deep Learning Feature Encoding and Decoding," *Ieee Access*, vol. 12, pp. 38382–38398, 2024.

[23] L. Almuqren, M. Maray, S. S. Aljameel, R. Allafi, and A. A. Alneil, "Modeling of Improved Sine Cosine Algorithm with Optimal Deep Learning-Enabled Security Solution," *Electronics*, vol. 12, no. 19, 2023.

[24] Z. Guan, P. Zhao, X. Wang, and G. Wang, "Modeling Radio-Frequency Devices Based on Deep Learning Technique," *Electronics*, vol. 10, no. 14, 2021.

[25] J. Guan, R. Lai, H. Li, Y. Yang, and L. Gu, "DnRCNN: Deep Recurrent Convolutional Neural Network for HSI Destriping," *Ieee Transactions on Neural Networks and Learning Systems*, vol. 34, no. 7, pp. 3255–3268, 2023.

[26] X. Liu, C. Qian, W. Yu, D. Griffith, A. Gopstein, and N. Golmie, "Using Deep Reinforcement Learning to Automate Network Configurations for Internet of Vehicles," *Ieee Transactions on Intelligent Transportation Systems*, vol. 24, no. 12, pp. 15948–15958, 2023.

[27] N. G. B. Amma, "A vector convolutional deep autonomous learning classifier for detection of cyber attacks," *Cluster Computing-the Journal of Networks Software Tools and Applications*, vol. 25, no. 5, pp. 3447–3458, 2022.

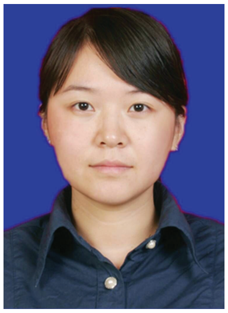
[28] V. Nasir and F. Sassani, "A review on deep learning in machining and tool monitoring: methods, opportunities, and challenges," *International Journal of Advanced Manufacturing Technology*, vol. 115, no. 9–10, pp. 2683–2709, 2021.

[29] S. V. Mahadevkar et al., "A Review on Machine Learning Styles in Computer Vision-Techniques and Future Directions," *Ieee Access*, vol. 10, pp. 107293–107329, 2022.

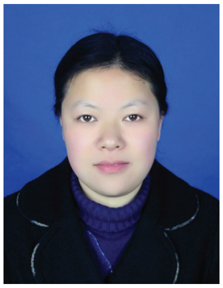
[30] J. Cui et al., "Collaborative Intrusion Detection System for SDVN: A Fairness Federated Deep Learning Approach," *Ieee Transactions on Parallel and Distributed Systems*, vol. 34, no. 9, pp. 2512–2528, 2023.

Biographies

Li Xiao, graduated from Wuhan University of Technology in 2015, I am currently a lecturer at Wuhan University of Bioengineering, with a research focus on machine learning and intelligent software engineering.



Tianheng Pan, graduated from Zhongnan University of Economics and Law in 2008, I am currently employed at Wuhan University of Bioengineering, Research interests include software engineering and computer application technology.



Xiaoling Wu, graduated from the School of Computer Science, Wuhan University in 2012 with a PhD in Engineering. I am currently an associate professor at the School of Software Engineering, Wuhan University of Biotechnology, with a main research focus on intelligent software engineering.

Youkang Zhu, graduated from Jiangxi University of Science and Technology in 2019, majoring in Computer Science and Technology. Full-time teacher and lecturer of Wuhan College of Biological Engineering. Research interests in intelligent computing and computational migration.