Proceedings of the 3rd International Conference on Mechatronics and Smart Systems
DOI: 10.54254/2755-2721/117/2025.20956

Survey of Research on Network Security Situation Awareness Technology Based on Machine Learning

Siming Chen[1,a,*]

[1]*College of Information and Intelligent Science and Technology, Hunan Agricultural University, Changsha, Hunan, China*
a. 3359781311@stu.hunau.edu.cn
**corresponding author*

Abstract: As the development of progress of the cyberization, the networking environment is becoming increasingly complex. Therefore, normal passive defense technology has been unable to meet the need for basic cybersecurity. Nowadays, network security situational awareness active defense technology based on machine learning has become one of the key research topics in the field of cybersecurity. According to the model classification, three types of techniques will be discussed separately— situation analysis of network security based on improved SKNet-SVM, network security situation assessment based on GA-Light and network security situation prediction based on Radial Basis Function neural network, draw schematic diagrams for these three types of technologies based on the literature, explain the workflow of these three types of technologies through schematic diagrams and the advantages and disadvantages of the three will be summarized. In the end, the current flaws in the field and will be analyzed. Meanwhile, suggestions for future development directions will be provided.

Keywords: cyber security, SKNet-SVM, GA-LightGBM, RBF neural network.

1. Introduction

With the advent of information age, Internet has penetrated into every corner of the world, the Internet accelerates the pace of the world's integrated and coordinated development. But at the same time, complexity of network environment has also brought more problems and challenges to network security. In 2023, over 80 countries were frequently subjected to cyber-attacks, such as the APT attack called "Triangular Operation" targeting Apple devices, the GoAnywhere attack on Fortra in the United States, and the IOS XE attack on Cisco. With the development of Internet technology, network attacks are becoming increasingly diversified, traditional network security defense techniques cannot fully resist new types of network attacks, the academic research on the situation of network security is becoming increasingly in-depth. Based on combination of machine learning technology, a new network security protection system based on intelligent perception, evaluation, and prediction of Network Security Situation (NSS) has emerged [1].

In 1999, Bass et al. first applied situational awareness to cyberspace and proposed the concept of network situational awareness [2]. In 2013, after General Secretary Xi Jinping proposed that "without cybersecurity, there can be no national security", China began to vigorously develop the field of cybersecurity [3]. So far, many scholars have conducted in-depth research on network security

DOI: 10.54254/2755-2721/117/2025.20956

situational awareness technology and integrated different technologies into network security situational awareness technology to improve its performance and accuracy. For example, scholars such as Guo Shangwei and Liu Shufeng proposed a model-based network security situational awareness method in the Journal of Computer Engineering. This method integrates models of Stack Sparse Autoencoder (SSAE), Convolutional Neural Network (CNN), Bidirectional Gated Recurrent Unit (BiGRU), and Attention Mechanism (AM). SSAE and CNN are used to extract data features, and network security situational quantification indicators are combined to classify network threats [4];Chen Ming and Gao Jinhu scholars proposed a cybersecurity situational awareness technology based on threat intelligence in an intelligence journal, this technology fully utilizes relevant knowledge from fields such as security, intelligence, and systems engineering to construct a cybersecurity situational awareness model based on threat intelligence and detect, understand, and threaten network security threats in the "physical social information" three-dimensional space [5];Scholars Wang Chenfei, Xu Liyang, Li Huiqin, and Ma Jianxun suggested a situational awareness system for network security based on constructing behavior portraits, this mechanism obtains statistical feature labels through data mining and utilizes the modeling ability of bidirectional long short-term memory (BiLSTM) neural network to form behavioral feature labels for user behavior, the two types of tags are used to jointly build the portrait, and the threat level is defined according to the similarity between the portrait [6].

This paper discusses three kinds of technologies - evaluation of the state of network security technology on the basis of improved SKNet-SVM, review of the state of network security technology through LightGBM, and predictive technology for network security situations based on neural network. According to the literature, schematic diagrams of these three types of technologies are drawn. Through the schematic diagrams, the workflow of these three types of technologies is explained and the advantages and disadvantages of these three types of technologies are summarized, the technology of network situation awareness based on machine learning is deeply studied.

2. Network Security Situation Assessment Technology Based on Improved SKNet-SVM

2.1. Situation Assessment Model Based on Improved SKNet-SVM

The situation assessment model on the basis of improved SKNet-SVM mainly consist of four modules, namely, data preprocessing module, feature extraction module, attack classification module and situation value calculation module. The specific framework is shown in Figure 1:

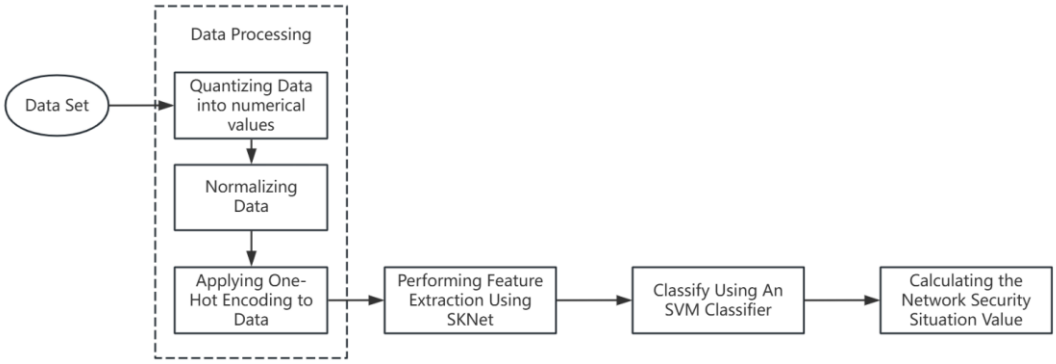

Figure 1: A Situation Assessment Model Based on Improved SKNet-SVM

Before SVM classification, the model needs to use an improved SKNet convolution neural network to extract features from the preprocessed dataset, then select the features that have a significant impact on the data samples, and then use the SVM classifier to classify, finally, based on

DOI: 10.54254/2755-2721/117/2025.20956

the classification results, calculate the network security situation value [7]. This model is mainly used to enhance the stability and robustness of the system, and is generally used in important fields such as large enterprises and financial institutions, it can monitor the network traffic in real time and warn potential network attacks in time.

2.2. Advantages And Disadvantages of Situation Assessment Technology Based on Improved SKNet-SVM

The improved SKNet convolution neural network technology is integrated into SVM technology to accelerate the convergence speed of the model. In terms of improving prediction accuracy, Chen et al. have integrated the idea of regression prediction [8]. The effective features screened by SVM classifier reduce the order of magnitude of feature parameters and the amount of calculation and improve stability and efficiency of network security situation assessment. Compared with the single SVM classification model, the improved SKNet-SVM model has better classification effect and significantly improved accuracy.

However, the integration of technologies enhances the complexity of the model and has a great impact on the performance of network security situation evaluation. Therefore, a long way is needed to go in the future to reduce model complexity and improve technical efficiency.

3. Network Security Situation Assessment Technology Based on Lightweight Gradient Elevator

3.1. GA-LightGBM Network Security Situation Assessment Model

The GA-LightGBM network security situation assessment model which is based on PRF-RFE CV feature optimization consists of three modules, namely, Situation Extraction Module (SEX M), situati-on Assessment Module (SASM), and Situation Visualization Module (SVM) [9]. T he specific architecture is shown in Figure 2:

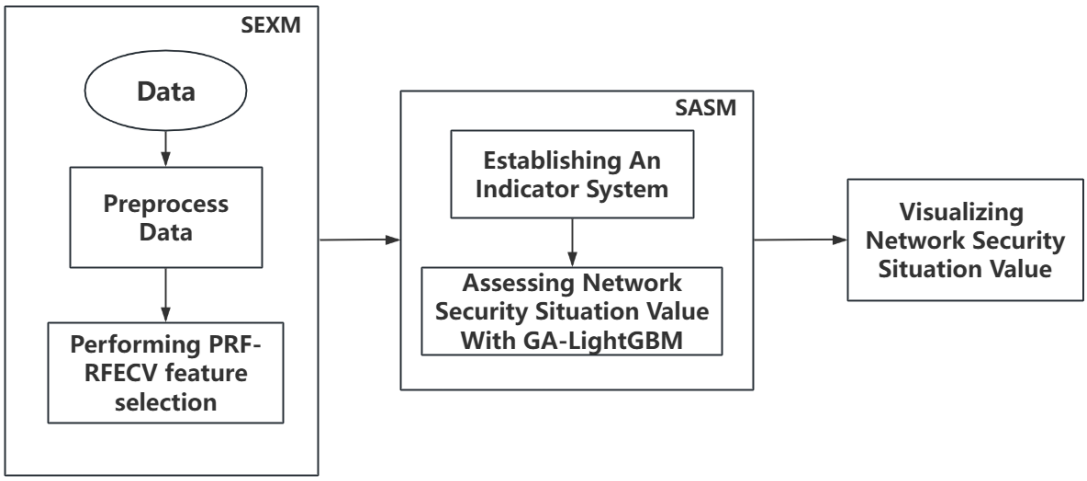

Figure 2: The PRF-RFECV-GA-LightGBM Framework for Situation Appraisal

The data processing component is the substance of network security situation assessment, it is used for data pre-processing, including data integration, data reduction, data fusion and other operations; The situation assessment module is the core part of the model, this module selects the authoritative indicator system to standardize the quantitative indicators and optimize the results; the situation visualization module presents the results in an intuitive and understandable way, timely reflect the

DOI: 10.54254/2755-2721/117/2025.20956

network security situation value, help management personnel to carry out risk early warning and reduce asset losses. This model is mainly applied to situation estimation of cyber security scenarios with massive and high-dimensional data, the core task is featuring optimization, while improving the effectiveness of network security situation assessment, ensure the accuracy of data.

3.2. Advantages And Disadvantages of Network Security Situation Assessment Technology Founded on Lightweight Gradient Elevator

The GA-LightGBM cyber security situation assessment model framework anchored in PRF-RF ECV feature optimization uses a variety of optimization algorithms, it can effectively avoid ov er fitting and improve accuracy of forecasting, meanwhile, the training speed is fast, the techni cal adaptability is strong, and it can effectively face today's complex and diverse network attac ks.

The algorithm uses genetic algorithm (GA) to optimize the parameters, but it affects the per formance of the algorithm to a certain extent. Therefore, in the future, more accurate paramete r finding algorithms are needed to improve the real-time performance of the technology and fa cilitate the implementation of dynamic network security awareness.

4. Network Security Situation Prediction Based on RBF Neural Network

4.1. RBF Neural Network Model

RBF neural network model is a single hidden layer feedforward neural network, which is constructed by the entry layer, hidden layer and input/output layer, although its topology is simple, each level has its own functions, and each level has different functions [10]. The first layer is called embedding layer, which is consist in signal source nodes, it only serves as the transmission of data information and does not transform the input information; the second layer is the hidden layer, and the number of nodes depends on the needs, the kernel function of hidden layer neurons is Gaussian function, and the input information is spatially mapped; the third layer is the output layer, which responds to the input mode, the action function of the neurons in the output layer is a linear function. The information output by the neurons in the hidden layer is linearly weighted and then output as the output result of the entire neural network. The topological structure is shown in Figure 3 below:

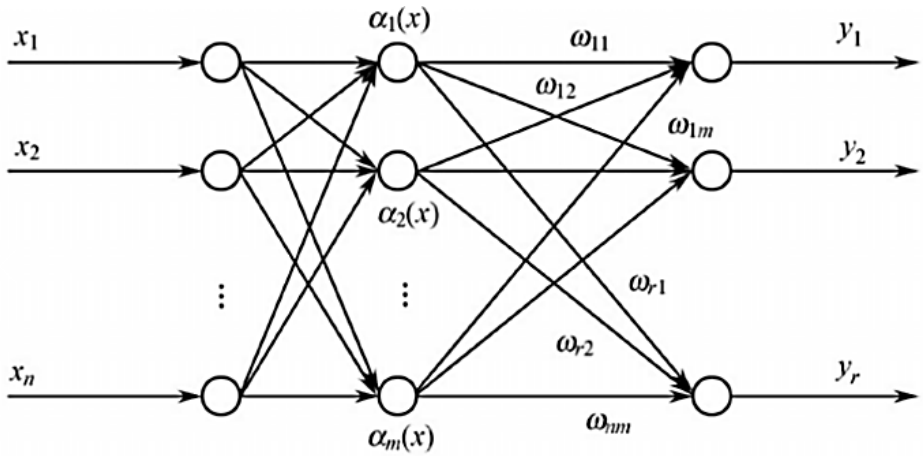

Figure 3: The Topology Diagram of RBF

Where x is the n-dimensional input vector, or is the activation function of the hidden node, Wnm is the connection weight value from the nth node to the mth node of the output layer, a-nd y is the n-dimensional output vector.

DOI: 10.54254/2755-2721/117/2025.20956

Combined with this model, data regression prediction, time series prediction and data classification prediction can be realized by using Matlab code [11]. After integrating PSO algorithm and KPCA algorithm, it is specially designed to deal with the security factors of data dimension explosion.

4.2. Advantages and Disadvantages of RBF Neural Network Situation Prediction Technology

RBF can accelerate the learning speed of neural network while avoiding the problem of local minima. Using RBF as the "base" of the hidden unit to form the hidden layer space, hidden space can directly mapping input vectors. After the RBF center point is determined, the mapping relationship is also determined accordingly. The mapping from hidden layer space to output space is linear, the output of the network is the linear weighted sum of the hidden elements, where the weights are the adjustable parameters of the network. In conclusion, the mapping of the network from input to output is nonlinear, while the network output is linear for adjustable parameters, as a result, the weights of the network can be directly contacted through the system of linear equations, thus RBF can speed up learning while avoiding local minima.

Although the RBF neural network situation awareness technology has fast learning speed an d small amount of calculation, it is difficult to select important parameters, which will affect t he accuracy and efficiency of the prediction model to a certain extent and will be greatly affec ted by subjective experience. Therefore, using parameter optimization algorithm to improve RB F neural network situation awareness technology has become the key development direction of this technology in the future, genetic algorithm can be combined with this technology to enhan ce the accuracy of data [9].

5. Discussion

This experiment mainly studies three types of network security situational awareness technologi es based on machine learning, By studying the structure diagrams and core functions of the thr ee technologies, the paper can see that, the main advantage of integrating machine learning int o network security situational awareness technology is to accelerate the learning speed of the model, improve the robustness and accuracy of the technology, however, due to the integration of multi class algorithms into technology, the complexity of the model will be increased, whi ch will affect the performance of the model.

The shortcomings brought by machine learning cannot be denied, however, it can be seen fr om practice that, the advantages of machine learning in the field of network security are far gr eater than the disadvantages of the model after it is integrated into the model.

6. Conclusion

This paper specifically analyzes three types of technologies - network security situation assess ment technology based on improved SKNet-SVM, network security situation assessment techno logy based on lightweight gradient elevator, and network security situation prediction technolog y based on RBF neural network, according to the references and academic learning, the schem atic diagrams of these three types of technologies are drawn. Through the schematic diagrams, the workflow of these three types of technologies is explained and the advantages and disadva ntages of the three types of technologies are summarized. At the same time, the main applicati on fields and scope of each technology are proposed respectively.

The improvement of Internet technology has increased the network penetration rate. Massive and high-dimensional network security data means that the network security field is facing hu ge challenges, it has become an inevitable trend to further study the technology of network sec

DOI: 10.54254/2755-2721/117/2025.20956

urity situational awareness based on machine learning. Although current machine learning can l argely make up for the shortcomings of traditional network security defense technology, there i s still no mature architecture. For satisfying the current network security needs, the following s uggestions are made for development of cyber security situational awareness technology founde d on machine learning:

(1) Try to innovate the hybrid model to advance exaction and efficiency of technology.

(2) Learn more vulnerability types and algorithms to make network security situational awareness technology fitter for the current cyber environment.

(3) Popularize the algorithm optimization pattern to decline model's complexity and enhanc e efficiency of model without affecting performance.

(4) Expand the field of use. Combine various technologies in other fields with network security situational awareness technology based on machine learning and realize interoperability between various fields, and form a relatively complete network security architecture.

References

[1] *Xiang, C. C., Wu, C. J., Liu, Q. H. & Zhou, S. J. (2023). Overview of research on network security situation prediction technology Computer Application and Software (05), 19-28+36.*

[2] *Bass, T., Gruber, D. A glimpse into the future of ID.The Magazine of USENIX & SAGE, (1999). 24(3) : 40-49.*

[3] *Xu, J. H. (2016) Research and Implementation of Network Security Situation Prediction Method Based on Machine Learning (Master's Thesis, Beijing University of Posts and Telecommunications) master.*

[4] *Guo, S. W., Liu, S. F., Li, Z. M., Ouyang, D. Q., Wang, N. & Xiang, T. (2024) Network security situation awareness method based on fusion model Computer Engineering (11), 1-9. Doi: 10.19678/j.issn.1000-3428.0069758*

[5] *Chen, M. & Gao, J. H. (2024) Research on Cyberspace Security Situation Awareness Based on Threat Intelligence Information Journal (08), 25-33*

[6] *Wang, C. F., Xu, L., Li, H. Q. & Ma, J. X. (2024) Network security situational awareness mechanism based on building behavioral portrait Computer application 1-9.*

[7] *Zhao, D. M., Sum, M. W., Su, M. Y. & Wu, Y. X. (2024) Network security situation assessment based on improved SKNet-SVM. Journal of Applied Sciences, (2): 334-349.*

[8] *Ren, G. K. (2023). Research on Network Security Situation Awareness Based on Machine Learning (Master's Thesis, Tianjin University of Technology) master. https://link.cnki.net/doi/10.27360/d.cnki.gtlgy.2023.000285doi:10.27360/d.cnki.gtlgy.2023.000285*

[9] *Cheng, J. G., Qi, Z. H. & Chen, T. T. (2019) Network security situation awareness based on RBF neural network Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition) (04), 88-95. Doi: 10.14132/j.cnki.1673-5439.2019.04.012*

[10] *Chen, S. (2020) Research and implementation of network security situation awareness system based on neural network. Nanjing: Nanjing University of Posts and Telecommunications.*

[11] *Chen, G. (2017) RF-SVM based awareness algorithm in intelligent network security situation awareness system Proceedings of 2017 3rd Workshop on Advanced Research and Technology in Industry Applications. Institute of Management Science and Industrial Engineering, 5.*