International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 6, 2025
https://theaspd.com/index.php

Research And Application Of Big Data Cybersecurity Situation Awareness Technology: An Improved LSTM Cybersecurity Situation Prediction Model Based On SSA

Hui Zeng[1], Xiaolei Zhang[2]
[1]Binary Graduate School, Ioi Business Park, NO. 1, 47100 Puchong, Selangor
[2]Binary Graduate School, Ioi Business Park, NO. 1, 47100 Puchong, Selangor
Corresponding Email: 13273714631@163.com

Abstract
In the current era of rapid global informatization, network coverage has permeated all aspects of life and industry, bringing about significant conveniences while also posing serious cybersecurity challenges. This paper explores the urgent need for an efficient and reliable cybersecurity defense system to address increasingly complex threats, emphasizing the importance of rationalizing perceptions of cybersecurity issues and enhancing security measures. The study focuses on Network Security Situation Awareness (NSSA) technology, which provides strong support for network monitoring through real-time analysis. It highlights the significance of NSSA in promptly identifying risks and predicting security situations to minimize potential threats effectively. By reviewing existing research on situation awareness models, including Endsley's three-level model and other advanced methodologies, this paper discusses how these frameworks can be applied to improve cybersecurity. Additionally, it examines the integration of big data technology with NSSA to handle massive datasets efficiently. The proposed approach not only enhances the accuracy of threat detection but also supports decision-making processes. Experimental results demonstrate that the SSA-LSTM model outperforms traditional models like LSTM and BP neural networks in terms of prediction accuracy and error rates.

Keywords: *Cybersecurity； Situation Awareness； NSSA Technology； Big Data Analysis*

1. INTRODUCTION

1.1 Research Background

In the current era of rapid development of global informatization, the breadth and depth of network coverage continue to expand and have fully permeated into all fields of people's lives and industrial links. Many aspects of life and industry have applied online platforms. For instance, QR code payment and online shopping in China's daily life all rely on network support(Huang et al., 2023).

From a macro perspective, this key technology has also been widely applied in national-level security systems, visual operation platforms, etc., greatly enhancing the convenience of people's lives and promoting the prosperous development of society. However, while online platforms bring many conveniences, they also hide drawbacks that cannot be ignored, among which the issue of network security is particularly prominent. Some lawbreakers make use of high-tech means to turn the Internet into an attack tool(Endsley,1988).

Especially in industries related to the economic lifeline of the country and sensitive fields related to political stability, the application of the Internet is more in-depth. Therefore, against this backdrop, ensuring cyber security has become a key concern for both the country and numerous research scholars. According to a report released by the National Internet Emergency Response Center, in the first half of 2021, the situation of computer infections in China was severe, with the number of infected devices exceeding 4 million, a significant increase compared to the previous year. Meanwhile, data from the National Vulnerability Sharing Platform (CNVD) shows that the number of security vulnerabilities

discovered during this period has exceeded 13,000, with a year-on-year growth of more than 10%. It can be seen from this that the current cybersecurity issues are becoming increasingly prominent and present complex and changeable characteristics.

Against this background, it is particularly urgent and crucial to construct an efficient and reliable network security defense system. Rationalizing the perception of cyber security issues and emphasizing the effective control of security measures are the key points of current work. If the existing analytical technologies fail to accurately predict and assess cyber security incidents, or cannot promptly identify and respond to threat technologies, it will directly endanger national security and social stability. Therefore, the research on related technologies is of great significance to the current network security work.

This technology can comprehensively examine the real environment and thereby formulate diverse preventive measures. At the same time, the overall status of the network is explored and analyzed to effectively control the overall security situation and lay the foundation for the development and construction of subsequent protection measures(Brannon et al.,2009). Furthermore, the introduction of Network Security Situation Awareness (NSSA) technology provides strong support for network monitoring. Through real-time monitoring and analysis, this technology can assist managers in making prompt decisions and fully grasping the overall status of the network.

1.2 Research Significance

With the rapid development of Internet technology and the continuous evolution of big data platforms, the connection between humans and the network is becoming increasingly close. However, the network structure is becoming increasingly complex and the volume of data is growing explosively, making it difficult for people to detect potential security risks in real time and control the dynamics of security risks. As a result, the network is frequently attacked, with serious consequences. Therefore, the issue of cyber security has gradually become a focal topic of widespread concern in all sectors of society.

Meanwhile, cyber attack techniques are constantly being updated, challenging the basic security defense line. To ensure network security, it is necessary to adopt multiple technical means to build a comprehensive protection system to meet the basic security requirements. Under the background of the big data era, traditional data processing methods have been difficult to meet the processing requirements of massive data by the network security situation awareness system. Big data technology, with its distributed storage, high concurrent computing and real-time processing capabilities, provides a new solution for the situation awareness system.

Timely identification of risks and early detection of security incidents are of vital importance for accurately predicting the security situation and minimizing risks to the greatest extent. The technology of network security situation awareness precisely provides strong support for solving this problem at the theoretical level. This technology can efficiently process massive data, quickly extract information related to network security, effectively evaluate the network status, and grasp the uncertainty of network attacks, thereby providing a scientific decision-making basis for network security protection.

1.3 Research Status

1.3.1 Current Situation Awareness

The term "situation awareness" originated in the aviation field in the 1980s, referring to the rational analysis of the overall state around the battlefield, effectively grasping the battle situation and predicting subsequent trends, thereby providing a scientific basis for decision-makers. The core lies in understanding the current environmental state through the collation and analysis of historical data and exploring its changing trend. Therefore, situation awareness has become a research focus since its proposal and has gradually expanded to multiple fields such as cyber security.

Scholars such as Endsley pointed out that situation awareness is a comprehensive exploration of environmental factors under specific conditions. Through the sorting and analysis of these factors, it enables the prediction of future states. Specifically, situation awareness mainly consists of three components: the first is the perception and understanding of the situation, the second is the effective interpretation of the situation, and the last is the scientific and reasonable prediction. Throughout the entire process, the first step is the comprehensive collection of data, the second step is to accurately grasp the behavioral characteristics of the object, and the last step is to predict the future development trend by analyzing historical data.

1.3.2 Current Status of Network Security Situation Awareness

The concept of situation awareness was originally aimed at enhancing the efficiency of the Air Force in carrying out tasks. Its core idea is to achieve the strategic goal of "knowing oneself and the enemy" by reasonably predicting the actions of the opponent. With the development of technology, this concept has been gradually introduced into other industries to enhance work efficiency and competitiveness[1,2]. In the aviation field, pilots mainly rely on the environmental perception in the cabin to judge the changes around them. Therefore, the situation awareness system needs to fully consider sudden problems. However, human cognitive abilities have limitations. Therefore, situation awareness should not rely solely on people's subjective judgments.

Scholars such as Ask T proposed that situational awareness should clearly grasp the composition of the surrounding environment . Endsley et al. advocate collecting and analyzing the basic characteristics of environmental elements to predict their future development. In the field of networks, Samuel et al. first proposed the concept of integrating network development with situation awareness at the end of the last century, and pointed out that the reason why it was difficult to conduct reasonable situation awareness of the network state at that time was the lack of sensor data fusion and knowledge system construction (Samuel,2021).

In 2006, some scholars attempted to apply Bayesian theory to the target estimation and analysis of the system, conducting situation awareness operations in line with the basic concept of probability distribution.proposed the idea of using resonance mechanisms to build a perception framework structure, which is widely used in current datasets and can capture trends, adapt to real environments and evaluate initial situations. In 2013, scholars such as Brannon improved the D-S theory. By analyzing the attack status and related factors, they obtained the specific security situation results. Experimental verification indicated that this model had a better situation awareness ability.

In the same year, some scholars innovatively proposed a method of intelligence analysis that combines the dimensions of time and space. This method can mine valuable information from the briefing materials in the absence of background information, helping operators master the attack process and identify highly threatening attack behaviors, providing support for managers to respond to threats quickly(Wang et al.,2007).

In 2019, some scholars designed a new model that integrates the Markov model and the transferable model, addressing the shortcomings of existing models in dealing with persistent threats. Research verification shows that this model has a good ability of situation awareness and can quickly identify concealed dangers.

In 2021, some scholars further proposed a new idea of constructing models by combining machine learning with other deep learning algorithms. After the integration of multiple algorithms, the performance of the model was significantly improved. Experimental results showed that its accuracy rate was as high as over 98% .

In 2023, some scholars were dedicated to optimizing the communication efficiency among members

within the network and proposed a three-dimensional hybrid network structure for the problem of situation awareness. Compared with the traditional two-dimensional topological structure, this three-dimensional structure has achieved a significant improvement in performance. Practical application verification shows that the 3D hybrid model improves the decision-making speed and communication efficiency of the team (Zhang,2023).

From this perspective, since its birth in the early 21st century, network situation awareness technology has been highly valued by security management departments of various countries. At present, countries are actively deploying cybersecurity situation awareness technologies through diverse channels to address increasingly complex cybersecurity challenges. This research field has become a key part of the national cybersecurity strategy and has attracted much attention (Yin et al.,2023).

2. LITERATURE REVIEW

Situation awareness is an important way to evaluate the network status reasonably. This chapter mainly focuses on the relevant theoretical basis analyzed through NSSA technology, elaborates in detail the specific operation methods of perception model evaluation, and deeply explores the contents of intrusion detection algorithms and other fusion algorithms, laying a solid theoretical foundation for the design and optimization of subsequent algorithms. Situation elements: Extract and collect specific basic indicator data and conduct preprocessing. Situation prediction: It involves establishing indicators and then calculating situation values for the three dimensions (operational dimension, threat dimension, and vulnerability dimension). Situation assessment and perception: Based on the situation values obtained from the situation assessment, the SSA-LSTM model is used for assessment.

2.1 Endsley Three-Level Situation Awareness Model

At present, NSSA technology is developing rapidly at an unprecedented speed and has shown broad application prospects in the research of situation awareness. Given the wide variety of framework structures constructed in this field, this subsection will focus on conducting an in-depth analysis and introduction of several commonly used perception models at present. Among them, the Endsley three-level model and the TimBass situation awareness model are particularly classic. They have played a significant role in the development process of situation awareness and are also the premise for other scholars to study situation awareness in the later period (Zhang et al.,2023).

The specific structure of the Endsley three-level model is shown in Figure 2.1. This model is divided into three core links: element perception, overall situation understanding, and situation prediction. In the element perception stage, the model accurately captures key elements from the complex and changeable environment. These elements cover the overall state of the environment and its various attribute characteristics, and consider the possible changes in the future. Subsequently, in the stage of understanding the overall situation, the model integrates and analyzes these obtained elements to explore whether there is a certain correlation among each element, thereby grasping the core content of the overall situation (Wen et al.,2023). Finally, in the situation prediction stage, the model integrates the results of the previous understanding to make scientific and reasonable predictions about the future development trend, providing strong support and basis for people's decision-making.

(1) Situation Element Extraction

This stage is dedicated to summarizing and sorting out all data related to the environment, and extracting core information through preliminary data analysis. Based on the requirements of subsequent evaluation indicators, carry out the initial screening and preprocessing steps of the data to ensure the availability and accuracy of the data and lay a solid foundation for subsequent analysis.

(2) Situation Understanding

This stage focuses on the assessment process of the situation. The core lies in conducting in-depth analysis using the data obtained in the previous stage and initially exploring the impact of these elements on the overall environment, laying the foundation for the later calculation of the situation value (Gong et al.,2023).

(3) Situation Prediction

In this stage, mainly based on the current network operation status and the obtained element information, the overall operation of the network in the future is predicted. Entering this stage marks the initiation of the effective perception and prediction process, which is also the core purpose of constructing this model, aiming to provide a scientific basis for network management operators to carry out network security management tasks. The subsequent content will specifically introduce the relevant technologies in element extraction, as well as how to conduct evaluation and prediction, etc. (Lu et al.,2022), with the aim of comprehensively presenting the complete process of model construction and application.

2.2 Situation Element Extraction Technology

In the overall operation process of situation awareness, the precise extraction of situation elements is not only the primary step but also the cornerstone for the smooth progress of other subsequent links. The process of element collection needs to be carried out comprehensively and from multiple perspectives. The primary consideration is the depth and breadth of data collection to ensure the comprehensiveness and accuracy of the data. This step, based on the pre-constructed indicator system, screens out relevant indicators as the basis for data collection to accurately capture the required information. Furthermore, the initial preprocessing operation is an indispensable part of fully obtaining the effective elements, which lays a solid foundation for the subsequent utilization of the data. This section mainly covers two core parts: data collection and preprocessing. The following will elaborate on each one in detail:

2.2.1 Data Acquisition

In this stage, ensuring the wide coverage and accuracy of data collection is of vital importance, as the overall environment during the operation of the network is relatively complex and is frequently subject to network attacks. In response to this challenge, scholars at home and abroad generally focus on adopting diversified data collection models to deal with it. Specifically, in their research, scholars such as Jia Yan divided the data of situation awareness into three levels, namely network assets, existing vulnerabilities in the network, and encountered dangers(Zhang et al.,2022).

2.2.2 Data Pre-processing

In the actual data collection and processing procedures, the obtained data often may contain various types of defects and challenges, such as partial data missing, non-standardized data formats, and potential outliers, etc. Therefore, before embarking on the construction of a prediction or analysis model, a data preprocessing step is required, which specifically includes the following types.

I. Data Cleaning

As the primary step of data preprocessing, its core task lies in dealing with the problems of missing data and missing attributes. This stage is crucial for ensuring the data quality of subsequent model operations and is also the basis for guaranteeing the validity of data during the model testing phase. When performing data cleaning, it is essential to fully consider the unique attributes of the data, which is the key to accurately identifying and distinguishing each data entity. Specifically, if the number of a certain data point in the dataset can no longer effectively reflect the distribution characteristics of the entire sample, then this data point should be regarded as invalid and excluded. For such situations, there are usually three operation methods, such as direct use, or completion, and direct deletion processing (Zhao et al.,2022). In the completion operation stage, there are multiple approaches, such as mean completion

or final value completion, as well as modeling and prediction completion, etc. The handling of outliers mainly involves deleting or replacing outliers that exist in the data set.

Ii. Data Integration

The core essence lies in systematically integrating the data collected from multiple different sources and ultimately summarizing them into a unified dataset. However, this process inevitably faces the challenge of inconsistent data formats, so data integration operations are particularly important. Generally speaking, it involves the identification of entities as well as data redundancy analysis and operation. Specifically, entity recognition, as a core element of data integration, shoulders the important responsibility of effectively distinguishing whether the data and its attributes in different data sources remain consistent. Meanwhile, data redundancy analysis is dedicated to distinguishing whether there is a derivation relationship among data attributes, that is, determining whether a certain attribute can be derived based on other attributes. If a certain attribute can indeed be derived from other attributes, it indicates that there is redundancy and necessary deletion processing is required to simplify the data set and improve the data quality.

Iii. Data Protocol

In this stage, data reduction, as a crucial link, its core objective is to ensure that the original appearance of the data is retained to the greatest extent while effectively reducing the volume of data. This process usually covers two core strategies: the rational selection of attributes and the compression processing of multiple data.

Iv. Data Changes

The three core aspects of data change are data smoothing processing, attribute construction and data aggregation. Data smoothing, essentially, is a sophisticated technique aimed at eliminating noise in data. By implementing smoothing processing, the data curves are effectively smoothed and noise interference is reduced, thereby revealing the true trends and patterns behind the data. Attribute construction is based on the characteristics of existing data attributes, accurately capturing the intrinsic connections among existing attributes, and ingeniously transforming these connections into new and more insightful attributes, making the entire attribute more centralized. Data aggregation is an operation that integrates and summarizes data content, simplifies data representation, reduces the complexity of data processing, and retains the key features of the data at the same time, providing a strong basis for subsequent data analysis and decision support.

V. Data Fusion

It refers to the process of integrating and comprehensively analyzing multi-dimensional data from different sources, different network structures, and different time points to ensure the acquisition of more comprehensive data content. In the field of situation awareness, the application of data fusion technology is particularly crucial. Situation awareness refers to the ability to monitor, analyze and predict various dynamic change information in a complex environment in real time, and data fusion is precisely the fundamental operation to achieve this goal.

2.3 Situation Assessment Technology

Security situation assessment is an important link for perception in the later stage. The main task is to perform mapping operations on the overall network status to form the result of situation awareness. The situation assessment indicators will be analyzed and evaluated through diverse analytical methods.

2.3.1 Evaluation method Based on Index system

If this operation mode is adopted, then the first step is to fully consider the status of the network operation, then obtain the relevant element information, construct the index system, and set the index weights

through the corresponding learning algorithm. Analyze according to the overall influence degree of the system and indicators to achieve the purpose of evaluation, and determine the initial indicators in accordance with the relevant operation principles. Previously, many scholars have also analyzed and studied this indicator system. For example, scholars such as Wang Juan have fully considered the vulnerabilities of the network with basic operational concepts such as the combination of stratification and movement.

2.3.2 Evaluation method based on Hierarchical network analysis

In this operation method, it mainly relies on the analysis and exploration of some information obtained through the intrusion detection stage. Whether there are some aggressive information among these pieces of information, conduct a hierarchical exploration of the state of the entire network from this perspective, thereby achieving the assessment of the situation. Under normal circumstances, through a hierarchical analysis model, the following concept is top-down. The operation mode of analyzing from a certain part to the whole starts from the information of network attacks to explore the overall status of the network structure and the host and other servers. This operation mode mainly analyzes offensive information and network vulnerability information, classifies the specific threat degree through the threat level, thereby calculating the situation value of each service, and then analyzes the situation value of the host with the help of the importance of the situation in the service, thus forming a hierarchical analysis mode. Moreover, this operation mode attaches great importance to being bottom-up. The operation concept of progressive layers.

2.3.3 Evaluation method Based on Analytic Hierarchy Process

This operation method relies on rationalizing the selection of analysis indicators, or setting influence indicators based on the existing information in the network. With the help of the form of the Analytic Hierarchy Process, the weight situation of each indicator is set, and then the indicators are divided according to the information in the network, thereby analyzing and obtaining the situation value.

In essence, the Analytic Hierarchy Process (AHP) simplifies the problem into multiple factors and sets up a multi-level model structure based on the connections among these factors. Moreover, during this process, the determination of the relative importance among factors relies on expert experience for measurement, and quantitative analysis is conducted on the weight issue of each indicator. During the implementation process, how the weights were allocated was explored. After selecting some elements, the weight information was divided through the Analytic Hierarchy Process (AHP), and the situation value was calculated accordingly. However, usually this operation mode is affected by individual subjective factors, so other models can be integrated to ensure the scientific nature of the evaluation.

2.4 Situation Prediction Technology

Nowadays, the development of neural network technology is very rapid, and its integration with other fields is also increasing. It is applied in the process of analyzing and predicting network security situations. Generally, there are backpropagation neural network algorithms, long short-term memory networks, recurrent neural networks, etc. Next, we will specifically introduce these several neural network algorithms.

(1) Backpropagation neural Network

Firstly, the reverse neural network algorithm, usually after training through the BP neural algorithm, constructs a multi-level neural network structure, mainly including three levels, and the nodes between each level are not effectively connected. The final result is obtained through the input layer, the hidden layer and the output layer. Then, in the input layer, mainly D neurons are involved, and in the output layer, Y neurons are involved.

The specific learning of this algorithm mainly involves the forward propagation of signals and the backward propagation of errors. The former indicates that all signals will pass through these three levels and eventually be output by the outuser. If the output is not carried out as expected at this time, error backpropagation will occur. At this point, the essence of the error is to be distributed and transmitted to other neurons, and then each unit value is modified to a certain extent. At this time, the operation will be re-performed from the input layer until the final error can meet the requirements.

(2) Recurrent Neural Network

This structure is essentially inconsistent with the previous neural network structure. In this structure, there may be some circular circulation patterns. At this time, the output result of the neuron can be used as the input in the later stage. Therefore, its structure includes three levels. The output at time t is jointly influenced by the input at the previous time and the output at the next time.

The structure of recurrent neural networks is usually constructed with the help of Elman networks. In this structure, the output result of the hidden layer interacts simultaneously with the input situation at the next moment.

(3) Recurrent Neural Network

The neurons within this neural network structure are closely connected, and the relationship between the previous level and the subsequent level is also relatively strong. This can further promote data communication and information exchange between Windows. It is quite different from the fully connected neural network structure. Firstly, the hidden layer is not directly presented, and the data of the hidden layer is influenced by the input value and the value of the hidden layer at the previous moment.

A specific analysis of the structure of recurrent neural networks reveals that, under normal circumstances, they can handle some persistent tasks. First, it is A, and then a loop body is constructed in the form of copy and paste. However, if a unidirectional recurrent neural network structure is adopted, it is impossible to analyze the data at subsequent moments. During the actual operation process, if the constructed sequence is too long, it will affect the gradient explosion problem. Meanwhile, in the structure of recurrent neural networks, there is also a situation of long-term dependence, which means that relevant information cannot be obtained for some moments with relatively large time intervals. Then, next, the neural network structure of long short-term memory can be utilized to handle these problems.

(4) Long Short-Term Memory Neural Network

This type of neural network structure mainly involves input gates, output gates and intermediate forgetting, which can ensure the reasonable processing of some historical information content.

In the structure of the long short-term memory neural network, there are four function units at the bottom. These four function units are the s function. The one on the far left is the data input, while the second one is the input gate. If the final result obtained is very close to 0, then this data will not flow to the next level. The third one belongs to the forgetting gate. If the output result at this time is within the zero-order limit, then the number will be chosen to be forgotten or deleted. The last gate belongs to the output gate.

3. The LSTM network security situation prediction model improved based on SSA

3.1 LSTM Neural Network

This algorithm is a cyclic neural network structure and has unique advantages. The specific structure is shown in Figure 3.1. It has an internal loop mechanism. Data is continuously input in the later stage, and the result of the previous state can be used as the current input. Through multiple iterative training and learning, the final output result is achieved.

However, in this structure, backpropagation will prolong the training time. Moreover, due to the complex structure, the problem of vanishing gradients is prone to occur, making it difficult to be applied to the data processing of long time series. The Long Short-Term Memory Network (LSTM) effectively resolves this conflict and can better deal with the difficulties in the time dimension.

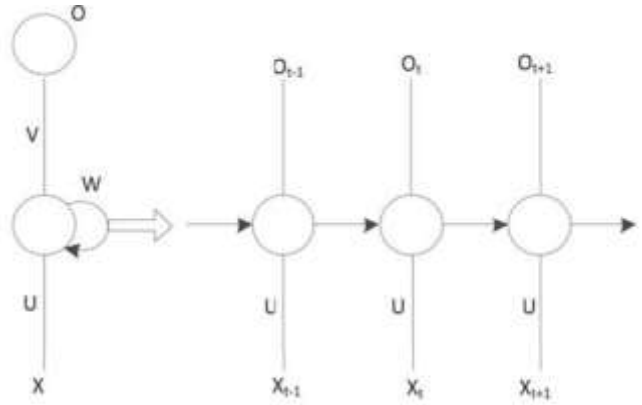

Figure 3.1 RNN Neural Network

Under normal circumstances, only one state occurs during a single loop operation. However, if it is a long short-term memory network algorithm, there will be four situations within a loop structure. At the same time, a persistent state can be used to determine whether to pass on the information obtained at the previous level. A single loop structure mainly involves four parts. They are respectively the input gate, the output gate, the forget gate and the specific unit situation.

The input gate will also affect the amount of data in this input process, while the forget gate determines whether to save these data and transfer them to the next stage. The output gate refers to the quantity of the current state output. The specific structure is shown in Figure 3.2.

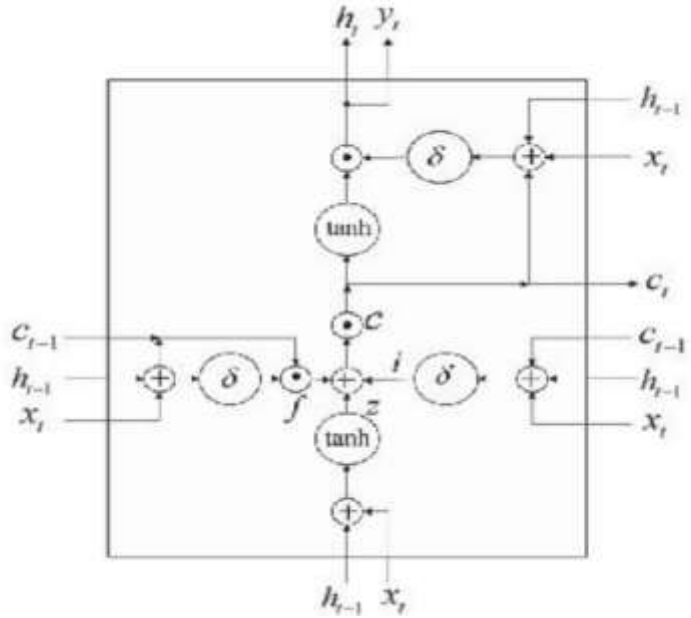

Figure 3.2 Single Loop Structure of LSTM

3.2BP neural network

After training through the BP neural algorithm, a multi-level neural network structure was constructed, mainly including three levels, and the nodes between each level were not effectively connected. The final result was obtained through the input layer, the hidden layer and the output layer. This structure is shown in Figure 3.3. Then, in the input layer, the first neuron is mainly involved, and in the output layer, Y neurons are involved.

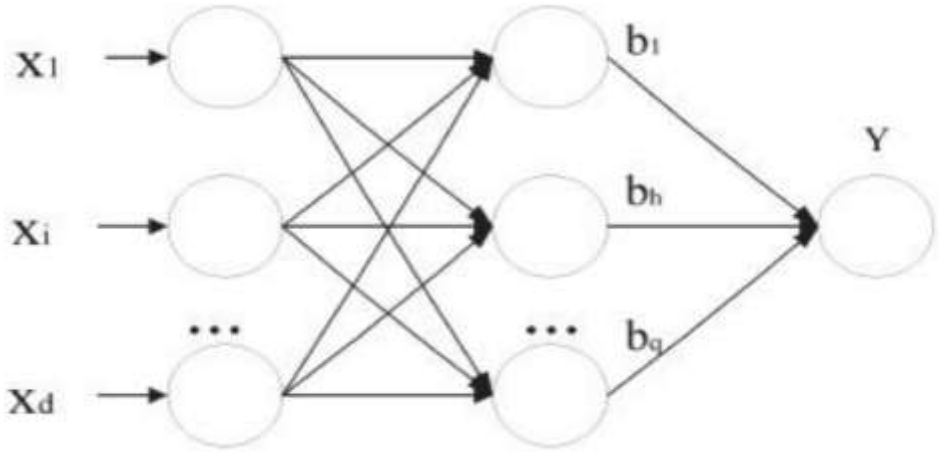

Figure 3.3 BP Network Picture

The specific learning of this algorithm mainly involves the backpropagation of the forward propagation error of the signal. The former indicates that all signals will pass through these three levels and eventually be output by the outuser. If the output is not carried out as expected at this time, it will form an operation mode of backpropagation of error. At this point, the essence of the error is to be distributed and transmitted to other neurons, and then each unit value is modified to a certain extent. At this time, the operation will be re-performed from the input layer until the final error can meet the requirements.

Zhang et al. proposed a BP neural network prediction model based on the hybrid rice algorithm to predict the future network security situation. By taking advantage of the global search and rapid convergence of the hybrid rice algorithm, the speed and accuracy of situation prediction are improved.

3.3 Sparrow Search Algorithm

This algorithm was initially proposed by scholars such as Xue, and it is an operation for optimizing traditional algorithms (Guang et al.,2023). During the actual operation of this algorithm, its search ability is relatively strong and it can converge in a short time. During the operation of a sparrow population, it is usually divided into two roles: one is the data searcher, and the other is the follower. The former has a relatively higher adaptability and can provide specific search directions and relevant guidance for subsequent followers. Then, in order to obtain more energy, usually, followers will follow the searchers in front to carry out foraging operations. Moreover, to ensure the foraging is as successful as possible, they will monitor and control other searchers, so as to prevent them from coming to compete for food. Then during the entire operation of the model, if some other dangers are encountered at this time, in order to occupy a better position, the sparrows at the edge positions will move to some relatively better positions.

3.4 Design of SSA-LSTM Model for Network Security Situation Prediction

During the process of this analysis, the characteristics of the reverse learning strategy and the traditional flight strategy were fully exerted to improve and optimize the previous sparrow search algorithm. Then, the initialized populations are thus formed, and the fitness of these populations is relatively good. This can effectively solve the local optimal situation that occurs in the traditional sparrow search algorithm and ensure the basic performance of global search. The specific operation is as follows.

Firstly, the initialization analysis of the improved LSTM model was carried out, and then the number of neurons in the input layer and the number of output layers were clarified.

Then, the operation of initializing the parameter information of the sparrow search algorithm is carried out, mainly involving the overall population size and the number of iterations of early warning values, etc. Next, set the basic dimensions and numerical range of the population reasonably. Because the basic

dimensions mainly involve the number of iterations of the model, the number of hidden layers, etc.
Then, the fitness function of the SSA algorithm is set and analyzed. From this, the initialized population is generated, and the fitness value of sparrows is reasonably analyzed and obtained. The initial population is obtained through the reverse learning strategy, thereby forming the optimal solution.
In order to ensure that the system can evaluate the situation values as comprehensively as possible, the SSA-LSTM model should be used for analysis. After optimizing and comparing the traditional algorithms through the sparrow search algorithm, it is found that the effect in terms of parameters is relatively good. Then, the characteristics of the sparrow search algorithm will be fully exerted to find the hyperparameter information of the long short-term memory network model, thereby achieving the prediction of the situation.

4. Research Design

4.1Experimental data collection. Research on Network Security Situation Prediction Model

During this analysis process, it is necessary to collect a variety of data contents related to situation values. Through the analysis of the previous situation, it can be known that it mainly includes the indicator contents of several levels such as the operation dimension, the vulnerability dimension and the threat dimension. During the verification process of the SSA-LSTM model this time, and the attack behavior on the network is simulated through IDs informer and missed scan tools. Among the entire server, the first to the fifth servers were all attacked. Data content was collected for 30 days, involving a total of over 4,500 pieces of data. Then, the data collected in the first 29 days was divided into the training set, and the data collected on the last day was divided into the test set.
Simulate the operation of the attack through IDS Informer and missed scan tools, and during the attack process, take
We have detected aggressive behaviors such as host scanning attacks, ARP attacks, and denial-of-service attacks, and obtained information about this server
The vulnerability information of the server is shown in Table 4.1 as follows.

Server number	Running services	CVE#	Vulnerability description
1	nginx	CVE-2022-41741	nginx buffer error vulnerability
2	mysql	CVE-2012-2122	Allow remote attackers to commit Execute with malicious SQL queries SQL injection attack
3	Linux	CVE-1999-0634	The SSH version information can be obtained
		CVE-2008-5161	OpenSSH CBC mode information leakage Expose loopholes
4	web	CVE-1999-0646	Allow remote attackers to send Obtain it with a specific HTTP request Sensitive information or execute arbitrary commands
5	Redius	CVE-2024-3596	Allow attackers to access without authorization Enter the network and obtain network management permissions

Table 4.1 Vulnerability Information of the Server

4.2 Big Data Preprocessing and Parsing

This platform adopts a system called Kafka, which features high throughput and distribution and operates under a publish-subscribe model. It can handle all the action flow data on the website. During this process, Kafka plays the role of a message queue. Through this section, decoupling from the data source can be achieved, and the processing capacity of the background during the peak balance stage can be improved.
Research and design an ETL tool to receive different data in Kafka. Based on the established parsing rules and related field completion rules, the goal of comprehensive data parsing is achieved. Finally, the parsed data is stored in ElasticSearch to prepare for the subsequent short-cycle display and statistical analysis work. Meanwhile, a copy of the data can be copied and stored on the HDFS file system for future retention and offline analysis.

5. Research Findings and Discussion

5.1 Analysis of Prediction Results

During the research, Mean absolute Error (MAE), root mean square error (RMSE), and Mean absolute Percentage Error (MAPE) were adopted for exploration. The specific calculation formula for evaluating the model is as follows.

$$MAE = \frac{1}{n}\sum_{i=1}^{n}\left|y_i - y_i^{'}\right|$$

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left|y_i - y_i^{'}\right|^2}$$

$$MAPE = \frac{100\%}{n}\sum_{i=1}^{n}\frac{\left|y_i - y_i^{'}\right|}{\left|y_i\right|}$$

Through the previous section 3.2, the optimized algorithm was obtained, and the training model was constructed. The training set and test set of the data were divided, and the test results in Figure 5.1 were obtained. The blue line represents the real result and the orange line represents the predicted result. The changing trends of these two curves are basically the same, which means that the model designed in this paper can make reasonable predictions and analyses of the network security situation.

In order to further explore that the designed algorithm has certain advantages, the results of analyzing and comparing it with the traditional LSTM algorithm and the BP neural network algorithm were obtained. Compared with the other two algorithms, the model designed in this paper is closer to the real situation.

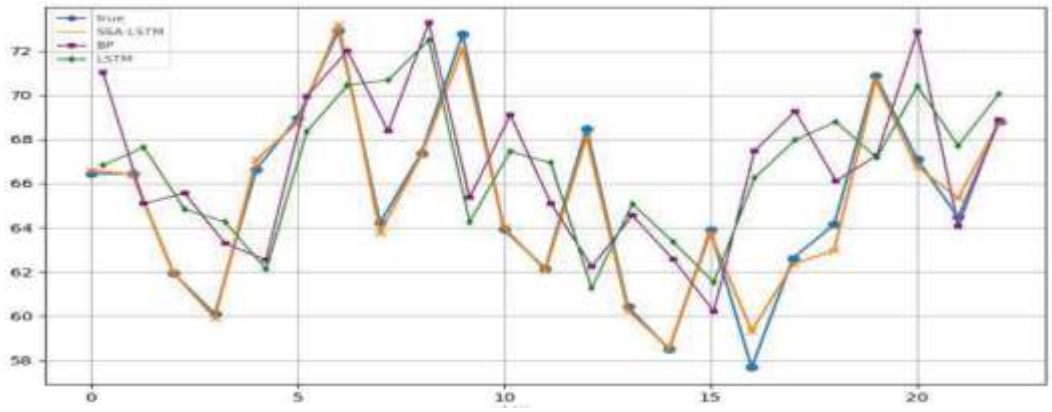

Figure 5.1 Comparison of situation values of different models

（Among the figure, the X-axis represents time and the Y-cycle represents the comparison of model effects）

In order to measure the overall performance of this model more clearly, the prediction errors were compared with those of other models. The specific results are shown in Table 4.3. By observing Figure 4.7, it can be known that the SSA-LSTM model designed in this paper has smaller error results in all aspects than other models, which fully demonstrates the superiority of this model. Therefore, it is finally determined to apply the SSA-LSTM model for the perception and predictive analysis of the security situation.

Table 5.2 Error Analysis of Different Models

modle	MAPE(%)	RMES	MAE
SSA-LATM	2.6	2.03	1.67
LSTM	6.31	2.92	2.34
BP	7.94	4.34	3.73

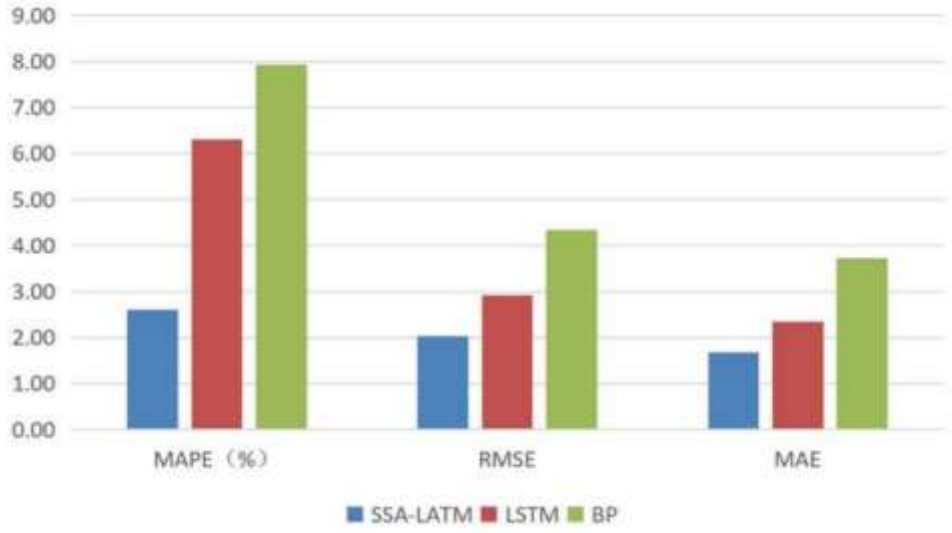

Figure 5.2 Error ratios of different models

6. CONCLUSION

With the increasing complexity of the network environment and the rapid development of information technology, network security has become an important issue in information construction. Facing the continuously expanding network scale and the increasing security threats, it is particularly important to perceive the network security situation in a timely manner. Based on the relevant theories of deep learning and machine learning, this paper deeply analyzes the basic characteristics of network traffic and discusses the identification and prediction methods of network attacks. The main contents of the research include: sorting out the relevant research results on network security situation awareness at home and abroad, constructing a situation awareness model based on a three-level structure, extracting key situation elements and determining their evaluation methods and technical paths; On this basis, the Sparrow Search Algorithm (SSA) was introduced to improve the traditional LSTM model, and the SSA-LSTM situation prediction model was constructed. The experimental comparative analysis shows that this model is superior to the traditional LSTM and BP neural network models in terms of prediction accuracy, effectively improving the prediction ability for changes in the network security situation. Overall, this research provides feasible technical support and practical paths for improving the level of network security situation awareness and prediction.

REFERENCES

1. Brannon, N. G., Seiffertt, J. E., Draelos, T. J., & et al. (2009). Coordinated machine learning and decision support for situation awareness. Neural Networks, 22(3), 316–325. https://doi.org/10.1016/j.neunet.2009.03.004

2. Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. In Proceedings of the Human Factors Society annual meeting (Vol. 32, pp. 97–101). Sage Publications. https://doi.org/10.1177/154193128803200215

3. Gong Xiaogang, Wu Xinyu, Zhou Xuxiang. Deep learning-based security situational

4. Huang, F., Wang, T., Liu, Z., & Miao, Q. (2023). Multi-dimensional security status awareness technology for 5G networks in ship communication systems. Ship Science and Technology, 45(22), 186–189.

5. Lu, L., Liu, M., Chen, W., Liu, G., & Yang, Y. (2022). Power monitoring network security situation awareness system based on knowledge map. Journal of Physics: Conference Series, 2354(1), Article 012067. https://doi.org/10.1088/1742-

6596/2354/1/012067

6. Song, G., Wang, M., Yu, Y., & Zhang, B. (2023). The current research status of AI-based network security situational awareness. Electronics, 12(10), Article 2256. https://doi.org/10.3390/electronics12102256

7. Wang, J., Zhang, F., Fu, C., & et al. (2007). Research on the index system in network situation awareness. Journal of Computer Applications, 27(8), 1907–1909, 1912.

8. Wen, Z., Zhang, L., Wu, Q., & Deng, W. (2023). A network security situation awareness method based on GRU in big data environment. International Journal of Pattern Recognition and Artificial Intelligence, 37(1), Article 2350001. https://doi.org/10.1142/S021800142350001X

9. Yin, M. J., Luo, X. Y., Liu, X. N., & Li, Z. Y. (2023). Constructing a curriculum system for cyber situation awareness education. Computer Education, 2023(8), 121–125.

10. Zhang, J., Feng, H., Liu, B., & Zhao, D. (2023). Survey of technology in network security situation awareness. Sensors, 23(5), 2608–2608. https://doi.org/10.3390/s23052608

11. Zhang, X. (2023). Research on network security situation awareness strategy based on deep learning: A case study of network operation and maintenance analysis at Tianjin Normal University. Network Security Technology & Application, 2023(8), 33–35.

12. Zhang, Y., Kaur, A., Jagota, V., & Neware, R. (2022). Study on data mining methods of network security situation perception based on cloud computing. Journal of Intelligent Systems, 31(1), 1074–1084. https://doi.org/10.1515/jisys-2021-0089

13. Zhao, D., Wu, Y., & Zhang, H. (2022). A situation awareness approach for network security using the fusion model. Mobile Information Systems, 2022, 1–12. **Funding Information**

14. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

15. Author Contributions

16. The manuscript has a single author who was solely responsible for the research design, data collection and analysis, and the drafting and revision of the manuscript.

17. Conflict of Interest Statement

18. The author declares no conflicts of interest.

19. Ethical Statement

20. This study adhered to all relevant ethical standards for academic research. Where applicable, any research involving humans or animals was conducted in accordance with ethical guidelines.