Computer Network Security Situation Assessment Integrating Least Squares Support Vector Machines and Optimized Bidirectional Long Short-Term Memory Network Algorithm

Chun Zheng* and Hua Jin

School of Modern Health and Regimen Industry, Anhui Sanlian University, Hefei 230601, China
E-mail: Chun_Zheng@tom.com
**Corresponding Author*

Received 17 April 2024; Accepted 31 October 2024

Abstract

Accurately evaluating and forecasting the state of computer network security has become essential due to the rise in network threats. The study proposed a model to build a systematic computer network security situation assessment index system by combining the optimized BiLSTM (Bidirectional Long Short-Term Memory) and the least squares support vector machine. This model addresses the issues of low accuracy and lack of prediction ability with current assessment methods. And validate the model performance through a complex and dynamic dataset of 200 samples, the research results show that the least squares support vector machine model shows higher evaluation accuracy, with an average evaluation accuracy of 96.12%. The model combining the least squares support vector machine and the optimized BiLSTM is more consistent with the real situation value, with an average absolute error of about 0.05. The outcomes of the simulation indicate that the least squares

Journal of Cyber Security and Mobility, Vol. 14_2, 259–282.
doi: 10.13052/jcsm2245-1439.1421

support vector machine has a high degree of fitting and clearly illustrates its better scenario assessment performance. The research model's prediction of computer network security situation shows overall high results. The research results provide decision-makers with more accurate and timely intelligence support, helping them respond quickly and reduce potential security risks.

Keywords: LSSVM (Least Squares Support Vector Machines), optimized BiLSTM, computer network, security posture, indicator system.

1 Introduction

In today's digital age, computer networks have become an indispensable infrastructure for information sharing and communication. The topic of network security (NS) scenario evaluation is vital because as network applications get more complicated and numerous, so do the dangers to NS [1]. In order to assist decision-makers in implementing the necessary defensive measures, security posture assessment entails real-time monitoring, analysis, and prediction of the likelihood and impact of cybersecurity incidents. A variety of machine learning (ML) methods have been extensively employed in NS scenario analysis in recent years. These algorithms can extract valuable information from massive data and help security experts quickly identify and respond to security threats [2]. Least Squares Support Vector Machine (LSSVM) is used to evaluate NS situation due to its advantages in handling small sample, nonlinear and high- dimensional data problems. However, a single ML algorithm may be difficult to handle the sequential and dynamic characteristics of network security situation assessment (NSSA) [3]. With the development of deep learning technology, Bidirectional Long Short-Term Memory Network (BiLSTM) has become an effective tool for processing time series data, especially showing significant capabilities in capturing the before and after dependencies of data [4]. By using the BiLSTM network model, researchers can better understand and predict security events and situation changes in complex networks. This research aims to integrate the LSSVM algorithm and the optimized BiLSTM network model to build an advanced computer NSSA framework. This is also the innovation of this research. Combining the LSSVM and the optimized BiLSTM network model can build an efficient computer NSSA and prediction framework.

The contribution of the research lies in three aspects. Firstly, an advanced network security situation framework and evaluation index system were constructed, providing a more refined index management level for computer

network security management. Secondly, the application of LSSVM and BiLSTM algorithms has effectively analyzed the prediction model to improve its accuracy and efficiency. Finally, the framework and prediction model of network security situation can provide a good technical reference for Internet data protection.

There are four primary sections to this research. A review of the existing literature on NS and intelligent algorithms is included in the first section. The study methodology, which comprises the development of the computer NSSA index system, computer NSSA based on LSSVM, and computer NS scenario prediction based on optimized BiLSTM network algorithm, is covered in the second section. The outcome analysis, which primarily does simulation analysis on the study methodology, makes up the third section. The research findings and limitations are outlined in the conclusion, which is the fourth section.

2 Related Works

NS research is crucial to protecting critical information infrastructure and user data from increasingly complex network threats. To solve the security difficulties of future 5G network services, Yu and colleagues suggested a novel immunology-based NS architecture. This architecture is based on maintaining a balance between security and availability, and improves defense capabilities through community cooperation and active adaptation strategies to effectively respond to network threats [5]. Corallo et al. proposed an impact assessment method to identify key assets and assess the business impact of potential network attacks (NAs). The approach, which covered manufacturing cells based on networked computer numerical control machine tools and 3D printers, was carried out as a case study in an aerospace component manufacturing company. The findings indicate that this approach can help businesses define important data in smart manufacturing settings and evaluate and separate the effects of NS breaches on their operations [6]. Scholars like Zhang created a weight-based integrated ML algorithm to detect anomalous signals in the vehicle controller LAN bus network in order to address the high security and high reliability difficulties in 6G vehicle networks. Experimental results show that this method performs well in improving accuracy and reducing false alarm rates, and significantly enhances the security of the in-vehicle network [7]. In order to solve the security problem in video transmission, Zhao designed a new dot multiplication algorithm based on scalable video coding and applied it to the sliding window. The outcomes revealed that

the algorithm significantly reduces the amount of calculation and storage requirements while improving efficiency, and is suitable for devices with limited memory such as smart cards. In addition, the research also improves the encryption algorithm and provides a comprehensive analysis of scalable video coding technology [8]. Shu proposed a new QoS framework based on SDN and NFV, which can implement network slicing of different network resource allocation algorithms. Simulation tests show that this framework can schedule resources for different NS types according to QoS requirements to ensure users' E2E QoS [9]. Schieber B et al. proposed to address the scheduling problem of energy demand by utilizing time-dependent tasks and energy harvesting, and maximizing the weights of their scheduling tasks to achieve maximum throughput for real-time tasks [10]. In addition, in international relations, Dezfuli S M K P's analysis of international targeted killings is that the mixed and asymmetric threats of international terrorism are in the process of normalization, and the transformation of concepts such as national sovereignty and the existence of inclusive standards in international relations can promote the ability of state relations to respond to non military threats [11].

With the development of intelligent algorithms, different scholars widely use algorithms such as SVM and BiLSTM to deal with different prediction and evaluation problems. Researchers like Zheng K created a quantitative assessment technique based on support vector machines (SVMs), which enables continuous and quantitative risk assessment by simulating interaction forces, in order to increase the accuracy of ship collision risk assessment. The results of a simulation experiment demonstrate that this new approach can more precisely estimate the risks of a ship accident and is more effective than the conventional approach [12]. Sareen et al. suggested a weight optimization neural network model based on the modified sine and cosine algorithm to improve the stability prediction and lower the costs of offshore and coastal buildings. Using grid search, the model automatically determines the optimal configuration for long short-term memory, ordinary recurrent neural networks, and gated recurrent networks. According to experimental findings, the optimized model outperforms the baseline model in terms of mean absolute error (MAE), root mean square error, and mean square error [13]. Huang and other scholars proposed a hybrid model that combines sparse autoencoders and BiLSTMs to solve the problem of wastewater flow prediction caused by excessive rainfall in domestic sewage systems. Through data preprocessing, feature dimensionality reduction, and time series prediction (TSP), the model performed superiorly in experiments on real-world hydrological time series

datasets, thus validating its ability to accurately predict Effectiveness in terms of wastewater flow rate [14]. Abbasihafshejani et al. proposed a role-based approach to detect and punish selfish nodes in blockchain networks regarding security issues, demonstrating that this method can reduce selfish behavior and improve algorithm throughput [15]. Abolfathi M et al. proposed using multi-path routing and deception as defense methods to enhance randomization strategies for network traffic security issues, and employed zero sum games; To demonstrate the optimal defense strategy and the accuracy of reducing attack behavior [16]. Hamdia K M et al. proposed an optimized maximum likelihood structure considering supervised learning process for machine learning model design and performance issues, and used genetic algorithm to perform inference analysis on the model system to demonstrate the high prediction accuracy of robot learning methods [17].

It can be seen from the above research that advanced algorithms play a very good role and importance in improving NS situation awareness and response capabilities. In view of this, this study combines LSSVM and optimized BiLSTM network algorithms to evaluate the computer network security situation (CNSS).

3 Computer NSSA and Prediction by Integrating LSSVM and Optimized BiLSTM Network Algorithm

For computer NSSA and prediction, the research first constructs a comprehensive computer NSSA index system, and proposes an assessment and prediction model that integrates LSSVM and optimized BiLSTM. The NS strategy's ability to promptly respond to possible attacks is successfully improved by first using LSSVM to do real-time security situation assessment, followed by the optimized BiLSTM being utilized to predict the future security scenario.

3.1 Construction of Computer NSSA Index System

Computer NSSA is a key link in NS, aiming to accurately understand and predict NS conditions. Computer NSSA is a key task, involving comprehensive analysis and prediction of computer NS conditions [18, 19]. In the initial stage of situation assessment, network-related data needs to be collected from various data sources and pre-processed to filter out key information that reflects the NS status. This process is called situation element extraction. Effective extraction is based on selecting appropriate indicators, that is, establishing a comprehensive indicator system.

Table 1 Index System for Computer NSSA

Target Layer	Primary Indicators	Secondary Indicators
Computer NSSA	Vulnerability	Number and level of network vulnerabilities
		Number and level of critical device vulnerabilities
		Number of security devices within the subnet
	Threatening	Number and level of alarms
		TCP protocol packet ratio
		UDP protocol packet ratio
		Historical frequency of security incidents within a subnet
		Subnet bandwidth usage rate
		Growth rate of subnet inflow
		The proportion of data packets with a size of = 64 bytes
		>The proportion of 1518 bytes of data packets
	Stability	Subnet traffic change rate
		The rate of change in the distribution ratio of different protocol packets within a subnet
		The rate of change in the distribution ratio of packets of different sizes within a subnet

When constructing the indicator system, specific principles need to be followed to ensure the accuracy and practicality of the assessment [20]. Network administrators can obtain a thorough and precise picture of the state of NS through such an evaluation, which enables them to make informed decisions when developing security plans and countermeasures. Based on the aforementioned concepts, Table 1 displays the construction of a computerized NSSA index system with 3 first-level indications and 14 second-level indicators.

In Table 1, the first-level indicators of the computer NSSA index system are vulnerability, threat, and stability. Vulnerability refers to the potential risk a network faces due to its internal security flaws, which is typically related to the network's hardware and software configuration. A network with a high vulnerability is more open to attack. The network threat indicator calculates the current attack damage level that the network is exposed to. The network's security standing deteriorates with increasing threat levels. The stability of a network focuses on the persistence of its condition and is often associated with the rate of change. A lower rate of change means that the network state is more stable.

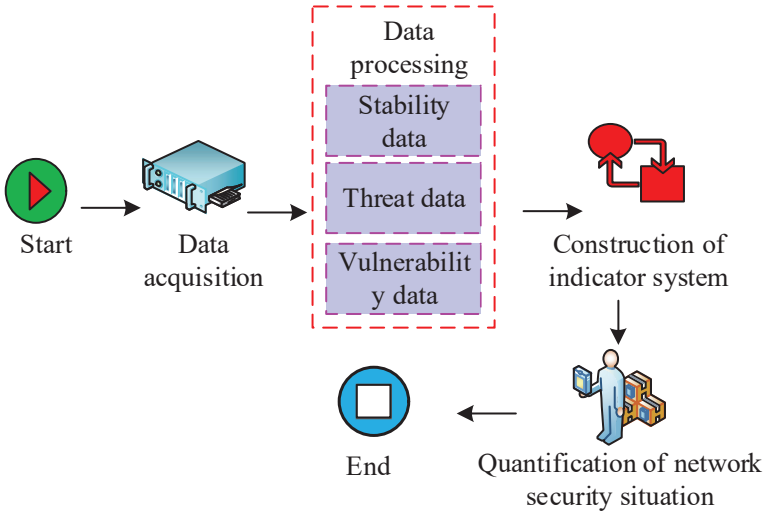

Figure 1 NSSA process.

3.2 Computer NSSA Based on LSSVM

After constructing a complete computer NSSA index system, this system can be used to conduct in-depth analysis of network behaviors and events and assess NS risks. Through real-time monitoring and analysis of key indicators such as intrusion detection data, system vulnerabilities, network traffic anomalies and other factors, the current security level of the network can be comprehensively measured, and potential security threats can be discovered and responded to in a timely manner, thus providing data support for NS decisions. Effectively improve the security protection capabilities of the overall network. In Figure 1, the NSSA procedure is displayed.

Pattern matching identifies threats by matching known attack patterns. ML algorithms play an important role, such as SVM algorithm and Various neural networks [21]. SVM is a popular ML technique that improves generalization capabilities based on a structural risk minimization strategy, which is different from empirical risk minimization. SVM is dedicated to solving small sample size and nonlinear problems by constructing an optimal decision boundary, that is, a hyperplane, to achieve effective classification of data sets. Consider a mathematical model, which consists of a sample set labeled as positive or negative, in the form of $S = \{(x_i, y_i)_{i=1}^{n} | x_i \in R^N, y_i \in \{-1, 1\}\}$, where $i = 1, 2, \ldots, l$ each sample x_i is sample data and y_i its corresponding sample type [22, 23]. Equation (1) illustrates how to solve a

particular objective function and meet a set of constraints in order to produce the ideal classification hyperplane.

$$\begin{cases} \min \dfrac{1}{2}\|w\|^2 \\ s.t.\ y_i(wx_i + b) \geq 1 \end{cases} \tag{1}$$

In formula (1), b and w are respectively the bias vector and the weight vector. When slack variables are added $\xi_i \geq 0, i = 1, 2 \ldots n$, formula (2) is obtained.

$$\begin{cases} \min \dfrac{1}{2}\|w\|^2 + c\sum\limits_{i=1}^{n} \xi_i(\xi_i \geq 0) \\ s.t.\ \begin{cases} y_i(wx_i + b) \geq 1 - \xi_i \\ c \geq 0 \end{cases}, \ (i = 1, 2, \ldots, n) \end{cases} \tag{2}$$

In formula (2), c represents the penalty factor. In order to alleviate potential conflicts in the performance evaluation criteria of the algorithm, the penalty factor can be adjusted for optimization. Equation (3) illustrates how the SVM classification task can be represented as a quadratic optimization problem.

$$\begin{cases} \max W(a) = \sum\limits_{i=1}^{n} a_i - \dfrac{1}{2}\sum\limits_{i,j=1}^{n} a_i a_j y_i y_j K(x_i x_j) \\ s.t.\ \sum\limits_{i=1}^{n} a_i y_i (0 \leq a_i \leq c, i = 1, 2, \ldots, n) \end{cases} \tag{3}$$

In formula (3), $K(x_i x_j)$ is a kernel function and satisfies the conditions $K(x_i x_j) = \langle \varphi^T(x_i) \cdot \varphi(x_j) \rangle$. Among them, $\langle \cdot \rangle$ represents the inner product operation, and the prediction category of the data sample can be calculated through the decision function, and $f(x)$ the expression is as shown in formula (4).

$$\begin{aligned} f(x) &= sign\left(\sum_{i=1}^{n} a_i y_i \langle \varphi^T(x_i) \cdot \varphi(x_j) \rangle + b\right) \\ &= sign\left(\sum_{i=1}^{n} a_i y_i \langle K(x_i x_j) \rangle + b\right) \end{aligned} \tag{4}$$

In Support Vector Machines (SVM), the Radial Basis Function (RBF) can be employed as the kernel function to efficiently represent the nonlinear features in the data. Expression (5) defines the RBF kernel, which has good nonlinear approximation properties.

$$K(x_i x_j) = \exp(-\|x_i - x_j\|^2 / 2g^2) \tag{5}$$

In formula (5), g it represents the kernel parameters that affect SVM classification performance. The SVM algorithm is a ML method widely used for classification and regression tasks, and LSSVM is an improved version of the SVM algorithm. LSSVM simplifies the optimization problem that needs to be solved by replacing the hinge loss function (LF) used in standard SVM with a least squares LF. LSSVM has advantages in processing small samples, nonlinear and high-dimensional data. The original data is subjected to early feature extraction using LSSVM with the goal of reducing the dimensionality of the data while maintaining meaningful information. LSSVM uses the least squares method to transform the original optimization problem into a system of linear equations, which is easier to solve and faster to calculate than the quadratic optimization problem of traditional SVM. Different from the inequality constraints usually adopted by SVM, LSSVM uses equality constraints, which makes the solution process simpler.

Lagrange multiplier solving is made easier with LSSVM since equality constraints take the place of SVM's inequality constraints. Formula (6) illustrates how the classification problem of LSSVM is defined as a quadratic programming problem.

$$\begin{cases} \min\limits_{w,b,e} J(w,e) = \dfrac{1}{2} w^T w + \dfrac{1}{2} \gamma \sum\limits_{k=1}^{N} e_k^2 \\ s.t.\ y_k[b + w^T \varphi(x_k)] = 1 - e_k,\ k = 1, 2, \ldots, N \end{cases} \tag{6}$$

The equality constraint in LSSVM introduces an error variable e, and a regular term containing the error variable is added to the original function. Subsequently, through the Lagrange multiplier method, the problem is transformed into α the maximum value problem to be solved, and this transformation can be expressed by formula (7).

$$L(w, b, e, \alpha) = J(w, e) - \sum_{k=1}^{N} \alpha_k \{b + e_k - 1 + w^T \varphi(x_k)\} \tag{7}$$

Then, the derivatives of w, b, e_k, α_k are taken in sequence, and assuming that the derivative is 0, the α sum b is solved to obtain the classification

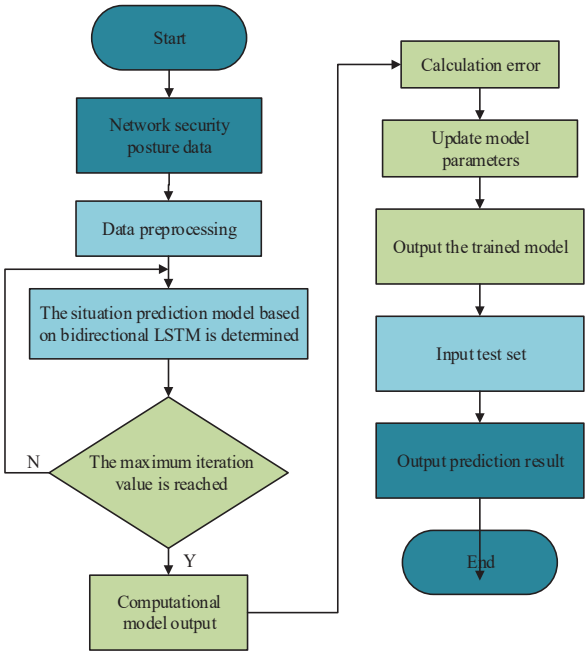

Figure 2 Process of computer NSSA based on LSSVM.

expression of LSSVM, as shown in Equation (8).

$$y(x) = sign\left[\sum_{k=1}^{N} \alpha_k y_k K(x, x_k) + b\right] \tag{8}$$

Through the accurately constructed LSSVM classification model, the research can effectively assess the security posture of computer networks. An accurate and efficient evaluation of the state of NS can be obtained by utilizing the classification expression of LSSVM in conjunction with integrated deep learning technology. Figure 2 depicts the computerized NSSA procedure based on LSSVM.

3.3 CNSS Prediction Based on LSSVM and Optimized BiLSTM Network Algorithm

The prediction of NS situation is the key to the perception of NS environment. It provides decision-making assistance to network administrators by estimating NS status in the future. NAs often show certain patterns in time,

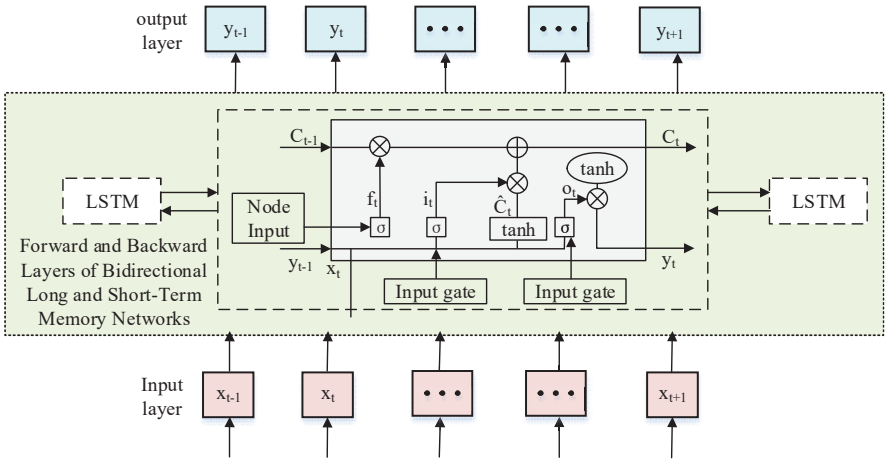

Figure 3 The network structure of BiLSTM.

and BiLSTM neural networks perform well in processing time series data. BiLSTM can comprehensively utilize historical and future information for learning, which makes up for the limitations of traditional LSTM networks. BiLSTM is composed of two LSTM layers, one is responsible for processing positive sequence time data, and the other is responsible for processing reverse sequence data. This structure makes it more efficient in TSP.

Due to its superior time series data processing capabilities, BiLSTM is extensively utilized in numerous domains, including speech recognition, language translation, and sentiment analysis. However, as the complexity of data sequences increases, a single BiLSTM structure often cannot meet the growing processing needs [24, 25]. Recently, the academic community has made significant progress in neural network research. Especially in some specific application fields, neural networks have shown better prediction capabilities than traditional ML methods. Based on these developments, this study proposes an improved BiLSTM model for CNSS prediction. With a dual-layer BiLSTM, a dropout layer, and a dense layer, the model seeks to increase prediction efficiency and accuracy. The network structure of BiLSTM is shown in Figure 3.

Since LSSVM has reduced the data dimension while retaining key information, this will help the BiLSTM network learn and extract features more efficiently. In order to shorten manual debugging time and stimulate the best performance of the model, the study uses Bayesian optimization technology to finely adjust the hyperparameters. Additionally, to avoid the problem of

slow model learning or overfitting, the Xavier weight initialization method and Dropout technique are used to improve the model learning efficiency and its expressiveness on unknown data. Bayesian optimization is a global optimization method that relies on Bayes' theorem. It gradually increases sampling points to better fit the posterior probability of the objective function, and adjusts hyperparameters accordingly. Its process starts from Gaussian process regression to obtain the posterior distribution, and then relies on the acquisition function to select new sample points. Following the selection of sample points, the new parameter combination is used to update the posterior distribution. This process is repeated until the maximum number of iterations is reached or convergence takes place. Therefore, the LSSVM method that preserves key information can quickly adapt to the feature extraction of the model and enhance its performance together with Bayesian optimization methods.

Weight initialization is a crucial technology in machine learning (ML) that influences the network's convergence pace as well as the solution's quality and ability to adapt to new challenges. Choosing an appropriate weight initialization strategy can more effectively solve complex nonlinear problems while controlling computational complexity [26]. The Xavier initialization weight is related to the output and input nodes of the layer of the neural network. The specific initialization formula is shown in Equation (9).

$$W \sim Uniform\left(-\frac{\sqrt{6}}{\sqrt{fan_{in}+fan_{out}}}, \frac{\sqrt{6}}{\sqrt{fan_{in}+fan_{out}}}\right) \tag{9}$$

In formula (9), fan_{in} and fan_{out} respectively denote the input nodes and the output nodes of a certain layer in the neural network, which $Uniform$ are uniformly random values.

Neural networks can be effectively kept from overfitting with the use of dropout technology. This method is frequently applied in the field of deep learning to lower the possibility of overfitting during training. Its primary purpose is to increase the model's capacity for generalization on unknown data, particularly in cases where the original model was prone to overfitting [27, 28]. The core mechanism of Dropout is to randomly discard a portion of neurons during the training process. This randomness reduces the interdependence between neurons and forces the network to learn more robust feature representations. In short, Dropout enhances the generalization performance of the entire network by creating the effect of multiple sub-models. Figure 4 depicts the CNSS prediction procedure based on an optimized BiLSTM.

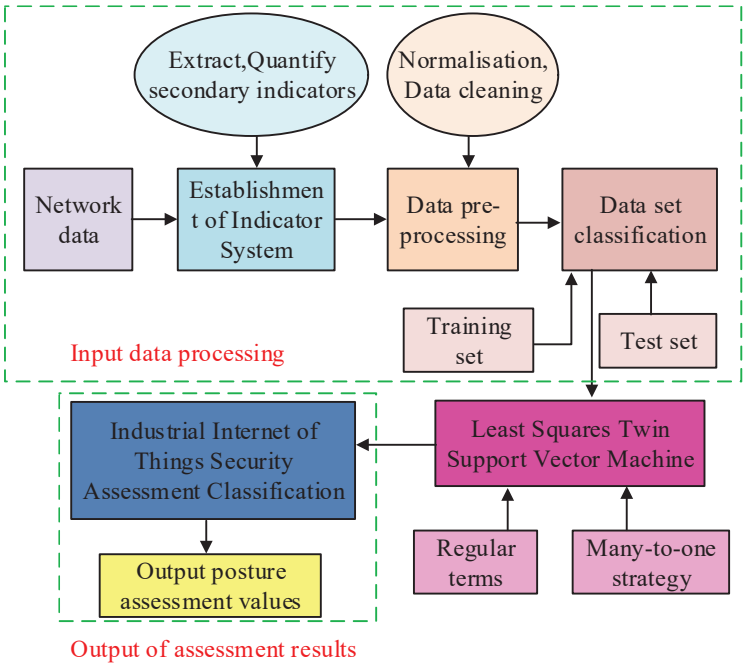

Figure 4 CNSS prediction process based on optimizing BiLSTM.

4 Computer NSSA and Prediction Analysis Integrating LSSVM and Optimized BiLSTM Network Algorithm

Initially, the effectiveness of the situation assessment and prediction techniques was compared, confirming the superiority of LSSVM-BiLSTM, before the computer NSSA and prediction were analyzed. After that, simulation analysis was used to confirm the research method's efficacy in NSSA and prediction.

4.1 Security Situation Assessment and Predictive Performance Analysis

Collect network traffic data, log files, intrusion detection system alerts, etc., clean the data, and extract features such as traffic size, packet frequency, protocol type, etc. The data sample set consists of 200 samples. The study used 5-fold cross validation to select parameters, extracted experimental samples, and used 80% as the training set and 20% as the testing set. At the same time, the setting of the number of nodes in the network structure

Table 2 Experimental environment

Environment	Name	Content	Unit/version
Hardware environment	CPU	Execute program instructions and process data	GHz
	GPU	A processor for graphics processing and image calculations	GB
	RAM	Temporary storage of running programs and data	GB
Software environment	Python	High-level programming language	Python 3.8
	TensorFlow	Building and training deep learning models	TensorFlow 2.0
	Keras	Open source neural network library	Keras 2.3.0

layers of the model can provide better reference for model performance. In order to prevent excessive feature extraction of the model, which may affect detection accuracy, the number of layers of the model is set to three, and multiple algorithms are selected to verify the training performance of the model. Table 2 displays the particular experimental setting.

In the experiment, the CNSS level was divided into 5 levels from low to high, marked 1–5 in sequence. Using Sequential Minimal Optimization – Support Vector Machine (SMO-SVM), which is a potent tool that optimizes the SVM training process and is widely used in various ML applications like image recognition, text classification, bioinformatics, and handwriting recognition, you can compare the evaluation performance of LSSVM with SVM and, to further increase comparability, add SMO-SVM to the comparison. First, compare the evaluation results of the three algorithms of SVM, SMO-SVM, and LSSVM, and select samples No. 1–10 for evaluation. The results are shown in Figure 5.

In Figure 5, the three models show different accuracy when assessing the CNSS. The SVM model had evaluation errors in samples 1, 3, 4, 7, and 10, and these samples were misestimated to level 2 respectively. The SMO-SVM model has errors in the evaluation of samples 2, 4, 6, and 9, and these sample errors are estimated to be levels 2, 1, 3, and 3 respectively. In contrast, the LSSVM model shows higher estimation accuracy, only misestimating sample 4 as level 2. After 50 iterations of the experiment, the average evaluation accuracy of the three algorithms was determined using statistical methods. The results are shown in Figure 6.

Figure 6(a), (b) and (c) show the average evaluation accuracy of LSSVM, SMO-SVM, and SVM respectively. In Figure 6, the average evaluation

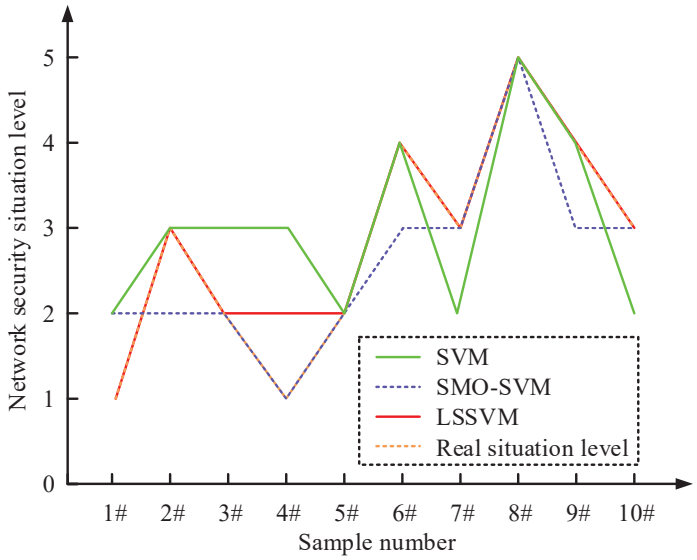

Figure 5 Evaluation results of SVM, SMO-SVM, and LSSVM algorithms.

accuracy rates of the three algorithms LSSVM, SMO-SVM, and SVM are 96.12%, 81.57%, and 74.15% respectively. That is, LSSVM has better assessment accuracy than SVM and SMO-SVM in computer NSSA.

Next, the CNSS prediction performance of Integrating LSSVM and Optimizing BiLSTM (LSSVM-BiLSTM) is analyzed. To improve the research's comparability, the improved BiLSTM is contrasted with both BiLSTM and SSA-LSTM. Among them, the Adaptive Whale Optimization Algorithm – Long Short-Term Memory (SSA-LSTM) is suitable for complex and dynamically changing data sets, and has strong global search capabilities and time-series data processing capabilities. The network situation prediction results of optimized BiLSTM, BiLSTM, and SSA-LSTM for sample No. 1–10 are shown in Figure 7.

As can be seen from Figure 7, the findings illustrate that the LSSVM-BiLSTM model is consistent with the true situation value on some samples, but the prediction accuracy is not high in most cases. The prediction performance of BiLSTM and SSA-LSTM has been improved compared to BiLSTM, especially on some key samples, the prediction is more accurate. However, these models still have limited predictive capabilities in the face of severe fluctuations in true situation values. In contrast, the LSSVM-BiLSTM model outperforms the other two models in overall prediction effect, showing

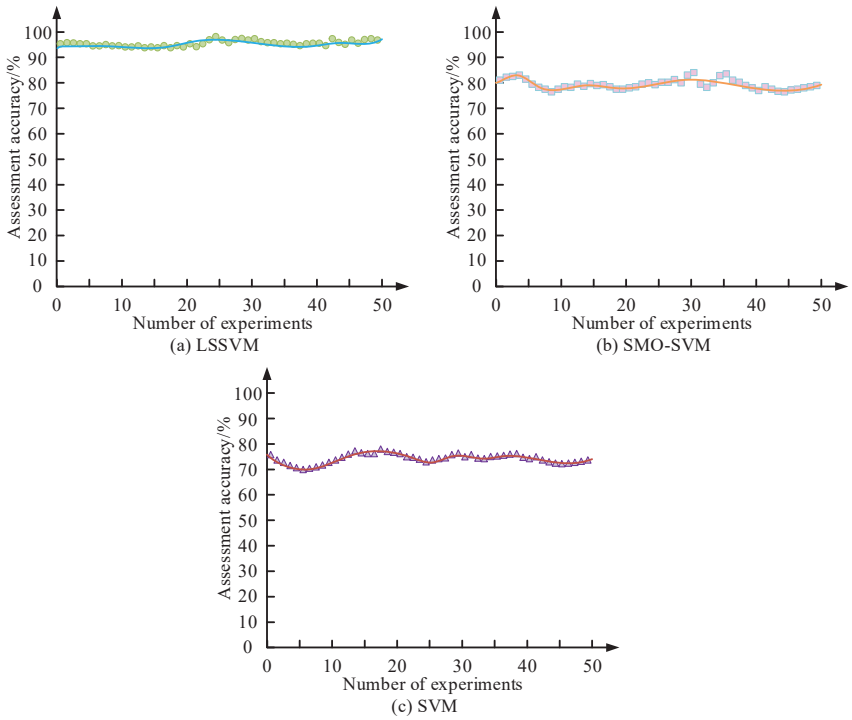

Figure 6 Average evaluation accuracy of three algorithms.

better adaptability and accuracy. The experiment was repeated 50 times to compare the MAE of the three algorithms. The results are shown in Figure 8.

As can be seen from Figure 8, the MAE differences between the three algorithms of LSSVM-BiLSTM and BiLSTM and SSA-LSTM are obvious. As the experiments increases, the MAE of BiLSTM and SSA-LSTM both show an upward trend, while the average absolute error of LSSVM-BiLSTM tends to be stable during the experiment, with smaller fluctuations, and the average MAE is about 0.05. The average MAE of BiLSTM and SSA-LSTM are 0.65 and 0.31 respectively. It can be seen that, relatively speaking, the prediction error value of LSSVM-BiLSTM is smaller and is more suitable for predicting the CNSS.

4.2 Simulation Analysis

After verifying the computer network situation assessment and prediction performance of LSSVM-BiLSTM, it was applied to different windows for

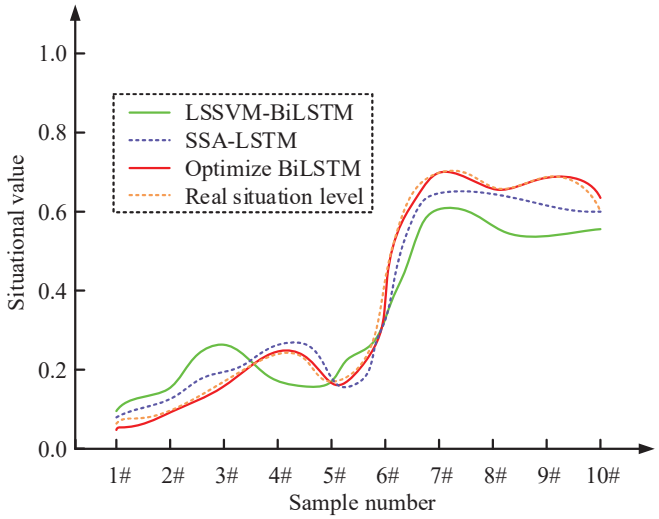

Figure 7 Optimize the network situation prediction results of BiLSTM and BiLSTM, SSA-LSTM.

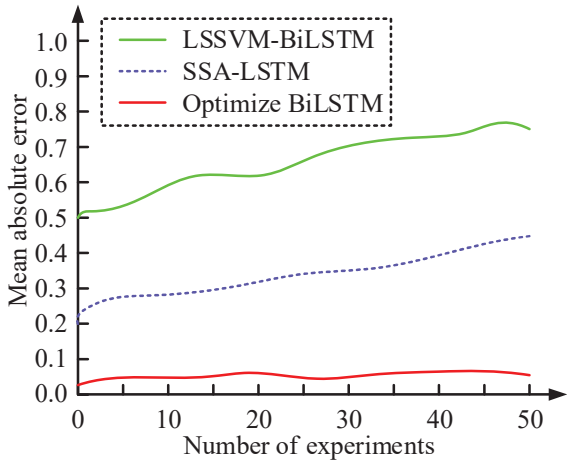

Figure 8 The average absolute error of three algorithms.

simulation analysis. Studies were carried out using window values of 4 and 6, correspondingly. The scenario value of the upcoming time period was predicted using the data from the previous three time periods when the window value was 4, and the previous five time periods when the window value was 6. information for forecasting. Use Mean Squared Error (MSE),

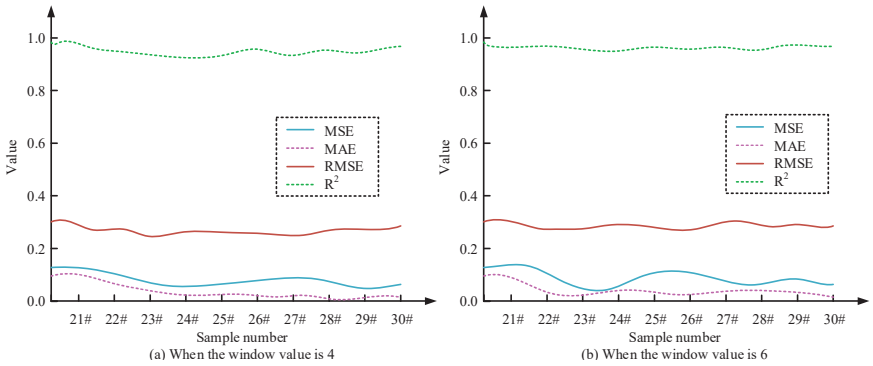

Figure 9 Evaluation results under two different windows.

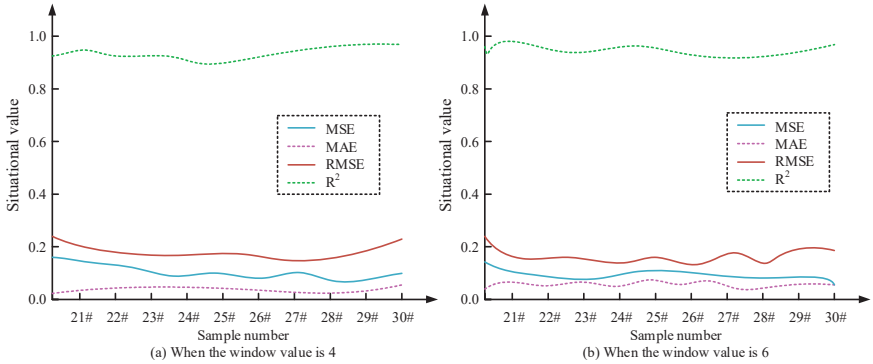

Figure 10 Prediction results under two different windows.

MAE, Root Mean Squared Error (RMSE)-fitting coefficient (Coefficient of Determination, R 2) as evaluation indicators, analyze samples No. 20–30 of the validation set, and the evaluation results under the two windows are shown in Figure 9.

The computer NSSA MSE, MAE, RMSE, and R 2 of the LSSVM-BiLSTM are displayed in Figures 9(a) and 9(b) for window values of 4 and 6, respectively. Figure 9 illustrates that the LSSVM-BiLSTM R 2 values under both windows range from [0.92, 1.0]. The closer the 1.0 value is to 1, the more closely the model fits the data. At the same time, the MSE, MAE, and RMSE values of LSSVM-BiLSTM under the two windows are all low, close to 0.35, 0.16, and 0.07 respectively, which comprehensively demonstrates the superior situation assessment results of LSSVM-BiLSTM. The prediction results under the two windows are shown in Figure 10.

Table 3 Performance comparison results of different algorithms in HCR

Algorithms	Convergence Scalability/%	Running Time/s	Accuracy/%
Random Forest	76.23%	34 s	81.46%
Decision tree	79.54%	33 s	80.91%
XGBoost	80.63%	29 s	83.16%
Deep neural network	86.27%	15 s	90.52%
Support Vector Machine	85.42%	10 s	89.77%
Stacking	89.15%	6 s	88.74%
LSSVM-BiLSTM	93.48%	3 s	94.35%

The LSSVM-BiLSTM's MSE, MAE, RMSE, and R 2 in the window values of 4 and 6, respectively. Figure 10 illustrates that the LSSVM-BiLSTM prediction of CNSS yields better overall results. The average R 2 is 0.92 and 0.93, the average RMSE is 0.21 and 0.22, and the average MAE and MSE under the two windows are 0.04 and 0.08, respectively. Overall, as the window of the LSSVM BiLSTM model increases, its computational complexity also increases, while the overall evaluation metrics remain relatively unchanged. The LSSVM-BiLSTM prediction results have a lower error value and a better fitting degree than the actual scenario value when the window value is fixed.

To further validate the performance of the proposed model, a large-scale network simulation platform, the Heetian Cyber Range (HCR), was selected for the study. Its environment is close to the real network environment, with rich and clear situations, and compared with other advanced algorithms, as shown in Table 3.

From Table 3, it can be concluded that in the HCR environment, the scalability and efficiency of random forests and decision trees are relatively low, with values of 76.23% and 79.54%, respectively. The accuracy of deep neural networks and support vector machines are 90.52% and 89.77%, respectively, but the LSSVM BiLSTM method proposed in the study has a scalability of 93.48% and an accuracy of up to 94.35%. Therefore, it proves the superiority of the model proposed by the research institute.

5 Conclusion

In the face of complex and ever-changing NS threats, research is committed to developing a more accurate and forward-looking computer NSSA tool to enhance network defense capabilities and prevent potential attacks

in advance. First, a comprehensive computer NSSA index system is constructed, LSSVM is used to conduct real-time security situation assessment, and then LSSVM-BiLSTM is used to predict the future security situation. The outcomes revealed that as the number of experiments increases, the MAE of LSSVM-BiLSTM and SSA-LSTM both show an upward trend, while the average absolute error of LSSVM-BiLSTM tends to be stable during the experiment, with smaller fluctuations and an average The MAE is about 0.05. The average MAE of BiLSTM and SSA-LSTM are 0.65 and 0.31 respectively. The simulation outcomes revealed that the R 2 value of LSSVM under both windows is between [0.92, 1.0]. The average MAE of LSSVM-BiLSTM under the two windows are 0.04 and 0.08 respectively. The research results confirm the effectiveness of the method, showing a more prominent ability in detecting new and mutated NAs. In addition to increasing computer NSSA's accuracy, the integration of LSSVM and the optimized BiLSTM network algorithm strengthens the model's capacity to manage intricate nonlinear issues and long-term information dependence, offering strong technical support for computer NS protection. This study still has some shortcomings, the network security situation assessment method lacks authenticity and real-time verification in practical application networks, and fails to comprehensively analyze the diversity of NS threats. In addition, the dual layer BiLSTM network structure is not sufficient to use more complex and changing environments, and its structure needs further optimization. At the same time, the combination of LSSVM method with different network models in the process of dimensionality reduction of data features can easily lead to data loss. Further research is needed in the data processing of LSSVM.

Funding

Research on teaching learning and intelligent control methods for robot operation (KJ2021A1184).

References

[1] Zacharis A, Katos V, Patsakis C. Integrating AI-driven threat intelligence and forecasting in the cyber security exercise content generation lifecycle. International Journal of Information Security, 2024, 23(4): 2691–2710.

[2] Sheng Y, Li J, Di X, Man Z, Liu Z. Bit-level image encryption algorithm based on fully-connected-like network and random modification of edge pixels. IET Image Process. 2022, 16(10):2769–2790.
[3] Pan X, Zhao T, Chen M, Zhang S. DeepOPF: A Deep Neural Network Approach for Security-Constrained DC Optimal Power Flow. IEEE Transactions on Power Systems, 2021, 36(3):1725–1735.
[4] Martini B, Mori P, Marino F, Saracino A, Castoldi P. Pushing Forward Security in Network Slicing by Leveraging Continuous Usage Control. IEEE Communications Magazine, 2020, 58(7):65–71.
[5] Yu Q, Ren J, Zhang J, Liu S, Zhang W. An Immunology-Inspired Network Security Architecture. IEEE Wireless Communications, 2020, 27(5):168–173.
[6] Corallo A, Lazoi M, Lezzi M, Pontrandolfol P. Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level. IEEE Transactions on Engineering Management, 2023, 70(11):3745–3765.
[7] Zhang Z, Cao Y, Cui Z, Zhang W, Chen J. A Many-Objective Optimization Based Intelligent Intrusion Detection Algorithm for Enhancing Security of Vehicular Networks in 6G. IEEE Transactions on Vehicular Technology, 2021, 70(6):5234–5243.
[8] Zhao X. A network security algorithm using SVC and sliding window. Wireless networks, 2023,29(1):345–351.
[9] Shu Z, Taleb T. A Novel QoS Framework for Network Slicing in 5G and Beyond Networks Based on SDN and NFV. IEEE Network, 2021, 35(3):212–222.
[10] Schieber B, Samineni B, Vahidi S. Interweaving real-time jobs with energy harvesting to maximize throughput. International Conference and Workshops on Algorithms and Computation. Cham: Springer Nature Switzerland, 2023, 13(3): 305–316.
[11] Dezfuli S M K P. Targeted killings and the erosion of international norm against assassination. Defense & Security Analysis, 2023, 39(2): 191–206.
[12] Zheng K, Chen Y, Jiang Y, Qiao S. A SVM based ship collision risk assessment algorithm. Ocean Engineering, 2020, 202(Apr.15):107062.1–107062.11.
[13] Sareen K, Panigrahi B K, Shikhola T, Nagdevel R. An integrated decomposition algorithm based bidirectional LSTM neural network approach for predicting ocean wave height and ocean wave energy. Ocean engineering, 2023,281(Aug.1 Pt.2):1.1–1.16.

[14] Huang J, Yang S, Li J, Oh J, Kang H. Prediction model of sparse autoencoder-based bidirectional LSTM for wastewater flow rate. Journal of supercomputing, 2023,79(4):4412–4435.
[15] Abbasihafshejani M, Manshaei M H, Jadliwala M. Detecting and Punishing Selfish Behavior During Gossiping in Algorand Blockchain. 2023 IEEE Virtual Conference on Communications (VCC). 2023, 26(3): 45–55.
[16] Abolfathi M, Shomorony I, Vahid A, Jafarian J H. A game-theoretically optimal defense paradigm against traffic analysis attacks using multipath routing and deception. Proceedings of the 27th ACM on symposium on access control models and technologies. 2022, 8(6):67–78.
[17] Hamdia K M, Zhuang X, Rabczuk T. An efficient optimization approach for designing machine learning models based on genetic algorithm. Neural Computing and Applications, 2020, 33(6):1923–1933.
[18] Du Y, Li F F, Zheng T, Li J. Fast Cascading Outage Screening Based on Deep Convolutional Neural Network and Depth-First Search. IEEE Transactions on Power Systems, 2020, 35(4):2704–2715.
[19] Mazurczyk W, Bisson P, Jover R P, Nakao K, Cabaj K. Challenges and Novel Solutions for 5G Network Security, Privacy and Trust. IEEE Wireless Communications, 2020, 27(4):6–7.
[20] Sun H, Chen M, Weng J, Liu Z, Geng G. Anomaly Detection for In-Vehicle Network Using CNN-LSTM With Attention Mechanism. IEEE Transactions on Vehicular Technology, 2021, 70(10):10880–10893.
[21] Liu J, Ma C, Gui H, Wang S. Transfer learning-based thermal error prediction and control with deep residual LSTM network. Knowledge-based systems, 2022, 237(Feb.15):107704.1–107704.25.
[22] Furdek M, Natalino C, Lipp F, Hock D, Schiano M. Machine Learning for Optical Network Security Monitoring: A Practical Perspective. Journal of Lightwave Technology, 2020, 38(11):2860–2871.
[23] Chen Z, Pasqualetti F, He J, Cheng P, Bullo F. Guest Editorial: Special Issue on Security and Privacy of Distributed Algorithms and Network Systems. IEEE Transactions on Automatic Control, 2020, 65(9):3725–3727.
[24] Pal M, Dedijer S, Laszlo K, Gregor-Svetec D, Cigula T, Pavlovic Z, Milic-Kerestes N. Fold cracking of coated papers: investigation on automated computer-aided visual assessment method. Nordic pulp & paper research journal, 2021, 36(4):626–642.

[25] Wang J, Shi K, Wang L, Pan R, Gao W. A computer vision system for objective fabric smoothness appearance assessment with an ensemble classifier. Textile Research Journal, 2020, 90(3–4):333–343.
[26] Kennedy I R, Hodzic M, Crossan A N, Crossan N, Acharige N, Runcie J W. Estimating Maximum Power from Wind Turbines with a Simple Newtonian Approach. Archives of Advanced Engineering Science, 2023, 1(1):38–54.
[27] Li Wentao, Construction and Analysis of QPSO-LSTM Model in Network Security Situation Prediction, Journal of Cyber Security and Mobility, 2024, 13(3):417–438.
[28] Jiabin Li, Attribute Based Signature Encryption Scheme Based on Cloud Computing in Medical Social Networks, Journal of Cyber Security and Mobility, 2024, 13(3):517–540.

Biographies

Chun Zheng, male, from Hefei, Anhui Province, served at Anhui Sanlian University, master's degree, associate professor. Rresearch interests: Computer network, Internet of Things technology and application. Participated in presiding over 5 national projects, 8 projects of Anhui Provincial Department of Education, published more than 10 papers, participated in the editing of 5 textbooks, and guided the students to participate in AB events to win more than 30 awards at the provincial level and above.

Hua Jin, male, from suzhou, Anhui Sanlian University, master's degree, associate professor. Research interests: Artificial Intelligence.