Hindawi
Mobile Information Systems
Volume 2022, Article ID 6214738, 14 pages
https://doi.org/10.1155/2022/6214738

Research Article

A Situation Awareness Approach for Network Security Using the Fusion Model

Dongmei Zhao,[1,2,3] **Yaxing Wu**,[1] **and Hongbin Zhang**[4]

[1]*College of Computer and Cyber Security, Hebei Normal University, Shijiazhuang, Hebei 050024, China*
[2]*Hebei Provincial Key Laboratory of Network and Information Security, Shijiazhuang, Hebei 050024, China*
[3]*Hebei Provincial Engineering Research Center for Supply Chain Big Data Analytics & Data Security, Shijiazhuang, Hebei 050024, China*
[4]*School of Information Science and Engineering, Hebei University of Science and Technology, Shijiazhuang, Hebei 050018, China*

Correspondence should be addressed to Yaxing Wu; wyxhebnu@stu.hebtu.edu.cn

Received 13 June 2022; Accepted 5 August 2022; Published 21 August 2022

Academic Editor: Muhammad Zakarya

Aiming at the limited learning ability of a single model, the objective of this paper is to investigate situational awareness of the network security which is established on the fusion model. In this paper, a convolutional neural network (CNN) and long short-term memory (LSTM)-based model for situational assessment of the network security condition are provided. According to different fusion methods, the parallel and serial CNN-LSTM fusion models were constructed to evaluate the UNSW-NB15 data set, and both the situation values and levels were obtained. The investigational outcomes illustrate that the evaluation accuracy of the two models can reach up to 85.19% and 92.59%, respectively. A situation prediction model called IPSO-ABiLSTM is suggested and is based on improved particle swarm optimization (IPSO) and attention fusion bidirectional long short-term memory (ABiLSTM). The IPSO has the characteristics of faster convergence speed to optimize the ABiLSTM network parameters and obtain the optimal parameters for situation prediction. The investigational outcomes illustrate that the suggested IPSO-ABiLSTM model has a fitting degree of up to 0.9922, which can effectively achieve the situation prediction in the network security.

1. Introduction

With the prompt growth of 5G networks, the Internet, and smart cities, it is becoming more and more difficult to defend against attacks. Traditional network security facilities include anti-virus software, firewalls, vulnerability scanning, and other facilities, all of which belong to passive protection systems. When each new virus appears, it often takes several days or tens of days for manufacturers to make the passive protection system detect. When it comes to these new viruses, the time difference between them will stance a great threat to the network security, and it is challenging to encounter the network security requirements of the current era. Therefore, the research on this passive protection system has encountered a bottleneck. Being able to evaluate the current situation of the network security in a timely manner, and founded on the present and past security situation, forecast the change tendency of the situation for network security in the next period of time is particularly critical to protect resource security. For that reason, the research on awareness of the network security situation is an urgent need.

The idea of situation awareness and assessment was first suggested by Endsley [1] in 1988. With the goal of improving pilots' air combat capability, the authors constructed a classic three-layer situation awareness model, namely situation: (i) element extraction, (ii) assessment, and (iii) prediction. The application of perception is only in the Air Force combat domain. Subsequently, Bass et al. [2] combined the concept of situational awareness with the cybersecurity, which indicated that the next-generation network intrusion detection system (IDS) should be integrated with the data gathered by multiple short-term network sensors and long-term data to achieve cyberspace situation awareness. Due to these limitations, the situation awareness in the network security has become a major research hotspot.

Yan et al. [3] constructed a network security threat assessment model by combining the fuzzy concept with the game matrix and demonstrated the evaluation usefulness of the suggested model with an example. Zhang et al. [4] applied convolutional neural networks (CNN) to network security situation prediction. In order to enhance the learning capability of the CNN and reduce the training time of the CNN, a network based on composite convolution structure was suggested. The network security condition is well predicted, but in fact, the effect of the CNN on time series prediction problems needs to be improved. Chen et al. [5] constructed a network security condition prediction prototype which is established on the Gravitational Search Algorithm (GSA) that can help to elevate Support Vector Machine (SVM). To a certain extent, the accuracy of situation forecasting has been improved, but SVM is slightly insufficient in the ability of time series forecasting, and the accuracy of situation prediction needs to be improved. Zhang et al. [6] constructed a network security condition assessment model using a deep self-encoding network, combining unsupervised training and supervised fine-tuning training. The investigational outcomes expressed that the suggested model has high evaluation correctness, but the disadvantage is the data set used. It is too old and needs to be verified on a new dataset. Wang et al. [7] optimized the correction factor of probabilistic neural networks (PNN) through genetic algorithm (GA), which improved the stability and accuracy of the model, but when dealing with small sample data. The disadvantage is that the evaluation takes a relatively long time. Xu et al. [8] proposed a reasoning method to realize network security situational awareness, which is more capable than traditional methods. Zhang et al. [9] combined LSTM and decision tree to achieve network security situation prediction. LSTM was used to predict data sets, and DT to identify attack types. The experiments proved that the situational awareness model proposed in this paper has a high accuracy.Dai et al. [10] constructed a zero-trust method situational awareness model, which is a new theory emerging in recent years and has good application prospects.

To sum up, machine learning models are being used to a greater extent in the arena of network security, in particular for situation awareness, nonetheless, we believe that the learning ability of a distinct model is still limited. Bestowing to the advantages and characteristics of dissimilar models, this paper will conduct in-depth investigation on the two key parts of network security, that is, (i) position assessment, and (ii) prediction. The suggested work is in fact established on the fusion model, so that relevant personnel can have a deeper understanding of the network security condition, and at that moment make reasonable decisions. In terms of the former point (i) for network security, a situation calculation method for the network security is suggested that combines both the classical CNN and LSTM networks. In fact, the CNN and the LSTM are two models with strong learning abilities in deep learning. Similarly, in order to build a model with stronger learning ability and to realize condition assessment in the network security, CNN's convolution and pooling operations can extract important local features, while LSTM has certain advantages in extracting time series data. The model evaluation after the fusion of the two models is that the accuracy can reach 85.19% and 92.59%.

In terms of situation prediction within the context of network security, in this paper, we suggest a forecasting model which is established over the idea of an IPSO, Attention, Fusion, and Bidirectional Long Short Term Memory (IPSO-ABiLSTM) network with improved particle swarm optimization and attention mechanism. This should be noted that the IPSO balances the global and the local searching abilities, speed up the convergence swiftness, and relieves the procedure from deteriorating into the local optimal solution. Furthermore, the BiLSTM approach can combine the before and after conditions, and then integrate the BiLSTM approach with the attention technique to improve the model's attention to key information. The network structure of the ABiLSTM approach is optimized by IPSO algorithm to increase the performance of the suggested model. The investigational outcomes express that associated with other models, in this paper, the forecasting influence of the suggested technique is better than others. The fundamental contributions of this research are listed, in bullets form, as follows:

(i) A network security situation assessment model which is established on the fusion of CNN and LSTM techniques is suggested.

(ii) According to the different fusion methods, the parallel serial CNN-LSTM fusion models were constructed to evaluate the UNSW-NB15 data set, and both the situation values and levels were obtained.

(iii) A condition forecasting model which is grounded on the IPSO, as well as, the ABiLSTM, that is, IPSO-ABiLSTM is suggested.

(iv) The IPSO has the characteristics of faster convergence speed to optimize the ABiLSTM network parameters and obtain the optimal parameters for situation prediction.

The rest of this manuscript is prescribed in the following fashion: in Section 2, we talk over the CNN-LSTM fusion network security condition valuation model. In Section 3, creation of the network security condition indicator system is deliberated. In Section 4, we discuss BiLSTM fusion Attention Mechanism network security situation prediction. In Section 5, experimental analysis and the attained outcomes are discussed in detail. Finally, Section 6 completes this article and delivers future research guidelines and instructions.

2. The CNN-LSTM Fusion Network Security Situation Assessment Model

2.1. The CNN Model. In 1989, LeCun suggested that the LeNet5 convolutional neural network is constructed on gradient descent for reading documents and text recognition [11]. The LeNet5 is the classic structure of modern CNN, and then CNN was widely used to solve multiclass problems, such as image segmentation [12], object recognition [13], and computer vision [14]. The basic structure of the CNN model, in fact, comprises five layers, that is (i) an input layer,

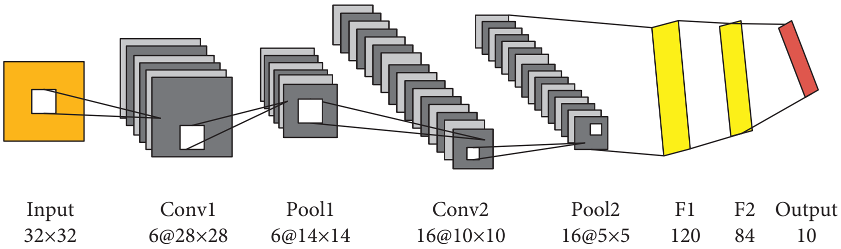

Figure 1: The basic organization of the CNN model.

(ii) a convolutional layer, (iii) a fully connected layer, (iv) a pooling layer, and (v) an output layer. The basic view of the CNN construction and various layers is shown in Figure 1.

We assume, in this paper, that the activation function of each layer of the CNN model embraces the RELU function. The RELU function can answer the main issue of gradient disappearance that may potentially exist in the model training. Furthermore, this may also help to reduce the computation and calculation amount of the model training, over the datasets, and subsequently accelerate the training process of the network model.

2.2. The LSTM Model. The recurrent neural network (RNN) model establishes a connection between neurons in the concealed layer. In other words, that is, the output of a neuron can be used as an input at the next moment, so that the entire network structure has a memory function. For that reason, it can be used as an input and also can be used to deal with the computation timing issues.

After a lot of practice, the RNN has been proved to have the major issue of gradient explosion and gradient disappearance [15]. Therefore, it only has the ability of short-term memory. In order to recover the issues existing in the RNN model, Schmidhuber et al. [16] suggested the LSTM approach. The LSTM model, in fact, improves the working principle of the concealed layer which is used in the RNN model. This should be noted that the LSTM structure comprises forgetting gate, input gate, output gate, memory unit, candidate memory unit, and output value. The specific mathematical equations of a particular LSTM unit at particular time, denoted by t, are as follows from formula (1 to 6):

$$\tilde{c}_t = \tan h\left(W_c \cdot \left[h_{t-1}, x_t\right] + b_c\right), \tag{1}$$

$$i_t = \sigma\left(W_i \cdot \left[h_{t-1}, x_t\right] + b_i\right), \tag{2}$$

$$f_t = \sigma\left(W_f \cdot \left[h_{t-1}, x_t\right] + b_f\right), \tag{3}$$

$$c_t = f_t \otimes c_{t-1} + i_t \otimes \tilde{c}_t, \tag{4}$$

$$o_t = \sigma\left(W_o \cdot \left[h_{t-1}, x_t\right] + b_o\right), \tag{5}$$

$$h_t = o_t \otimes \tan h\left(c_t\right). \tag{6}$$

In equations (1) to (6), W and b are the equivalent weights and biases, $\tan h$ is the tangent activation function, σ is the sigmoid activation function, and $\otimes$ represents the matrix Hadamard product. Note that further discussion and explanation of these equations are given in subsequent sections.

2.3. Implementation of the Situation Assessment for Network Security Founded on the CNN-LSTM Fusion Model. Each neural network model has its own unique advantages. For example, CNN can successfully excerpt local structures and characteristics of data through convolution kernels, but cannot learn the relationship between data time series. The gating mechanism introduced in LSTM can be very good. In case of handling relative time series data, it should be kept in mind that the features in the network attack PCP data that are complex and changeable and have different degrees of importance. There may also be some relationship between the attack data. According to the respective advantages of CNN and LSTM, this paper combines the two neural network models. Each has its own advantages to increase the correctness of network attack recognition.

In fact, the fusion of CNN and LSTM has two methods: serial and parallel. Serial fusion is to extract the input data through CNN features and then go through LSTM. The parallel fusion is that CNN and LSTM approaches usually extract various characteristics from the input data at the same time, and then subsequently connect the extracted features from the two parts. The effects of the two methods may also be different on different problems. In this paper, Serial CNN-LSTM (CNN-LSTM-S) and Parallel CNN-LSTM (CNN-LSTM-P) are constructed, respectively. Two models are used to verify the advantages of the fusion model for situation assessment in the network security. The specific structures of the CNN-LSTM-S and the CNN-LSTM-P models that are used in this paper are revealed in Figures 2 and 3, respectively.

The situation assessment process of the network security system of the CNN-LSTM approach is shown in Figure 4.

3. Construction of the Network Security Condition Indicator System

The realization of situation assessment for the network security first requires the support of the network security condition index system, and at that moment builds a suitable evaluation model. The model evaluates the network security position value as well as its level rendering to the index system of the network security situation. The assessment results can enable relevant personnel to comprehend the present situation of the network security. Whether it is safe

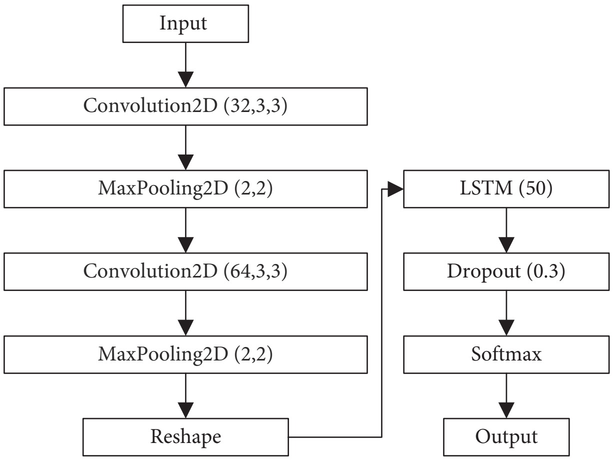

Figure 2: The CNN-LSTM-S model structure.

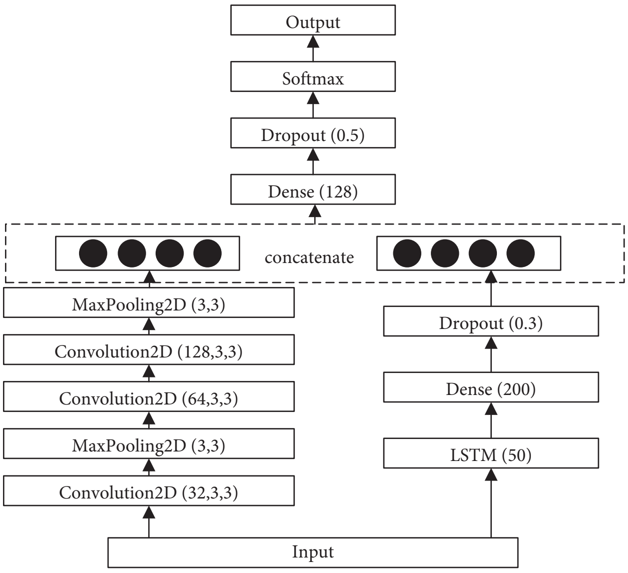

Figure 3: The CNN-LSTM-P model structure.

and what kind of threats exist, make corresponding decisions according to the problems existing in the network.

3.1. Network Security Position Indicator System Established on Attack Impact. In this paper, we establish a situation indicator system for the network security founded on the attack impact. First, fully consider the internal correlation of each main influencing element in the network. Second, the means of network attacks are increasingly complex, diversified, and frequent, and different types of attacks have different impacts on the entire network. Only by improving the detection rate of the network attacks received can the network status be more accurately perceived.

Situation indicator factors include the following:

(1) Attack quantity factor: This factor refers to the number of attack samples received by the network in a certain period of time, represented by N.

(2) Attack threat factor: This factor refers to the degree of threat to network security by different attack types in the network, represented by X.

The calculation formula of the situation value of the period is as follows in formula (7):

$$\begin{aligned}\mathrm{SA}(t) &= f\left(N, X_i\right)\\ &= \sum_{i=1}^{N} X_i.\end{aligned} \tag{7}$$

The attack traffic characteristics and methods collected by the commonly used KDD cup99 and NSL-KDD [17, 18] datasets can no longer represent the network conditions of the current era. The novel UNSW-NB15 dataset [19, 20] does not contain the situation value in the UNSW-NB15 dataset, so we adopt the above calculation method to generate the situation value representing the security degree of the network. According to the sequence of each sample collected in UNSW-NB15, 3000 samples are taken as a period. The threat factors corresponding to the attacks in the data set are shown in Table 1 The true situation value of the data set is calculated according to formula (7), and the data set is the situation values of all periods are converted into the [0, 1] interval. After quantification, the UNSW-NB15 test set consists of 27 periods in total. The UNSW-NB15 dataset attack threat factors are presented in Table 1.

3.2. Classification of Network Security Situation Levels. This paper combines the introduction of the straightforward network security condition, along with a simple assessment model, of the National Internet Emergency Center with the actual situation of modern networks. The network security level is divided into four levels, which correspond to different situation value intervals. By dividing the security level, relevant departments can understand more intuitively and quickly the current state of the network. The grading rules are displayed in Table 2.

4. The BiLSTM Fusion Attention Mechanism for Network Security Situation Prediction

4.1. The BiLSTM Model. The BiLSTM model consists of forward and reverse LSTM layers superimposed [21]on each other, and the output is jointly determined by the two LSTM layers, and its structure is shown in Figure 5. This should be noted that the forward layer of the LSTM model can be regarded as a forward calculation from the start time to the last time. On the other way, the reverse layer of the LSTM model can be regarded as a reverse calculation from the last time to the start time. Note that both layers are treated and handled in the same manner. Finally, the model combines the outputs of the model's forward layer and the model's reverse layer, at each moment, in order to get the output of the model at that particular moment.

4.2. The Attention Mechanism. The BiLSTM model has achieved good results in extracting sequence information,

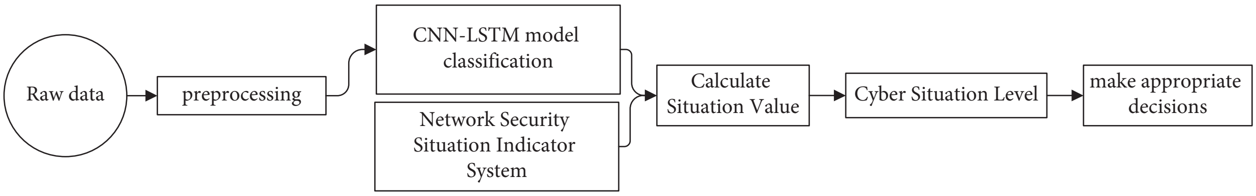
Raw data
preprocessing
CNN-LSTM model classification
Network Security Situation Indicator System
Calculate Situation Value
Cyber Situation Level
make appropriate decisions

Figure 4: The CNN-LSTM model network security situation assessment process.

Table 1: The threat factors in the UNSW-NB15 dataset attack.

Attack category	Attack threat factor	Attack category	Attack threat factor
Normal	1	Generic	6
Analysis	2	Shellcode	7
Reconnaiss	3	Worms	8
Fuzzers	4	Exploits	9
Dos	5	Backdoor	10

Table 2: The classification of network security levels.

Level	Situation value	Security level	Situation description
1	[0.00–0.25]	Safety	Network is working fine
2	(0.25–0.50]	Low risk	Network is slightly affected
3	(0.50–0.75]	Medium risk	Network is affected
4	(0.75–1.00]	High risk	Network is highly affected

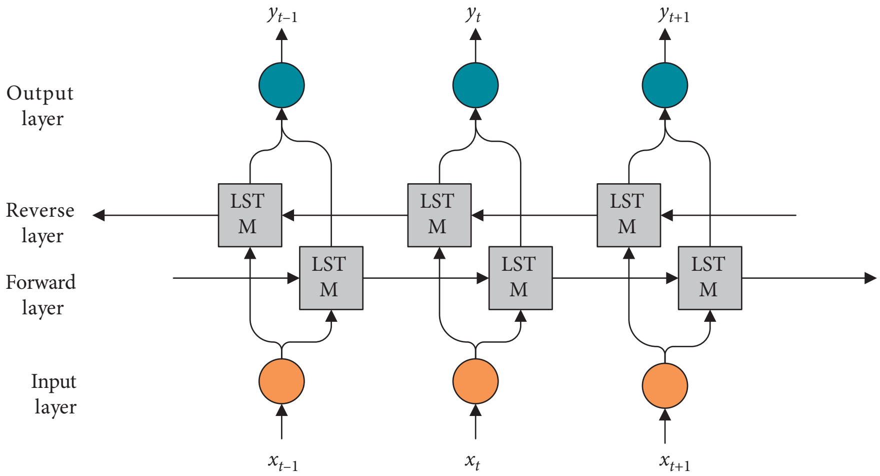

Figure 5: The basic structure of the BiLSTM network.

but the importance of different features in real network conditions is also very different. BiLSTM alone cannot identify the importance of features in sequences.

The attention mechanism is inspired by the working mechanism of human brain. In the process of cognition of the things around us, people will always give priority to what they want to see, thus ignoring some things they do not need. This is evident from the literature that the attention method has been widely implemented and used in many research fields. For example, literatures [22–24] applied the attention mechanism in the arenas of image analysis, computer vision, and natural language processing, and accomplished worthy and noble outcomes. Adding the attention mechanism to BiLSTM can offer more consideration to the influence of different inputs on the output and focus on selective learning of the input to improve the learning effects of the neural network [25]. The basic view of various layers and organization of the ABiLSTM model, constructed in this paper, is exposed in Figure 6.

For the ABiLSTM network, the parameter selection in its structure is crucial to the effect of the model, for instance, the total amount of hidden layers, weights, the quantity of hidden layer units, and the frequency or rate of learning. Many researchers determine these parameters based on

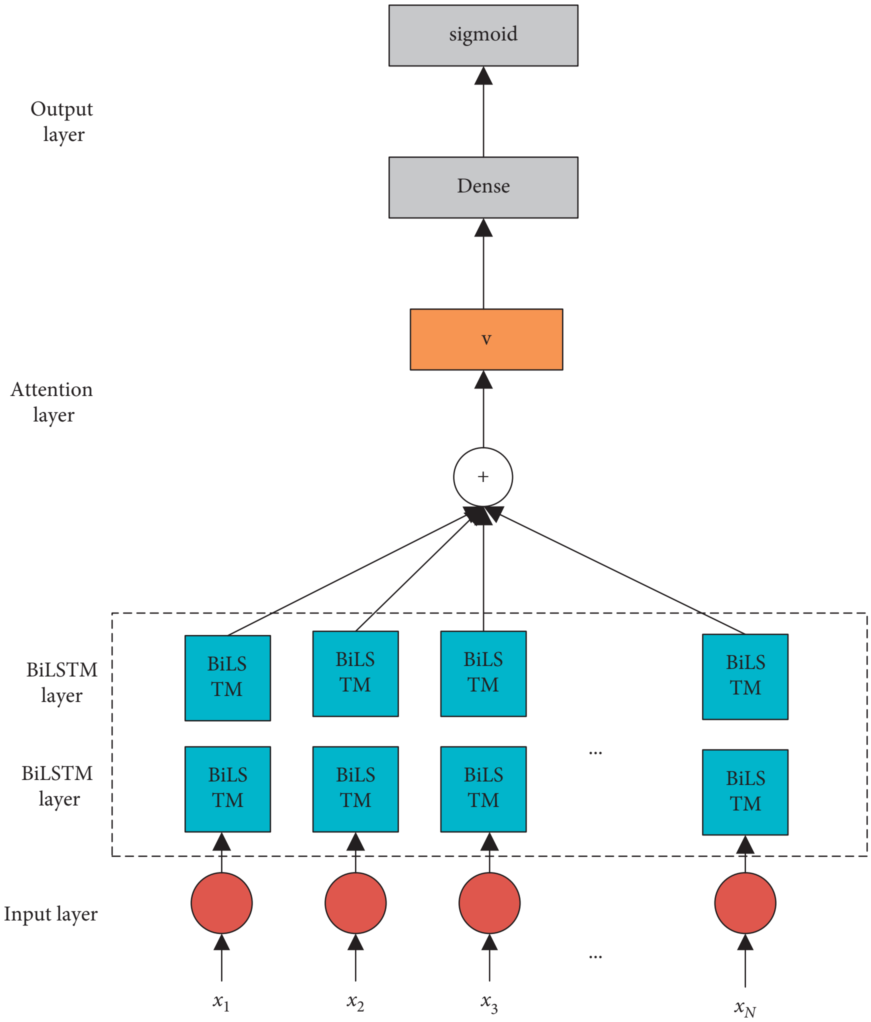

Figure 6: The ABiLSTM model network structure and layers.

experience or trial and error. Parameters which make the robustness and accuracy of the model unreliable. Therefore, this paper selects the well-known and widely used particle swarm optimization procedure, which is simple in principle, low in complexity, fast in convergence speed, and suitable for dealing with real-valued problems, to optimize the structural parameters of the ABiLSTM network.

4.3. The IPSO Method. The PSO method is a bionic swarm optimization procedure suggested by Dr. Eberhart and Dr. Kennedy [26] in the year 1995. The algorithm originated from the investigation on the regular predation comportment of birds. The straightforward knowledge of the PSO method is to treat each answer of the problem as a D-dimensional massless particle. Moreover, every particle has a fitness value which is computed through the fitness function. In the search space, each particle is optimal according to the individual. The location and, more formally, the global optimal location are used to update its own speed and position, and through iterative search, the optimal station of the complete particle swarm is obtained [27].

In each iteration, the particles in the swarm determine the direction and distance of their search by their velocity. The update formulas both for the particle's velocity, as well as, position of the basic particle swarm are as given in equations (8) and (9), respectively:

$$V_{i\,d}^{k+1} = wV_{i\,d}^{k} + c_1 r_1 \left(p\,\text{best}_{i\,d}^{k} - X_{i\,d}^{k}\right) + c_2 r_2 \left(g\,\text{best}_{g\,d}^{k} - X_{i\,d}^{k}\right), \tag{8}$$

$$X_{i\,d}^{k+1} = X_{i\,d}^{k} + V_{i\,d}^{k+1}. \tag{9}$$

In equations (8) and (9), w exemplifies the inertia weight factor, that is, the ability of the particle to inherit the speed of the previous iteration, and k exemplifies the present iteration number. Furthermore, c_1 and c_2 represents the two acceleration factors, which are used to regulate the guidance of the specific optimal solution and the global optimal solution on the speed of each iteration. Note that the sum is a random number between [0, 1]. Moreover, both the V_{id}^{k} and X_{id}^{k} variables characterize the speed and position of the d-dimensional space of the ith particle in the kth iteration, correspondingly. Finally, the $p\text{best}_{\text{id}}^{k}$ and the $g\text{best}_{g\,d}^{k}$

variable correspondingly characterize the specific optimal position (the former one) and the global optimal position (the latter one) of the dth dimensional space of the ith particle in the kth iteration.

In the PSO algorithm, the factor of inertia weight and the factor of acceleration are very important to the efficiency and results of the PSO algorithm. When the factor of inertia weight and the factor of acceleration are significantly large, then the global optimization ability is better. However, if the factor of inertia weight and the factor of acceleration is small, then the smaller the factor, the better is the local optimization ability. Since the factor of inertia weight and the factor of acceleration coefficient in the traditional particle swarm optimization procedure are stationary, then along with the local optimization capability, the global optimization ability of the procedure is also limited. Furthermore, it is also very trivial and easy to make the algorithm fall into the local minimum value, that is, premature convergence. In view of the limitations of the algorithm, the factor of inertia weight and the factor of acceleration are improved in this paper, so that the change of speed is changed from linear to nonlinear.

The improvement to the inertia weight factor w is mathematically illustrated using (10) as follows:

$$w = -\pi * \arcsin(0.01 * (t - \max\_\text{iter})). \tag{10}$$

The improvements to the acceleration factors are as follows and mathematically illustrated in (11) and (12):

$$c_1 = c_{1\max} - (c_{1\max} - c_{1\min}) * \left(\frac{t}{\max\_\text{iter}}\right) * * 2, \tag{11}$$

$$c_2 = c_{2\max} - (c_{2\max} - c_{2\min}) * \left(\frac{t}{\max\_\text{iter}}\right) * * 2. \tag{12}$$

In equations (11) and (12), max_iter exemplifies the maximum amount of iterations, and t symbolizes the present numeral figure of iterations. Similarly, the two variables $c_{2\max}$ and $c_{2\min}$ characterizes the maximum and minimum values for the factors of acceleration, in the previous iteration, correspondingly. It should be noted that the two variables denoted by $c_{1\max}$ and $c_{1\min}$ exemplifies the maximum and minimum values for the factor of acceleration coefficient, after the update, correspondingly.

4.4. Implementation of the Situation Assessment in the Network Security Constructed on the Suggested IPSO-ABiLSTM Model.

The process for situation prediction in the network security using the suggested IPSO-ABiLSTM model is given away in Figure 7.

5. Experimental Analysis

The computer and its hardware specification that was used for the tests to evaluate the method suggested in this paper, which is as follows: the system model was Intel(R) Core(TM) i5-8250U CPU @ 1.60 GHz CPU and having 1 TB mechanical hard disk, 12 GB memory, 64 bit Windows operating system, and NVIDIA GeForce GT 730 graphics card. The experimental environment was Tensorflow2.2.0 and Keras2.3.1 framework based on *Python* 3.6 environments, and the IDE was PyCharm2020.2.3. We used machine learning libraries such as Sklearn, integrated with Matplotlib in order to assist in completing experiments.

5.1. Experimental Results Analysis for the Situation Assessment Model

5.1.1. Experiment Evaluation Index. In order to authenticate the model's performance that is suggested in this paper, we choose the commonly used evaluation indexes and metrics in the field of network intrusion detection, prediction, and machine learning, that is, (i) Accuracy, (ii) Precision, (iii) Recall, and (iv) F1 score. Using these indexes, we compare the performance of suggested model with other state-of-the-art techniques and closest rivals.

(1) *Accuracy* is represented by *Acc* and is defined as the proportion of data samples that were appropriately categorized or predicted by the suggested approach to the entire quantity of data samples.

(2) *Precision* is represented by P and is defined as the proportion of ordinary data samples that were properly categorized or predicted by the suggested approach to entire data samples categorized as positive.

(3) *Recall* is represented by R and defined as the proportion of normal data samples that were acceptably categorized or predicted by the suggested approach to the complete amount of true normal samples.

(4) *F1 score* is represented by $F1 -$ score, is in fact denotes the harmonic average of accuracy (precision), and the recall rate. Taking precision recall into consideration, the higher the F1 score, the more balanced the precision and recall, and the improved or higher the overall performance of the model.

The above four evaluation metrics are calculated using formulas (13)–(16) which are given as follows:

$$\text{Acc} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}, \tag{13}$$

$$P = \frac{\text{TP}}{\text{TP} + \text{FP}}, \tag{14}$$

$$R = \frac{\text{TP}}{\text{TP} + \text{FN}}, \tag{15}$$

$$F1 - \text{socre} = \frac{2 * P * P}{P + R}. \tag{16}$$

In equations (13)–(16), TP refers to the quantity of normal data samples appropriately classified, and TN represents the amount of abnormal data samples acceptably classified by a particular model. Furthermore, FP represents the abnormal data samples that were in fact erroneously classified, and FN represents the inappropriate and incorrect classification by the model in terms of the normal data sample.

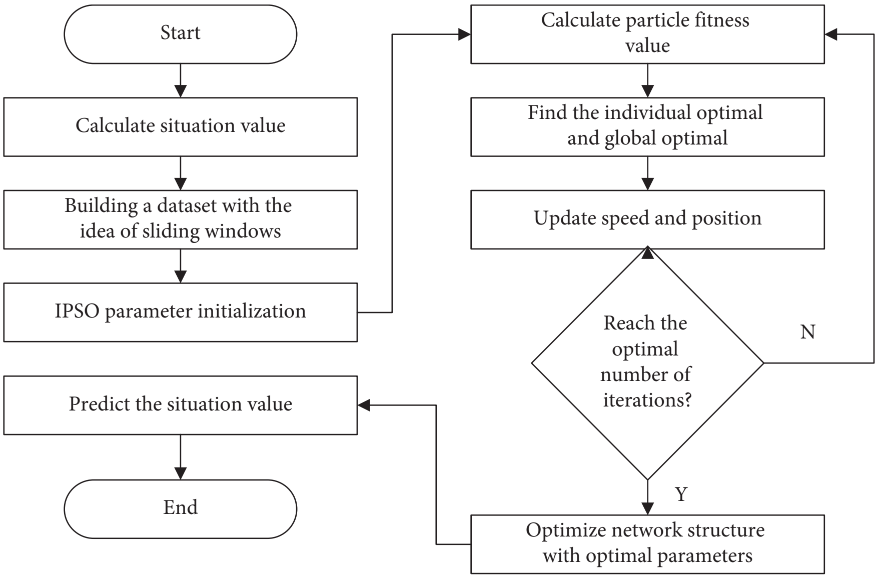
Start
Calculate situation value
Building a dataset with the idea of sliding windows
IPSO parameter initialization
Predict the situation value
End
Calculate particle fitness value
Find the individual optimal and global optimal
Update speed and position
Reach the optimal number of iterations?
N
Y
Optimize network structure with optimal parameters

Figure 7: The IPSO-ABiLSTM prediction process.

5.1.2. Two Classification Experimental Analysis. In the first experiment, the labels of the dataset are distributed into two groupings: (i) normal, and (ii) abnormal. In order to prove that the suggested CNN-LSTM fusion technique has a stronger learning ability, it is compared with a single model. The evaluation index results of each model are given away in Table 3.

Table 3: Assessment of the two classification results of each model.

Model	Acc (%)	P (%)	R (%)	F1 score (%)
CNN-LSTM-P	89.71	95.22	82.43	88.36
CNN-LSTM-S	87.32	97.53	74.33	84.35
CNN	85.63	98.55	69.03	81.19
LSTM	82.13	92.03	61.47	75.56
BiLSTM	83.55	94.02	67.70	78.72
GRU	82.56	96.66	63.39	76.57

By observing Table 3, it can be comprehended that the correctness, as well as, the recall rate of the CNN-LSTM-P and CNN-LSTM-S methods that were suggested above are significantly higher than the closest rivals, that is, the four single models, ranking first and second, respectively. At the same time, the precision rate is also second only to CNN. Considering the contradiction among the accuracy rate and the recall rate, we further investigated and observed the index of the F1 score. The F1 score of the two models suggested in this paper are 88.36% and 84.35%, respectively, ranking first and second. Second place, and well above the F1 score of the other models.

Model time is also a very realistic metric. In the same experimental environment, the detection time of the two models suggested in this paper is shown in Table 4. This can be comprehended from the observations and assessment that the two-classification time of the CNN-LSTM-P technique is approximately 79.41s less than that of the CNN-LSTM-S method. Moreover, we also noted that the attack recognition effectiveness of the CNN-LSTM-P model is significantly higher than the CNN-LSTM-S method.

5.1.3. Ten Classification Experimental Analysis. The second experiment is a ten-category experiment. The model that is suggested in this paper is matched with a single model. The evaluation index outcomes of various models and methods are shown in Table 5.

By observing Table 5, this can be easily comprehended that the correctness, exactness, recall, and the F1 score index of the suggested CNN-LSTM-P and CNN-LSTM-S models are meaningfully superior than the other four single methods. Among them, the correctness rate, recall rate, and F1 score of the CNN-LSTM-S method are the best values among all compared models. The CNN-LSTM-P model accuracy, recall, and F1 score are all suboptimal values for all models, and the precision is the optimal value. Combining the experimental results of two-class and ten-class, this could be observed and well understood that the learning performance of the suggested model has been meaningfully enriched as matched with the traditional single methods.

In the subsequent discussion, we further investigate and analyze the performance of the suggested model from the perspective of time consumption. Under the same experimental environment, the detection time of the two models suggested in this paper is shown in Table 6. The ten-class time-consuming of the CNN-LSTM-P method is approximately 93.15s less than that of the CNN-LSTM-S method. Furthermore, the CNN-LSTM-S method has relatively lower performance. The detection efficiency of the CNN-LSTM-P model is higher than all the closest rivals. Combining the time-consuming comparison of the two classifications methods, it can be understood that the suggested CNN-LSTM-P method is always less time-consuming than the CNN-LSTM-S method, and is more efficient while maintaining accuracy.

Table 4: Time-consuming comparison of two classifications.

Model	Training duration (seconds)	Testing duration (seconds)	Total time (s)
CNN-LSTM-P	585.79	10.26	596.05
CNN-LSTM-S	665.31	10.15	675.46

Table 5: Assessment of ten classification results of each model.

Model	Acc/%	P/%	R/%	$F_{1\text{-score}}$/%
CNN-LSTM-P	77.15	96.78	78.60	86.75
CNN-LSTM-S	78.47	95.38	82.94	88.72
CNN	75.27	95.56	74.49	83.72
LSTM	72.61	95.06	69.87	80.54
BILSTM	72.71	93.12	71.16	80.67
GRU	72.73	95.48	69.28	80.29

Table 6: Time-consuming comparison of 10 categories.

Model	Training duration (seconds)	Testing duration (seconds)	Total time(s)
CNN-LSTM-P	587.23	10.59	597.82
CNN-LSTM-S	680.73	10.24	690.97

5.1.4. Analysis of Network Security Situation Assessment Results. The training results of the suggested CNN-LSTM-P method, as well as, the CNN-LSTM-S model are quantified according to Formula (7). In this way, we are able to acquire the situation value of each and every period, and the network security level corresponding to each period is divided according to Table 2, and the security level of 27 periods is obtained. The comparison between the network security situation assessment outcomes of the suggested model and the real situation level is presented in Figure 8.

Observing Figure 8, this could be easily understood that the suggested CNN-LSTM-S method has errors in only two periods. In the fourth period, the “high risk” error is evaluated as “medium risk,” and in the eighth period, the “medium risk” error is evaluated as “Low risk.” In fact, through analyzing this, this could be even more easy to found that the suggested CNN-LSTM-S method has a weak ability to identify attacks with a high degree of threat and tends to identify attacks with a relatively low degree of threat. The evaluation grades for the remaining periods matched the true grades exactly. This should be noted that the CNN-LSTM-P model has more mis-evaluation periods, which are in 8, 23, 25, and 27 periods, respectively.

In the 27 evaluation periods, the number of correct evaluations and the correct rate of the model in this paper are shown in Table 7.

By observing Table 7, the number of correct samples for the evaluation of the CNN-LSTM-P model is 23, and the correct rate is approximately 85.19%. Similarly, the number of correct samples for the evaluation of the CNN-LSTM-S model is 25, and the correct rate reaches 92.59%. Although, the model still has many shortcomings, it is enough to prove that the suggested model can be precisely implemented on situation assessment in the network security.

5.2. Analysis of the Results of the Situation Prediction Experiment

5.2.1. Number of BiLSTM Input and Output Neurons. According to the sliding window idea, the situation value data set used for prediction is divided according to its time sequence, and the organization of the divided data set is presented in Table 8.

In the second row of Table 8, $m+1$ represents the size of the sliding window, and the amount of neurons in the input layer of the LSTM model is equivalent to m during prediction. As the experiment in this paper is a single-value prediction, we assume that the amount of neurons in the output layer is 1.

5.2.2. Experiment Evaluation Index. In order to confirm the predictive capability of numerous methods that are used in this paper, the Coefficient of Determination (R^2) and the Mean Absolute Percentage Error (MAPE) were selected as the model evaluation indicators. The calculation formulas for the MAPE and R^2 metrics are as given in (17) and (18), respectively.

$$\text{MAPE} = \frac{1}{N}\sum_{i=1}^{N}\left|\frac{\hat{y}_i - y_i}{y_i}\right| \times 100\%, \tag{17}$$

$$R^2 = 1 - \frac{\sum_{i=1}^{N}\left(y_i - \hat{y}_i\right)^2}{\sum_{i=1}^{N}\left(y_i - \overline{y}\right)^2}. \tag{18}$$

In equations (17) and (18), the variable y_i exemplifies the true situation value, while the variable $\hat{y}_i$ symbolizes the forecasted situation value. Furthermore, N characterizes the quantity of samples, while the variable $\overline{y}$ signifies the

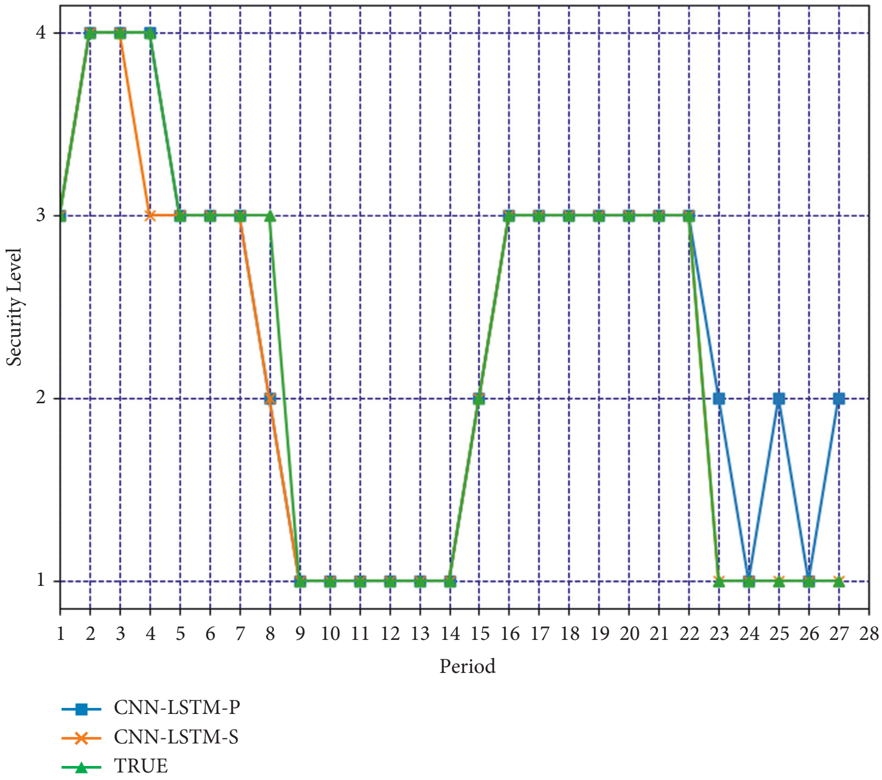

Figure 8: Evaluation outcomes for situation assessment in network security.

Table 7: Assessment of correct rates of network security situation assessment.

Model	Correct number	Correct rate (%)
CNN-LSTM-P	23	85.19
CNN-LSTM-S	25	92.59

Table 8: Data set structure for prediction.

Number	Input	Output
1	$(x_1, x_2, \ldots, x_m)$	x_{m+1}
2	$(x_2, x_3, \ldots, x_{m+1})$	x_{m+2}
...	...	...
$n-m$	$(x_{n-m}, x_{n-m+1}, \ldots, x_{n-1})$	x_n

statistical mean value of the true situation value. This should be noted that the lesser the mean percentage error, the better and superior will be the model performance and vice versa. Furthermore, the coefficient of determination of the goodness of fit is between the range of [0, 1]. Note that, for the goodness of the fit, the nearer its value to 1, the superior will be the model fitting and vice versa.

5.2.3. Experimental Analysis of Situation Prediction for Network Security. In order to confirm the specific prediction effect of each model, this paper provides the prediction outcomes of every method when the window size is 2, 3, and 4, as shown in Figures 9–11. A window of 3 means that the situation values of the previous two time periods are selected to predict the situation values of the next time period.

In fact, this can be comprehended from Figures 9 to 11 that when the window is 2, the IPSO-ABiLSTM suggested in this paper almost completely fits the real situation value, while the other three models all have a certain degree of fitting deviation. The window size is 3 and 4. In the first three time periods, the IPSO-ABiLSTM prediction effect suggested in this paper is not ideal, but it is almost completely fitted in the later time periods. Overall, the fit of IPSO-ABiLSTM is still better than the other three models. The evaluation indicators of each model in different windows are presented in Table 9.

From the outcomes of various methods and their analysis, as given away in Table 9, the following fundamental conclusions can be drawn:

(1) When the window value is 2, the MAPE value of the suggested IPSO-ABiLSTM method is 0.0223, 0.1583, and 0.2278 lower than that of PSO-BiLSTM, PSO-LSTM, and BiLSTM, respectively, and the fitting coefficient R^2 is compared with the other three models. They were 0.0115, 0.1203, and 0.2277 higher, respectively. In fact, this confirms that the performance of the suggested approach is superior than the other three methods when the window value is 2.

(2) When the window value is 3, the MAPE value of the suggested IPSO-ABiLSTM approach is 0.0878, 0.0968, and 0.0533 lower than that of PSO-BiLSTM, PSO-LSTM, and BiLSTM, respectively, and the

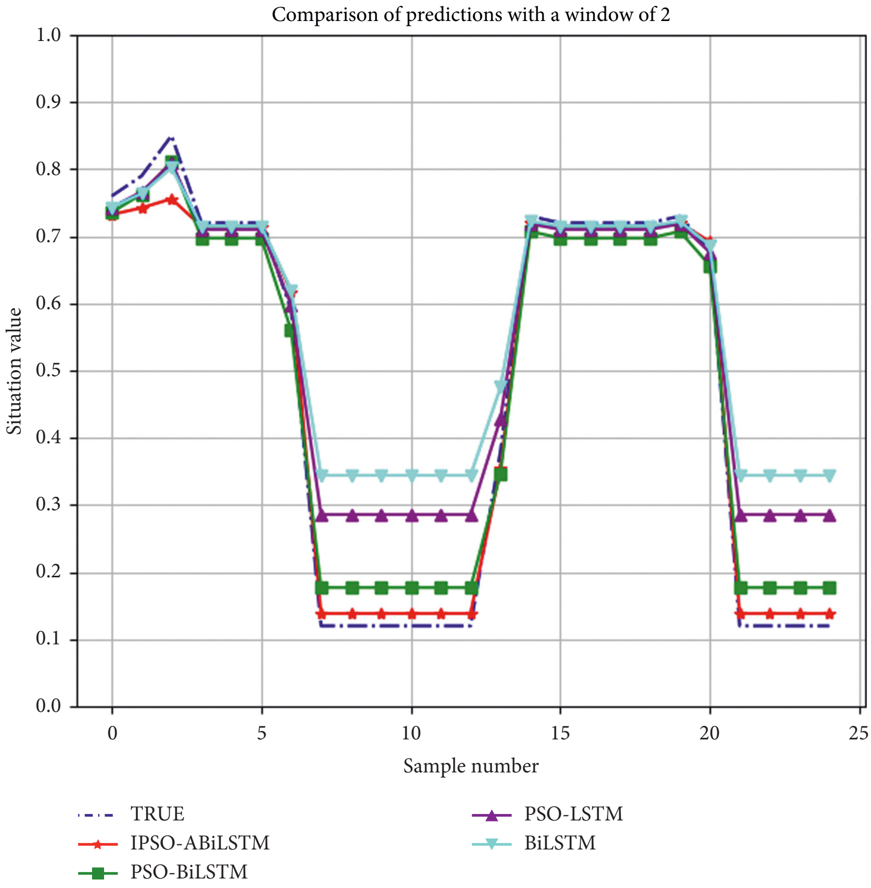

Figure 9: Comparison of window value 2.

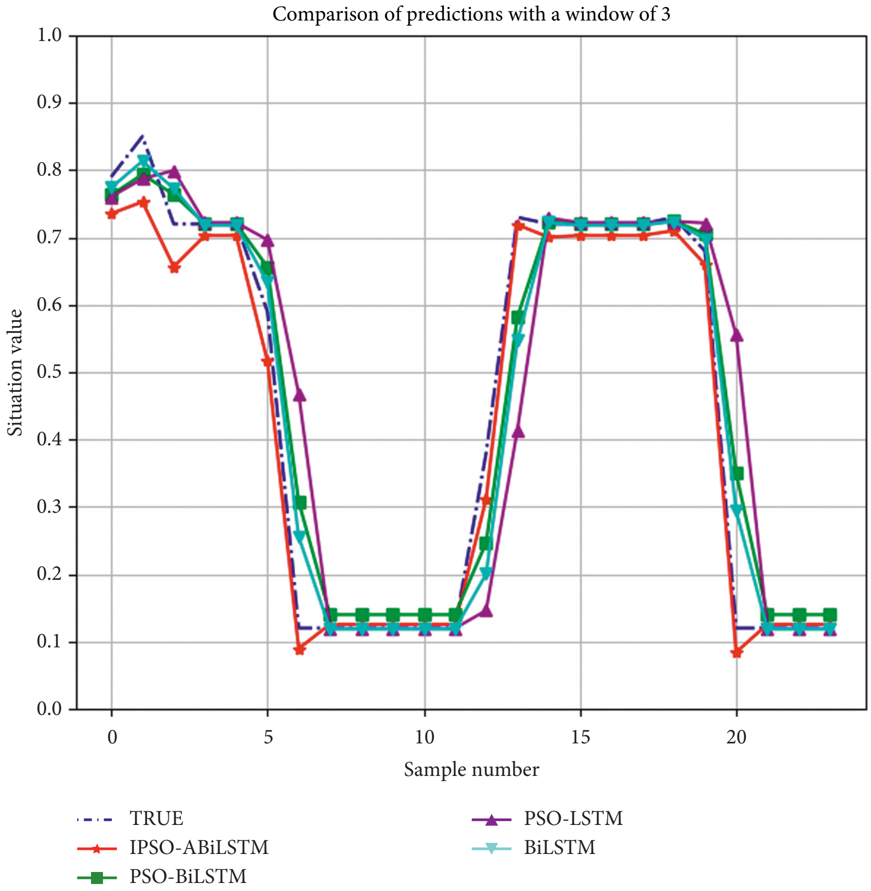

Figure 10: Comparison of window value 3.

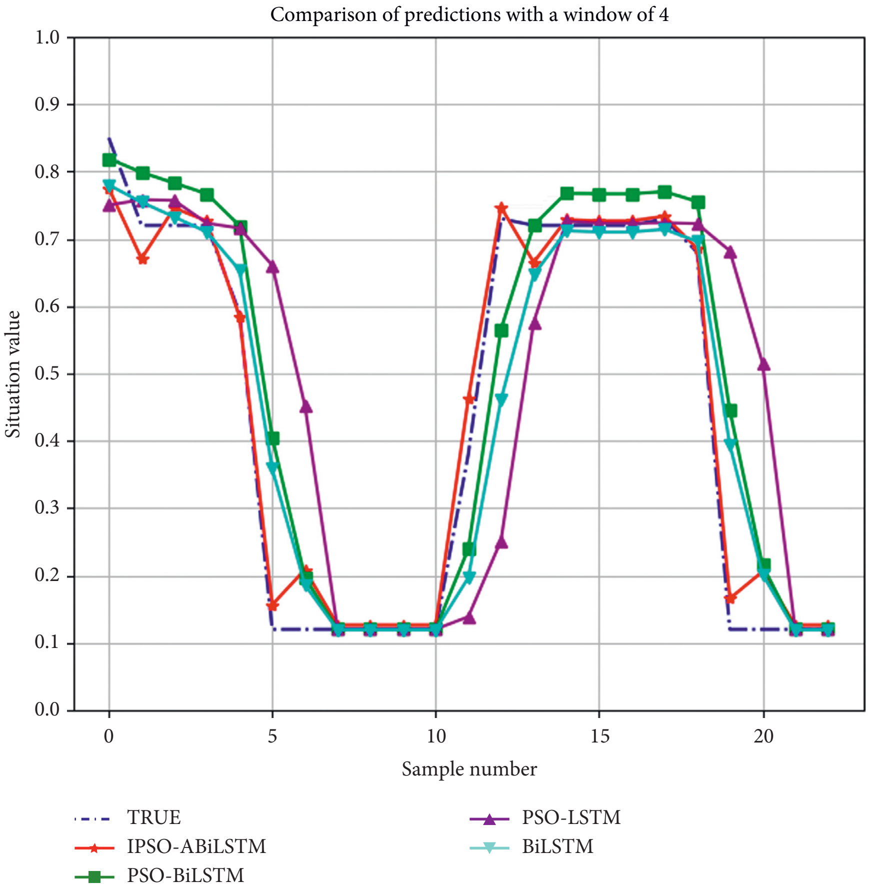

Figure 11: Comparison of window value 4.

Table 9: Assessment outcomes of evaluation indexes of each model.

Size	Index	IPSO-BiLSTM	PSO-BiLSTM	PSO-LSTM	BiLSTM
2	MAPE R^2	1.4038 0.9922	1.4261 0.9807	1.5621 0.8719	1.6316 0.7645
3	MAPE R^2	1.3712 0.9849	1.4590 0.9327	1.4680 0.7678	1.4245 0.9425
4	MAPE R^2	1.4541 0.9809	1.5728 0.8528	1.5617 0.3910	1.4328 0.8666

fitting coefficient R^2 is lower than the other three models are 0.0522, 0.2171, and 0.0424 higher, respectively. The performance of the suggested approach is superior than the other three methods when the window value is 3.

(3) When the window value is 4, the MAPE value of the suggested IPSO-ABiLSTM approach is 0.1187 and 0.1076 lower than that of PSO-BiLSTM and PSO-LSTM, respectively, and the fitting coefficient R^2 is higher than that of the other three models: 0.1281, 0.5899, and 0.1143. Combining the two indicators, the suggested method performs superior than the other three models when the window value is 4.

(4) For prediction problems, different window sizes often have an influence on the prediction outcomes. This paper also conducts comparative experiments on more window values. As far as the method in this paper is concerned, when in fact the value of the window is slighter, then the prediction effect of each model is often the better. Through the lateral analysis of (1)–(3), when the sliding window size is the same, the IPSO-BiLSTM model suggested in this paper has a higher fitting degree than the PSO-LSTM method, the PSO-BiLSTM approach, and the traditional BiLSTM approach. This should be kept in mind that, at the same time, the fitting coefficient R^2 of each model is compared longitudinally when the window value is 2, 3, and 4. As displayed in Figure 12, this can be easily comprehended and concluded that when the window value is 2, the model in this paper can accomplish the paramount fitting impact, and the fitting coefficient can be 0.9922, which is almost a complete fit. Subsequently, the above discussion and

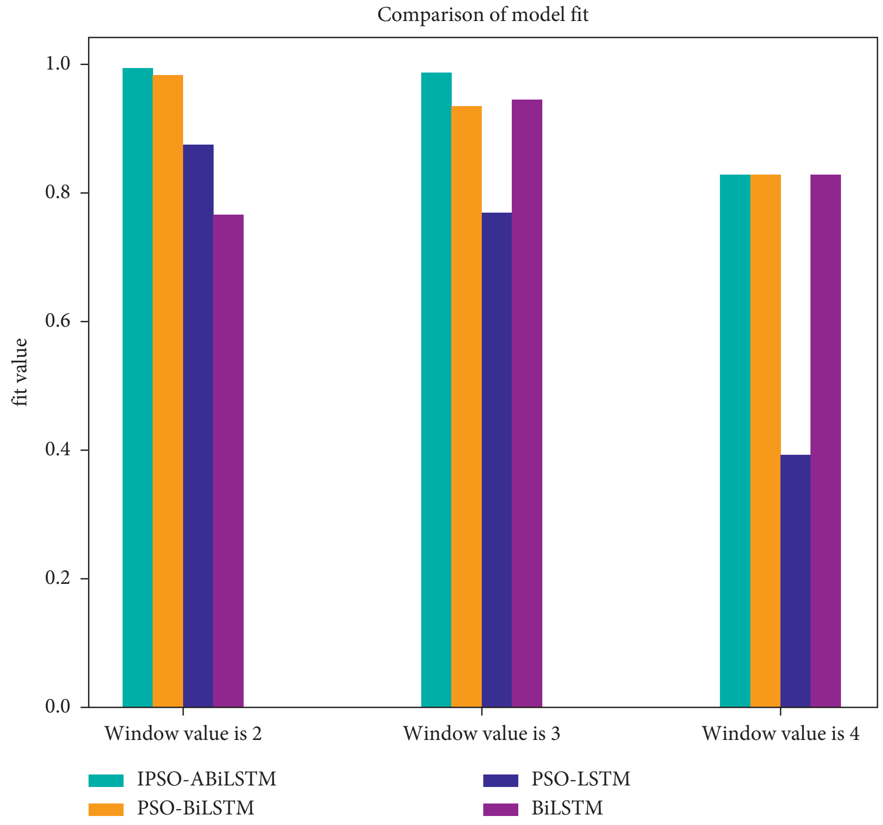

Figure 12: Comparison of model fitting degree.

analysis of the outcomes prove the efficiency of the prediction approach suggested in this paper, in particular, for the problem of network security situation prediction.

6. Conclusions and Future Work

Aiming at the problem of insufficient learning ability of a single model, in this paper, we constructed a network security position assessment and forecasting model which is established on the fusion model, and expounds the specific implementation of the fusion model. In fact, for network security condition assessment, this paper constructs two fusion models, that is, (i) CNN-LSTM-P; and (ii) CNN-LSTM-S, respectively, and conducts two-class and ten-class experiments on the UNSW-NB15 dataset. The attained outcomes illustrate that the detection effect of the CNN-LSTM fusion model is better, and the correct rate of situation assessment can reach 85.19% and 92.59%. Moreover, for network security condition forecast, we also suggest a network security condition extrapolation model which is established on the IPSO-ABiLSTM method. In the model construction, in view of the defects of slow convergence of the PSO technique and its defect of informal collapse into the local minimum, nonlinear inertia weight, and acceleration are introduced. We believe, these factors can help to improve the PSO algorithm and its immature convergence. At the same time, in order to learn more about the correlation between sequences, the BiLSTM network integrating the attention mechanism is introduced to forecast the situation, and the suggested IPSO mechanism is implemented to enhance and boost the ABiLSTM, as well as, to increase the forecasting ability of the suggested model. The investigational outcomes confirm that the IPSO-ABiLSTM model has higher fitting degree and smaller prediction error.

In the future, we will use other variants of the PSO method that have the capabilities to adaptively adjust numerous factors with the aim of the algorithm convergence can be enriched. Moreover, we will consider the Markov jumping technique in the PSO that can divide the entire populations in to substages and avoid the local optima convergence. On the hand, we will also look deeply into other deep learning models and improve the prediction accuracy. Limited resources are also considered as a fundamental issue that unswervingly distresses the training and prediction durations of the network. Therefore, we will investigate, in the future, how the big data analysis and technologies like cloud and edge infrastructure within the domain of networks will help to reduce the durations for the model training and prediction.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by National Natural Science Foundation of China, Network security situation assessment based on attack intent in big data environment (61672206), the Central Government Guides Local Science and Technology Development Projects, research on key technologies of network security situational awareness based on deep learning (216Z0701G), and S&T Program of Hebei, Research on Key Technologies of Large-Scale Network Asset Risk Monitoring System (20310701D).

References

[1] M. R. Endsley, "Design and evaluation for situation awareness enhancement," *Proceedings of the Human Factors Society annual meeting*, SAGE Publications, vol. 32, no. 2, pp. 97–101, The Johns Hopkins University Applied Physics Laboratory, Los Angeles, CA, USA, 1988.

[2] T. Bass, "Multisensor data fusion for next generation distributed intrusion detection systems," in *Proceedings of the Iris National Symposium on Sensor & Data Fusion*, pp. 24–27, 1999.

[3] H. Z. Yan, C. Z. Hu, and H. M. Tan, "Network security threat assessment based on fuzzy matrix game," *Computer Engineering and Applications*, vol. 38, no. 13, pp. 4-5+10, 2002.

[4] R. C. Zhang, Y. C. Zhang, J. Liu, and Y. D. Fan, "Network security situation prediction method using improved convolutional neural network," *Computer Engineering and Applications*, vol. 55, no. 6, pp. 86–93, 2019.

[5] Y. X. Chen, X. C. Yin, and R. Tan, "A network security situation prediction model based on GSA-SVM," *Journal of Air Force Engineering University (Natural Science Edition)*, vol. 19, no. 5, pp. 78–83, 2018.

[6] Y. C. Zhang, R. C. Zhang, and J. Liu, "Network security situation assessment using deep self-encoding networks," *Computer Engineering and Applications*, vol. 56, no. 6, pp. 92–98, 2020, in Chinese.

[7] J. H. Wang, Z. L. Shan, and H. S. Tan, "Network security situation assessment based on genetic optimization PNN neural network," *Computer Science*, vol. 48, no. 6, pp. 338–342, 2021, in Chinese.

[8] G. Xu, Y. Cao, Y. Ren, X. Li, and Z. Feng, "Network security situation awareness based on semantic ontology and user-defined rules for Internet of Things," *IEEE Access*, vol. 5, Article ID 21046, 2017.

[9] H. Zhang, C. Kang, and Y. Xiao, "Research on network security situation awareness based on the LSTM-DT model," *Sensors*, vol. 21, 2021.

[10] Z. Dai, L. Nige, Y. Guoquan, and Z. Xinijan, "Research on power mobile Internet security situation awareness model based on zero trust," in *Proceedings of the International Conference on Artificial Intelligence and Security*, July 2022.

[11] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278–2324, 1998.

[12] Z. Z. Yang, N. Kuang, and L. Fan, "Overview of image classification algorithms based on convolutional neural networks," *Signal Processing*, vol. 34, no. 12, pp. 1474–1489, 2018, in Chinese.

[13] L. L. Fan, H. W. Zhao, and H. Y. Zhao, "A review of target detection research based on deep convolutional neural networks," *Optical Precision Engineering*, vol. 28, no. 5, pp. 1152–1164, 2020, in Chinese.

[14] C. Chen and F. Qi, "Review of the development of convolutional neural network and its application in the field of computer vision," *Computer Science*, no. 3, pp. 63–73, 201946, in Chinese.

[15] Y. Bengio, P. Simard, and P. Frasconi, "Learning long-term dependencies with gradient descent is difficult," *IEEE Transactions on Neural Networks*, vol. 5, no. 2, pp. 157–166, 1994.

[16] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[17] M. Tavallaee, E. Bagheri, W. Lu, and A. G. Ali, "A detailed analysis of the KDD CUP99 data set," in *Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications*, pp. 1–6, IEEE Press, Ottawa, ON, Canada, July 2009.

[18] A. Kumarshrivas and A. Kumar Dewangan, "An ensemble model for classification of attacks with feature selection based on KDD99 and NSL-KDD data set," *International Journal of Computer Application*, vol. 99, no. 15, pp. 8–13, 2014.

[19] M. S. Al-Daweri, K. A. Zainol Ariffin, S. Abdullah, and M. F. E. Senan, "An analysis of the KDD99 and UNSW-NB15 datasets for the intrusion detection system," *Symmetry*, vol. 12, no. 10, 2020.

[20] S. Choudhary and N. Kesswani, "Analysis of KDD-cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT," *Procedia Computer Science*, vol. 167, pp. 1561–1573, 2020.

[21] B. Ameen, D. Hussain, J. Ali, and F. Hassan, "Fall event detection using the mean absolute deviated local ternary patterns and BiLSTM," *Applied Acoustics*, vol. 192, 2022.

[22] K. Xu, B. Jimmy, K. Ryan, K. Cho, C. Aaron, and Z. Rich, "Show, attend and tell: neural image caption generation with visual attention," in *Proceedings of the 32nd International Conference on Machine Learning(ICML)*, pp. 2048–2057, Lille, France, July 2015.

[23] M. Carrasco and A. Barbot, "Spatial attention alters visual appearance," *Current Opinion in Psychology*, vol. 29, pp. 56–64, 2019.

[24] L. Shi, Y. Wang, Y. Cheng, and R. B. Wei, "A review of attention mechanism research in natural language processing," *Data Analysis and Knowledge Discovery*, vol. 4, no. 5, pp. 1–14, 2020.

[25] P. Y. Gong, Y. F. Luo, Z. M. Fang, and F. Dou, "Short-term power load forecasting method based on attention-BilSTM-LSTM neural network," *Journal of Computer Applications*, vol. 41, no. S1, pp. 81–86, 2021.

[26] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proceedings of the 1995 International Conference on Neural Networks*, pp. 1942–1948, IEEE, Perth, WA, Australia, November 1995.

[27] D. Zhao and J. Liu, "Study on network security situation awareness based on particle swarm optimization algorithm," *Computers & Industrial Engineering*, vol. 125, pp. 764–775, 2018.