Construction and Analysis of QPSO-LSTM Model in Network Security Situation Prediction

Li Wentao

Zhengzhou Shuqing Medical College, Department of Health Administration, Computer teaching and research Department, Zhengzhou 45000, China
E-mail: 1239806392@qq.com

Received 15 September 2023; Accepted 16 October 2023;
Publication 09 April 2024

Abstract

The continuous improvement of artificial intelligence technology has deepened its application in many fields and provided more support for predicting network security situations. QPSO-LSTM model based on LSTM neural network and fused with QPSO algorithm provides more options for improving network security situation prediction, further enhancing the effectiveness of network security situation prediction, and enabling more efficient and accurate prediction and analysis of network security situations. By comparing the applications of different types of algorithms in network security situation prediction, it was found that the QPSO-LSTM model has smaller prediction errors, can achieve higher prediction accuracy, and can also obtain higher F_1*-score* and *AUC* values; the shorter identifying runtime also lays the foundation for improving the speed and efficiency of network security situation prediction. Therefore, in the field of network security situation prediction,

Journal of Cyber Security and Mobility, Vol. 13_3, 417–438.
doi: 10.13052/jcsm2245-1439.1334

the application of QPSO-LSTM model can provide more support for further improvement and improvement of security situation prediction performance in this field.

Keywords: Network security, QPSO algorithm, LSTM neural network, model construction, situation prediction.

1 Introduction

Continuous updating and development of artificial intelligence technology has brought significant changes to modern society for technologies and services such as instant messaging, virtual economy, online social networking, and the Internet of Things. The network has been integrated into various aspects of daily life. The internet has promoted cultural exchange and knowledge popularization, promoting the deep integration of various fields such as online education, entrepreneurship, healthcare, shopping, finance, and modern life. It has become an indispensable support for economic and modern technological development [1, 2]. The Internet not only promotes technological progress, but also hides enormous risks. More and more network security issues have attracted more attention. The emergence of security risks not only leaks personal privacy information and commercial operation secrets, but also may lead to the loss of national interests in severe cases. Therefore, network security not only affects the interests of individuals and enterprises, but also relates to the stability and development of national politics, economy, and national defence security. Timely and efficient detection of hidden dangers in network security, prediction and analysis of security situations, and the construction of a more secure network communication system are severe and urgent challenges that need to be solved. They are also one of the important issues that must be faced and solved in the current artificial intelligence society [3, 4].

In the complex and ever-changing network security environment, perceiving and predicting network security status from a macro perspective has become an important technical link in the field of Network Security Situation Awareness. For network security situational awareness technology, the acquisition of situational elements, situational assessment, and situational prediction are important key links in the research field of this technology. Network security situational awareness technology can integrate internal and external network environment information, and conduct comprehensive analysis and evaluation of the collected relevant information [5]. By conducting situational assessment on the results obtained from fusion calculations, it is possible to provide a more comprehensive analysis of network security situational information while ensuring accuracy. Finally, it can also predict the future cybersecurity situation based on past cybersecurity situations and the current state of cybersecurity situation information [6, 7]. At present, the prediction of network security situations still faces the problem of relatively low recognition efficiency and accuracy values. Further improving the efficiency of network security situation recognition and the accuracy of prediction is still an important aspect that needs to be studied. In the process of continuous development and improvement of modern artificial intelligence technology, LSTM neural network, as an improvement of RNN neural network, can improve the efficiency of feature recognition in network security situation prediction, further improve the accuracy of model prediction, and lay the foundation for the evaluation of network security situation [8, 9].

The performance in time series data processing is a significant advantage of RNN, and LSTM neural networks overcome the long-term dependence and easy forgetting problems that exist in RNN. Therefore, LSTM is more suitable for processing network security situation data. However, although the LSTM neural network has good processing ability for time series data, the algorithm involves many parameters during model training, and the selection of the number of hidden layer nodes and batch size has a certain degree of subjectivity [10]. Moreover, multiple adjustments are needed to train the model based on the number of neural elements and batch size. The model obtained through training may still have a certain performance gap with the optimal model. Therefore, it is necessary to improve and enhance the LSTM neural network to further enhance its performance in network security situation prediction.

As a basic theoretical algorithm for network security situation prediction, Particle Swarm Optimization (PSO) is an intelligent optimization algorithm based on Swarm Intelligence. This algorithm assumes that there are *N* birds in the forest, and there are several unknown positions of food. The bird swarm searches for food by transmitting information about the location of the found food until it finds the optimal food location in the forest. Treat each bird as a particle, and each particle adjusts its flight strategy and position based on its own and group optimal position information until it finds the global optimal position. Compared with other intelligent optimization algorithms, the main characteristics of particle swarm optimization algorithm are wide search range and fast convergence speed [11, 12]. The quantum particle swarm optimization algorithm (QPSO) formed by further improving the particle swarm optimization algorithm has further improved and strengthened its global search ability compared to traditional PSO algorithms, which can better eliminate subjective factors in parameter selection of LSTM neural networks. Therefore, this article uses QPSO algorithm to find the number of hidden layer nodes and batch size of LSTM networks. Among them, the mean square error is used as the fitness function of the algorithm [13].

Based on the above analysis and considering the temporal nature of network security situation values, this paper selects the LSTM neural network, which is good at processing temporal data, to predict and analyse network security situation values. In addition, due to the difficulty in determining hyperparameters and being prone to falling into local minima in LSTM neural networks, this paper further introduces the QPSO algorithm with global search ability to search for relevant parameters of LSTM neural networks, and establishes a QPSO-LSTM network security situation prediction model [14, 15].

2 Prediction of Network Security Situation in Artificial Intelligence

2.1 Application Status of Artificial Intelligence in Network Security Prediction

The application of artificial intelligence technology in predicting and analysing network security situations is mainly reflected in its ability to continuously improve system performance through computational means and the use of experience. For a given set of data, machine learning in artificial intelligence generates a model composed of several rules by calculating and analysing the internal laws of the data. When facing new data, corresponding judgments can be made based on the already constructed model. Artificial intelligence can construct deep neural network models by imitating biological neural mechanisms, which have stronger representation capabilities for the internal connections of raw data. Therefore, applying such learning algorithms to network security situation prediction systems, utilizing a large amount of recorded connected data, and using deep learning algorithms in artificial intelligence for computational learning, can construct a detection model with better performance, which can better judge the threats to network security and achieve prediction and analysis of security situations [16–18]. Therefore, in the face of a large amount of network security data, constructing a suitable and efficient security situation prediction model to timely and

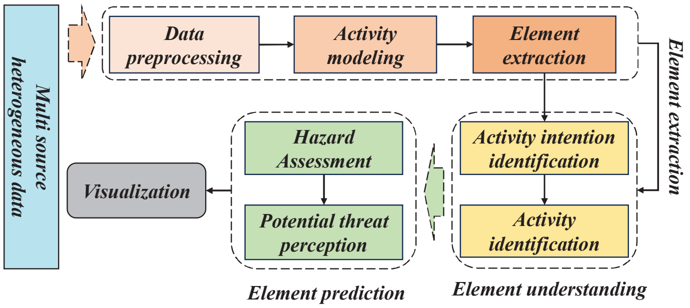


Figure 1 Logic diagram of network security situation prediction model.

accurately detect security attacks is a key research link in network security situation prediction technology. In the analysis process of network security situation, core links such as element extraction, element understanding, and element prediction are involved, ultimately achieving visualization of security situation prediction. As shown in Figure 1, a basic model for predicting and perceiving network security situations is presented.

Through the above analysis, it can be found that LSTM neural network technology can significantly improve recognition efficiency and relatively low prediction accuracy in predicting and analysing network security situations, improve the overall prediction performance of the model, and provide more guidance for network security. Combining the performance advantages of LSTM neural networks, the QPSO algorithm is introduced to further improve the shortcomings of the model’s large number of parameters during training and the strong subjectivity of related parameter processing. The constructed QPSO-LSTM algorithm model can further improve and enhance its performance, providing more efficient support for network security situation analysis and prediction in the context of continuous updates in modern science and technology.

2.2 Theory of LSTM Neural Networks

Long Short Term Memory neural network is a variant of RNN. LSTM solves the problems of weak processing of medium to long sequence data, easy gradient vanishing, and explosion in RNN, and is more suitable for processing long delay and long interval time series data [19]. The LSTM neural network can effectively filter out useful new information for memory while maintaining long-term information of sequence data, discarding redundant old information, making LSTM more efficient in processing various long

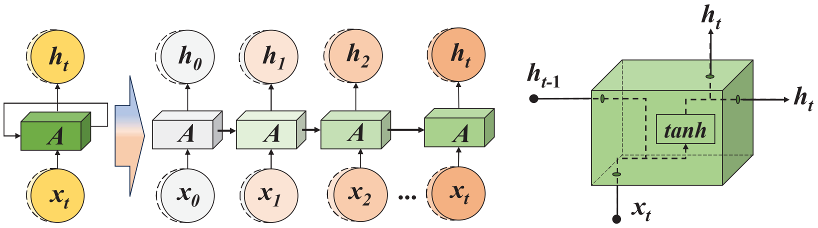


Figure 2 Internal and expanded structure of RNN neural network.

and short sequence data information. For the internal structure of a standard RNN neural network, it usually only has a simple tanh layer, with each node having two input values, one of which is the current input value and the other is based on the value obtained from the previous node; Each node also has two outputs, one for outputting the result and the other for the input of the next node, which are essentially the same value [20]. LSTM has a similar chain structure to traditional RNN, but there are significant differences in the internal unit structure. As shown in Figure 2, a logical schematic diagram of the internal deployment structure of the RNN neural network is provided.

In RNN neural networks, the output at time t is the value O_t, while the input value at time t is x_t, and h_t represents the hidden layer state at time t. From the unfolding diagram, it can be seen that recurrent neural networks are different from general multi-layer feedforward neural networks, as they share parameters in different parts of the network model.

Based on the basic starting point of filtering important information and avoiding unimportant information, the LSTM neural network uses memory blocks to lock in important information, without relying on all memory information to avoid gradient explosion phenomenon. Each memory block is composed of one or more self connected memory cells, with a single memory cell composed of three multiplication control units. These gate control units provide functions similar to read, write, and reset. LSTM has one more input and one more output compared to RNN. The two additional values are the input and output values of the cell state of the memory and forgetting mechanism of LSTM, which is usually represented by *C*. The cell state can determine the storage and deletion of relevant data during specific network information processing [21, 22]. The emergence of cell states not only effectively avoids the problem of gradient vanishing in RNN neural networks, but also avoids the gradient explosion problem that often occurs in models. As shown in Figure 3, the basic logic diagram of the LSTM neural network is presented in conjunction with its internal structure.

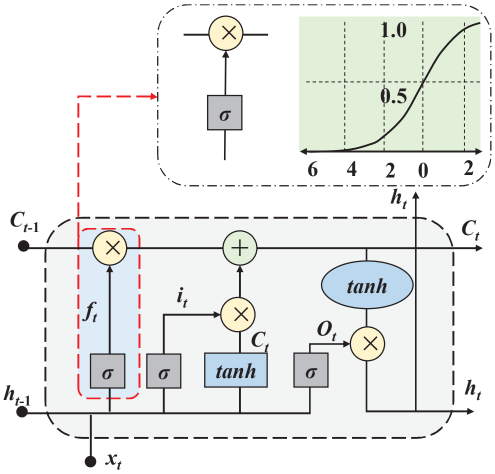


Figure 3 Internal structure logic diagram of LSTM neural network.

In addition to external loops, the LSTM neural network adds cell state units internally to store long-term state information, with state units represented by s_i^t. In this neural network, the sigmoid function is used to control the forgetting gate. Based on the output from the previous time and the input from the current time, a numerical value is generated, ranging from 0 to 1, to determine whether to let the information learned from the previous time pass. The forgetting gate F_i^t of cell i at time t is shown in Formula (1):

$$F_i^t = sigmoid\left(\sum_j U_{i,j}^f \cdot x_j^t + \sum_j W_{i,j}^f \cdot h_j^t + b_i^f\right) \tag{1}$$

where, x_t is the input vector at time t, h_t is the hidden layer state vector at time t. U^f, W^f, and b^f represent the input weight, the cyclic weight of the forgetting gate, and the bias, respectively. The input gate G_i^t also uses the sigmoid function to generate a value between 0 and 1, which determines the data used to update information, as shown in Formula (2):

$$G_i^t = sigmoid\left(\sum_j U_{i,j}^g \cdot x_j^t + \sum_j W_{i,j}^g \cdot h_j^t + b_i^g\right) \tag{2}$$

Among them, the input weight, the loop weight of the input gate, and the offset are U^g, W^g, and b^g, respectively. The update method for the internal state of cells obtained from the input gate and forgetting gate is s_i^t, as shown in Formula (3):

$$s_i^t = s_i^{t-1} \cdot F_i^t + G_i^t \cdot sigmoid\left(\sum_j U_{i,j} \cdot x_j^t + \sum_j W_{i,j} \cdot h_j^{t-1} + b_i\right) \quad (3)$$

Among them, U, W, and b represent the input weight, cycle weight, and bias of the cell, respectively. Based on this, the output h_i^t of the hidden layer controlled by the output gate is shown in Formula (4):

$$h_i^t = tanh(s_i^t) \cdot sigmoid\left(\sum_j U_{i,j}^o \cdot x_j^t + \sum_j W_{i,j}^o \cdot h_j^{t-1} + b_i^o\right) \quad (4)$$

The backpropagation process of LSTM neural network is roughly the same as that of RNN, except that LSTM has additional cell units that store memory information. Therefore, LSTM has more parameters compared to RNN, and the calculation of gradients is also more complex. In each iteration, adjusting the parameters of the neural network requires more time [23, 24].

3 Construction of QPSO-LSTM Model in Network Security Situation Prediction

3.1 Model Architecture of QPSO-LSTM

Based on the above analysis of QPSO algorithm and LSTM neural network, it can be found that the introduction of QPSO algorithm can improve the recognition efficiency and accuracy of LSTM neural network models. In the QPSO-LSTM algorithm model, each particle in the population has a memory function, which can remember the optimal position (p_{best}) of the individual it has searched for, and each particle can determine the global optimal position (g_{best}) of the entire population. Particles adjust their forward speed and position through p_{best} and g_{best}. For the update and change of particle velocity of i in the *D-th* dimension, Formula (5) can be used to provide [25]:

$$v_{id}^k = w \cdot v_{id}^{k-1} + c_1 \cdot r_1(p_{best\text{-}id} - x_{id}^{k-1}) + c_2 \cdot r_2(g_{best\text{-}id} - x_{id}^{k-1}) \quad (5)$$

In addition, the position update of particle i in the *D-th* dimension can be described by Formula (6):

$$x_{id}^k = x_{id}^{k-1} + v_{id}^{k-1} \quad (6)$$

Therefore, this article combines the advantages of the QPSO algorithm to improve the model in network security situation prediction. It is considered that every particle has a quantum state, which is an important quantum idea in the QPSO algorithm. The position where particles appear in the search space has arbitrariness, and the probability of their occurrence at a certain position is determined by a distributed function [26, 27]. In the implementation of specific algorithms, the particle positions at the $t + 1$ iteration are derived during the t iteration. As shown in Formula (7), combined with the update of particle positions in the QPSO-LSTM model, the specific description of particle positions is given:

$$M_{best} = \frac{1}{m}\sum_{i=1}^{m} p_{best-i} \tag{7}$$

In this algorithm, $p_{best-i}$is the local optimal value of the *i-th* particle in the current iteration process, which can be described by Formula (8):

$$p_{best-i} = \frac{1}{\varphi}[p_i - (1-\varphi)p_{gest}] \tag{8}$$

Among them, p_{gest} represents the current global optimal solution of the population; φ represents a uniformly distributed numerical value on (0,1).

In addition, for the position X_i of the *i-th* particle in the current iteration and the position $X_i + 1$ of the i-th particle in the next iteration, Formula (9) can be used to calculate:

$$X_{i+1} = p_i \pm \lambda |M_{best} - X_i| ln\left(\frac{1}{\mu}\right) \tag{9}$$

Among them, λ It is the only control parameter in the QPSO algorithm model, representing the innovation coefficient; μ Represents a uniformly distributed numerical value on (0,1).

3.2 Construction of QPSO-LSTM Model in Network Security Situation Prediction

3.2.1 Identification and extraction of internet security situation features

In complex environments, the Internet may face potential security risks due to the intrusion of unsafe factors, which in turn pose a threat to the overall security situation of the network. At this time, the characteristic distribution of the information flow invaded by unsafe factors on the *n-th* terminal of the Internet can be described in detail. Set the distribution variables of the Internet under the influence of external factors to be labelled as $(x_1, x_2, \ldots, x_m)$, where m represents the dimension. Therefore, the characteristic state distribution of interference factors in security situation prediction is described in Formula (10):

$$\begin{cases} v_s = \left\| X_s - \sum_{i=1}^{m} \omega_i (1 - X_s) \right\| \\ \omega_s = \sum_{i=1}^{m} v_s + \sum_{j=1}^{m} V_m + \zeta \end{cases} \tag{10}$$

Among them, vs represents the mutated behaviour of the internet after being invaded by security hazards; X_s represents the difference value; The i here represents the coefficient; ω_i represents deviation; ζ Represents a constant; V_m represents the intrusion status of security hazards in network security situation prediction.

At this point, the conditional transition probability of network security situational threats is described by Formula (11):

$$P = C - n \sum_{j=1}^{m} \log \sigma_s - \sum_{s=1}^{m} \sum_{i=1}^{m} (\omega_s - r_t)^2 / 2\sigma_s \tag{11}$$

Among them, P represents the conditional transition probability; C represents the threat invasion immune constant; σ_s represents the state vector for collecting network security situation data; r_t represents deviation.

Based on internet security threat intrusion immune control models established in different fields, the model is used to recombine network attack features and obtain the iterative function of network attack feature distribution space, as shown in Formula (12):

$$\theta_1(k+1) = \theta_1(k) - \varepsilon E(y_k + k) \tag{12}$$

Among them, $\theta_1(k)$ represents the initial state vector of the network after being threatened; y_k represents the coordinate axis; k represents a threat attack in the network.

In order to achieve the recognition and extraction process of internet security situation features, the collected security situation signal is set as $x(k) = s(k) + w(k)$, and this equation expression represents a quasi-stationary random signal. Use the established model to obtain the threat index of network security situation, and define it using Formula (13) [28]. At the same time, the security situation index of network security being threatened can be further obtained, as shown in Formula (14).

$$\begin{cases} x_k = f(x_{k-1}) + v_k \\ y_k = h(x_k) + e_k \end{cases} \tag{13}$$

$$p(\omega_k) = t_{v_k}\left(\vec{u}_k, \sum k\right) = \frac{\Gamma v_k}{2} + v_k \pi \tag{14}$$

Among them, $p(\omega_k)$ indicates the situation index; $\vec{u}_k$ represents the state vector; Σk represents a variable; $\frac{\Gamma v_k}{2} + v_k \pi$ represents the Sigma function; t_{v_k} represents the acquisition time of the state vector.

Based on the analysis process of QPSO-LSTM model for network security situation feature recognition and extraction, it can be concluded that using unsupervised layer by layer pre training method can obtain IoT security situation features, and then iteratively train them. After the training is completed, all networks are stacked together, and under supervised learning, labeled security situation data is used to fine tune network parameters, thus completing the training of network security situation. By analysing the training results to determine the fluctuation of the network security situation, the final identification results are obtained, and the design of the automatic identification algorithm for the network security situation is achieved.

3.2.2 Security Situation Prediction Process Based on QPSO-LSTM

The main processes involved in the QPSO-LSTM situation prediction model process include data processing, sample set reconstruction, initialization of QPSO parameters, model training and prediction [29]. Firstly, data processing: The distribution range of network security situational values is relatively large, which has a significant impact on the training and decision-making speed of LSTM network models. To eliminate the impact of situational data range, the data is normalized. Next is sample set reconstruction: convert one-dimensional network security situation data into multidimensional data, use sliding time windows to construct the sample set, use data from the past 5 time periods to predict data from the next period, set the sliding time window to 6, and slide one data backward each time. In addition, the reconstructed samples need to be divided into a training set and a testing set, respectively, for model training and testing [30]. Then, for initializing the

QPSO parameters, it is necessary to initialize the quantum particle swarm parameters, including the number of iterations, population size, innovation coefficient, etc., and optimize the QPSO based on the number of neural units in the first and second hidden layers of the LSTM neural network, as well as the batch size.

In addition, the training process of the model is achieved by inputting the training set into the neural network, and an optimizer is used in iterative learning to optimize the network parameters of LSTM. The algorithm updates the local and global optimal positions of particles based on the size of the fitness value. The criterion for terminating the algorithm is to find the global optimal position of the particles or to reach the maximum number of iterations in the calculation process, thereby obtaining the optimal LSTM model [31]. Finally, for QPSO-LSTM model prediction, the optimal LSTM model obtained is used to input the test set into the trained model, in order to achieve prediction and analysis of network security situation values. As shown in Figure 4, the QPSO-LSTM model security situation prediction flowchart is provided.

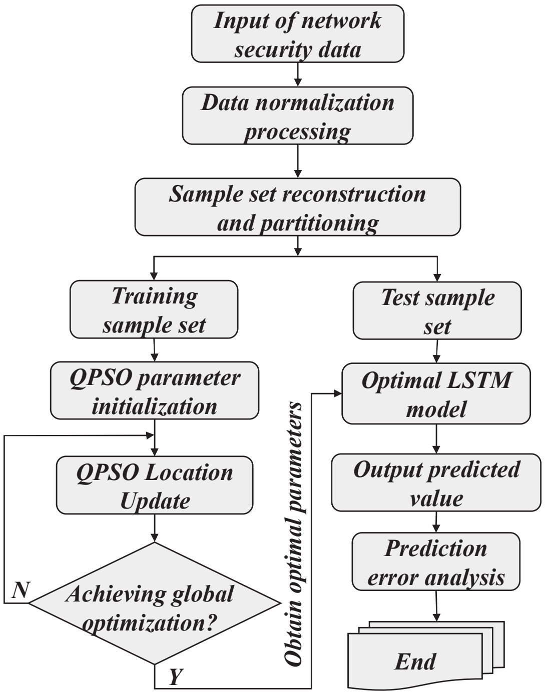

Input of network security data
Data normalization processing
Sample set reconstruction and partitioning
Training sample set
Test sample set
QPSO parameter initialization
QPSO Location Update
Achieving global optimization?
N
Y
Obtain optimal parameters
Optimal LSTM model
Output predicted value
Prediction error analysis
End

Figure 4 Flow chart of QPSO-LSTM model security situation prediction.

4 Model Experiment and Result Analysis

4.1 Model Evaluation Indicators

To analyse and study the predictive ability of the QPSO-LSTM model more clearly, it is necessary to determine relevant evaluation indicators to quantitatively analyse the predictive effect of the model. At the same time, while verifying the overall effectiveness of the QPSO-LSTM model in network security situation prediction, this article compared experimental data with other algorithms and the QPSO-LSTM model. The mean absolute error (MAE) of the selected evaluation indicators is shown in Formula (15):

$$MAE = \frac{1}{n}\sum_{i=1}^{n} |y_i - \hat{y}_i| \tag{15}$$

The calculation of Mean Square Error (MSE) is shown in Formula (16):

$$MSE = \frac{1}{n}\sum_{i=1}^{n} (y_i - \hat{y}_i)^2 \tag{16}$$

In addition, as shown in Formula (17), the calculation process of Root Mean Square Error (RMSE) is given:

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n} (y_i - \hat{y}_i)^2} \tag{17}$$

For the above three evaluation indicators, the smaller the calculation result, the higher the consistency between the true value and the predicted value of the model, indicating that the model has better predictive ability.

In the experiment, precision, recall, and F_1-*score* were used to comprehensively evaluate the performance of the QPSO-LSTM algorithm model. In addition, a comparative analysis was conducted on the runtime, *ROC* curve, and *AUC* value of vulnerability identification for different algorithms. The calculation of *accuracy*, *recall*, and F_1-*score* is given by Formula (18):

$$\begin{cases} Precision = \dfrac{TP}{TP + FP} \\ Recall = \dfrac{TP}{TP + FN} \\ F_{1\text{-}score} = \dfrac{2 \times P \times R}{P + R} \end{cases} \tag{18}$$

In the above formula, *TP* represents the number of samples divided into positive classes, *FP* represents the number of samples divided into positive classes for negative classes, *FN* represents the number of samples divided into negative classes for positive classes, $TP + FP$ represents the actual number of samples classified, and $TP + FN$ represents the expected number of samples.

The accuracy of QPSO-LSTM model prediction can be determined by combining *TP*, *TN*, *FP*, and *FN*, as shown in Formula (19), which provides the accuracy of the model:

$$Ac = \frac{TP + TN}{TP + FP + TN + FN} \tag{19}$$

4.2 Data Normalization Processing

Due to the different ranges of values for continuous numerical features, some values in each data may differ significantly. To prevent attributes with large values from affecting the final classification results, it is necessary to unify the basic measurement units of the data and normalize the matrixed data. In this article, the *Min-Max* processing method is used to perform linear transformations on the data and map the results between [0,1]. The specific data normalization method is shown in Formula (20):

$$x_i' = \frac{x_i - x_{min}}{x_{max} - x_{min}} \tag{20}$$

Among them, x_i and x_i' represent the original and normalized network security situation values, respectively; x_{min} and x_{max} represent the minimum and maximum values of network security situational values, respectively.

After normalizing each sample data according to its features, the maximum and minimum values are taken on each feature, and the corresponding values are obtained using the normalization formula. Since most of the training of classifiers involves calculating the distance between samples, normalization processing can make the contribution of each feature to the results the same, improving the accuracy of the classification model.

4.3 Analysis of Model Testing Results

During the model testing process, the dataset used for situation prediction is the top 10% of the KDD99 dataset. According to the situation value calculation method, a network security situation value is generated for every 1000 pieces of data, resulting in a total of 500 situation values. The visualization

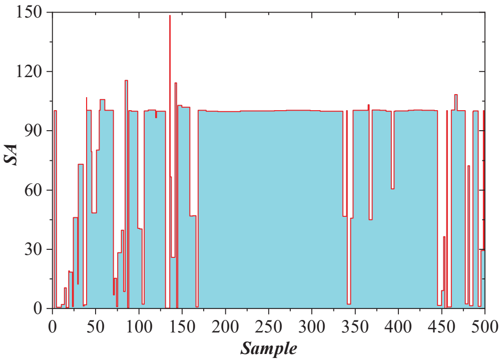


Figure 5 Flow chart of QPSO-LSTM model security situation prediction.

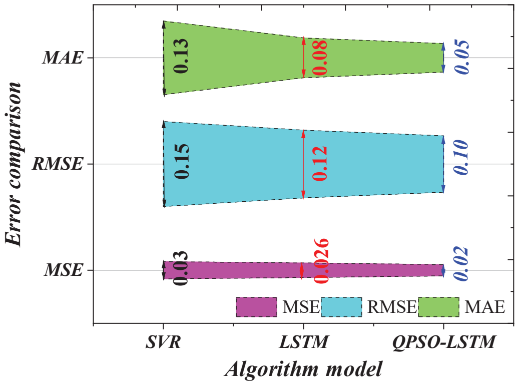
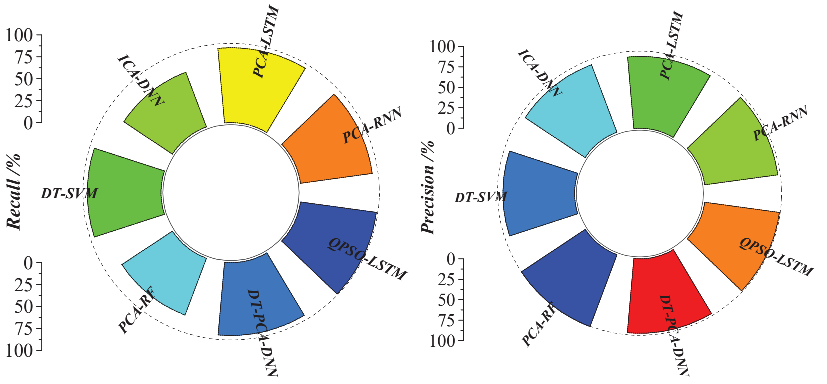


Figure 6 Comparison of prediction errors between different algorithm models.

of situational values is shown in Figure 5, where *SA* represents situational values. The larger the value, the higher the risk faced by the network during the current time period.

Based on the processing of the above data, combined with the processing performance of SVR and LSTM neural network models, as shown in Figure 6, a comparative analysis of errors between three different models, SVR, LSTM, and QPSO-LSTM, is presented. As shown in the figure, the QPSO-LSTM model has lower values than the SVR and LSTM models in all three evaluation indicators. From the specific prediction model error values in the table, it can be calculated that the QPSO-LSTM model reduces the MSE evaluation index by 61.5% and 28.5% compared to SVR and LSTM, decreases the RMSE evaluation index by 33.3% and 16.7%, and decreases the MAE evaluation index by 33.3% and 23.1%, respectively. Because the



a) Recall Rate of Different Algorithms

b) Precision of Different Algorithms

Figure 7 Comparison of prediction performance of different algorithm models.

smaller the evaluation index value of the model, the better the prediction effect of the model. Therefore, overall, the SVR model has the worst prediction effect, the LSTM model has the moderate prediction effect, and the QPSO-LSTM model has the best prediction effect. This further reflects the advantages of the QPSO-LSTM prediction model constructed in this article.

Recall and accuracy of different models in network security situation prediction are also important performance parameters of the model. As shown in Figure 7, a comparative analysis of the recall and accuracy of different model algorithms is presented. From the figure, among the seven different models compared, the QPSO-LSTM model has a recall rate of 87.5%, which is 20.8% higher than the lowest value ICA-DNN model of 66.7%. In addition, for the accuracy of the prediction model, the QPSO-LSTM model is 92.27%. Among the seven models compared, the difference of 92.63% compared to the PCA-RF model is 0.36%, indicating that the performance of the two models is basically consistent in the accuracy dimension. Therefore, through comparison, it can be found that the algorithm constructed in this article has relatively more obvious comprehensive advantages in indicators such as recall rate and prediction accuracy.

F_1*-score* is a comprehensive evaluation of accuracy and recall, reflecting the overall performance of the classification model. As shown in Table 1, the F_1*-score* comparison of different models is presented. Based on the analysis of the recall rate and F_1*-score* of the model, it can be concluded that the F_1*-score* of the QPSO-LSTM model is 88.35, which is 0.5 higher than the PCA-RNN model and has greater advantages compared to other models.

Table 1 Comparison of F_1-*score* of different models

Algorithm Model	F_1-*score*
QPSO-LSTM	88.35
PCA-RNN	87.85
PCA-LSTM	83.47
DT-PCA-DNN	83.47
DT-SVM	82.64
PCA-RF	81.21
ICA-DNN	75.40

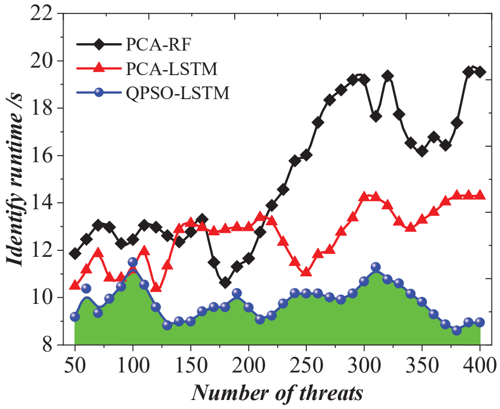


Figure 8 Identifying runtime tests.

Therefore, from the comprehensive analysis of the recall rate and F_1-*score*, the F_1-*score* of the QPSO LSTM model has more significant advantages compared to other algorithms.

In addition, the identifying runtime of PCA-RF and PCA-LSTM models was compared and analysed with the model constructed in this paper. As shown in Figure 8, a comparison of the identifying runtime of the three models is presented. Taking the threat count of 300 as an example, the identifying runtime of the PCA-RF model is about 19 s, the automatic identifying runtime of the PCA-LSTM algorithm security situation is about 14 s, and the network security situation identifying runtime of the QPSO-LSTM algorithm is about 8 s, which is reduced by 11 s and 6 s compared to the previous two models, respectively. Therefore, the QPSO-LSTM algorithm constructed in this article has the advantage of short automatic identification time in the process of network security situation prediction, ensuring higher recognition efficiency.

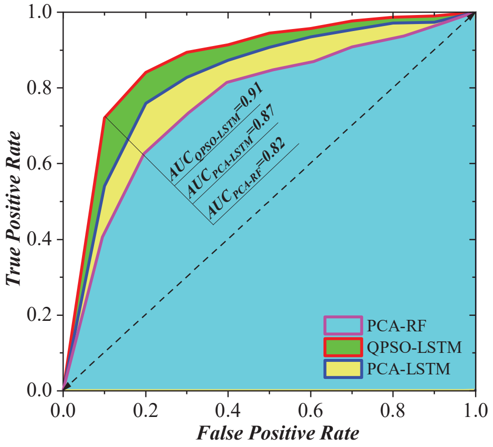


Figure 9 Comparative analysis of *ROC* and *AUC* of different algorithms.

For network security situation prediction, the *ROC* curves and *AUC* values of different models can also reflect the performance of the model, and this indicator is also independent of whether the samples are balanced. For the *ROC* curve, the abscissa represents the false positive rate FPR and the ordinate represents the true rate TPR. A good classification model should be as close to the upper left corner of the *ROC* graph as possible. A randomly guessed model *ROC* should be on the diagonal, with an *AUC* value of 0.5.

In order to further analyse the performance characteristics of the QPSO-LSTM model, as shown in Figure 9, the *ROC* curves and *AUC* values of the PCA-RF, PCA-LSTM, and QPSO-LSTM models were compared. From the figure, the *ROC* curve of the QPSO-LSTM model shows that it has relatively better predictive performance; At the same time, the highest *AUC* value of the model is 0.91, followed by PCA-RF with an *AUC* value of approximately 0.87, and the lowest is PCA-RF with an *AUC* value of approximately 0.82.

In summary, in the prediction of network security situation, the QPSO-LSTM model has shown good performance advantages in the analysis and evaluation of main relevant indicators, especially in terms of prediction error, vulnerability identification time, and *AUC* value, which are higher than other methods. Therefore, the QPSO-LSTM model constructed in this article can provide more reliable prediction results for network security situation prediction, while also achieving shorter prediction time, ensuring the efficiency of security situation prediction, and providing important support for comprehensive analysis of network security situation.

5 Conclusions

The continuous progress of artificial intelligence has promoted the continuous updating and improvement of network security situation prediction technology, laying a technical foundation for the detection and analysis of network security hazards. Based on the application of LSTM network model in network security situation prediction, this paper constructs a QPSO-LSTM network security situation prediction model using QPSO algorithm. Further comparative research is conducted on the basic performance parameters of the model, such as prediction error, identifying runtime, accuracy, and F_1-*score*. The application advantages of the model in the field of network security situation prediction are summarized. The main conclusions obtained are as follows:

(1) Combining the QPSO algorithm, the QPSO-LSTM network security situation prediction model constructed can achieve better overall performance compared to other models, effectively improving the problems of more training parameters and subjectivity in selecting relevant data in existing models, and achieving further improvement in prediction performance. By improving the QPSO-LSTM model, the prediction error in network security situation prediction is relatively low; Its recall rate is 87.5%, which is 20.8% higher than the lowest value ICA-DNN model of 66.7%, and the accuracy of the prediction model reaches 92.27%.

(2) In the comparison of running recognition time, when the number of threats is 300, the QPSO-LSTM model recognition run time is about 8 s. For PCA-RF and PCA-LSTM models, the recognition run time is reduced by 11 s and 6 s respectively, ensuring higher recognition efficiency. The F_1-*score* and *AUC* values of the model constructed in this article are 88.35 and 0.91, respectively, which are significantly improved compared to existing models and demonstrate more advantageous comprehensive prediction performance. This provides support for comprehensive prediction and analysis of network security situations.

References

[1] Li X. Research on the Impact of Internet Economy on International Economics and Trade[J]. Information Systems and Economics, 2022, 3(3):124–139.

[2] Dongmei L, Jie C, Zilong Y, et al. Prediction Methods for Energy Internet Security Situation Based on Hybrid Neural Network[J]. IOP Conference Series: Earth and Environmental Science, 2021, 645(1): 12–26.

[3] Hongwu Z, Kai K, Wei B. Hierarchical network security situation awareness data fusion method in cloud computing environment[J]. Journal of Computational Methods in Sciences and Engineering, 2023, 23(1):237–251.

[4] Zhicheng W, Longxin Z, Qinlan W, et al. A Network Security Situation Awareness Method Based on GRU in Big Data Environment[J]. International Journal of Pattern Recognition and Artificial Intelligence, 2023, 37(1):126–138.

[5] Zhang L, Liu Y. Network Security Prediction and Situational Assessment Using Neural Network-based Method[J]. Journal of Cyber Security and Mobility, 2023, 12(04), 547–568.

[6] Ying Z, Guodong Z, Roobaea A, et al. Research on data mining method of network security situation awareness based on cloud computing[J]. Journal of Intelligent Systems, 2022, 31(1):520–531.

[7] Guanling Z, Lisheng H, Lu L, et al. Prediction of Industrial Network Security Situation Based on Noise Reduction Using EMD[J]. Mobile Information Systems, 2022.

[8] Xue X, Zheng Y, Lu C. Wireless Network Safety Status Prediction Based on Fuzzy Logic. Journal of Cyber Security and Mobility[J], 2023, 12(04), 589–604.

[9] Li, X. Construction of a Smart City Network Information Security Evaluation Model Based on GRA-BPNN. Journal of Cyber Security and Mobility[J]. 2023, 11(06), 755–776.

[10] Pooja T, Purohit S. Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security[J]. Global Transitions Proceedings, 2021, 2(2):448–454.

[11] Priyanka J, Ramakrishnan M. Security Establishment in Cybersecurity Environment Using PSO Based Optimization[J]. Wireless Personal Communications, 2023, 129(3):1807–1828.

[12] Oluwaseun R O, Bamidele J A, Peter S, et al. An Enhanced Intrusion Detection System using Particle Swarm Optimization Feature Extraction Technique[J]. Procedia Computer Science, 2021, 193(1):504–512.

[13] Pavani M, Rao T P. Adaptive PSO with optimised firefly algorithms for secure cluster-based routing in wireless sensor networks[J]. IET Wireless Sensor Systems, 2019, 9(5):274–283.

[14] Gang W. Comparative study on different neural networks for network security situation prediction[J]. Security and Privacy, 2020, 4(1):24–39.

[15] Yuan Y, Yuangang L. A Modified Hybrid Method Based on PSO, GA, and K-Means for Network Anomaly Detection[J]. Mathematical Problems in Engineering, 2022.

[16] Shandilya, S. K. Design and Deployment of Network Testbed for Web Data Security. Journal of Cyber Security and Mobility[J]. 2021, 11(02), 127–140.

[17] Qinghui L, Tianping Z. Deep learning technology of computer network security detection based on artificial intelligence[J]. Computers and Electrical Engineering, 2023, 110.

[18] Odumuyiwa, V., Alabi, R. DDOS Detection on Internet of Things Using Unsupervised Algorithms. Journal of Cyber Security and Mobility[J]. 2021, 10(3), 569–592.

[19] Guiwen J. Security Detection Design for Laboratory Networks Based on Enhanced LSTM and AdamW Algorithms[J]. International Journal of Information Technologies and Systems Approach (IJITSA), 2023, 16(2):1–13.

[20] Youfeng N, Mingxi G, Wenhao Y, et al. A Bayesian optimization-based LSTM model for DGA domain name identification approach[J]. Journal of Physics: Conference Series, 2022, 2303(1):546–569.

[21] Su, Yishan, Xia, et al. Exposing DeepFake Videos Using Attention Based Convolutional LSTM Network[J]. Neural Processing Letters, 2021, 53(6):1–17.

[22] Li S, Zhao D, Li Q. A Framework for Predicting Network Security Situation Based on the Improved LSTM[J]. EAI Endorsed Transactions on Collaborative Computing, 2020, 4(13):56–72.

[23] Mostofa A, Rahul G, Minhaz M C, et al. Enhancing Machine Learning Prediction in Cybersecurity Using Dynamic Feature Selector[J]. Journal of Cybersecurity and Privacy, 2021, 1(1):199–218.

[24] Panagiotis A P, Lazaros I, Antonios P, et al. COREM2 project: a beginning to end approach for cyber intrusion detection[J]. Neural Computing and Applications, 2022, 34(22):1965–1984.

[25] B V, Preethi G. Network Security Based on Multi-objective Ant Colony Optimization Algorithm[J]. Journal of Research in Science and Engineering, 2021, 3(9):23–36.

[26] Zhao D, Liu J. Study on network security situation awareness based on particle swarm optimization algorithm[J]. Computers & Industrial Engineering, 2018, 125(6):764–775.

[27] Zeng J. Research on secure encryption method of multi-domain fiber network based on particle swarm optimization algorithm[J]. Journal of Intelligent & Fuzzy Systems, 2019, 38(1):139–145.

[28] Shabbir J A, Faisal B, Naseer K Q, et al. Deep learning-based feature extraction and optimizing pattern matching for intrusion detection using finite state machine[J]. Computers and Electrical Engineering, 2021, 92.

[29] Oluwaseun R O, Bamidele J A, Peter S, et al. An Enhanced Intrusion Detection System using Particle Swarm Optimization Feature Extraction Technique[J]. Procedia Computer Science, 2021, 193(2):504–512.

[30] Wang H, Ruan J, Ma Z, et al. Deep learning aided interval state prediction for improving cyber security in energy internet[J]. Energy, 2019, 174(6):1292–1304.

[31] Davoud Sedighizadeh, Ellips Masehian, Mostafa Sedighizadeh et al. GEPSO: A new generalized particle swarm optimization algorithm[J]. Mathematics and Computers in Simulation, 2021, 179:194–212.

Biography

Li Wentao received his Bachelor's degree in Engineering from Nanyang Normal University in 2006, Master's degree in Modern Educational Technology from Henan University in 2016, and PhD candidate from Lincoln University Malaysia in 2023. He is currently a lecturer at Shuqing Medical College in Zhengzhou. His main research field and direction are computer network security.