Hindawi
Computational Intelligence and Neuroscience
Volume 2022, Article ID 6314262, 8 pages
https://doi.org/10.1155/2022/6314262

Research Article

Multimedia Security Situation Prediction Based on Optimization of Radial Basis Function Neural Network Algorithm

Gan Chen

Guangzhou Institute of Technology, Guangzhou, Guangdong 510075, China

Correspondence should be addressed to Gan Chen; 2016056028@stu.gzucm.edu.cn

Received 24 December 2021; Revised 9 February 2022; Accepted 18 February 2022; Published 8 April 2022

Academic Editor: Qiangyi Li

Aiming at the problem of prediction accuracy in network situation awareness, a network security situation prediction method based on a generalized radial basis function (RBF) neural network is proposed. This method uses the K-means clustering algorithm to determine the data center and expansion function of the RBF and uses the least-mean-square algorithm to adjust the weights to obtain the nonlinear mapping relationship between the situation value before and after the situation and carry out the situation prediction. Simulation experiments show that this method can obtain situation prediction results more accurately and improve the active security protection of network security. Compared with the PSO-RBF model, AFSA-RBF model, and IAFSA-RBF model, the maximum relative error and minimum relative error of the IAFSA-PSO-RBF model are reduced by 14.27%, 8.91%, and 32.98%, respectively, and the minimum relative error is reduced by 1.69%, 12.97%, and 0.61%, respectively. This shows that the IAFSA-PSO-RBF model has reduced the prediction error interval, and the average relative error is 5%. Compared with the other three models, the accuracy rate is improved by more than 5%, and it has met the requirements for the prediction of the network security situation.

1. Introduction

The rapid development of Internet technology has caused more and more security vulnerabilities and security incidents faced by network security management. In the offensive and defensive confrontation of network security, single detection equipment and defense equipment often cannot detect, analyze, and handle network security incidents in time. It can only respond passively after a security incident occurs. Research hotspots in the field of network security have also evolved from the construction of passive security systems to overall situational awareness of the global network. Drawing on the theory and technology of ATC situational awareness in air traffic supervision, the concept of network situational awareness CSA can be derived [1]. Network security situation prediction, as an advanced stage of network security situation awareness, can predict the development trend of network security status and assist network administrators to adjust defense strategies in a targeted manner, so that network security management changes from passive to active. In the prediction method based on time series, the iterative algorithm to complete parameter learning has low operating efficiency and long calculation time. The security situation prediction model based on the radial basis function (RBF) neural network has a faster learning speed. However, in practical applications, genetic algorithms have many control parameters and are prone to premature convergence, which may lead to local minimums, resulting in decreased prediction accuracy. Prediction is based on grasping the historical data, in accordance with certain methods and laws to speculate on the future value or trend, that is, for the situation value time series $\{x_i\}(i = 1, 2, \ldots)$, using the historical data $\{x_n, x_n + 1, \ldots, x_{n+m}\}$, to predict the value of the future $n + m + 1$ time, that is, to find the nonexistence of the future time series $\{x_i\}(i = 1, 2, \ldots)$, which is to find the nonlinear functional relationship of the future time series $\{x_n, x_{n+1}, \ldots, x_{n+m+1}\}$ linear function relationship[2, 3].

2. Literature Review

With the popularity of the Internet and the explosive growth of various applications, network security problems have become increasingly serious. Although network security products such as intrusion detection systems (IDS) and firewalls have been widely used, due to the shortcomings of false negatives, false positives, and inconsistent reporting formats, traditional single security methods can no longer meet security requirements. As a result, network security situational awareness technologies have emerged. These technologies can dynamically reflect the overall network security situation and predict and warn the development trend of network security. Jae-Hong, L, and others proposed the concept of network situation awareness (CSA) and pointed out that network situation awareness based on fusion will become the development direction of network management [4]. Li et al. pointed out that the network situation refers to the current state and changing trend of the entire network composed of various network equipment operating conditions, network behaviors, and user behaviors. The situation emphasizes the environment, dynamics, and the relationship between entities. It is a concept of a state, a trend, and a whole. Any single situation or state cannot be called a situation [5]. Chen found that network situation awareness refers to the acquisition, understanding and evaluation of factors that cause changes in the network situation in a large-scale network environment, as well as the prediction of actual and future development trends [6]. Guo and Yang believe that as an important part of network security situational awareness, situation prediction can reflect the changing trend of network security status at a macro level and make timely and effective defenses against possible network threats to achieve the goal of improving the level of network security [7]. Zhang and Wei pointed out that situation prediction refers to the prediction of the development trend of the overall or partial security situation of the network at a certain point in time or within a period of time in the future based on the results of past and current situations assessment [8]. Situation forecasting is based on actual data and historical data on the development and change of cyber security threats, using scientific theories, methods, and various experiences, judgments, and knowledge to speculate, estimate, and analyze its possible changes in a certain period of time in the future. Some research results have been made in the field of network security situation prediction at home and abroad. Lai et al. have proposed a situation prediction model that combines game theory with Bayesian networks [9]; Saxena et al. have proposed a situation prediction model. The prediction method is based on linear regression [10]; Zhou et al. proposed the grey system theory and used the GM model for prediction. However, the final prediction results obtained by these prediction models have poor accuracy and cannot effectively reflect the changing trend of network security [11]. Aiming at network security, which is affected by various factors, such as network attack behaviors, viruses, own vulnerabilities, and Trojan horses, and has a high degree of nonlinearity and time-varying complexity, they proposed a generalized radial basis function (RBF) neural network. A method for situation prediction based on generalized radial basis function (RBF) neural network is proposed [12]. The generalized RBF neural network is the main form of forward neural network. Because of its simple topology and the ability of the nonlinear learning process, learning is fast and efficient, and it is widely used in real-time adaptive systems. The generalized RBF neural network performs a nonlinear mapping from the m-dimensional input space to the n-dimensional output space and can approximate any single-valued continuous function with arbitrary precision. The RBF neural network diagram is shown in Figure 1.

3. Method

3.1. RBF Neural Network. The RBF neural network optimizes three adjustable parameters in the network, so the learning can be divided into two parts: (1) Determine the corresponding center c and b, according to the hidden layer nodes; (2) Determine the hidden layer nodes: the connection weight Wki between the node and each output node. The first part can be selected by external input data; that is, the distribution of the sample or the center point of the hidden layer can be calculated, and the width can be calculated by the corresponding center; the selection of the connection weight can be learned by the optimization algorithm. The current learning algorithms for the parameters in the network include clustering algorithm, orthogonal least square method, and gradient descent method [14–16].

3.1.1. K-Means Clustering Algorithm. This algorithm was first proposed by Moody et al. In this model, the algorithm is used to determine the center of the network. The idea is to first use a clustering algorithm to process the sample data and calculate the cluster center, and then use a supervised learning algorithm to calculate the weight of each output node and hidden layer node.

The specific steps of the K-means clustering algorithm are as follows:

(i) The number of clusters k is determined and n objects are assigned to the selected k center points according to the principle of minimum distance; that is, the n objects are divided into k clusters. In this way, the similarity of objects in the cluster is high, and the similarity between clusters is low

(ii) The center of the cluster where each object is located and redivide it with the new center.

(iii) Steps (1) and (2) are repeated until the object has no longer oscillates.

The main point of the K-means clustering algorithm is to minimize the sum of squared errors. However, due to the limitations of the algorithm, it cannot guarantee the global

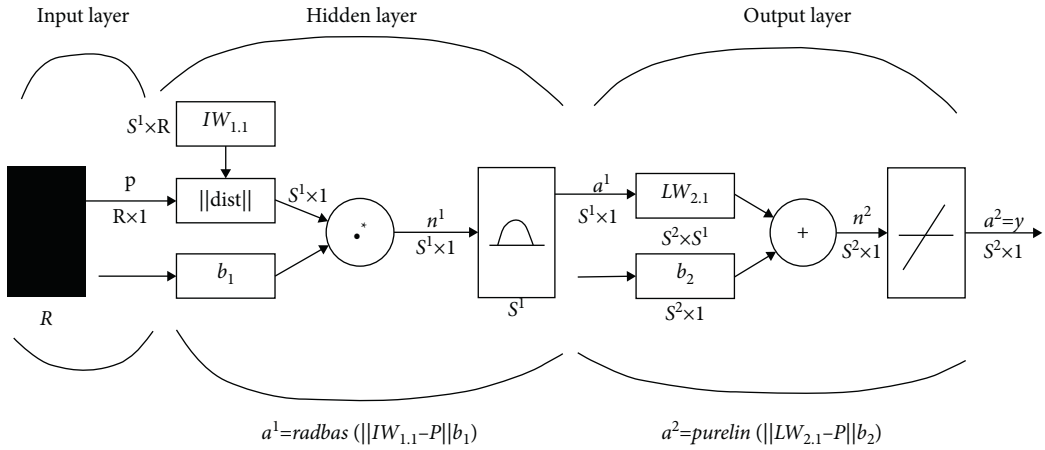

Figure 1: RBF neural network.

optimum. Moreover, the choice of the initial center largely determines the effect of the clustering algorithm, and the slight gap between the initial clustering centers will cause serious deviations. The usual optimization strategy is to initialize the cluster centers through different initial selection methods and select the optimal initialization method according to the results.

3.1.2. Orthogonal Least-Square Algorithm. The theoretical basis of the orthogonal least-squares algorithm is that different inputs have different degrees of influence on the selection of the center. The input sample is selected that has a greater impact on the center of the hidden layer as the network center so that the network structure can be simplified. The advantage of this algorithm is that it does not need to be tuned many times, and only the center is determined according to the magnitude of the input influence; the disadvantage is that the application range is narrow, it is suitable for batch learning, and the amount of calculation is huge.

3.1.3. Gradient Descent Method. In this method, the parameters that need to be tuned form an objective function in the form of variables, and the objective function is minimized and adjusted to finally determine the data center c_i, width b_i, and output connection weights w_i.

First, the error function is defined as

$$e_j = y_j - F\left(x_j\right) = y_j - \sum_{i=1}^{k} w_i \ell\left(x_j\right). \tag{1}$$

The objective function is defined as

$$E = \frac{1}{2}\sum_{j=1}^{N} e_j^2. \tag{2}$$

The parameters and output weights w^{ji} are found when the above formula is the smallest, and the gradient descent training algorithm for each parameter of the RBF neural network can be achieved.

$$\begin{aligned}
&\text{Correction direction of cente } C_i\text{: r}\nabla_{ci} = \frac{2w_i}{b_i}\ell_i(x)\left(x - c_i\right),\\
&\text{Correction direction of width } b_i\text{: } \nabla_{bi} = \frac{2w_i}{b_i^2}\ell_i(x)\left\|x - c_i\right\|^2,\\
&\text{Correction direction of weight } w_{\text{ji}}\text{ : } \nabla_{wi}F(x) = \ell_i(x).
\end{aligned} \tag{3}$$

The correction formula for gradient descent can be obtained.

$$\begin{aligned}
c_i(n+1) &= c_i(n) - \eta_1\frac{2w_i}{b_i}\sum_{j=1}^{N} e_j\ell_j\left(x_j\right)\left(x_j - c_j\right),\\
b_i(n+1) &= b_i(n) - \eta_2\frac{w_i}{b_i^3}\sum_{j=1}^{N} e_j\ell_j\left(x_j\right)\left\|x_j - c_j\right\|^2,\\
w_i(n+1) &= w_i(n) - \frac{1}{2}\eta_3\sum_{j=1}^{N} e_j\ell_i\left(x_j\right).
\end{aligned} \tag{4}$$

Among them, $\ell_i(x_j)$ represents the input of hidden layer node i to x_j, and 7, 1, 7 represent the learning rate.

Through the introduction of the above three algorithms, each has its own shortcomings. K-means clustering algorithm is difficult to determine the initial center selection criteria; the orthogonal least-squares method has a large amount of calculation; the gradient descent algorithm is easy to make the parameters in the network fall into a local minimum. In recent years, intelligent optimization algorithms have gradually become a research hotspot. Among them, the swarm intelligence optimization algorithm is one of the important research directions. The following will introduce two swarm intelligence optimization algorithms and improvements for optimizing RBF neural networks [17–20].

3.2. Particle Swarm Algorithm. The flowchart of the particle swarm algorithm is shown in Figure 2.

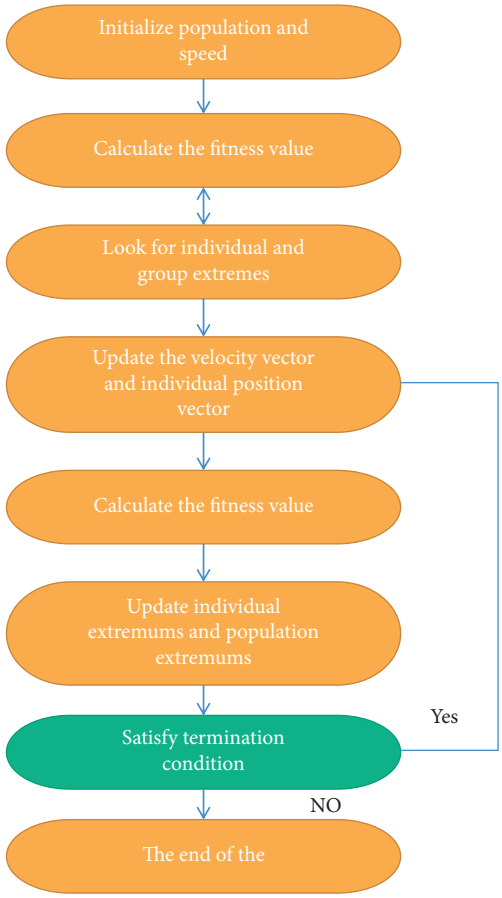

Figure 2: Flowchart of particle swarm algorithm.

The calculation steps of the particle swarm algorithm are as follows:

(1) The initial position vector and velocity vector of each particle in the population are initialized, and the relevant parameters of the particle swarm algorithm are initialized.

(2) The fitness value of each particle is calculated, and the initial individual extreme value and the group extreme value are set. Then, the iterative optimization operation of the particles to adjust the particle position vector and velocity vector is started.

(3) The fitness value of the new population according to the objective function is recalculated.

(4) For each particle, two comparison updates are required. One is to compare and update the current fitness value with the individual extreme value. The second is to compare and update the current fitness value with the optimal extremum in the population.

(5) The termination conditions (the maximum number of iterations is reached or the fitness value reaches the minimum error) are checked, and if the termination conditions are met, the optimal position and extreme value are outputted; otherwise, the iteration is continued.

The advantages of the particle swarm algorithm are as follows: no in-depth understanding of the problems that need to be dealt with, and strong universality; the algorithm has certain memory ability. At the same time, its shortcomings are very obvious: the algorithm still has local optimization problems; the setting of algorithm parameters requires a certain amount of manual operation.

In view of the shortcomings of the convergence performance of the particle swarm algorithm, some scholars propose to introduce a shrinkage factor that changes with the iteration in the iteration; some scholars overcome the problem that the particle swarm algorithm cannot approach the target in the later stage by introducing the concept of neighborhood. Two common ways to improve are described as follows.

3.2.1. Particle Swarm Algorithm with Inertial Weight. This method improves the global search ability of the algorithm by changing the inertia weight. The improvement formula is as follows:

$$v_{im}(t+1) = wv_{im}(t) + c_1 r_1 \left(p_{im}(t) - x_{im}(t)\right) + c_2 r_2 \left(p_{gm}(t) - x_{im}(t)\right), \quad (5)$$

where w is the inertia weight. The improvement idea is that the particles run at a high speed at the very beginning and can search a large space in a short time. Then, w decreases, the particle speed decreases, and a detailed search is performed in the optimal solution domain at a low speed.

In addition, a linear change method for weights is proposed.

$$w = w_{\max} - \frac{(w_{\max} - w_{\min})k}{k_{\max}}. \quad (6)$$

When the w in the formula is larger, it is helpful to avoid local extrema, and when it is smaller, the convergence speed is improved.

3.2.2. Particle Swarm Algorithm with Shrinkage Factor. In 1999, Clerc proved mathematically that the convergence factor can ensure the convergence of the PSO algorithm. The improved model is as follows:

$$v_{im}(t+1) = k\left(v_{im}(t) + c_1 r_1 \left(p_{im}(t) - x_{im}(t)\right)\right) + c_2 r_2 \left(p_{gm}(t) - x_{im}(t)\right). \quad (7)$$

$$\frac{k = 2}{\left|2 - \ell - \sqrt{\ell^2 - 4\ell}\right|}, \quad \text{among them,} \quad \ell = c_1 + c_2 > 4. \quad (8)$$

$$x_{im}(t+1) = x_{im}(t) + v_{im}(t+1). \quad (9)$$

Usually, ℓ is set to 4.1, and then, k can be calculated by formula (8).

4. Results and Analysis

The parameters of the particle swarm algorithm are set as follows: the number of particles in the particle swarm popcount = 20, the acceleration factor is $c_1 = 2, c_2 = 2$, the particle dimension poplength = $5 \times 6 + 6 \times 1 + 6 + 1 = 43$, and the maximum number of iterations MaxEpoch = 200. The obtained prediction results are shown in Figure 3 by using this model to predict the last 10 sample data, and Table 1.

This section uses the improved and standard artificial fish school algorithm to optimize the parameters of the RBF neural network. The RBF neural network is still a 5-6-1 structure, and the hidden layer uses the Gaussian function as the transfer function. The artificial fish school parameters of the two algorithms are set as follows: the population size of the artificial fish school $N = 20$, the maximum number of iterations $m = 200$, the perception range of the artificial fish Visual = 3.5, the maximum step length of the artificial fish Step = 1.5, and the crowding factor 1 = 0.38.

Using this model to predict the last 10 sample data, the obtained prediction results are shown in Figure 4 and Table 2.

It can be seen from Figure 4 that the prediction results of the IAFSA-RBF model are closer to the actual results than the AFSA-RBF model. It can be seen from Table 2 that the maximum relative error of the improved artificial fish school prediction reached about 47%, but the overall relative error has generally decreased, indicating that the improved algorithm has a certain optimization and improvement effect on the RBF neural network parameters, and improves the overall prediction accuracy.

The prediction results of the three models are shown in Figure 5.

The maximum relative error, minimum relative error, and average relative error of the four models are shown in Table 3.

(1) From the comparison in Figure 5, it can be seen that the prediction curve of the IAFSA-PSO-RBF model for the network security situation is closer to the actual prediction value than the prediction curve of the IAFSA-RBF model and the PSO-RBF model [8, 21, 22].

(2) By comparing the three error indicators of the absolute maximum relative error, the absolute minimum error, and the average relative error of the prediction results of the four models, it can be seen that the maximum relative error and the minimum relative error of the IAFSA-PSO-RBF model are compared to the PSO-RBF model. AFSA-RBF model and IAFSA-RBF model are reduced by 14.27%, 8.91%, and 32.98%, respectively, and the minimum relative error was reduced by 1.69%, 12.97%, and 0.61%, respectively. This shows that the IAFSA-PSO-RBF model has reduced the prediction error interval, and the average relative error is 5%. Compared with the other three models, the accuracy rate is improved by more than 5%, and it has met the requirements for the prediction of the network security situation.

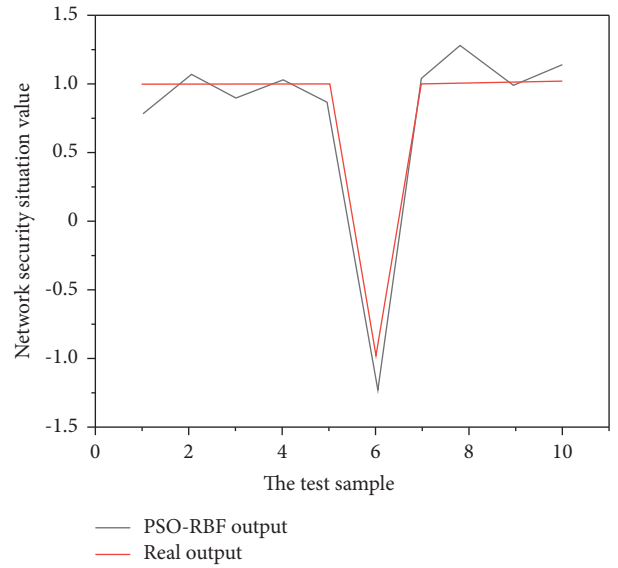

Figure 3: Comparison of PSO-RBF model prediction results and actual values.

Table 1: Comparison of PSO-RBF model forecast situation results and actual network situation values.

Sample actual	Predicted value	Absolute value	Error relative	Error (%)
1	1	1.22	0.22	22
2	1	0.96	0.04	4
3	1	1.1	0.1	11
4	1	0.97	0.03	3
5	1	1.14	0.15	15
6	−1	−0.72	0.28	28
7	1	0.82	0.17	17
8	1	0.87	0.13	13
9	1	1.02	0.02	2
10	1	0.88	0.12	12

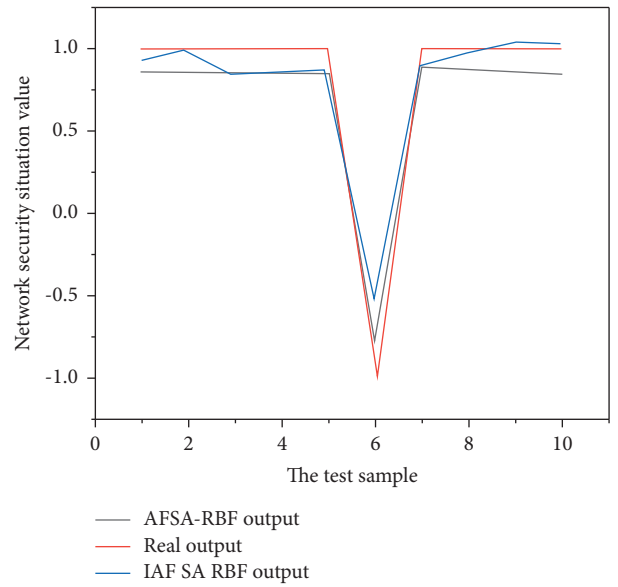

Figure 4: Comparison of prediction results and actual values of AFSA-RBF model and AFSA-RBF model.

Table 2: Comparison of predicted situation results of IAFSA-RBF model and AFSA-RBF model and actual network situation values.

Sample	Actual value	IAFSA-RBF model			AFSA-RBF model		
		Predicted value	Absolute error	Relative error (%)	Predicted value	Absolute error	Relative error (%)
1	1	0.95	0.05	5	0.85	0.15	15
2	1	0.99	0	1	0.85	0.15	15
3	1	0.86	0.14	14	0.85	0.15	15
4	1	0.89	0.11	11	0.85	0.15	15
5	1	0.86	0.14	14	0.85	0.15	15
6	−1	−0.53	0.47	47	0.77	0.23	23
7	1	0.87	0.13	13	0.85	0.15	15
8	1	0.96	0.04	4	0.87	0.13	13
9	1	1.03	0.03	3	0.86	0.14	14
10	1	1.03	0.02	2	0.85	0.15	15

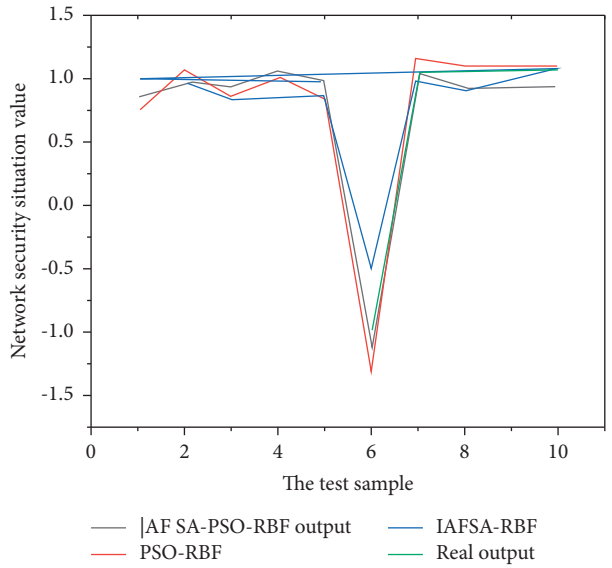

Figure 5: Comparison of the predicted results and actual values of the three models.

Table 3: Comparison table of four model errors.

	PSO-RBF model	AFSA-RBF model	IAFSA-RBF model	IAFSA-PS0-RBF model
Maximum relative error (%)	28	23	47	14
Minimum relative error (%)	2	13	1	0.3
Average relative error (%)	13	15	11	6

5. Conclusion

It can be seen from the increasing number of network security incidents in the last year that today's network environment has become more and more complex, and the network security situation is worrisome. Therefore, the self-learning and nonlinear function fitting capabilities of artificial neural networks are used to predict the network security situation [20, 23, 24]. RBF neural network is superior to other neural network algorithms in terms of nonlinear approximation ability and learning speed, but its disadvantage is that it is difficult to select the optimal parameters. Therefore, it is proposed to use the improved artificial fish school and particle swarm algorithm to optimize the prediction model of the RBF neural network to predict the future network security situation. Using simulated annealing algorithm and Gaussian mutation operator to enhance the global search ability of artificial fish school algorithm, the accuracy of artificial fish school optimization is improved, and the advantages and disadvantages of artificial fish school and particle swarm are analyzed and compared. Aiming at the problem of RBF neural network parameter selection, the improved artificial fish school and particle swarm hybrid algorithm are used to optimize the RBF neural network parameters to form an IAFSA-PSO-RBF neural network prediction model and apply it to the prediction of the domestic network security situation. Simulation experiments show that the prediction results of the model are basically consistent with the actual values,

which effectively predicts the network security situation. In order to further verify the effectiveness of the model, the experimental simulation results of the RBF neural network prediction model optimized by the hybrid algorithm are compared with the prediction results of the PSO-RBF model, AFSA-RBF model, and IAFSA-RBF model, and the RBF neural network optimized by the hybrid algorithm is found The network prediction model is better than the other three models in the accuracy of the prediction of the domestic network security situation, and it improves the problem of particle swarms that are easy to fall into local extremes and the shortcomings of slow convergence of artificial fish schools. [25–27].

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 study was supported by the Characteristic Innovation Project of Colleges and Universities in Guangdong Province in 2019: Exploration and Research on business registration based on blockchain technology (2019GKTSCX074).

References

[1] X. Meng, L. Nie, and J. Song, "Iot individual privacy features analysis based on convolutional neural network," *Cognitive Systems Research*, vol. 57, pp. 126–130, 2019.

[2] P. Lin and Y. Chen, "Network security situation assessment based on text simhash in big data environment," *International Journal on Network Security*, vol. 21, no. 4, pp. 699–708, 2019.

[3] P. Zhao, H. Cheng, Y. Fang, and X. Wang, "A secure storage strategy for blockchain based on mcmc algorithm," *IEEE Access*, vol. 8, pp. 160815–160824, 2020.

[4] L. Jae-Hong, K. Do-Hyung, J. Seong-Nyum, and C. Seong-Ho, "Diagnosis and prediction of periodontally compromised teeth using a deep learning-based convolutional neural network algorithm," *Journal of Periodontal & Implant Science*, vol. 48, no. 2, pp. 114–123, 2018.

[5] F. W. Li, X. Y. Zhang, J. Zhu, and Q. Huang, "Network security situation prediction based on apde-rbf neural network," *Xi Tong Gong Cheng Yu Dian Zi Ji Shu/Systems Engineering and Electronics*, vol. 38, no. 12, pp. 2869–2875, 2016.

[6] Y. Chen, "Prediction algorithm of pm2.5 mass concentration based on adaptive bp neural network," *Computing*, vol. 100, no. 8, pp. 825–838, 2018.

[7] C. X. Guo and S. U. Yang, "A new optimized algorithm based on quantum eolutionary strategy for network security situation prediction," *Journal of Chinese Computer Systems*, vol. 35, no. 6, pp. 1248–1252, 2014.

[8] W. Zhang and D. Wei, "Prediction for network traffic of radial basis function neural network model based on improved particle swarm optimization algorithm," *Neural Computing & Applications*, vol. 29, no. 4, pp. 1143–1152, 2018.

[9] J.-B. Lai, H.-Q. Wang, X.-W. Liu, Y. Liang, R.-J. Zheng, and G.-S. Zhao, "Wnn-based network security situation quantitative prediction method and its optimization," *Journal of Computer Science and Technology*, vol. 23, no. 2, pp. 222–230, 2008.

[10] D. Saxena, K. S. Verma, and S. N. Singh, "Power quality event classification: an overview and key issues," *International Journal of Engineering Science and Technology*, vol. 2, no. 3, pp. 186–199, 2010.

[11] Z.-J. Zhou, G.-Y. Hu, B.-C. Zhang, C.-H. Hu, Z.-G. Zhou, and P.-L. Qiao, "A model for hidden behavior prediction of complex systems based on belief rule base and power set," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1649–1655, 2018.

[12] X. Lv, "Review of mid- and long-term predictions of China's grain security," *China Agricultural Economic Review*, vol. 5, no. 4, pp. 567–582, 2013.

[13] P. Shi, Y. Yuan, L. I. Xiaobing, and Y. Chen, "Land use pattern adjustment under ecological security: look for secure land use pattern in China," *Geographical Review of Japan*, vol. 77, no. 12, pp. 866–882, 2008.

[14] E. A. Ashley, R. E. Hershberger, C. Caleshu, P. T. Ellinor, J. G. N. Garcia, and D. M. Herrington, "Genetics and cardiovascular disease: a policy statement from the american heart association," *Circulation*, vol. 126, no. 1, pp. 142–157, 2012.

[15] C. Tang, Q. Tan, Y. Han, W. An, and H. Tang, "An energy harvesting aware routing algorithm for hierarchical clustering wireless sensor networks," *KSII Transactions on Internet and Information Systems(TIIS)*, vol. 10, no. 2, pp. 504–521, 2016.

[16] S. Vasilica and M. Rimbasiu, "[essential periodontopathy. the "osipov-sinesti" concept of anatomic-clinical, biological and radiological interpretation, and on its therapeutic resolution by means of an original and personal operative method]," *Rev Fr Odontostomatol*, vol. 9, no. 4, pp. 767–776, 1969.

[17] F. W. Li, X. Y. Zhang, J. Zhu, and Q. Huang, "Network security situation prediction based on apde-rbf neural network," *Xi Tong Gong Cheng Yu Dian Zi Ji Shu/Systems Engineering and Electronics*, vol. 38, no. 12, pp. 2869–2875, 2016.

[18] H. E. Seim, M. Fletcher, C. Mooers, J. R. Nelson, and R. H. Weisberg, "Towards a regional coastal ocean observing system: an initial design for the southeast coastal ocean observing regional association," *Journal of Marine Systems*, vol. 77, no. 3, pp. 261–277, 2009.

[19] W. Chen, B. Feng, and J. Sun, "Simulation study on the parameters optimization of radial basis function neural network based on qpso algorithm," *Journal of Computer Applications*, vol. 26, no. 8, pp. 1928–1931, 2006.

[20] S. Chen and Y. Wu, "Combined genetic algorithm optimization and regularized orthogonal least squares learning for radial basis function networks," *IEEE Transactions on Neural Networks*, vol. 10, no. 5, pp. 1239–1243, 1999.

[21] D. S. Huang and J. X. Du, "A constructive hybrid structure optimization methodology for radial basis probabilistic neural networks," *IEEE Transactions on Neural Networks*, vol. 19, no. 12, pp. 2099–2115, 2008.

[22] L. Long, J. Sun, D. Zhang, G. Du, C. Jian, and W. Xu, "Culture conditions optimization of hyaluronic acid production by streptococcus zooepidemicus based on radial basis function neural network and quantum-behaved particle swarm optimization algorithm," *Enzyme and Microbial Technology*, vol. 44, no. 1, pp. 24–32, 2009.

[23] G. Fu, H. Gong, H. Gao, T. Gu, and Z. Cao, "Integrated thermal error modeling of machine tool spindle using a

chicken swarm optimization algorithm-based radial basic function neural network," *International Journal of Advanced Manufacturing Technology*, vol. 105, no. 5-6, pp. 2039–2055, 2019.

[24] X. Li and Y. Sun, "Stock intelligent investment strategy based on support vector machine parameter optimization algorithm," *Neural Computing & Applications*, vol. 32, no. 6, pp. 1765–1775, 2020.

[25] H. Sarimveis, A. Alexandridis, S. Mazarakis, and G. Bafas, "A new algorithm for developing dynamic radial basis function neural network models based on genetic algorithms," *Computers & Chemical Engineering*, vol. 28, no. 1/2, pp. 209–217, 2004.

[26] M. Sheikhan, M. Pezhmanpour, and M. S. Moin, "Improved contourlet-based steganalysis using binary particle swarm optimization and radial basis neural networks," *Neural Computing & Applications*, vol. 21, no. 7, pp. 1717–1728, 2012.

[27] W. Huang and Y. Yang, "Water quality sensor model based on an optimization method of rbf neural network," *Computational Water, Energy, and Environmental Engineering*, vol. 09, no. 1, pp. 1–11, 2020.