Received: 9 November 2021 | Revised: 7 March 2022 | Accepted: 22 March 2022 | Published online: 25 March 2022

RESEARCH ARTICLE

Journal of Computational and Cognitive Engineering
2022, Vol. 1(3) 103–108
DOI: 10.47852/bonviewJCCE149145205514

BON VIEW PUBLISHING

Research on Internet Security Situation Awareness Prediction Technology Based on Improved RBF Neural Network Algorithm

Zhihua Chen[1,*]

[1]*Guangdong Polytechnic Normal University, China*

Abstract: With the increasing scale and complexity of the network, the network attack technology is also changing, such as malicious program attack, Trojan horse, distributed denial of service attack, worm, virus, web code injection, botnet, and other new network attack tools emerge in large numbers. As the core hotspot of network information security, network security situational awareness has received more and more attention. The traditional way of network security situational awareness prediction is relatively single. Usually, only one algorithm is used for perception and prediction, and its prediction accuracy is limited. To explore the application effect of intelligent learning algorithm, this study takes radial basis function (RBF) neural network as the main research object, optimizes RBF by simulated annealing (SA) algorithm and hybrid hierarchy genetic algorithm (HHGA), constructs RBF neural network prediction model based on SA–HHGA optimization, and carries out relevant experiments. The results show that the predicted situation value of the optimized RBF neural network in 15 samples is very close to the actual situation value. The neural network has good prediction effect and can provide assistance for the maintenance of network security.

Keywords: RBF neural network, network security, situation awareness, prediction, application

1. Introduction

In the complex cyberspace, it is extremely necessary to construct an effective network security situation assessment model, which can provide real-time and effective prediction of the dynamic evolution of the network model and ensure network security by providing corresponding security strategies (Raissi & Karniadakis, 2018). To achieve accurate prediction of network security situation awareness, it is necessary to adopt certain intelligent learning algorithms. Among them, the radial basis function (RBF) neural network has good results in finding the nonlinear mapping relationship of network security situation values, but there are still problems such as local optimization (Butler et al., 2018; Cooper et al., 2019). Peng and other researchers believe that improving the energy efficiency of various air-conditioning systems helps to reduce greenhouse gas emissions. A demand-driven control strategy is constructed through machine learning algorithm, which successfully improves the operation efficiency of the system (Peng et al., 2018). Karaa WBA and other scholars found that the relationship between different semantic information can be effectively extracted by computer algorithm. Support vector machine classifier is used to extract information, which significantly improves the extraction efficiency and accuracy (Tian et al., 2020). Miller GA and his research partners use animal-mounted sensor technology and corresponding machine learning algorithms to predict working hours and related data and improve the prediction efficiency to a certain extent (Miller et al., 2020). Yang and other experts and scholars found that the application scope of machine learning algorithms has gradually expanded, and a variety of machine learning algorithms have been applied to the actual process of data estimation, successfully improving the estimation accuracy and ensuring the accuracy and reliability of data (Mayer et al., 2020). Aiming at the problem that drugs are environmental pollutants to another extent, A T H M et al. used machine learning algorithm for systematic analysis and prediction and conducted a detailed analysis on bioconcentration factors. Finally, they successfully enhanced the accuracy and effectiveness of machine learning algorithm prediction (Miller et al., 2019). JF Hern á ndez and other scholars conducted in-depth research on the bankruptcy of insurance companies in the field of financial research, compared and analyzed two different nonparametric machine learning technologies, and finally verified that the machine learning algorithm based on multilayer perceptron has strong prediction performance (Wang et al., 2020).

This research innovatively uses simulated annealing (SA) algorithm and hybrid hierarchy genetic algorithm (HHGA)

*Corresponding author: Zhihua Chen, Guangdong Polytechnic Normal University, China. Email: hansun288@163.com

algorithm to optimize RBF, which can more accurately predict the future situation, and provides support for the research of relevant network security situation.

2. Network Model Construction Based on Optimized RBF Neural Network Algorithm

2.1 RBF neural network model and its structure analysis

RBF neural network is a single hidden layer feedforward neural network that can effectively process nonlinear data. When a new sample is obtained in the RBF neural network, not all neurons in it need to be adjusted accordingly, and only the neurons that are similar to the input sample vector need to be adjusted, which is usually called local approximation network (Alix et al., 2019). Compared with other neural network models, RBF neural network has stronger learning, classification, and approximation capabilities. Figure 1 shows the structure of the network.

According to Figure 1, the RBF neural network mainly contains three network layers, namely the input layer, the hidden layer, and the output layer. The input layer contains a large number of perceptual units, which can serve as the connecting element between the neural network and the external environment; the hidden layer is located between the input layer and the output layer, in which there is a set of RBF functions, which can realize nonlinear conversion; the core of the output layer is to use mathematical means to process the output signal of the hidden layer and realize the final output (Kou et al., 2019). Figure 1 shows the commonly used RBF function φ_n, as shown in formula (1).

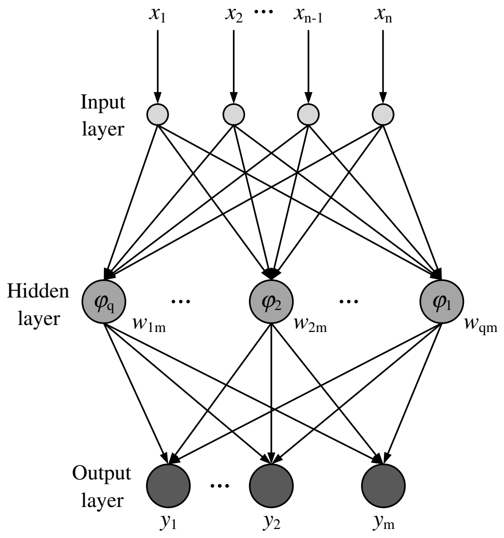
$$\varphi(r) = \frac{1}{\sqrt{r^2 + \sigma^2}} \tag{1}$$

In formula (1), $r = \|X - c_i\|^2$, and $i = 1, 2, 3, \ldots, q$, where c_i represents the center point of the neuron, q represents the number of nodes in the hidden layer, σ represents the expansion constant of the basis function, and its value determines the width of the RBF function. When the RBF neural network performs linear weighting, the output of its network mapping is shown in formula (2):

$$y_m = \sum_{j=1}^{q} w_{jk}\varphi_j \tag{2}$$

where w_{jk} represents the weight of the j-th neuron in the hidden layer when it is connected to the output layer.

Figure 1
Structure of RBF neural network



2.2 Implementation of HHGA algorithm and its optimized RBF neural network algorithm

As an effective algorithm to realize parameter optimization and solve network topology problems, HHGA algorithm includes different chromosomes, including parameter gene sequence and control gene sequence. Whether the former can play its due role depends on the latter (Xi et al., 2019). The former is composed of real number coding, while the latter is mainly composed of various binary codes, “0” indicates that the corresponding parameter gene is not activated and is in an invalid or dormant state, and “1” indicates that it is in an effective or activated state (Gorham, 2020). All chromosomes of HHGA algorithm adopt a mixed coding mode, and the coding and decoding process is shown in Figure 2.

It can be seen from Figure 2 that HHGA algorithm mainly includes two chromosomes, which are, respectively, composed of parameter gene sequence and control gene sequence. During decoding, all parameter genes corresponding to “1” in the control gene will be activated in real time, while all parameter genes corresponding to “0” will be completely ignored (Rapuzzi & Repetto, 2018; Xu, 2018). After the activation, the parameter genes will be recombined to become the numerical sequence required by HHGA algorithm. It can be seen that the parameter genes in the two chromosomes are divided into two groups, one is 1,2,5,6, and the other is 3,4,7,8. When applying HHGA algorithm to optimize RBF neural network algorithm, it mainly includes four steps: first, to encode the chromosome and initialize the population; second, to call fitness function; third, to carry out genetic operation to improve the global search ability of the algorithm; and finally fourth, to calculate the output weight of RBF neural network (Goodall et al., 2018; Zhang et al., 2019a). In the first step, the focus is on coding the chromosome, as shown in Figure 3.

In HHGA algorithm, the length of parameter gene will lead to a certain difference in the number of hidden layer nodes, and the former is closely related to the dimension of input data in RBF neural network. Based on this, the number of nodes in the hidden

Figure 2
Example diagram of HHGA algorithm

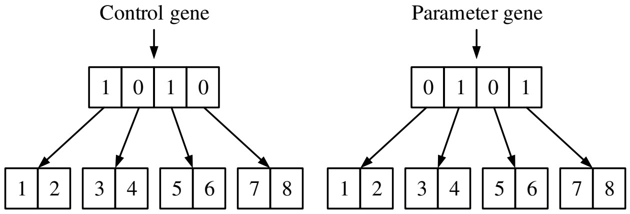
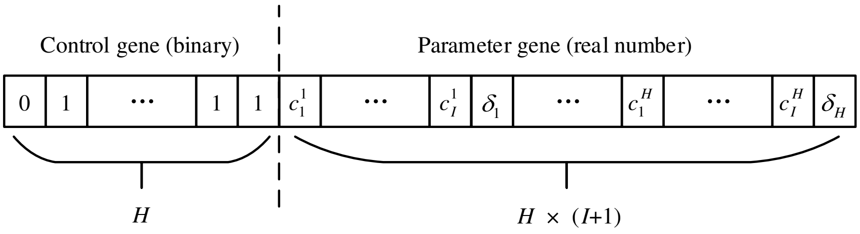


Figure 3
Schematic diagram of chromosome coding processing



layer and the input layer can be H and I, respectively, so $H \times (I + 2)$ can be used to represent the length of chromosome (Zhang et al., 2019b).

2.3 Network security situation awareness prediction model based on optimized RBF neural network algorithm

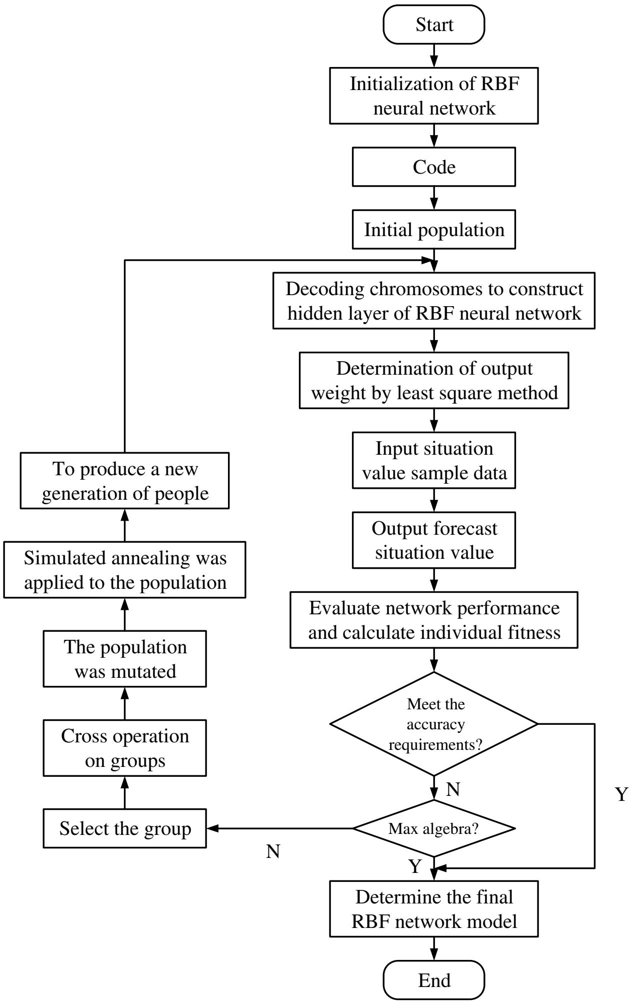
Since the output layer of RBF neural network is linear neuron, it can be optimized by HHGA (Yang et al., 2019). HHGA can determine the parameters related to nodes in the hidden layer of RBF neural network and then obtain the corresponding output weights with the help of least square method. As an extension of local search algorithm, SA algorithm can effectively avoid local optimization (Demirel & Deveci, 2017). SA algorithm is usually applied to combinatorial optimization problems. Its basic idea is to make a feasible solution of a specific problem X. The optimization objective of the problem is regarded as a fixed micro state, which is x. The capability contained therein is defined as E. The continuously decreasing control parameter t in the algorithm can be regarded as the temperature T of the solid in the annealing process (Deveci & Demirel, 2017). For T that constantly generates updated values, different feasible solutions will appear randomly, and the probability of transfer between feasible solutions is shown in equation (3).

$$p(X_{old} \rightarrow X_{new}) = \begin{cases} 1 & f(X_{old}) \leq f(X_{new}) \\ \exp\left(\frac{f(Xnew)-f(Xold)}{T}\right) & f(X_{old}) > f(X_{new}) \end{cases} \quad (3)$$

In equation (3), p represents the transition probability, X_{old} and X_{new} represent the current solution and the new solution, respectively. SA algorithm first generates an X randomly from the objective function f. Then, the elements in X are replaced to obtain an X_{new}, then calculate the difference between the objective function values of X_{old} and X_{new}, and judge the relationship between the difference and 0. Finally, X_{new} is accepted, and the optimal solution is returned. In this process, if X_{new} does not meet the termination conditions, it can be processed circularly by slowly reducing the temperature until the return value of the optimal solution is obtained. Therefore, the optimization of RBF neural network can be realized by organically combining HHGA and SA algorithm, as shown in Figure 4.

Figure 4 shows that the RBF neural network needs to be initialized first and then performs operations such as encoding, population initialization, decoding, and weight determination in sequence. After outputting the predicted network security situation value, the performance of the neural network can be objectively evaluated, and the accurate calculation of individual fitness can be completed. If the obtained results meet the accuracy requirements, the final RBF neural network model can be obtained; otherwise, it is judged whether the maximum algebra is reached, and if it is reached, the final RBF neural network model can also be obtained. If it is not reached, it is necessary to perform operations such as selection, crossover, mutation, and SA on the population in turn and return to the decoding step after generating a new generation of population until the two judgment requirements are met and the final RBF neural network model is determined.

Figure 4
Flow chart of RBF neural network algorithm based on SA–HHGA


Start
Initialization of RBF neural network
Code
Initial population
Decoding chromosomes to construct hidden layer of RBF neural network
Determination of output weight by least square method
Input situation value sample data
Output forecast situation value
Evaluate network performance and calculate individual fitness
Meet the accuracy requirements?
N
Y
Max algebra?
N
Y
Determine the final RBF network model
End
Select the group
Cross operation on groups
The population was mutated
Simulated annealing was applied to the population
To produce a new generation of people

3. Application Effect of Optimized RBF Neural Network in Network Security Situation Awareness Prediction

To explore and optimize the application effect of RBF neural network in network security situation awareness prediction, in this subject experiment, a data set containing 120 samples is selected. First, it is subjected to a comprehensive normalization process, and then it is made into a network security situation prediction sample. According to the time series division method, 15 test samples are selected. Data sets are directly selected from network security samples. The input and output, respectively, represent the actual value and predicted value of the network security situation. In this study, 15 prediction samples with typical characteristics were selected according to the division of time series, and each sample contains a large amount of network security data information, which is enough for neural network training and security situational awareness and prediction. The average error index here is not as intuitive as the comparison between the actual value and the predicted value of the network security situation. Then, the super parameters of SA–HHGA neural network are set so that the hidden layers of its deep neural network are 3, that is, the most common neural network structure and its layers, to avoid the impact caused by too many or different layers of the network. Finally, the RBF neural network algorithm model optimized based on SA–HHGA is used to sense the situation of this batch of test samples. The comparison between the results and the actual situation value is shown in Figure 5.

It can be seen from Figure 5 that in samples 1, 4–10, and 14, there is a small gap between the predicted network security situation value based on the RBF neural network algorithm model optimized by SA–HHGA and the actual network security situation value; the predicted value of network security situation in other samples is almost consistent with the actual value. This shows that the neural network algorithm can effectively complete the perception and prediction of network security situation. To further explore the advantages of the optimized RBF neural network, a comparative experiment is carried out in this study, and the results are shown in Figure 6.

Figure 6 shows the prediction results of network security situation awareness by BP (Back Propagation Neural Network) neural network and RBF neural network. There is a certain difference from the actual situation value. The trend of the situation value curve of 15 samples is basically the same, but there is a large gap between samples 1–7 and 13–14. The RBF neural network optimized based on SA–HHGA has a good prediction effect, and the situation value at each sample is almost completely close to the actual situation value. To make the comparison results more clear and accurate, the errors of the predicted values of the three neural network algorithm prediction models have been marked in Figure 6. Comparing the error lines of the three, it can be seen that the error line of RBF neural network optimized based on SA–HHGA is the shortest, indicating that its prediction accuracy is the highest. To further judge the rationality and reliability of the algorithm in this paper, the output value of RBF neural network algorithm before and after optimization is compared with the expected value. The results of comparative analysis are shown in Figure 7.

Figure 5
Comparison of network security situation awareness prediction results

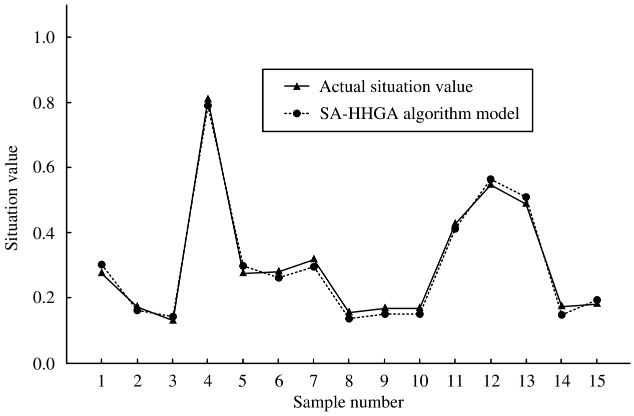


Figure 6
Comparison results of different neural network models for network security situation awareness prediction

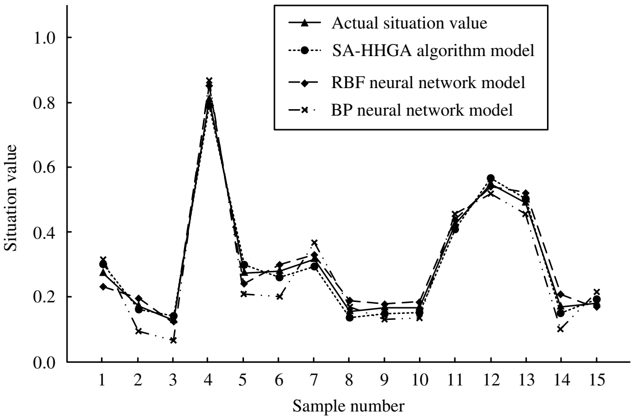
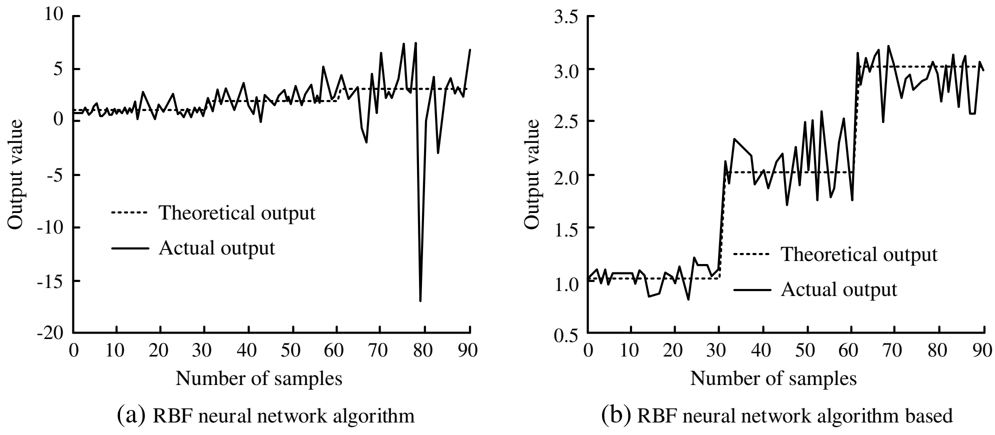


Figure 7(a) shows the output results of RBF neural network algorithm before optimization. It can be seen that when the number of samples is small, the actual output of the algorithm is basically consistent with the theoretical output. However, in the process of increasing the number of samples, the actual output fluctuates greatly, which is significantly different from the theoretical output. Figure 7 (b) shows the output results of RBF neural network algorithm optimized based on SA–HHGA. In the process that the theoretical output value increases with the increase of the number of samples, its actual output value always fluctuates around the theoretical output value, and its overall change trend remains the same. This shows that the RBF neural network algorithm based on SA–HHGA optimization has better recognition and prediction performance.

4. Conclusion

As the application of massive data continues to expand, the importance of network security has become increasingly prominent. To improve the prediction accuracy of network security situational awareness, this subject experiment is aimed at the RBF neural network in the intelligent learning algorithm, using the SA algorithm and the HHGA algorithm to optimize it to a certain extent and apply it to the actual prediction of the corresponding sample. The results show that the predicted situation value of the

Figure 7
Comparison of test output of RBF neural network algorithm before and after optimization



(a) RBF neural network algorithm

(b) RBF neural network algorithm based on SA-HHGA optimization

RBF neural network optimized based on SA–HHGA in 15 samples is basically consistent with the actual situation value, and the gap is much smaller than the BP neural network and the RBF neural network. This means that the network model has good fitting effect and high prediction accuracy and can be widely applied to network security situation awareness prediction. In the era of big data, the security needs of network operation and development are increasing day by day. The prediction accuracy of network security situational awareness of this algorithm needs to be improved. In the future, different types of algorithms should be used for optimization and simulation analysis, to ensure the operation security of the Internet including massive data.

Conflicts of Interest

The author declares that he has no conflicts of interest to this work.

References

Butler, K. T., Davies, D. W., Cartwright, H., Isayev, O., & Walsh, A. (2018). Machine learning for molecular and materials science. *Nature*, *559*(7715), 547–555.

Cooper, H. M., Zhang, C., Davis, S. E., & Troxler, T. G. (2019). Object-based correction of LiDAR DEMs using RTK-GPS data and machine learning modeling in the coastal Everglades. *Environmental Modelling & Software*, *112*, 179–191.https://doi.org/10.1016/j.envsoft.2018.11.003

Demirel, N.Ç., & Deveci, M. (2017). Novel search space updating heuristics-based genetic algorithm for optimizing medium-scale airline crew pairing problems. *International Journal of Computational Intelligence Systems*, *10*(1), 1082–1101. https://doi.org/10.2991/ijcis.2017.10.1.72

Goodall, J. R., Ragan, E. D., Steed, C. A., Reed, J. W., Richardson, G. D., Huffer, K. M., ..., & Laska, J. A. (2018). Situ: Identifying and explaining suspicious behavior in networks. *IEEE Transactions on Visualization and Computer Graphics*, *25*(1), 204–214. https://doi.org/10.1109/TVCG.2018.2865029

Gorham, C. L. (2020). Developing enterprise cyber situational awareness. *International Journal of Managing Information Technology*, *12*(3), 1–8. https://doi.org/10.5121/ijmit.2020.12301

Kou, G., Wang, S., & Tang, G. (2019). Research on key technologies of network security situational awareness for attack tracking prediction. *Chinese Journal of Electronics*, *28*(1), 166–175. https://doi.org/CNKI:SUN:EDZX.0.2019-01-022

Mayer, K. S., Soares, J. A., & Arantes, D. S. (2020). Complex MIMO RBF neural networks for transmitter beamforming over nonlinear channels. *Sensors*, *20*(2), 378. https://doi.org/10.3390/s20020378

Miller, G. A., Mitchell, M., Barker, Z. E., Giebel, K., Duthie, C-A. (2020). Using animal-mounted sensor technology and machine learning to predict time-to-calving in beef and dairy cows. *Animal*, *14*(6), 1304–1312. https://doi.org/10.1017/S1751731119003380

Miller, T. H., Gallidabino, M. D., MacRae, J. I., Owen, S. F., Bury, N. R., & Barron, L. P. (2019). Prediction of bioconcentration factors in fish and invertebrates using machine learning. *Science of the Total Environment*, *648*, 80–89. https://doi.org/10.1016/j.scitotenv.2018.08.122

Peng, Y., Rysanek, A., Nagy, Z., & Schluter, A. (2018). Using machine learning techniques for occupancy-prediction-based cooling control in office buildings. *Applied Energy*, *211*, 1343–1358. https://doi.org/10.1016/j.apenergy.2017.12.002

Raissi, M., & Karniadakis, G. E. (2018). Hidden physics models: Machine learning of nonlinear partial, differential equations. *Journal of Computational Physics*, *357*, 125–141. https://doi.org/10.1016/j.jcp.2017.11.039

Rapuzzi, R., & Repetto, M. (2018). Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model. *Future Generation Computer Systems*, *85*(8), 235–249. https://doi.org/10.1016/j.future.2018.04.007

Tian, Y., He, Y. L., & Zhu, Q. X. (2020). Soft sensor development using improved whale optimization and regularization-based functional link neural network. *Industrial & Engineering Chemistry Research*, *59*(43), 19361–19369. https://doi.org/10.1021/acs.iecr.0c03839

Xi, R., Yun, X., & Hao, Z. (2019). Framework for risk assessment in cyber situational awareness. *IET Information Security*, *13*(2), 149–156. https://doi.org/10.1049/iet-ifs.2018.5189

Xu, W. (2018). Study on trust model for multi-users in cloud computing. *International Journal of Network Security*, *20*(4), 674–682. https://doi.org/10.6633/IJNS.201807 20(4).09)

Yang, S., Yin, D., Song, X., Dong, X., Manogaran, G., Mastorakis, G., …, & Batalla, J. M. (2019). Security situation assessment for massive MIMO systems for 5G communications. *Future Generation Computer Systems*, *98*, 25–34. https://doi.org/10.1016/j.future.2019.03.036

Wang, Y., Shi, Y., Cai, M., & Xu, W. (2020). Predictive control of air-fuel ratio in aircraft engine on fuel-powered unmanned aerial vehicle using fuzzy-RBF neural network. *Journal of the Franklin Institute*, *357*(13), 8342–8363. https://doi.org/10.1016/j.jfranklin.2020.03.016

Zhang, J., Jia, Y., Zhu, D., Hu, W., & Tang, Z. (2019a). Study on the situational awareness system of mine fire rescue using faster ross girshick-convolutional neural network. *IEEE Intelligent Systems*, *35*(1), 54–61. https://doi.org/10.1109/MIS.2019.2943850

Zhang, Y., Ren, W., Zhu, T., & Ren, Y. (2019b). SaaS: A situational awareness and analysis system for massive android malware detection. *Future Generation Computer Systems*, *95*, 548–559. https://doi.org/10.1016/j.future.2018.12.028

How to Cite: Chen, Z. (2022). Research on Internet Security Situation Awareness Prediction Technology Based on Improved RBF Neural Network Algorithm. *Journal of Computational and Cognitive Engineering* 1(3), 103–108, https://doi.org/10.47852/bonviewJCCE149145205514