Applied Mathematics and Nonlinear Sciences

<https://www.sciendo.com>

Network monitoring and processing accuracy of big data acquisition based on mathematical model of fractional differential equation

Ming Si^{1†}, Xiaoteng Liu¹, Adel A. Bahaddad², Moaiad Ahmad Khder³¹ Xinxiang Vocational and Technical College, Teachers College, Xinxiang 453000, China² Department of Information System, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia³ Applied Science University, Al Eker, Kingdom of Bahrain

Submission Info

Communicated by Juan Luis García Guirao

Received June 17th 2021

Accepted September 24th 2021

Available online December 27th 2021

Abstract

Aiming at the lack of subjectivity of the network security situation assessment method and the complexity and non-linearity of data obtained through situational factors, a fuzzy neural network security situation which is optimised based on an improved gravitational search algorithm combined with fractional differential equation analysis, as an Evaluation model, is proposed. In order to quickly and accurately predict the situation value of the network security situation at that moment, a method for situation prediction of long-term and short-term memory networks based on an improved Nadam algorithm to optimise the online update mechanism is proposed. Note that the situation time series obtained from online assessment cannot be used in a better and efficient manner. The model can minimise the cost function and update the model more effectively by updating the model parameters online Prediction accuracy. In order to improve the problem of slow convergence speed during model network training, the Look-ahead method is used to improve Nesterov's adaptive gradient momentum estimation algorithm to accelerate the model's convergence. Finally, the simulation results analyse and compare the prediction model, which not only improves the convergence speed of the prediction model, but also greatly reduces the prediction error of the model.

Keywords: fractional differential equation, big data acquisition, network monitoring**AMS 2010 codes:** 12H99

1 Introduction

In the era of big data, the network can collect various types of data formats, including network device log, security device log and information running in the service system. Therefore, the information age should have

[†]Corresponding author.Email address: xyssm@126.com

more sources for network security situation awareness than the past. Another feature of big data is the rapid processing of massive data. Parameters of network traffic and network data can be analysed in depth [1–5]. Computing resources need to meet the needs of highly intelligent algorithm model. There are four main aspects of network security analysis: first of all, through the study of network attack cases, establishing a knowledge base, including principles, characteristics, environment, methods and the most commonly used equipment. Second, the knowledge base of environmental vulnerabilities is established by analysing the system vulnerabilities. Third, by analysing the architecture topology and equipment, the environmental threat knowledge base is established [6–8]. Finally, by analysing and comparing these three kinds of knowledge bases, the validity of security events is confirmed and then analysing the historical security events to identify network attacks that affect the current network is done. Finally, security status evaluation elements are generated, including security threats, vulnerabilities and operating conditions [9, 10].

The Internet has brought the third wave of development of the global information industry [11]. Closer collaboration among users, networks and sensing devices provides opportunities for the growth of malware and web pages. In the report released online, a total of 1,509,934 new malware were found in the first half of 2017, which means that 8,342 new types of malware are generated on average every day. In China, the number of network crimes is increasing, involving denial of service, intrusion attempt, malicious code, spam and other types of attacks; the total number of cases reached 10,636. The growth in the numbers of crimes has brought severe challenges and network security problems. In addition, most defence factors can directly respond to these attacks without any early warning assessment, resulting in a large number of positive and negative reactions. Situational awareness is a global concept. Based on the recent research and analysis, a multi-level conceptual model of network security situation awareness is proposed. The model is divided into three layers, as shown in Figure 1.

Fig. 1 Network security situation awareness model

Reasonable anti-virus measures must be based on an in-depth understanding of computer virus epidemic information and controlling virus epidemic factors. JO Kephart proposed a new anti-virus mechanism called the killer signal (KS) (warning for possible infection). During the virus epidemic, the signal KS will be released from the infected computer to other computers on the network. Once the KS is successfully received, the infected computer may get rectified immediately and try to send a KS signal to its neighbours. The susceptible computer also obtained an antidote programme from KS. Ren Jianguo and Xu Yonghong described the KS early warning mechanism from a mathematical point of view, and proposed the SEIR-KS model based on the SEIR model as shown in Figure 2. Studies in recent years show that fractional calculus is widely used in the field of

image processing and has achieved good results. For example, it is used in the fields of image denoising, image enhancement, image registration and image repair. This is because the fractional differential has the following excellent characteristics: first, the integer order differential is widely studied, and the fractional order is an extension of the integer order; it can make the calculus order to have a better continuity; the fractional order operation range can be expanded. Second, fractional calculus can enhance the information in the middle and high frequency regions, while retaining the information in the low frequency regions.

Fig. 2 SEIR-KS computer virus propagation model. KS, killer signal

With the rapid development of network attack technology, the characteristics of network attack are complexity, diversity and speed. Traditional network security technology cannot solve these problems and thus network security problems have become more serious. Although most security devices have the function of recording security events and security logs, security devices are independent of each other, hence security information is scattered and cannot be shared. Once an attack occurs, it is difficult for the security administrator to take appropriate measures according to the security information. Security visualisation technology makes it easier for people to understand network security information, find abnormal values or errors in data, find new attack patterns and then conduct security defence.

Therefore, it is very important to study network security situation awareness technology. Data fusion technology is one of the key technologies of network security situation. It collects different security devices and converts them into standard data formats to monitor security logs or warnings. From the historical analysis of security events, we can know that the prediction of network conditions is accurate. After network security data fusion, a large number of data need to be calculated by a specific mathematical formula to obtain a certain range of values reflecting the network security status. Time. There are four main calculation methods of network security evaluation: AHP, FAHP, Delphi and comprehensive analysis, and three types of network security situation prediction namely qualitative prediction, time series and causal prediction. Combined with the current security status data of network security equipment and using scientific theory and reasonable methods, the future security threats and hidden dangers can be predicted.

2 Fractional differential equation model

Fractional calculus is essentially derived based on the integer order. Although it has been developed for >300 years, its research and improvement over a long period of time has often focused on the understanding and development of pure mathematical theory. It is relatively slow, and its application in other fields is relatively rare. It was not until 1965 when Professor Mandelbrot of Yale University combined Riemann-Liouville (RL) fractional calculus to propose a new theory of fractal. Applied to signal processing and analysis, biomedicine, electromagnetic, materials, power and other aspects, the application of fractional calculus in various fields of digital image processing has also developed rapidly in recent years. The following three are the most classic and

commonly used definitions of fractional calculus. The Grnwald-Letnikov definition is a generalisation based on the integer order. It is a more classic definition of fractional order. Here it is referred to as GL definition and according to the definition of integer order differential, in the interval ba , $[(ba, Rba)$. The memory is a function tf , continuously differentiable, and the first-order differential definition of the continuous function is as follows:

$$f'(x) = \lim_{q \rightarrow 0} \frac{f(x+q) - f(x)}{q} \quad (1)$$

In Eq. (1), Rhh represents the step size. According to the first-order differential definition above, the continuous function tf can be obtained. The second-order differential of, which is defined as follows:

$$f''(x) = \lim_{q \rightarrow 0} \frac{f'(x+q) - f'(x)}{q} = \lim_{q \rightarrow 0} \frac{f(x+2q) - 2f(x+q) + f(x)}{q^2} \quad (2)$$

By analogy, the integer order can be pushed from the first order to the n order, so that the n -th derivative of the continuous function can be obtained, which is defined as follows:

$$f^n(x) = \lim_{q \rightarrow 0} \frac{1}{q^n} \sum_{p=0}^n (-1)^p \cdot (np) f(x - pq) \quad (3)$$

By extending the integer order n to the entire real number range and introducing the gamma function, a fractional differential definition of G-L of any order can be obtained:

$${}_a^G D_t^\nu f(x) = \lim_{q \rightarrow 0} \frac{1}{q^\nu} \sum_{p=0}^{\frac{x-a}{q}} (-1)^p \frac{T(\nu+1)}{p! T(\nu-p+1)} f(x - pq) \quad (4)$$

Image repair based on the TV model will result in smooth texture transitions introduced the G-L fractional order differential into the TV repair model. This method solves the problem in smooth transition smoothly. However, this method is still not ideal for the preservation of information with texture details (such as texture details with weak derivatives), and causes computational difficulties during the minimisation of the model. Regular items and data items cannot be performed at the origin.

The main problem is the problem of differential calculation. This article proposes to introduce a minimum value during the model solving process, that is, to add a minimum value to the denominator of the regular term of formula (5), as follows:

$$-div \frac{\Delta^a u}{|\Delta^a u| + p} + \gamma_e(u - u^o) = 0 \quad (5)$$

In the formula, u is the fractional step, and p is the minimum parameter and is also the regularisation parameter. Now simplify it to get the following expression (6):

$$U_o = \frac{\sum_{x \in B} \frac{u_x}{\sqrt{|\Delta^a u_x| + p^2}} + \gamma_e(O) u_O^o}{\sum_{x \in B} \frac{1}{\sqrt{|\Delta^a u_x| + p^2}} + \gamma_e(O)} \quad (6)$$

In Eq. (6), the parameter is a fractional order. When $n = 1$, the fractional TV model is a TV model in which the integer order is replaced with a fractional order. The parameter p in the formula is the introduced minimum value, and its selection principle is given as follows: when p is relatively small, a sharp edge can be maintained; when p is large, the degree of diffusion can be made higher. Therefore, when the area of the area to be repaired is small, we choose a smaller p -value to obtain better repair results; however, when the area to be repaired is large, we should take a large p -value in the TV repair model. The p -value makes the diffusion low, which results

in smoothing the noise in the area to be repaired prior to the diffusion of the boundary information. Therefore, a relatively sharp edge is formed, which eventually leads to the wrong repair result, and thus choosing a larger p value can well avoid this problem of repairing errors.

There are three parameters, and p in the experiments in this article. The regularisation parameter determines the weight of the regular terms and data items. According to experience, $\lambda = 0.005$ is used in this article and the initial value of the parameter p is 0.05.

We can see from the amplitude-frequency characteristic curve of the fractional-order differential operator in Figures 2 and 3 that when the frequency is between 0 and 1, for the differential operator with a smaller order, the amplitude increases faster. When the frequency is >1 , the differential operator with a smaller order increases its amplitude more slowly. As the order becomes larger, the amplitude of the middle and low frequency parts increases at a faster rate.

When the order is <1 , it can be equivalent to a filter, which plays a role in enhancing the release of low and medium frequencies and compressing high frequencies. When the order is >1 , it can be regarded as a high-pass filter.

In image processing, the low-frequency part of the image corresponds to the texture information of the image and the weak edges of the image, and the contour and noise of the image correspond to the high-frequency part.

In general, the same order cannot be applied to all goals, so we have to choose different orders for different goals. For larger orders, we can effectively enhance our mid-frequency and high-frequency signals. In image repair, mid-low frequencies correspond to the smoothed part of the broken image and high frequencies correspond to the boundary part of the image. The goal of this paper is to solve the problem which is boundary is not sufficiently diffused and over-smoothed and so it is necessary to retain edge information and texture information. From the amplitude-frequency characteristic curve, we can see that when the order is between 0 and 1, the signal can be effectively enhanced. Therefore, the order in this article is recommended to be between 0 and 1. The subsequent experiments also prove the Rationality order. Assuming that there are N bodies in a search space, the position of i -th body can be defined as N . The algorithm randomly places individual parameters in the search space. In all iterations, the gravitational force of individual j at time t is defined as follows:

$$F_{jk}^d(x) = G(x) \frac{M_{pk}(x) \cdot M_{ak}(x)}{R_{jk}(x) + \varepsilon} \left(z_k^d(x) - z_k^d(x) \right) \quad (7)$$

Among them, M_{aj} is the mass of Active Gravitational individual j , M_{pi} is the mass of Passive Gravitational individual i , $G(t)$ is the gravitational constant at time t and $R_{ij}(t)$ is the Euclidean distance between i and J .

According to the gravitational formula (7), the elements in the formula are defined as follows:

Definition 1. $R_{ij}(t)$ represents the Euclidean distance between individuals i and j . The calculation formula is as follows:

$$R_{ij} = \sqrt{\sum_2 (X_i(t) - X_j(t))^2} \quad (8)$$

Definition 2. $G(t)$ indicates that the gravitational constant is a function of the initial value G_o and time t . The calculation formula is as follows:

$$G(t) = (G_o, t) = G_o \cdot \exp\left(-a \cdot \frac{t}{T}\right) \quad (9)$$

Among them, a and G_0 are the descent coefficients and initial values, t is the current number of iterations and T is the maximum number of iterations.

Definition 3. M_{aj} and M_{pj} respectively represents the mass of active individuals and the mass of passive individuals. The calculation formula is as follows:

$$M_{aj} = M_{pj} = M_{ii} = M_i, \quad i = 1, 2, I \quad (10)$$

The importance of the fitness function is based on the search path. The goal here is to minimise errors, so the fitness function is mathematically expressed as:

$$fitness = \min(Error) = \frac{1}{2} \sum_{i=1}^p (t(i) - I(i))^2 \quad (11)$$

Among them, t_i and O_i are both the expected output and the actual output of neuron i in the output layer. According to the minimisation problem, the best and worst fitness are:

$$best(g) = \min fit_j(g), \quad j \in 1, \dots, I \quad (12)$$

$$worst(g) = \max fit_j(g), \quad j \in 1, \dots, I \quad (13)$$

Among them, $\max fit_j(g)$ and $\min fit_j(g)$ represent the maximum and minimum fitness values of the j -th parameter during g iterations,

$$m_i(g) = \frac{fit_i - worst(g)}{best(g) - worst(g)} \quad (14)$$

$$M_i = \frac{m_i(g)}{\sum_{j=1}^I m_j(g)} \quad (15)$$

In order for GSA to be random, the total force acting on individual i in the d dimension is defined as the random weighted sum of the d -th component of the force from other individuals as:

Among them, K is the K individual with the best fitness value and maximum quality. K decreases in each iteration, and only one individual exerts force on other individuals at the end.

3 Results analysis

For the security and stability of the entire Internet, it is necessary to improve the legal system and the security and comprehensive design of computers, servers, software, and hardware. Otherwise, it will be difficult to eliminate risk factors because of the open environment of the Internet. The continuous development of Internet technology requires better management and situational awareness detection capabilities, so management and information of real-time attacks are required as well as vulnerability detections and possible attack predictions. In order to make it easier for security administrators to detect network situations, the concept of network security situation awareness is proposed, which is to extract the situational elements, evaluate the network security situation and predict the situation value at that instant. Network security situation assessment is to analyse and evaluate the security situation of the network system, fully understand the threat of the network system, judge the vulnerability of the network and quantitatively evaluate the network situation value. The fundamental purpose of network security situation assessment is to realise the security of network systems through scientific methods and procedures. Based on the evaluation results, the risk of the entire network is minimised.

The validity and superiority of the LAHP-IGFNN-based situation assessment method is verified using the LLDOS1.0 attack scenario in the DARPA2000 dataset [?] as the background. By placing the data set in the network scenario shown in Figure 3, the quantitative data of threat attacks on this network scenario is taken as experimental data every hour. By simulating the attack values of the network affected by the threat attacks in the network scenario at each moment in 24 h, and further Trend situation, a method to verify the situation assessment method is proposed in this article. The attack scenario model is shown in Figure 3.

Fig. 3 Network scenario

Through the analysis of the influencing factors of the attack on the network system, the effectiveness of the improved AHP (LAHP) in the calculation of the weight of the network index is verified and compared with the traditional AHP to verify the superiority of LAHP. Looking at the table, we can know the random consistency index RI 1.12 of the scale, and the simulation results can be used to compare the consistency ratio (CR) obtained by the two methods of LAHP and AHP.

Table 1 Comparison of consistency analysis

algorithm	LAHP	AHP
α max	4.92	5.07
CI	0.001	0.004
CR	0.0019	0.0024

According to the simulation results, when $CR \leq 0.1$, it can be judged that the inconsistency of the judgement matrix is within an acceptable range, and there is a good consistency, which verifies the effectiveness of LAHP. Therefore, not only can we see that LAHP can solve the subjective experience problem, but also the index of consistency of LAHP is smaller than that of traditional AHP on the index. It is also verified that the consistency of the matrix obtained by the LAHP method in this article is smaller and found that the consistency of the calculated judgement matrix is better.

An IGSA-optimised FNN evaluation model is proposed here. By improving the updated formula of the GSA algorithm, it solves the problem of being easily trapped into a local optimum, and improves the convergence speed to reach convergence faster. By using the basic FNN model and GSA-FNN proposed in this paper, the model, improved GSA-FNN model and PSO-FNN model are compared for simulation. The main parameters of FNN in the experiment are: the dimension of the input sample is 4, the dimension of the output sample is 1, the number of hidden nodes is 8, the maximum number of iterations is 200 and the learning rate is 0.35.

In order to verify the effectiveness of the NAWLILSTM prediction method, the experiment uses the historical log information of a network company's firewall, IDS, etc. and used the data collected for 95 days from July to September to conduct experiments on the original data set. Information is collected once for the sample. Note that 177 days is used as the training set for the LSTM model and 78 95 days is used as the model's prediction set while the original data is used to quantify the original data to obtain the network security posture value. The important parameters of ILSTM in the experiment are: n input = 28, n steps = 28, n hidden = 128, n chasses = 10, and batch size = 128.

Analysing the time complexity according to the algorithm steps described above, we can get the equation $O(K(H + CS + (H + 3SC)I)) = O(KW)$, where K is the number of output units and C is the storage unit block, S is the size of the storage unit block, H is the number of hidden layers, I is the number of forward connection units with memory cells, gate units, and hidden units, $W \leq K(H + CS) + (H + CS + 2C)I$ is the weight. The above expression is obtained by considering the calculation of all the derivatives of the output unit in terms of

weight: $H + SC$ is the number of directly connected output units, CSI is the number of connected memory cells, HI is the number of hidden layers and $2CI$ is the connection gate of the number of units. Since a single gate unit affects S memory cells, the block size is summed by the chain rule: the derivatives of all the output units leading to the gate unit can be calculated as complexity $2CIS$. It can be concluded that by giving N memory cells, the algorithm complexity of ILSTM can be calculated as $2ON$.

As shown in Figure 4, the output error of the standard FNN model quickly begins to decline. When the decline rate reaches the maximum, the training is at the 11th iteration, and then gradually decreases so that the curve is a soft curve. It reaches convergence when it is trained to 93 times, and then decreases to reach. The minimum and minimum training error is 0.0346. The other three optimised FNN algorithms show good performance in early iterations. In the first 30 trainings, the disadvantages of premature convergence of the standard FNN algorithm and local optimisation are avoided. In 38 training sessions, the gradients on the left and right sides descend to depth optimisation. But the GSA-FNN algorithm also failed to jump out of the local optimum. It stabilises after 70 iterations and the minimum training error is 0.0156. The PSO-FNN algorithm slowly converged after 83 iterations, with a minimum error of 0.0218. However, the IGSA-FNN algorithm of the proposed method is reduced again in a short time, and then enters the full optimisation, which solves the problem of local optimisation. Finally, it started to converge at 69 times, and it also enters the convergence state earlier than the other two optimisation algorithms in terms of convergence speed. By improving the convergence speed of the algorithm, the training error has become 0.0108.

Fig. 4 Convergence comparison of each optimisation algorithm

The fitness curves of the two GSA optimisation algorithms are shown in Figure 5. It can be seen that the fitness curve of GSA-FNN converged faster in the first 10 iteration cycles, but basically flat in the later period and after that the fitness value no longer changes. The early convergence speed of the improved GSA-FNN fitness curve is not as good as that of the unimproved GSA-FNN, but it has been reducing. The results show that the algorithm can effectively balance the global and local optimal performance of the parameters during the training process. After the parameters are searched, the final fitness value is less than the unimproved gravitational search algorithm, and it enters a convergence state with other optimisation algorithms earlier to reduce the convergence speed of the algorithm.

By inputting the data set DARPA2000 into the network scenario in Figure 3, the situation values of the network under five major types of attacks such as DDos and U2R are recorded at every moment in 24 h. The 24 h is divided into 8 equal parts, that is, every 3 h, the network situation is calculated. According to the above method, the situation value is obtained by calculating four first-level indicators. The initial settings of the operating system, device model and network bandwidth of each host in the experimental environment are basically the same. The situation assessment method of LAHP-IGFNN proposed is basically the same. The security situation value of each host is calculated in the network system, as shown in Figure 6:

Fig. 5 Fitness curve of GSA-FNN before and after improvement

Fig. 6 Host security posture

It can be seen from Figure 6 that the host posture is mainly caused by external threat attacks in the experimental environment. Hosts d1 and d2 are hardly threatened by network attacks, and their posture values have not changed much. The hosts d3 and d4 generate vulnerability information in the period of 9–15 h, causing the situation values of the hosts d3 and d4 to rise to a more dangerous state. The host d5 has a higher posture value than other hosts in the 1–6 h period because the host has not taken any security protection measures. During the period of 18–21 h, host d5 is under threat and the security posture value changes significantly, and thus the host d5 network security status is more dangerous. When the analysis results are obtained through the evaluation method, the data obtained by the network administrator will take network security remedial measures to eliminate threat attacks and prevent further attacks on the network.

When the original TV model is used to repair the image, when the local area of the image has a large gradient, the diffusion often stops, which leads to the problem of local optimisation. So, we propose a TV model repair algorithm based on an improved diffusion coefficient. The algorithm constructs a new three stage diffusion coefficient function and combines it with the TV model's gradient descent equation, thereby solving the problem of the original TV model's diffusion stop at large gradients, and also enabling the image to be repaired. In the implementation, the edge area diffusion is small and the smooth area diffusion is large. The edge model and step effects in image restoration are overcome and the accuracy of image restoration is improved. It can be concluded from the experimental results that the improved model in this article can better deal with edge blurring and excessive unnatural phenomena and the repair accuracy has been greatly improved compared with

other related methods. However, since the diffusion coefficient uses three piecewise functions, the repair time is slightly increased. However, the algorithm used in this article is improved by fusing the diffusion coefficients. For the images to be repaired, there is a problem that the information such as texture details and weak edges with weak derivatives are not kept sufficiently, which limits the application of the algorithm.

The security situation of the entire network system can be obtained by calculating the weight value of each host and the situation value of the host. And compared with the situational values obtained by the evaluation methods in [?, ?], the weight values of the host are the same fixed values used in the method [?, ?]. The comparison of the network system situation values of the method is shown in Figure 7. As can be seen from Figure 7, as the evaluation method of the fuzzy neural network is adopted in this article, the complex situational element data obtained by the processing of the fuzzy neural network is highly recognisable. Further, the judgement matrix obtained by the LAHP method reduces subjectivity. It can be seen that the network situation value of our method is significantly higher than the literature and slightly higher than the network situation value obtained by the method of literature.

Fig. 7 Network system security situation

This paper proposes a network security situation assessment method based on linear programming (LP) combined with AHP method combined with improved GSA optimised FNN. First, the method solves the subjectivity problem that requires expert experience to give a judgement matrix through LP combined with the AHP method, and improves the consistency of the judgement matrix, so that it can obtain more objective and reasonable first-level index weight values. Then, we also improved the GSA optimisation algorithm to solve the problems of slow convergence and easy to fall into local optimisation. Through simulation, we compared the fast convergence with the unimproved GSA and PSO optimisation algorithms, and also entered the parameters for the global optimisation.

After many experiments, when the value of α is at 0.1 and k is equal to 1, the MSE value is the smallest and the PSNR value is the largest. That is, when the template is 3 and the order α is equal to 0.1, the repair effect is the best.

This image has a lot of texture information. Considering the template size of 3×3 selected in this experiment. When the order is relatively large, for a weakly textured image, a higher order will cause high-frequency signals to be blurred (such as edge information), so the repair effect is not particularly ideal and hence the order of α equal to 0.1 works best. The comparison is more reasonable. In weakly textured images, the gradient information in the middle and low frequency regions is weak, so there is a need to enhance it. After many experiments, the restoration effect is best when the texture direction of the Barbara picture is (1, 1). Therefore, when the template is 33 and the order is equal to 0.1, each index reaches the best, that is, the repair effect is the best.

In order to reflect the advantages of the proposed method, the four most commonly used prediction models,

LSTM, RBF, and SVM, which have not been improved, are compared with the methods proposed in this article, as shown in Figure 8. It can be concluded from the figure that all prediction methods can handle historical data well, but several traditional prediction results are not good as more online data is used to update the parameters of the ILSTM prediction model. It can be seen in the figure that the predicted value of the method is closer to the actual value than other prediction methods, and other methods have different degrees of error from the actual value. Therefore, the method can make good use of online data to improve prediction accuracy and the experimental results verify the effectiveness of the algorithm.

In order to evaluate the prediction performance of different prediction models more comprehensively, a comparative analysis is performed from two aspects of the mean square error and the average relative error, as shown in Figure 8. It can be found in the figure that compared with the traditional LSTM, RBF, and SVM, the ILSTM prediction model can obtain results closer to the real network and the prediction error is relatively smaller. It shows that the proposed prediction model has better prediction performance and is closer to the actual network security situation time series.

Introducing the GL fractional order differential into the TV model, on the one hand, introduced the extremely small parameter values α in the gradient calculation process, which overcomes the problem that the regular term and the data term are not differentiable at the origin, and increases the stability of the model, which can make the model more stable. The weak derivative property of the texture area is well maintained; on the other hand, the texture direction of the area to be repaired is determined according to the prior of the known area of the image during the repair process, making full use of the texture details and weak edge information in the image, thereby improving Repair accuracy.

In addition, the relationship between repair effect, order and template width k is given through experiments, which provides a basis for selecting the best template parameters. In addition, we can also get from experiments: although the best parameters of different types of images are different, the best repair order is generally between 0 and 1 as the smooth part of the image corresponds to the low frequency part of the signal. The texture details of the image correspond to the intermediate frequency part of the signal and the TV algorithm is not ideal for the repair of weakly textured areas. To enhance the gradient information in this area, the low frequency and intermediate frequency parts need to be improved. Therefore, it is better to use the order between 0 and 1. Both theoretical analysis and experimental results show that the algorithm used by us can improve the repair accuracy of weak textures and weak edge images, which is an important extension and extension of the TV model. In the process of traditional image repair, iterative gradient descent is usually used to repair the image. For each newly input image to be repaired, it is necessary to iteratively optimise the objective function to achieve the repair, which severely limits its speed. It also ignores the inherent pattern of sharing when dealing with the same data set. The deep learning method can automatically learn the effective information in the complex to-be-repaired image, and during the repair process, the calculation has better parallelism. Compared with the traditional method, it has a simpler execution and faster operation. Subsequent consideration can be given for the usage of deep learning for image repair.

BP neural network, also known as backpropagation network, is a multilayer feedforward neural network. It consists of input layer, output layer and many number of hidden layers. The input layer divides the input vector into every neuron in the hidden layer to balance the network load. The hidden layer is the main structure of knowledge acquisition network. The output layer and hidden layer use the s activation function. The output layer is the process of network output format. The defects of BP algorithm are more obvious in two aspects. First of all, learning time is too long. The traditional BP algorithm has a fixed step size. When the error is large and the learning rate is correct, the optimal solution will not be very fast. The second is the local minimum problem. In the description of surface error, there are many pits, and the error is increasing in all directions at the bottom of the pit, which is not the best solution for the whole.

RBF neural network has the best approximation performance and global optimality, and can approximate any continuous function with any precision. However, based on the evaluation results of clustering algorithm, the centre value of RBF neural network algorithm and the key parameters of RBF hidden layer are determined.

Fig. 8 Comparison of situation values predicted by different algorithms

Fig. 9 Error comparison of different prediction models

This results in unstable results, because in some isolated cases, clustering algorithm is easy to fall into the local optimisation problem, and changes the data processed by the real-time situational awareness application centre.

LP is a mathematical technique used for quantitative analysis to solve problems with linear objective functions and linearly constrained objectives. LP technology is similar to the problem that evaluators must allocate scarce resources in competitive activities to optimise measurable goals. The main purpose of adding LP to the AHP that solves the problem of index weight allocation is to select the optimal contrast matrix based on the quantified value of the index system established to evaluate the network situation.

Each LP problem consists of four main parts, namely decision variables, objective functions, constraints and variable boundaries. The decision variables used in the established index system for situation assessment include stability, threat, vulnerability and disaster tolerance. They represent a number of attributes related to the affected network situation. There are four objective functions used to solve the optimisation values of the decision variables. The AHP method has a four-step process. The first step is to build the problem into an independent standard decision hierarchy according to the priority score of the problem standard. The second step is to create a pairwise comparison matrix for each option on each criterion. The third step is the dual comparison matrix. The average value of each row in the normalisation matrix is used as the weighting factor for each optional item of the standard. The fourth step is to synthesise the results by checking for consistency.

4 Conclusion

To solve the inability to effectively deal with the complexity of the network system data and the analytic hierarchy process requires expert experience to obtain a judgement matrix. This paper uses an improved analytic hierarchy process and a network security situation assessment method combined with an improved gravitational search algorithm. First, in order to change the subjectivity of the AHP method, a comparison matrix can be calculated using improved LP, rather than obtained from expert experience; then, in order for FNN to better handle high-complexity input, output and nonlinear mapping, we propose improved gravitational search algorithm that can avoid the algorithm from falling into local optimum problem and improve the convergence speed of FNN. The method is used to simulate and evaluate the network security situation, and the convergence analysis is compared. The results show that the algorithm has better convergence and the effectiveness of the evaluation method. Note that the research on the two key steps of situation assessment and situation prediction on network security setting bring awareness and achieve results.

References

- [1] Dusunceli F. New Exact Solutions for Generalized (3+1) Shallow Water-Like (SWL) Equation[J]. *Applied Mathematics and Nonlinear Sciences*, 2019, 4(2):365-370.
- [2] Harisha, Ranjini P S, Lokesha V, et al. Degree Sequence of Graph Operator for some Standard Graphs[J]. *Applied Mathematics and Nonlinear Sciences*, 2020, 5(2):99-108.
- [3] Yang J, Ma Y, Yun L. Analysis of hot events based on the big data acquisition system[J]. *C e Ca*, 2017, 42(1):415-419.
- [4] Nguyen H, Cao J. Trustworthy answers for top-k queries on uncertain Big Data in decision making[J]. *Information Sciences*, 2015, 318:73-90.
- [5] Liang J, Gong J, Sun J, et al. Automatic Sky View Factor Estimation from Street View Photographs—A Big Data Approach[J]. *Remote Sensing*, 2017, 9(5):411.
- [6] Won K, Sim C. Automated Transverse Crack Mapping System with Optical Sensors and Big Data Analytics[J]. *Sensors*, 2020, 20(7):1838.
- [7] Palmer A D, Alexandrov T. Serial 3D Imaging Mass Spectrometry at Its Tipping Point[J]. *Analytical Chemistry*, 2015, 87(8):4055-62.
- [8] X Li, Zhao N, Jin R, et al. Internet of Things to network smart devices for ecosystem monitoring[J]. *ence Bulletin*, 2019, 64(17):1234-1245.
- [9] Xu J, Wang L, Shen Y, et al. Family-Based Big Medical-Level Data Acquisition System[J]. *IEEE Transactions on Industrial Informatics*, 2019, 15(4):2321-2329.
- [10] Prüfer, J., & Prüfer, P. Data science for entrepreneurship research: studying demand dynamics for entrepreneurial skills in the Netherlands. *Small Business Economics*., 2020. 55(3): 651-672.
- [11] Arvidsson, H. G., Coudounaris, D. N., & Arvidsson, R. The shift from causation to effectuation for international entrepreneurs: Attitudes and attitude change versus social representations. *International Journal of Entrepreneurship*., 2020. 24(3): 1-23.

This page is intentionally left blank