Digital Communications and Networks 2 (2016) 139–144

HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.elsevier.com/locate/dcan

A network security situation prediction model based on wavelet neural network with optimized parameters

Haibo Zhang [a,b], Qing Huang [a,*], Fangwei Li [a], Jiang Zhu [a]

[a] Chongqing Key Lab of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[b] Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27695, USA

ARTICLE INFO

Article history:
Received 11 March 2016
Received in revised form
14 June 2016
Accepted 26 June 2016
Available online 9 July 2016

Keywords:
Network security
INGA
Situation prediction
WNN
Adaptive genetic algorithm

ABSTRACT

The security incidents ion networks are sudden and uncertain, it is very hard to precisely predict the network security situation by traditional methods. In order to improve the prediction accuracy of the network security situation, we build a network security situation prediction model based on Wavelet Neural Network (WNN) with optimized parameters by the Improved Niche Genetic Algorithm (INGA). The proposed model adopts WNN which has strong nonlinear ability and fault-tolerance performance. Also, the parameters for WNN are optimized through the adaptive genetic algorithm (GA) so that WNN searches more effectively. Considering the problem that the adaptive GA converges slowly and easily turns to the premature problem, we introduce a novel niche technology with a dynamic fuzzy clustering and elimination mechanism to solve the premature convergence of the GA. Our final simulation results show that the proposed INGA-WNN prediction model is more reliable and effective, and it achieves faster convergence-speed and higher prediction accuracy than the Genetic Algorithm-Wavelet Neural Network (GA-WNN), Genetic Algorithm-Back Propagation Neural Network (GA-BPNN) and WNN.

1. Introduction

With the social development and greater communication requirements among people, big data increasingly becomes a cornerstone technology for our lifestyle [1–3]. The network plays a more and more important role in our daily life, including computer networks, wireless communication networks, etc. [4–6]. Correspondingly, the network-attack becomes more frequent and harmful when people get online to transmit and receive private data. According to the existing literature, it is very hard to solve these security problems only by the single defense method. Under such a tough environment, The Network Security Situation Awareness (NSSA), a comprehensive technology which obtains and processes the security information, has received extensive attention [7–9].

The research on NSSA mainly focuses on three stages. The 1st stage is the extraction of the network security situational factors [10,11], the 2nd stage is the assessment of network security information [12,13] and the 3rd stage is the Network Security Situation Prediction (NSSP) [14]. The NSSP, as the final step of the whole situation awareness, analyzes and deals with the previous and current situation information, and then makes a prediction for the future. To solve a series of technical problems in the situation prediction, a lot of scholars began taking some in-depth exploration into prediction methods. The authors of [15] built a Hidden Markov Model to connect the past and future information in NSSA, then predicted the future security situation reliably. The authors of [16] analyzed the characteristics of the network situation, and proposed a prediction model based on a generalized regression neural network. The authors of [17] used the residual error correction function of the interval Verhulst model to explore the rule of network situation, and then introduced grey theory. The authors of [18] constructed an evaluation model of the hierarchical network structure and used a support vector machine (SVM) to predict the nonlinear characteristics for the network situational value. In addition, many various prediction methods were introduced in [19–21]. However, the scale of networks are getting larger and larger, these traditional prediction algorithms mentioned above have some problems, such as the low prediction accuracy and slow convergence speed. Also it is easy to fall into premature convergence. As a result, the prediction results cannot properly reflect the network security situation. The administrators cannot make reasonable decisions.

* Corresponding author.
E-mail addresses: zhanghb@cqupt.edu.cn (H. Zhang), huangq46@163.com (Q. Huang), lifw@cqupt.edu.cn (F. Li), zhujiang@cqupt.edu.cn (J. Zhu).

Peer review under responsibility of Chongqing University of Posts and Telecommunications.

http://dx.doi.org/10.1016/j.dcan.2016.06.003

In addition, because the Artificial Neural Network (ANN) has some potential advantages, including high adaptability, self-learning ability and good nonlinear-approximation ability, it has been widely used in the field of NSSA [22,23]. However, the traditional solutions to get the parameters for the ANN may produce some deviations. So the widely used artificial intelligence optimization algorithm was introduced, which optimizes the parameters of ANN and was generally applied to all kinds of models of ANN. Some scholars began to gradually research the combination of a intelligent optimization algorithm and ANN and obtained some better results. In order to predict the network security situation, a quantitative prediction method of the network security situation based on Wavelet Neural Network (WNN) was proposed, where the gradient descent method was adopted to train and optimize the parameters of WNN [24].

However, the network security situation prediction is an emerging technique and has many research contents unsolved until now. In this paper, in order to provide more effective and accurate prediction, an improved niche genetic algorithm is introduced to optimize the WNN prediction model. Firstly, WNN with better non-linear capability and approximation speed is adopted for prediction rather than a BP or RBF neural network. Secondly it uses the adaptive genetic algorithm to optimize the parameters of WNN, which has strong global searching ability. Thirdly, to solve the problems such as slow convergence speed and premature convergence from traditional adaptive genetic algorithms, we introduce a dynamic fuzzy clustering niche technology [25,26], which assists the predict model. In addition, it knocks out the niche to maintain the population diversity, and increases convergence speed, and avoids premature convergence. Ultimately, the better prediction is achieved.

2. INGA-WNN prediction model

2.1. WNN modeling

WNN is generally divided into relax-type and close-type by the different wavelet-basis functions. And our prediction adopts the close-type with a three-layer feed-forward neural network. In our model, we assume that the network topology appear as is shown in Fig. 1, and there are m nodes in the input layer, h nodes in the hidden layer and n nodes in the output layer. The input samples are denoted by X_1~X_m, the output samples are denoted by Y_1~Y_n. The stretching and translating parameters are denoted by a_1~a_h, b_1~b_h respectively. The link-weights in the network between the input layer to hidden layer and the hidden layer to output layer are denoted by w_{11}~w_{mh}, w'_{11}~w'_{hn} respectively.

For the hidden layer, we select *Morlet* as the mother wavelet function, the equation is shown as follows:

$$\psi(x) = \cos(1.75x)\exp(-x^2/2) \tag{1}$$

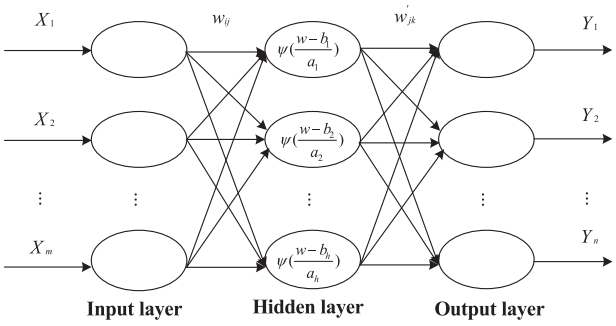

Fig. 1. Network topology of WNN.

According to Kolmogorov theory, the number of hidden layer nodes h is determined by the number of input layer nodes m. The calculation equation is

$$h = 2m + 1 \tag{2}$$

The sigmoid function is still used as the activation function shown as follows

$$g(x) = 1/[1 + \exp(-x)] \tag{3}$$

where x in (1) and (3) denotes the data of the previous layer.

By the wavelet basis function, the output results of WNN are

$$Y_t = \sum_{s=1}^{h} w'_{st}\psi\left(\frac{\sum_{r=1}^{m} w_{rs} - b_s}{a_s}\right) \tag{4}$$

Usually, the gradient descent method is used to calculate the network connection weights, by which the parameters in WNN are more accurate than before. However, the extreme value point from this method is just the approximate value. Meanwhile, it is vulnerable to the local optimal network problem. So we prepare to use the Improved Niche Genetic Algorithm (INGA) for optimizing the local network parameters.

2.2. INGA algorithm

Based on the principle of natural selection also referred to as survival of the fittest, the Genetic algorithm (GA) originated in the 1960s, which is a global optimization algorithm. GA is a probability optimization algorithm, and has great advantages in terms of parallelism and expansibility. So the algorithm is a good option for dealing with nonlinear problems. We can quickly obtain the global optimal solution for large-scale networks.

GA is mainly used to simulate the survival process of chromosomes. The process includes five steps: encoding, the determination of the fitness function, the genetic selection, crossover and mutation. Encoding makes the problem in the form of code and presents it to the computer. This paper adopts the real-number encoding. After completing encoding, this algorithm realizes a series of operators such as selection, crossover and mutation. Through the comparison of fitness and Iterative optimization, we will find the code of the optimal solution.

- Fitness function
  The increasing fitness value determines the evolutionary direction of GA. The error E of WNN is defined as the individual fitness function:

$$E = \frac{1}{2}\sum_{t=1}^{n}(Y_t - Y'_t)^2 \tag{5}$$

$$f = \frac{1}{1+E} \tag{6}$$

  where Y_t denotes the real value of the t th output node and Y'_t denotes the predicting output.
- Genetic selection
  The most common selection operation is the roulette selection. However, in order to avoid damaging the best individual in a small sample size, the prediction model adopts the expectation value method for selection. The expectation value is calculated by (7). Thus, the probability problem is converted into the frequency problem. Meanwhile, the retention mechanism of the superior individual directly preserves the contemporary highest fitness value of the individual for the next generation.

$$q_i = \frac{f_i}{f_{sum}/N}, \quad i \le N \tag{7}$$

where f_{sum} denotes the sum of individual fitness values in the population. f_i denotes the ith individual fitness value. N denotes the total number of individuals in the population. Also, q_i needs to be rounded.

- Genetic adaptive crossover and mutation

The choice of parameters is very important in the simulation process of GA. For the fixed values, the classic GA always relies on the crossover and mutation probability. But it can't dynamically adjust the probability in an evolution-processing population, and the convergence speed is not stable. In addition, in order to deal with the crossover operator and mutation operator, this paper utilizes the adaptive method. The adaptive probability p_c and p_m are defined in Eqs. (8) and (9).

$$p_c = \begin{cases} \alpha_1 - \dfrac{(\alpha_1 - \alpha_2)(f_{max} - f')}{f_{max} - f_{avg}}, & f' \ge f_{avg} \\ \alpha_2, & \text{else} \end{cases} \tag{8}$$

$$p_m = \begin{cases} \beta_1 - \dfrac{(\beta_1 - \beta_2)(f_{max} - f)}{f_{max} - f_{avg}}, & f \ge f_{avg} \\ \beta_2, & \text{else} \end{cases} \tag{9}$$

where α_1, α_2, β_1, β_2 denote a random value between [0, 1] respectively. In this paper, we assume that $\alpha_1 = 0.8$, $\alpha_2 = 0.5$, $\beta_1 = 0.05$, $\beta_2 = 0.001$. f_{max} denotes the largest individual fitness value in the population. The average individual fitness value is denoted by f_{avg}. The parent fitness value before the crossover operation is denoted as f'. And f denotes the fitness value which belongs to the mutate individual. Assuming that $N \times m \times n$ data are randomly generated by the initial population, the complexity of the algorithm is $O(m^2 \times n^2)$.

- An improved niche technology

The premature convergence indicates the decreasing diversity of the population. At the select stage of the genetic operation, there is a problem when a special individual's fitness value is much higher than the average fitness value. The number of individuals in the population will rise sharply, and even dominate the entire population. However, the crossover operation and mutation operation cannot jump out of the state effectively. In order to solve the premature convergence of the classic GA, this paper introduces a dynamic fuzzy clustering niche technology which is based on the punishment mechanism. The main idea of this technology is to adopt the dynamic fuzzy clustering method to compare each fitness value of individual in the niche. Finally, we get a penalty factor and a relatively small fitness value. Then we may eliminate some low fitness values of individuals. Hence, the niche is optimized.

Assume that there is a population of N individuals with Chromlen dimensions. The different magnitudes of the individual genes may generate some problems in real-number encoding. Therefore, all of the real-number genetic codes should be normalized through the following function.

$$\hat{x}_{pj} = (x_{pj} - x_{pj\,min})/(x_{pj\,max} - x_{pj\,min}) \tag{10}$$

where x_{pj} denotes the genetic code of the pth individual at its j th point in the genetic sequence.

After normalized by (10), the fuzzy similar matrix R among individuals is established by (11).

$$R_{pq} = \frac{\sum_{k=1}^{Chromlen} min(\hat{x}_{pk}, \hat{x}_{qk})}{\sum_{k=1}^{Chromlen} max(\hat{x}_{pk}, \hat{x}_{qk})} \tag{11}$$

The fuzzy similar matrix satisfies reflexivity and symmetry. According to [27], the fuzzy equivalence matrix solves the problem of the niche more efficiently. Therefore, through looking for the minimum transitive closure of the fuzzy similar matrix R, we obtain the corresponding fuzzy equivalence matrix T, which clusters the population.

If the similarity coefficient λ is less than the coefficient T_{pq} for each pair of individuals, i.e., $\lambda \le T_{pq}$, then the individual x_p and x_q are divided into the same niche, until all individuals are divided into the niches.

$$Niche(k) \Leftarrow \{x_p \ldots x_q\} \quad (1 \le k \le Chromlen) \tag{12}$$

According to the fuzzy equivalence matrix and the number of the population, the similarity coefficient λ is updated dynamically as follows:

$$\lambda_t = \frac{\sum_{j=1}^{N} T_{maxj}}{N} \tag{13}$$

where $T_{max\,j}$ denotes the equivalent coefficient between the individual of the maximum fitness value x_{max} and individual x_j.

In classic niche technology, considering the unstable of iteration error of GA, the fitness values of some niches are much less than other individual niche fitness values. Although the crossover and mutation operation dissolvable for part of the problem, they can't significantly improve the overall situation of the niche. In addition, with population increasing, the area is different from the classic niche technology, so the search efficiency reduces when the GA searches for the optimal solution of the area. In this situation, we calculate the individual fitness value, and then compare them with the best of the same generation individual fitness value. If the difference between them is under a certain threshold value, then a qualified niche will be replaced. The improved niche genetic algorithm process is shown in Fig. 2.

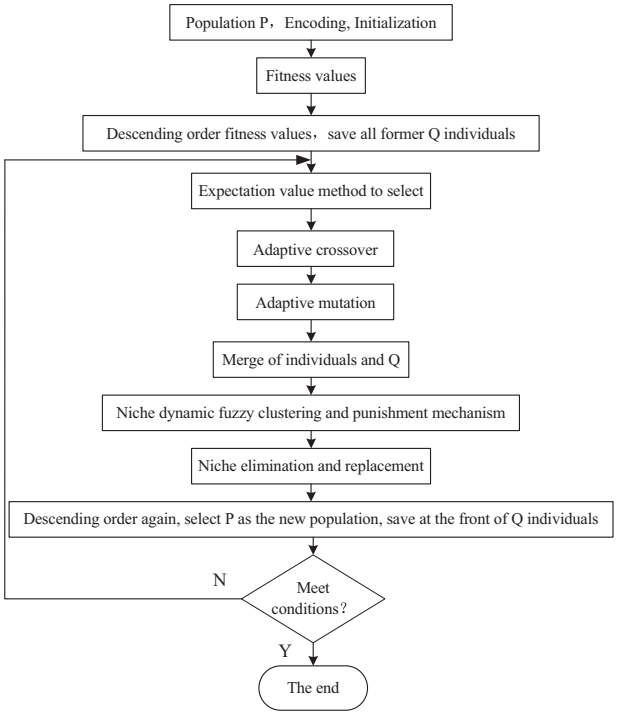

Fig. 2. Flow chart for the improved niche genetic algorithm.

For quantitative analysis of the diversity with the improved niche genetic algorithm, Eq. (15) is defined to calculate the diversity of population.

$$d_t = -\sum_{n=1}^{Q} p_n \log(p_n) \tag{15}$$

$$p_n = L_{mn}/N \tag{16}$$

where Q means the number of sub-population in the No. t generation, L_{mn} denotes the quantity of the nth sub-population and N denotes the total number of individuals of the species. A higher d means the greater diversity.

Aiming at a situation that the fitness value in an ecological niche is much smaller than others, i.e.,

$$\left|f_i - f_{max}\right| < f_{default} \tag{17}$$

then

$$f_i = f_{niche}(i), \quad 1 \le i \le n \tag{18}$$

$$f_{niche} = (f_1', f_2', f_3' \cdots f_n') \tag{19}$$

where f_{max} is the highest fitness value in the same generation. The default threshold of the fitness value is $f_{default}$. $f_{niche}(i)$ representing the ith individual fitness.

3. System simulation and analysis

3.1. Data preprocessing

In order to inspect the effectiveness of the prediction model, we adopt real safety data provided by the network simulation security platform in the laboratory, and effectively achieve the prediction of the network security situational values based on network security situation assessment [28].

The experiment randomly selects a continuous 90-day data from the security platform, which are divided into two parts, including the former 76-days as training samples, and the remaining 14-days as test samples. Based on the analysis of the safety data, we find that a periodically serious attack occurs within 5 days. Therefore, we choose 5 days as the vector dimension input and 1 day as the vector dimension output. The selection of the security situation dimension is shown in Table 1 Referring to (2), the prediction model of the WNN network structure is confirmed as 5-11-1.

The training of the neural network will be affected if the differences of orders of magnitude of the network security situational values are very big. In order to avoid this phenomenon, the network security situational values for 90-day are normalized as follows:

$$\hat{X} = (X - X_{min})/(X_{max} - X_{min}) \tag{20}$$

where X_{min} and X_{max} are the minimum and maximum network security situational values of the samples. X and $\hat{X}$ are the previous and later normalized network security situational values respectively.

Table 1
Selection of security situation dimension.

Input samples	Output samples
X_1, X_2, X_3, X_4, X_5	X_6
X_2, X_3, X_4, X_5, X_6	X_7
…	…
$X_{71}, X_{72}, X_{73}, X_{74}, X_{75}$	X_{76}

The absolute error (*AE*), mean relative error (*MRE*), and root mean square error (*RMSE*) are chosen as the judgment criteria in the prediction precision, which are defined as follows.

$$AE = \left|Y_k - Y_k'\right| \tag{21}$$

$$MRE = \frac{1}{N}\sum_{k=1}^{N}\left|\frac{Y_k - Y_k'}{Y_k}\right| \tag{22}$$

$$RMSE = \sqrt{\frac{1}{N}\sum_{k=1}^{N}\left(Y_k - Y_k'\right)^2} \tag{23}$$

where N is the sample number of the network security situational values. Y_k denotes the real security situational value on the network and Y_k' means the prediction value.

3.2. Results analysis and comparison

To demonstrate the superiority of the proposed model, the experiment compares the performance with WNN, GA-BP and GA-WNN. After completely training with these algorithms, the convergence speed, diversity and the prediction accuracy are chosen to judge the advantages in these algorithms and prove the effectiveness of the proposed model.

- Convergence speed.

Referring to Figs. 3 and 4, the abscissa represents the generation, and the ordinate represents the root mean square error. We see that the different algorithms have different convergence speeds. The convergence speed of INGA-WNN is fastest, it converges at the 68th generation. The second fastest algorithm is GA-WNN which ends at 118th generation. GA-BP and WNN stop running to reach convergence precision at the 139th and 359th generations respectively. So, we draw a conclusion that the model combining the improved niche technology and WNN reduces the convergence time effectively and improves the prediction efficiency.

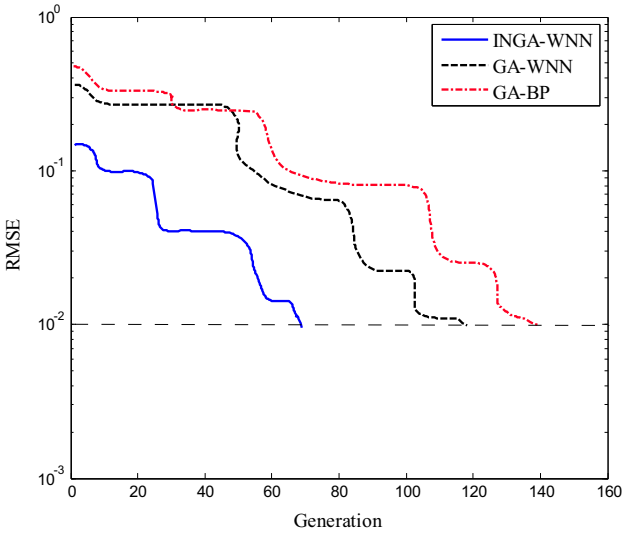

Fig. 3. Convergence speed of prediction models.

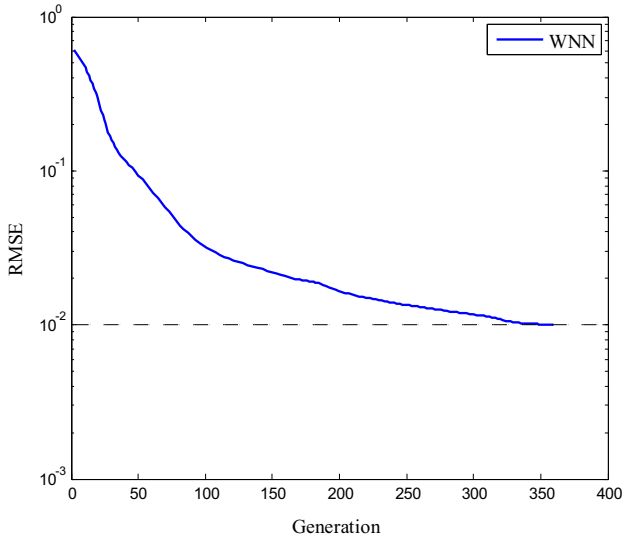

Fig. 4. Convergence speed of WNN.

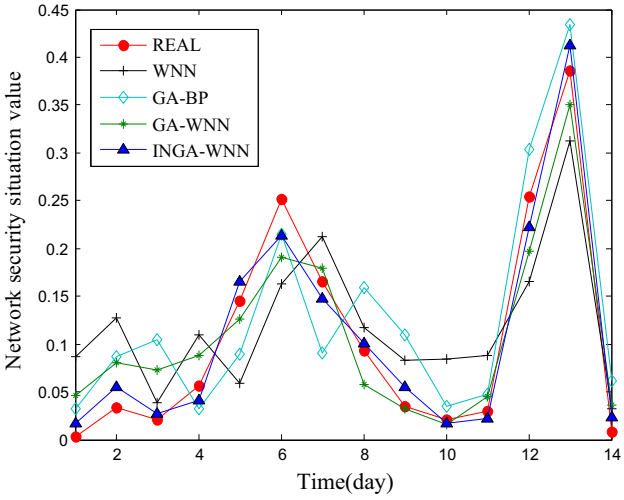

Fig. 5. Security situation prediction curves for models.

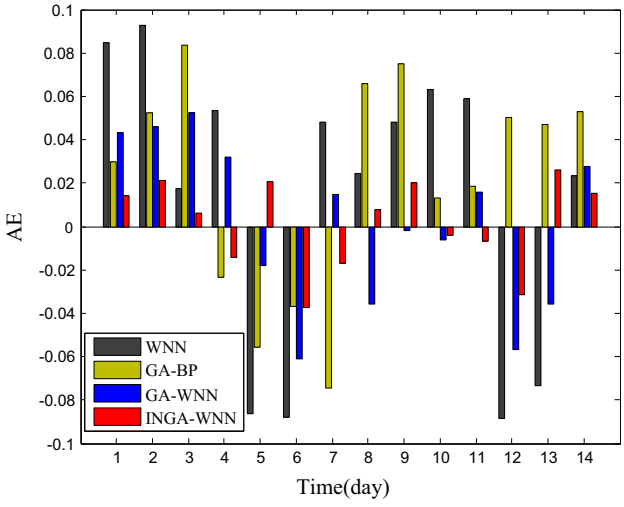

Fig. 6. AE bar graphs for prediction models.

Table 2
Diversity of population.

Generation	*Diversity of population*	
	GA	INGA
0	0.9436	0.9352
10	0.6752	0.7965
30	0.4216	0.7634
60	0.2163	0.6942
100	0.1484	0.6936
150	0.1432	0.6932
200	0.1426	0.6931

- Diversity of population

The main purpose of introduction of the niche technology is to maintain the diversity of the GA. The diversity of population is an important index which can judge whether the GA is easy to fall into the premature convergence or not. Therefore, we try to increase the population diversity to improve the premature problem of the GA. Eq. (15) is about the quantitative analysis of the diversity of population. From the Table 2, the diversity value of the INGA can be steady around 0.69 in the early time. Compared with the classic GA, the INGA has a big advantage in terms of keeping the diversity of population.

- Prediction accuracy

Based on Figs. 5 and 6, we can find that four prediction models have achieved good prediction effect fairly. But INGA-WNN is closer to the real network situational values and has smaller value in prediction error than WNN, GA-BP and GA-WNN. Based on the analysis of the results, the main reason is that INGA-WNN adopts an improved niche genetic algorithm to optimize WNN so that it has higher fitting capacity in nonlinear ability. As a result, the problem of genetic diversity of population is solved and the premature convergence is avoided effectively. Consequently, INGA-WNN can converge a better solution.

In Table 3, INGA-WNN has the lowest prediction error value of the four algorithms, which means that INGA-WNN has the strongest capacity of prediction. According to the accuracy results of INGA-WNN and WNN, we find that the improved niche genetic algorithm is better than the steepest descent method for optimizing WNN parameters. Meanwhile, comparing the results of GA-WNN with the GA-BP, we see that the WNN has a better fitting capacity than BPNN in a nonlinear system.

Table 3
Prediction model accuracy inspection standard.

Prediction models	WNN	GA-BP	GA-WNN	INGA-WNN
MRE	0.7758	0.6812	0.6497	0.4723
RMSE	0.1034	0.0804	0.0651	0.0214

4. Conclusion

In this paper, we put forward a network security situation prediction model, which is based on WNN with the parameters optimized by the improved niche genetic algorithm. The prediction model combines the improved niche technology with the adaptive genetic algorithm. Hence, the novel niche technology has the improved optimization capacity of GA and the convergence speed. Furthermore, the improvement of diversity of population solves the problems of the premature and lower convergence

effectively. The experiment proved the reliability and effectiveness of the INGA-WNN, which also more precisely predicts the network security situation.

Acknowledgment

This work was partially supported by the National Natural Science Foundation of China (Nos. 61271260 and 61301122) and the Natural Science Foundation of Chongqing Science and Technology Commission (No. cstc2015jcyjA40050, cstc2014jcyjA40052), Scientific and Technological Research Program of Chongqing Municipal Education Commission (KJ1400405). Research Fund for Young Scholars of Chongqing University of Posts and Telecommunications (A2013-30), the Science Research Starting Foundation of Chongqing University of Posts and Telecommunications (A2013-23).

References

[1] X.J. Ding, Y. Tian, Y. Yu, A real-time big data gathering algorithm based on indoor wireless sensor networks for risk analysis of industrial operations, IEEE Trans. Ind. Inf. 12 (3) (2016) 1232–1242.
[2] Y. He, F.R. Yu, N. Zhao, H. Yin, H. Yao, R.C. Qiu, Big data analytics in mobile cellular networks, IEEE Access 4 (3) (2016) 1985–1996.
[3] P. Chopade, J. Zhan, M. Bikdash, Node attributes and edge structure for large-scale big data network analytics and community detection, in: Proceedings of the 2015 IEEE International Symposium on technologies for Homeland Security (HST), 2015, pp. 1–8.
[4] Dapeng Wu, Jing He, Honggang Wang, Chonggang Wang, Ruyan Wang, A hierarchical packet forwarding mechanism for energy harvesting wireless sensor networks, IEEE Commun. Mag. 53 (8) (2015) 92–98.
[5] Dapeng Wu, Hongpei Zhang, Honggang Wang, Chonggang Wang, Ruyan Wang, Yi Xie, Quality of protection (QoP)-driven data forwarding for intermittently connected wireless networks, IEEE Wirel. Commun. 22 (4) (2015) 66–73.
[6] Dapeng Wu, Yanyan Wang, Honggang Wang, Boran Yang, Chonggang Wang, Ruyan Wang, Dynamic coding control in social intermittent connectivity wireless networks, IEEE Trans. Veh. Technol. PP (99) (2015) 1.
[7] Z.H. Gong, Y. Zhou, Research on cyberspace situational awareness, J. Softw. 21 (7) (2010) 1605–1619.
[8] S. Jajodia, P. Liu, V. Swarup, C. Wang, Cyber Situational Awareness: Issues And Research, Springer, New York 2010, pp. 25–34.
[9] C. Onwubiko, Functional requirements of situational awareness in computer network security, in: Proceedings of the IEEE International Conference on Intelligence and Security Informatics, ISI '09, 2009, pp. 209–213.
[10] T. Bass, Intrusion detection systems and multisensor data fusion, Commun. ACM 43 (4) (2000) 99–105.
[11] A.P. Lu, J.P. Li, Y. Ling, A new method of data preprocessing for network security situational awareness, in: Proceedings of the 2010 2nd International Workshop on Database Technology and Applications (DBTA), 2010, pp. 1–4.
[12] Y. Wei, Y.F. Lian, D.G. Feng, A network security situational awareness model based on information fusion, J. Comput. Res. Dev. 46 (3) (2009) 353–362.
[13] X.W. Liu, J.G. Yu, M.L. Wang, Network security situation generation and evaluation based on heterogeneous sensor fusion, in: Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing, WiCom '09, 2009, pp. 1–4.
[14] D.S. Pereira Salazar, P.J. Leitao Adeodato, A. Lucena Arnaud, Continuous dynamical combination of short and long-term forecasts for nonstationary time series, IEEE Trans. Neural Netw. Learn. Syst. 25 (1) (2014) 241–246.
[15] Z.C. Wen, Z.G. Chen, Network security situation prediction method based on hidden Markov model, J. Cent. South Univ. (Sci. Technol.) 46 (10) (2015) 3689–3695.
[16] Y. Zhuo, Q. Zhang, Z.H. Gong, GRNN model of network situation forecast, J. PLA Univ. Sci. Technol. (Nat. Sci. Ed.) 13 (4) (2012) 147–151.
[17] G.S. Zhao, H.Q. Wang, J. Wang, A situation awareness model of network security based on grey Verhulst model, J. Harbin Inst. Technol. 40 (5) (2008) 798–801.
[18] E.E. Elattar, J. Goulermas, Q.H. Wu, Electric load forecasting based on locally weighted support vector regression, IEEE Trans. Syst. Man Cybern. Part C: Appl. Rev. 40 (7) (2010) 438–447.
[19] Y.L. Liu, D.G. Feng, Y.F. Lian, Network situation prediction method based on spatial-time dimension analysis, J. Comput. Res. Dev. 51 (8) (2014) 1681–1694.
[20] J.J. Wang, K.Q. Shi, Y.J. Lei, Method of situation forecast based on function S-Rough sets, Syst. Eng. Electron. 29 (2) (2007) 214–216.
[21] S.Y. Hao, Prediction of Network Security Situation Based on Cloud (M.S. thesis), National University of Defense Technology, 2010.
[22] F. He, D. He, A. Xu, Hybrid model of molten steel temperature prediction based on ladle heat status and artificial neural network, J. Iron Steel Res. (Int.) 21 (2) (2014) 181–190.
[23] X.O. Yi-Ju Tseng, Ping, J.D. Liang, Multiple-time-series clinical data processing for classification with merging algorithm and statistical measures, J. Biomed. Health Inform. 19 (5) (2015) 1036–1043.
[24] J.B. Lai, H.Q. Wang, X.W. Liu, A Quantitative prediction method of network security situation based on wavelet neural network, in: Proceedings of the First International Symposium on Data, Privacy, and E-Commerce, 2007, pp. 197–202.
[25] A. Celikyilmaz, I.B. Turksen, Enhanced fuzzy system models with improved fuzzy clustering algorithm, IEEE Trans. Fuzzy Syst. 16 (6) (2008) 779–794.
[26] Chiu-Hung Chen, Liu Tung-Kuan, Chou Jyh-Horng, A novel crowding genetic algorithm and its applications to manufacturing robots, IEEE Trans. Ind. Inform. 10 (8) (2009) 1705–1716.
[27] Y.J. Lei, B.S. Wang, J.H. Hu, Method for constructing intuitionistic fuzzy equivalent matrixes, Syst. Eng.-Theory Pract. 7 (7) (2007) 127–131.
[28] F.W. Li, Network Security Risk Assessment Based on Item Response Theory. Available online: ⟨http://eudl.eu/doi/10.4108/icst.mobimedia.2015.259024?ticket=ST-15515-kYAczeS2IXHPl645IRNd-cas.eai.eu⟩, 2015 (accessed 01.03.16).