 DOI 10.1515/jisys-2014-0004 — J. Intell. Syst. 2015; 24(1): 55–67

Lan Ma*, Shaopu Ma and Zhijun Wu

WNN-Based Prediction of Security Situation Awareness for the Civil Aviation Network

Abstract: The security of the civil aviation network is closely related to flight safety. Security situation prediction is the advanced stage of situational awareness in the civil aviation network. In this article, a prediction approach of security situations for the air traffic management network is proposed on the basis of the wavelet neural network. The proposed approach adopts the wavelet theory and neural network, combining a time-series forecasting method for the prediction of security situations in the civil aviation network. The experimental results show that this approach has the advantages of fast training and high prediction accuracy.

Keywords: Security, situation awareness, prediction, wavelet, neural network.

***Corresponding author: Lan Ma,** School of Air Traffic Management, Civil Aviation University of China, No. 2898 Jinbei Road, Dongli District, Tianjin 300300, China, e-mail: lma@cauc.edu.cn
Shaopu Ma and Zhijun Wu: Electronics & Information Engineering, Civil Aviation University of China, Tianjin 300300, China

1 Introduction

Air traffic management (ATM) is a network-enabled intelligent system that is composed of aeronautical communication, navigation, and surveillance systems, employing computer and network technologies, including aeronautical telecommunication networks, satellite systems, data communication links, radar systems, and automatic dependent systems together with various levels of automation, applied in support of a seamless global collaborative decision making in the air transportation system (ATS) [8].

Advanced ATM can realize the sharing of air traffic control (ATC) information and flight operation information. The ATC, airlines, airports, and related units having the same trend of flight operation can effectively reduce the workload of air traffic controllers, and is conducive to the rational allocation of runways and empty domain controller resources for the purpose of improving the efficiency and enhancing the security of the ATS [8].

Network security situational awareness is a new technology to monitor the security of networks. Civil aviation is the core of the transport sector in a country, and the security of civil aviation networks is an important guarantee of civil aviation safety. With the rapid development of civil aviation, the requirements for the security of ATM networks become higher. At the same time, with the continuous development of the network interconnection of the civil aviation information system, the security issues of ATM networks are increasingly becoming prominent. Therefore, it is an important task to ensure the safety of ATM networks and the security of national information, as well as to perform network security situation assessment and prediction for ATM systems [9]. These can enable network administrators to timely detect risks and threats that exist in the network system and then adjust the appropriate security measures accordingly.

The information security of ATM networks has its own specialty because ATM supports a different business from the general network. ATM services run with four subsystems, such as ATC communication, navigation, surveillance, and automation, including meteorology, intelligence, ATC message, radar navigation, and other important data, which have a direct impact on the safety of civil aviation. Therefore, timely and accurately assessing the aviation network and predicting short-term security situations with comprehensive historical data are of great significance for the network administrator, in order to deploy active measures to resist threats to ATM.

In this article, the originality of the work is summarized as follows:

1. A security situation prediction mode of the ATM network is built by using wavelet neural network (WNN).
2. A prediction approach of security situation for the ATM network based on the WNN model is proposed.
3. A time-series forecasting method of security situation prediction for the ATM network is presented.

2 Related Work

Artificial neural network (ANN) has had great achievements in the field of network security. Methods based on ANN [13] can also be used as a security assessment for the current operating state of the system. The combination of fuzzy analytic hierarchy process (FAHP) and ANN [16] can be used for E-government information systems. Moreover, the combination of the fuzzy theory with WNN [20] can be used for the risk assessment of information security. Shi et al. [12] proposed a method based on mathematical morphology and ANN to discriminate between the magnetizing inrush and the internal fault of a power transform. Compared with ANN, the Bayesian network can deal with incomplete data, and learn the cause–effect relationship of variables. Thus, Filiol and Josse [4] presented an approach of viral detection by means of spectral analysis based on Bayesian networks to detect viral codes for network security. Fu and Delcroix [5] proposed a method using a special structure of Bayesian network based on AHP to make a decision. Dobigeon et al. [3] proposed a Bayesian model based on a correlated Bernoulli–Gaussian model to exploit the spatial correlations between the image pixels in the frequency domain. Adankon et al. [1] established the semisupervised learning model by using the Bayesian approach with one and two levels of inference. Hwang et al. [7] combined the Bayesian network with genetic algorithm (GA) to deal with uncertainty and dynamic properties in the real world. Amini et al. [2] redefined the Bayesian estimation problem in the Fourier domain with the help of characteristic forms. The backpropagation (BP) algorithm is proposed to solve the training of a multilayer neural network. Wang and Song [15] performed research on the steam turbine exhaust wetness fraction forecast based on a GA BP ANN method. The fuzzy comprehensive evaluation based on the combination of the BP neural network and experts system [6] can be useful for the prevention of investment risk. The BP neural network combined with the fuzzy theory [11] can evaluate the risk of information systems. A BP neural network can be combined with a GA [18] to improve learning ability. A BP neural network evaluation model can be used to evaluate a bank's credit risk and optimize its management [21]. An improved three-layer BP neural network is used to solve the information security problems of an ATM system [17]. As AHP can provide a hierarchical thinking framework, which makes it easier to organize the thoughts, Sang et al. [10] proposed an assessment index system based on BP neural networks and AHP to evaluate the competitiveness of small and medium-sized manufacturing enterprises, and inducted a sensibility analysis to discriminate the importance of each index in the system. Although the safety evaluation method for the communication system is effective, it does not give the scope of the evaluation model to which it is applicable. Although the WNN is similar to the radial basis function (RBF) network, the wavelet analysis theory can guide the network initialization and parameter selection, providing the network a simpler topology and faster convergence rate. In this article, by using the parallelism of the WNN, fault tolerance, and self-learning, as well as a good non-linear mapping ability, we aimed to accurately reflect the complex relationship of the situation value in ATM networks and accurately predict the security situation of the civil aviation network.

3 Prediction Model for Aviation Network Security Situation Based on the WNN

ATM is a complex application information platform that is a real-time operation system. The security situation of the ATM network has a close relationship with the past and current time. To use the WNN to accurately

predict the security situation of the aviation network, it is necessary to identify the factors that affect the civil aviation security situation, as well as determine the structure of the prediction model.

3.1 Introduction of the ATM Network

The ATM network is the backbone network for civil aviation information transmission and sharing. It consists of aeronautical communication, navigation, surveillance, and automation subsystems, as shown in Figure 1.

The ATM network is connected to the local authority by means of automatic message switching, packet switching, and satellite communications. It mainly covers all international and domestic routes, assumes the ATC message, aviation weather information, flight plan and dynamic message, integrated management, international data exchange, and other services. These data and information have a direct impact on the safety of civil aviation. The security information of the ATM network can guarantee business safety and its efficient operation.

The security of network equipment, operating systems, and application can affect the safety of the ATM. Network equipment include communications, navigation, meteorological, intelligence, and other network equipment. The operating system refers to the host and the server operating system that runs on the ATM network, and application refers to the various services available in the ATM network. The security of the ATM network is related to the safety of civil aviation. It is necessary to design appropriate information security measures in these areas, including data encryption, secure authentication, firewall, intrusion detection system, and redundancy backup.

To change the status quo that the civil aviation network security incident response lags behind, it is necessary to carry out measures for the network security situational awareness of the ATM and understand the dynamic changes in network security, in addition to taking passive safety measures. It is of great significance for improving the emergency response capabilities of the aviation network system, alleviating the hazards of network attacks and finding potentially malicious intrusions.

To predict the security situation value of the ATM, we can evaluate the security situation in each subsystem, analyze the services of the network, and evaluate the security measures taken in each subsystem. The security situation for the entire ATM network system is obtained from the security situation of the four subsystems in a comprehensive way, as shown in Figure 2.

3.2 A Learning Method Based on the WNN

The topology of the WNN is similar to the BP network; however, the transfer function of the hidden layer is a wavelet basis function. The WNN topology [14, 19] is shown in Figure 3.

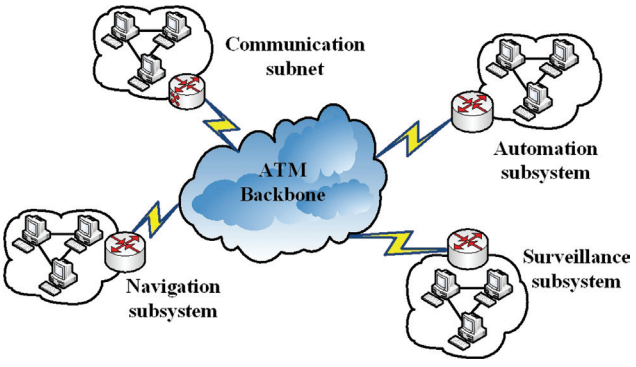

Figure 1. ATM System Structure.

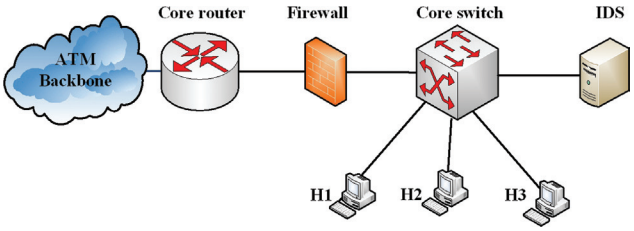

Figure 2. Topology for Subnets of the ATM.

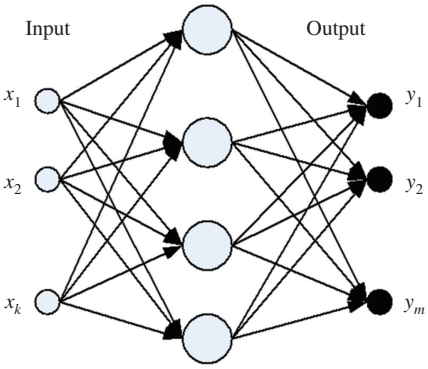

Figure 3. Topology of the WNN.

In Figure 3, X_1, X_2, ..., X_k indicate the input of the WNN, and Y_1, Y_2, ..., Y_m are the prediction outputs of the WNN.

When the input sequence is $x_i(i = 1, 2, ..., k)$, the output of the hidden layer is calculated by formula (1):

$$h(j) = h_j\left(\frac{\sum_{i=1}^{k} w_{ij}x_i - b_j}{a_j}\right) \quad j = 1, 2, ..., l, \tag{1}$$

where $h(j)$ denotes the output of the hidden layer, j indicates the number of hidden layer nodes, w_{ij} is the weight between the input layer and the hidden layer, b_j is the translation factor of the wavelet basis functions, a_j is the stretching factor of the wavelet basis function, and h_j is a wavelet basis function. Because the Morlet wavelet function has power-stable computing ability and strong anti-jamming capability, in this article, we apply the Morlet wavelet function as the basis function in the WNN. The expression is shown in formula (2):

$$y = \cos(1.75x)e^{-x^2/2}. \tag{2}$$

The output of WNN is

$$y(k) = \sum_{i=1}^{l} w_{ik}h(i) \quad k = 1, 2, ..., m. \tag{3}$$

In formula (3), w_{ik} is the weight between the hidden layer and the output layer, $h(i)$ is the output of node i of the hidden layer, l is the number of nodes for the hidden layer, and m is the number of nodes for the output layer.

Using a gradient correction method to adjust the weights of the WNN, concrete steps are performed as follows [6]:

(a) Computing the prediction error of neural network by using formula (4):

$$e = \sum_{k=1}^{m} yn(k) - y(k), \tag{4}$$

where, $yn(k)$ is the expected result and $y(k)$ is the prediction output of the WNN.

(b) Adjusting the weights and wavelet basis function coefficients of the WNN based on the prediction error by using the following equations:

$$w_{n,k}^{(i+1)} = w_{n,k}^{i} + \Delta w_{n,k}^{(i+1)}, \tag{5}$$

$$a_{k}^{(i+1)} = a_{k}^{i} + \Delta a_{k}^{(i+1)}, \tag{6}$$

$$b_{k}^{(i+1)} = b_{k}^{i} + \Delta b_{k}^{(i+1)}, \tag{7}$$

where $\Delta w_{n,k}^{(i+1)}$, $\Delta a_{k}^{(i+1)}$, and $\Delta b_{k}^{(i+1)}$ are calculated on the basis of the network prediction error:

$$\Delta w_{n,k}^{(i+1)} = -\eta \frac{\partial e}{\partial w_{n,k}^{(i)}}, \tag{8}$$

$$\Delta a_{k}^{(i+1)} = -\eta \frac{\partial e}{\partial a_{k}^{(i)}}, \tag{9}$$

$$\Delta b_{k}^{(i+1)} = -\eta \frac{\partial e}{\partial b_{k}^{(i)}}, \tag{10}$$

where η is the learning rate.

The training steps of the WNN are as follows:

(a) Initialize the network. Initialize the wavelet function dilation factor a_k; translation factor b_k; the network connection of the right weight w_{ij}, w_{jk}; and set the learning rate μ.
(b) Put the sample into the WNN. Use the input samples to train the network structure.
(c) Predict the output of the WNN. Train samples to the network, compute the network-predicted output, and calculate the error of the network output and the desired output e.
(d) Modify the weight. Adjust the weights and parameters of the wavelet function for the neural network on the basis of the prediction error, and make the predicted values of the network approach expectations.
(e) Determine whether the algorithm is ended; if it is not the end, return to (c).

3.3 Prediction Model of the ATM Network Security Situation

According to the theory of the WNN, we can use the historical security situation of the ATM network that is obtained from the assessment of the ATM to train the WNN, and then use the trained network to predict the value of the security situation in the coming period. The prediction model is shown in Figure 4.

In this model, the WNN has a single hidden layer structure; the input is the civil aviation network security situation value at the historical moment normalized using the trial method to determine the hidden layer. The output layer node is the one that indicates the situation value of the current moment.

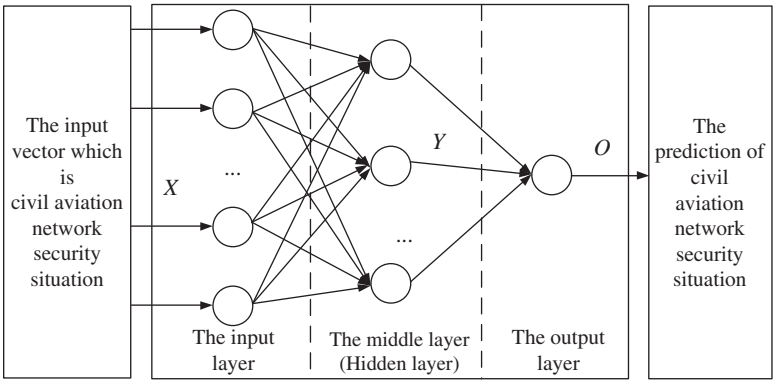

Figure 4. Model of Time-Series Forecasting Based on the WNN.

4 Experiments

To verify the feasibility of the prediction model based on the WNN, an experimental network is built as shown in Figure 5. This experimental environment simulates the ATM network according to the ATM, ATS, and ATC services in the local area network (LAN) structures.

The simulated ATM network is structured by using four layers as follows: the first layer is the backbone network; the second layer is the subnets, such as the communication subnet; the third layer is the host systems; and the fourth layer consists of services and security measures. These services protect the host from attacks such as DoS and PROBE. Through safety measures such as encryption, access control, digital signature, audit, routing control, and authentication, the security measures can ensure confidentiality, integrity, availability, reliability, and non-repudiation, as shown in Figure 5.

The test is performed on the platform that has the safety functions, and it takes 4 days divided into 1 h as a unit to collect data.

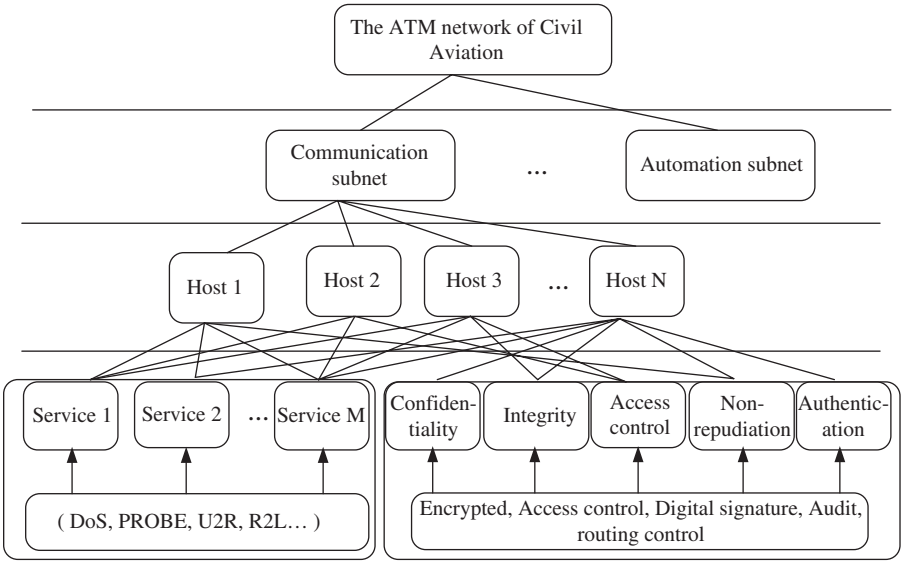

Figure 5. Experimental Network.

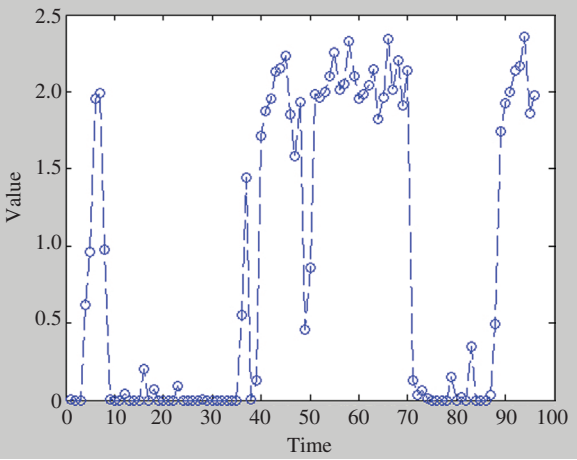

Figure 6. Values of the Network Security Situation in the First 4 Days.

4.1 Calculating the Trend Value

Weights and attacks to the four subnets are assumed under the same conditions, and the network's security situation values can be calculated by using a series of mathematical methods. These values are able to demonstrate some of the characteristics of the network operating conditions. When the frequency of network security incidents and the level of threats are not the same, the network's security situation values are different. The greater the value of the network security situation, the more unsafe the network would be.

In this article, ratio of weighted threats to weighted defenses solving security situation values for the network is used:

$$F_{SA}(T_i, N_i) = \frac{\sum_{i=1}^{n} T_i \times N_i}{\sum_{i=1}^{n} N_i \times DS_i}, \tag{18}$$

where $F_{SA}(T_i, N_i)$ indicates the value of the network security situation, N_i is the number of times the attack occurred, T_i is the threat level corresponding to the attack of i, and DS_i is the defense capability of the system for those kinds of attacks. According to the statistics of the attacks, we use the statistical average value DS_i instead of the defense capability. Actually, 5-day data are used in the test. In this study, the data of the first 4 days are used as historical data to forecast the network security situation of the next 24 h, and the prediction span is 1 h. The data of the fifth day are used for comparison with the 24-h data predicted previously, and the prediction error can be minimized by the comparison. By using formula (18), the values of the network security situation in the first 4 days can be easily computed, as shown in Figure 6. The prediction starts from the zeroth hour and ends at the 96th hour.

The formula of the network security situation shows that the network security situation has non-linear characteristics, and access to the network security situation can be considered as the processing of a time series. Hence, the WNN model is used to solve the non-linear problem.

4.2 Determination of the Model of the WNN

A single hidden layer network model is applied in this article. The input layer of the WNN has four nodes, indicating the network security situation of four time points before the current time point. The number of nodes of the hidden layer is 6, whereas that of the output layer is 1, which indicates that the network security

situation will be forecasted. The number of nodes of the hidden layer has a great influence on the prediction of the WNN; when the number of nodes is too few, the network would display a bad learning experience and the number of training would increase. By changing the hidden nodes, the impact on predicting performance with different hidden nodes can be explored. In this experiment, the number of nodes of the hidden layer is 6. The initialization weights of the network are random parameters.

The number of training sets for the WNN is 100; the learning rates are $lr1 = 0.01$, $lr2 = 0.001$; and the target of error is 0.001. Then, the trained neural network is used to predict the network security situation of the next 24 h and analyze the forecasting result.

4.3 Prediction Based on the WNN and BP Neural Network

We apply the WNN model and the BP neural network model to predict the next 24 h trend value and compare the predictive performance of the two algorithms with the convergence rate, forecasting error, and regression.

4.3.1 Comparison of Error Convergence Speed

Applying the WNN and BP neural network to train the trend value, the number of training sets is 100. The training error curves are shown in Figures 7 and 8.

Because the WNN must adjust the translation factor and the dilation factor in addition to the network structure parameters and weights during the training, the convergence speed of the WNN is slower than that of the BP neural network. The training error of the BP neural network reaches 0.0311, compared with 0.0452 for the WNN. Therefore, the effect of learning samples based on the WNN is weaker than that based on the BP neural network.

4.3.2 Comparison of the Prediction of Results

The value of the network security situation is predicted by using the trained network. The predicted results are shown in Figures 9 and 10.

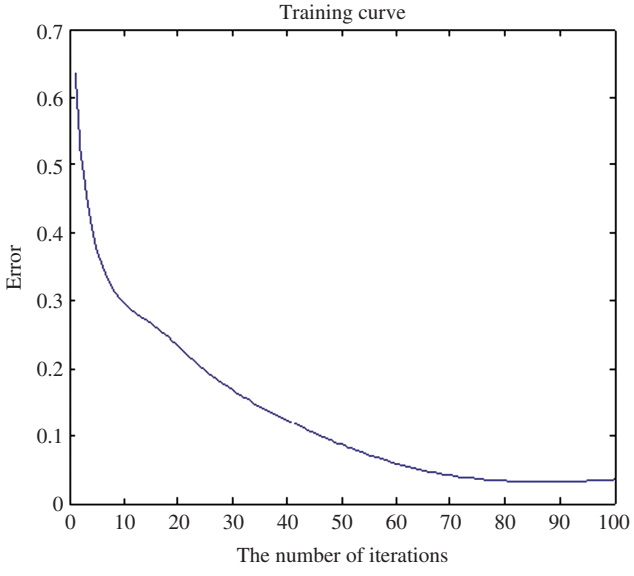

Figure 7. Training Curve of the WNN.

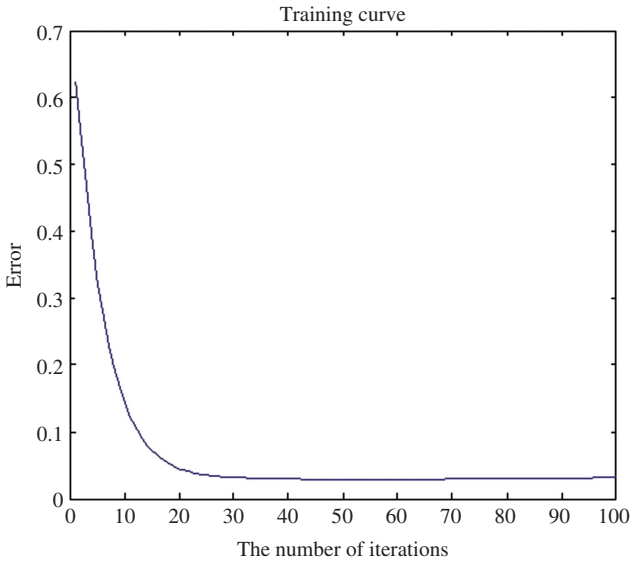

Figure 8. Training Curve of the BP Neural Network.

In the figures, "o" represents the actual value,"*" indicates the predicted value, and the bottom curve represents the prediction error. The corresponding numerical results are shown in Table 1.

According to the error curves in Figures 9 and 10, we can see that range of prediction error for the WNN is smaller than that of the BP neural network. The absolute forecasting errors in Table 1 show that prediction of most of the time points based on WNN is more accurate than that based on the BP neural network. Therefore, the learning ability and the generalization ability of the WNN are better than those of the BP neural network.

4.3.3 Analyzing the Regression Performance

To validate the performance of the WNN, this article adopts the plotstreg function as the prediction output of the WNN and BP neural network, targets the output non-linear regression, and then analyzes and compares the results. The correlation coefficient between the two indicates that the network approximation of the target data is the basis of the merits of the discriminant of the performance for the WNN prediction. The linear regression curves are shown in Figures 11 and 12.

In this article, we analyze the linear regression between the output vector of the neural network and the actual vector, and adopt the correlation coefficient between the target vector and the prediction as a sign

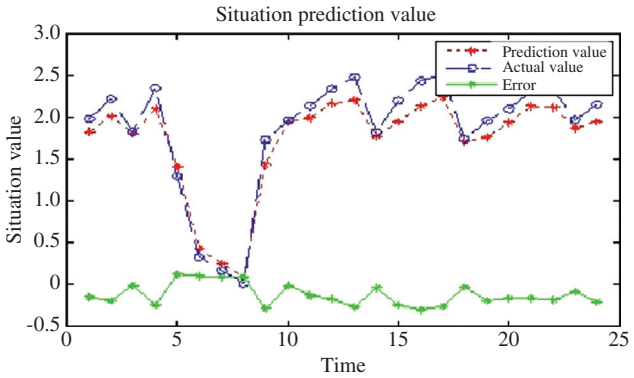

Figure 9. Prediction of the WNN.

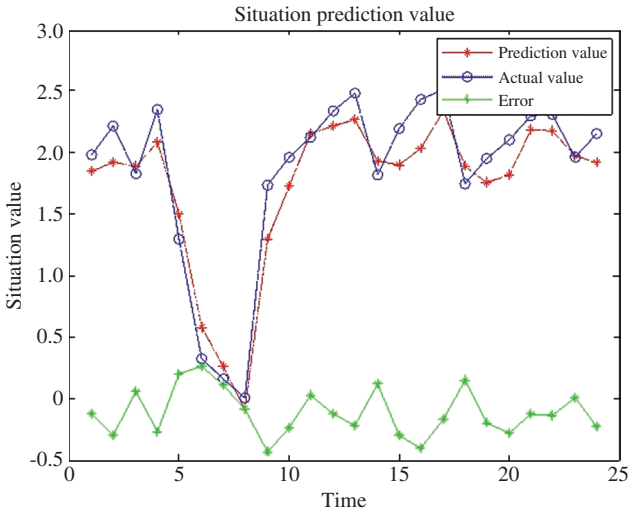

Figure 10. Prediction of the BP Neural Network.

of network performance evaluation. When network performance is in good condition and is achieved to a certain extent, the network-predicted output value should be equal to the actual output value, which means that the correlation coefficient is in the first quadrant of the axes on the diagonal. At this point, the intercept is equal to 0, slope is equal to 1, and the goodness of fit is equal to 1. In practical applications, a goodness of fit of >0.80 will be acceptable. From Figures 11 and 12, we can see that the correlation coefficient of the WNN is 0.99016, higher than the coefficient of 0.97584 of the BP neural network, which indicates that the capability of non-linear function approximation of the WNN is better than that of the BP neural network.

Table 1. Numerical Results of Prediction.

Time point	Actual value	Predictive value of WNN	Predictive value of BP neural network	Absolute predictive error of WNN	Absolute predictive error of BP neural network
1	1.977	1.8238	1.8468	0.1532	0.1302
2	2.215	2.0116	1.9161	0.2034	0.2989
3	1.826	1.8077	1.8857	0.0183	0.0597
4	2.354	2.1013	2.0824	0.2527	0.2716
5	1.298	1.4113	1.4982	0.1133	0.2002
6	0.320	0.4188	0.5785	0.0988	0.2585
7	1.620	0.2501	0.2665	0.0881	0.1045
8	0.050	0.0864	0.0854	0.0814	0.0904
9	1.732	1.4384	1.3008	0.2936	0.4312
10	1.964	1.9469	1.7280	0.0171	0.2360
11	2.130	1.9929	2.1545	0.1371	0.0245
12	2.345	2.1622	2.2143	0.1828	0.1307
13	2.485	2.2132	2.2668	0.2718	0.2182
14	1.815	1.7718	1.9308	0.0432	0.1158
15	2.201	1.9437	1.8990	0.2573	0.3020
16	2.435	2.1303	2.0342	0.3047	0.4008
17	2.51	2.2443	2.3450	0.2657	0.1650
18	1.746	1.7100	1.8939	0.036	0.1479
19	1.956	1.7602	1.7596	0.1958	0.1964
20	2.103	1.9359	1.8184	0.1671	0.2846
21	2.304	2.1349	2.1814	0.1691	0.1226
22	2.314	2.1209	2.1757	0.1931	0.1383
23	1.965	1.8688	1.9719	0.0962	0.0069
24	2.153	1.9458	1.9220	0.2072	0.2310

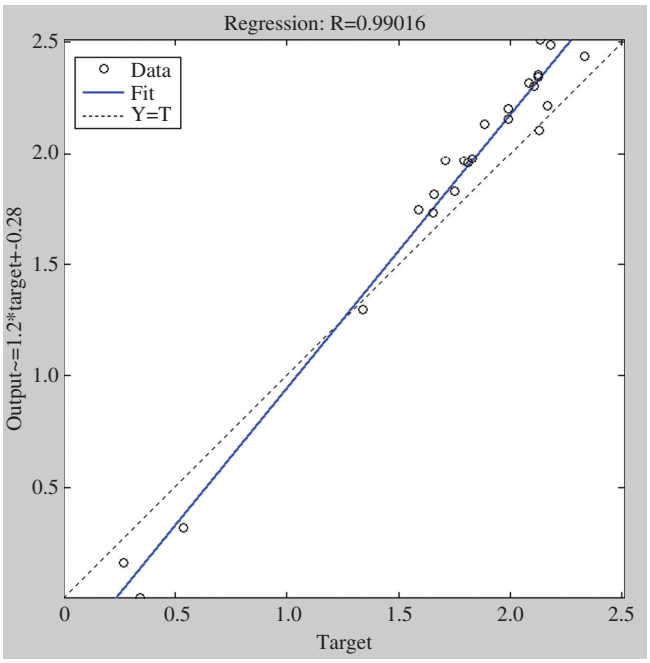

Figure 11. Regression Performance of the WNN.

According to the prediction of the WNN and BP neural network, we can find the following:

1. The approximation capability of the WNN prediction method is better than that of the BPNN method where there are numerical mutations in the value.
2. Because the WNN must adjust the translation factor and the dilation factor in addition to the network structure parameters and weights during the training, the WNN has a problem in parameter selection and debugging; it cannot guarantee that each forecast result is convergent. If the initial value is set as unreasonable, the network easily gets into the local minimum area, resulting in oscillation increases

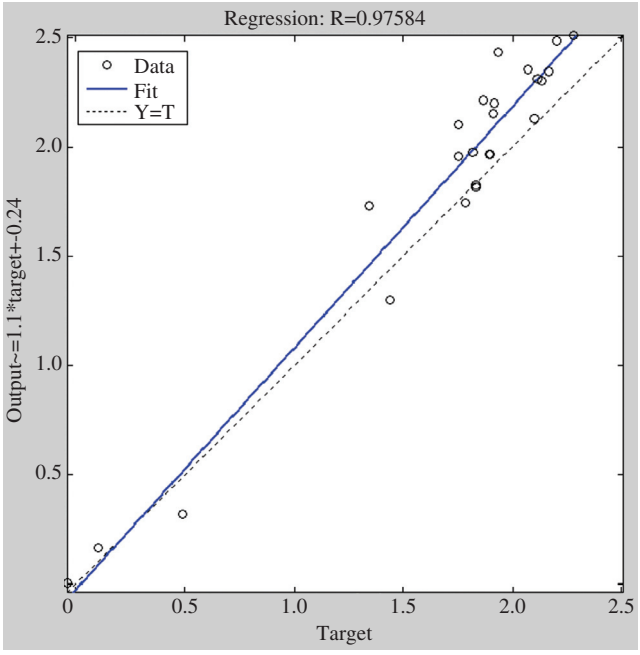

Figure 12. Regression Performance of the BP Neural Network.

Table 2. Comparison of the Proposed Approach with Classic Techniques.

Method	Error precision	Training speed
BP	Low	Slow
RBF	Low	Fast
FNN	High	Faster
WNN	Higher	Fast

and non-convergence of the network. In the next work, we can use the initial weights and thresholds to optimize the WNN to predict the network security situation.

A comparison of the proposed approach with classical techniques is shown in Table 2.

We can conclude that situation prediction based on the WNN is feasible and effective, through a series of experiments. The prediction is of high accuracy, and the error is very small. The WNN has non-linear capabilities, generalization ability, and fault tolerance. It can be used for the prediction of the actual security situational awareness in the civil aviation network.

5 Conclusion and Future Work

The ATM network is a complex intelligent system. The WNN is used to predict the security situation of the ATM network by adopting the non-linear mapping ability of the WNN. The predicted results show that the proposed approach is an effective prediction method with a small prediction error, and that it meets the requirements of security situation analysis. This proposed approach can help the ATM network administrator improve the situation of network security and make better decisions to defend against cyber-attacks. The experimental results show that the proposed approach is feasible and effective.

In future research work, the proposed algorithm will be optimized to provide more accurate results of security situation awareness.

Acknowledgments: This work was supported in part by the National Natural Science Foundation of China (grant nos. 61170328 and U1333116), Key Project of Tianjin Natural Science Foundation (grant no. 12JCZDJC20900), Fundamental Research Funds for the Central Universities of CAUC (grant nos. 3122013P007, 3122013D007, and 3122013D003), Civil Aviation Science and Technology Innovation Fund in 2013, Research Laboratory Construction Funds of Civil Aviation University of China (CAUC) in 2014–2016, and the Postgraduate Courses Construction Funds of Civil Aviation University of China (CAUC) in 2013 (grant no. 10501034).

Received October 10, 2013; previously published online April 9, 2014.

Bibliography

[1] M. M. Adankon, M. Cheriet and A. Biem, Semisupervised learning using Bayesian interpretation: application to LS-SVM, *IEEE T. Neural Networ.* **22** (2011), 513–524.

[2] A. Amini, P. Thevenaz, J. P. Ward and M. Unser, On the linearity of Bayesian interpolators for non-Gaussian continuous-time AR(1) processes, *IEEE T. Inform. Theory* **59** (2013), 5063–5074.

[3] N. Dobigeon, A. Basarab, D. Kouame and J.-Y. Tourneret, Regularized Bayesian compressed sensing in ultrasound imaging, in: *2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO)*, pp. 2600–2604, 2012.

[4] E. Filiol and S. Josse, New trends in security evaluation of Bayesian network-based malware detection models, in: *Proceedings of 2012 45th Hawaii International Conference on System Sciences*, TBD, Maui, HI, USA, 4–7 Jan 2012.

[5] Z. Fu and V. Delcroix, Bayesian network based on the method of AHP for making decision, in: *2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, Vol. 1, pp. 223–227, 2011.
[6] Y. Huang, C. Tian and F. Wei, Fuzzy comprehensive evaluation mode on the investment risk of real estate based on BP neural network and expert system, in: *E-Business and Information System Security, 2009, EBISS'09, International Conference*, pp. 1–5, 2009.
[7] J.-W. Hwang, Y.-S. Lee and S.-B. Cho, Structure evolution of dynamic Bayesian network for traffic accident detection, in: *2011 IEEE Congress on Evolutionary Computation (CEC)*, pp. 1655–1671, 2011.
[8] International Civil Aviation Organization (ICAO), *Global Air Navigation Plan for CNS/ATM Systems*, Doc 9750 AN/963, 2nd ed., 2002.
[9] R.-T. Nie, Y. Zhao and J.-H. Dai, Evaluation on safety performance of air traffic management based on fuzzy theory, in: *2009 ICMTMA'09 International Conference on Measuring Technology and Mechatronics Automation*, Vol. 2, pp. 554–557, 2009.
[10] J.-Y. Sang, Z.-J. Wu and Z.-F. Qi, An empirical study on the competitiveness of small and medium-sized manufacturing enterprises in China, in: *2011 IEEE 18Th International Conference on Industrial Engineering and Engineering Management (IE&EM)*, Vol. 1, pp. 672–676, 2011.
[11] S. Shen and Y. She, Approach to information systems security risk assessment based on fuzzy-BP neural network, *Computer Simulation* **28** (2011), 91–94.
[12] D.Y. Shi, J. Buse Q. H. Wu, L. Jiang and Y. S. Xue, Fast identification of power transformer magnetizing inrush currents based on mathematical morphology and ANN, in: *2011 IEEE Power and Energy Society General Meeting*, pp. 1–6, 2011.
[13] K. S. Swarup and P. B. Corthis, ANN approach assesses system security, *IEEE Computer Applications in Power* **15** (2002), 32–38.
[14] Y.-H. Wang and X. Cheng, Wavelet neural network optimization applied to intrusion detection, in: *2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT)*, Vol. 6, pp. 3109–3112, 2011.
[15] S. Wang and T. Song, The application on the forecast of steam turbine exhaust wetness fraction with GA BP neural network, in: *World Automation Congress (WAC)*, pp. 1–4, 2012.
[16] G. Wei, X. Xhang, X. Zhang and Z. Huang, Research on E-government information security risk assessment – based on fuzzy AHP and artificial neural network model, in: *2010 First International Conference on Networking and Distributed Computing (ICNDC)*, pp. 218–221, 2010.
[17] Z. Wu, L. Wang and R. Shi, Approach of information security assessment for ATM based on improved BP neural network method, *J. Commun.* **32** (2011), 150–158.
[18] S. Xin, A BP neural network model based on genetic algorithm for comprehensive evaluation, in: *Circuits, Communications and System*, pp. 1–5, 2011.
[19] M. Zhang, W. Dehu, S. Lv, E. Quan, S. Chen and Y. Li, Research on the wavelet neural network pattern recognition technology for chemical agents, in: *2010 International Conference of Information Science and Management Engineering (ISME)*, Vol. 2, pp. 241–244, 2010.
[20] D. M. Zhao, J. Liu and Z. Zhang, Method of risk evaluation of information security based on neural networks, in: *2009 International Conference on Machine Learning and Cybernetics*, Vol. 2, pp. 1127–1132, 2009.
[21] C. Zhu, Research on BP neural network evaluation model of credit risk of bank clients, in: *Management and Service Science*, pp. 1–5, 2010.