The Security Evaluation of ATM Information System Based on Bayesian Regularization

Lan Ma
School of Air Traffic Management, Civil Aviation University of China, Tianjin, China
Email: lma@cauc.edu.cn

Jia Xu, Zhijun Wu, Xiaoyu Zhang, Jiusheng Chen
Tianjin Key Laboratory for Advanced Signal Processing, Civil Aviation University of China, Tianjin, China
Email: xujia_1102@126.com, zjwu@cauc.edu.cn

Sarhan M. Musa
Engineering Technology Department, Prairie View A&M University, USA
Email: smmusa@pvamu.edu

Abstract—**Air Traffic Management (ATM) system is enticing targets of cyber-attacks since 9.11 event, and the security situation of ATM information system is closely related to the safety flight of air transportation. In this paper, an approach of security evaluation for ATM system is proposed based on artificial neural network (ANN). The proposed approach combines neural networks with Bayesian regularization to simulate ATM system in ANN. An indicator system of security situation for ATM system is established as the input of ANN, and the output is system security level, which is obtained by training the ANN with the daily recoded data of ATM system. Experimental results show that the proposed method has a certain precision and practicality.**

Index Terms—**Air Traffic Management; Information security evaluation; Bayesian regularization**

I. Introduction

Air Traffic Management (ATM) system, especially next generation air transportation system (NextGen), network-enabled intelligent information systems face great risk of cyber-attacks. A major driver behind these threats is the ATM system's growing reliance on IP-enabled computer systems for storing, processing and communicating aeronautic business-critical information across organizations and country boundaries, and the increase of telecommunications across the satellite and data-link[1]. ATM system may be disrupted by large scale cyber incidents. As early as 1996, Information Security Working Group of ATN (Aeronautical Telecommunication Network) of ICAO (International Civil Aviation Organization) pointed out that ATM data's exchanging in the data link faced with the serious risks of being modified, replayed and masqueraded. And the group raised that all the applications in CNS/ATM(Communication Navigation Surveillance/Air Traffic Management) are also easily attacked by DDoS (Distributed Denial of Service) [2,3]. Therefore, the cybersecurity of ATM system not only involves protecting the infrastructure by preventing, detecting, and responding to cyber incidents, but also exquisite knowledge of what is happening internally as well as externally to ATM system. The civil aviation organization must improve ATM system situational awareness to establish a long term security evaluation mechanism for ATM system.

In order to accurately evaluate the security situation of the air traffic control information systems, a security evaluation method based on Bayesian regularization is presented in this paper. Under the framework of Bayesian analysis, we introduce a new error function to adjust the network weights and thresholds based on posteriori conditional probability obtained from priori assumptions and relevant parameters[4]. The output of training is smoother, and the generalization capability of the network will not over fit in the training.

II. Related Work

Artificial neural network (ANN) and Bayesian network have got great achievements in the evaluation of information security. E. Filiol and S. Josse [4] studied on the trends in security evaluation of Bayesian network-based malware detection models, they presented an approach of viral detection by means of spectral analysis based on Bayesian networks. K. S. Swarup and P. B. Corthis [5] proposed a method based on ANN to evaluate the security of system. G. A. Ramos, A. Torres, and J. P. Rognon, etc. [6] analyzed industrial system IEEE 493 based on Bayesian condition. A. Taktak [7] studied on the external validation of a Bayesian neural network model in survival analysis. D. Wei and M. L. Zhang [8] proposed nonlinear identification model of neural network based on

Manuscript received September 15, 2013; revised October 27, 2013; accepted November 17, 2013.
Corresponding author: Zhijun Wu zjwu@cauc.edu.cn.

doi:10.4304/jsw.9.6.1587-1594

Bayesian method. D. M. Zhao, J. X. Liu and Z. H. Zhang [9] combined the fuzzy theory with wavelet neural network, and put forward an evaluation method for network information security. G. H. Gao, X. Y. Li, B. J. Zhang and W. X. Xiao [10] performed information security risk assessment based on information measure and fuzzy clustering, applied a new measure method and fuzzy clustering in security risk assessment, the new method quantified risk factors of all data and the dependence degree of safety with the mutual information computing; it could overcome the K-means's shortcoming of sensitive to initial value. Y. S. Huang, C. F. Tian and F. Wei [11] combined BP neural network with ES (Experts system) and proposed a method to evaluate the risk factors in information systems and its weight. X. Sun [12] proposed a hybrid neural network based on the combination of GA (Genetic Algorithm) and BP algorithms; this method improved the weights of the neural network and enhanced the training precision of the neural network in comprehensive evaluation. F. Lin, W. H. Zeng, J. B. Xiaohou and Y. Jiang [13] proposed optimizing for large time delay systems by BP neural network and evolutionary algorithm improving, utilized the initial weights of neural network to choose controller performance, analyzed and studied its algorithm and system architecture, and this new control system got better results and energy saving. Z. J. Wu, L. Wang, and R. Shi [14] designed an evaluation model for ATM system based on an improved three-layer BP neural network to solve the air traffic management (ATM) information security problems. Z. B. Zhou and J. L. Zhou [15] proposed a probabilistic safety evaluation methods for system based on Bayesian networks. Y. Fu and X. P. Wu [16] introduced the Bayesian network inference algorithm, combined expert knowledge with Bayesian network inference rules to build an information security risk evaluation model. J. G. Zhao, Q. Zhang, and Y. Fu [17] proposed a security risk evaluation method based on Bayesian network, established Bayesian network model for the information systems from the real application, combined a priori information given by experts with obtained evidence, and applied Pearl method to complete evaluation of the model. H. Y. Liu, W. F. Wang, and H. L. Cai [18] proposed a model which combines artificial networks and the methods of fuzzy comprehensive evaluation. S. K. Shen and Y. M. She [19] put forward an improved method of fuzzy theory and BP neural network for evaluation. Q. Yu and L. Feng [20] proposed a network security evaluation method based on BP neural network. M. S. Liu, W. Z. Liao and S. J. Sun [21] proposed a risk assessment method which combines wavelet neural network (WNN) and entropy-grey correlation, creates a WNN model. Although the safety evaluation method for the communication system is effective, it does not give the scope of the evaluation model which it is applicable to. The application of the evaluation model is still immature, especially for the specific air traffic control system. The relationships between many targets' attribute are non-linear, thus it is difficult for general methods to reflect this relationships. Many sources of information are incomplete; the evaluation rules are often contradictory, even incoherent to follow.

III. The Evaluation Model Of ATM Information System Based On Bayesian Regularization

The information security of ATM system is affected by natural conditions, the human factors, system performance and device performance. Air traffic control system is a highly complex nonlinear system which makes the traditional safety evaluation method no effective. The neural network used in the security evaluation for ATM system improves evaluation accuracy and evaluation speed, and it also overcomes deficiencies presented in the traditional methods such as AHP (Analytic Hierarchy Process) , gray theory and fuzzy evaluation method.

In the realm of evaluation for air traffic control information systems, Z. J. Wu, L. Wang, and R. Shi [14] proposed an approach of information security evaluation for ATM system based on an improved BP model of artificial neural network. BP neural network was widely used in function approximation, intelligent control, pattern recognition and many other fields. However, the standard BP algorithm is slowly convergent and easy to get into local minima. Adopting increased momentum and conjugate gradient learning algorithm can improve the generalization ability of BP neural network, which did not achieve the desired result. The generalization capability is an important measurement of the neural network performance. BP neural network based on Bayesian regularization can improve the generalization capability and convergence speed of the network. This method applied to the evaluation of the air traffic control information systems can further improve the evaluation of accuracy and speed.

A. The Indicator System Hierarchy of ATM Security Evaluation

ATM is an important part of the civil aviation communication system, running with the air traffic control communication, navigation, surveillance, weather, intelligence, air traffic control data, as well as communication equipment, communication media, navigation equipment, meteorological equipment, aeronautical information equipment and other related hardware [22]. With comprehensive considerations about the safety of ATM system, network and management, we use AHP to establish an indicator system which fits to air traffic control systems.

We select 25 representative indicators from the operation safety of ATM system, the security of ATM network and the security of integrated management of air traffic control system, and then establish an evaluation indicator system which is shown in TABLE I.

This indicator system can sufficiently reflect the performance of the ATM system from the following aspects [23]: (a) The normal operation ratio of equipment. (b) Equipment running in good ratio. (c) Reliability of the ATM system. (d) Availability of the system. (e) The

ATM system accuracy or system error. (f) Missing ratio. (g) False alarm ratio. (h) Flight consistency. (i) Backup and recovery management. (j) Data encryption. (k) Digital signatures. (l) Key handshake. (m) Authority and the access control technology. (n) Message authentication code. (o) Vulnerability scanning. (p) Network isolation. (q) Security audit. (r) Intrusion detection. (s) Firewall. (t) Management mechanism set up. (u) Safety of personnel management. (v) The management of contingency plans. (w) Environmental management. (x) The management of technical information. (y) Review and revision.

TABLE I.
EVALUATION INDICATOR SYSTEM

Goal	Missions	Assets and Capacities
The Security of ATM (A)	The security of ATM equipment (B1)	The normal operation ratio of equipment. (C_1)
		Equipment running in good ratio (C_2)
		Reliability of the system (C_3)
		Availability of the system (C_4)
		The system accuracy or system error (C_5)
		Missing ratio (C_6)
		False alarm ratio (C_7)
		Flight consistency (C_8)
		Backup and recovery management (C_9)
	Software & Hardware Security (B2)	Data encryption (C_{10})
		Digital signatures (C_{11})
		Key handshake (C_{12})
		Authority the access control technology (C_{13})
		Message authentication code (C_{14})
		Vulnerability scanning (C_{15})
		Network isolation (C_{16})
		Security audit (C_{17})
		Intrusion detection(C_{18})
		Firewall(C_{19})
	Management Security (B3)	Management mechanism set up (C_{20})
		Safety of personnel management (C_{21})
		The management of contingency plans (C_{22})
		Environmental management (C_{23})
		The management of technical information(C_{24})
		Review and revision(C_{25})

B. Classifications of the Level of Security

Combing requirements of Information Security Techniques-Protection Guide of Information Security Classification Level [24] with the characteristics of air traffic control information systems, we divide the security levels of ATM system into five levels as highly safe , safe , dangerous, highly dangerous , extremely dangerous, then we quantify five levels between 0-1, shown in TABLE II.

TABLE II.
TYPE SIZES FOR CAMERA-READY PAPERS

Highly safe	Safe	Dangerous	Highly dangerous	Extremely dangerous
0.8-1.0	0.6-0.8	0.4-0.6	0.2-0.4	0.0-0.2
A	B	C	D	E

C. Evaluation Model of ATM Information Systems

The steps to model network for ATM security situation evaluation based on Bayesian neural are quantifying and normalizing the air traffic control information systems' security indices, then regarding the normalized values as input vector for Bayesian neural network. The network outputs the security level index. We use training samples to train the network model, and different output values will be obtained from different input vectors. Training will be terminated when network achieves the specified accuracy. Thus the trained network can be an effective tool for air traffic control information systems security evaluation. The evaluation model based on Bayesian neural network is shown in Fig.1.

The model contains a single hidden layer, and the input layer is quantified in 25 index and normalized. In the Bayesian neural network, hidden nodes are determined by trials, the number of node for the output layer is one, and the output combined with classifications of the security level in air traffic control system (shown in TABLEII) can be the appropriate level of evaluation.

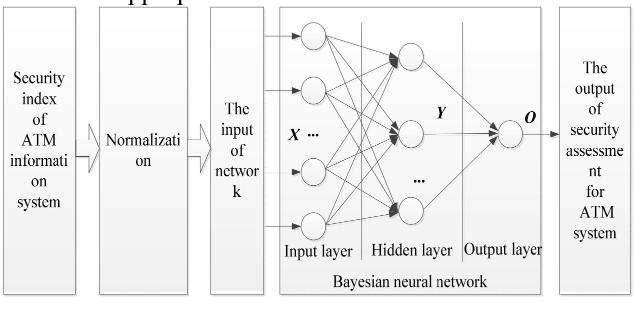


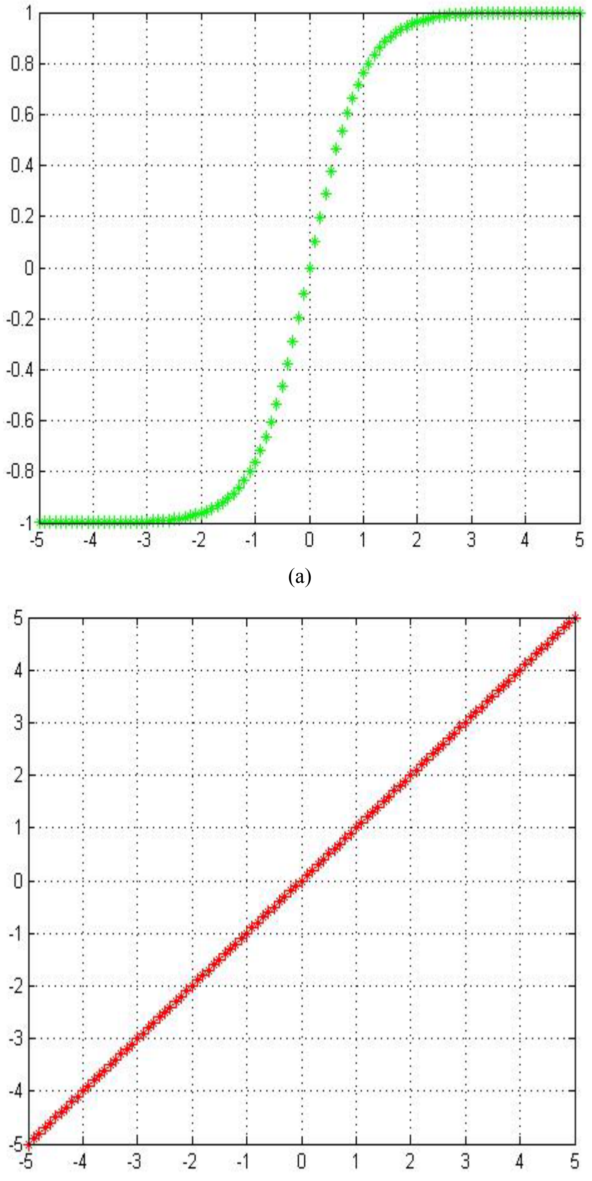
Figure 1. Bayesian neural network evaluation model for ATM information systems

IV. EXPERIMENTS ANALYSIS AND RESULTS

We apply the real operating data of air traffic control information systems and the proposed indicator system to simulate and test the network based on Bayesian rules, and then validates the proposed evaluation model through simulating and testing to solve the complicated nonlinear relationship among information security measurements of the air traffic control system.

A. Modeling and Parameter Settings

According to the indicator system for air traffic management information system evaluation, we use the data provided by Communication, Navigation and Surveillance Systems Operation and Maintenance Procedures in Civil Aviation of China [25], in which 25 security indicators of air traffic control information systems are regarded as the input of Bayesian neural network. Safety evaluation level is the output of the neural network. In the Matlab simulation environment, we use training function *trainbr* to train learning samples for network, and we adopt logarithmic function *S* as the transfer function from the input layer to the hidden layer, while function *purelin* is used as transfer function from the hidden layer to the output layer. Logarithmic function *S* and function *purelin* are demonstrated in Fig.2, with parameters in the Bayesian neural network being shown in TABLE III.



(a)

(b)

Figure 2. Bayesian neural network evaluation model for ATM information systems

TABLE III.
TRAINING PARAMETER SETTINGS FOR BAYESIAN NEURAL NETWORK

Parameter	Parameter values
epochs	1000
goal	0.0001
learning rate	0.075
adjust parameters by Marquardt algorithm	0.005
show	10
other	default

We determine the nodes of hidden layer by trials. Hidden layer nodes have a significant impact on system performance. If the number of hidden nodes is too small, information capacity of the network obtained from the sample will be poor, and the law of sample will be not enough to be summarized and embodied in the training set. On the other hand, if the number of hidden nodes is too large, the non-regular contents (such as noise) of the sample will be learned and remembered, in which the problem called "overfitting" will occur, reducing the generalization capability and increasing the training time. The following formulas are used for reasonable determination of the number of the hidden layer.

$$m = \sqrt{n+l} + a = \log_2 n = \sqrt{nl} \qquad (1)$$

In (1), m indicates the hidden layer nodes, n is the input layer nodes, l is the output layer nodes, a is a constant between 1 and 10. We observe the impact of hidden layer neurons on the performance of the system by following experiments.

When the number of neurons in the hidden layer is 5, the curve of error performance is shown in Fig.3, where we can see that the network stops training after nine iterations. The best error value is less than 0.0001, but the error curve of test is unstable. The error of the test has actually increased after six iterations.

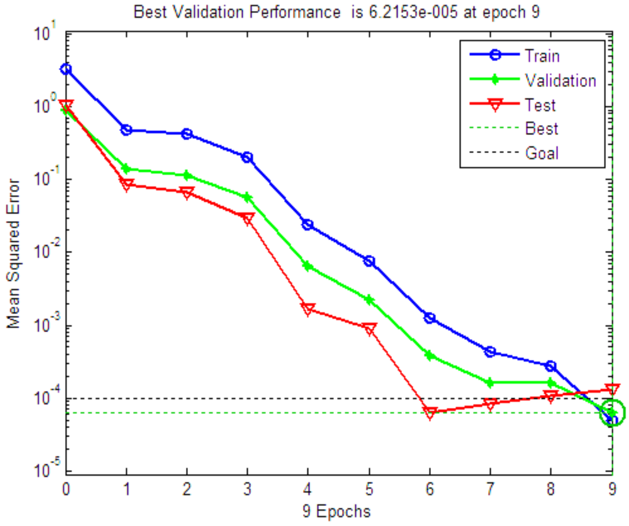


Figure 3. Error performance curve of 5 neurons in the hidden layer

When the number of neurons in the hidden layer is 6, the curve of error performance is shown in Fig.4.

In Fig.4, we can see that the network stops training after ten iterations. The best error value is less than 0.0001, but the error curve of test is unstable. The error of the test has actually increased after eight iterations.

When the number of neurons in the hidden layer is 7, the curve of error performance is shown in Fig.5, where we can see that the network stops training after ten iterations. The best error value is less than 0.0001, but the error curve of test is either unstable.

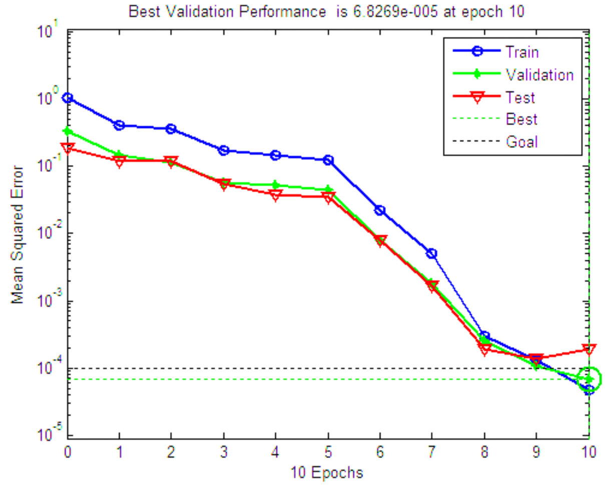


Figure 4. Error performance curve of 6 neurons in the hidden layer

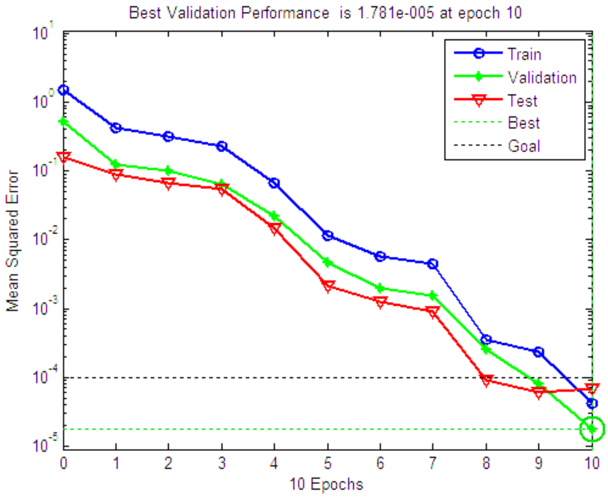


Figure 5. Error performance curve of 7 neurons in the hidden layer

When the number of neurons in the hidden layer is 8, the curve of error performance is shown in Fig.6.

According to the curves in Fig.6, we can see that the network stops training after nine iterations. The best error value is less than the goal error value, validation and test error values are less than the trained error value. The error performance curves decline gradually to reach the goal error value, and the overall trend of three curves is almost the same. The error performance of the system curve is the most stable, and the generalization ability of this model is the best.

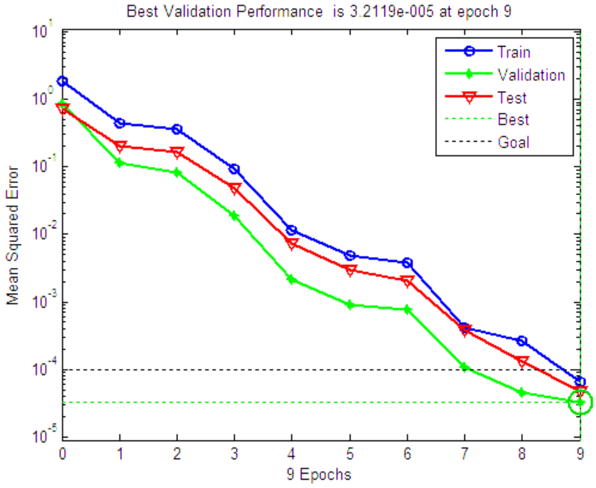
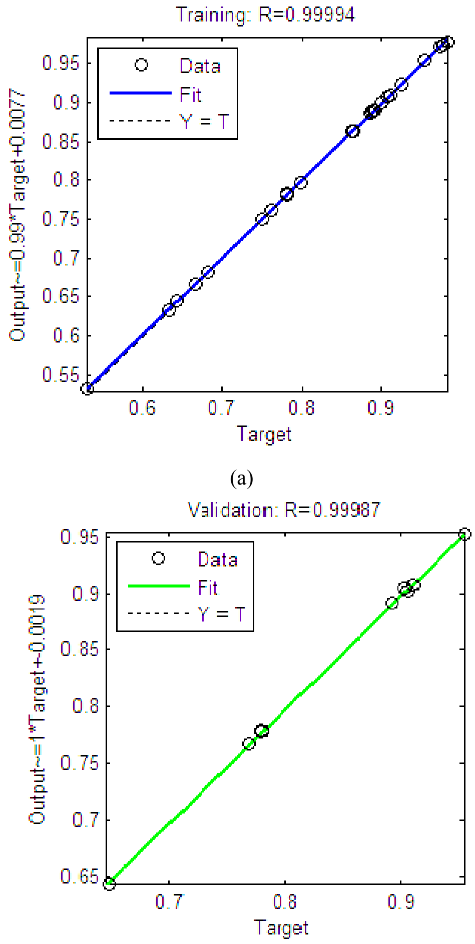


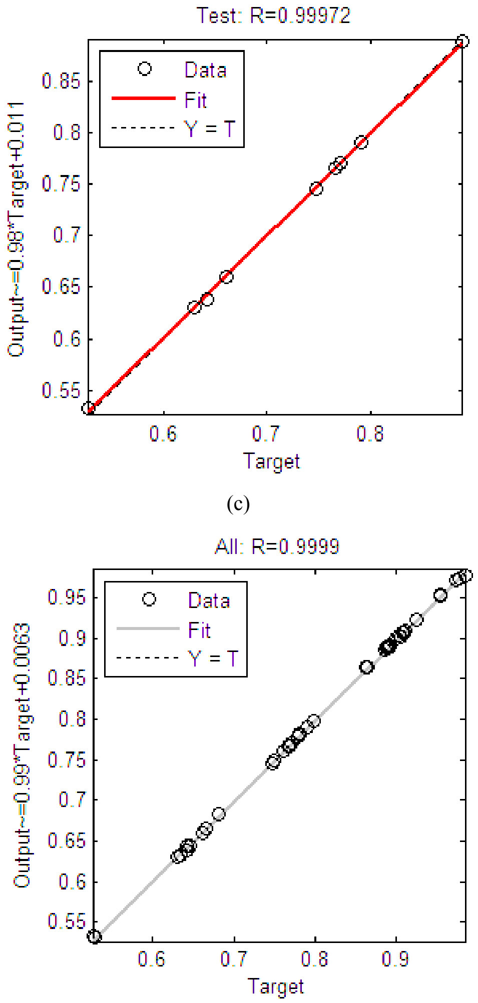
Figure 6. Error performance curve of 8 neurons in the hidden layer

To further validate the performance of this network, we use function *postreg* to analyze the non-linear regression between the output of the network and the actual output. Approximation effect is learned from the correlation coefficient between output of network and the actual data, which can be considered as the discriminated basis of the network training results. When the hidden layer node is 8, regression curve of expectations-output is demonstrated in Fig.7.



(a)

(b)



(c)

(d)

Figure 7. Expectations - output regression curve for 8 neurons in the hidden layer

In this paper, we use linear regression between the simulation output vector of network (the actual assessment results of ATM Information System) and the target vector (evaluation of the ATM network information system) to analyze the result, and regard the output correlation coefficient as the performance evaluation mark of the network. When the network performance is in good condition and reaches to a certain extent, the simulation values are equal to the actual output values of network. At this point, the intercept is equal to 0, the gradient is 1 and the goodness-of-fit is 1. In practical applications, the goodness-of-fit R is taken greater than 0.80. According to Fig.8, when the node number in the hidden layer is 8, goodness-of-fit of validation, training, testing, and all samples are close to 0.999, which indicates that the performance of network is very good.

According to the above experiments, we can conclude that when the number of neurons in the hidden layer is 8, training speed is faster, error is smaller, fitting is better, the performance of network is also better. Therefore, the structure of the neural network is identified as 25-8-1, and the weights obtained from training in this model can be treated as security evaluation for the air traffic control information systems.

B. Test with Bayesian Neural Network

When the network is identified and the training has been completed, we use the trained network to test the evaluation model, and test the performance of the proposed network through selecting the data of four kinds of test samples under different circumstances from the actual running state of the air traffic control information systems. The test data are shown in TABLE IV and test results are demonstrated in TABLE V.

TABLE IV.
TEST SAMPLES

	E1	E2	E3	E4	E5
C1	0.83	0.45	0.9	0.8	0.8
C2	0.80	0.52	0.92	0.8	0.82
C3	0.82	0.63	0.93	0.76	0.75
C4	0.77	0.62	0.9	0.75	0.79
C5	0.75	0.48	0.85	0.75	0.75
C6	0.84	0.46	0.9	0.84	0.8
C7	0.83	0.39	0.96	0.8	0.8
C8	0.8	0.36	0.91	0.83	0.8
C9	0.76	0.54	0.85	0.75	0.75
C10	0.86	0.4	0.95	0.8	0.8
C11	0.76	0.56	0.9	0.75	0.75
C12	0.74	0.5	0.9	0.78	0.75
C13	0.76	0.45	0.95	0.75	0.85
C14	0.72	0.55	0.98	0.78	0.75
C15	0.85	0.6	0.85	0.75	0.78
C16	0.83	0.5	0.9	0.8	0.8
C17	0.72	0.56	0.85	0.72	0.76
C18	0.75	0.6	0.85	0.79	0.75
C19	0.75	0.7	0.88	0.75	0.78
C20	0.80	0.5	0.94	0.8	0.84
C21	0.90	0.66	0.9	0.73	0.7
C22	0.80	0.69	0.92	0.85	0.82
C23	0.80	0.72	0.91	0.8	0.8
C24	0.75	0.5	0.85	0.75	0.75
C25	0.78	0.6	0.9	0.81	0.8

TABLE V.
TEST PERFORMANCE OF BAYESIAN NEURAL NETWORK

Test set	Desired output	Actual output	Network error	Level of security
E1	0.896	0.884	1.2%	A
E2	0.965	0.970	0.51%	A
E3	0.774	0.772	0.25%	B
E4	0.550	0.554	0.12%	C
E5	0.340	0.350	2.5%	D

According to the test results of the network, we can see that the test results are in line with the security level set of the air traffic control information systems. The test results illustrate that the evaluation model for air traffic control information systems based on Bayesian regularization is practical. The performance of neural network is stable and the error is very small. Test results are consistent to actual results. At the same time, we can conclude that neural network based on Bayesian regularization has good performance in nonlinear capacity, generalization ability and fault tolerance. It can be used for security evaluation in the actual air traffic control information systems.

V. Conclusion

According to indicator elements related with the security of the air traffic control information systems, we establish an evaluation indicator system which is scientific, full-scale covered and optimized. On the basis of this indicator system, we propose a security evaluation model for ATM system based on Bayesian regularization. Simulation results show that the evaluation method reflects the safe operation state of the air traffic control information systems. The test results show that the error meets the requirement of equipment running with the normal ratio and equipment integrity, which are required by Communication, Navigation and Surveillance Systems Operation and Maintenance Procedures in Civil Aviation of China[24]. With the proposed method, we can analyze and study the information security threats that the air traffic control information systems are facing, and the information security events occur in ATM system. Then we can guide the ATM system to establish, improve an information security system, and timely find out the existing risks in the system, Thus we may take appropriate safety measures to compensate for the vulnerability of the system as soon as possible, prevent information security incidents from occurring, and ensure the air transport safety and efficient operation.

Acknowledgment

This work was supported in part by China National Science Foundation under Grant No.61170328 and U1333116, Key Project of Tianjin Natural Science Foundation under Grant No.12JCZDJC20900, and the Fundamental Research Funds for the Central Universities of CAUC under grant 31122013P007, 3122013D007, and 3122013D003.

References

[1] S. Patel and J. Zaveri, "A Risk-Assessment Model for Cyber Attacks on Information Systems," *Journal of Computer*, vol. 5, pp. 352-358, March 2010.

[2] Overall Security Concept, *ICAO ATNP Security Working Group-ATN Panel Working Group 1*, August 1996.

[3] T. McParland, V. Patel, and W. J. Hughes, "Securing air-ground communications," *2001. DASC. 20th Conference on Digital Aviation Systems, Daytona Beach, FL,* vol.2, pp.7A7/1 - 7A7/9, October, 2001.

[4] E. Filiol and S. Josse, "New Trends in Security Evaluation of Bayesian Network-based Malware Detection Models," *Proceedings of 2012 45th Hawaii International Conference on System Sciences, USA*, January 2012.

[5] K. S. Swarup and P. B. Corthis, "ANN approach assesses system security," *IEEE Computer Applications in Power*, vol. 15, pp. 32-38, January 2002.

[6] G. A. Ramos, A. Torres and J. P. Rognon, "Análisis de Confiabilidad de Sistemas Industriales Aplicando Redes Bayesianas Considerando Aspectos de PQ y Seguridad - Caso de Estudio Sistema IEEE 493," *IEEE. Latin America* Transactions, vol. 5, pp. 605-610, December 2007.

[7] A. Taktak, A. Eleuteri, M. Aung, et al. "External Validation of a Bayesian Neural Network Model in Survival Analysis," *ICMLA 2008, San Diego, California, USA*, pp. 607-612, December 2008.

[8] D. Wei and M. L. Zhang, "Nonlinear identification model of neural network based on Bayesian method", *Computer Engineering and Applications*, vol.41, pp. 5-11, November 2005.

[9] D. M. Zhao, J. X. Liu and Z. H. Zhang, "Method of Risk Evaluation of Information Security Based on Neural Networks," *Machine Learning and Cybernetics, 2009 International Conference*, vol. 2, pp. 1127-1132, July 2009.

[10] G. H. Gao, X. Y. Li, B. J. Zhang, and W. X. Xiao, "Information Security Risk Assessment Based on Information Measure and Fuzzy Clustering," *Journal of Software*, vol. 6, no. 11, pp. 2159-2166, November 2011.

[11] Y. S. Huang, C. F. Tian and F. Wei, "Fuzzy Comprehensive Evaluation Mode on the Investment Risk of Real Estate Based on BP Neural Network and Expert System," *E-Business and Information System Security, 2009. EBISS '09. International Conference,* pp. 1-5, May 2009.

[12] X. Sun, "A BP Neural Network Model Based on Genetic Algorithm for Comprehensive Evaluation", *2011 Third Pacific-Asia Conference on Circuits, Communication and system, China,* pp. 1-5, August 2011.

[13] F. Lin, W. H. Zeng, J. B. Xiaohou, and Y. Jiang, "Optimizing for Large Time Delay Systems by BP Neural Network and Evolutionary Algorithm Improving", *Journal of Software*, vol. 6, no. 10, pp. 2050-2055, October 2011.

[14] Z. J. Wu, L. Wang, and R. Shi, "Approach of information security assessment for ATM based on improved BP neural network method," *Journal of Communications*, vol. 32, pp.150-158, 2011.

[15] Z. B. Zhou and J. L. Zhou, "Probabilistic safety assessment research based on Bayesian networks," *Systems Engineering*, vol. 21, pp. 636-644, 2006.

[16] Y. Fu, X. P. Wu, and C. H. Yan, "The method of information security risk assessment using Bayesian network," *Technology of Wuhan University*, vol.52, pp. 631-634, 2006.

[17] J. G. Zhao, Q. Zhang, and Y. Fu, "Application of Bayesian network inference in security risk assessment of information systems," *Naval University of Engineering*, vol. 19, pp. 67-70, 2007.

[18] H. Y. Liu, W. F. Wang, and H. L. Cai, "A comprehensive security evaluation model of information systems based on artificial neural networks," *Computer Engineering and Science*, vol. 30, pp. 16-18, 2008.

[19] S. K. Shen and Y. M. She, "Approach to information systems security risk assessment based on fuzzy-BP neural network," *Computer simulation*, vol.28, pp. 91-94, 2011.

[20] Q. Yu and L. Feng, "Approach for network security evaluation based on BP neural network", *Computer Engineering and Design*, vol. 29, pp. 1963-1966, 2008.

[21] M. S. Liu, W. Z. Liao, and S. J. Sun, “Research on Applying the Theory of Wavelet Neural Network and Entropy-Grey Association to the Security Risk Assessment for E-Government Information System,” *Journal of Computers*, vol. 6, no. 8, pp.1699-1706, 2011.

[22] Y. Shen and P. Zhao, “BP models and empirical Bayes method in the research on complaint behavior tendency,” *Statistical Research*, vol. 11, pp. 55-59, 2004.

[23] CCAR-93TM-R4, “Air Traffic Management,” *Air Traffic Management Bureau of China's Civil Aviation Authority*, April 2007.

[24] GB/T 22240-2008, “Information Security Technology-Information System Security Protection Rating Guide,” *Standardization Technical Committee of the National Information Security*, January 2008.

[25] AP-115TM-134-R1, “Communication, Navigation and Surveillance Systems Operation and Maintenance Procedures in Civil Aviation of China,” *Air Traffic Management Bureau, Civil Aviation Administration of China,* October 2004.

Lan Ma, born in 1966. She received Master degree in computer science and technology and PhD degree in system engineering from Tianjin University, Tianjin city, China, in 2006 and 2011 individually. Her main research field is Air Traffic Management.

She is associate professor with school of air traffic management, Civil Aviation University of China (CAUC).

Jia Xu, born in 1987, Master Degree Candidate in Civil Aviation University of China (CAUC), main research field is information security.

Zhijun Wu, born in 1965, PhD, Professor in Civil Aviation University of China (CAUC), main research field is network and information security.