Air Targets Threat Assessment Based on BP-BN

Haiyan Yang, Cheng Han, and Congliang Tu
Air Control and Navigation College of Airforce Engineering University, Xi'an and 710051, China
Email: Haiyan Yang, yanghy07@yeah.net; Cheng Han, 597931972@qq.com; Congliang Tu,534995138@qq.com

Abstract —Air targets threat assessment is an important part of command and control. Recently, the technical difficulties of assessment are how to deal with quantitative and qualitative information effectively, and how to analyze and process uncertain information. Owing to the singleness and the insufficiency of traditional processing methods, a new parallel processing method is put forward. In order to get the dynamic threat value, the strong generalization ability of Back-Propagation is used to deal with quantitative indicators, at the same time, the strong reason ability of Bayesian network is used to analyze qualitative indicators to acquire the static threat value. Finally, we get comprehensive threat value by linear weighting the two kinds of threat values. Through the case analysis and the prediction of ten batches of target, combined with the simulation in the Matlab and Genie software, the method is proved to be effective. The result of the simulation shows: the comprehensive threat value is more credible than that got by traditional method.

Index Terms—Threat assessment, Back-Propagation netwrok, Bayesian network

I. INTRODUCTION

With regard to the current research on Threat Assessment (TA), there are some works at home and abroad. The common threat assessment methods mainly include multi-attribute decision-making method, rough set method, neural network method, Bayesian network method etc. The commonality of these methods is to sort the threat values, the inadequacies are the classification of the assessment is too subjective, the treatment of the threat factor is not appropriate. Literature [1] lists 22 threat factors, but from the perspective of real-time evaluation, we need to reasonably choose corresponding threat factors. In [2], a fuzzy Bayesian method is proposed to evaluate the threat level, but the selection of membership function is not convincing. In [3], combat ability is added to the evaluation index, but the typical logarithmic method cannot deal with incomplete information. In the literature [4], a method of BP neutralization of local Bayesian network is proposed. The method improves the local precision, but what BP neutral network outputs still serves as the root node in the whole Bayesian network. It remains to be proved whether the accuracy of the entire network is improved. Literature [5] proposed a parallel assessment method. The idea is that qualitative and quantitative indicators are assessed separately, but the scientific disposition of quantitative indicators is not strong.

Manuscript received September 18, 2017; revised January 16, 2018.
This work was supported by the National Science Foundation of China under Grant No. 61472441.
Corresponding author email: 597931972@qq.com.
doi:10.12720/jcm.13.1.21-26

This paper proposes a new method of target threat assessment based on BP-BN. BP network has a good self-learning ability to predict, its powerful nonlinear functional ability can predict the data in real-time changes. Bayesian Network (BN) is similar to the human brain's thinking model, and its causal association model has an advantage for the expression and reasoning of uncertainty knowledge. Therefore, this paper combines the BP network functional capability with strong reasoning ability of the threat assessment method of BN network, besides; the comprehensive threat value of 10 batches is obtained by simulation and compared with the original threat value to prove the validity and rationality of the method.

II. INTRODUCTION OF THE RELEVANT PRINCIPLES

A. Introduction of BP Neural Network

Neural network has been widely used in pattern recognition, intelligent control and signal processing in recent years. It has the ability of self-learning, self-organization and strong robustness. BP neural network belongs to the multi-layer neural network, which contains the input layer, the output layer and a number of hidden layers. The specific number of each layer is decided by specific issues. The main principle of BP neural network is to continuously adjust the connection weights between neurons and front and back layers by studying the samples. The process has obvious advantages for dealing with nonlinear indexes, and is not subjective and man-made. So it has higher reliability. Common BP network structure is shown in Fig. 1.

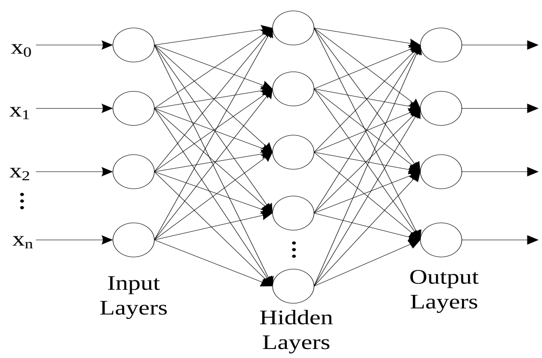

Fig. 1. BP network structure

B. Introduction of Bayesian Networks

Bayesian Network (BN) is a representation and reasoning model of uncertain knowledge based on probability analysis and graph theory, which can be represented by a pair of tuples $B=\langle G,P\rangle$.(1) $G=\langle V,E\rangle$ means network structure that represents a directed acyclic graph. $V=\{V_1,V_2,\cdots V_n\}$ is a set of nodes in a directed acyclic graph. E represents the set of directed edges. (2) P represents the conditional probability table set of the network nodes. The conditional probability of the root node is a prior probability, and the other nodes use the conditional probability table to represent the connected relation between the node and its parent node. By the assumption of conditional independence, the joint probability between several variables can be decomposed into:

$$P(V_1,V_2,\cdots,V_n)=\prod_{i=1}^{n}P\left(V_i\middle|Pa(V_i)\right) \tag{1}$$

C. Air Target Measurement Principle Model

The east-north-day coordinate system is constructed for the air attack target, where the zonal is the X axis and the positive east is positive; the meridional direction is the Y axis, the north is positive; the vertical direction is the Z axis, , Assuming that at some point, our radar to detect the target shown in Fig. 2.

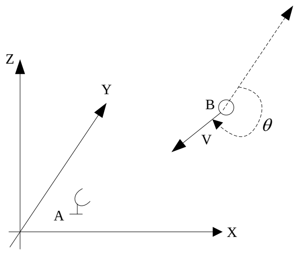

Fig. 2. Radar detect air target coordinate system.

where A is our radar, B is for the incoming target, θ represents the provisions of the flight direction and the angle of the north for the heading angle. Radar for the distance, speed, height of the detection formula is as follows:

$$s=\frac{1}{2}c\cdot\Delta t_1 \tag{2}$$

$$v=\frac{s_2-s_1}{\Delta t_2} \tag{3}$$

$$H=h+R\times\sin\delta+\frac{R^2}{R_m} \tag{4}$$

c represents the propagation speed of the radar pulse, Δt_1 , Δt_2 is for the time interval between the transmitted pulse and the echo pulse, R is the radial distance of the target, R_m is the Earth's radius. The movement of the target has the characteristics of continuous non-linearity. h represents the altitude of the radar antenna, δ is for the antenna elevation.

The type of target can be based on the radar from the target's three directions to determine the RCS value. The intention of the target is mainly obtained by other information. Combat capability and interference ability can be determined when the target type is determined, we do not repeat this due to the space reasons

These indicators include both non-linear quantitative indicators such as speed, height, distance, heading angle; and qualitative indicators such as type, intention, combat capability, interference ability, which intention also has the uncertainty of the source of intelligence. How to deal with these indicators scientifically and assess the threat of incoming targets comprehensively is the difficult problem.

III. A Treat Assessment Method of Incoming Targets Based on BP－BN

The traditional approaches to assess speed, heading angle, height, distance, interference ability and other indicators are too simple; even worse, the selection of the evaluation indicators does not reach a unified opinion. In this paper, literatures [5]-[7] are the main references to select the indicators of TA. The target size, target speed, target heading angle, target interference ability, target height, target distance, target combat capability and target intention are selected as the threat evaluation index set. The target type, the target interference ability, the target combat capability, the target intention are the qualitative indexes, the target speed, the heading angle, the height and the distance can be measured by the ground radar in real time. The variation relationship of these quantitative indicators is unknown, but it can be measured by the BP network training. Using its nonlinear mapping ability, dynamic threat value can be obtained. Through the Bayesian network reasoning and the use of its uncertainty for the strong reasoning information, static threat value of the qualitative indicators can be acquired. Finally, we use the linear weight to get the ultimate threat of the target. The threat assessment framework is shown in Fig. 3.

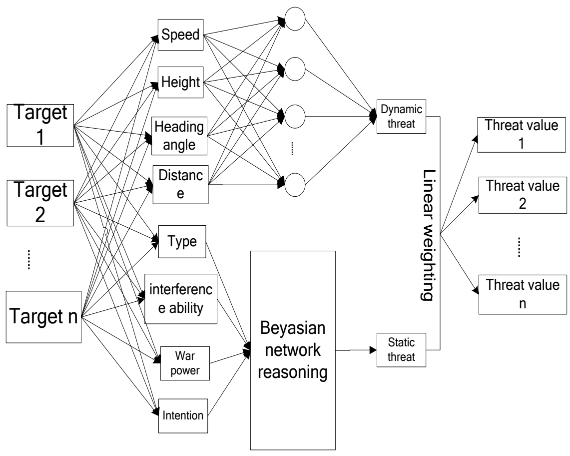

Fig. 3. Threat assessment framework.

A. Dynamic Assessment Method of Target Movement Information Based on BP

Firstly, the sample information is pretreated and normalized. The pretreatment was based on G. A. Miller's 9-level quantification theory:

The target speed is quantified as 1 to 9 in equal intervals of 0-1800 m/s (200 m/s), and the target heading is quantified to 9-1 in equal intervals of 0-360^{o} and so on (40^{o}). The target height is quantified to 1-9 in the order of 1-9Km; target distance is quantified to 9-1 in equal intervals of 0-450Km.The datum are normalized by:

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{5}$$

According to the empirical formula (6) and several training, the suitable number of hidden layer nodes is obtained. The number of hidden layer nodes is controlled by the nodes of the input and output layers.

$$q = \sqrt{r+s} + (1 \sim 10) \tag{6}$$

The network training algorithm selects the gradient descent algorithm, and the node transfer function uses the Sigmoid function. Finally, the trained network is used to dynamically predict the threat value according to the parameters of the moving target. The above method is shown in Fig. 4.

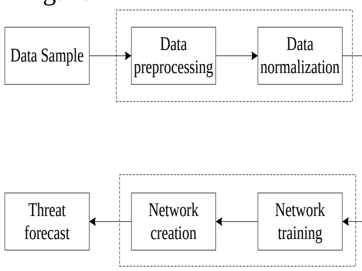

Fig. 4. Target threat assessment on BP.

B. Static Threat Assessment Process Based on BN

As for the four qualitative indicators, i.e. target type, target intention, target interference ability and target combat capability, in order to analyze their influence on the threat degree; we construct the BN network model to continue the analysis.

(1) Network construction

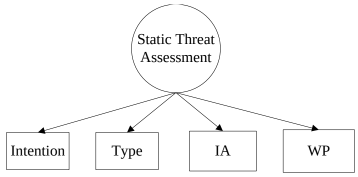

Fig. 5. Target Threat Assessment based on BN.

The status of each node in Fig.5 is expressed as follows:

Threat degree (TD): threat degree is divided into High, Medium, and Low.

Intention (In): Attack, Invest, Patrol.

Target Type (Type): the big target, small target and helicopter are mainly considered.

Interference ability (IA): Strong, Medium, Weak.

War power (WP): Strong, Medium, Weak.

(2) Parameter learning

After establishing the BN evaluation model, we need to study the parameters of the network nodes so as to obtain the model that can be used to reason. Network parameters can be learned from a large number of data samples or identified by relevant domain experts. In this paper, we obtain the conditional probability table of the corresponding node through the expert knowledge. As for the prior probability of the threat degree, we designate it as. After determining the conditional probability table of each node, we can carry out the posterior probability reasoning of relevant threat degree. The corresponding node conditional probability table is shown in Table I.

TABLE I: NODE CONDITIONAL PROBABILITY TABLE

TD	P(IN/TD)			P(Ty/TD)			P(IA/TD)			P(WP/TD)		
	Attack	Invest	Patrol	Big	Small	Copter	Stron	Mediu	Weak	Stron	Mediu	Weak
High	0.8	0.1	0.1	0.76	0.18	0.06	0.6	0.2	0.2	0.7	0.1	0.2
Medium	0.6	0.3	0.1	0.4	0.4	0.2	0.45	0.3	0.25	0.5	0.3	0.2
Low	0.45	0.25	0.3	0.3	0.5	0.2	0.4	0.45	0.15	0.4	0.2	0.4

(3) Reasoning method

The reasoning method mainly uses Bayesian reasoning, according to the observation evidence of the evidence nodes; the posterior probability of the threat node is calculated. The reasoning formula is shown as below.

$$P(T|E=e) = \frac{P(T, E=e)}{\sum_{T} P(T, E=e)} \tag{7}$$

After obtaining the posterior probability of the threat node, it needs to be converted into a specific threat value, that is, to find the static threat value of the target. This paper defines the high, medium and low expectation value of 0.9, 0.5, 0.1, the static threat is:

$$T_s = 0.9 \cdot P(TD = high) + 0.5 \cdot P(TD = medium) + 0.1 \cdot P(TD = low) \tag{8}$$

Finally, the dynamic threat value and the static threat value are linearly weighted to obtain the total threat degree

$$T = \varepsilon T_d + (1-\varepsilon) T_s \tag{9}$$

In this formula, the weight factor ε represents the degree of preference of qualitative indicators or quantitative indicators. If $\varepsilon > 0.5$, it indicates that the threat places emphasis on quantitative indicators, on the contrary, it tends to qualitative indicators.

IV. Simulation Verification

In this paper, Matlab R2012b and Genie software are used to achieve the above method. First, select 60 sets of data as the training samples, test samples, 10 sets of data. The test data samples are shown in Table II.

BP network parameter setting: the number of input layer nodes is 4, the number of hidden layer nodes is 8, the number of output nodes is 1, the learning rate is 0.01, and the training target is 0.001. As input signal and expected output, 60 sets of training sample data are used to carry out the BP network training, as shown in Fig. 6. The trained BP network can predict the dynamic threat of 10 sets of test targets. BN network parameter settings are shown in Table I. Take the target 1 as an example，its simulation results are shown in Fig. 9.

TABLE II: Test Sample Data

No.	Type	velocity (m/s)	Intention	Height (Km)	Heading angle (°)	War power	Distance (Km)	In
1	Big	450	Invest	3	80	Medium	300	Medium
2	Big	400	Invest	7	30	Medium	100	Strong
3	Big	450	Invest	3.6	160	Medium	200	Medium
4	Big	800	Attack	7.5	40	Strong	100	Strong
5	Small	530	Attack	5	60	Strong	230	Strong
6	Small	650	Invest	6	80	Medium	200	Strong
7	Small	700	Attack	3.9	120	Medium	320	Strong
8	Copter	90	Patrol	1.5	120	Weak	240	Weak
9	Copter	110	Invest	3	30	Weak	300	Weak
10	Copter	100	Patrol	4.5	90	Weak	100	Weak

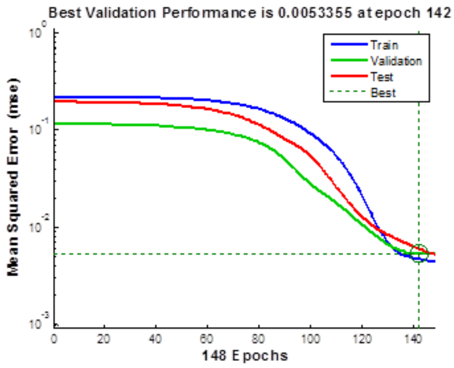

Fig. 6. BP network error curve.

It can be seen from Fig.6, after 148 iterations, BP network mean square error meets the requirement that we already set.

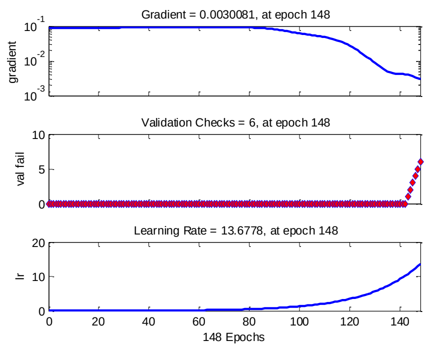

Fig. 7. BP network training status.

Fig. 7 shows that the learning rate increasing rapidly following the decreasing of the gradient from the 80th epochs. The learning rate reaches the highest level about 13.6778 at the 148th epochs.

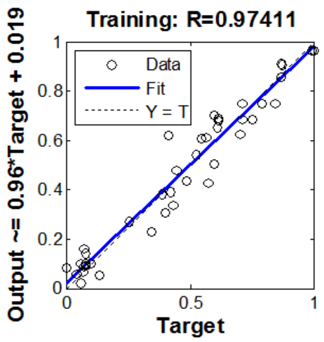

Fig. 8. Sample linear data regression graph.

The results of the linear regression analysis of the sample data are shown in Fig. 8, R represents the correlation coefficients of the training samples and the training results. In the figure, the abscissa is the target output, the ordinate is the actual output of the network, the solid line represents the ideal regression line, and the dotted line represents the optimal regression line. The data is more evenly distributed on both sides of the regression line, and the correlation between the actual output of the network and the target vector is very good. The dynamic threat value can be got after entering the above test sample into the constructed BP network.

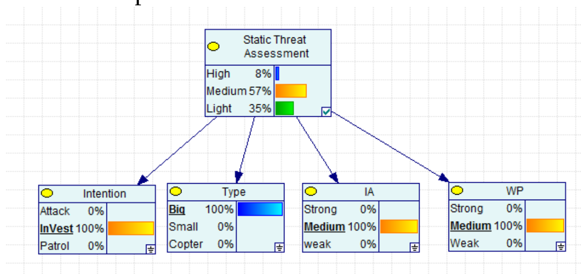

Fig. 9. BN static threat degree reasoning.

Fig. 9 shows that the probability of high, medium and low static threat is 0.08, 0.57 and 0.35 respectively, under the circumstances of investing, big type, medium IA and WP. From the equation (8), it can be calculated that static threat value is 0.392.

The dynamic threat values, static threat values, and comprehensive threat values for 10 batches of targets are shown in Table III. Set ε=0.5.

TABLE III: TARGET (STATIC) STATE THREAT

No.	Dynamic threat	Static threat	Comprehensive threat	True value
1	0.639	0.392	0.516	0.584
2	0.623	0.480	0.552	0.571
3	0.621	0.392	0.506	0.690
4	0.763	0.784	0.774	0.690
5	0.687	0.549	0.618	0.743
6	0.637	0.372	0.505	0.634
7	0.745	0.436	0.591	0.554
8	0.687	0.224	0.455	0.393
9	0.757	0.328	0.543	0.435
10	0.626	0.224	0.425	0.358

The order of comprehensive threat degree of goals is: Goal 4> Goal 5> Goal 7> Goal 2> Goal 9> Goal 1> Goal 3> Goal 6> Goal 8> Goal 10. That the threat degree of goal 4 becomes higher is due to the fact that the combat intent is taken into account, and the distance of the target 4 is nearest and the speed fastest. The result is consistent with the prior knowledge of the battlefield.

It can be seen from Fig. 10, based on BP-BN method, the forecast results for the target threat value is basically the same with the trend of the actual value. Compared with BN method, the prediction result of air multi-target threat based on BP-BN method is closer to the actual value and the average relative error is smaller.

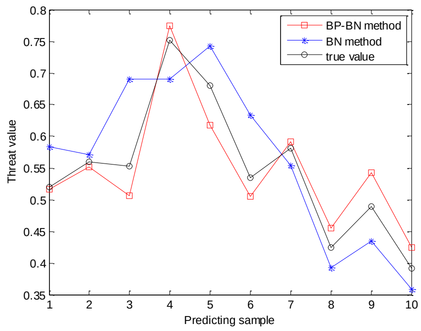

Fig. 10. Results forecast graph.

V. CONCLUSIONS

In this paper, BP neural network is used to combine with Bayesian network to deal with the method of evaluating air targets, comprehensive threat values are obtained by the combination of dynamic threat values and static threat values. The simulation shows that the predicted results of the 10 batch air targets are basically the same as the actual results. The disadvantage of this method is that the results of qualitative evaluation and quantitative evaluation are simply weighted fusion, and the gain of weight is subjective. Challenges of the threat assessment are how to deal with different kind of information from the sensor effectively and how to predict the threat value accurately. The next research can be carried out to improve the fusion method by the tandem use of various evaluation methods.

REFERENCES

[1] M. Libhaber and B. Feher, "Naval air defense threat assessment: Cognitive factors and model," in *Proc. Command and Control Research and Technology Symposium*, 2000, pp. 1-30.

[2] Y. Liu, S. D. Chen, *et al.*, "Threat assessment of manned/unmanned combat aerial vehicle formation air-to-ground attack based on FBNs," *Systems Engineering and Electronics*, vol. 34, no. 8, pp. 1636-1639, 2012.

[3] H. Chen and Q. Gong, "Threat ordering method based on overall combat effectiveness," *Electronic Technology*, vol. 28, no. 7, pp. 97-100, 2015.

[4] X. Zhou, C. F. Zhong, P. S. Chun, *et al.*, "Battle damage assessment of air-raid based on BP neuralized bayesian network," *Fire and Command Control*, vol. 41, no. 4, pp. 20-24, 2016.

[5] F. Tao and W. Jun, "Threat assessment of aerial target in air-defense," *Command Control & Simulation*, vol. 38, no. 3, pp. 64-69, 2016.

[6] E. G. Little and G. L. Rogova, "An ontological analysis of threat and vulnerability," in *Proc. Ninth International Conference on Information Fusion*, Italy,2006, pp. 1-8.

[7] Y. Zhang, B. Li, and J. Cui, "Method of target threat assessment based on cloud bayesian network," *Computer Science*, vol. 40, no. 10, pp. 127-131, 2013.

Haiyan Yang was born in Hebei Province, China, in 1972. She received the B.S. degree from Nanjing University of Science & Technology in 1995. She received the M.S. degree in the Aeronautics and Astronautics Engineering College of Air Force Engineering University in 2001. In 2012, she received her Ph.D. degree in instrument science and technology from Tsinghua University. Her research interests include situation assessment and Bayesian estimation.

Cheng Han was born in Hubei Province, China, in 1990. He received the B.S. degree from the Air Force and Engineering University, Xi'an, in 2015. He is currently pursuing the M.S. degree with the Air Traffic Control and Navigation College of Air Force Engineering University. His research interests include situation assessment and Bayesian estimation.

Congliang Tu was born in Zhejiang Province, China, in 1991. He received the B.S. degree from the Air Force and Engineering University, Xi'an, in 2015. He is currently pursuing the M.S. degree with the Air Traffic Control and Navigation College of Air Force Engineering University. His research interests include complex network, airspace operation and airspace safety.