Target Threat Assessment Based on Dynamic Bayesian Network

Xin Wang, Jialiang Zuo*, Rennong Yang, Zhenxing Zhang, Longfei Yue and Huiliang Liu
Air Traffic and Navigation College, Air Force Engineering University, Xi’an, China
Email: wxshhh@163.com

Abstract. Conventional threat assessment model based on Bayesian Network is a reasoning process in static environment, which is difficult to deal with a large number of broken air combat data in a complex dynamic battlefield environment. Motivated by this fact, a Dynamic Bayesian Network-based threat assessment model is established, and a theoretical method based on Expectation Maximization to deal with missing data is proposed. Finally, simulations are presented to verify the effectiveness of the proposed structure.

1. Introduction
Threat assessment is a typical non-structural complex multi-attribute decision problem related to uncertainty reasoning [1], which is an important basis for the force deployment and fire distribution [2].

Conventional threat assessment models are mainly based on Multi-index decision-making method, Bayesian reasoning, DS evidence theory, neural networks and fuzzy set theory. Several researches of threat assessment models based on multi-index decision are proposed [3-5]. However, these above methods are sensitive to data and difficult to adapt to the actual operational environment.

Thus, target threat assessment based on BP, IGSO-BP, and RBF neural networks are introduced [6-8]. But the difficulty of acquiring network training data makes it hard to apply this method in practice.

The above methods are just applicable to the evaluation in static environment. With the rapid change of air combat data, it is difficult to judge the threat degree of enemy in real air combat environment in time. Besides, due to the use of electromagnetic interference, tactical deception and other tactics in actual combat environment [1,9], air combat data for model computing collected by airborne and ground sensors is uncertain or even missing.

Motivated by these challenges, in this paper, the time factor is introduced into the modeling process of threat assessment based on Bayesian Network [10-11], and a Dynamic Bayesian Network (DBN) model is established, which is more capable of dynamic assessment under uncertain conditions. And a theoretical method to deal with missing data by Expectation Maximization is proposed. Simulation results show the feasibility of the proposed algorithm.

2. Dynamic Bayesian Network Based Threat Assessment
In this paper, threat assessment is carried out in air defense operations based on DBN. And this section is mainly divided into the following contents: indicators for threat assessment, Dynamic Bayesian Network model, model inference mechanism, EM-based Bayesian Network learning method.
2.1 Indicators for Threat Assessment

Threat assessment of enemy targets refers to the degree of threat to us inferred from the perception of current situation and battlefield elements in actual combat environment [12]. Thus, the first step in a threat assessment is to determine the various indicators that affect the threat level of an enemy aircraft against us.

There are two main types of indicators to consider. One is the dynamic indicators reflecting the air combat situation of fighters, which indicates the attack intention of enemy aircrafts. Such indicators mainly include altitude, heading angle, speed and distance, etc. In general, the smaller the heading angle, the lower the altitude and the greater the speed, the more obvious the attack intention of the enemy is.

The other is static indicators of fighter performance including electronic interference capability, aircraft type and weapons, which determine the damage ability of enemy aircraft. The above indicators are shown in figure 1.

2.2 Dynamic Bayesian Network Model

A Bayesian Network is a Directed Acyclic Graph (DAG) with a probability. Suppose a set of random variables \( U = \{X_1, X_2, ..., X_n\} \), where the variables have a finite number of states. The Bayesian Network is represented as a binary group \( S = (G, P) \), in which \( G \) is a directed acyclic graph and nodes represent the set of random variables \( U \) used to represent the events of the incoming targets in air defense operations. Conditional dependencies of events are represented by directed edges. To use the Bayesian Network method to evaluate the threat of an attacking target in air defense operations, the following assumptions need to be made: For any random variable \( P \) given set of parent nodes, it is independent of its non-descendant nodes. That is, any random variable does not affect other variables that are not directly related to it. \( P \) is used to represent the conditional probability set, and each node \( X \) in the network \( G \) has a conditional probability table representing its relationship with the parent node \( Pa(X) \), and its size represents the strength of the relationship between events.

This paper mainly establishes a threat assessment model based on DBN. The DBN combines the Static Bayesian Network with the time series information, considering the transition probability and the mutual influence of before and after events. In order to simplify the model, necessary model assumptions are made here:

- Assume that the dynamic probability process satisfies Markovian property, that is, the state transition probability at the current moment is only related to the state probability at the previous moment, Namely,

\[
P(X(t) \mid X(1), X(2), ..., X(t)) = P(X(t + 1) \mid X(t)) \]

(1)

- Suppose that the conditional probability of adjacent time is stationary in a finite time, that is, \( P(X(t + 1) \mid X(t)) \) is the same for any time.

Based on the above assumptions, the DBN can be divided into a prior network \( B_0 \) (initial state probability transition network) and a transition network \( B_n \) (transition probability defined on variables \( X(t) \) and \( X(t + 1) \)).

Therefore, the joint probability distribution for the given DBN model on \( X(1), X(2), ..., X(t) \) is shown as formula (2).

\[
P(X(1), X(2), ..., X(t)) = P_{B_0}(X(1)) \prod_{t=1}^{T} P_{B_n}(X(t + 1) \mid X(t))
\]

(2)

The basis of DBN inference is Bayesian formula and its conditional independent assumption, namely
\[ p(x \mid y) = \frac{p(xy)}{p(y)} = \sum \frac{p(xy)}{p(y)} \]

\[ p(x_i, x_2, \ldots, x_n) = \prod_{i=1}^{n} p(x_i \mid pa(x_i)) \]

(3)

Where, \((x_1, x_2, \ldots, x_n)\) represents the set of nodes in the network, \(p(x_i, x_2, \ldots, x_n)\) represents the joint distribution of all nodes in the network, and \(pa(x_i)\) is the set of parent nodes of node \(x_i\).

2.3 Model Reasoning Mechanism

For a Bayesian Network with \(m\) observation nodes and \(n\) hidden nodes, the inference algorithm is

\[ p(x_1, x_2, \ldots, x_n \mid y_1, y_2, \ldots, y_m) = \frac{\prod j \ p(y_j \mid pa(y_j)) \prod \ p(x_i \mid pa(x_i))}{\sum_{x_1, x_2, \ldots, x_n} \prod j \ p(y_j \mid pa(y_j)) \prod \ p(x_i \mid pa(x_i))} \]

(4)

Where, \(pa(x_i)\) and \(pa(y_j)\) respectively represent the parent node set of node \(x_i\) and \(y_j\), \(j = 1, 2, \ldots, m; i = 1, 2, \ldots, n\).

When the observed values have only one combined state, the distribution of hidden variables of the DBN with \(T\) time periods is as follows

\[ p(x_{k1}, x_{k2}, \ldots, x_{km}, y_{j1}, y_{j2}, \ldots, y_{jm} \mid y_{j1}, y_{j2}, \ldots, y_{jm}) = \]

\[ \frac{\prod j \ p(y_j \mid pa(y_j)) \prod \ p(x_{ki} \mid pa(x_{ki}))}{\sum_{x_{k1}, x_{k2}, \ldots, x_{km}, y_{j1}, y_{j2}, \ldots, y_{jm}} \prod j \ p(y_j \mid pa(y_j)) \prod \ p(x_{ki} \mid pa(x_{ki}))} \]

(5)

Where, \(x_{ki}\) and \(y_{ji}\) represent the \(K\)th time period of nodes c and d, while \(pa(x_{ki})\) and \(pa(y_{ji})\) represent the set of parent nodes \(x_{ki}\) and \(y_{ji}\), \(k = 1, 2, \ldots, T; j = 1, 2, \ldots, m; i = 1, 2, \ldots, n\).

The paper mainly considers the following indicators to evaluate the threat of the target. They are target distance (L), target course angle (A), target height (H), target velocity (V), target type (ID) and target electronic interference capability (R). As can be seen from Figure 1, target threat assessment based on DBN is a dynamic process.

![Figure 1. Target Threat Assessment Based on Bayesian Networks.](image-url)
The specific indicators in Figure 1 are as follows: target threat (TH) = \{high threat (H), medium threat (M), low threat (L)\}; target intention (IN) = \{attack (A), investigation (I), vigilance (V)\}; damage ability (DA) = \{strong damage ability (S), medium damage ability (M), weak damage ability (W)\}; target distance (D) = \{distance (F), medium distance (M), close range (S)\}; target heading angle (A) = \{Large heading angle (H), medium heading angle (M), small heading angle (L)\}; target height (H) = \{high (H), medium (M), low (L)\}; target speed (V) = \{high speed (H), medium speed (M), low speed (L)\}; target type (ID) = \{large target (H), medium target (M), small target (S), stealth target (C)\}; Target interference capability (R) = \{strong interference capability (H), medium interference capability (M), low interference capability (L), non-interference ability (N)\}.

2.4 EM-based Bayesian Network Learning Method
Using Discrete Dynamic Bayesian Network (DDBN) to reason and calculate the threat level of incoming targets is a common method to deal with such problems. However, in the complex actual combat environment, the data obtained by the sensors is incomplete. Under this condition, although the original method can get the result, the missing data makes the estimated threat quite different from the actual situation. Therefore, DBN based threat assessment still faces some challenges. In this paper, a method of estimating DBN parameters based on mathematical Expectation Maximization (EM) is proposed under the condition of missing sample data.

If the sample data is missing, some of the statistical factors $N_{ik}$ and $N_{ik}$ are unknown. First, the current Bayesian Network structure and parameters are used to calculate the missing ESS of the sample: $E(N_{ik}) \cdot E(N_{ik})$. Then $E(N_{ik})$ and $E(N_{ik})$ are used to re-estimate the parameters of the current Bayesian Network. The EM algorithm can be described as:

Initialize the parameters $\theta$ of the Bayesian Network and repeat the process E-Step and M-Step until the algorithm converges.

- E-Step process: using the Bayesian network parameter $\theta$ of the t-th iteration, calculate $E(N_{ik} | \theta), E(N_{ik} | \theta)$ through the Bayesian network inference mechanism;
- M-Step process: Recalculate the parameters of the Bayesian network by using $E(N_{ik} | \theta), E(N_{ik} | \theta)$ in the E-Step process instead of part of the $N_{ik}, N_{ik}$ that does not exist: $\theta^{t+1} = E[N_{ik}] / E[N_{ik}]$.

3. Experimental Simulation
In the process of inferring the target threat degree, it is necessary to divide the threat assessment into several time segments based on the structured event cycle of air defense battle command and control. According to expert experience and real-time data of target situation, the threat degree of target is analyzed in each time segment. In this process, the model parameters of the DBN need to be determined first.

3.1. Determine Model Parameters
Based on expert experience, the model can infer different events reflected by situation data. For example, the target of low-altitude flight may be a missile, and the target with strong electromagnetic interference capability is generally an electronic jammer. In this paper, the transition probability between some major time segments is obtained by consulting experts. Table 1 shows the transition probabilities of DBN.

| $T_i$ | $T_{i+1}$ | $H$ | $M$ | $L$ |
|------|----------|----|----|----|
| $H$  | 0.75     | 0.15 | 0.10 |
| $M$  | 0.25     | 0.40 | 0.35 |
| $L$  | 0.20     | 0.20 | 0.60 |
The conditional probability of threat assessment model is given in Table 2.

### Table 2. Training Sample Data.

| Factors | Target type (ID) | Velocity (V) | Heading Angle(A) | Height (H) | Distance (D) | Jamming ability(R) |
|---------|------------------|--------------|------------------|------------|--------------|-------------------|
| High threat(H) | H/ID1 0.05 | H/V1 0.50 | H/A1 0.20 | H/H1 0.20 | H/D1 0.20 | H/R1 0.50 |
|          | H/ID2 0.15 | H/V2 0.30 | H/A2 0.30 | H/H2 0.30 | H/D2 0.30 | H/R2 0.20 |
|          | H/ID3 0.20 | H/V3 0.20 | H/A3 0.50 | H/H3 0.50 | H/D3 0.50 | H/R3 0.20 |
|          | H/ID4 0.60 | -            | -            | -            | -            | H/R4 0.10 |
| Medium threat(M) | M/ID1 0.05 | M/V1 0.60 | M/A1 0.10 | M/H1 0.15 | M/D1 0.15 | M/R1 0.45 |
|          | M/ID2 0.10 | M/V2 0.30 | M/A2 0.15 | M/H2 0.35 | M/D2 0.25 | M/R2 0.35 |
|          | M/ID3 0.10 | M/V3 0.10 | M/A3 0.75 | M/H3 0.60 | M/D3 0.60 | M/R3 0.10 |
|          | M/ID4 0.75 | -            | -            | -            | -            | M/R4 0.10 |
| Low threat (L) | H/ID1 0.10 | L/V1 0.55 | L/A1 0.20 | L/H1 0.25 | L/D1 0.10 | L/R1 0.60 |
|          | H/ID2 0.20 | L/V2 0.25 | L/A3 0.35 | L/H2 0.30 | L/D2 0.30 | L/R2 0.25 |
|          | H/ID3 0.20 | L/V3 0.20 | L/A3 0.45 | L/H3 0.40 | L/D3 0.60 | L/R3 0.10 |
|          | H/ID4 0.50 | -            | -            | -            | -            | L/R4 0.05 |

### Table 3. Target Observation Value.

| Factors | Target type (ID) | Velocity (V) | Heading Angle (A) | Height (H) | Distance (D) | Jamming ability (R) |
|---------|------------------|--------------|------------------|------------|--------------|-------------------|
| Time    |                  |              |                  |            |              |                   |
| 1       | (0010)           | (0.2 0.3 0.5)| (0.5 0.3 0.2)    | (0.6 0.2 0.2)| 0.7 0.2 0.1   | (0.2 0.2 0.4 0.2)  |
| 2       | (0010)           | (0.3 0.3 0.4)| (0.4 0.1 0.5)    | (0.4 0.3 0.3)| 0.5 0.3 0.2   | (0.2 0.2 0.4 0.2)  |
| 3       | (0010)           | (0.3 0.5 0.2)| (0.3 0.2 0.5)    | (0.3 0.4 0.3)| 0.6 0.2 0.2   | (0.2 0.2 0.4 0.2)  |
| 4       | (0010)           | (0.4 0.4 0.2)| (0.3 0.2 0.5)    | (0.2 0.4 0.4)| 0.5 0.2 0.3   | (0.2 0.2 0.4 0.2)  |
| 5       | (0010)           | (0.5 0.2 0.3)| (0.3 0.2 0.5)    | (0.2 0.3 0.5)| 0.5 0.2 0.3   | (0.2 0.2 0.4 0.2)  |
| 6       | (0010)           | (0.5 0.3 0.2)| (0.2 0.3 0.5)    | (0.3 0.2 0.5)| 0.5 0.2 0.3   | (0.2 0.2 0.4 0.2)  |
| 7       | (0010)           | (0.6 0.3 0.1)| (0.2 0.3 0.5)    | (0.2 0.2 0.6)| 0.4 0.2 0.4   | (0.2 0.2 0.4 0.2)  |
| 8       | (0010)           | (0.6 0.3 0.1)| (0.2 0.2 0.6)    | (0.2 0.2 0.6)| 0.3 0.2 0.5   | (0.2 0.2 0.4 0.2)  |
| 9       | (0010)           | (0.6 0.3 0.1)| (0.2 0.2 0.6)    | (0.1 0.2 0.7)| 0.2 0.2 0.6   | (0.2 0.2 0.4 0.2)  |
| 10      | (0010)           | (0.7 0.2 0.1)| (0.2 0.2 0.6)    | (0.1 0.2 0.7)| 0.2 0.2 0.6   | (0.2 0.2 0.4 0.2)  |

### 3.2. Reasoning Process

Suppose an enemy aircraft is flying towards our air defense position. Using sensors to continuously observe 10 moments, we have obtained the situation observations value of the enemy aircraft during that time period. The observed data have the following rules: heading Angle, height and distance are decreasing, and speed is increasing. Specific observation values are shown in Table 3. Based on the DBN threat assessment model proposed in this paper, the threat values of enemy aircraft at the above ten moments are deduced. The specific data is shown in Table 4, and the threat probability curve of the target at 10 moments is drawn in Figure 2.
Table 4. Target Threat Reasoning Value.

| Factors | High threat | Medium threat | Low threat |
|---------|-------------|---------------|-----------|
| Time    |             |               |           |
| 1       | 65.20%      | 24.60%        | 10.20%    |
| 2       | 70.40%      | 20.30%        | 9.30%     |
| 3       | 79.10%      | 12.70%        | 8.20%     |
| 4       | 85.60%      | 7.90%         | 6.50%     |
| 5       | 86.30%      | 8.00%         | 5.70%     |
| 6       | 88.40%      | 6.70%         | 4.90%     |
| 7       | 89.50%      | 5.70%         | 4.80%     |
| 8       | 90.90%      | 6.70%         | 2.40%     |
| 9       | 92.30%      | 6.20%         | 1.50%     |
| 10      | 94.70%      | 4.40%         | 0.90%     |

As can be seen from the above figure, in the 10 observation moments, the high threat degree of the target is gradually increasing, which is consistent with the actual situation. At the last moment, the high threat level reached 94.70%, indicating that the enemy aircraft posed the highest threat to us.

Figure 2. Threat Curve.

4. Conclusion
The simulation results show that the threat assessment model based on Dynamic Bayesian Network can play an effective role in real combat environment. However, it should be noted that the conditional probability matrix of the Bayesian Network in the model is given by experts based on their empirical knowledge and actual combat situation, which reflects the basic relationship between the interrelated variables in practical problems. Therefore, it is inevitable to have subjective factors, and there may be a lack of objective argumentation in practical operation, which is also one of the main problems faced by Dynamic Bayesian Networks.

5. Acknowledgments
The authors would like to thank reviewers and Mr. Boyang Zhang for their valuable comments and suggestions to improve the quality of the paper.

6. References
[1] Ding D L Luo J J and Wang Y 2014 Threat level assessment based on fuzzy bayesian networks
Electronics Optics & Control 21(9) 7-10

[2] Duquet J R Bergeron P Blodgett D E Couture J Macieszczak M and Mayrand M et al 1998 Spie proceedings [spie aerospace/defense sensing and controls - orlando fl (monday 13 april 1998)] sensor fusion: architectures algorithms and applications ii - Proceedings of SPIE - The International Society for Optical Engineering 3376 198-209

[3] Bingsong X Yangwang F and Shiguo H U 2009 New threat assessment method in beyond-the-horizon range air combat[J] Systems Engineering & Electronics 31(9):2163-2166

[4] Si-Yu Z Wen-Hai W U Zhi-Gang Q U and Meng Z 2011 Analysis of air combat situation assessment based on nonparametric methods Aeronautical Computing Technique

[5] Endsley and Mica R 1993 A survey of situation awareness requirements in air-to-air combat fighters The International Journal of Aviation Psychology 3(2) 157-168

[6] Xuan H Li-Hong G Jiang L I and Yang Y U 2017 Target threat assessment based on bp neural network optimized by modified particle swarm optimization Journal of Jilin University(Engineering and Technology Edition)

[7] Jie-Yu C Pei-Yang Y Bo W and Dong-Dong S 2015 Dynamic threat assessment based on structure entropy and igso-bp algorithm Systems Engineering & Electronics 37(5) 1076-1083

[8] Xu K Kong D and Chen J 2015 Target threat assessment based on improved rbf neural network

[9] Fang Y Li W Zhou X and Xie X 2011 Threat Assessment Based on Adaptive Intuitionistic Fuzzy Neural Network Fourth International Symposium on Computational Intelligence & Design

[10] Narayana R P Sudesh K K Girija G and Debanjan M 2013 Situation and Threat Assessment in BVR Combat Aiaa Guidance Navigation & Control Conference

[11] Okello N and Thorns G 2003 Threat assessment using bayesian networks Information Fusion Sixth International Conference of IEEE

[12] Ximeng X U Rennong Y Ying F U and Yu Z (2018) Target threat assessment in air combat based on elm__adaboost strong predictor Systems Engineering and Electronics