# Air Defense Threat Assessment Based on Dynamic Bayesian Network

Wang Yi[1]，
[1]Department of Ordance Science and Technology
Naval Aeronautic and Astronautical University
Yantai, , China

Sun Yuan[2],Li Ji-Ying[2]，Xia Sun-Tao[2]
[2]Scientific Research Department
Naval Aeronautic and Astronautical University
Yantai, , China

*Abstract*—By understanding the process of threat assessment, the evaluation parameters, which affect threat level, have been analyzed comprehensively. Then the threat assessment of the Bayesian network model has been established. The dynamic Bayesian network reasoning method is used to estimate threat so that the objective factors and individual characteristics of different time slices of the same characteristics can correct each other. This method overcomes the subjectivity and uncertainty of expert assessment partially. Simulation results show that the threat level based on dynamic Bayesian network evaluation algorithm is an effective assessment algorithm, the results can more accurately reflect the true source of the threat level of threat.

**Keywords-threat assessment; dynamic Bayesian network; probabilistic reasoning;**

## I. FOREWORD

With the increasing complexity of the air raid environment, the attack modes of air raid today are all whole airspace, multi-sorties, multi-batches, multidirection, multi-level, continuous and saturated. Therefore, in practical operations, we must make threat assessment on the air raid targets, determine the threat level, and make target optimal distribution according to the threat level ofthe target. Only in this way can we attack high threat level targets with limited firepower and get the optimal operation effect.

There are mainly several threat evaluating methods such as the fuzzy comprehensive evaluation, the method based on the neural network, the grey correlation method. The fuzzy comprehensive evaluation may cause distortion; the method based on the neural network can not be practically used because it lacks reliable training set. Although the grey correlation method considers the effect of non-maxima information, it only analyzes data and lacks qualitative description.

Meanwhile, most of the existing air raid target threat evaluation methods are based on static circumstances, evaluations are independent of each other, and the influence of the change of the target information on the threat evaluation in the air defense operation cycle has not been considered. Furthermore, the attack attempt of the target and the importance of the team members has been ignored, so the results are slightly rough. They can only be adapted to single-ship and short-range point air defenses, or circumstances in which there are a few team members and air defense fire channels.

The dynamic Bayesian network is a modeling and reasoning tool developed in recent years for dynamic systems. It has added time factor on the base of the static Bayesian network, so that the reasoning process is continuous, which is more in line with reality. Meanwhile it combines probabilistic method and expert knowledge to describe, and combines historical information and evidence base, which makes it has the information time cumulating ability, so that the uncertainty of the information fusion reasoning process of different levels has been more effectively reduced. It is more reasonable than the static Bayesian network. Therefore, this paper uses the dynamic Bayesian network to assess situations and to provide decision support for commanders[4].

## II. BAYESIAN NETWORK MODEL

First, confirm that you have the correct template for your pa The Bayesian network is a probabilistic graph model which is built on the basis of the dependence between variables[5]. A Bayesian network can be represented by duality group: $B =< G, P >$. In which:

1) $G$ is the structure of the Bayesian network, $G =< V, A >$ is a directed acyclic graph $(DAG)$, in which node $V$ represents random variables, $A$ is the collection of arc, which indicates the causal relationship between nodes(variables).

2) $P$ is network parameter, which represents the collection of conditional probability. Each node $V_i$ in $G$ has a conditional probability table to indicate the relationship between $V_i$ and its parent node $Pa(V_i) : P(V_i / Pa(V_i))$. In Bayesian network, node $V_i$ and its indirect parent node $V_j$ are conditionally independent of its parent node $Pa(V_i)$, that is $P(V_i / V_j, Pa(V_i)) = P\left(V_i / Pa(V_i)\right)$. According to conditional independence, the joint probability of N variables in Bayesian network can be resolved into: $P(V_1, V_2, \cdots, V_n) = \prod_{i=1}^{n} P(V_i / Pa(V_i))$.

## III. DYNAMIC BAYESIAN NETWORK

The dynamic Bayesian network (DBN) is based on the


978-1-4673-0199-2/12/$31.00 ©2012 IEEE

static Bayesian network. It combines the static structure of network and timing information, and expands the probability distribution in fixed variable set into tense field by simulating randomly evolved model *DBN* of any variable set on the timeline.

Assuming $X=(X_1,X_2,\cdots,X_n)$ is a time varying variable set, and it has been sorted by network topological structure. $X_i[t]$ is the value of variable $X_i$ on time $t$, $X[t]$ is the value of variable *X* on time $t$. The dynamic Bayesian network can use process $X[0]\to X[1]\to\cdots\to X[n]$ to represent timing. Obviously, using such a dynamic Bayesian network needs the collection of conditional probability of all the variable sets $X[0]\cup X[1]\cup\cdots\cup X[n]$. In fact, it is very difficult to obtain such conditional probability, and the network inference is very complicated, too. Therefore, the Bayesian network in this paper uses the assumptions below:

1）Assume that in a limited time the changing process of conditional probability is stable to all *t.*

2）Assume that dynamic probability process is *markovian*，that is：

$$P(X[t]\,|\,X[1],X[2],\cdots,X[t])=P(X[t+1]\,|\,X[t])$$

Which means that the probability of future time is only related to present time, and is independent of past time.

3）Assume that the conditional probability of adjacent times is stable, that is $P(X[t+1]\,|\,X[t])$ is independent of time *t*, thus we can easily get transition probability of different times $P(X[t+1]\,|\,X[t])$.

On the basis of the assumptions above, the joint probability distribution *DBN* built on random process time track consists of two parts：

1)Prior network $B_0$，the joint probability distribution defined on the initial state $X[1]$；

2)Transition network $B_{\to}$，the transition probability $P(X[t+1]\,|\,X[t])$ defined on variable $X[1]$ and $X[2]$（tenable to all *t*）.

Therefore, if we set a *DBN* model, then the joint probability distribution on $X[0],X[1],\cdots,X[t]$ is：

$$P(X[1],X[2],\cdots,X[t])=P_{B_0}(X[1])\prod_{t=1}^{T}P_{B_{\to}}(X[t+1]\,|\,X[t]) \tag{1}$$

## IV. BAYESIAN NETWORK REASONING MECHANISM

Reasoning model is built according to prior information. If the state probability distribution of leaf node does not change, the network keeps in equilibrium; if the state of leaf node changes according to the observation information, all the nodes in the network will update their state probability distribution according to the Peal algorithm. This paper uses Bayesian network tree as reasoning model, and its structural feature is that each node has no more than one parent node. Think about a typical aroborescent Bayesian network, node *X* has *m* child node $Y_1,Y_2,\cdots Y_m$ and one parent node $u$, the structure is as shown in figure1.

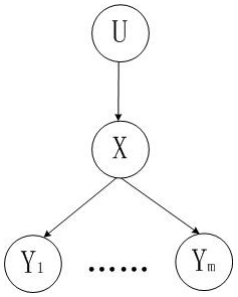


Figure1 Bayesian Network Tree Structure

Variables in the algorithm are defined as follow:

$Bel$：The state probability distribution of the node;

$\lambda$：Diagnostic information gotten from child node;

$\pi$：Causal information gotten from parent node;

The algorithm is centered on a single node. It get $\lambda$ from the child node, and get $\pi$ from the parent node, then calculate $Bel$, $\lambda$ and $\pi$ of the node and trigger adjacent node to update. Repeat this cycle till all the nodes' posterior probability equals prior probability, then the network reaches a new equilibrium state. Specific calculation is divided into three steps as follow:

First step：Update its confidence;

$$\begin{aligned} Bel(x)&=\alpha\lambda(x)\pi(x)\\ \lambda(x)&=\prod_j\lambda_{Y_j}(x)\\ \pi(x)&=\pi_x(u)\times M_{x|u}\end{aligned} \tag{2}$$

Second step：Update from the bottom to the top:

$$\lambda_x(u)=\lambda(x)\times M_{x|u} \tag{3}$$

Third step：Update from the top to the bottom：

$$\pi_{Y_i}(x)=\alpha\pi(x)\prod_{k\neq j}\lambda_{Y_k}(x) \tag{4}$$

The update of the Bayesian network is triggered by events, so the Bayesian network is a reasoning process based on diagnosis. This is the same as people's way of thinking when they are making situation assessment. From the cognitive perspective, the reasoning result of the Bayesian network provides high credibility.

### *A. Analysis of factors that affect threat level*

The duty of threat assessment is to conclude the threat level of enemy object according to various data to provide basic basis for the reasonable and efficient use of ship-borne weapon resources. The battlefield environment today has become more and more complicated. The attack modes are all whole airspace, multi-batches, multi-direction, multi-level,

continuous and saturated. Therefore, in practical operations, we must make threat assessment on incoming targets to determine targets' threat level, and make target optimal distribution according to the threat level of the targets. Only in this way can we attack high threat level targets with limited firepower and get the optimal operation effect[6].

Threat assessment mainly concerns with two questions as follow:

（1）Dose the incoming threat has the intent to attack our ship?

（2）If the incoming threat has the intent to attack our ship, how much damage will it make on our ship?

According to the two questions above, threat assessment process mainly includes two aspects, that is intent assessment and ability assessment. When using Bayesian network to assess threat, we should analyze and extract related factors of specific problems, determine the causal relationship and conditional dependent relationship between the factors of threat assessment, build correct network structure model, determine prior probability and conditional probability, and choose appropriate reasoning method.

The threat level of air target depends on various factors. Generally, it mainly includes velocity, range, acceleration, location, height, course, course shortcut, target type, attacking intent, electronic jamming, and damaging ability. These factors affect and relate to each other, forming attack intent and threat level to the formation. This paper has chosen related target attributes including target type, range, velocity, height and course shortcut which can obviously reflect target's attack threat to research[7].

According to the characteristic factors above and combining with the cycle period of command and control structured events of the formation's air defense operation，we divide the threat judgment and intercept sort in the operation process into many time slices. The cycle period of each time slice is generally consistent with the transducer's target data updating cycle or the air defense weapon firing cycle. Thus we build the dynamic Bayesian network model of threat assessment as follow：

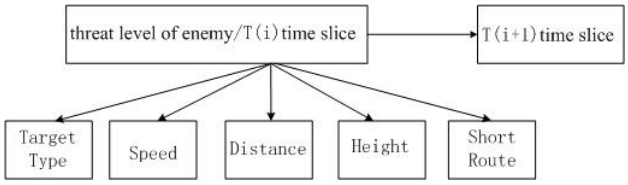


Figure2 Dynamic Bayesian Network Model of Threat Assessment

In the model of figure2, each variable state set is:

Target type：ID={missile，fighter plane，electronic war fare plane}；

Velocity：V={high velocity；medium velocity；low velocity}；

Range：R={far；medium；near}；

Height：H={low altitude；medium；high altitude}；

Course shortcut：P={in range；on edge；out of rang e}；

## *B. Determine Model Parameters*

The variable state set above shows the experimental knowledge of domain experts. Take height as an example, vehicles that hedgehop are always antiship missiles; low-altitude flights are always helicopters or cruise missiles; bombardment aircrafts need to dive to medium height to make pinpoint bombing; electronic jammers and early warning aircrafts are often in high altitude. According to the domain expert knowledge, we get main node conditional probability as is shown in figure1.

Table 1 Dynamic Bayesian Network State Transition Probability

| $T_{i+1}/T_i$ | $H$ | $M$ | $L$ |
|---|---|---|---|
| $H$ | 0.7 | 0.15 | 0.15 |
| $M$ | 0.35 | 0.40 | 0.25 |
| $L$ | 0.15 | 0.35 | 0.50 |

Table 2 Threat Assessment Model Conditional Probability

| Threat Level | Type($K$) | Velocity($V$) | Range($R$) | Height(M) | Course Shortcut(L) |
|---|---|---|---|---|---|
| High($H$) | $H/K_1$ 0.7<br>$H/K_2$ 0.2<br>$H/K_3$ 0.1 | $H/V_1$ 0.7<br>$H/V_2$ 0.2<br>$H/V_3$ 0.1 | $H/R_1$ 0.2<br>$H/R_2$ 0.2<br>$H/R_3$ 0.6 | $H/M_1$ 0.2<br>$H/M_2$ 0.2<br>$H/M_3$ 0.6 | $H/L_1$ 0.2<br>$H/L_2$ 0.2<br>$H/L_3$ 0.6 |
| Medium($M$) | $M/K_1$ 0.2<br>$M/K_2$ 0.6<br>$M/K_3$ 0.2 | $M/V_1$ 0.2<br>$M/V_2$ 0.6<br>$M/V_3$ 0.2 | $M/R_1$ 0.2<br>$M/R_2$ 0.6<br>$M/R_3$ 0.2 | $M/M_1$ 0.2<br>$M/M_2$ 0.55<br>$M/M_3$ 0.25 | $M/L_1$ 0.2<br>$M/L_2$ 0.6<br>$M/L_3$ 0.2 |
| Low($L$) | $L/K_1$ 0.1<br>$L/K_2$ 0.2<br>$L/K_3$ 0.7 | $L/V_1$ 0.1<br>$L/V_2$ 0.2<br>$L/V_3$ 0.7 | $L/R_1$ 0.7<br>$L/R_2$ 0.2<br>$L/R_3$ 0.1 | $L/M_1$ 0.65<br>$L/M_2$ 0.25<br>$L/M_3$ 0.1 | $L/L_1$ 0.6<br>$L/L_2$ 0.2<br>$L/L_3$ 0.2 |

## V. SIMULATION EXAMPLE

Assume that a target is detected in our destroyer escort formation, and we observe the target three times. According to the target's characteristic data, we get reasoning parameters as is shown in the figure below.

Table 3 Reasoning Figure Table

| | | Type($K$) | Velocity($V$) | Range($R$) |
|---|---|---|---|---|
| Target1 | Time1 | (0.7,0.2,0.1) | (1,0,0) | (0.6,0.2,0.2) |
| | Time2 | (0.8,0.1,0.1) | (1,0,0) | (0.5,0.3,0.2) |
| | Time3 | (0.9,0.1,0) | (1,0,0) | (0.3,0.4,0.3) |
| | | Height($M$) | Course Shortcut($L$) | |
| Target1 | Time1 | (0.2,0.3,0.5) | (0.7,0.2,0.1) | |
| | Time2 | (0.2,0.2,0.6) | (0.4,0.5,0.1) | |
| | Time3 | (0.1,0.2,0.7) | (0.2,0.2,0.6) | |

After reasoning and calculating, we can get the threat level probability of the target on three times.

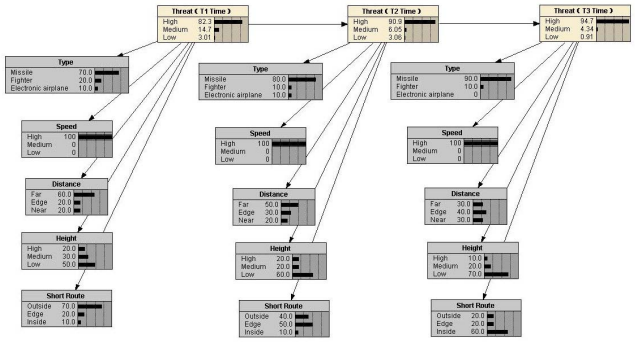


Figure3 Target Threat Level Probability Reasoning

From the simulation result, we can find that the target range, height and course shortcut all decrease, the threat level increases, and the high threat level probability sharply increases from 0.823 to 0.947. It coincides with the fact and other reasoning results are consistent with combat scenarios.

## VI. CONCLUSIONS

To counter the feature of threat assessment that a lot of data vary with time, this paper builds dynamic Bayesian network model, analyzes its reasoning process, and makes simulation experiment. The simulation results show that the dynamic Bayesian network can efficiently use time information in data, and timely and dynamically deal with factors that affect analysis and decision. To a certain extent, this method overcomes subjectivity and uncertainty brought by expert assessment, and the assessment results can support commanders to make decision better.

## VII. REFERENCES

[1]WU Chuan-yu, LIU Fu-xian. New model of target threat assessment for air defense operation based on fuzzy theory[J]. SYSTEMS ENGINEERING AND ELECTRONICS,2004,26 (8) :1068～1071.

[2]QIAN Jiang,XU Jiang-hu. Threat Sequencing for Aerial Target Based on BP Neural Network[J].Modern Defence Technology,2001,29(6):56～58.

[3]LUO Wen-hui,YANG Jian-jun.Application of Grey TOPSIS to Evaluation of Aerial Targets Threat[J].Fire Control and Command Control,2009,34 (2) : 130～133.

[4] CHAI Hui-min,WANG Bao-shu.Application of dynamic Bayesian networks in tactical situation assessment[J].Application Research of Computers,2011,28(6):2151-2160.

[5] YANG Jian,GAO Wen-yi,LIU Jun.Threat assessment method based on bayesian network[J].Journal of PLA University of Science and Technology(Natural Science Edition),2010,11(1):43-48.

[6] SHEN Wei-wei,XIAO Bing,DING Wen-fei,FAN Zhi-yu.Application of Dynamic Bayesian Network to Situation Assessment[J].Journal of Air Force Radar Academy,2010,24(6):414-417.

[7] Xu Hong-quan Li Xiao-ming.Research on Region Aerial Defense Warfare Techniques of Surface Vessels Formation System[J].Ship Electronic Engineering,2010,30(10):9-13.

[8] Xiao Bing Shen Wei-wei Jin Hong-bin.Study on Threat Assessment Based on Dynamic Bayesian Network[J].Automation & Information Engineering,2010,4:4-7.