Study on Algorithm of UAV Threat Strength Assessment Based on Bayesian Network

Yan GE
Dept. of Information Science and Technology
Qingdao University of Science & Technology
Qingdao, China
gygeyan@163.com

Wei SHUI
Dept. of Automation
Qingdao University of Science & Technology
Qingdao, China
shuiwei198149@163.com

Abstract — As one of the most important harvest in AI field, Bayesian networks is widely used in uncertain problem’s reasoning and decision-making. After the theory and inference mechanism of Bayesian networks was introduced, this paper mainly studies the application of Bayesian networks in overlapped threat strength assessment. A model based on Bayesian networks is provided. Simulation result shows that the algorithm is effective and is able to reflect the real threat strength of UAV.

Keywords — Bayesian Network; Threat Strength; Inference; Algorithm

I. INTRODUCTION

Route Planning as one of the key technologies of unmanned air vehicle (UAV) mission planning is based mainly on the terrain and the enemy's firepower threat information, under certain restrictive conditions, from the starting point to find a feasible route target points [1]. UAV route planning system should meet feasibility, optimality and real-time requirements. In order to improve the efficiency of UAV route planning, UAV must correctly assess threat strength at first.

At present, many methods are used to assess threat strength. In this aspect, neural network has achieved the expected results [2,3], but neural network is a kind of iterative algorithm and needs network training, it would be difficult to meet real-time battlefield environment in threat level assessment. Bayesian network can be easily dealt with uncertain information, learning the causal relationship between the variables; relative to the above-mentioned method, which is simple, less computing and real-time. Reference [4] can accurately reflect independent threat level, but under real-time battlefield environment, there still exist overlapped threat, it is very important to assess overlapped threat level to improve efficiency of UAV route planning and survival probability.

Therefore, in this paper, on the basis of Bayesian inference, the algorithm synthesizes independent threat strength assessment and overlapped threat strength assessment to satisfy real-time battlefield requirement for solving some problems in aspect of UAV path planning.

II. BAYESIAN NETWORK

A. Bayesian network structure

Bayesian network is a dual group $S = \langle G, P \rangle$, where $G$ is a directed acyclic graph (directed acyclic graph, DAG) and has $N$ nodes, the nodes in the graph represent random variables, it could be any question’s abstract; the arcs in the graph represent the causal relationship between variables, So the arc between node $U$ and node $X$ reflects the causal relationship between two nodes. To facilitate the description, usually use capital letters $X = \{X_1, X_2, \ldots, X_n\}$ to represent node variable and lowercase letters $x = \{x_1, x_2, \ldots, x_n\}$ to represent the value of variables.

(1) $G$ is a directed acyclic graph (directed acyclic graph, DAG) and has $N$ nodes, the nodes in the graph represent random variables, it could be any question’s abstract; the arcs in the graph represent the causal relationship between variables, So the arc between node $U$ and node $X$ reflects the causal relationship between two nodes. To facilitate the description, usually use capital letters $X = \{X_1, X_2, \ldots, X_n\}$ to represent node variable and lowercase letters $x = \{x_1, x_2, \ldots, x_n\}$ to represent the value of variables.

(2) $P = \{X_j \mid \text{parents}(X_j)\}$, conditional probability represent the strength of causal influence, where parents$(X_j)$ represent the father nodes $X_j$. We use the conditional probability distribution table (CPT) to reflect the relationship between variables during modeling process.

B. The key of Bayesian network

(1) Identify the network structure

The establishment of Bayesian networks relies mainly on knowledge from experts, who give causal relationship between each node according to their experience. Therefore, the establishment of network structure is necessary to consider a number of comprehensive expert’s advice. The paper [5] mentioned a method to establish the network structure by data fusion and knowledge, its essence is to use experts’ knowledge to remove the fundamentally impossible network structure, and the uncertain parts can be verified by learning algorithm.

(2) Determine conditional probability distribution

It is most difficult to determine conditional probability distribution in the establishment of Bayesian network. There are two common methods, one is proposed by Renooij [6], the other is directly learning probability distribution from data and do not rely on experts.
(3) Reasoning

Assuming node $X$ has $m$ child nodes $(Y_1, Y_2, \ldots, Y_m)$ and $n$ father nodes $(Z_1, Z_2, \ldots, Z_n)$. $M_{X|Z} \rightarrow P(X | x \in Z = z)$ represents the probability of $x$ when $z$ happened, $Bel$ represents posterior probability distribution, $\lambda$ represents the diagnostic information obtained from child nodes, $\pi$ represents the causal information obtained from father nodes. Because $X$ has a number of discrete values, therefore, $\lambda(x)$, $\pi(x)$ is a vector:

$$\lambda(x) = [\lambda(X = x_1), \lambda(X = x_2), \ldots, \lambda(X = x_k)]$$

$$\pi(x) = [\pi(X = x_1), \pi(X = x_2), \ldots, \pi(X = x_k)]$$

Bayesian reasoning uses the single node as the central, it obtains $\lambda$ from its child node and obtain $\pi$ from its father node, then calculate its $Bel$, $\lambda$ and $\pi$, and trigger the adjacent nodes to update themselves. The process is as follow [7]:

Step 1: update their posterior probability

$$Bel(x) = \alpha \lambda(x) \pi(x)$$

$$\lambda(x) = \prod_j \lambda_{Y_j}(x)$$

$$\pi(x) = \prod_i \pi_{Z_i} M_{X|Z}$$

Where $\alpha$ is normalized factor, let $\sum_x Bel(x) = 1$

Step 2: Bottom-up update

$$\lambda_{X\setminus Z}(z) = \lambda(x) M_{X|Z}$$

Step 3: Top-down update

$$\pi_{Y_j}(x) = \alpha \pi(x) \prod_{K \neq j} \lambda_{Y_j}(x)$$

III. BAYESIAN NETWORK FOR THREAT LEVELS ASSESSMENT

A. Questions need to resolve

UAV path planning system should meet feasibility, optimality and real-time requirements. First of all, threat cost must be calculated. According to different condition, we can use different methods to calculate threat cost. In this paper, we use the following equation to describe threat cost [8]:

$$J_{\text{threat}}^j = \sum_{j=1}^{N} TS_j \left( R_{ij}^2 + R_{2j}^2 + R_{3j}^2 + R_{4j}^2 + R_{5j}^2 \right)$$

Where $TS_j$ represents the strength of threat $j$, in this paper according to the type of threat and the ability to confront the threat of UAV, using Bayesian network to speculate on threat strength; $R_{ij}$ represents the distance between each point on the edge and a threat $j$; $N$ represents the number of threats at present.

B. Quantify threat strength

In many existing algorithms of threat level assessment [4], the algorithms only consider independent threats, and the threat level was divided into three grades, named high, medium and low. But under actual battlefield environment, threat has characters of diversity and complexity, threat level is divided into six grades in this paper. We use threat strength ($TS$) to describe the influence of threat, $TS_1$ represents the strength of independent threat and $TS_2$ represents the strength of overlapped threat. $TS$ increase according to power exponent. Threat level and threat strength are shown in Table I.

<table>
<thead>
<tr>
<th>Threat Strength (TS)</th>
<th>Threat Level (TL)</th>
<th>Threat Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>I</td>
<td>Radar</td>
</tr>
<tr>
<td>4</td>
<td>II</td>
<td>Anti-aircraft artillery</td>
</tr>
<tr>
<td>9</td>
<td>III</td>
<td>Missile</td>
</tr>
<tr>
<td>16</td>
<td>IV</td>
<td>RA</td>
</tr>
<tr>
<td>25</td>
<td>V</td>
<td>RM</td>
</tr>
<tr>
<td>36</td>
<td>VI</td>
<td>RMA</td>
</tr>
</tbody>
</table>

Where RA represents radar and anti-aircraft artillery are overlapped, RM represents radar and missile are overlapped, RMA represents radar, missile and anti-aircraft artillery are overlapped.

C. Factors affecting threat strength

Threats of UAV Route Planning can be divided into fixed threat (terrain threats) and firepower threat (radar threats, the missile threat, etc.). In this paper, we only consider the threat of firepower.

Take into account real-time battlefield firepower threat is not isolated settings, the threat of firepower between the adjacent fire zones overlap, so we construct two Bayesian networks, they are named Bnet1 and Bnet2, and the Bayesian networks are shown in Figure 1 and Figure 2.
Set variables in the model as follows:

- Strength of independent threats ($TS_1$):
  \[ TS_{1_1} = 1 , \quad TS_{1_2} = 4 , \quad TS_{1_3} = 9 \]

- Strength of overlapped threats ($TS_2$):
  \[ TS_{2_1} = 16 , \quad TS_{2_2} = 25 , \quad TS_{2_3} = 36 \]

- Independent threat identification ($ID$):
  \[ ID_1 = 'Radar' \]
  \[ ID_2 = 'Anti-aircraft artillery' \]
  \[ ID_3 = 'Missile' \]

- Overlapped threat identification ($AT$):
  \[ AT_1 = 'RA' , \quad AT_2 = 'RM' , \quad AT_3 = 'RMA' \]

- Ability to confront the threat of aircraft ($ATC$):
  \[ ATC_1 = 'Good' , \quad ATC_2 = 'Medium' , \quad ATC_3 = 'Poor' \]

- Location of firepower threat and weapon employment zone ($WEZ$):
  \[ WEZ_1 = 'Within' \]
  \[ WEZ_2 = 'Edge' \]
  \[ WEZ_3 = 'Outside' \]
  \[ WEZ_4 = 'Azimuth relationship exists only' \]

D. Probability distribution

The conditional probability is given based on expert knowledge, so it is inevitably subjective. In the modeling process, the network structure have known, therefore, we can determine the probability distribution by EM algorithm according to the incomplete sample data. So the conditional probability can be moderately adjusted to improve the reliability of assessment. The conditional probability needed to specify in this model are shown as follow:

| TABLE II. CONDITIONAL PROBABILITY DISTRIBUTION TABLE (CPT) OF INDEPENDENT THREAT |
| TS1 | $P(ID | TS1)$ |
|-----|----------------|
| $TS_{1_1}$ | $P(ID_1 | TS1) = 0.6$ , $P(ID_2 | TS1) = 0.2$ , $P(ID_3 | TS1) = 0.2$ |
| $TS_{1_2}$ | $P(ID_2 | TS1) = 0.4$ , $P(ID_2 | TS1) = 0.3$ , $P(ID_3 | TS1) = 0.3$ |
| $TS_{1_3}$ | $P(ID_3 | TS1) = 0.1$ , $P(ID_2 | TS1) = 0.4$ , $P(ID_3 | TS1) = 0.5$ |

| TS1 | $P(WEZ | TS1)$ |
|-----|----------------|
| $TS_{1_1}$ | $P(WEZ_1 | TS1) = 0.1$ , $P(WEZ_2 | TS1) = 0.45$ , $P(WEZ_2 | TS1) = 0.45$ |
| $TS_{1_2}$ | $P(WEZ_2 | TS1) = 0.6$ , $P(WEZ_2 | TS1) = 0.2$ , $P(WEZ_2 | TS1) = 0.1$ |
| $TS_{1_3}$ | $P(WEZ_3 | TS1) = 0.8$ , $P(WEZ_3 | TS1) = 0.1$ , $P(WEZ_3 | TS1) = 0.1$ |

In table II and table III, $P(ID | TS1)$, $P(ATC | TS1)$, $P(WEZ | TS1)$ represent the size of threaten strength depends on the type of independent threat, ability to confront the independent threat of aircraft, location of firepower threat and weapon employment zone; $P(WEZ | TS1)$, $P(ATC | TS1)$, $P(WEZ | TS1)$ represent the size of threaten strength depends on the type of overlapped threat, ability to confront the independent threat of aircraft, location of firepower threat and weapon employment zone.

IV. SIMULATION

A. Algorithm procedure

- Step1 Initialize networks; define network nodes, the priori probability and the conditional probability.
- Step2 Establish network (Bnet1, Bnet2).
- Step3 Check information of child nodes, if their information has been updated entered Step 3, else enter Step 4.
- Step4 According to information, judge threat identification and trigger network to infer in accordance with updated information, output the probability distribution of $TS_1$ or $TS_2$.
- Step5 Output threat strength which have the greatest probability and ultimately to complete an assessment of threat strength, then calculate threat cost to complete UAV path planning.

B. Examples

We assign a UAV to complete some mission and assume that there is some information in advance, so we specify $P(TS1) = [0.3, 0.2, 0.5]$ $P(TS2) = [0.2, 0.8, 0.0]$ . After the departure of UAV, the aircraft get real-time information and judge that...
the first threat is independent threat. At moment $t_1$ we assume every nodes update data as shown in table IV.

**TABLE IV. SIMULATION RESULTS ONE**

<table>
<thead>
<tr>
<th>Net</th>
<th>State of Nodes</th>
<th>Probability of Root Nodes</th>
<th>TL</th>
<th>TS1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bnet1</td>
<td>$ID$</td>
<td>$[0.8 0.1 0.1]$</td>
<td>0.8344</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>$ATC$</td>
<td>$[0 0 1 0.9]$</td>
<td>0.1656</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$WEZ$</td>
<td>$[0 0 0 1]$</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Can be seen from the above data, in Bnet1 the main threat is radar threat, ability to confront the threat of aircraft is poor and azimuth relationship between UAV and threat exists only, so we can infer that the threat strength under this circumstance is one.

If at moment $t_2$ network detect the threat status changed (e.g., as shown in Table V) and judge that the second threat is overlapped threat, according to the algorithm of this paper we can infer that the threat strength is twenty-five.

**TABLE V. SIMULATION RESULT TWO**

<table>
<thead>
<tr>
<th>Net</th>
<th>State of Nodes</th>
<th>Probability of Root Nodes</th>
<th>TL</th>
<th>TS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bnet2</td>
<td>$AT$</td>
<td>$[0.2 0.2 0.6]$</td>
<td>0.0961</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>$ATC$</td>
<td>$[0.1 0.1 0.8]$</td>
<td>0.6568</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$WEZ$</td>
<td>$[0 0.8 0.2]$</td>
<td>0.2471</td>
<td></td>
</tr>
</tbody>
</table>

V. CONCLUSION

In this paper, algorithm of UAV threat strength assessment based on Bayesian network has been researched. In order to meet real-time battlefield requirement, the threat level has been divided into six levels and been described by threat strength. In the process of threat strength assessment, the algorithm considers independent threats and overlapped threats at same time. Simulation results verify that the method can satisfy real-time environment and improve operational efficiency and survival probability; the final result demonstrates the efficiency of the algorithm.

ACKNOWLEDGMENT

The author would like to thank Y.HAN for their help and support in making this work possible. The author is also grateful to K. Murphy for sharing his Bayesian network toolbox.

REFERENCES.


