doi: 10.7690/bgzdh.2019.12.018

基于动态贝叶斯网络的空袭目标威胁评估

侯　夷[1]，任小平[2]，王长城[1]，王　伟[1]
（1. 中国兵器装备集团自动化研究所有限公司特种产品事业部，四川 绵阳 621000；
2. 北方工程设计研究院有限公司，石家庄 050011）

摘要：针对现有方法在处理不确定性信息推理上的不足，提出一种威胁评估的动态贝叶斯网络模型。基于对动态贝叶斯网络的研究及对空袭目标威胁影响因素的分析，给出网络中节点的状态转移概率表和条件概率表，结合证据观测值推理得到目标威胁的后验概率，对典型航路空袭目标的威胁度进行仿真分析。结果表明：该模型合理有效，能较准确地反映目标的真实威胁度，从而对空袭目标实施有效的末端拦截。

关键词：动态贝叶斯网络；威胁评估；概率推理；吉布斯采样
中图分类号：TP393.02　　**文献标志码：**A

Threat Assessment of Air Attack Target Based on Dynamic Bayesian Network

Hou Yi[1], Ren Xiaoping[2], Wang Changcheng[1], Wang Wei[1]
(1. *Department of Special Product*, *Automation Research Institute Co*., *Ltd. of China South Industries Group Corporation*, *Mianyang* 621000, *China*;
2. *Norendar International Ltd*., *Shijiazhuang* 050011, *China*)

Abstract: In order to solve the shortcomings of the existing methods in dealing with uncertainty information reasoning, a dynamic Bayesian network model for threat assessment is proposed. The state transition probability table and conditional probability table of the nodes in the network are given based on analysis of dynamic Bayesian network and the analysis of the influencing factors of air strike target threat. The posterior probability of the target threat is obtained by reasoning with the evidence observations, and the threat level of the typical airway air attack target is simulated and analyzed. The results show that the model is reasonable and effective, and can accurately reflect the real threat level of the targets, thus effective terminal interception is implemented for air attack targets.

Keywords: dynamic Bayesian network; threat assessment; probabilistic reasoning; Gibbs sampling

0　引言

现代空袭兵器呈多样化、高速化，战术灵活，空袭手段向末端机动突防、多批次饱和攻击趋势发展，使末端防御面临极大挑战。对敌方空袭目标的威胁做出快速准确的评估和判断，从而对指挥员的决策给予辅助极其重要。目标威胁评估是指通过持续获取数据和信息，得到敌方武器可能对己方造成的损害程度的量化与排序，为武器目标分配和火力协调提供直接依据[1]。

目前，目标威胁评估常用的方法有模糊综合评价法[2]、层次分析法[3]、TOPSIS 法[4]、灰色关联分析法[5]及人工神经网络法[6]等。这些方法在特定条件下有一定效果，但也有明显的缺点：模糊综合评价法在指标集较大时可能出现超模糊现象导致评判失败；层次分析法的完全补偿性在解决实际问题时未必可行；TOPSIS 法涉及的正负理想解与原始数据有关，可能导致结果不稳定；灰色关联分析法要求对各项指标的最优值进行现行确定，主观性过强；神经网络法需要大量训练样本，且无法解释推理依据和过程。此外，由于作战过程中获取目标信息的不确定性，以上方法都不能有效地解决在该条件下进行威胁评估的推理问题；因此，选择合理的方法处理此类信息，获得及时准确的威胁评估，对达到最佳的末端拦截效果具有重要的意义。

贝叶斯网络（Bayesian network）是描述事件之间因果关系的概率网络模型，能够运用概率表达不确定性知识，并且信息间的推理是采用可视化的网络方法来表示，能很好地将样本数据与专家知识结合来处理不完备的信息。另外，对于快速变化的战场环境，基于静态模型的威胁评估不再适用。动态贝叶斯网络模型是静态贝叶斯网络在时间维度的扩展，使得概率推理过程更加连续和完整，有效降低不确定性，更好地为指挥决策提供辅助；因此，笔者采用动态贝叶斯网络对来袭目标进行威胁评估。

收稿日期：2019-07-09；**修回日期：**2019-07-23
基金项目：国防基础科研项目（JCKY2018209B010）
作者简介：侯　夷（1995—），男，四川人，学士，从事嵌入式计算机技术、火力控制技术研究。E-mail: houyi1915@163.com。

1 贝叶斯网络概述

1.1 贝叶斯网络

贝叶斯网络是一种基于网络结构的有向图解模型，由有向无环图(directed acyclic graph，DAG)和条件概率表(conditional probability table，CPT)2 部分组成，具有强大的知识表达和概率推理能力。它用节点表达随机变量，用有向边表达变量间的条件依赖或独立关系，CPT 用来表达变量之间的影响程度。贝叶斯网络来源于贝叶斯统计分析，经典的贝叶斯公式[7]如下：

$$P(B_i \mid A)=\frac{P(B_i)P(A \mid B_i)}{\sum_{j=1}^{n}P(B_j)P(A \mid B_j)}。\tag{1}$$

式中由先验概率 $P(B)$和条件概率 $P(A \mid B)$估计后验概率 $P(B \mid A)$，基于此可对贝叶斯网络推理。

1.2 动态贝叶斯网络

动态贝叶斯网络在保留了静态贝叶斯网络特性的基础上，增加了对时间因素的考虑。在时间轴上展开后，定义每段时间间隔下的贝叶斯网络为时间片。网络的拓扑结构、变量集合间的内部关系在每个时间片下都是相同的。设 $X[t]$为 t 时刻网络中节点变量，如果要得到 $X[0]\cup X[1]\cup\cdots$上的概率分布既复杂又无太大实际意义，可作如下假设[8]：

1) 在 X 中的变化过程满足马尔科夫链(Markov chain)模型，即：

$$P(X[t+1] \mid X[0],\cdots,X[t])=P(X[t+1] \mid X[t])。\tag{2}$$

式(2)说明变量在 t+1 时间的状态只依赖于 t 时间的状态，与其他时刻无关。

2) 在有限时间范围内该过程是平稳的，即转移概率 $P(X[t+1] \mid X[t])$ 与时间 t 无关。

在上述假设的基础上，还需要确定初始状态 $X[0]$的概率分布，组成一个完整的动态贝叶斯网络如图 1 所示。

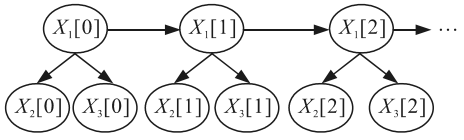

图 1 动态贝叶斯网络结构

设变量 X_i 的父节点集为 Pa_i，则 n 个节点的联合概率分布[9]为：

$$P(X_1,X_2,\cdots,X_n)=\prod_{i=1}^{n}P(X_i \mid Pa_i)。\tag{3}$$

1.3 概率推理

将已知变量观测值称为证据，概率推理是通过证据推测待查询变量的过程。贝叶斯网络中由联合概率分布来计算后验概率称为精确推理。然而当网络中节点较多、连接繁杂时，精确推理计算复杂费时。此时可以适当降低精度要求，在有限时间内求得近似解。实际应用中，通常使用吉布斯采样方法[10]进行贝叶斯网络的近似推理。以下对吉布斯采样进行简要的介绍。

设 $Y=\{Y_1,Y_2,\cdots,Y_m\}$ 为待查询变量，其中 $y=(y_1,y_2,\cdots,y_m)$ 是待查询变量的一组取值，$X=\{X_1,X_2,\cdots,X_n\}$ 表示证据变量，已知其取值为 $x=\{x_1,x_2,\cdots,x_n\}$。推理的目标就是计算后验概率 $P(Y=y \mid X=x)$。吉布斯采样算法首先随机产生一个与证据 $X=x$ 一致的样本 $\boldsymbol{y}^0$ 作为起始点，之后每步由当前样本产生下一个样本。即在第 k 次采样中，算法先假设 $\boldsymbol{y}^k=\boldsymbol{y}^{k-1}$，然后对非证据变量逐一采样改变其值，采样概率根据贝叶斯网络与其他变量的当前值计算获得。假设经 K 次采样得到的与 $\boldsymbol{y}$ 一致的样本共有 n_y 个，则可用下式估算出后验概率：

$$P(Y=\boldsymbol{y} \mid X=\boldsymbol{x})\simeq\frac{n_y}{K}。\tag{4}$$

在贝叶斯网络中无极端概率为 0 或 1 时，吉布斯采样第 k 步的状态分布在 $k\to\infty$ 时，必须收敛于平稳分布 $P(Y \mid X=x)$；因此，在 K 很大时，确保了式(4)收敛于 $P(Y=y \mid X=x)$。

2 基于动态贝叶斯网络的目标威胁评估

对空袭目标威胁评估的基本目的是区分目标对我方威胁程度的大小和次序，以保证辅助决策系统的快速性及准确性。使用贝叶斯网络进行威胁评估时，首先要分析来袭威胁目标的各个影响因素及其状态集合，然后确定贝叶斯网络模型结构及参数，最后选择适当的算法推理。

2.1 确定影响因素

空中目标的威胁程度受多种因素影响，主要分为攻击能力、攻击意图和飞临时间[11]。这些因素又受目标类型、载弹量、机动能力、高度、航路捷径、角度、距离和速度等影响。这些因素相互作用、相互联系，体现了目标对己方的攻击企图和威胁程度。

目标类型：通过目标识别得到的关于空中来袭

目标的属性，如巡航导弹、固定翼飞机、无人机等。目标类型决定了其攻击能力。

目标攻击能力主要由载弹量、机动能力和目标类型等决定。目标载弹量越大、机动能力越强，则攻击能力越强，对我方的威胁也越大。

目标攻击意图主要由目标高度、航路捷径和角度等决定。目标高度越低、航路捷径越小、飞行方向与敌我连线夹角越小，则目标攻击意图越明显，对我方的威胁也就越大。

飞临时间主要由目标距离、速度和角度等决定。目标距离越近、速度越大、角度越小，则飞临我方的时间越短，威胁也越大。

贝叶斯网络的推理复杂度随节点状态数的增加呈指数增长，故状态数取 3 个左右为宜[12]。设定各节点的状态集合如表 1 所示。

表 1　各节点的状态集合

节点	状态		
目标威胁度(X)	高(X_H)	中(X_M)	低(X_L)
攻击能力(C)	强(C_S)	中(C_M)	弱(C_W)
攻击意图(I)	强(I_A)	中(I_M)	弱(I_W)
飞临时间(T)	短(T_S)	中(T_M)	长(T_L)
载弹量(P)	多(P_R)	中(P_M)	少(P_F)
机动能力(M)	强(M_G)	中(M_M)	弱(M_L)
目标类型(K)	导弹(K_M)	战斗机(K_F)	侦察机(K_S)
目标高度(H)	低空(H_L)	中空(H_M)	高空(H_U)
航路捷径(S)	范围内(S_I)	边缘(S_B)	范围外(S_O)
目标角度(A)	小(A_S)	中(A_M)	大(A_B)
目标距离(D)	近(D_N)	中(D_M)	远(D_F)
目标速度(v)	高速(v_F)	中速(v_M)	低速(v_L)

2.2　威胁评估的动态贝叶斯网络模型

根据 2.1 节中的影响因素，结合领域专家经验构建静态贝叶斯网络，在时间维度上展开得到动态贝叶斯网络威胁评估模型。时间片的间隔由目标信息实际更新周期决定。建立威胁评估的动态贝叶斯网络模型结构如图 2 所示。

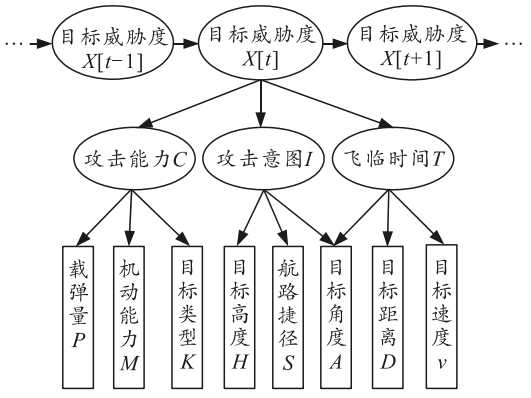

图 2　动态贝叶斯网络威胁评估模型结构

结合专家知识，对已知样本数据进行极大似然估计，得到该模型的条件概率如表 2—7 所示。

表 2　目标威胁度转移概率

$X[t]$	$P(X[t+1] \mid X[t])$		
	X_H	X_M	X_L
X_H	0.70	0.18	0.12
X_M	0.18	0.60	0.22
X_L	0.11	0.23	0.66

表 3　威胁度条件概率

X	$P(C \mid X)$			$P(I \mid X)$			$P(T \mid X)$		
	$[C_S$	C_M	$C_W]$	$[I_A$	I_M	$I_W]$	$[T_S$	T_M	$T_L]$
X_H	0.72	0.17	0.11	0.71	0.17	0.12	0.71	0.17	0.12
X_M	0.15	0.63	0.22	0.18	0.62	0.20	0.19	0.62	0.19
X_L	0.09	0.20	0.71	0.08	0.24	0.68	0.11	0.21	0.68

表 4　攻击能力条件概率

C	$P(P \mid C)$			$P(M \mid C)$			$P(K \mid C)$		
	$[P_R$	P_M	$P_F]$	$[M_G$	M_M	$M_L]$	$[K_M$	K_F	$K_S]$
C_S	0.71	0.19	0.10	0.67	0.22	0.11	0.68	0.19	0.13
C_M	0.18	0.63	0.19	0.18	0.66	0.16	0.18	0.65	0.17
C_W	0.09	0.25	0.66	0.11	0.20	0.69	0.10	0.21	0.69

表 5　攻击意图条件概率

I	$P(H \mid I)$			$P(S \mid I)$		
	$[H_L$	H_M	$H_U]$	$[S_I$	S_B	$S_O]$
I_A	0.72	0.21	0.07	0.73	0.19	0.08
I_M	0.14	0.62	0.24	0.17	0.64	0.19
I_W	0.09	0.21	0.70	0.08	0.21	0.71

表 6　攻击意图及飞临时间联合条件概率

I	T	$P(A \mid I, T)$		
		A_S	A_M	A_B
I_A	T_S	0.79	0.16	0.05
I_A	T_M	0.52	0.37	0.11
I_A	T_L	0.52	0.11	0.37
I_M	T_S	0.49	0.38	0.13
I_M	T_M	0.08	0.77	0.15
I_M	T_L	0.07	0.45	0.48
I_W	T_S	0.46	0.17	0.37
I_W	T_M	0.08	0.38	0.54
I_W	T_L	0.08	0.13	0.79

表 7　飞临时间条件概率

T	$P(D \mid T)$			$P(v \mid T)$		
	$[D_N$	D_M	$D_F]$	$[v_F$	v_M	$v_L]$
T_S	0.68	0.21	0.11	0.68	0.20	0.12
T_M	0.17	0.68	0.15	0.19	0.63	0.18
T_L	0.08	0.18	0.74	0.10	0.21	0.69

表 2—7 既充分利用了样本数据信息，又保留了专家的经验知识，但仍有可能与实际情况偏离。可以根据结果适当调整 CPT 中的数据，以提高评估结果的准确性。

3　仿真分析

用如下案例进行仿真分析。假定雷达已发现空中有 3 个目标同时向我方袭来，我方对这 3 个空袭目标连续跟踪观测了 6 个时间(间隔为 1 s)。使用贝叶斯网络分析专用工具 Netica 建立网络模型，导入样本数据后对生成的条件概率表进行适当的调整。在未输入任何证据的条件下各节点的先验概率如图 3 所示。

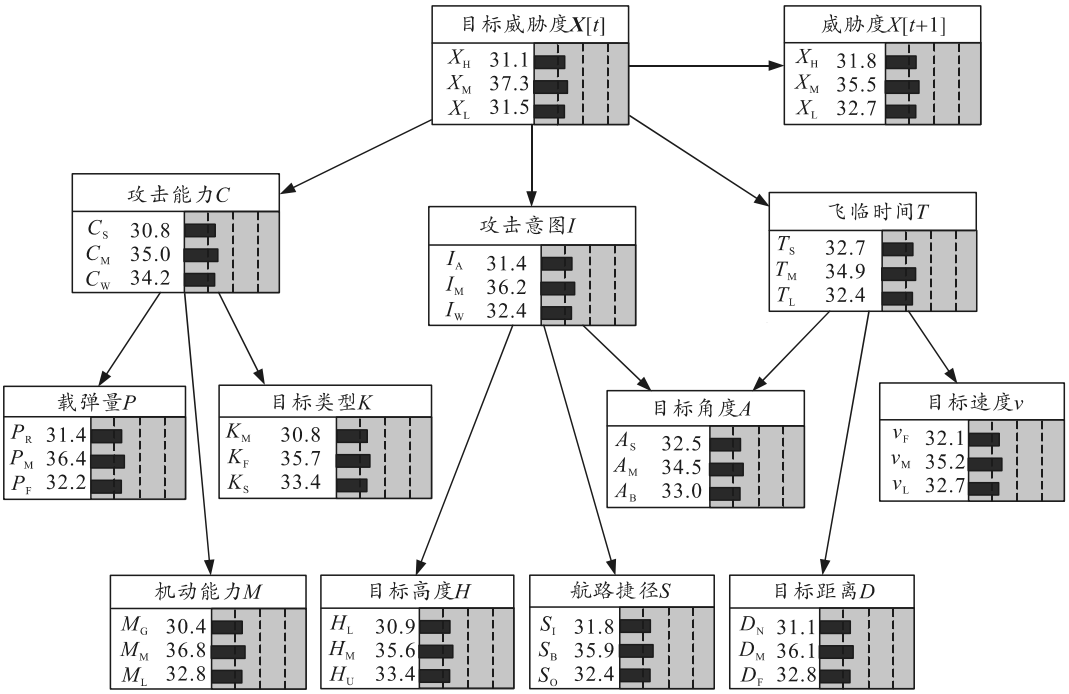

图 3　贝叶斯网络威胁评估模型先验概率

图中每个节点各状态的先验概率比较接近，其中每个影响因素取中间状态的概率略高于其他状态，这与人在没有得到任何信息条件下的判断倾向一致。

由于获取的证据信息具有误差和不确定性，可采用隶属度函数[13]，将证据模糊离散化。得到目标 1 的似然证据信息如表 8 所示。

表 8　目标 1 不同时刻的似然证据信息

时间/s	目标 1 各变量证据概率/%			
	(P_R,P_M,P_F)	(M_G,M_M,M_L)	(K_M,K_F,K_S)	(H_L,H_M,H_U)
1	(62,24,14)	(35,43,22)	(18,54,28)	(47,43,10)
2	(63,28,9)	(40,32,28)	(27,55,18)	(41,43,16)
3	(63,28,9)	(62,26,12)	(18,65,17)	(27,49,24)
4	(43,42,15)	(65,21,14)	(11,73,16)	(34,33,33)
5	(24,57,19)	(32,44,24)	(7,47,46)	(11,31,58)
6	(21,65,14)	(36,37,27)	(26,47,27)	(13,37,50)
时间/s	(S_I,S_B,S_O)	(A_S,A_M,A_B)	(D_N,D_M,D_F)	(v_F,v_M,v_L)
1	(71,16,13)	(63,29,8)	(36,51,13)	(61,29,10)
2	(61,28,11)	(71,25,4)	(66,26,8)	(66,25,9)
3	(26,60,14)	(51,43,6)	(64,22,14)	(35,37,28)
4	(26,57,17)	(40,50,10)	(24,62,14)	(37,45,18)
5	(17,25,58)	(34,58,8)	(14,42,44)	(52,37,11)
6	(9,14,77)	(18,67,15)	(21,27,52)	(68,19,13)

由表可知：目标 1 大致为战斗机先向我方飞临再偏离，期间爬升了高度；另外，目标 2 为导弹由远及近直线向我方飞临；目标 3 为侦察机于较远处高空盘旋。

根据各目标的似然证据信息，利用动态贝叶斯网络威胁评估模型，得到目标 1 攻击能力、攻击意图及飞临时间节点的后验概率如表 9 所示。

表 9　目标 1 攻击能力、攻击意图及飞临时间后验概率

时间/	$P(C\|P,M,K)$			$P(I\|H,S,A)$			$P(T\|A,D,V)$		
s	$[C_S$	C_M	$C_W]$	$[I_A$	I_M	$I_W]$	$[T_S$	T_M	$T_L]$
1	0.49	0.35	0.16	0.65	0.26	0.09	0.58	0.33	0.09
2	0.55	0.33	0.12	0.62	0.29	0.09	0.72	0.22	0.06
3	0.54	0.37	0.09	0.39	0.48	0.13	0.57	0.31	0.12
4	0.41	0.46	0.13	0.35	0.47	0.18	0.37	0.50	0.13
5	0.21	0.49	0.30	0.17	0.41	0.42	0.33	0.45	0.22
6	0.25	0.49	0.26	0.12	0.40	0.48	0.35	0.37	0.28

得到目标 1 威胁度各时间分别为高、中、低的后验概率如图 4 所示。

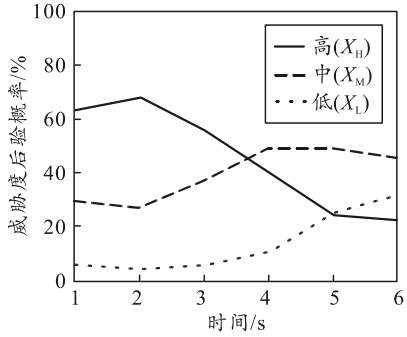

图 4　目标 1 威胁度后验概率变化趋势

由以上动态贝叶斯网络的推理结果可知：目标 1 威胁度为高的概率先小幅度上升，在第 2 时间后呈下降趋势，与表 9 中目标的攻击能力、攻击意图及飞临时间相适应。根据目标 1 的状态结合 2.1 节中的分析，仿真结果与实际情况相符。

再分别对目标 2 和目标 3 进行仿真分析，得到各目标威胁度分别为高、中、低的后验概率如表 10 所示。

表 10　各目标威胁度后验概率

时间/s	目标 1 $P(X\|C,I,T)$			目标 2 $P(X\|C,I,T)$			目标 3 $P(X\|C,I,T)$		
	$[X_H$	X_M	$X_L]$	$[X_H$	X_M	$X_L]$	$[X_H$	X_M	$X_L]$
1	0.64	0.30	0.06	0.48	0.33	0.19	0.08	0.31	0.61
2	0.68	0.27	0.05	0.58	0.31	0.11	0.06	0.23	0.71
3	0.56	0.38	0.06	0.73	0.22	0.05	0.05	0.18	0.77
4	0.40	0.49	0.11	0.85	0.12	0.03	0.04	0.19	0.77
5	0.25	0.49	0.26	0.93	0.05	0.02	0.03	0.22	0.75
6	0.23	0.45	0.32	0.93	0.05	0.02	0.06	0.25	0.69

得到威胁度的后验概率后，通常可采用加权方法[12]，计算目标的静态威胁值。定义威胁度为高、中、低的期望值分别为 1.00，0.55，0.10，则威胁值

$$\boldsymbol{X}_{\text{th}}=[1.00 \quad 0.55 \quad 0.10]\cdot\begin{bmatrix}P(\boldsymbol{X}=X_{\text{H}})\\P(\boldsymbol{X}=X_{\text{M}})\\P(\boldsymbol{X}=X_{\text{L}})\end{bmatrix}。\tag{5}$$

求得各目标威胁值随时间的变化如图 5 所示。

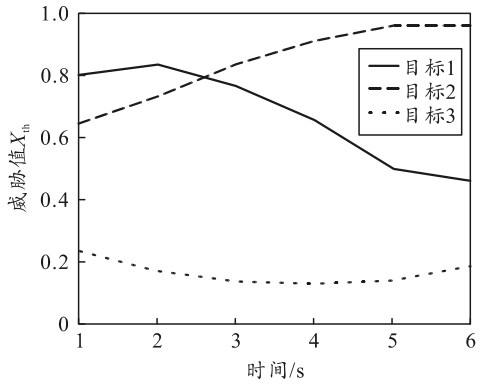

图 5　各目标加权后威胁值变化趋势

由图可知：目标 2 初始的威胁值较目标 1 小，为 0.68 左右，随后持续上升，在第 3 时间超过了目标 1，在第 6 时间达到最大值 0.96。目标 3 的威胁值始终低于目标 1 和目标 2，在 0.25 左右浮动。结合目标的状态变化，以上威胁值的变化结果均与实际情况一致，即采用动态贝叶斯网络模型可有效地对空袭目标的威胁进行评估与排序。

4　结束语

笔者提出了一种威胁评估的动态贝叶斯网络模型。针对影响目标威胁度的攻击能力、攻击意图和飞临时间等因素，采用样本估计结合专家知识的构建方法得到条件概率表，运用吉布斯采样的近似推理方法得到威胁度的后验概率。仿真结果表明：该模型合理有效，能为火力分配辅助决策提供支撑，最终对空袭目标实施有效的末端拦截。需要指出，贝叶斯网络是基于先验概率进行的推理，故威胁估计的准确性与先验概率及推理方法有极大的关系；因此，下一步的研究方向是如何通过参数学习提高模型精度以及选择合适的推理算法，进而提高威胁评估的准确度和速度。

参考文献：

[1] 晏师励, 李德华. 基于动态贝叶斯网络的空战目标威胁等级评估[J]. 计算机与数字工程, 2015, 43(12): 2150-2154, 2198.

[2] 孙宁, 冯琦, 高晓光, 等. 缺失数据下基于直觉模糊的动态威胁评估[J]. 火力与指挥控制, 2018, 43(8): 91-95.

[3] 闫冲冲, 郝永生. 基于层次分析法(AHP)的空中目标威胁度估计[J]. 计算技术与自动化, 2011, 30(2): 118-121.

[4] 韩其松, 余敏建, 高阳阳, 等. 云模型和距离熵的 TOPSIS 法空战多目标威胁评估[J]. 火力与指挥控制, 2019, 44(4): 136-141.

[5] 张浩为, 谢军伟, 盛川, 等. 基于改进灰色关联算法的目标威胁评估[J]. 计算机工程与科学, 2017, 39(10): 1908-1914.

[6] 陈侠, 刘子龙. 基于模糊小波神经网络的空中目标威胁评估[J]. 战术导弹技术, 2018(3): 53-59.

[7] 王朔. 基于贝叶斯网络的舰艇导弹防御系统决策模型算法研究[D]. 长沙: 国防科学技术大学, 2005: 11-12.

[8] 李亮. 基于动态贝叶斯网络方法的战场态势重构技术研究[D]. 南昌: 南昌航空大学, 2013: 31-32.

[9] 马晓明, 丁平, 晏卫东. 基于贝叶斯网络的舰船目标毁伤评估[J]. 兵工自动化, 2016, 35(6): 72-75.

[10] 周志华. 机器学习[M]. 北京: 清华大学出版社, 2016: 161-162.

[11] 张银燕. 基于云模型理论的空中目标威胁评估方法[D]. 郑州: 解放军信息工程大学, 2013: 15-16.

[12] 付涛, 王军. 防空系统中空中目标威胁评估方法研究[J]. 指挥控制与仿真, 2016, 38(3): 63-69.

[13] 卞泓斐, 杨根源. 基于动态贝叶斯网络的舰艇防空作战威胁评估研究[J]. 兵工自动化, 2015, 34(6): 14-19.