doi:10.3969/j.issn.1671-637X.2014.09.002

基于模糊贝叶斯网的威胁等级评估研究

丁达理[1,2]， 罗建军[2]， 王 铀[1]， 刘万俊[1]
（1.空军工程大学航空航天工程学院,西安 710038； 2.西北工业大学航天学院,西安 710072）

摘 要：针对现代复杂战场环境下威胁等级评估信息的不确定性,结合模糊数学及贝叶斯网提出了基于模糊贝叶斯网的威胁等级评估方法。在充分考虑威胁源相对于UCAV的距离、方位角对其隐身能力影响的基础上,从不确定性知识的概率化入手,综合天气、威胁类型、距离、方位角等不确定因素对威胁等级进行评估,采用加拿大Norsys软件公司的Netica软件建立贝叶斯网威胁评估模型并进行仿真。结果表明,该方法能快速、准确地评估威胁等级,具有一定的参考价值。

关键词：自主攻击；威胁等级评估；隐身能力；模糊理论；贝叶斯网
中图分类号：V279；TP391.9 **文献标志码**：A **文章编号**：1671-637X(2014)09-0007-04

Threat Level Assessment Based on Fuzzy Bayesian Networks

DING Da-li[1,2], LUO Jian-jun[2], WANG You[1], LIU Wan-jun[1]
(1. Engineering College of Aeronautics and Astronautics, Air Force Engineering University, Xi'an 710038, China;
2. College of Astronautics, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract: Aiming at the uncertainty of Threat Level Assessment (TLA) data sources under modern complex battlefield, a fuzzy Bayesian network TLA method was proposed by integrating the fuzzy set theory into Bayesian networks. After well considering about the effect of the distance and azimuth angle of threat sources relative to a UCAV on its stealth capability, the threat level was evaluated by integrating such uncertain factors as weather, threat type, distance and azimuth angle based on randomization of uncercain knowledge. Then a TLA Bayesian network was established by adopting Netica software of the Norsys Software Company in Canada, and simulation was carried out. The simulation results show that the method can assess the threat level rapidly and accurately.

Key words: autonomous combat; threat level assessment; stealth capability; fuzzy set theory; Bayesian network

0 引言

在UCAV自主攻击轨迹决策时,为选择一条威胁较小的轨迹,尽可能地减少被敌方发现和摧毁的危险,应根据战场环境的威胁信息和接收控制站发送的信息,及时将规划环境内的威胁进行量化并表示出来,这就需要对威胁等级进行评估[1-2]。

在威胁等级评估过程中,存在很多不确定性因素,这些因素对轨迹决策具有很大的影响。针对上述问题,本文结合模糊数学在不确定性知识表达方面的优点及贝叶斯网(Bayesian Networks, BN)在不确定性知识推理方面的强大功能,提出了基于模糊贝叶斯网(Fuzzy Buyesian Networks, FBN)的威胁等级评估方法[3-5]。该方法从不确定性知识的概率化入手,将不确定性因素的影响考虑到威胁评估中,提高了评估结果的可信性。

收稿日期:2013-06-15 **修回日期**:2013-11-14
基金项目:航空科学基金(20105196016)
作者简介:丁达理(1980—),男,湖南益阳人,博士,副教授,研究方向为无人飞行器武器系统总体技术。

1 模糊贝叶斯网(FBN)

1.1 FBN的定义

1981年,HOWARD R和MATHESON J结合贝叶斯概率方法和有向无环图(Directed Acyclic Graphs, DAG)网络拓扑结构,提出一种基于概率分析和图论的不确定性知识表达和推理的模型,用来描述数据变量之间概率依赖关系,这就是贝叶斯网。例如,可以将一个二元组 $BN=(G,\theta)$,表示为一个贝叶斯网。其中,

网络结构 $G=(V,A)$，是一个 DAG，$V=\{V_1,V_2,\cdots,V_n\}$，为节点，$n\geq 1$，A 为弧的集合；网络参数 θ 是描述节点相关的条件概率表(Conditional Probability Table，CPT)，表示为 $P(V_i|Pa(V_i))$，即节点 V_i 与父节点 $Pa(V_i)$ 间的条件概率，若节点无父节点，则用先验概率表示其条件概率。

FBN 将贝叶斯网的节点变量由连续推广为模糊。假定可用一个有限的节点集 $X=\{x_1,x_2,\cdots,x_n\}$ 表示一个问题，用 u_i 表示 x_i 的所有可能状态集。

假定 $x_i\in X$ 可被模糊化为模糊随机变量 u_i，且 x_i 的所有可能状态被 u_i 继承，则 x_i 的模糊集为

$$u_i=\{u_{i1},u_{i2},\cdots,u_{ik}\} \tag{1}$$

式中：k 为 u_i 的模糊状态数；u_{ij} 为 u_i 的第 j 个模糊状态，表示为

$$u_{ij}=\{x_i,\mu_{ij}(x)\,|\,x_i\in X\} \tag{2}$$

式中，$\mu_{ij}(x)$ 为变量 x_i 隶属于 u_i 中第 j 个模糊状态 u_{ij} 的程度，用 u_{ij} 在给定 x_i 条件下的概率表示。

假定 $U=\{u_1,u_2,\cdots,u_n\}$，并用有向弧来表示其中变量的因果依赖关系，即

$$L=\{(u_i,u_j)\,|\,i\neq j,i,j=1,2,\cdots,n\}\subset U\times U \text{ 。} \tag{3}$$

用条件概率表表示因果依赖的概率性，即

$$P=\{P(u_i|\pi(u_i))\,|\,i=1,2,\cdots,n\} \tag{4}$$

式中，$\pi(u_i)$ 为模糊变量 u_i 父节点的集合。

因此，FBN 可表示为三元组

$$FBN=\{U,L,P\} \text{ 。} \tag{5}$$

1.2 模糊概率转换

比较模糊逻辑和贝叶斯网，前者在知识表示上优于后者，而后者在推理能力上又优于前者。为结合两者的优点，需引入模糊概率转换公式，从而将连续节点的模糊隶属度转换成可进行网络推理的概率。

设 $Q=\{q_1,q_2,\cdots,q_n\}$，为一个离散有限集合，取 Q 中的一个变量 x，$x=q_i$ 时的概率为 $p(q_i)$，$x=q_i$ 时的可能性为 $\pi_x(q_i)$，模糊集合 F 的隶属度函数为 $\mu_F(q)$。

Zadeh 认为，可能性理论是模糊集理论的扩展，因此，模糊集上的隶属函数可决定可能性理论中的可能性分配 π，则

$$\pi_x(q)=\mu_F(q) \text{ 。} \tag{6}$$

Geer 和 Klir 认为，在可能性概率转换过程中提出“信息转换保护”(Information Transforming Preservation)，即在两种理论相互转换的过程中，信息的不确定性应保持不变。所提转换公式[6]为

$$p(q_i)=\frac{\pi(q_i)^{1/\alpha}}{\sum_{k=1}^{n}\pi(q_k)^{1/\alpha}},\quad 0<\alpha<1 \tag{7}$$

式中，常量 α 表示可能性概率满足转换一致性条件的程度。α 趋向 0，则转换概率 $p(q_i)$ 间的差异较大；α 趋向 1，则差异较小。

联立式(6)和式(7)，得到

$$p(q_i)=\frac{\mu(q_i)^{1/\alpha}}{\sum_{k=1}^{n}\mu(q_k)^{1/\alpha}} \text{ 。} \tag{8}$$

运用式(8)，就可以将模糊因素转换为概率形式，使得在利用贝叶斯网评估威胁等级时，可以考虑模糊不确定性因素的影响，从而提高评估结果的可信度。

2 FBN 威胁等级评估模型

2.1 FBN 威胁等级评估建模

为了分析上述模型的准确性和有效性，建立如图 1 所示的贝叶斯网威胁等级评估模型进行仿真。

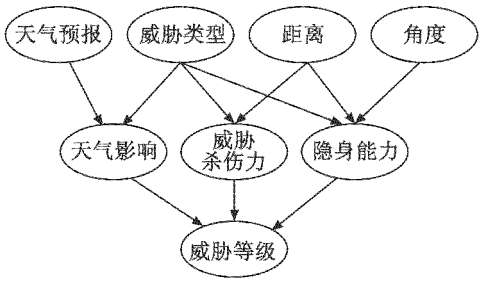

图 1 贝叶斯网威胁等级评估模型

Fig. 1 The model of threat level assessment based on Bayesian networks

2.2 模型中各节点的知识表示

贝叶斯网威胁等级评估模型中集成了大量的离散和连续节点，必须要对所有的节点统一进行表示，将连续节点的值转换为其处于各对应状态的概率，才能满足贝叶斯网的应用要求，以完成网络学习和推理[7]。威胁等级评估所考虑的离散变量如下所述。

天气预报(F_W)：天气状况可分为晴朗(Fine)、多云(Cloudy)、阴天(Overcast)。

威胁类型 T_T：由于是对地攻击，主要考虑雷达(Radar)、高炮(Artillery)、地空导弹(Missile)。

威胁等级评估所考虑的连续型变量取值均为 0～1 之间，规定各节点模糊评价等级如下所述。

距离影响：地面防空威胁一般包括雷达(Radar)、高炮(Artillery)、地空导弹(Missile)，其作用半径分别为 57 km、6 km、43 km。据此可将威胁源与 UCAV 的距离划分为：近距(near range)，其范围为 0～6 km；中距(medium range)，其范围为 6～43 km；远距(far range)，其范围为 43～57 km；超远距(supper far range)，其范围为大于 57 km。

角度影响：可将威胁源相对于 UCAV 的方位角划分为：0°(near 0 degree，N0D)，其范围为方位角的

±50°;90°(near 90 degree,N90D),其范围为方位角的50°~130°;180°(near 180 degree,N180D),其范围为方位角的130°~230°;270°(near 270 degree,N270D),其范围为方位角的230°~310°。

天气影响:对不同类型的威胁,不同的天气条件会对其产生不一样的影响,影响程度分为无影响(E_N)、轻度影响(E_L)、中度影响(E_M)、严重影响(E_S)4 个等级。

威胁杀伤力:地面威胁的杀伤力主要与威胁类型和距离有关,分为高(H)、中(M)、低(L)。

隐身能力:隐身能力对于提高 UCAV 的突防能力起着至关重要的作用。UCAV 相对雷达波照射方向形成不同反射面导致不同的 RCS,目标头向和尾向 RCS 相对较小,两翼部分 RCS 最大。随着 UCAV 与威胁源距离减小,其隐身能力逐渐降低。本文将隐身能力的影响主要考虑为与角度和距离有关,分为高(H)、中(M)、低(L)。

对威胁等级评估数据知识表示的研究,包括对天气、距离、角度等的模糊处理,并且根据概率转换获取各节点相应状态的概率。

主要步骤如下:1)通过专家评分或威胁等级评估软件仿真得到相应节点的确定值;2)根据相应节点的模糊划分,构造与之相对应的模糊隶属度函数;3)对各节点相应状态的隶属度进行概率转换,获得可进行贝叶斯网推理的概率值。

对距离采用梯形隶属度函数,即

$$g(x;a,b,c,d)=\begin{cases}0, & x<a\\ (x-a)/(b-a), & a\leqslant x\leqslant b,\\ 1, & b\leqslant x\leqslant c\\ (d-x)/(d-c), & c\leqslant x\leqslant d\\ 0, & x\geqslant d\end{cases}\quad(9)$$

式中,4 个语言值近距(near range)、中距(medium range)、远距(far range)、超远距(supper far range)的参数$[a,b,c,d]$取值分别为$[-2,0,4,8]$,$[4,8,41,45]$,$[41,45,55,59]$,$[55,59,\infty,\infty]$。隶属度曲线如图 2 所示。

假设确定距离为 42 km,则对应隶属度为(0,0.75,0.25,0),通过式(8)进行概率转换可得(0,0.9,0.1,0)(参数$\alpha=0.5$)。

对角度影响节点,语言变量的隶属度函数可采用梯形隶属度函数。式(9)中,4 个语言值为 0°、90°、180°、270°的参数$[a,b,c,d]$分别取值为[305,315,45,55],[45,55,125,135],[125,135,225,235],[225,235,305,315]。隶属度曲线如图 3 所示。

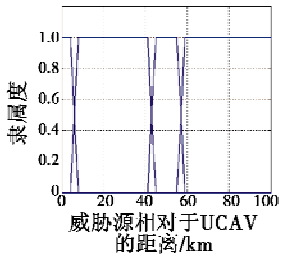

图 2　距离影响节点隶属度曲线

Fig. 2　Membership curve of distance

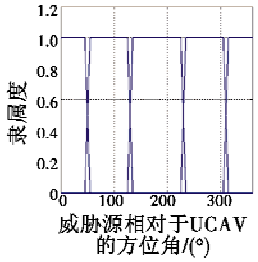

图 3　角度影响节点隶属度曲线

Fig. 3　Membership curve of angle

2.3　参数学习

建立贝叶斯网模型之后,还需对网络参数进行学习后才能获得可用的推理模型,网络参数的学习可通过样本学习或者专家知识以确定网络中各节点的条件概率。本文主要通过专家知识进行参数学习,确定各节点的条件概率。在确定每个节点的初始概率之后,就可进行贝叶斯网推理,以获得各节点所有可能状态的概率分布,建立威胁等级评估模型。

3　数字仿真与结果分析

3.1　仿真流程

整个过程的仿真流程如图 4 所示。

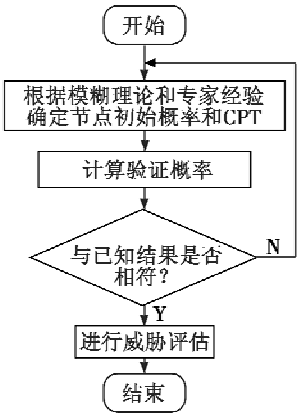

图 4　仿真流程图

Fig. 4　Flow chart of simulation

首先根据模糊理论和专家经验确定各节点的初始概率和条件概率表,然后计算验证概率是否与计算结果相符,如果相符进行威胁评估,如果不相符,则修正节点初始概率。

威胁评估算法采用加拿大 Norsys 软件公司的 Netica 软件,建立的贝叶斯网威胁评估模型如图 5 所示。

对不同作战条件下的威胁等级进行评估,结果均以威胁程度高的概率的形式给出。此软件的原理是根据节点初始概率,对各级采用条件概率公式和全概率公式求解,例如以在不同天气预报(Fine,Cloudy,Over-

cast)和不同威胁类型(Radar,Artillery,Missile)条件下确定天气影响(E_W)为无影响(E_N)的概率$P(E_W=E_N)$为例,计算过程为

$$P(E_W=E_N)=P(E_W=E_N|F_W)P(F_W)+P(E_W=E_N|T_T)P(T_T)=P(E_W=E_N|F_W=\text{Fine})P(F_W=\text{Fine})+P(E_W=E_N|F_W=\text{Cloudy})P(F_W=\text{Cloudy})+P(E_W=E_N|F_W=\text{Overcast})P(F_W=\text{Overcast})+P(E_W=E_N|T_T=\text{Radar})P(T_T=\text{Radar})+P(E_W=E_N|T_T=\text{Artillery})P(T_T=\text{Artillery})+P(E_W=E_N|T_T=\text{Missile})P(T_T=\text{Missile})\quad。\tag{10}$$

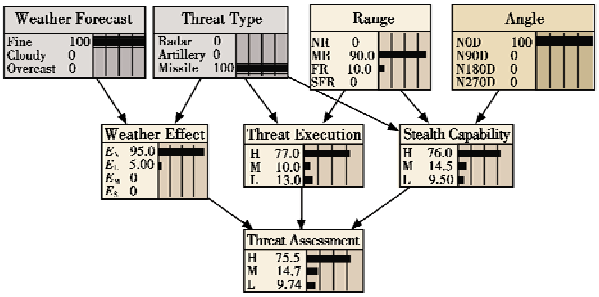

图5 贝叶斯网仿真模型

Fig. 5 Simulation model of Bayesian network

3.2 仿真结果及分析

仿真1:不同距离条件下的仿真。

假设天气晴朗,方位角恒为0°,在不同距离条件下对威胁等级评估进行仿真,如表1所示。

表1 不同距离条件下威胁仿真结果

Table 1 The results under different distances

类型	距离/km		
	56	42	5
雷达	10.9%	15.6%	19.5%
高炮	0.1%	0.1%	80.3%
地空导弹	10.2%	75.5%	85.2%

结合图5和表1可以看出,在同一威胁类型条件下,距离越小,威胁等级越高。这是由于随着距离的接近,地面威胁的杀伤能力在增强,而隐身能力却被削弱,此消彼长,导致威胁增大,因而威胁等级增高,这与实际是相符的。

仿真2:不同方位角条件下仿真。

假设天气晴朗,距离恒为42 km,在不同方位角条件下对威胁等级评估进行仿真,结果如表2所示。

表2 不同角度条件下威胁仿真结果

Table 2 The results with different angles

类 型	方 位 角/(°)		
	0	90	150
雷达	15.6%	18.5%	16.2%
高炮	0.1%	0.1%	0.1%
地空导弹	75.5%	78.3%	76.4%

结合图5和表2可以看出,在同一威胁类型条件下,方位角为90°时,威胁等级较高,150°时次之,0°时较小。这是由于UCAV相对雷达波照射方向形成不同反射面导致不同的RCS,目标头向和尾向RCS相对较小,两翼部分RCS最大。这就意味着方位角为0°和180°时威胁等级最小,而90°和270°时威胁等级最大,与实际是相符的。

隐身能力对于提高UCAV的突防能力起着至关重要的作用。综合威胁源相对UCAV的距离、方位角对UCAV隐身能力的影响评估威胁等级,体现了现代战争隐身作战的特点,对UCAV自主攻击轨迹决策具有重要意义。

4 结语

本文在充分考虑UCAV相对于威胁源的距离、方位角对其隐身能力影响的基础上,综合天气、威胁类型、距离、方位角等不确定因素对威胁等级进行评估。该方法从不确定性知识的概率化入手,将不确定性因素的影响考虑到威胁评估中,提高了评估结果的可信性。模型可以对收集到的威胁等级数据进行学习,不断地进行网络更新,从而使UCAV可以对不同作战条件下威胁等级进行实时评估,大大提高了决策过程的灵活性、快速性以及自动化和智能化程度。

参 考 文 献

[1] 黄长强,曹林平,翁兴伟,等. 无人作战飞机精确打击技术[M]. 北京:国防工业出版社,2011:1-3.
HUANG C Q, CAO L P, WENG X W, et al. Precision strike technology for UCAV[M]. Beijing: National Defense Industry Press, 2011:1-3.

[2] 丁达理,宋磊,贺建良,等. 基于Voronoi图和离散微粒群优化算法的UCAV攻击轨迹决策[J]. 空军工程大学学报:自然科学版,2012,13(2):1-5.
DING D L, SONG L, HE J L, et al. Attack trajectory decision-making for UCAV based on Voronoi diagram and DPSO algorithm[J]. Journal of Air Force Engineering University: Natural Science Edition, 2012, 13(2):1-5.

[3] 税薇,葛艳,韩玉. 基于贝叶斯网络的火力威胁等级评估算法[J]. 系统仿真学报,2009,21(15):4625-4627,4631.
SHUI W, GE Y, HAN Y. Algorithm of fire power threat level assessment based on Bayesian network [J]. Journal of System Simulation, 2009, 21(15):4625-4627, 4631.

[4] 杨健,高文逸,刘军. 一种基于贝叶斯网络的威胁估计方法[J]. 解放军理工大学学报:自然科学版,2010,11(1):43-48.

(下转第15页)