文章编号：1003-501X(2008)05-0001-05

基于模糊贝叶斯网络的态势威胁评估模型

康长青[1,2]，郭立红[1]，罗艳春[1,2,3]，王心醉[1,2]

(1. 中国科学院长春光学精密机械与物理研究所，长春 130033;
2. 中国科学院研究生院，北京 100039; 3. 空军航空大学，长春 130022)

摘要：针对传感器测量数据的不确定性，提出基于模糊贝叶斯网络的态势威胁评估模型。该模型首先将不确定性数据分为模糊域和概率域两大类，然后在模糊域使用模糊综合评判得到威胁目标的动态威胁度，接着运用可能性概率转换理论将模糊表示的动态威胁度转化成概率域知识，最后在概率知识域使用贝叶斯网络推理算法得到目标的威胁等级。实例计算表明，该方法能够较好的反映威胁源的威胁等级，为武器系统选择跟踪打击目标提供决策依据，具有一定的实用性。

关键词：态势评估；威胁评估；模糊综合评判；贝叶斯网络

中图分类号：TP391.9 **文献标志码**：A

Model of Situation and Threat Assessment Based on Fuzzy Bayesian Network

KANG Chang-qing[1,2], GUO Li-hong[1], LUO Yan-chun[1,2,3], WANG Xin-zui[1,2]

(1. *Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun* 130033, *China*; 2. *Graduate School of Chinese Academy of Sciences, Beijing* 100039, *China*;
3. *Aviation University of Air Force, Changchun* 130022, *China*)

Abstract: To process uncertain data obtained in sensors, a model of Situation and Threat Assessment (STA) based on fuzzy Bayesian network was proposed. The uncertain sensor data were divided into vagueness domain and probability domain. The vague data type of the threat target was handled by fuzzy comprehensive evaluation, and the dynamic threat degree was obtained in fuzzy domain. And then the fuzzy dynamic threat degree was translated into the probabilistic type by the possibility/probability theory. All the uncertain data were figured in probabilistic type and processed by Bayesian network to produce the threat level of the target. An example indicates that the fuzzy Bayesian network can obtain the real threat levels and is feasible for weapon system to automate decision-making on target-selecting and target-striking.

Key words: situation assessment; threat assessment; fuzzy comprehensive evaluation; Bayesian network

1 引 言

态势威胁评估为防空指挥控制系统的重要功能之一，它对指挥员准确的判断敌情，正确的进行目标分配和火力分配，起着至关重要的作用。态势威胁评估位于美国国防部联合领导实验室提出的数据融合模型[1]中的第二级和第三级，与一级融合(位置和身份估计)相比，态势威胁建模要困难得多[2]。国内外研究人员对态势威胁评估建模应该采用什么样的方法和技术，并没有达成一致的意见。

目前威胁评估建模的方法主要有多属性决策方法，神经网络方法，和基于知识的表示和推理等方法[3-5]。

收稿日期：2007-08-20; 收到修改稿日期：2008-02-20
基金项目：国防武器装备预研项目
作者简介：康长青(1979-)，男(汉族)，湖北襄樊人，博士研究生，主要研究方向 C^3I 系统建模仿真，信息融合等。E-mail:kangchangqing@163.com
通讯作者：郭立红(1964-)，女(汉族)，吉林舒兰人，研究员，博士生导师，主要研究方向是计算机应用技术。

多属性决策方法简便灵活，便于工程实践，主要用于已知目标类型的空中目标威胁排序，缺点是对数据的缺失比较敏感。神经网络具有很好的自适应能力、自学习能力和高度线性和非线性映射能力，主要用于威胁假定和态势支持的偏好识别，缺点是训练样本的获取存在困难，输出结果难以解释。而基于知识的表示推理方法是目前态势威胁建模的主要方法，主要技术有专家系统，黑板模型，逻辑模板匹配和贝叶斯网络推理等技术。

本文针对贝叶斯网络推理方法在输入数据的表示较弱的特点，提出基于模糊贝叶斯网络的威胁评估模型。该模型首先将不确定知识分为两类，分别用模糊方法和概率方法表示出来。接着运用模糊综合评判方法计算得到了空中目标的动态威胁度，并用可能性概率转换理论将动态威胁度以概率的形式表示出来。然后将所有概率表示的威胁参数输入贝叶斯网络评估模型进行评估，得到目标的总威胁。

2 威胁评估的数据流模型

真实环境下态势场景急剧动态变化，态势威胁评估不可能提供预先定义的场景来进行简单的模式匹配，态势威胁评估应该是一个自适应的动态处理过程。因此提出威胁评估的功能数据流模型[2]，如图 1 所示。其中包括的各个处理部分的功能为：1) 数据收集 使用传感器管理和数据挖掘来获得真实环境中的实体,关系和事件；2) 假设产生 建立与提供数据相一致的候选威胁假设；3) 假设评价 对每一个候选威胁假设评分，并需要额外的数据来支持或拒绝假设；4) 假设选择 在全部可能性的基础上从候选假设中选择；5) 威胁警报 指示当前和预测的威胁态势和威胁事件；6) 模型管理 威胁模型的建立和提炼。

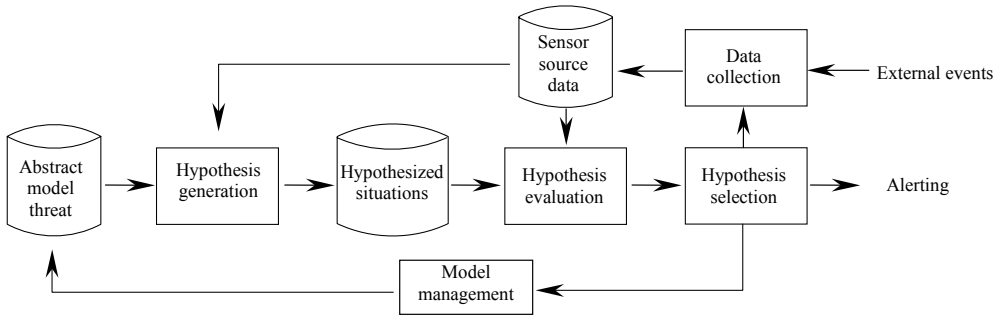

图 1 威胁评估功能流

Fig.1 Functional workflow of threat assessment

在图 1 中，威胁假设在威胁态势和威胁事件不断变化中，被连续不断的产生，评价和选择。同时由识别或预测出的态势事件建立的威胁模型被不断的抽象和提炼。

3 基于模糊贝叶斯网络的态势威胁评估模型

假定一个不明空中目标飞向某型武器系统的场景。武器系统利用多个传感器(雷达，跟踪电视，敌我识别系统等)可以获取的目标信息如目标类型，航迹等。由于传感器测量的数据带有不确定性，如何结合专家知识对这些不确定信息进行表示和推理，是进行态势威胁评估的关键所在。

依据 Klir 提出的不确定知识分类法，将不确定知识大体分为模糊(Vagueness)知识和多样性(Ambiguity)两大类[6]。例如，目标的距离很远，就是模糊知识。而目标可能是一架直升机或轰炸机，就是多样性知识。在数据融合研究中，模糊逻辑是处理模糊域知识的有力工具，而概率理论是处理多样性知识的有力工具。针对这两种不确定知识，本文建立以模糊综合评判，模糊—概率转换理论，贝叶斯网络为基础的态势威胁评估模型。

3.1 模糊综合评判

Zadeh 教授在 1965 年首先提出论文 Fuzzy Sets 奠定了模糊理论的基础。模糊理论的基本思想偏重于人类的经验及对问题的特性的掌握程度，也就是将传统数学从二值逻辑扩展到连续多值，利用隶属度函数描

述一个概念特性值。

模糊综合评判[7]的基本思想是利用模糊线性变换原理和最大隶属度原则，考虑与被评判事物相关的各个因素，对其做出合理的综合评价。其数学模型可分为一级或多级，一级评判的步骤如下: 1) 建立事物的因素集和评价集; 2) 确定因素的隶属函数，构成评判矩阵; 3) 确定因素的重要程度矩阵; 4) 进行模糊矩阵的复合运算，得到评价结果。而多极评判是将因素集中的元素按属性分成几类，先对每一类作综合评判，然后对评判结果进行类元素的高层次综合评判。

3.2 贝叶斯网络

贝叶斯网络[8]是指基于概率分析、图论的一种不确定性知识的表达和推理的模型。在概率分配已知的情况下，贝叶斯网络可以对不确定性进行定性和定量的表示，因此可以将系统建模为一个赋值的复杂因果关系网络图。

贝叶斯网络模型描述随机变量间概率依赖关系，表示为二元组B=(G，P)，网络包括两部分:

1) 具有N个节点的有向无环图G (Directed Acyclic Graph)。图中节点代表随机变量，节点间的弧代表相互关联关系(节点间的概率依赖);

2) 节点相关的条件概率表P (Conditional Probabilities Table)。条件概率表可以用$P(V_i \mid Pa(V_i))$来表示，用来表示节点V_i与父节点$Pa(V_i)$之间的条件概率，对没有父节点的节点，直接使用其先验概率。

创建贝叶斯网络的步骤如下: 1) 确定节点内容和节点关系; 2) 分配条件概率和选择推理算法; 3) 创建贝叶斯网络; 4) 输入推理证据，产生推理结果。

3.3 基于模糊贝叶斯网络的威胁评估模型

模糊逻辑在知识表示上优于贝叶斯网络，而贝叶斯网络在推理能力上又优于模糊逻辑。结合模糊逻辑和贝叶斯网络在知识表示和推理上的优点，我们引入模糊概率转换公式。

设$U=\{u_1,u_2,\cdots,u_n\}$是一个离散有限集合，X是取自U中的一个变量，$p(u_i)$表示$X=u_i$时的概率，$\pi(u_i)$表示$X=u_i$时的可能性，$\mu_A(u)$是模糊集合A上的隶属度函数。

Zadeh 认为，可能性理论是模糊集理论的扩展，因此可能性理论中可能性分配π可以由模糊集上的隶属函数决定。于是得到

$$\pi_\chi(u)=\mu_A(u) \tag{1}$$

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 preserving transformation),即信息中的不确定性在一种两种理论的相互转换过程中应保持不变。他们提出的转换公式[9]

$$p(u_i)=\frac{\pi(u_i)^{1/\alpha}}{\sum_{k=1}^{n}\pi(u_k)^{1/\alpha}} \qquad 0<\alpha<1 \tag{2}$$

其中常量α的取值范围为0<α<1，表示可能性概率转换一致性条件满足的程度。α趋向 0，则转换的概率$p(u_i)$间差异较大; α趋向 1，则$p(u_i)$间差异较小。

将式(1)，式(2)合并，得到

$$p(u_i)=\frac{\mu(u_i)^{1/\alpha}}{\sum_{k=1}^{n}\mu(u_k)^{1/\alpha}} \quad 0<\alpha<1 \tag{3}$$

运用式(3)，我们可以将模糊逻辑和贝叶斯网络的集成为模糊贝叶斯网络，于是得到了图 2 所示的威胁处理框图。

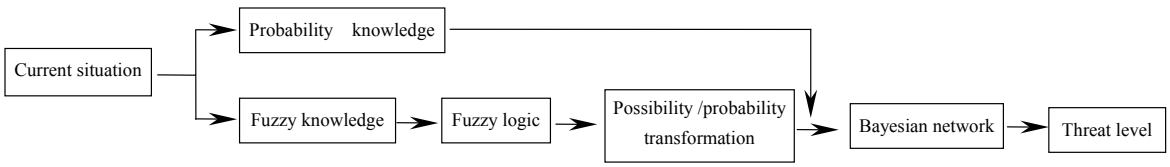

图 2　威胁评估流程图

Fig.2　Flow chart of threat assessment

4 实例计算

假设某武器系统的多个传感器探测到一批空中目标，选定一个目标后进行一段时间的跟踪和识别，获得目标的特性参数。将参数按模糊和概率两个域进行知识分类得到表 1。

表 1 目标参数表

Table 1 Target parameters

Factors	Fuzzy domain		Factors	Probability domain	
	Domain	Parameters		Domain	Parameters
Close point	[-30，+30]	-5	Type	[missile，bomber，miniplane，Unknown]	Bomber
Least time	[-600，+1 800]	250	Performance	[High，Medium，Low]	High
Velocity	> 0	320	Equipment state	[High，Medium，Low]	Medium
Altitude	[0 +30 000]	3 000	IFF	[Foe，Friend，neutral]	Foe
			Radar frequency	[On，Off]	On

4.1 动态威胁度的计算

在表 1 的模糊域中，使用模糊综合评判进行动态威胁度的计算。设因素集 U=(航路捷径 c，临界时间 t，速度 v，高度 h)，评语集为 V=(动态威胁度 D)。建立各个因素的隶属度函数如下所示:

$$\mu_1(c)=\exp(-5\times10^{-3}\times c^2)\quad -30\le c\le 30\quad ,\quad \mu_3(v)=1-\exp(-10^3\times v)\quad v>0\quad ,$$

$$\mu_2(t)=\begin{cases}\exp(-2\times10^{-6}\times t^2) & 0\le t\le 1\,800\\ \dfrac{1}{1-10^{-7}\times t^3} & -600\le t<0\end{cases},\quad \mu_4(h)=\begin{cases}1 & 0\le h\le 1\,000\\ \exp(-10^{-8}\times(h-1\,000)^2) & 1\,000<h\le 3\,000\end{cases}$$

将参数代入建立的隶属度函数可以得到评判矩阵 $\boldsymbol{R}$=[0.882 5　0.882 5　0.798 1　0.960 8]。利用专家给出威胁因素间相对权重矩阵 $\boldsymbol{A}$=[0.350 9　0.350 9　0.189 1　0.109 1]，使用加权平均运算，得到动态威胁度 $D=\boldsymbol{AR}$=0.875 1。

4.2 动态威胁度的概率形式转换

由于贝叶斯网络的输入使用概率的形式表示，所以将需要使用模糊概率转换理论对得到的动态威胁度进行概率转换。

首先动态威胁度分为三个等级(低，中，高)，我们建立动态威胁度与等级(低，中，高)的隶属度函数如图 3 所示。于是我们得到的动态威胁度(低，中，高)为(0.017 57，0.095 6，0.882 14)。利用上文提供的式(3)，

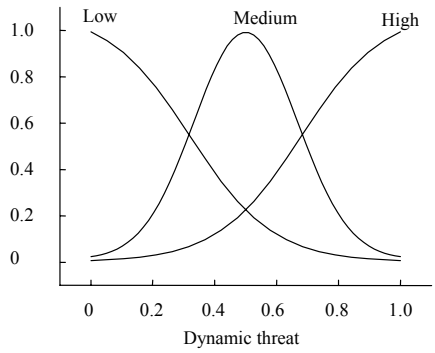

图 3 动态威胁度的隶属函数图

Fig.3 Membership function of dynamic threat degree

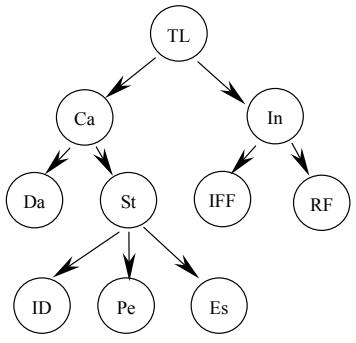

图 4 贝叶斯网络威胁模型

Fig.4 Threat model of Bayesian network

取 $\alpha=0.5$ 进行概率转换计算，得到威胁(低，中，高)的概率分别为(0.000 391 86,0.011 8,0.987 8)。

4.3 目标综合威胁的计算

经过上面的模糊概率转换，目标的所有信息全都用概率的形式表达。这样就可以利用贝叶斯对目标综合威胁进行计算。将目标的综合威胁(TL)分为能力威胁(Ca)和意图威胁(In)两部分，建立贝叶斯网络的一个威胁模型如图 4 所示。图中 Da 表示动态能力威胁，St 表示静态能力威胁，ID 表示目标类型，Pe 表示作战

性能，Es 表示战备等级，IFF 表示敌我识别，RF 表示雷达频率。

表 2　条件概率表

Table 2　Conditional probabilities

P(Ca/TL)	TL1	TL2	TL3		P(In/TL)	TL1	TL2	TL3		P(Da/Ca)	Ca1	Ca2	Ca3
Ca1	0.6	0.4	0.1		In1	0.6	0.4	0.1		Da1	0.6	0.4	0.1
Ca2	0.3	0.4	0.3		In2	0.3	0.4	0.3		Da2	0.3	0.4	0.3
Ca3	0.1	0.2	0.6		In3	0.1	0.2	0.6		Da3	0.1	0.2	0.6
P(St/Ca)	Ca1	Ca2	Ca3		P(RF/In)	In1	In2	In3		P(IFF/In)	In1	In2	In3
St1	0.6	0.4	0.1		RF1	0.8	0.5	0.3		IFF1	0.7	0.5	0.2
St2	0.3	0.4	0.3		RF2	0.2	0.5	0.7		IFF2	0.1	0.2	0.6
St3	0.1	0.2	0.6		P(ID/St)	St1	St2	St3		IFF3	0.2	0.3	0.2
P(Pe/St)	St1	St2	St3		ID1	0.5	0.1	0.0		P(Es/St)	St1	St2	St3
Pe1	0.6	0.4	0.1		ID2	0.3	0.4	0.15		Es1	0.6	0.4	0.1
Pe2	0.3	0.4	0.3		ID3	0.2	0.4	0.35		Es2	0.3	0.4	0.3
Pe3	0.1	0.2	0.6		ID4	0.0	0.1	0.5		Es3	0.1	0.2	0.6

我们设定先验概率 $\pi(\mathrm{TL})=(0.33,0.34,0.33)$，建立条件概率表 2。

选择连接树推理算法，计算得到最后威胁高中低的概率是(0.499 6，0.376 9，0.123 5）。将计算结果和事先先验概率进行对比可知，威胁高的概率增长最大，威胁中的概率稍有变化，威胁低的概率减小最大。评估结果表明，目标处于威胁程度高的概率最大，根据最大概率法可以评定目标的威胁程度为高。同理，运用模糊贝叶斯网络可以对同一时刻多个批次的目标进行威胁程度评定排序，为武器系统选择跟踪打击目标提供决策依据。

5　结　论

在武器指挥控制系统中，态势威胁估计为指挥员准确判断敌情，选择跟踪打击目标提供基本依据。针对传感器数据的不确定性，本文使用模糊贝叶斯网络，对模糊域和概率域数据进行处理融合处理，获得了目标的威胁等级。模糊贝叶斯网络方法符合人的思维推理，具有便于理解，数据表示力强、数据连续和时间累计等特性，因此具有一定的实用性。

参考文献：

[1] Hall D L，Llinas J. An Introduction to Multisensor Data Fusion [J]. **Proceedings of the IEEE**，1997，**18**(5)：145−153.

[2] Steinberg Alan N. Threat Assessment Technology Development [J]. **Lecture Notes in Computer Science**，2005，**3554**：490−500.

[3] QU Chang-wen，HE You. A method of threat assessment using multiple attribute decision making [J]. **Proceeding of the IEEE Signal Processing**，2002，**2**：1091−1095.

[4] 唐雪松，郭立红，陈长喜. 基于积因子方法的空中目标威胁排序研究 [J]. 光电工程，2006，**33**(11)：17−21，141.
TANG Xue-song，GUO Li-hong，CHEN Chang-xi. Threat sorting of air attack targets based on product factor method[J]. **Opto-Electronic Engineering**，2006，**33**(11)：17−21，141.

[5] 刘同明，夏祖勋，解洪成. 数据融合技术及其应用 [M]. 北京：国防工业出版社，1998.
LIU Tong-ming，XIA Zu-xun，XIE Hong-chen. **Data fusion technology and application** [M]. Beijing：National Defense Industry Press，1998.

[6] Jousselme A. Uncertainty in a situation analysis perspective [J]. **Proceedings of the International Society on Information Fusion Conference**，2003，**2**：1207−1214.

[7] 陈水利，李敬功，王向公. 模糊集合及其应用 [M]. 北京：科学出版社，2005.
CHEN Shui-li，LI Jing-gong，WANG Xiang-Gong. **Fuzzy set and application** [M]. Beijing：Science Press，2005.

[8] Jensen F. **An Introduction to Bayesian Networks** [M]. New York：Springer，1996.

[9] Koichi yamada. Probability-Possibility Transformation Based On Evidence Theory [J]. **Proceeding of the IEEE IFSA World Congress**，2001，**1**：70−75.