基于云贝叶斯网络的目标威胁评估方法

张银燕 李弼程 崔家玮
(解放军信息工程大学信息系统工程学院 郑州 450002)

摘 要 将云模型和贝叶斯网络相结合,形成云贝叶斯网络,并建立了基于云贝叶斯网络的威胁评估模型。首先,根据实际应用背景确定贝叶斯网络结构,并对连续型观测节点进行云模型转换;然后,将观测变量值输入云贝叶斯网络,推理得到目标属于各个威胁等级的概率;最后,为消除目标信息的不确定性对总的威胁度的影响,进行了多次重复推理,通过概率合成公式求得最终的威胁程度。以联合防空作战为背景,仿真实现了空中目标的威胁评估,验证了该方法的有效性。

关键词 威胁评估,云贝叶斯网络,云模型,贝叶斯网络,信息融合
中图法分类号 TP391 **文献标识码** A

Method of Target Threat Assessment Based on Cloudy Bayesian Network

ZHANG Yin-yan LI Bi-cheng CUI Jia-wei
(Information System Engineering Institute, PLA Information Engineering University, Zhengzhou 450002, China)

Abstract Cloudy bayesian network was proposed by combining cloud model and bayesian network, and a threat assessment model was built based on cloudy bayesian network. Firstly, the bayesian network structure was designed according to the background, and continuous observation node was transformed into cloud model. Secondly, the observation variable value was input to the cloudy bayesian network, reasoning out the probabilities of target which belongs to each threat level. Finally, repeat reasoning was made to eliminate the influence of target information uncertainty on the overall threat grade, and the final threat grade was obtained by probability-composing formula. The validity of the method was checked by simulation for aerial targets threat assessment against a background of joint air defense operations.

Keywords Threat assessment, Cloudy bayesian network, Cloud model, Bayesian network, Information fusion

1 引言

威胁评估是建立在目标状态与属性估计以及态势评估基础上的高层信息融合技术。在现代信息化战场,作战人员能够从各种先进的侦察设备和战场传感器获得敌方目标信息,由于获取的目标信息带有一定的不确定性(主要是模糊性和随机性),因此,如何对战场情报中这些不确定性目标信息进行分析处理,迅速、准确地判断出敌方的威胁程度,以适应高技术条件下现代战争对作战指挥"快节奏、高效率"的要求,是一项充满挑战的课题。

目前,国内外对威胁评估已经进行了许多探索性的研究,主要采用的理论、方法有:多属性决策、模糊逻辑方法、证据理论、粗糙集理论、贝叶斯网络、神经网络、支持向量机、直觉模糊推理、遗传算法等。这些方法各有所长,分别适应不同的情形,它们的有机结合,可以取长补短,提高处理的效率和有效性,满足一定场合的需求。在众多的组合方法中,模糊贝叶斯网络综合了模糊集的知识表达优势和贝叶斯网络灵活的推理能力,受到越来越多学者的青睐[1-3]。

云模型是一种定量数值与定性概念之间的不确定性转换模型,在知识表示方面,能够兼顾模糊性和随机性,从而很好地表达数据的不确定性以及专家知识,比模糊集理论更胜一筹。文献[4]将云模型运用于威胁评估,取得了很好的效果。为了充分发挥云模型和贝叶斯网络的优势,本文将云模型与贝叶斯网络有机地结合,形成云贝叶斯网络,进而提出一种基于云贝叶斯网络的威胁评估方法。

本文第2节给出云模型及贝叶斯网络的相关知识;第3节详细介绍基于云贝叶斯网络的威胁评估模型;第4节是实例仿真分析;最后对全文进行总结。

2 相关基础知识

本节介绍云模型和贝叶斯网络的基础知识,给出了云模型的定义、数字特征以及贝叶斯网络的主要思想。

2.1 云模型

定义 1[5] 设 U 是一个用精确数值表示的定量论域,C 是 U 上的定性概念。若定量值 $x\in U$,且 x 是定性概念 C 的一次随机实现,x 对 C 的确定度 $\mu(x)\in[0,1]$ 是具有稳定倾向性的随机数

$$\mu:U\to[0,1],\ \forall x\in U,x\to\mu(x)$$

到稿日期:2012-12-18 返修日期:2013-03-12 本文受国家863项目(2012AA7032030D),全军军事研究生课题(军事学YJS1062)资助。
张银燕(1986—),女,硕士生,主要研究方向为信息融合,E-mail:jessica718@126.com;李弼程(1970—),男,教授,博士生导师,主要研究方向为智能信息处理;崔家玮(1989—),男,硕士生,主要研究方向为信息融合。

则 x 在论域 U 上的分布称为云，每一个 x 称为一个云滴，表示为 $drop(x,\mu(x))$。

云是由云滴组成的，一个云滴是定性概念在数量上的一次实现，云滴越多越能反映该定性概念的整体特征。其中，云滴的确定度类似于模糊集合的隶属度，反映了模糊性，同时这个值自身也是个随机值，也可以用其概率分布函数描述。因此，云将模糊性和随机性有机地结合起来。

云可以用期望 Ex、熵 En、超熵 He 等 3 个数字特征来表征一个概念，用 $C(Ex,En,He)$ 表示。其中，期望 Ex 是云滴在论域空间上分布的期望，是该概念语言值量化的最典型样本。熵 En 为该定性概念语言值的不确定性度量，由该语言值的模糊性和随机性共同决定，表示在论域空间可以被定性概念接受的取值范围大小。超熵 He 为熵的不确定性度量，即熵的熵，由 En 的模糊性和随机性共同决定。

正态云是最重要的一种云模型，它具有普适性。图 1 分别示意了 $Ex=10, En=2, He=0.2$ 且云滴数为 1500 的半升正态云、正态云和半降正态云模型。

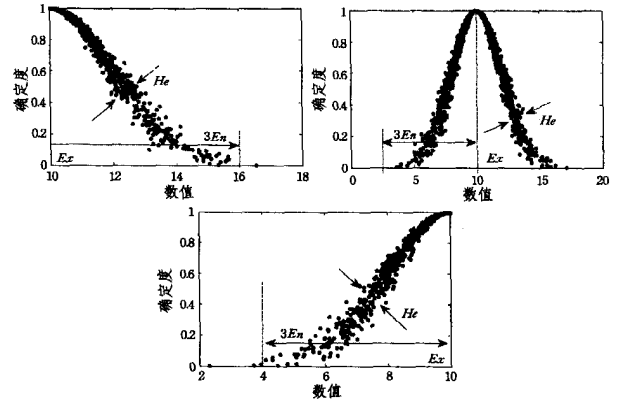

图 1　半升正态云、正态云和半降正态云模型

云的“厚度”反映了确定度的随机性的大小，靠近概念中心或远离概念中心处，确定度的随机性较小，而远离概念中心不近不远的位置确定度的随机性大，这与人的主观感受相一致。

在云模型中，定性概念与定量数值之间的转换是通过云发生器来实现的。云发生器分为正向云发生器和逆向云发生器，正向云发生器实现从定性概念到定量值的映射，相反地，逆向云发生器实现从定量值到定性概念的转换。本文方法中将用到正向正态云发生器中的 X 条件云发生器。以下是 X 条件云发生器的实现算法。

输入：定性概念 C 的数字特征(期望值 Ex，熵 En，超熵 He)及特定值 a。

输出：对应特定值 a 的云滴 a 及确定度 μ。

算法步骤：

(1)生成一个以 En 为期望值、He^2 为方差的正态随机数 $En'=NORM(En,He^2)$；

(2)计算特定值 a 的确定度 $\mu=e^{-\frac{(a-Ex)^2}{2(En')^2}}$；

(3)输出一个具有确定度 μ 的云滴 a。

由上述步骤可见，如果给定论域 U 中的一个特定点 a，通过 X 条件云发生器，可以生成这个特定点 a 属于概念 C 的确定度分布。

2.2　贝叶斯网络

贝叶斯网络一种基于概率分析和图论的不确定性知识表达和推理模型，模型采用网络描述事件和假想之间的相互关系，以条件概率描述节点之间的关联程度。

一般用符号 $B(G,P)$ 表示一个贝叶斯网络，G 是一个具有有限节点的有向无环图，有向边代表了节点之间的一种因果关系，这种关系用条件概率 P 表示。节点变量可以是任何问题的抽象，例如测试值、观测现象等。每一节点都附有与该变量相联系的条件概率分布函数，如果变量是离散的，则它表现为给定其父节点状态时该节点取不同值的条件概率表 CPT(根节点的条件概率用其先验概率表示)。贝叶斯网络规定，对于任意一个节点 V_i，在给定 V_i 的直接父节点的条件下，V_i 与任意除 V_i 及其后代节点以及直接父节点以外的其它节点条件独立。

贝叶斯网络推理是指利用贝叶斯网络的结构及其条件概率表，在给定证据后，计算某些节点取值的概率。贝叶斯网络的推理算法分为精确算法和近似算法两种，其中比较常见的有精确算法中的消息传递算法、联结树算法和近似算法中的基于搜索的方法。

在基于贝叶斯网络的威胁估计中，可以根据网络模型，从观测到的事件出发进行推理，得到威胁状态。

3　基于云贝叶斯网络的威胁评估模型

云贝叶斯网络由模糊贝叶斯网络启发而来，是对于一般离散贝叶斯网络和模糊贝叶斯网络的一种改进。云理论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云推理，因此云贝叶斯网络模型综合了云理论所具有的模糊性和随机性的知识表达能力以及贝叶斯网络所具有的推理能力，成为一种新的能够同时考虑模糊性、随机性的不确定性推理模型。在贝叶斯网络中，节点变量既可以是离散型，也可以是连续型，若以连续型变量作为离散型变量的父节点，将会造成条件概率难以确定[6]。为便于实现，本文先对网络中的连续型变量进行归一化处理，然后运用云模型转换对归一化变量进行离散化处理，使网络统一为离散型贝叶斯网络，同时，通过确定度-概率转换公式将确定度转换为概率，这就是云贝叶斯网络的基本思想。

本文建立基于云贝叶斯网络的目标威胁评估模型。首先，根据实际应用背景确定贝叶斯网络结构，通过云模型转换对连续型观测节点进行离散化处理，使网络统一为离散型贝叶斯网络，并依据客观知识和专家经验，确定各个节点的条件概率表；然后，将从探测设备获得的证据信息(观测变量值)输入云贝叶斯网络，选择合适的推理算法，通过贝叶斯网络推理获得目标威胁属于各个等级的概率；最后，为消除目标信息的不确定性对总的威胁度的影响，进行多次重复推理，通过概率合成公式求得最终的威胁程度。基本流程如图 2 所示。

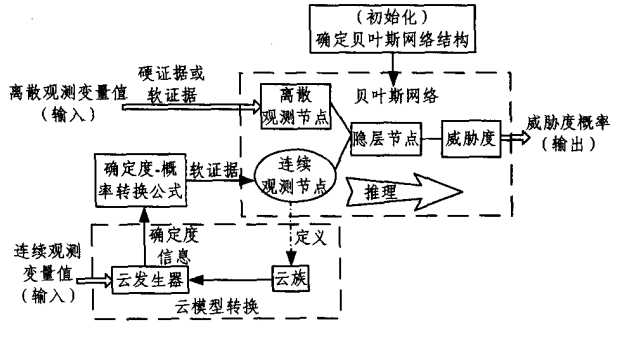

图 2　基于云贝叶斯网络的威胁评估模型

具体实现步骤如下：

Step1　根据实际应用背景，确定贝叶斯网络结构。

Step2　针对网络中的连续型节点，定义各节点的云族，并按照云族的特征和 X 条件云发生器实现算法设计云发生器。

Step3　依据客观知识和专家经验，确定各节点的条件概率表(CPT)。

Step4　从探测设备获得节点变量的取值。对连续型节点变量进行云模型转换，根据确定度-概率转换公式将确定度转换为概率作为节点的软证据(soft evidence)；对于离散型节点，若能给出确切的取值，则该取值可以作为节点的硬证据(hard evidence)，若仅能给出节点的可能分布概率，则此分布概率也以软证据的形式输入到贝叶斯网络。

Step5　选择合适的推理算法(如消息传递算法、联结树算法)，对贝叶斯网络进行推理，求得威胁度节点的概率。

Step6　重复 Step4、Step5 $f(f\geqslant 100)$ 次，并记录各次推理结果，通过概率合成公式，最终给出目标的威胁程度。

归纳起来，以上威胁评估方法的 6 个步骤中包括 3 项关键点：云模型转换技术、确定度-概率转换公式、概率合成公式。下面分别对 3 项关键点进行阐述。

3.1　云模型转换

所谓云模型转换，就是在连续型变量的归一化论域中定义一个云族，并根据云族的定义设计相应的一组云发生器，每个云发生器对应一个特定的定性概念。将归一化变量值输入到云发生器，输出得到变量值属于各定性概念的确定度。下面给出云族的定义。

定义 2　设 U 为贝叶斯网络中某连续型节点所对应的归一化论域，$U=[0,1]$，$D_1,D_2,\cdots,D_k$ 是论域 U 的一个划分，且满足如下 3 个条件：

(1) $\bigcup_{i=1}^{k} D_i=U$；(2) $\bigcap_{i=1}^{k} D_i=\varnothing$；(3) 对于 $\forall u_i\in D_i$，$\forall u_j\in D_j$，若 $i<j$，则 $u_i<u_j$。

$U_1,U_2,\cdots,U_k$ 为相对于该划分的定性语言值，用以表征该节点的离散状态。对于 $\forall u\in[0,1]$，若 u 对 $U_i(i=1,2,\cdots,k)$ 的确定度 $\mu_{U_i}(u)\in[0,1]$ 是具有稳定倾向的随机数，则 u 在 U_i 上的分布称为云(C_{U_i})，每一个 u 称为一个云滴，表示为 $drop(u,\mu_{U_i}(u))$，同时将 $C_{U_1},C_{U_2},\cdots,C_{U_k}$ 统称为云族。云的期望是最能代表定性概念的值，对应各区间的中心值，论域的划分情况及相应的云的数字特征如表 1 所列。

表 1　论域的划分情况及相应的云的数字特征

	U_1	$U_i,i=2,3,\cdots,k-1$	U_k
论域划分	$[0,\frac{1}{2(k-1)}]$	$[\frac{2(i-1)-1}{2(k-1)},\frac{2(i-1)+1}{2(k-1)}]$	$[\frac{2k-1}{2(k-1)},1]$
Ex	0	$\frac{i-1}{k-1}$	1
En	$\frac{1}{6(k-1)}$	$\frac{1}{6(k-1)}$	$\frac{1}{6(k-1)}$
He	$\frac{1}{60(k-1)}$	$\frac{1}{60(k-1)}$	$\frac{1}{60(k-1)}$

鉴于正态云的普适性，本文设计 C_{U_1} 为半降正态云，C_{U_k} 为半升正态云，$C_{U_2},C_{U_3},\cdots,C_{U_{k-1}}$ 为正态云。在实际应用中，可根据数据特点选择合适的云模型。由于正态分布是正态云在 $He=0$ 时的特例，在一个正态云中，$[Ex-3En,Ex+3En]$ 区间对云所表示的概念的贡献达到 99.74%(即所谓的“$3En$ 规则”)，这与正态分布的“3σ 原则”极为相似。因此，为较好地区分云族的各个云，保证各个云在相应论域的优势，云的熵 En 设定为论域宽度的 1/6，云的超熵 He 由熵的随机性和模糊性共同决定，根据经验[7,8]，$He=En/10$。

例如，论域 U 设计 3 个云，分别为 C_{U_1} (0,1/12,1/120)、C_{U_2} (1/2,1/12,1/120)、C_{U_3} (1,1/12,1/120)，分别表示为 U_1、U_2、U_3，如图 3 所示。

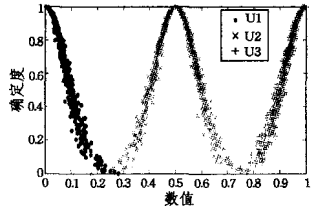

图 3　云族示意图

针对所定义的云族构建若干相应的 X 条件云发生器，如图 4 所示。

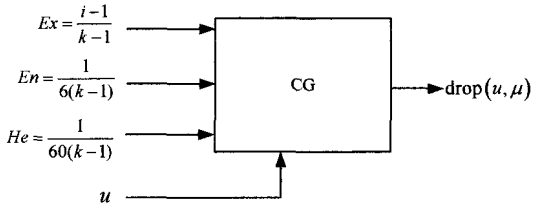

图 4　云发生器

由图 4 可知，输入归一化变量值 u，通过 X 条件云发生器可得到一个云滴 $drop(u,\mu)$，其中，μ 表示值 u 对 U_i 的确定度，从而实现了定性概念到定量数值的映射。

值得一提的是，本文所定义的云族中的云、定性概念以及云发生器三者是一一对应的。

3.2　确定度-概率转换公式

由于云所表征的定性概念与变量的离散状态对应，因此获得的对各个云的确定度就与变量的观测值属于各个状态的概率保持一致。由于确定度不具备概率所需的规范性，因此本文采用如下公式将确定度转换为概率：

$$P(u_i)=\frac{\mu(u_i)^{1/\alpha}}{\sum_{i=1}^{k}\mu(u_i)^{1/\alpha}} \tag{1}$$

其中，$0<\alpha\leqslant 1$，为常量，α 越大，确定度与概率的一致性越大，本文取 $\alpha=1$。

3.3　概率合成公式

为消除目标信息的不确定性对总的威胁评估值的影响，本文进行多次重复推理，通过概率合成公式，最终给出目标属于各威胁等级的概率。

假设将目标威胁分为 k 个等级：$W_1,W_2,\cdots,W_k$，经过 f 次重复推理，获得第 f 次的推理结果 $\boldsymbol{P}_f$：

$$\boldsymbol{P}_f=[P_f(W_1),P_f(W_2),\cdots,P_f(W_k)] \tag{2}$$

合成各次推理结果 $\boldsymbol{P}_1,\boldsymbol{P}_2,\cdots,\boldsymbol{P}_f$，得到目标属于各威胁等级的概率 $\boldsymbol{P}$：

$$\boldsymbol{P}=[P(W_1),P(W_2),\cdots,P(W_i),\cdots,P(W_k)] \tag{3}$$

其中，$P(W_i)=\dfrac{\sum_{n=1}^{f}P_n(W_i)}{\sum_{m=1}^{k}\sum_{n=1}^{f}P_n(W_m)}$，$i=1,2,\cdots,k$。

4　仿真分析

在现有的目标威胁评估方法中，以联合防空背景进行实例仿真的居多，本文在前人的研究基础上进行实验。

4.1 实验准备

文献[9]分析了联合防空作战中空天来袭目标影响威胁评估的主要因素，选取了目标类型、距离、空袭样式、速度、航向角、干扰能力、机载武器这7个因素作为空中目标威胁评估的属性，本文结合这些因素进行分析。Steinberg[10]认为威胁分析包括3个方面：能力(capability)、意图(intent)和机会(opportunity)，而机载武器和干扰能力体现了空中目标的作战性能，目标类型、空袭样式以及航向角在一定程度上表明了目标的攻击意图，速度和距离决定了目标到达被保卫物的时间，即目标造成威胁的机会性。因此构建了如图5所示的贝叶斯网络结构。

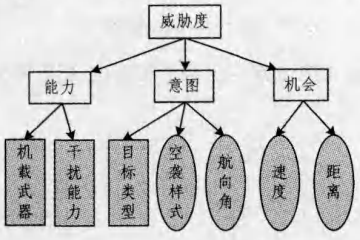

图5 空中目标威胁评估的贝叶斯网络结构图

图5中，用阴影标示的是观测节点，其中，离散型节点用方框标注，连续型节点用椭圆形标注。本文设计各节点变量的离散状态为3个或4个，在实际应用中，可根据需要增加变量的离散状态个数，以获取更大的精度。依据客观知识和专家经验，确定各节点的条件概率，如表2(a)－2(d)所列。

表2(a) 威胁度节点条件概率表

威胁度(W)	P(N/W)	P(Y/W)	P(J/W)
	能力N [强 中 弱]	意图Y [大 中 小]	机会J [大 中 小]
高(W_1)	[0.8 0.1 0.1]	[0.7 0.15 0.15]	[0.65 0.2 0.15]
中(W_2)	[0.1 0.8 0.1]	[0.15 0.7 0.15]	[0.1 0.8 0.1]
低(W_3)	[0.1 0.2 0.7]	[0.05 0.1 0.85]	[0.15 0.2 0.65]

表2(b) 能力节点条件概率表

能力(N)	P(Q/N)	P(F/N)
	机载武器Q [核弹 常规武器 其他]	干扰能力F [强 中 弱 无]
强(N_1)	[0.75 0.15 0.1]	[0.7 0.2 0.1 0]
中(N_2)	[0.15 0.7 0.15]	[0.2 0.4 0.3 0.1]
弱(N_3)	[0.1 0.15 0.75]	[0 0.1 0.4 0.5]

表2(c) 意图节点条件概率表

意图(Y)	P(T/Y)	P(H/Y)	P(B/Y)
	目标类型T [小型 大型 其他]	空袭样式H [低空 中空 高空]	航向角B [临近 侧翼临近 背离]
大(Y_1)	[0.8 0.15 0.05]	[0.7 0.2 0.1]	[0.8 0.15 0.05]
中(Y_2)	[0.2 0.7 0.1]	[0.2 0.6 0.2]	[0.15 0.7 0.15]
小(Y_3)	[0.1 0.1 0.8]	[0.1 0.2 0.7]	[0.1 0.2 0.7]

表2(d) 机会节点条件概率表

机会(J)	P(S/J)	P(R/J)
	速度S [高速 中速 低速]	距离R [近距 中距 远距]
强(J_1)	[0.6 0.3 0.1]	[0.7 0.2 0.1]
中(J_2)	[0.2 0.6 0.2]	[0.15 0.7 0.15]
弱(J_3)	[0.1 0.1 0.8]	[0.05 0.1 0.85]

运用基于云贝叶斯网络的目标威胁评估方法，既可对目标威胁的等级进行判断，也可实现对多批次目标的威胁排序。在计算出目标属于各威胁等级的概率值后，可按照如下规则[6]得到目标的威胁排序结果：

(1)根据目标威胁度属于“高”的概率进行排序，概率越大，目标的威胁越大。

(2)若目标威胁度属于“高”的概率相同，再依据目标属于“中”的概率大小进行排序，依此类推，直到明确所有目标的威胁度排序。

4.2 实例仿真——静态云贝叶斯网络

本文在MATLAB环境中，采用K. P. Murphy的BNT工具箱实现仿真。建立贝叶斯网络，进行初始化，设置好各节点条件概率表，选择联结树算法(BNT工具箱中的jtree_inf_engine引擎)作为推理算法。

假设在时刻1通过雷达等侦察设备探测到空中有6批目标，6批目标的观测值如表3所列。

表3 时刻1目标观测值

目标	机载武器	干扰能力	目标类型	空袭样式(m)	航向角	速度(m/s)	距离(km)
1	核弹	强	大型	22000	0°	300	100
2	常规	无	大型	6000	18°	500	360
3	核弹	中	小型	12000	6°	420	300
4	常规	弱	小型	8000	8°	800	280
5	常规	强	武直	300	6°	60	60
6	常规	中	武直	100	18°	40	120

将表3中的定性数据以硬证据的形式输入到云贝叶斯网络；对于定量数据，先采用文献[9]中的目标属性函数进行归一化处理，经过云模型转换和确定度-概率转换后，再以软证据的形式输入到云贝叶斯网络。因为预先没有任何情报信息，设定威胁度的先验概率为 $P^{(0)}=[P^{(0)}(W_1),P^{(0)}(W_2),P^{(0)}(W_3)]=[0.33,0.34,0.33]$。在主频3.1GHz、内存1G的台式机上进行云贝叶斯网络推理，10ms后，得到各目标威胁度分别属于高、中、低的概率，如表4所列。

表4 时刻1目标威胁度属于高、中、低的概率

	高	中	低
1	0.8405	0.1323	0.0272
2	0.0177	0.9330	0.0493
3	0.6584	0.3265	0.0151
4	0.3346	0.6271	0.0384
5	0.7179	0.1987	0.0834
6	0.1360	0.6142	0.2498

由表4可知，目标1、3、5的威胁等级为高，目标2、4、6的威胁等级为中。根据4.1节威胁度排序规则，6批目标的威胁度大小排序为：1、5、3、4、6、2。

在现有的目标威胁评估方法中，由于应用背景、属性选取、结果呈现形式的不同，不同方法之间很难进行合理的比较。文献[9]中6批目标的威胁度分别为：0.980、0.230、0.852、0.804、0.897、0.495，将其与本文方法的威胁评估结果进行比较，如图6所示。

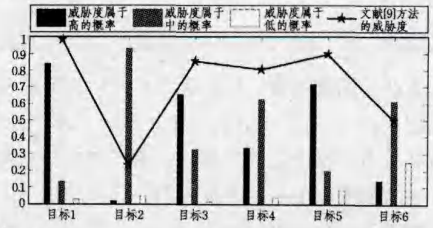

图6 本文方法与文献[9]方法的比较

由图6所知，采用本文基于云贝叶斯网络的威胁评估方

法，能正确、快速地给出目标的威胁程度，与采用文献[9]的自适应直觉模糊推理方法所得结论基本一致，符合专家经验判断。相对于自适应直觉模糊推理方法，本文方法无需训练样本，减少了计算量，具有很好的实用性能。

4.3 实例仿真——动态云贝叶斯网络

时刻2，6批目标的观测值发生了变化，如表5所列，其中，时刻2相对于时刻1有所变化的数据用加粗字体标示。

表5 时刻2目标观测值

目标	机载武器	干扰能力	目标类型	空袭样式(m)	航向角	速度(m/s)	距离(km)
1	核弹	强	大型	22000	0°	300	80
2	常规	无	大型	6000	18°	**300**	330
3	核弹	中	小型	**6000**	6°	420	280
4	常规	弱	小型	8000	**18°**	800	220
5	常规	强	武直	300	6°	**80**	58
6	常规	中	武直	**300**	**6°**	40	118

假定两个时间片的状态转移概率如表6所列。

表6 两个时间片的状态转移概率

转移概率	高	中	低
高	0.4	0.35	0.3
中	0.3	0.35	0.3
低	0.3	0.3	0.4

结合表4中时刻1的威胁度分别属于高、中、低的概率，求得时刻2各目标威胁度的先验概率，如表7所列。

表7 时刻2目标威胁度先验概率

先验概率	高	中	低
1	0.3841	0.3486	0.3027
2	0.3018	0.3475	0.3049
3	0.3658	0.3492	0.3015
4	0.3335	0.3481	0.3039
5	0.3718	0.3458	0.3083
6	0.3136	0.3375	0.3250

将时刻2新得到的证据信息输入到云贝叶斯网络，得到时刻2各目标的威胁度，如图7所示。

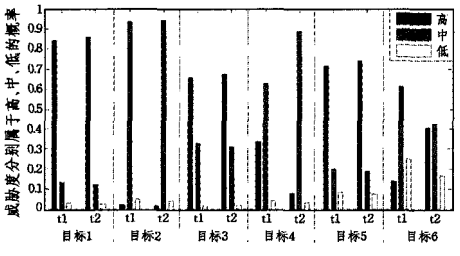

图7 时刻1(t1)和时刻2(t2)目标威胁度的比较

根据威胁度排序原则，6批目标的威胁大小排序更新为：1、5、3、6、4、2。

对比时刻1和时刻2各目标的威胁度，可得到如下结论：

(1)对于目标1，时刻1威胁度属于高的概率很大；时刻2，目标在速度基本保持不变的情况下，距离更近，因此威胁度属于高的概率相对于时刻1进一步增大，目标威胁程度有增大的趋势。

(2)对于目标2，时刻1威胁度属于中的概率很大；时刻2，距离变小，但由于目标速度减小，威胁度属于高的概率略微减小、属于中的概率稍有增大，可见目标的威胁程度略微减小。

(3)对于目标3，时刻1威胁度属于高的概率较大；时刻2，目标高度大幅度减小，同时距离变小，因此目标威胁度属于高的概率升高，属于中、低的概率相应减小，目标的威胁程度增大。

(4)对于目标4，时刻1威胁度属于中的概率较大；时刻2，距离变小，但目标航向角由8°调整为18°，因此相对于时刻1，威胁度属于高的概率显著减小，属于中的概率显著增大，目标的威胁程度减小。

(5)对于目标5，时刻1威胁度属于高的概率较大；时刻2，目标的速度稍有增大，并且目标距离更近，因此目标威胁度属于高的概率增大，目标的威胁程度增大。

(6)对于目标6，时刻1威胁度属于中的概率较大；时刻2，目标高度有所增大，但航向角明显减小且距离更近，因此目标威胁度属于高的概率增加，属于中、低的概率有所下降，目标的威胁程度相对时刻1明显增大。

由上述结论可见，运用动态云贝叶斯网络进行威胁评估，所得到的结果与实际情况完全相符，从而验证了本文方法的有效性。

结束语 针对目标信息具有不确定性的特点，本文研究了一种基于云贝叶斯网络的目标威胁评估方法。在云模型转换过程中充分考虑了目标观测数据的模糊性和随机性，经过多次重复性的贝叶斯网络推理，进一步消除了数据的不确定性对总的威胁度的影响，该方法具有很好的容错性和鲁棒性。以空中目标为例进行了仿真实验，仿真结果表明，运用本文的威胁评估方法，可以通过概率形式给出目标的威胁程度，既可对目标威胁的等级进行判断，也可对多批次目标进行威胁排序，不仅能实现目标的静态威胁评估，还能实现动态威胁估计。本文所提出的方法简单、有效，为目标威胁评估提供了新的思路。

参 考 文 献

[1] Chai Hui-min, Wang Bao-shu. A Hierarchical Situation Assessment Model Based on Fuzzy Bayesian Network[J]. Lecture Notes in Computer Science, Artificial Intelligence and Computational Intelligence, 2011, 7003: 444-454

[2] Liao Qin, Qiu Zhi-cong, Zeng Jie-peng. Fuzzy Bayesian Networks and Its Application in Pressure Equipment's Security Alerts[C]// Seventh International Conference on Natural Computation. 2011: 1507-1511

[3] Soheila A T, Mohammad R, Akbarzadeh T. Fuzzy-Bayesian network approach to genre-based recommender systems[C]// IEEE International Conference on Fuzzy Systems(FUZZ). 2010: 1-7

[4] 麻士东，韩亮，龚光洪. 基于云模型的目标威胁等级评估[J]. 北京航空航天大学学报，2010，36(2)：150-153

[5] 李德毅，杜鹢. 不确定性人工智能[M]. 北京：国防工业出版社，2005：143-158

[6] 孟光磊，龚光红. 基于混合贝叶斯网的空域目标威胁评估方法[J]. 系统工程与电子技术，2010，32(11)：2398-2401

[7] 王守信，张莉，王帅，等. 一种目标可满足性定性、定量表示与推理方法[J]. 软件学报，2011，22(4)：593-608

[8] 陈昊，李兵. 云推理方法及其在预测中的应用[J]. 计算机科学，2011，38(7)：209-211

[9] 雷英杰，王宝树，路艳丽. 基于自适应直觉模糊推理的威胁评估方法[J]. 电子与信息学报，2007，29(12)：2805-2809

[10] Steinberg A. Threat Assessment Technology Development[J]. Lecture Notes in Computer Science, 2005, 3554: 490-495