文章编号: 2095-6134(2015)02-0264-09

基于多模块贝叶斯网络的恐怖袭击威胁评估*

魏 静[1†], 王菊韵[2], 于 华[1]

(1 中国科学院大学工程管理与信息技术学院, 北京 100049; 2 中国传媒大学理学院, 北京 100024)

(2014 年 3 月 31 日收稿; 2014 年 5 月 7 日收修改稿)

Wei J, Wang J Y, Yu H. Terrorism threat assessment with multi-module Bayesian network [J]. Journal of University of Chinese Academy of Sciences, 2015, 32(2): 264-272.

摘 要 通过考察恐怖袭击事件可能造成的后果,针对恐怖袭击事件评估信息的多样性、不确定性及模糊性,提出用贝叶斯网络方法对恐怖袭击威胁进行评估,从而为反恐决策者提供决策支持,以减少恐怖袭击所造成的影响. 针对恐怖袭击事件的复杂性,提出多模块贝叶斯网络的恐怖袭击威胁评估模型,并对多模块贝叶斯网络的结构学习、参数学习和推理进行研究,提出多模块贝叶斯网络的推理算法. 最后,给出恐怖袭击威胁度的计算方法,并对多模块贝叶斯网络的威胁评估模型进行实例分析. 实例表明,基于多模块贝叶斯网络的恐怖袭击威胁评估模型,能有效评估恐怖袭击事件的威胁程度.

关键词 恐怖袭击; 威胁评估; 多模块; 贝叶斯网络; 推理

中图分类号: TP399 **文献标志码:** A **doi:** 10.7523/j.issn.2095-6134.2015.02.017

Terrorism threat assessment with multi-module Bayesian network

WEI Jing[1], WANG Juyun[2], YU Hua[1]

(1 *College of Engineering and Technology, University of Chinese Academy of Sciences, Beijing* 100049, *China*; 2 *College of Science, Communication University of China, Beijing* 100024, *China*)

Abstract This study intends to provide decision support for counter-terrorism according to the threat of terrorist attacks. Because of the diversity, uncertainty, and ambiguity of assessment information about terrorist attacks, Bayesian network is proposed to assess threat from the consequence of attacks. This study presents a multi-module Bayesian network threat assessment model for the complexity of the terrorist attacks, and this model combines the qualitative and quantitative assessment. We study the multi-module Bayesian network structure learning, parameter learning, and inference. Finally we compute the terrorism threat degree and conduct instance analysis. Simulation results show that this model effectively assesses the real threat degree of terrorist attacks.

Key words terrorist attacks; threat assessment; multi-module; Bayesian network; inference

* 国家重点基础研究发展计划(2011CB706900)、国家自然科学基金(70971128)和北京市自然科学基金(9102022)资助

† 通信作者, E-mail: weijingsx@163.com

20 世纪 90 年代以来,世界恐怖主义活动日益严重,以“9·11”事件为代表的一系列暴力恐怖事件的发生,不仅给世界各国人民的生命财产安全带来严重危害,而且造成了巨大的经济损失,已经成为影响世界稳定和地区安全的首要威胁. 如 2006 年发生在世界各地的恐怖事件高达 616 起,造成 2 320 人死亡,3 450 人受伤[1]. 近期发生在中国各地的恐怖袭击事件,严重影响了中国的社会治安,使民众陷于恐慌之中. 所以,必须采取有效措施,以减少恐怖袭击的发生.

恐怖袭击威胁评估作为反恐活动的重要组成部分,是对恐怖袭击进行有效预警、控制和处理的基础. 本文通过考察恐怖袭击事件可能造成的后果,对恐怖袭击威胁进行综合评估,从而为反恐决策者提供决策支持,以减少恐怖袭击造成的影响.

目前用于评估的方法很多,依据评估方法所用数据为定性和定量表达,可大致归为 3 类: 定性评估、定量评估、定性与定量相结合方法. 对于定性方法,由于太过于依赖评估人的主观判断,往往使评估结构出现错误; 定量评估方法虽然客观,但舍弃了那些无法量化的信息,可能导致评估结果不符合实际,与专家的经验和知识以及人们的直觉相悖. 所以本文用定性与定量相结合的方法,以克服以上 2 种方法的缺陷.

对于定性与定量相结合的评估方法,目前主要有层次分析法[2]、模糊综合评判法[3]、人工神经网络方法[4]和灰色综合评估方法[5]等. 但是这些方法都较难解决恐怖袭击威胁评估的本质问题: 结合专家知识进行基于不确定信息的推理. 作为一种知识表示和进行概率推理的框架,贝叶斯网络在具有内在不确定性的推理和决策问题中得到广泛的应用[6-8],能很好地表示变量之间的不确定性和相关性,并进行不确定性推理. Allanach 等[9-10]也曾指出贝叶斯网络是进行恐怖袭击信息整合的有效手段. 贝叶斯网络在战时威胁评估中得到了很好的应用,而此处的恐怖袭击与战争场景极为相似,都是在高度的不确定性和时间压力下,根据所获得包括干扰、欺骗等不完整、不准确的海量信息,迅速做出决策. 所以本文用贝叶斯网络进行恐怖袭击威胁评估. 近年来,该方法在战时态势决策、医疗诊断、故障诊断及不确定环境下多属性决策等[11-13]很多领域,都得到广泛应用.

本文提出用多模块的贝叶斯网络进行恐怖袭击威胁评估. 首先分析并阐述用于恐怖袭击威胁评估的多模块贝叶斯网络的结构学习和参数学习方法; 其次,分析并提出用于该多模块贝叶斯网络结构的推理算法; 最后,分析基于多模块贝叶斯网络的威胁评估模型在反恐中的应用,并进行了实例分析.

1　多模块贝叶斯网络的结构学习

利用贝叶斯网络进行恐怖袭击的威胁评估,首先必须学习贝叶斯网络的结构. 贝叶斯网络的结构学习是一个组合爆炸问题. 本节主要针对恐怖袭击的威胁评估,按照一定的原则和方法,构建一个合理的网络结构.

1.1　多模块贝叶斯网络的提出

贝叶斯网络的结构构建方法主要有样本训练学习的方法和根据节点变量之间的依赖关系人工构建的方法. 其中,前者适用于有充足样本数据的情况,后者适用于领域专家给定节点变量之间的条件依赖关系的情况. 对于恐怖袭击的威胁评估,由于其受多种因素的影响,构建贝叶斯网络非常复杂. 用贝叶斯网络进行战时态势评估时,也遇到了类似的问题,为了解决这一问题,Laskey 等[14-15]提出了贝叶斯网络片断的构建思想. 本文借鉴 Laskey 的网络片断思想,对恐怖袭击威胁评估的贝叶斯网络采用多模块的构建方法,即构建多个贝叶斯网络模块,然后由各模块共同组成完整的贝叶斯网络结构.

根据恐怖袭击可能造成的后果,本文将用于恐怖袭击威胁评估的贝叶斯网络分为 4 个模块,它们分别是恐怖袭击威胁评估的分级贝叶斯网络模块,以及 3 个后果子模块: 财产损失模块、人员伤亡模块和不良社会影响模块. 如图 1 所示,是恐怖袭击威胁评估的分级贝叶斯网络模块,其中的灰色节点称为置换节点,即该节点可以被相应的贝叶斯网络模块所置换.

其中,TL(threat level)表示威胁等级,PD(property damage)和 CeP(casualties except perpetrators)是恐怖主义活动造成财产损失和人员伤亡情况,其中人员伤亡中不包括肇事者,ASI(adverse social impacts)是恐怖主义活动造成的不良社会影响程度.

对于 3 个贝叶斯网络子模块: 财产损失模块、人员伤亡模块和不良社会影响模块,由于财产损

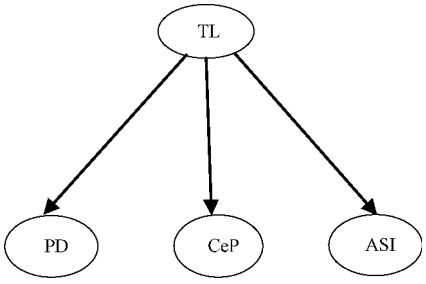

图 1 分级贝叶斯网络模块

Fig. 1 Hierarchical Bayesian network module

失模块和人员伤亡模块目前有一定量的样本数据,所以,该 2 个子模块,本文用样本学习的方法来构建. 对于不良社会影响模块,由于样本获取困难,所以,用人工的方法,根据专家知识来构建较为合理.

1.2 财产损失和人员伤亡模块贝叶斯网络的结构学习

财产损失和人员伤亡模块的构建方法类似,本文只对财产损失贝叶斯网络模块的构建进行详细的分析.

1.2.1 节点变量

财产损失贝叶斯网络模块中的节点,表示对财产损失评估有意义的情报信息或者经过情报机构的专业人员通过数据融合获得的信息. 比如,通过对恐怖组织网络的分析和研究来发现恐怖分子的可疑行动[9];用正规概念分析和时间概念分析等方法判断恐怖分析将在何时何地行动[10]等.

本文对 Joonghoon 提出的全球恐怖主义数据库(Global Terrorism Database,简称 GTD)中 1970—2011 年发生的恐怖袭击事件进行整理,具体的整理步骤如下.

第 1 步 提取确定是恐怖袭击事件的样本;

第 2 步 根据所能获得的情报信息提取所需属性;

第 3 步 将含有缺失数据的样本剔除;

第 4 步 合并属性: 因原数据集中恐怖袭击所致死亡人数和伤亡人数中包含了恐怖分子的死亡和伤亡人数,而本文评估的死伤人数不包含恐怖分子,所以用总的死伤人数分别减去恐怖分子死伤人数得到所需的死亡和伤亡人数;

第 5 步 部分属性离散化: 因学习贝叶斯网络结构需离散数据,本文根据《生产安全事故报告和调查处理条例》中的人员伤亡等级划分标准,对数据集中的死亡和伤亡人数属性进行离散,得到人员伤亡属性,具体的等级划分情况见下文;

第 6 步 因第 1 步和第 3 步的操作,使得数据集中某些属性的取值不连续,找到这些属性,并将它们的取值连续化. 例如: 财产损失的取值为 2,3,4,5,将其连续化后为 1,2,3,4.

经过以上整理,最后得到具有 3 143 条样本量的完整数据集,其中有财产损失 1 个类节点和 11 个属性节点,对应的节点编号、节点名称、节点大小和节点取值等信息如表 1 所示.

表 1 财产损失模块贝叶斯网络结构中的节点变量说明

Table 1 Node information in property damage Bayesian network module

node ID	node name	node size	node value
1	Property Damage	4	1 = None 2 = Minor (likely < $1 million) 3 = Major (likely > $1 million but < $1 billion) 4 = Catastrophic (likely > $1 billion)
2	Region	13	1 = North America 2 = Central America …… 13 = Australasia & Oceania
3	Country (Location)	88	1 = Afghanistan 2 = Albania …… 88 = Kosovo1
4	Criterion1: political, economic, religious, or social goal	2	1 = "Yes" (The incident meets Criterion 1) 2 = "NO" (The incident does not meet Criterion1 or there is no indication)

表 1(续)

node ID	node name	node size	node value
5	Criterion2: intention to coerce, intimidate or publicize to large audience(s)	2	1 = "Yes" (The incident meets Criterion 2) 2 = "NO" (The incident does not meet Criterion 2 or there is no indication)
6	Successful Attack?	3	1 = Yes, 2 = No, 3 = Unknown
7	Suicide Attack?	2	1 = Yes, 2 = No
8	Attack Type	9	1 = Assassination 2 = Armed assault …… 9 = Unknown
9	Target/Victim Type	22	1 = Business 2 = Government (General) …… 22 = Unknown
10	Number of Perpetrators	5	1 = 1 ≤ nperps < 10 2 = 10 ≤ nperps < 100 3 = 100 ≤ nperps < 500 4 = nperps ≥ 500 5 = Unknown
11	Weapon Type	10	1 = Chemical 2 = Radiological …… 10 = Unknown
12	Ransom Demanded?	3	1 = Yes, 2 = No, 3 = Unknown

1.2.2　结构学习及评估

用样本数据进行贝叶斯网络结构学习的方法,大致可分为 2 类: 一类是打分 - 搜索的方法,另一类是依赖分析的方法. 打分 - 搜索方法过程简单规范,适用于变量较少的稠密贝叶斯网络结构的学习; 依赖分析方法过程比较复杂,适合于建立多变量稀疏贝叶斯网络结构. 对于本文的财产损失贝叶斯网络模块,其节点变量较少,所以本文用打分 - 搜索方法中的 K2 算法来构建贝叶斯网络. 尽管这个算法在使用中具有众多优点,但是,这个算法需要指定结点的先验顺序[17]. 该节点顺序主要包括邻域知识或节点偏序指定的约束,例如: 父节点必须出现在其子节点的前面.

一般将定向后的最大权重跨度树的拓扑排序作为 K2 算法的初始节点序,但有向无环图的拓扑排序通常并不唯一. 为了确定唯一的初始节点序,我们首先基于定向后的最大权重跨度树对节点块排序,结点块的排序是唯一的,然后再采用局部完全有向无环图法对块内节点排序,最终得到所有节点的排序[18-19]. 用该方法对本文的财产损失子模块节点变量进行排序,排序结果为 [2,11,3,9,8,10,12,4,5,1,6,7]. 学习得到财产损失模块的贝叶斯网络结构如图 2 所示.

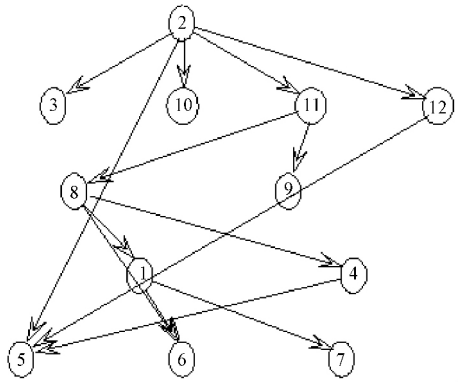

图 2　财产损失模块的贝叶斯网络结构

Fig. 2　Property damage Bayesian network module

同理,人员伤亡模块的贝叶斯网络结构如图 3 所示. 节点 1 表示人员伤亡情况,其他节点信息如表 1 所示.

本文用 10 折交叉有效性(10-fold cross-validation)验证方法,对财产损失模块贝叶斯网络的分类准确性进行评估,实验验证该模块对财产损失类节点的分类准确率分别高达 88.22%; 同

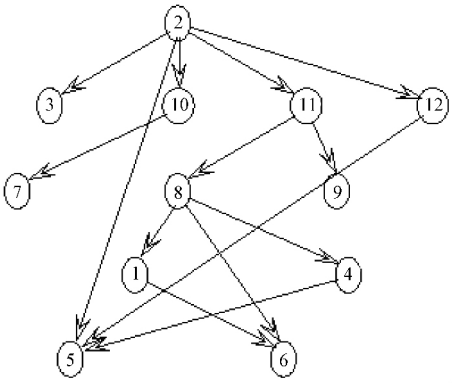

图 3 人员伤亡模块的贝叶斯网络结构

Fig. 3 Casualty Bayesian network module

理,得到人员伤亡模块贝叶斯网络的分类正确率为 70.03%. 由此可见,用贝叶斯网络对恐怖袭击可能造成的后果进行评估是可行有效的.

1.3 不良社会影响模块贝叶斯网络的结构

恐怖袭击事件不良社会影响的形成是一个连锁反应. 恐怖袭击事件产生恐怖效应,恐怖效应引发不良社会心理,不良社会心理导致不良社会影响; 而恐怖袭击事件之所以能引发恐怖效应,是由于恐怖袭击事件的高破坏性、隐蔽性、恐怖气氛的渲染性和袭击手段的残忍性[20]. 由此可知,恐怖袭击事件造成的不良社会影响跟恐怖袭击事件造成的人员伤亡、财产损失,恐怖主义活动发生前是否威胁、恐吓或向大众传播某种恐怖消息,以及民众或反恐决策人员对恐怖袭击的知情程度密切相关. 由此可以得到如图 4 所示的不良社会影响模块的贝叶斯网络结构.

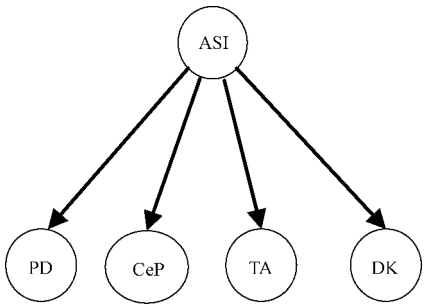

图 4 不良社会影响模块的贝叶斯网络结构

Fig. 4 Adverse social impact Bayesian network module

其中,ASI, PD 和 CeP 如图 1 中所示变量; TA (terrorist atmosphere) 是恐怖分子是否在恐怖活动前威胁、恐吓或向大众传播某种恐怖消息; DK (degree of knowledge) 是民众或决策人员对恐怖袭击的了解程度. PD 和 TA 变量的状态集合如表 1 所示,ASI,CeP 和 DK 变量的状态集合如下:

ASI = { Minimal, Minor, Major, Catastrophic }

CeP = { None,

Minimal ($1 \leqslant$ nkill < 3 or $1 \leqslant$ nwound < 10),

Minor ($3 \leqslant$ nkill < 10 or $10 \leqslant$ nwound < 50),

Major ($10 \leqslant$ nkill < 30 or $50 \leqslant$ nwound < 100),

Catastrophic (nkill $\geqslant 30$ or nwound $\geqslant 100$) }

DK = { Minimal, Minor, Major, Catastrophic }

其中,ASI 和 DK 变量的状态是专家对这 2 个变量的模糊评语; CeP 变量的状态集合是对 GTD 数据库中死亡人数、伤亡人数进行合并处理,并根据中国《生产安全事故报告和调查处理条例》中的人员伤亡等级划分对其离散化.

2 多模块贝叶斯网络的参数学习

贝叶斯网络的参数学习实质上就是在已知网络结构的条件下,学习每个节点的概率分布表. 对于本文所构建的多模块贝叶斯网络,其中财产损失模块和人员伤亡模块贝叶斯网络,由于存在观测数据,可以从数据中学习参数的概率分布表,但没有与分级贝叶斯网络和不良社会影响模块贝叶斯网络相关的观测数据,所以这 2 个贝叶斯网络模块的概率分布表采用专家知识来确定. 具体方法借鉴主观赋权法来确定.

主观赋权法是根据专家知识为各指标赋权,本文借鉴这一方法,用专家知识来确定贝叶斯网络的概率分布表. 设贝叶斯网络中某一节点 A,它有 n 个取值,每个取值的先验概率为 $p(a_i)$,且 $\sum_{i=1}^{n} p(a_i) = 1$,节点 A 有一取 m 个值的子节点 B, $\boldsymbol{p}(\mathrm{B}\mid\mathrm{A})$ 的条件概率矩阵为

$$\boldsymbol{P} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1m} \\ p_{21} & p_{22} & \cdots & p_{2m} \\ \vdots & \vdots & & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nm} \end{bmatrix}, \qquad (1)$$

其中, $\sum_{j=1}^{m} p_{ij} = 1, p_{ij} \geqslant 0, (i = 1,2,\cdots,n)$.

考虑多个专家 $\boldsymbol{PM}_k (k = 1,2,\cdots,q)$ 分别给出 $\boldsymbol{p}(\mathrm{B}\mid\mathrm{A})$ 的条件概率矩阵为

$$\boldsymbol{P}^k = \begin{bmatrix} p_{11}^k & p_{12}^k & \cdots & p_{1m}^k \\ p_{21}^k & p_{22}^k & \cdots & p_{2m}^k \\ \vdots & \vdots & & \vdots \\ p_{n1}^k & p_{n2}^k & \cdots & p_{nm}^k \end{bmatrix}, \quad (2)$$

$k = 1,2,\cdots,q$, 设每个专家的重要程度为 $\boldsymbol{h} = (h_1,h_2,\cdots,h_q)^{\mathrm{T}}$, 其中 $\sum_{k=1}^{q} h_k = 1$, 且 $h_k \geqslant 0$. 从主观赋权法的角度,为了确定各条件概率值,建立如下的优化模型:

$$\min L = \sum_{i=1}^{n} p(a_i) \sum_{k=1}^{q} \sum_{j=1}^{m} h_k (p_{ij} - p_{ij}^k)^2$$

$$\text{s.t.} \sum_{j=1}^{m} p_{ij} = 1 (i = 1,2,\cdots,n),$$

$$p_{ij} \geqslant 0 (i = 1,2,\cdots,n \text{ and } j = 1,2,\cdots,m). \quad (3)$$

模型(3) 的含义是找到一个条件概率矩阵,使条件概率 $p_{ij}(i = 1,\cdots,n, j = 1,\cdots,m)$ 与专家给出的条件概率 $p_{ij}^k(k = 1,\cdots,q, i = 1,\cdots,n, j = 1,\cdots,m)$ 之间的总偏差平方和最小.

$\partial L/\partial p_{ij} = 0$, 得

$$\sum_{k=1}^{q} h_k (p_{ij} - p_{ij}^k) = 0. \quad (4)$$

由公式(4) 可以得到条件概率的主观概率为

$$p_{ij} = \sum_{k=1}^{q} h_k p_{ij}^k (i = 1,\cdots,n, j = 1,\cdots,m). \quad (5)$$

那么,根据公式(5) 可以计算得到 $p(\mathrm{B}|\mathrm{A})$ 的条件概率矩阵. 同理,可以得到其他参数的条件概率矩阵.

3　多模块贝叶斯网络的推理算法

3.1　多模块贝叶斯网络推理算法的提出

贝叶斯网络推理是概率分布的计算过程,即寻求给定条件下事件发生的概率,也称为信念更新. 这里的信念指的是后验概率,简单地说,在给定模型中计算目标变量的后验概率就是贝叶斯网络推理. 根据本文的多模块贝叶斯网络,可以从观测到的事件出发,逐层推理,得到置换节点的状态,最后再由置换节点的状态推理得到恐怖袭击威胁等级.

对于贝叶斯网络的推理方法,目前可分为精确推理算法和近似推理算法 2 类. 精确推理算法主要有: 多树传播(polytree propagation) 推理算法[21-22]、联结树(junction tree propagation) 推理算法[23] 和基于组合优化的求解方法等. 近似推理算法主要有基于搜索方法和 Monte Carlo 算法等.

对于本文的贝叶斯网络,由于它是多模块集成的,不同模块的贝叶斯网络结构差异较大,所以针对不同的模块,选择不同的推理算法. 对于分级贝叶斯网络模块,贝叶斯网络中不含有 loop(不考虑弧方向的无向弧),本文采用 Pearl 提出的 polytree algorithm; 其他 3 个贝叶斯网络模块采用联结树推理算法.

3.2　多模块贝叶斯网络推理算法的步骤

根据已获得的关于恐怖袭击事件的证据信息 $[X_1,X_2,\cdots,X_n]$, 用联结树传播算法推理得到财产损失和人员伤亡的后验概率. 然后,根据这 2 个后验概率,用消息传递算法推理得到不良社会影响的后验概率. 最后,根据 3 个后果子模块得到的结果,用消息传递算法推理得到分级贝叶斯网络中恐怖袭击威胁等级的后验概率. 多模块贝叶斯网络的推理算法步骤具体如下.

输入　证据 $[X_1,X_2,\cdots,X_n]$, 多模块贝叶斯网络.

输出　根节点恐怖袭击威胁等级 TL 的置信度.

Step 1　根据部分证据 $[X_1,X_2,\cdots,X_i](i < n)$, 对人员伤亡和财产损失模块的贝叶斯网络,调用联结树传播算法计算得到财产损失节点 PD 和人员伤亡节点 CeP 的后验概率.

Step 2　用 PD 和 CeP 后验概率以及证据 $[X_j,\cdots,X_n](i < j \leqslant n)$, 对不良社会影响模块的贝叶斯网络调用联接树传播算法得到不良社会影响节点 ASI 的后验概率.

Step 3　对分级贝叶斯网络模块,确定根节点恐怖袭击威胁度 TL 的先验信息,并初始化根节点 TL 的置信度 Bel(TL), 令 $\mathrm{Bel}(\mathrm{TL}) = \pi(\mathrm{TL})$.

Step 4　对分级贝叶斯网络模块,若某一子节点 θ 的诊断信息发生变化,变化为 λ_θ, 则根节点 TL 的诊断信息变化为 $\lambda_{\mathrm{TL}} = \boldsymbol{M}_\theta \times \lambda_\theta$. 其中 $\boldsymbol{M}_\theta$ 为某一子节点关于根节点的条件概率矩阵.

Step 5　向上更新根节点 TL 的置信值,更新后根节点 TL 的置信度为 $\mathrm{Bel}(\mathrm{TL}) = \partial \times (\lambda_{\mathrm{TL}} \cdot \pi(\mathrm{TL}))$. 其中 "·" 为内积算子,$\partial$ 为归一化因子,其作用是使根节点 TL 不同状态的置信度的和为 1.

Step 6 向下更新子节点 θ 的置信度，更新后子节点 θ 的置信度为 $\mathrm{Bel}(\theta) = \partial \times \boldsymbol{M}_{\theta}^{\mathrm{T}} \times \mathrm{Bel}(\mathrm{TL})$.

Step 7 如果所有节点的后验概率与先验概率相等(If no change occurs)，则返回根节点 TL 的置信度，算法结束；否则，转第 4 步.

4 威胁评估模型的应用及分析

4.1 恐怖袭击威胁度的评估

根据已知的情报信息，用基于多模块贝叶斯网络的威胁评估模型从财产损失、人员伤亡、不良社会影响 3 个方面，对可能发生的恐怖袭击所面临的威胁进行评估，可以得到恐怖袭击威胁等级的后验概率. 如果简单地用贝叶斯网络的最大概率原则直接得到恐怖袭击的威胁等级，就会丢失其他等级的概率信息. 所以本文借鉴鞠彦兵和王爱华[24]计算突发事件影响度的方式来计算恐怖袭击的威胁度，具体的计算过程如下：

设 $Q = \{\mathrm{TL}_1, \cdots, \mathrm{TL}_n\}$ 为根节点 TL 的状态集合，其中 $\mathrm{TL}_i (i = 1, \cdots, n)$ 为决策者给出的关于恐怖袭击威胁等级的模糊评语. 例如，决策者关于某恐怖袭击事件给出的模糊评语可能是低(TL_1)、较低(TL_2)、较高(TL_3)、高(TL_4). $U(Q) = \{u(\mathrm{TL}_1), \cdots, u(\mathrm{TL}_n)\}$ 为决策者关于评语集中各状态的效用值集，$u(\mathrm{TL}_i)$ $(i = 1, \cdots, n)$ 为对应状态 TL_i 的模糊效用值，其取值范围为 $0 \leqslant u(\mathrm{TL}_i) \leqslant 1$. 对同一模糊评语集，不同的决策者给出的效用值可能是不同的.

由网络达到平衡状态时，根节点的后验概率和模糊效用值，可以计算得到恐怖袭击事件的威胁度，具体为

$$E(\mathrm{TL}) = \sum_{i=1}^{n} (u(\mathrm{TL}_i) \times \mathrm{Bel}(\mathrm{TL}_i)). \quad (6)$$

4.2 实例分析

对分级贝叶斯网络的根节点 TL 的模糊评语集为 $Q = \{$低(TL_1)，较低(TL_2)，较高(TL_3)、高(TL_4)$\}$，对应的模糊效用值集为 $U(Q) = \{0.25, 0.50, 0.75, 1.0\}$. 对于分级贝叶斯网络和不良社会影响模块的贝叶斯网络，由于没有样本数据，所以根据第 2 节中给出的方法，本实验中，我们聘请了 5 位专家，让他们分别给出这 2 个网络的条件概率矩阵. 此处专家给出的条件概率矩阵，反映的是恐怖袭击事件邻域专家知识对于网络中关联节点之间因果关系的看法，是一种专家知识. 取每位专家的重要程度是 $h = (1/5, 1/5, 1/5, 1/5, 1/5)$. 根据公式(5)得到分级贝叶斯网络和不良社会影响模块贝叶斯网络的条件概率矩阵分别见表 2 和表 3.

表 2 分级贝叶斯网络条件概率矩阵

Table 2 Conditional probability matrix of hierarchical Bayesian network module

threat	$\boldsymbol{p}(\mathrm{PD} \mid \mathrm{TL})$	$\boldsymbol{P}(\mathrm{C} \mid \mathrm{TL})$	$\boldsymbol{P}(\mathrm{ASI} \mid \mathrm{TL})$
level	none, minor, major, cata	none, min, minor, major, cata	min, minor, major, cata
min	0.50 0.44 0.05 0.01	0.65 0.25 0.06 0.03 0.01	0.80 0.15 0.04 0.01
minor	0.10 0.60 0.25 0.05	0.03 0.45 0.40 0.10 0.02	0.07 0.75 0.15 0.03
major	0.05 0.15 0.55 0.25	0.02 0.03 0.50 0.40 0.05	0.04 0.06 0.60 0.30
cata	0.02 0.08 0.25 0.65	0.01 0.02 0.03 0.29 0.65	0.01 0.09 0.15 0.85

注：min 是 minimal 的缩写，表示低，cata 是 catastrophic 的缩写，表示高.

表 3 不良社会影响模块的贝叶斯网络条件概率矩阵

Table 3 Conditional probability matrix of adverse social impact Bayesian network module

ASI	$\boldsymbol{p}(\mathrm{PD} \mid \mathrm{ASI})$	$\boldsymbol{P}(\mathrm{C} \mid \mathrm{ASI})$	$\boldsymbol{P}(\mathrm{TA} \mid \mathrm{TL})$	$\boldsymbol{P}(\mathrm{DK} \mid \mathrm{ASI})$
	none, minor, major, cata	none, min, minor, major, cata	yes, no	min, minor, major, cata
min	0.55 0.40 0.07 0.03	0.60 0.30 0.06 0.03 0.01	0.10 0.90	0.01 0.02 0.07 0.90
minor	0.10 0.60 0.25 0.05	0.03 0.45 0.40 0.10 0.02	0.40 0.60	0.03 0.07 0.70 0.20
major	0.05 0.15 0.55 0.25	0.02 0.03 0.50 0.40 0.05	0.60 0.40	0.15 0.80 0.03 0.02
cata	0.01 0.04 0.25 0.70	0.01 0.02 0.05 0.22 0.70	0.90 0.10	0.92 0.05 0.02 0.01

注：min 是 minimal 的缩写，表示低，cata 是 catastrophic 的缩写，表示高.

对于某恐怖袭击事件，假设预先没有任何情报信息，设定该恐怖袭击事件的威胁级别的先验

信息为 $\pi(\mathrm{TL}) = (0.25, 0.25, 0.25, 0.25)$,这反映了预估计者由于信息匮乏导致对可能性的估计不充分,认为各种情况的可能均相近.

假设初期情报机构或情报人员分析得知,某一恐怖组织准备以政治、经济、宗教或社会为目的,在北美地区的美国采用非自杀方式制造一起恐怖事件,并且胁迫和恐吓大众,此时民众或反决策人员对该恐怖活动的情况了解很少,根据这些情报信息进行仿真得到如表 4 中第 1 组所示的评估结果. 经过一段时间,又得到新情报,恐怖分子可能以破坏基础设施为目的,采用纵火方式袭击某一公共场所,此时民众或反恐决策人员对该恐怖活动的情况了解较多,根据最新信息进行仿真得到如表 4 中第 2 组所示的评估结果. 需要指出的是此处的情报信息与 2005 年 12 月发生在美国新墨西哥州的恐怖事件极为相似. 另外,表 4 中第 3 组数据是在第 2 组的基础上假设恐怖分子以自杀式袭击方式得到的评估结果. 第 4 组数据是在第 2 组的基础上,假设民众或反恐决策人员对该恐怖活动的情况了解较少得到的评估结果.

由第 1 组数据可以看出,在拥有部分情报信息的情况下,本文的威胁评估模型也能对恐怖活动造成的威胁进行评估,评估得到如果该恐怖活动成功,造成财产损失和人员伤亡较小的概率较大; 第 2 组数据是在第 1 组数据的基础上得到了更充分的情报信息,由于得知恐怖分子主要是以破坏基础设施为目的,所以评估得到如果该恐怖活动成功,造成小于 1 million 的财产损失和不造成人员伤亡的概率较大,并且该评估结果和 2005 年 12 月发生在美国新墨西哥州的恐怖袭击造成的后果相一致. 由第 1 组数据和第 2 组数据看来,通过先验信息,采用多模块的贝叶斯网络,能够对恐怖主义活动的威胁度进行动态评估; 由第 2 组数据和第 3 组数据可以看出,自杀式袭击的恐怖活动比非自杀式恐怖活动带来的威胁要高; 由第 2 组数据和第 4 组数据可以看出,民众或反恐决策人员对恐怖主义活动的情况越了解,造成的不良社会影响就会越低.

表 4　仿真结果

Table 4　Simulation results

组号	λ	Bel	威胁度
1	λ_{PD} = [0.662 5　0.332 9　0.003 0　0.001 5] λ_{C} = [0.007 1　0.971 8　0.007 1　0.006 8　0.007 1] λ_{ASI} = [0.164 1　0.537 0　0.134 2　0.164 7]	[0.356 3　0.641 3　0.001 7　0.000 7]	0.411 7
2	λ_{PD} = [0.034 8　0.908 3　0.056 9　0.000 0] λ_{C} = [0.926 0　0.069 3　0.004 6　0.000 0　0.000 0] λ_{ASI} = [0.247 7　0.743 2　0.008 0　0.001 1]	[0.757 3　0.238 3　0.003 2　0.001 3]	0.312 1
3	λ_{PD} = [0.157 9　0.720 1　0.102 4　0.019 6] λ_{C} = [0.293 5　0.043 0　0.177 7　0.483 6　0.002 2] λ_{ASI} = [0.004 6　0.927 0　0.059 6　0.008 7]	[0.037 6　0.854 4　0.068 4　0.039 6]	0.527 5
4	λ_{PD} = [0.034 8　0.908 3　0.056 9　0.000 0] λ_{C} = [0.926 0　0.069 3　0.004 6　0.000 0　0.000 0] λ_{ASI} = [0.196 6　0.206 4　0.589 7　0.007 4]	[0.712 3　0.168 1　0.112 1　0.007 5]	0.353 7

5　结论及展望

本文通过考察恐怖袭击事件可能造成的后果,用贝叶斯网络方法对可能发生的恐怖袭击所面临的威胁进行评估. 针对恐怖袭击事件的复杂性,本文提出多模块贝叶斯网络方法,用该方法对恐怖袭击的威胁进行评估,并且给出了多模块贝叶斯网络的结构学习、参数学习方法和推理算法. 基于多模块贝叶斯网络的威胁评估模型,不但能够集成专家的经验和知识,还能利用不同阶段得到的情报信息,进行多个阶段的评估,时刻掌握恐怖袭击事件的发展态势. 实验结果显示,该方法能较准确地反映恐怖袭击事件带来的威胁. 该方法的应用将有利于提高恐怖袭击事件应急决策过程的智能化及决策的有效性.

参考文献

[1] 李健和,王存奎,梅建明,等. 当代恐怖主义的特征与发展趋势[J]. 中国人民公安大学学报: 社会科学版,2008(3):1-7.

[2] Geng R, Xu G. Application of AHP FSE method in the network course quality evaluation [J]. Procedia Engineering, 2011, 15: 4 136-4 141.

[3] Li H, Chen Z, Chen S. The study of evaluation of the quality of the accounting information based on the fuzzy-AHP model [J]. Advances in Services Science and Services Information Technology (Set), 2014, 52: 185.

[4] Pradhan B. An assessment of the use of an advanced neural network model with five different training strategies for the preparation of landslide susceptibility maps [J]. Journal of Data Science, 2011, 9(1): 65-81.

[5] 沈阳武,彭晓涛,施通勤,等. 基于最优组合权重的电能质量灰色综合评价方法[J]. 电力系统自动化,2012,36(10): 67-73.

[6] Baesens B, Verstraeten G, Van den Poel D, et al. Bayesian network classifiers for identifying the slope of the customer lifecycle of long-life customers [J]. European Journal of Operational Research, 2004, 156(2): 508-523.

[7] Liu K F R, Lu C F, Chen C W, et al. Applying Bayesian belief networks to health risk assessment [J]. Stochastic Environmental Research and Risk Assessment, 2012, 26(3): 451-465.

[8] Weber P, Medina-Oliva G, Simon C, et al. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas [J]. Engineering Applications of Artificial Intelligence, 2012, 25(4): 671-682.

[9] Allanach J, Tu H, Singh S, et al. Detecting, tracking, and counteracting terrorist networks via hidden Markov models [C] // Aerospace Conference, 2004, Proceedings, IEEE. IEEE, 2004: 5.

[10] Singh S, Allanach J, Tu H, et al. Stochastic Modeling of a Terrorist Event via the ASAM system [C] // Systems, Man and Cybernetics, 2004 IEEE International Conference on. IEEE, 2004, 6: 5 673-5 678.

[11] Su X, Bai P, Du F, et al. Application of Bayesian networks in situation assessment [M]. Intelligent Computing and Information Science, Springer Berlin Heidelberg, 2011: 643-648.

[12] Julia Flores M, Nicholson A E, Brunskill A, et al. Incorporating expert knowledge when learning Bayesian network structure: a medical case study [J]. Artificial Intelligence in Medicine, 2011, 53(3): 181-204.

[13] 叶跃祥,糜仲春,王宏宇,等. 基于贝叶斯网络的不确定环境下多属性决策方法[J]. 系统工程理论与实践,2007(4):107-113.

[14] Laskey K B, Mahoney S M, Wright E. Hypothesis management in situation-specific network construction [C] // Proceedings of the Seventeenth Conference on Uncertainty in Artificial Intelligence. Morgan Kaufmann Publishers Inc, 2001: 301-309.

[15] Mahoney S M, Laskey K B. Constructing situation specific belief networks [C] // Proceedings of the Fourteenth Conference on Uncertainty in Artificial Intelligence. Morgan Kaufmann Publishers Inc, 1998: 370-378.

[16] Elzinga P, Poelmans J, Viaene S, et al. Terrorist threat assessment with formal concept analysis [C] // Intelligence and Security Informatics (ISI), 2010 IEEE International Conference on. IEEE, 2010: 77-82.

[17] Cooper G F, Herskovits E. A Bayesian method for the induction of probabilistic networks from data [J]. Machine Learning, 1992, 9(4): 309-347.

[18] Bouckaert R R. Optimizing causal orderings for generating DAGs from data [C] // Proceedings of the Eighth International Conference on Uncertainty in Artificial Intelligence. Morgan Kaufmann Publishers Inc, 1992: 9-16.

[19] 王双成. 贝叶斯网络学习、推理与应用[M]. 上海: 立信会计出版社,2010.

[20] 赵晓风. 恐怖主义活动的社会心理危害及对策探讨[J]. 理论导刊,2009(11):48-50.

[21] Pearl J. Fusin, propagation, and structuring in belief networks [J]. Artificial Intelligence, 1986, 29: 241-288.

[22] de Campos C P, Cozman F G. Complexity of inferences in polytree-shaped semi-qualitative probabilistic networks [C] // AAAI Conference on Artificial Intelligence. 2013: 217-223.

[23] Lauritzen S L, Spiegelhalter D J. Local computations with probabilities on graphical structures and their application to expert systems [J]. Journal of Royal Statistical Society, 1988, 50(2): 157-224.

[24] 鞠彦兵,王爱华. 基于贝叶斯网络的突发事件影响度研究[J]. 自然灾害学报,2011,20(5):40-46.