基于贝叶斯网络的复杂系统动态故障树定量分析方法

房丙午[1,2],黄志球[1],李 勇[1],王 勇[1]
(1. 南京航空航天大学计算机科学与技术学院,江苏南京 210016;2. 安徽财贸职业学院电子信息系,安徽合肥 230061)

摘 要: 动态故障树的贝叶斯网络分析方法存在局部组合爆炸和备件门节点失效时间仅能是指数分布的不足.首先,给出动态故障树转换为离散时间贝叶斯网络的方法,该方法使用一个确定性函数来替代条件概率表,避免了局部组合爆炸.然后,根据备件门的失效机理和对应的贝叶斯网络结构特征,解决了备件节点失效时间仅能是指数分布的限制.最后,提出一种基于动态故障树的贝叶斯网络精确推理算法,基于该算法给出了系统失效分布、组件重要度等概率计算.实验结果表明,该方法能有效地分析和评估安全攸关系统的概率特性.

关键词: 动态故障树;贝叶斯网络;定量分析;安全攸关系统
中图分类号: TP311 **文献标识码:** A **文章编号:** 0372-2112 (2016)05-1234-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.05.032

Quantitative Analysis Method of Dynamic Fault Tree of Complex System Using Bayesian Network

FANG Bing-wu[1,2], HUANG Zhi-qiu[1], LI Yong[1], WANG Yong[1]
(1. *College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu* 210016, *China*;
2. *Department of Electronics and Information, Anhui Vocational College of Finance and Trade, Hefei, Anhui* 230061, *China*)

Abstract: There exist limitations of local combinatorial explosion and only exponential distribution of spare nodes in Bayesian network(BN)-based dynamic fault tree(DFT) analysis method. First, an approach of mapping DFT into discrete-time BN is proposed in which a deterministic function instead of conditional probability tables is used to avoid local combinatorial explosion. Second, according to the failure mechanism and BN structure of spare door, we remove the limitation that the failure time of spare nodes in BN is only exponential distribution. Finally, an exact inference algorithm of DFT-based BN is presented and based on which the failure distribution of system and the importance measurement of components is calculated. Experimental results show that the proposed method can analyze and evaluate the probability characteristics of safety-critical systems effectively.

Key words: dynamic fault tree; Bayesian network; quantitative analysis; safety-critical system

1 引言

动态故障树(DFT)通过定义优先与门,备件门和功能依赖门等动态门来扩展故障树的建模能力,使其在具有时间相关性、功能相关性等复杂系统安全性分析领域获得广泛应用[1,2].DFT是半形式化模型,需要转换为数学模型进行分析[2],但是随着系统规模和复杂性的增长,DFT模型也越来越复杂,目前的分析方法存在状态空间爆炸和组件失效时间仅服从指数分布等缺点,难以适应大型复杂系统DFT分析需求.

DFT分析方法主要分为状态空间分析法[2~5],代数解析法[6~8],仿真方法[9,10]和贝叶斯网络分析法(BN)[11~19]四类.状态空间分析法存在状态空间爆炸和只能处理组件失效时间服从指数分布.代数解析法理论性强,无工具支撑,建模工作量大、易出错.仿真方法可以处理任意失效分布,但计算精度不高.BN分析法避免了全局状态空间爆炸,但存在条件概率表的参数组合爆炸和备件节点失效时间仅能是指数分布.针对上述不足,本文在离散时间BN(Discrete-Time BN, DTBN)分析法的基础上,提出针对大型复杂系统DFT分析方法:(1)给出一种DFT向DTBN转换方法.将非根节点CPD表示为父节点的一个确定性函数,避免条件概率表指数增长问题.(2)给出BN中备件节点CPD计算方法,克服了备件节点失效时间只能是指数分布的

收稿日期:2015-06-15;修回日期:2015-08-26;责任编辑:覃怀银
基金项目:国家自然科学基金(No.61272083, No.61562087);安徽省教育厅自然科学基金(No.KJ2013B009, No.KJ2015A400)

限制.(3)根据 DFT 转换的 BN 结构特征,提出一种基于 DFT 的 BN 推理算法. 实验结果表明,本文提出的方法计算效率和精度优于 DTBN 方法,能有效地避免条件概率表指数增长并能分析任意失效分布,满足大型复杂系统 DFT 分析需求.

2　DFT 向 BN 转换方法

DFT 逻辑门包括与门(AND)、或门(OR)和 K/M 选举门,动态门包括顺序增强门(Sequential Enforcing Gate,SEQ)、优先与门(Priority AND,PAND)、备件门(SPare,SP)和功能依赖门(Functional DEPendency gate,FDEP)[2,3]. K/M 选举门可由与门和或门组合表示[4],SEQ 可由备件门组合表示[11]. 本节给出 AND、OR、PAND、SP 和 FDEP 向 BN 转换. DFT 门表示、建模场景和失效机理参见相关文献[2,3].

2.1　DFT 门的 BN 结构表示

DFT 门对应的 BN 结构如图 1 所示,其中 $\boldsymbol{X}=(X_1,X_2,\cdots,X_m)$ 表示组件向量对应 BN 根节点集合,Y 表示(子)系统,对应 BN 的中间节点或叶节点. Y 的 CPD 表示 DFT 门的一种逻辑或时序关系,是父节点的一个确定性函数,如式(1)所示

$$P(Y\mid \mathrm{pa}_y)=\begin{cases}1, & Y=f(\mathrm{pa}_y)\\ 0, & \text{otherwise}\end{cases} \tag{1}$$

其中,pa_y 表示 Y 的父节点.

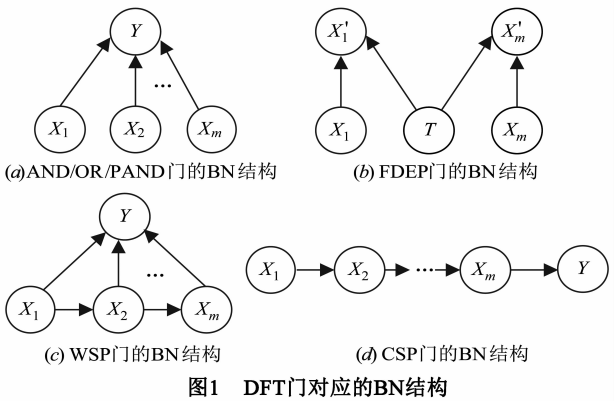


图1　DFT门对应的BN结构

为了表达动态门时序关系将 BN 节点 CPD 按失效时间离散化[12]. 整个时间 $[0,+\infty)$ 划分成 $n+1$ 个子区间,其中,任务时间区间 $[0,T]$ 被分成 n 个长度相等的子区间,每个子区间的长度为 $\Delta=T/n$,第 $n+1$ 个子区间是 (t,∞). 节点的状态由子区间 $(0,\Delta],(\Delta,2\Delta],\cdots,((n-1)\Delta,n\Delta],(n\Delta,+\infty)$ 来表示. 如果在任务时间 T 内,节点 X 在第 $i\in\{1,2,\cdots,n\}$ 个区间 $((i-1)\Delta,i\Delta]$ 内发生失效,记为 $X=i$. $X=n+1$ 表示 X 在 T 内未失效而是在 $[t,\infty)$ 内失效. 在整个时间 $[0,+\infty)$ 上,节点必然处在某一状态.

2.2　BN 中子系统节点参数表示

AND/OR/PAND 门对应的 BN 结构相同,如图 1(a)所示,但 Y 的 CPD 是不同的. 根据 AND 门失效机理,Y 状态是所有组件状态值的最大值,Y 的 CPD 由式(2)表示. 根据 OR 门失效机理,Y 状态是所有组件状态值的最小值,Y 的 CPD 由式(3)表示. PAND 门在 AND 门上增加组件失效时序约束,Y 的 CPD 由式(4)表示.

$$P(Y=l\mid \boldsymbol{X})=\begin{cases}1, & l=\max(X_1,X_2,\cdots,X_m)\\ 0, & \text{otherwise}\end{cases} \tag{2}$$

$$P(Y=l\mid \boldsymbol{X})=\begin{cases}1, & l=\min(X_1,X_2,\cdots,X_m)\\ 0, & \text{otherwise}\end{cases} \tag{3}$$

$$P(Y=l\mid \boldsymbol{X})=\begin{cases}1, & l=\max(X_1,X_2,\cdots,X_m)\ \text{and}\ (X_1\leqslant X_2\leqslant\cdots\leqslant X_m)\\ 0, & \text{otherwise}\end{cases} \tag{4}$$

FDEP 门对应的 BN 结构如图 1(b)所示,FDEP 门的组件要么由于自己失效,要么由触发事件触发强制失效,因此该门没有实际输出. X'_k 的 CPD 由式(5)表示.

$$P(X'_k=l\mid X_k,T)=\begin{cases}1, & l=\min(X_k,T)\\ 0, & \text{otherwise}\end{cases} \tag{5}$$

SP 门包括温备件门(WSP),冷备件门(CSP)和热备件门(HSP). WSP 和 CSP 门的 BN 结构如图 1(c)和(d)所示,X_1 为主件,$X_2,\cdots,X_m$ 为备件,HSP 门主件和备件同时处于工作状态,BN 结构和节点的 CPD 和 AND 门等价[14]. 根据 WSP 门失效机理,Y 的 CPD 和 AND 门 Y 的 CPD 相同由式(2)表示. CSP 对应的 BN 中一旦 X_m 失效,Y 立即失效,Y 的 CPD 由式(6)表示.

$$P(Y=l\mid X_m=j)=\begin{cases}1, & l=j\\ 0, & \text{otherwise}\end{cases} \tag{6}$$

2.3　BN 中备件节点 CPD 计算

在 SP 对应的 BN 中,备件节点失效行为受父节点的影响,目前的 BN 分析方法仅能处理节点失效时间服从指数分布[12-14],本节根据备件门失效机理和对应 BN 结构,将备件节点失效分布扩展为任意分布.

假设组件失效率为 $\lambda(t)$,作备件时,失效率由其工作状态决定,处于激活状态失效率为 $\lambda(t)$,处于备用状态失效率为 $\alpha\lambda(t)$(冷备件 $\alpha=0$,热备件 $\alpha=1$,温备件 $0<\alpha\lambda(t)<1$). X_{k-1} 和 X_k 是 SP 对应 BN 中的两个组件,X_{k-1} 是 X_k 父节点,失效时间分别为 t_k 和 t_{k-1}. 首先给出 WSP 对应 BN 备件节点的条件概率密度函数,分两种情况来讨论:

(1) $t_k\leqslant t_{k-1}$,X_k 在 X_{k-1} 之前或同时失效,也就是 X_k

在备用状态失效,X_k 失效不受 X_{k-1} 影响,条件概率密度函数如式(7)所示.

$$f_{X_k|X_{k-1}}(t_k \mid t_{k-1}) = f_{X_k}(t_k) = \alpha\lambda(t_k)\exp[-\int_0^{t_k}\alpha\lambda(\tau)\mathrm{d}\tau]$$
$$= \alpha\lambda(t_k)(\exp[-\int_0^{t_k}\lambda(\tau)\mathrm{d}\tau])^{\alpha} = \frac{\alpha f_{X_k}(t_k)}{R_{X_k}(t_k)}(R_{X_k}(t_k))^{\alpha}$$
$$= \alpha f_{X_k}(t_k)[1-F_{X_k}(t_k)]^{\alpha-1}, \quad t_k \leqslant t_{k-1} \tag{7}$$

(2)$t_k > t_{k-1}$,X_{k-1} 在 X_k 之前失效,由于 X_{k-1} 失效,使 X_k 进入工作状态,X_k 失效受 X_{k-1} 影响且 X_k 和 X_{k-1} 都在激活状态失效,条件概率密度函数如式(8)所示. X_k 的 CPD 分别由式(9)计算.

$$f_{X_k|X_{k-1}}(t_k \mid t_{k-1})$$
$$= \lambda(t_k)\exp[-(\int_0^{t_{k-1}}\alpha\lambda(\tau)\mathrm{d}\tau + \int_{k-1}^{t_k}\lambda(\tau)\mathrm{d}\tau)]$$
$$= \frac{f_{X_k}(t_k)}{R_{X_k}(t_k)}(R_{X_k}(t_{k-1}))^{\alpha}\frac{\exp[-\int_0^{t_k}\lambda(\tau)\mathrm{d}\tau])}{\exp[-\int_0^{t_{k-1}}\lambda(\tau)\mathrm{d}\tau]}$$
$$= \frac{f_{X_k}(t_k)}{R_{X_k}(t_k)}(R_{X_k}(t_{k-1}))^{\alpha}\frac{R_{X_k}(t_k)}{R_{X_k}(t_{k-1})}$$
$$= f_{X_k}(t_k)[1-F_{X_k}(t_{k-1})]^{\alpha-1}, \quad t_k > t_{k-1} \tag{8}$$

$$P(X_k = i \mid X_{k-1} = j) =$$
$$\begin{cases}\int_{(i-1)\Delta}^{i\Delta}\alpha f_{X_k}(t_k)[1-F_{X_k}(t_k)]^{\alpha-1}\mathrm{d}t_k \\ = [1-F_{X_k}((i-1)\Delta)]^{\alpha} - [1-F_{X_k}(i\Delta)]^{\alpha}, \quad i \leqslant j \\ \int_{(i-1)\Delta}^{i\Delta} f_{X_k}(t_k)[1-F_{X_k}(t_{k-1})]^{\alpha-1}\mathrm{d}t_k \\ = [1-F_{X_k}(j\Delta)]^{\alpha-1}[F_{X_k}(i\Delta) - F_{X_k}((i-1)\Delta)], \quad i > j\end{cases} \tag{9}$$

对于 CSP 门,$\alpha = 0$,X_k 不会在 X_{k-1} 之前失效,X_k 的 CPD 由式(10)计算,

$$P(X_k = i \mid X_{k-1} = j) =$$
$$\begin{cases}\int_{(i-1)\Delta}^{i\Delta} f_{X_k}(t_k)[1-F_{X_k}(t_{k-1})]^{-1}\mathrm{d}t_k \\ = [1-F_{X_k}(j\Delta)]^{-1}[F_{X_k}(i\Delta) - F_{X_k}((i-1)\Delta)], \quad i > j \\ 0, \quad \text{otherwise}\end{cases} \tag{10}$$

3 基于 DFT 的 BN 推理算法

DFT 转换的 BN 是典型的层次结构,失效行为传播方式是自底向上的,利用该特征来优化通用 BN 推理算法,以提高分析效率. 算法 1 通过 BN 中子系统节点来组织变量消元. 基本操作是 CPD 相乘和求和操作. 节点 CPD 是父节点的确定性函数,采用决策树存储 CPD[20]. 在算法 1 中,Φ 表示子系统的后验边缘分布,Ψ 表示节点 CPD,X_{ij} 和 Y_{ij} 分别表示第 i 层第 j 个组件和子系统,Z 和 C 分别表示 Y_{ij} 拥有的下层子系统和组件集合,P 表示 X_{ij} 父节点的集合.

算法 1 HBN4DFT(N,E,e)

输入: N——一个分层的 BN; E——表示证据变量的集合; e——是证据集合.

输出: $P(Y_{11}, E)$; Y_{11}——表示整个系统.

1: 在各节点的 CPD 中,将证据变量 E 的值设置为 e;
2: for($i = l$ to 1) //自底向上的推理.
3: 对第 i 层每个组件 X_{ik},如果父节点集合 P 不为空则计算
4: $\Psi(X_{ik}) = \Psi(X_{ik})\prod_{p\in P}\Psi(p)$
5: 对第 i 层每个子系统 Y_{ij},
6: 如果其子系统集合 Z 不为空,则计算
7: $f = \prod_{z\in Z}\Phi(z)$
8: 如果其组件集合 C 不为空,则计算
9: $g = \prod_{c\in C}\Psi(c)$
10: $\Phi(Y_{ij}) = \sum_{Z\cup C\setminus E} f.g.\ \Psi(Y_{ij})$
11: 将 $\Phi(Y_{ij})$ 存储在 Y_{ij} 节点处
12: end for

算法 1 效率分析,(1)时间复杂度用第 10 行函数来度量,该函数变量个数是 $|C|+|Z|+1$,假设 BN 中子系统结点个数为 m,组件个数为 k(一般 k 远大于 m),节点的状态数为 n,那么算法 1 时间复杂度为 $O(mn^{|C|+|Z|+1})$,而采用连接树推理算法[20]时间复杂度大于 $O((m+k)n^{|C|+|Z|+1})$. (2)存储空间方面,采用决策树存储 CPD,存储空间由 $O(mn^m)$ 降低为 $O(mn)$ 解决了局部存储空间爆炸问题(m 为某一节点的父节点数).

4 实验分析

根据 DFT 到 BN 转换方法,图 2 给出了心脏辅助系统(Cardiac Assist System, CAS) DFT 模型[12]等价的 BN 结构. BN 采用 SamIam 分析工具,CTMC 采用 Galieo DFT 分析工具,代数解析法(Algebraic Analysis, AA)采用 MATLAB 进行辅助计算. 实验平台配置为 CPU 型号为 Intel I5,主频为 2.6 GHz,内存为 4GB. 本文提出的方法记为 IDTBN,分别与 DTBN、CTMC 和 AA 进行比较.

4.1 性能分析

假设 CAS 各组件的失效时间服从指数分布,WSP 中 $\alpha = 0.5$,各组件失效率如表 1 所示.

表 1 CAS 系统各组件的失效率

序号	基本组件	失效率
1	CS/SS	0.2
2	P_CPU/ B_CPU	0.5
3	P_MOTOR	1.0
4	B_MOTOR	1.0
5	MOTOR_SW	0.01
6	PUMP_1/PUMP_2	1.0
7	B_PUMP	1.0

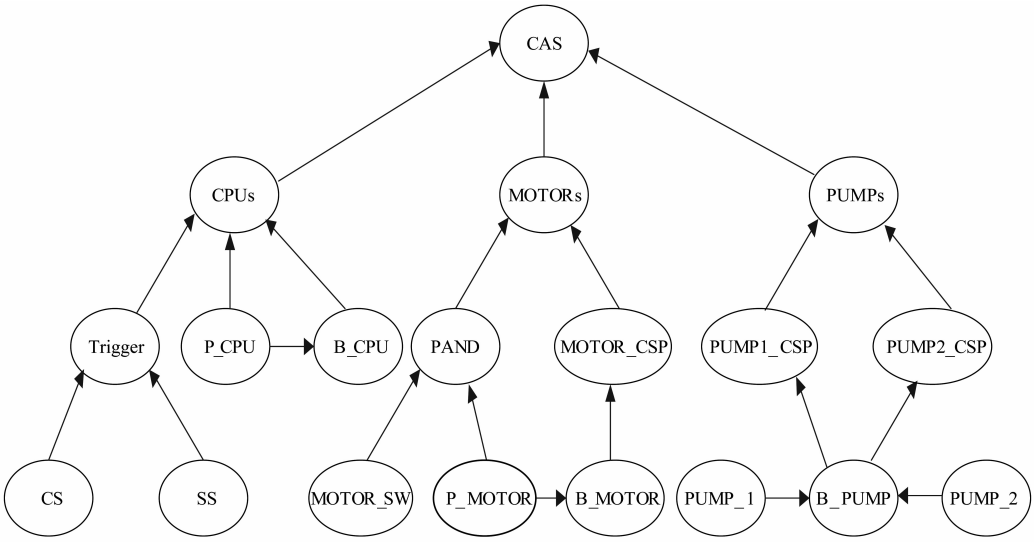


图2　CAS系统的BN模型

表 2 给出不同的离散时间粒度下 IDTBN 和 DTBN 的执行时间. 从表 2 可以看出,随着 n 的增大,IDTBN 时间性能明显优于 DTBN,当 $n=30$ 时计算时间相差两个数量级,IDTBN 时间性能基本满足系统实时分析的需求.

表 3 给出 $n=3$ 时,T 从 1h 到 10h,分别使用 CTMC、IDTBN 和 DTBN 计算的 CAS 失效概率.

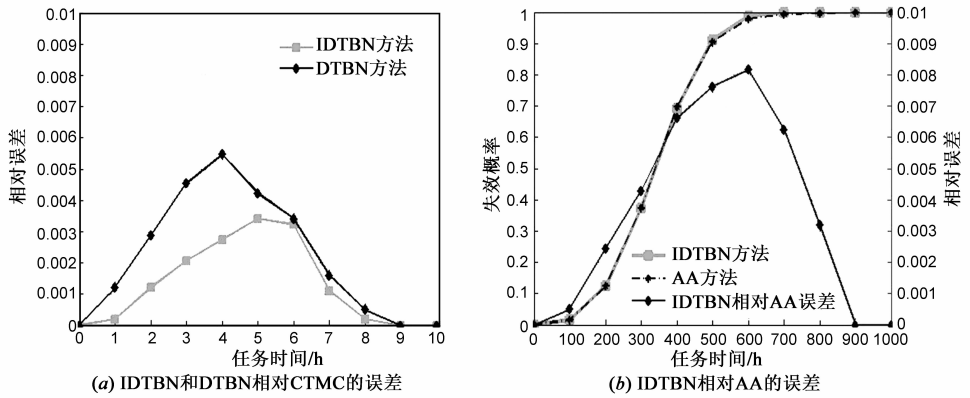
IDTBN 和 DTBN 计算结果相对 CTMC 的误差如图 3(a)所示,DTBN 最大相对误差为 5.47‰,算术平均误差是 2.29‰. 标准误差是 3.13‰;IDTBN 最大相对误差为 3.42‰,算术平均误差是 1.39‰. 标准误差是 1.92‰,从计算结果可以看出,IDTBN 计算精度要优于 DTBN.

表 2　IDTBN 和 DTBN 方法的执行时间

分析方法	执行时间(s)						
	$n=1$	$n=5$	$n=10$	$n=15$	$n=20$	$n=25$	$n=30$
DTBN	0.011	0.033	0.396	1.459	4.485	10.492	32.482
IDTBN	0.011	0.017	0.042	0.087	0.129	0.173	0.289

表 3　CTMCs 、IDTBN 和 DTBN 方法计算的系统失效概率

分析方法	系统失效概率									
	$T=1$	$T=2$	$T=3$	$T=4$	$T=5$	$T=6$	$T=7$	$T=8$	$T=9$	$T=10$
CTMC	0.6579	0.9075	0.9682	0.9863	0.9944	0.9959	0.9987	0.9998	1.0	1.0
DTBN	0.6571	0.9049	0.9638	0.9809	0.9902	0.9925	0.9971	0.9993	1.0	1.0
IDTBN	0.6579	0.9086	0.9702	0.9890	0.9976	0.9995	0.9998	1.0	1.0	1.0



(a) IDTBN和DTBN相对CTMC的误差　　(b) IDTBN相对AA的误差

图3　失效率计算及误差分析

选取 CPUs 子系统验证 IDTBN 处理失效时间服从任意分布的有效性,假设组件失效时间服从威布尔分布,尺度参数 $a=500$,形状参数 $b=3$,$T=1000$h,$n=3$. 图 3(b)分别给出了 IDTBN 与 AA 计算的 CPUs 子系统失效概率和相对误差,其中最大相对误差为 8.17‰,算术平均误差是 3.08‰. 标准误差是 4.52‰.

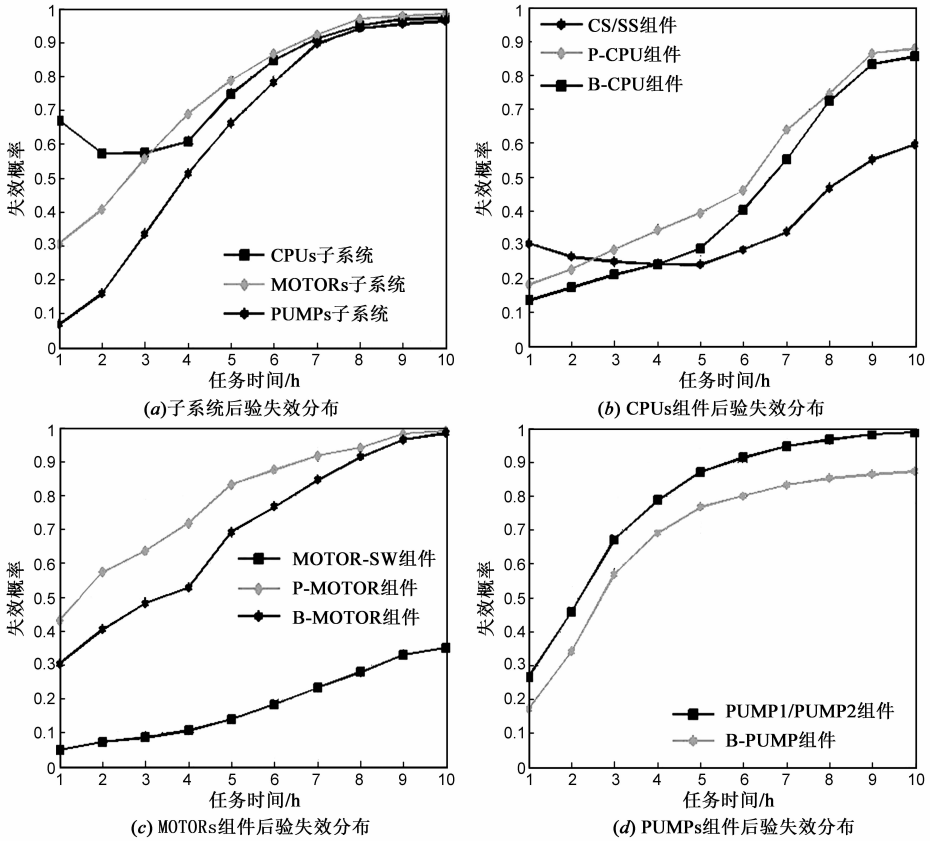
4.2 系统组件重要度及后验失效分布计算

在表 1 的参数设置下,$n=3$,$T=10$h,IDTBN 和 CTMC 的组件 Birnbaum 重要度计算结果如表 4 所示. 虽然结果存在一定的误差,但这并不影响组件重要度的定性.

和 CTMC 等其他方法相比,IDTBN 法能够在给定证据下进行后验概率查询. 当 CAS 系统失效时,IDTBN 计算的各子系统以及组件后验失效分布如图 4 所示.

表 4 组件 Birnbaum 重要度

序号	基本组件	Birnbaum 重要度	
		IDTBN	CTMC
1	CS/SS	0.3864	0.3792
2	P_CPU	0.1063	0.1103
3	B_CPU	0.1902	0.1867
4	P_MOTOR	0.1929	0.1906
5	B_MOTOR	0.4813	0.4769
6	MOTOR_SW	0.0699	0.0643
7	PUMP_1	0.0712	0.0698
8	PUMP_2	0.1299	0.1256
9	B_PUMP	0.0929	0.0899



(*a*)子系统后验失效分布 (*b*) CPUs组件后验失效分布

(*c*) MOTORs组件后验失效分布 (*d*) PUMPs组件后验失效分布

图4 子系统以及组件后验失效分布

5 总结

IDTBN 方法,克服了 BN 节点 CPD 组合爆炸缺点,消除了 BN 备件节点失效时间仅能是指数分布的限制,提高了分析效率和分析能力. 在实验中,将 IDTBN 和 DTBN,CTMC 等方法在时间性能、计算精度方法进行比较,然后利用该方法对系统失效分布和组件重要度等安全攸关系统概率特性计算,实验结果表明,IDTBN 方法的分析能力和效率优于现存的分析方法.

参考文献

[1] 黄志球,徐丙凤,阚双龙,等. 嵌入式机载软件安全性分析标准、方法及工具研究综述[J]. 软件学报,2014,25(2):200-218.
Huang ZQ, Xu BF, Kan SL, et al. Survey on embedded software safety analysis standards, methods and tools for airborne system[J]. Journal of Software, 2014, 25(2): 200-218. (in Chinese)

[2] JB Dugan, SJ Bavuso, MA Boyd. Dynamic fault-tree for

fault-tolerant computer systems[J]. IEEE Transactions on Reliability,1992,41(3):363 – 377.

[3] JB Dugan,KJ Sullivan,D Coppit. Developing a low cost high-quality software tool for dynamic fault-tree analysis[J]. IEEE Transactions on Reliability,2000,49(1):49 – 59.

[4] Liudong Xing, Morrissette BA, Dugan JB. Combinatorial reliability analysis of imperfect coverage systems subject to functional dependence[J]. IEEE Transactions on Reliability,2014,63(1):367 – 383.

[5] 徐丙凤,黄志球,胡军,等. 一种状态事件故障树的定量分析方法[J]. 电子学报,2013,41(8):1480 – 1486.
XU Bing-feng,HUANG Zhi-qiu,HU Jun,et al. A method for quantitative analysis of state/event fault tree[J]. Acta Electronica Sinica,2013,41(8):1480 – 1486. (in Chinese)

[6] G Merle,JM Roussel,JJ Lesage,et al. Probabilistic algebraic analysis of fault trees with priority dynamic gates and repeated events[J]. IEEE Transactions on Reliability,2010,59(1):250 – 261.

[7] Jun Ni, Wencheng Tang, Yan Xing. A simple algebra for fault tree analysis of static and dynamic systems[J]. IEEE Transactions on Reliability,2013,62(4):856 – 872.

[8] Daochuan Ge, Meng Lin, Yanhua Yang, et al. Quantitative analysis of dynamic fault trees using improved sequential binary decision diagrams[J]. Reliability Engineering and System Safety,2015,142(10):289 – 299.

[9] KD Rao,V Gopika,VVSS Rao,et al. Dynamic fault tree analysis using monte carlo simulation in probabilistic safety assessment[J]. Reliability Engineering and System Safety,2009,94(4):872 – 883.

[10] Peican Zhu, Jie Han, Leibo Liu, et al. A stochastic approach for the analysis of fault trees with priority and gates[J]. IEEE Transactions on Reliability,2014,63(2):480 – 495.

[11] Montani S,Portinale L,Bobbio A,et al. RADYBAN:a tool for reliability analysis of dynamic fault trees through conversion into dynamic Bayesian networks[J]. Reliability Engineering and System Safety,2008,93(7):922 – 932.

[12] Boudali H, Dugan JB. A discrete-time Bayesian network reliability modeling and analysis framework[J]. Reliability Engineering and System Safety, 2005, 87(3): 337 – 349.

[13] 周忠宝,周经伦,孙权. 基于离散时间贝叶斯网络的动态故障树分析方法[J]. 西安交通大学学报,2007,41(6):732 – 736.
Zhou Zhongbao, Zhou Jinglun, Sun Quan. Dynamic fault tree analysis based on dynamic Bayesian networks[J]. Journal of Xian Jiao Tong University,2007,41(6):732 – 736. (in Chinese)

[14] N Khakzad, F Khan, P Amyotte. Risk-based design of process systems using discrete-time Bayesian networks[J]. Reliability Engineering and System Safety, 2013, 109(1):5 – 17.

[15] Boudali H, Dugan JB. A continuous-time Bayesian network reliability modeling and analysis framework[J]. IEEE Transactions on Reliability,2006,55(1):86 – 97.

[16] Yan-Feng Li, Hong-Zhong Huang, Yu Liu, et al. A novel dynamic fault tree analysis method[A]. The Proceedings of 2013 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering[C]. Piscatawa:IEEE,2013. 81 – 84.

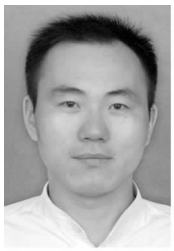
[17] Daniele Codetta-Raiteri, Luigi Portinale. Modeling and analysis of dependable systems through generalized continuous time Bayesian networks[A]. Reliability and Maintainability Symposium (RAMS), 2015 Annual[C]. Piscataway:IEEE,2015. 1 – 6.

[18] Xiaopeng Li, Nan Ao, Leilei Wu. The refining reliability modeling method for the satellite system[A]. The Proceedings of 2014 10th International Conference on Reliability Maintainability and Safety[C]. Piscataway: IEEE, 2014. 484 – 488.

[19] 王桢珍,姜欣,武小悦,等. 信息安全风险概率计算的贝叶斯网络模型[J]. 电子学报,2010,38(2A):18 – 22.
WANG Zhen-zhen, JIANG Xin, WU Xiao-yue, et al. Planning exploitation graph-Bayesian networks model for information security risk frequency measurement[J]. Acta Electronica Sinica,2010,38(2A):18 – 22. (in Chinese)

[20] Koller D, Friedman N. Probabilistic Graphical Models: Principles and Techniques [M]. Cambridge: MIT Press,2009.

作者简介



房丙午　男,1974 年生于安徽安庆. 现为南京航空航天大学计算机科学与技术学院博士研究生,副教授. 主要研究方向软件工程,软件系统安全性分析.
E-mail:bingwufang@163.com

黄志球(通信作者)　男,1965 年生于江苏南京. 现为南京航空航天大学教授,博士生导师,CCF 杰出会员. 主要研究方向为软件工程,形式化方法,软件分析与验证.
E-mail:zqhuang@nuaa.edu.cn