基于混合贝叶斯网络的混合系统安全性分析方法

房丙午[1,2],黄志球[1],王 勇[1],李 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 230601)

摘 要: 安全关键系统的安全性分析模型本质上是离散和连续失效分布共存的混合模型. 传统的故障树和马尔科夫链分析方法仅能处理离散分布或指数分布的系统,难以对混合系统进行安全性分析. 针对该问题,以 DFT 系统安全模型为基础,提出一种基于混合贝叶斯网络的混合系统安全性分析新方法. 首先,利用狄拉克函数和单位阶跃函数分别表示动态故障树节点间的确定性关系和时序关系,将动态故障树转换为贝叶斯网络. 然后,通过分段多项式来拟合网络节点的不同失效分布,提出一种 k 段 n 次多项式混合贝叶斯网络来表示动态故障树. 最后,给出该混合贝叶斯网络的推理算法. 实验分析表明本方法能有效地进行混合系统安全性分析.

关键词: 混合系统; 动态故障树; 混合贝叶斯网络; 安全性分析
中图分类号: TP311 **文献标识码:** A **文章编号:** 0372-2112 (2017)12-2896-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.12.010

A Novel Safety Analysis Method of Hybrid System on Hybrid Bayesian Network

FANG Bing-wu[1,2], HUANG Zhi-qiu[1], WANG Yong[1], LI 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* 230601, *China*)

Abstract: The safety analysis model of critical system is essentially a mixed model of both discrete variables and continuous variables. The traditional analysis methods can only deal with the system based on discrete distribution or exponential distribution, so these methods are incapable of analyzing the safety of the hybrid system. To solve the problem, this paper presents a novel safety analysis method of hybrid system on hybrid Bayesian network (HBN). First, by using the Dirac function and unit step function to represent the deterministic relation and timing sequence of nodes in DFT respectively, we convert the DFT into a Bayesian network (BN). Second, The HBN with k-piece and n-degree polynomials is proposed to represent the DFT, in which the different failure distributions of nodes are fitted by piecewise polynomial functions. Finally, the inference algorithm of HBN is proposed. The experimental results show that the presented method can effectively solve the safety analysis of hybrid system.

Key words: hybrid system; dynamic fault tree; hybrid Bayesian network; safety analysis

1 引言

在安全关键领域,故障树(FT)和动态故障树(DFT)具有直观、简洁和良好的描述能力已经成为系统安全性建模与分析的重要方法[1]. FT 是一个组合模型,通常使用二元决策图(BDD)进行分析,DFT 是一个状态空间模型,使用连续时间马尔可夫链(CTMC)进行分析. 但是这些分析方法存在一些重要的限制[2~4]:(1)状态空间爆炸,(2)仅能处理失效时间服从指数分布或离散分布的情况.

近年来,贝叶斯网络(BN)已经在系统可靠性建模与分析领域获得了广泛应用[5~7]. BN 拓展了 FT/DFT

收稿日期:2016-08-21;修回日期:2017-05-08;责任编辑:李勇锋
基金项目:国家 863 高技术研究发展计划(No. 2015AA015303);国家自然科学基金(No. 61272083, No. 61562087);安徽省高校自然科学基金重点项目(No. KJ2017A859);安徽省高校学科(专业)优秀拔尖人才学术资助计划(No. gxbjZD32)

的建模与分析能力,有效地缓解了状态空间爆炸并能进行混合系统分析. 通过 BN 分析 FT/DFT 模型的主要方法有离散时间贝叶斯网络(Discrete Time BN, DTBN)[8~12]、动态 BN(Dynamic BN, DBN)[13]和连续时间(Continuous Time BN, CTBN)[14~16]三种. 其中,DTBN 和 DBN 方法主要用来分析离散系统,对于混合系统虽然可以通过将连续失效分布离散化来分析,但只是粗略的近似,要获得较精确的解,需要很大的存储空间和计算代价. CTBN 方法主要用来分析连续系统,对于简单的失效分布可以获得精确的闭式解,对于较复杂的系统需要通过数值积分和蒙特卡洛仿真获得近似解,CTBN 方法本质上是一种代数解析法,缺少工具支撑,人工建模工作量大. 目前,对于连续和离散共存的混合系统安全性分析都是通过离散化将其转换为 DTBN 进行分析,然而,现代的安全关键系统(如航空电子系统)都是以软件为核心的,硬件、失效模式、环境和人为操作等关键要素相互依赖、相互作用的大型复杂混合系统,传统分析方法难以满足该类系统的安全性分析.

针对现有的研究还不能有效地解决混合系统安全性分析的需求,以 DFT 系统安全模型为基础,提出一种混合系统安全性分析新方法. 主要思想是将混合系统安全性分析问题约简到混合贝叶斯网络(Hybrid BN, HBN)的推理问题,利用 HBN 推理算法,可以对混合系统的失效分布、组件重要度和组件后验失效分布等安全攸关的系统概率特性进行计算. 方法的具体步骤如下:(1)在 HBN 中引入狄拉克函数和单位阶跃函数分别表示 DFT 节点间的确定性关系和时序关系,将 DFT 转换成 HBN;(2)使用基于切比雪夫点的 k 段 n 次多项式来拟合节点的失效概率分布,将 HBN 中的参数用 k 段 n 次多项式统一表示,从而将混合系统安全性分析问题规约到 k 段 n 次多项式 HBN 推理问题. (3)使用 k 段 n 次多项式 HBN 推理算法计算系统概率特性. 实验结果表明本文的方法和 DTBN 方法相比,具有更好的计算精度和效率.

2　DFT 向 HBN 转换方法

DFT 逻辑门包括与门(AND)、或门(OR)和 K/M 选举门,动态门包括优先与门(Priority AND, PAND)、备件门(Spare, SP)和功能依赖门(Functional Dependency Gate, FDEP). K/M 选举门可由 AND 和 OR 组合表示[3],FDEP 门可由 OR 来表示. 本文仅给出 AND、OR、PAND 和 SP 门向 HBN 转换方法. 为了能够表达 DFT 门节点间的确定性逻辑关系和时序关系,在 HBN 中引入了狄拉克函数和单位阶跃函数.

2.1　狄拉克和单位阶跃函数

狄拉克函数和单位阶跃函数定义域是$(-\infty,\infty)$,但在系统安全性建模和分析中,系统组件失效时间的定义域是$[0,\infty)$,所以下面给出两个函数的定义域也是$[0,\infty)$.

2.1.1　狄拉克函数

$$\delta(x)=\begin{cases}0, & x\neq 0\\ \infty, & x=0\end{cases},\text{并且}\int_0^{\infty}\delta(x)\,\mathrm{d}x=1$$

该函数可以看作均值为 0,方差为 σ^2 高斯分布在 $\sigma^2\to 0$ 时的极限,其矩生成函数在 $\sigma^2\to 0$ 时值为 1,所以可以将 $\delta(x)$ 在 $x=0$ 点的值看作概率 1.

2.1.2　单位阶跃函数

$$u(x)=\begin{cases}0, & x<0\\ 1, & x\geqslant 0\end{cases}$$

单位阶跃函数的导数是狄拉克函数,因此是一个几乎必然是零的随机变量的累积分布函数.

2.2　DFT 的 HBN 表示

DFT 向 HBN 转换可分为结构转换和参数转换两个步骤. 结构转换是利用 HBN 结构表达 DFT 门结构,DFT 到 HBN 的结构转换如图 1 和图 2 所示,图 1(a)、(b)和(c)分别是 DFT 的 AND、OR 和 PAND 门,它们对应 HBN 结构是相同的,如图 1(d)所示. DFT 备件门的 HBN 如图 2 所示,(a)表示 DFT 的备件门,(b)表示 WSP 门对应的 HBN 结构,(c)表示 CSP 门对应的 HBN 结构.

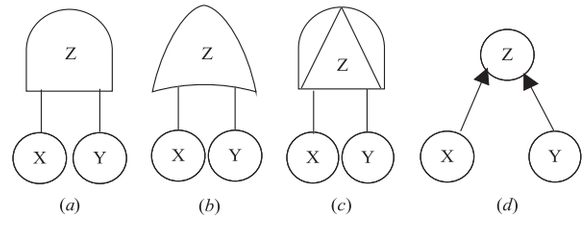


图1　DFT的AND,OR和PAND门对应的HBN结构

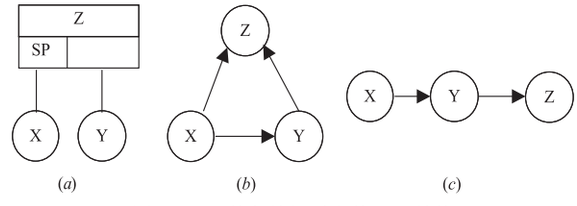


图2　DFT的备件门对应的HBN结构

下面分别给出 DFT 各种门的逻辑关系和时序关系的 HBN 参数表示方法.

2.2.1　AND 门的 HBN 参数表示

AND 门有两个以上的输入组件,输入组件是基本组件或是子系统. 所有输入组件失效,则 AND 门失效. 根据 AND 门失效机理,AND 门 Z 和输入组件 X,Y 的依赖关系如式(1)所示,

$$f_{Z|X,Y}(z|x,y)=u(x-y)\delta(z-x)+u(y-x)\delta(z-y)\tag{1}$$

其中 $u(x-y)\delta(z-x)$ 表示组件 X 在组件 Y 之后失效,Z 的失效取决于组件 X. $u(y-x)\delta(z-y)$ 表示组件 X 在组件 Y 之前失效,Z 的失效取决于组件 Y.

2.2.2 OR 门的 HBN 参数表示

OR 门有两个以上的输入组件,输入组件是基本组件或是子系统. 当输入组件至少有一个失效时,OR 门失效. 根据 OR 门失效机理,OR 门 Z 和输入组件 X,Y 的依赖关系如式(2)所示,

$$f_{Z|X,Y}(z|x,y)=u(x-y)\delta(z-y)+u(y-x)\delta(z-x) \tag{2}$$

其中 $u(x-y)\delta(z-y)$ 表示组件 X 在组件 Y 之后失效,Z 的失效取决于组件 Y. $u(y-x)\delta(z-x)$ 表示组件 X 在组件 Y 之前失效,Z 的失效取决于组件 X.

2.2.3 PAND 门的 HBN 参数表示

PAND 门有两个以上的输入组件,输入组件可以是基本组件或是子系统. 仅当组件按照从左至右的顺序或同时失效时,则 PAND 门失效,否则 PAND 门不会失效. 根据 PAND 门失效机理,PAND 门 Z 和输入组件 X,Y 的依赖关系如式(3)所示,

$$f_{Z|X,Y}(z|x,y)=u(y-x)\delta(z-y)+u(x-y)\delta(z-\infty) \tag{3}$$

其中 $u(y-x)\delta(z-y)$ 表示组件 X 在组件 Y 之前失效,Z 的失效取决于组件 Y. $u(x-y)\delta(z-\infty)$ 表示组件 Y 在组件 X 之前失效,此时 Z 不会失效.

2.2.4 SP 门的 HBN 参数表示

备件门所有输入组件都是基本组件,有一个主组件和多个备件. 当主组件失效时,它被第一个备件替换,当第一个备件失效时,它被下一备件替换,以此类推,直到主件和所有备件都失效,则备件门失效. 按照备件的备用模式不同,备件门可以分为冷备件门(CSP)、温备件门(WSP)和热备件门(HSP). 对于 HSP 门,备件和主件同时工作,两者失效行为是完全独立的,其失效机理和与门相同[2~4]. 对于 WSP 门,在系统工作过程中,组件 X,Y 非独立的,X 的工作状态影响 Y 的工作状态,因此在 HBN 的参数中要给出 Y 的条件概率. 假设组件失效率为 $\lambda(t)$, Y 的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 $0<\alpha<1$). Y 的条件失效率表示为 $\lambda(y|x)=u(x-y)\alpha\lambda(y)+u(y-x)\lambda(y)$,根据失效率和失效分布之间的关系,可以推导出 Y 的条件概率如式(4)所示[10],Z 的条件概率分布和 AND 门等价,由式(1)表示.

$$\begin{aligned}f_{Y|X}(y|x)=&u(x-y)\alpha f_Y(y)(1-F_Y(y))^{\alpha-1}\\&+u(y-x)f_Y(y-x)(1-F_Y(x))^{\alpha}\end{aligned} \tag{4}$$

对于 CSP 门,将 $\alpha=0$ 代入式(4),则 Y 的条件概率分布约简为式(5)所示. 由于当 Y 失效时,Z 就失效,Z 的条件概率分布如式(6)所示.

$$f_{Y|X}(y|x)=u(y-x)f_Y(y-x) \tag{5}$$

$$f_{Z|Y}(z|y)=\delta(z-y) \tag{6}$$

3 k 段 n 次多项式 HBN

在 DFT 转换的 HBN 中,节点的失效概率分布可能是指数分布、威布尔分布和泊松分布等,它们之间的乘法和边缘化运算都不是封闭的,因此无法在 HBN 中运行精确推理算法[17]. 通过 k 段 n 次多项式来拟合节点的失效分布函数,将 HBN 的参数统一表示成 k 段 n 次多项式. 由于多项式在求和、积分和相乘运算都是封闭的,因此在 BN 团树推理算法基础上可给出 HBN 推理算法.

3.1 k 段 n 次多项式的定义

定义 1 一维 k 段 n 次多项式函数 $\psi:\mathbb{R}\to\mathbb{R}$,具有如下形式:

$$\psi(x)=\begin{cases}\sum_{i=0}^{n}a_{ij}x^i, & x\in\Omega_j,j=1,\cdots,k\\ 0, & \text{otherwise}\end{cases}$$

,其中,$\Omega_1,\cdots,\Omega_k$ 是实数域$\mathbb{R}$上不相交的区间,a_{ij}是常数且 $a_{nj}\neq0$.

定义 2 $m(m>1)$维多项式函数 $f:\mathbb{R}^m\to\mathbb{R}$,具有如下形式:

$$\psi(x_1,x_2,\cdots,x_m)=\prod_{i=1}^{m}\psi(x_i),(x_1,x_2,\cdots,x_m)\in\Omega_X,$$

其中, $\Omega_X=\times_{i=1}^{m}\Omega_{x_i}$,$\psi(x_i)$由定义 1 表示.

3.2 k 段 n 次多项式插值算法

切比雪夫点多项式插值能最大限度地降低高次多项式插值龙格(Runge)现象并且插值多项式是失效分布函数的最佳一致逼近. 通过分段将失效分布函数划分为较小的区域,在每个区域内使用低次牛顿插值算法进一步克服龙格现象,提高函数拟合精度. 区间[a,b]内的切比雪夫点计算如式(7)所示.

$$x_j=\frac{1}{2}(a+b)+\frac{1}{2}(b-a)\cos\frac{2j-1}{2n}\pi,j=1,\cdots,n \tag{7}$$

k 段 n 次多项式的插值算法主要步骤如算法 1 所示,在段内采用牛顿插值法获得一个 n 次多项式,算法返回 k 个 n 次多项式的集合.

算法 1 **InterPoly($f(x)$,T,k,n)**

输入: $f(x)$,//组件 X 的失效分布;T,//任务时间;

输出: $\psi(x)$,//k 段 n 次多项式集合.

//将 T 划分 k 个相等的时间段

1: $t_i=[(i-1)T/k,iT/k]$,$i=1,2,\cdots k$;

2: For each t_i Do

3: 利用式(7)计算区间 t_i 内 n 个切比雪夫点;

4:　$\psi_i(x)=N_n(x)+R_n(x)$;//在区间 t_i 内牛顿插值
5:　将 $\psi_i(x)$ 增加 $\psi(x)$ 集合中;
6:End For;
7:return $\psi(x)$;

3.3　HBN 因子的运算

一个因子是定义在变量集 X 上的函数 $\phi:\Omega_X\to\mathbb{R}^+$,$\phi$ 是映射变量集 X 的每个实例到一个非负值的函数. 下面给出多项式因子乘法、因子边缘化和因子规范化等运算,在此基础上给出 HBN 推理算法.

3.3.1　因子乘法

设 ϕ_1 和 ϕ_2 是定义在变量集 X 和 Y 上的因子,两者的乘积是定义在 $Z=(X\cup Y)$ 上的一个因子:$(\phi_1\otimes\phi_2)(z)=\phi_1(x)\phi_2(y)$,$z\in\Omega_Z$. 离散因子的乘积是离散因子,连续因子和离散因子的乘积以及连续因子之间的乘积是连续因子. 分段多项式表示的因子其乘法满足交换律和结合律,因此,多个因子的乘法无需考虑计算顺序.

3.3.2　因子边缘化

因子的边缘化运算取决于被边缘化的变量是离散的还是连续的,离散变量的边缘化是因子求和运算,连续变量的边缘化是因子求积分运算.

首先考虑单个变量的边缘化运算,设 $\phi(Y,X)$ 是定义在变量集 $X\cup Y$ 上的因子,如果 Y 是离散变量则 Y 的边缘化如式(8)所示,如果 Y 是连续变量则 Y 的边缘化如式(9)所示.

$$\phi(Y,X)^{-Y}=\sum_{Y}\phi(Y,X) \tag{8}$$

$$\phi(Y,X)^{-Y}=\int^{\mathbf{R}}\phi(Y,X)\,\mathrm{d}Y \tag{9}$$

对于混合变量的边缘化运算,可设 $\phi(X)$ 定义在 $X=Y\cup Z$(其中 Y 是离散变量集合,Z 是连续变量集合)上的因子,$X'=Y'\cup Z'\subseteq X$,则对 X' 边缘化运算如式(10)所示,

$$\phi(X)^{-X'}=\sum_{y\in\Omega_{Y'}}\left(\int_{\Omega_{Z'}}\phi(y,z)\,\mathrm{d}z'\right) \tag{10}$$

容易证明,分段多项式因子的边缘化运算具有如下性质:

性质 1:$\sum_{y\in\Omega_{Y'}}\left(\int_{\Omega_{Z'}}\phi(y,z)\,\mathrm{d}z'\right)=\int_{\Omega_{Z'}}\sum_{y\in\Omega_{Y'}}\phi(y,z)\,\mathrm{d}z'$

性质 2:$\phi(X)^{-\{X_1,X_2\}}=(\phi(X)^{-X_1})^{X_2}=(\phi(X)^{-X_2})^{X_1}$,$X_1,X_2\in X$

性质 3:$(\phi(X_1)\otimes\phi(X_2))^{-X_1}=\phi(X_1)^{-X_1}\otimes\phi(X_2)$,$X_1\in X_1$,$X_1\notin X_2$

性质 1 表明边缘化运算的结果与积分、求和的运算顺序无关,性质 2 表明边缘化运算的结果与边缘化变量的先后顺序无关,性质 3 称为局部化运算. 这些性质能够简化 HBN 中推理运算的复杂性.

3.3.3　因子规范化

由于因子中并入证据,因子经过乘法、边缘化操作和消息传播后可能不是规范化的概率分布了,因此在团树中消息传播结束后需要规范化因子. 规范化运算是被规范化的因子除以规范化常数 $\phi(X)$ 规范化由式(11)表示,

$$\phi_{nor}(X)=\frac{\phi(X)}{\sum_{y\in\Omega_Y}\left(\int_{\Omega_Z}\phi(y,z)\,\mathrm{d}z\right)},X=Y\cup Z \tag{11}$$

3.4　HBN 团树推理算法

根据 HBN 的结构,使用团树构造算法生成相应的团树[18],令团树由团 $C_1\cdots$, C_k 组成的,其中节点 x 及父节点所在的团称为节点 x 的家族团,分割集 $S_{ij}=C_i\cap C_k$,HBN 中的每个因子都必须和一个团相关联. 算法 2 给出 HBN 团树推理算法.

算法 2　ClusTreeInfer(C_r,e)

输入:　C_r,//以 C_r 为根的团树;e //是证据集合;
输出:　Pr(C_r,e)
1:For each C_i Do
2:　$\phi(C_i)\leftarrow$将 C_i 所有因子相乘;
3:End For;
4:For each 在 e 中的变量 x Do
5:　找出变量 x 的家族团;
6:　$\phi(C_i)\leftarrow\phi(C_i)\delta(x-e_x)$;
7:End For;
8:While C_r 未收到所有相邻的团发来的信息 Do
9:　选择一个团 C_i,C_i 已经收到所有子节点团的信息;
10:　$\phi(C_i)\leftarrow\phi(C_i)\prod_{k\neq j}M_{ij}$;
11:　$M_{ij}\leftarrow\phi(C_i)^{-C_i\setminus S_{ij}}$;
12:End While;
13:return $\phi(C_r)\prod_k M_{kr}$;

在算法 2 中,语句 1 ~ 3 是初始化团树;语句 4 ~ 7 是将证据集 e 设置到相应的团中,其中 e_x 表示变量 x 的观测值;语句 8 ~ 12 从叶节点开始自底向上完成根团 C_r 的信息收集过程,其中 M_{ij} 表示团 C_i 到 C_j 之间传递的消息,语句 11 是根据集合 $C_r\setminus S_{ij}$ 中变量是离散的、连续的或混合的分别应用式(8)、(9)、(10)进行边缘化运算;语句 13 返回联合概率分布 $Pr(C_r,e)$,对该分布进行边缘化和规范化运算,即可得出系统或子系统失效分布和后验失效分布等. 算法 2 的时间复杂度为 $O(n*\exp(w))$,n 表示 HBN 中变量的数目,w 表示 HBN 的宽度. 至此,可以给出 k 段 n 次多项式 HBN 安全性分析主要步骤.

Step1:将 DFT 结构转换为 HBN 结构;

Step2:对所有组件的失效分布函数分别调用算法 1 获取 k 段 n 次多项式;

Step3:根据式(1)~(6)分别设置 AND 门、OR 门、PAND 门和 WSP 的条件概率分布;

Step4:根据 HBN 生成的团树,选择 HBN 中系统或子系统节点所在的团作为根团;

Step5:调用算法 2 进行系统概率特性计算.

4 实验分析

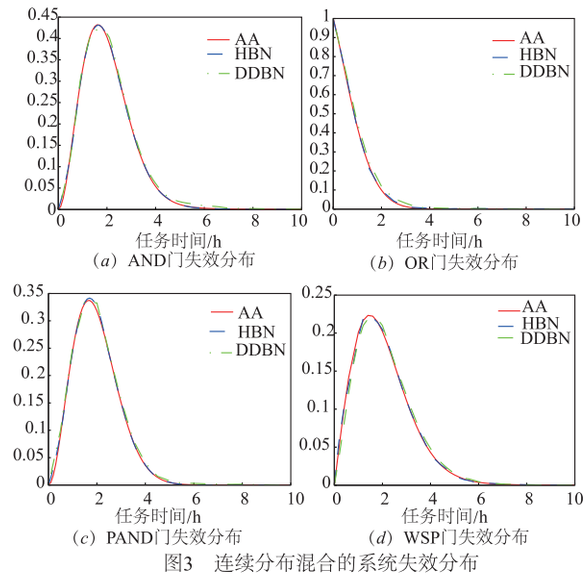
将 HBN 方法分别与动态离散化 DDBN 方法[12]和代数解析法(Algebraic Analysis,AA)[19]对各种门系统分析结果进行比较. HBN 采用 AgenaRisk 和 MATLAB 工具分析,DDBN 方法采用 AgenaRisk 工具分析,AA 方法采用 MATLAB 进行辅助计算,AA 方法只适合简单的系统,但能够给出精确的解. 实验分成两组,首先是连续分布混合的系统分析,然后是离散与连续分布混合的系统分析.

4.1 连续分布混合的系统分析

假设组件 X 失效分布服从 $\lambda=1$ 的指数分布,组件 Y 在失效分布服从形状参数和尺度参数均为 2 的威布尔分布,WSP 中失效率系数 $\alpha=0.5$,任务时间 $T=10$h,HBN 方法采用 6 段 3 次多项式,DDBN 方法迭代 40 次. 图(3)给出了不同连续混合分布下,AND 门、OR 门、PAND 门和 WSP 门分别使用 HBN、DDBN 和 AA 方法得出的失效概率分布. 从图 3 可以看出,HBN 方法拟合的曲线围绕 AA 方法曲线交替微小波动,而 DDBN 方法非交替波动,波动的幅度比 HBN 方法要大,而且基于多项式的 HBN 方法比基于离散化的 DDBN 方法拟合曲线要平滑. 图(4)给出了 HBN 和 DDBN 方法相对于 AA 方法的绝对误差. 在 AND 门中,HBN 方法最大绝对误差为 3.2‰,平均绝对误差为 0.9‰,DDBN 方法最大绝对误差为 7.1‰,平均绝对误差为 4.2‰. OR 门中,HBN 方法最大绝对误差为 3.6‰,平均绝对误差为 0.97‰,DDTBN 方法最大绝对误差为 7.7‰,平均绝对误差为 2.75‰. PAND 门中,HBN 方法最大绝对误差为 2.1‰,平均绝对误差为 0.5‰,DDBN 方法最大绝对误差为 5.9‰,平均绝对误差为 2.4‰. WSP 门中,HBN 方法最大绝对误差为 3.3‰,平均绝对误差为 1.1‰,DDBN 方法最大绝对误差为 7.6‰,平均绝对误差为 2.1‰. 从图 3 和图 4 可以看出,在失效分布函数值变化较快的区域,DDBN 方法和 HBN 方法的绝对误差都增加较快,但从误差分析中可以看出 HBN 方法的计算精度明显优于 DDBN 方法.

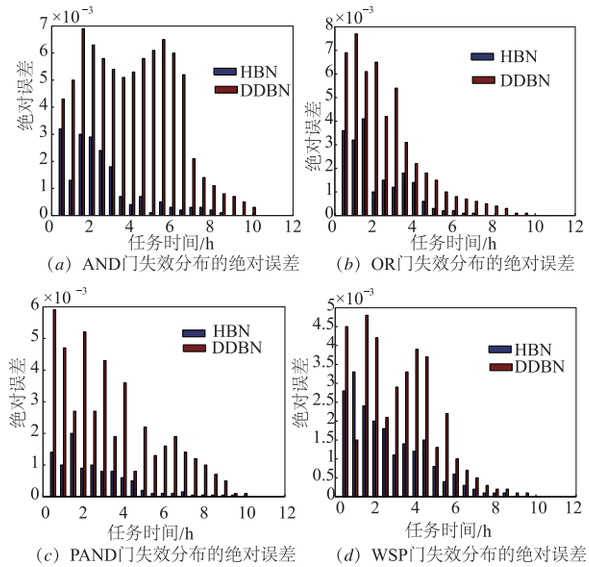
4.2 离散与连续分布混合的系统分析

假设组件 X 是离散的,在$[0,T/2]$时间区间内失效概率为 0.3,在$(T/2,T]$时间区间内失效概率为 0.7. 组件 Y 在失效分布服从形状参数 $k=5$,尺度参数 $\lambda=700$ 的威布尔分布. 任务时间 $T=1000$h,采用 8 段 3 次多项 HBN 方法. 表 1 给出了在离散和连续混合分布下的 AND 门、OR 门和 PAND 门分别使用 HBN 和 AA 方法计算的系统失效概率. 从表 1 中可以看出,系统最大误差为 3.6‰,最小误差为 0.1‰,HBN 方法产生的误差是围绕 AA 方法的计算值上下波动,其平均误差接近于 0,HBN 计算结果非常接近 AA 方法的解析值. 这是由于 HBN 方法是将任务时间划分 k 个区间,在每个区间内的采用 n 个切比雪夫交错点的牛顿插值算法,该算法产生的是最佳一致逼近多项式,能够使最大的误差最小化.



(a) AND门失效分布 (b) OR门失效分布 (c) PAND门失效分布 (d) WSP门失效分布

图3 连续分布混合的系统失效分布



(a) AND门失效分布的绝对误差 (b) OR门失效分布的绝对误差 (c) PAND门失效分布的绝对误差 (d) WSP门失效分布的绝对误差

图4 连续分布混合系统失效分布的绝对误差

表 1　HBN 和 AA 方法的系统失效概率及误差

系统	方法/误差	任务时间(h)									
		100	200	300	400	500	600	700	800	900	1000
AND	HBN	0.0008	0.0013	0.0162	0.0567	0.1726	0.3679	0.6343	0.8559	0.9728	0.9942
	AA	0.0001	0.0019	0.0144	0.0591	0.1697	0.3704	0.6321	0.8577	0.9702	0.9974
	Error	0.0007	-0.0006	0.0018	-0.0024	0.0029	-0.0025	0.0022	-0.0018	0.0026	-0.0032
OR	HBN	0.3010	0.3012	0.3129	0.3378	0.4220	0.8090	0.8896	0.9544	0.9911	0.9992
	AA	0.3000	0.3013	0.3100	0.3414	0.4188	0.8111	0.8896	0.9573	0.9942	0.9959
	Error	0.0010	-0.0002	0.0029	-0.0036	0.0032	-0.0021	0.0026	-0.0029	0.0031	-0.0033
PAND	HBN	0.0003	0.0005	0.0056	0.0156	0.0533	0.3692	0.6341	0.8555	0.9728	0.9945
	AA	0.0000	0.0006	0.0043	0.0177	0.0509	0.3679	0.6343	0.8559	0.9728	0.9942
	Error	0.0003	-0.0001	0.0013	-0.0021	0.0024	-0.0025	0.0022	-0.0018	0.0026	-0.0032

5　总结

安全关键系统安全性分析要综合考虑软件、硬件、运行环境和人工操作等因素相互影响. 由于不同的组件有不同的失效模式和失效分布,因此系统安全性分析需要处理一个离散和连续失效分布共存的混合系统. 传统的方法难以满足混合系统的安全性分析需求. 因此本文提出一个 k 段 n 次多项式 HBN 的混合系统安全性分析方法. 实验表明本文提出方法能够有效地进行混合系统安全性分析且计算精度明显优于其他方法. 但本文的方法还存在一些不足之处,如备件门中备件池共享以及备件门级联系统还不能进行有效分析,这将是下一步研究的方向.

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] 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 BF,HUANG ZQ,HU J,et al. A method for quantitative analysis of state/ event fault tree[J]. Acta Electronica Sinica,2013,41(8):1480-1486. (in Chinese)

[3] LIU DX,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.

[4] GE DC,LIN M,YANG YH,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.

[5] WEBER P,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.

[6] LI XP,AO N,WU LL. The refining reliability modeling method for the satellite system[A]. Proceedings of the 10th International Conference on Reliability Maintainability and Safety[C]. Piscataway:IEEE,2014. 484-488.

[7] LI MY,LIU J,LI J,et al. Bayesian modeling of multi-state hierarchical systems with multi-level information aggregation[J]. Reliability Engineering and System Safety,2014,124(124):158-164.

[8] 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.

[9] KHAKZAD N,KHAN F. Risk-based design of process systems using discrete-time Bayesian networks[J]. Reliability Engineering and System Safety,2013,109(2):5-17.

[10] 房丙午,黄志球,李勇,等. 基于贝叶斯网络的复杂系统动态故障树定量分析方法[J]. 电子学报,2016,44(5):1234-1239.
FANG BW,HUANG ZQ,LI Y,et al. Quantitative analysis method of dynamic fault tree of complex system using Bayesian network[J]. Acta Electronica Sinica,2016,44(5):1234-1239. (in Chinese)

[11] MORI J,MAHALEC V. Inference in hybrid Bayesian networks with large discrete and continuous domains[J]. Expert Systems with Applications,2016 ,(49):1-19.

[12] MARQUEZ D,NEIL M,FENTON N. Improved reliability modeling using Bayesian networks and dynamic discretization[J]. Reliability Engineering and System Safety,2010,95(4):412-425.

[13] 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.
[14] BOUDALI H, DUGAN JB. A continuous – time Bayesian network reliability modeling and analysis framework[J]. IEEE Transactions on Reliability, 2006, 55(1): 86 – 97.
[15] LI YF, HUANG HZ, LIU Y, et al. A novel dynamic fault tree analysis method[A]. International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering[C]. Piscatawa: IEEE, 2013. 81 – 84.
[16] DANIELE CR, PORTINALE L. Modeling and analysis of dependable systems through generalized continuous time Bayesian networks[A]. Reliability and Maintainability Symposium[C]. Piscataway: IEEE, 2015. 1 – 6.
[17] SHENOY PP. Two issues in using mixtures of polynomials for inference in hybrid[J]. International Journal of Approximate Reasoning, 2012, 53(5): 847 – 866.
[18] KOLLER D, FRIEDMAN N. Probabilistic graphical models: principles and techniques[M]. Cambridge, Massachusetts London: MIT Press, 2009. 345 – 378.
[19] NI J, TANG WC, XING Y. A simple algebra for fault tree analysis of static and dynamic systems[J]. IEEE Transactions on Reliability, 2013, 62(4): 856 – 872.

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