

doi: 10.3969/j.issn.1006-1576.2010.03.016

## 基于蒙特卡洛仿真的动态故障树分析

李堂经<sup>1</sup>, 王新阁<sup>1</sup>, 许卓然<sup>2</sup>

(1. 空军航空大学, 吉林 长春 130022; 2. 中国人民解放军 61267 部队, 北京 101114)

**摘要:** 针对基于马尔可夫链的动态故障树分析方法的局限性, 把蒙特卡洛方法用于动态故障树分析。研究了动态故障树分析的蒙特卡洛仿真法并给出了仿真的具体步骤, 然后利用实例对给定的动态故障树进行了蒙特卡洛仿真, 并把仿真结果与精确解进行了比较。结果表明, 把蒙特卡洛法用于动态故障树分析是有效的。

**关键词:** 动态故障树; 蒙特卡洛仿真; 模拟时钟

**中图分类号:** N945.13 **文献标识码:** A

## Dynamic Fault Tree Analysis Based on Monte Carlo Simulation

LI Tang-jing<sup>1</sup>, WANG Xin-ge<sup>1</sup>, XU Zhuo-ran<sup>2</sup>

(1. Aviation University of Air Force, Changchun 130022, China; 2. No. 61267 Unit of PLA, Beijing 101114, China)

**Abstract:** Aiming at the localization of dynamic fault tree analysis (FTA) based on Markov Chains, Monte Carlo method is used to instead of dynamic FTA analysis. Research Monte Carlo method of dynamic FTA, and given detailed steps, then progress Monte Carlo simulation using example to dynamic fault tree, and compare simulation result with exact solution. The result shows that Monte Carlo method is effective using dynamic FTA analysis.

**Keywords:** FTA; Monte Carlo simulation; Simulation timepiece

### 0 引言

动态故障树是在静态故障树的基础上, 引入表征时序相关性、容错性等动态特性的新的逻辑门类型, 把故障树扩展为动态故障树, 用于动态系统的可靠性分析。动态逻辑门主要有: 优先与门、功能相关门、冷备件门、温备件门、热备件门、顺序相关门等。动态故障树分析通常是通过把动态故障树转化为马尔可夫链, 然后应用马尔可夫理论进行分析。基于马尔可夫链的动态故障树分析方法假设底事件服从指数分布, 对底事件不服从指数分布的动态故障树并不适用, 对复杂的动态故障树存在组合爆炸问题, 故引入蒙特卡洛仿真, 求解底事件不服从指数分布的动态故障树和复杂动态故障树的顶事件发生概率和底事件概率重要度。

### 1 动态故障树蒙特卡洛仿真

蒙特卡洛仿真的基本思想是通过计算样本均值来估计总体均值。用蒙特卡洛仿真求解动态故障树, 对底事件所服从的分部类型没有限制, 非常适合于解底事件不服从指数分布的动态故障树和复杂动态故障树的求解分析。

#### 1.1 随机数<sup>[1-2]</sup>

从蒙特卡洛仿真的基本思想可以看出, 对给定

的分布进行抽样, 得到一个随机数样本的过程是蒙特卡洛方法具体应用的一个必不可少的步骤。

均匀分布随机数的产生是产生其它随机数的基础, 产生大量相互独立的均匀分布随机数至关重要。常用的均匀分布伪随机数产生方法有线性同余法、反馈位移寄存器法、组合同余法等, 其中, 线性同余法是目前应用最多的一种方法, 简称为 LCG, 线性同余法包括同余与线性同余法、混合同余法、乘同余法和素数模乘同余法。

同余和线性同余法的一般递推公式为:

$$\begin{cases} x_n = (ax_{n-1} + c) \bmod M \\ r_n = x_n / M \\ \text{初值 } x_0 \end{cases} \quad n = 1, 2, \dots \quad (1)$$

式中,  $M$  为模数,  $a$  为乘子,  $c$  为增量, 且  $x_n$ 、 $M$ 、 $a$ 、 $c$  均为非负整数。由式 (1) 产生的  $x_n (n=1, 2, \dots)$  满足  $0 \leq x_n \leq M$ 。从而  $r_n \in [0, 1]$ 。线性同余法的不同类型是根据选取的模数  $M$ 、乘子  $a$ 、增量  $c$  和初值  $x_0$  的不同来分类的, 比如当增量  $c=0$  时的 LCG 就称为乘同余法。在实例仿真中取  $M=2^{31}-1=2147483647$ ,  $a$  取 16807,  $c$  取 0,  $x_0$  取 3。

对于非均匀分布的随机数的产生常用的方法有: 分布函数抽样法、变换抽样法、值序抽样法、

收稿日期: 2009-10-21; 修回日期: 2010-01-13

作者简介: 李堂经 (1984-), 男, 江西人, 硕士, 从事航空装备技术保障研究。

拒绝抽样法、复合抽样法和近似抽样法。下面介绍分布函数抽样法。

考虑等式:

$$\int_{-\infty}^x f(u)du = F(x) = \xi \tag{2}$$

并求解  $x$  就能得到分布函数为  $F(x)$  的随机变量的一个样本观察值。这里,  $\xi$  是由定义在  $[0, 1]$  区间上的均匀分布  $u(x)$  所产生的一个随机数, 任何一台计算机采用上述均匀分布随机数产生方法都能很容易地产生这种均匀分布的随机数。

对于指数分布的概率密度函数, 等式 (2) 的形式为  $1 - e^{-\lambda t} = \xi$ , 抽样公式变为:

$$t = -\frac{\ln(1-\xi)}{\lambda} \tag{3}$$

故如果  $\xi$  是从  $[0, 1]$  区间上的均匀分布产生的一个随机数, 那么  $t$  就是指数分布随机变量的一个样本观察值。因为  $(1-\xi)$  也是  $[0, 1]$  区间上的均匀分布的随机变量, 可以将表达式简化为  $t = -(\ln \xi)/\lambda$ 。

对于威布尔分布的概率密度函数, 等式 (2) 的形式为  $1 - e^{-m/t_0} = \xi$ , 抽样公式变为:

$$t = \sqrt[m]{-t_0 \ln(1-\xi)} \tag{4}$$

### 1.2 仿真中模拟时钟的推进

动态故障树底事件服从连续时间分布, 设系统为不可修系统。每次系统仿真就是模拟系统从时刻 0 开始运行到给定的最大仿真运行时间, 故必须设置模拟时钟, 并由程序管理这个时钟的运行。当仿真开始时, 模拟时钟为 0, 而在仿真过程中不断地推进, 与日常时钟一样。蒙特卡洛仿真有固定时间步长和可变时间步长 2 种方式表示模拟中的时间进程。固定时间步长法模拟时钟总是按固定的时间增量推进, 在每个时间间隔内对系统的状态进行评估, 并对计算参数进行更新。用可变步长法仿真时, 时间增量由事件出现的时间间隔确定, 即把事件出现的时刻作为时钟推进点, 并在该时刻后对系统进行评估和更新计算参数。采用可变时间步长法。

### 1.3 仿真具体步骤

动态故障树蒙特卡洛仿真的具体步骤为:

1) 设置仿真总次数  $M$  和仿真时间  $T$ , 用  $m$  表示仿真次数,  $n$  表示动态故障树底事件个数,  $f$  表示  $M$  次仿真中顶事件发生的总次数,  $f_i$ ,  $r_i (i=1,2,\dots,n)$  分别表示  $M$  次仿真中顶事件发生的

条件下底事件  $i$  发生和不发生的次数,  $m=0$ ,  $f=0$ ,  $f_i=0$ ,  $r_i=0$ ;

2) 仿真运行时间  $t=0$ ,  $m=m+1$ , 判断  $m$  是否大于  $M$ , 若大于则转到 5);

3) 对各个组件运行时间即各底事件发生时间进行一次抽样, 得到各组件运行时间为  $t_1, t_2, \dots, t_n$ , 冷备份组件在启用之前不会发生故障, 算是正常运行, 所以冷备份组件的运行时间应是被备份组件的运行时间与冷备份组件启用后的运行时间之和, 对  $t_1, t_2, \dots, t_n, T$  进行排序, 最小时间为  $t_{\min}$ ,  $t=t_{\min}$ ;

4) 判断系统状态, 若顶事件发生或  $t \geq T$ , 更新数据记录, 转到 2), 否则,  $t=t+\Delta t_j$ ,  $\Delta t_j$  是可变时间步长, 重复执行这一步;

5) 根据公式及各统计数据计算给定时间内的顶事件发生概率和各底事件的概率重要度。在  $T$  时间内顶事件发生的概率为  $P(T) = f/M$ , 底事件  $i$  的概率重要度为  $I(i|T) = (f_i - r_i)/M$ 。

## 2 仿真实例

图 1 的动态故障树<sup>[5]</sup>包含 5 个动态逻辑门, 2 个冷备件门, 2 个功能相关门, 为便于仿真结果与马尔可夫方法计算结果进行比较假设各底事件服从指数分布, 各组件的失效率如表 1。在时间为 100 个时间单位时用马尔可夫理论计算所得的顶事件发生概率精确解为 0.246 65。

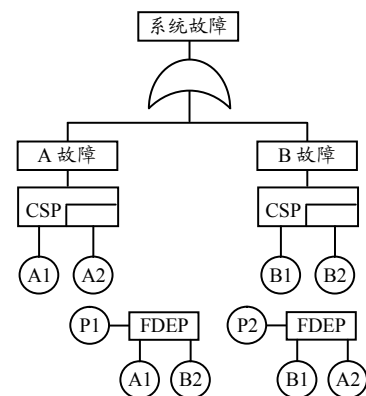


图 1 动态故障树

表 1 各组件失效率

组件	失效率
A1	0.001 0
A2	0.005 0
B1	0.002 0
B2	0.003 5
P1, P2	0.003 0

(下转第 46 页)

$$R = \begin{bmatrix} 0.017 & 0.013 & 0.001 & 0.129 & 0.011 & 0.010 & 0.001 & 0.045 & 0.012 & 0.019 & 0.470 & 1.248 & 0.001 & 0.020 \\ 0.019 & 0.012 & 0.001 & 0.171 & 0.015 & 0.009 & 0.000 & 0.041 & 0.012 & 0.018 & 0.470 & 1.248 & 0.001 & 0.016 \\ 0.018 & 0.011 & 0.000 & 0.129 & 0.014 & 0.009 & 0.000 & 0.040 & 0.009 & 0.018 & 0.385 & 1.273 & 0.000 & 0.018 \end{bmatrix}$$

根据各衡量条件的相对重要程度，经层次分析法可得出各指标的权重系数  $W$ ：

$$W = (0.063\ 4, 0.097\ 2, 0.130\ 7, 0.014\ 6, 0.014\ 5, 0.127\ 8, 0.047\ 5, 0.112\ 7, 0.086\ 3, 0.074\ 6, 0.049\ 3, 0.024\ 7, 0.069\ 2, 0.087\ 5)$$

将求得的单元化矩阵结合权重系数进行加权合成，可得到加权单位化矩阵  $G$ ：

$$G = \begin{bmatrix} 0.107 & 0.126 & 0.013 & 0.188 & 0.016 & 0.128 & 0.005 & 0.507 & 0.104 & 0.142 & 2.317 & 3.083 & 0.069 & 0.175 \\ 0.120 & 0.116 & 0.013 & 0.249 & 0.021 & 0.115 & 0.000 & 0.462 & 0.104 & 0.134 & 2.317 & 3.083 & 0.069 & 0.140 \\ 0.114 & 0.107 & 0.000 & 0.188 & 0.020 & 0.115 & 0.000 & 0.451 & 0.077 & 0.134 & 1.898 & 3.144 & 0.000 & 0.157 \end{bmatrix}$$

\*\*\*\*\*

(上接第 43 页)

### 2.4 确定正、负理想点，计算贴近度

确定供评估参考的正、负理想点，先取各指标的最大值构成正理想点：

$$g_j^+ = (0.120, 0.126, 0.013, 0.249, 0.021, 0.128, 0.005, 0.507, 0.104, 0.142, 2.317, 3.144, 0.069, 0.175)$$

再取各指标的最小值构成负理想点：

$$g_j^- = (0.107, 0.107, 0.000, 0.188, 0.016, 0.115, 0.000, 0.451, 0.077, 0.134, 1.898, 3.083, 0.000, 0.140)$$

按式 (4)、式 (5) 分别计算评价方案与正、负理想方案的贴近度：

$$L = (0.087\ 4, 0.088\ 6, 0.087\ 6) \quad H = (0.431\ 5, 0.429\ 4, 0.430\ 5)$$

### 2.5 综合评估比较

最终用评估指标与理想指标的接近程度来评估作战效能的优劣，由式 (6) 可算得：

$K = (0.831\ 6, 0.828\ 9, 0.830\ 9)$ ，对结果进行排序： $C_1 > C_3 > C_2$ 。

所以这 3 种火炮武器系统的作战效能的评估结果排序为：国产某型自行加榴炮 > M109A6-155 mm 自行加榴炮 > GCT155 mm 自行加榴炮。

## 3 结束语

采用正负理想点法对所选的 3 种火炮武器系统的作战效能综合评估，在建立模型的过程中解决了指标体系合成中的量纲问题。相比模糊综合评估法和灰色评估法，该方法区分度明显，评估可信度高。

### 参考文献：

[1] 马亚龙, 王精业, 徐享忠, 等. 基于正负理想点的仿真结果评估方法研究[J]. 计算机工程, 2002, 28(2): 21-22.  
 [2] 郑津生. 炮兵装备结构与作战效能[M]. 北京: 军事科学出版社, 2006.  
 [3] 郑津生. 155 自行火炮武器系统作战使用及指挥系统操作[M]. 北京: 国防大学出版社, 2001.  
 [4] 许柏树. 层次分析法原理[M]. 天津: 天津大学出版社, 1988.

用蒙特卡洛方法对图 1 动态故障树进行仿真，时间为 100 个时间单位，仿真所得顶事件发生概率如表 2。从仿真结果可见，用蒙特卡洛仿真方法分析动态故障树有效，相对误差在可接受的范围内。

表 2 仿真结果

仿真次数	顶事件发生概率仿真结果	相对误差
100	0.260 0	0.054 1
300	0.243 3	0.013 6
500	0.242 0	0.018 9
1 000	0.243 0	0.014 8
5 000	0.251 4	0.019 3

## 3 结束语

动态故障树一般通过转化为马尔可夫链进而用马尔可夫理论进行分析，但不是所有的动态故障树都能转化为马尔可夫链，因此，用该方法对动态故障树进行分析是很有必要且十分有效的。

### 参考文献：

[1] 张传林, 林立东. 伪随机数发生器及其应用[J]. 数值计算与计算机应用, 2002, 23(3): 188-208.  
 [2] A.杜比, 卫军胡. 蒙特卡洛方法在系统工程中的应用[M]. 西安: 西安交通大学出版社, 2007: 88-106.  
 [3] 王圣金. 基于蒙特卡洛仿真的液压系统动态可靠性研究[D]. 上海: 东南大学, 2006.  
 [4] David W. Coppit, Kevin J.Sullivan and Joanne Bechta Dugan. Bridging the Gap Between Systems and Dynamic Fault Tree Models[C]//Proceedings of The 45th Annual Reliability and Maintainability Symposium. New York USA: IEEE, 1999: 105-111.  
 [5] Tariq Assf, Joanne Bechta Dugan. Diagnostic Expert Systems from Dynamic Fault Trees[C]//Proceedings of The 50th Annual Reliability and Maintainability Symposium. New York: IEEE, 2004: 444-450.  
 [6] Ragavan Manian, Joanne Bechta Dugan. Combining Various Solution Techniques for Dynamic Fault Tree Analysis of Computer Systems[C]//Proceedings of the 3rd International High-Assurance Systems Engineering Symposium. Washington, D.C, USA: IEEE Computer Society, 1998: 21-28.