

# 一种嵌入式系统的可靠性测试与评价方法

郭振杰, 黄 斐

(苏州大学 计算机科学与技术学院, 江苏 苏州 215006)

**摘 要:**使用 Markov 模型进行嵌入式系统的可靠性测评,能够明显地节约计算时间,并保证可靠性测评的准确性,因而越来越受到人们的关注。在 Markov 模型中,可以使用敏感性因子描述嵌入式系统可靠性,建立敏感性因子和测试资源的关联,为系统模块分配可靠性指标,把嵌入式系统的可靠性测试,转化为相应的优化问题。文中介绍了一种基于 Markov 模型的嵌入式系统可靠性测试与评价方法,包括测评框架、设计指标分配和敏感性分析等内容,说明如何依照可靠性测评框架对嵌入式系统进行可靠性测评。

**关键词:**Markov 模型;嵌入式系统;可靠性测评

**中图分类号:**TP301

**文献标识码:**A

**文章编号:**1673-629X(2012)02-0153-03

## A Reliability Assessment Method of Embedded System

GUO Zhen-jie, HUANG Fei

(School of Computer Science and Technology, Soochow University, Soochow 215006, China)

**Abstract:** The reliability evaluation of embedded systems by using the Markov model could significantly save computing time, but still ensure the accuracy of reliability evaluation, which, therefore, is attracting more and more attention. In the Markov model, the sensitivity factor can be used to describe the reliability of embedded system, establishing the association between sensitivity factors and test resources, in order to distribute system reliability index modules for system modules. Meanwhile, the reliability test of embedded systems can be converted into the corresponding optimization problem. It proposes reliability test and evaluation methods of embedded system based on Markov model embedded system, covering the evaluation framework, design specification distribution and sensitivity analysis, etc. Besides, it showed the evaluation methods of the reliability of embedded system based on the reliability evaluation framework.

**Key words:** Markov module; embedded system; reliability assessment

### 1 嵌入式系统可靠性模型

通常 Markov 嵌入式系统模型的控制转换可以用 Markov 链描述<sup>[1]</sup>,各模块的转换概率用  $q_{ij}$  表示。例如某节能管理嵌入式系统包括 5 个模块,这些模块分别为主控模块(E)、节能模块(1)、设备管理模块(2)、系统监控模块(3)、接口控制模块(4)<sup>[2]</sup>,如图 1 所示。

某节能管理嵌入式系统的转换概率必须满足如下表达式:

$$q_{iE} + \sum_{j=1}^n q_{ij} = 1$$

假定嵌入式系统的节能模块代表初始状态,当嵌入系统成功完成执行时,系统控制由所在节能模块(1)以概率  $q_{1E}$  转向主控模块(E)。在嵌入式系统完

全可靠的情况下,模块(i)转换概率为  $q_{iE}$ 。如果系统模块存在缺陷,嵌入式系统不完全可靠,一旦触发缺陷,就会引发系统失效<sup>[3]</sup>。

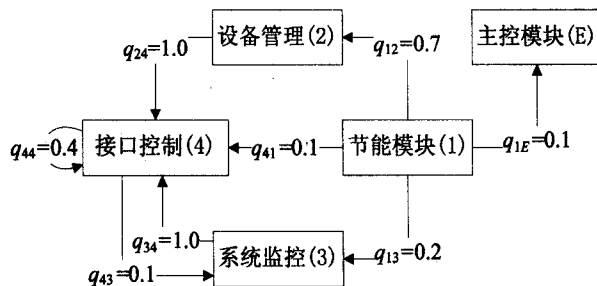


图 1 某嵌入式系统模型

假定失效状态为  $F$ ,嵌入式系统模块(i)进入失效状态为  $F$  的概率为  $1 - q_i$ ,模块(i)的运行可靠性为  $q_i$ 。在图 1 所示的嵌入式系统模型中,Markov 链的吸收状态有  $F$  和  $E$ ,区别于其他 4 个状态<sup>[4]</sup>。如果一个 Markov 嵌入式系统模型有  $n$  个状态,则 Markov 链具有  $n + 2$  个状态<sup>[5]</sup>,对应的转换矩阵  $P$  应满足的关系如下:

收稿日期:2011-06-30;修回日期:2011-10-09

基金项目:住房和城乡建设部科学技术项目计划资助项目(2008-k9-8)

作者简介:郭振杰(1987-),男,硕士研究生,研究方向为智能化信息处理技术;黄 斐,副教授,硕士生导师,研究方向为信息管理、电子商务。

$$\begin{cases} p_{ij} = r_i q_{ij} & i = 1, 2, \dots, n; j = 1, 2, \dots, n \\ p_{iF} = 1 - r_i & i = 1, 2, \dots, n \\ p_{FF} = p_{ss} = 1 \\ p_{ij} = 0 & \text{其它} \end{cases}$$

对于如图 1 所示的某节能管理嵌入式系统模型, 对应的转换矩阵  $P$  满足如下表达式:

$$P = \begin{bmatrix} 0 & q_{12}r_1 & q_{13}r_1 & 0 & q_{14}r_1 & 1-r_1 \\ 0 & 0 & 0 & r_2 & 0 & 1-r_2 \\ 0 & 0 & 0 & r_3 & 0 & 1-r_3 \\ q_{41}r_4 & q_{42}r_4 & q_{43}r_4 & q_{44}r_4 & 0 & 1-r_4 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 2 & 3 & 4 & E & F \end{bmatrix} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ E \\ F \end{matrix}$$

对于如图 1 所示的某节能管理嵌入式系统的运行可靠性  $R_s$  可以用如下表达式描述:

$$R_s = \sum_{i=1}^n (I_n - P)_{ii}^{-1} r_i q_{is}$$

其中  $R_s$  是系统从初始状态转移到吸收状态  $S$  的概率, 单位矩阵用  $I_n$  表示, 非吸收状态转移概率矩阵用  $P$  表示<sup>[6]</sup>。

## 2 嵌入式系统可靠性分配

如图 1 所示的某节能管理嵌入式系统模型, 假定节能模块(1)、设备管理模块(2)、系统监控模块(3)、接口控制模块(4)的运行可靠性为 0.999。用 MATLAB 仿真系统和模块之间的可靠性关系, 结果如图 2 所示。

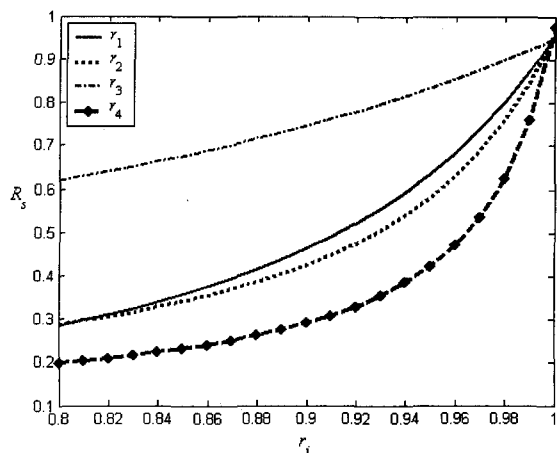


图 2 系统和模块之间的可靠性关系

图中  $R_s$  表示系统模块可靠性,  $r_i$  表示 4 个模块可靠性<sup>[7]</sup>。接口控制模块(4)对软件系统可靠性的影响最大, 而系统监控模块(3)则最小, 在可靠性分配时, 必须优先考虑接口控制模块(4)的可靠性。MATLAB 仿真源程序如下:

```
n = 4;
Q1 = [0,0.7,0.2,0.0,0.1; 0,0,0,1,0; 0,0,0,1,0;
       0.1,0.4,0.1,0.4,0];
r_res = 0.999 * ones(n,1);
II = eye(n, n); % 单位矩阵
for i = 1:n
    rr = r_res;
    for j=0:20
        rr(i) = 0.80+j/100; % r = 0.80, 0.81, ..., 1.00
        RR = spdiags(rr,[0],n,n);
        % 用对角元素数组 rr 生成矩阵方阵 RR
        Q2 = RR * Q1;
        Q3 = Q2(1:n,1:n); Q4 = Q2(:,n+1);
        M = inv(II - Q3); % 求 I - Q 矩阵逆矩阵
        Rs(j+1,i) = M(1,:) * Q4;
    end
end
X = 0.80:0.01:1.00; X = X';
% hline = plot(X,Rs(:,1),'k-',X,Rs(:,2),'b:',
% X,Rs(:,3),'m-',X,Rs(:,4),'rd--');
hline = plot(X,Rs);
hx = xlabel('\it{r}_i');
set(hx,'FontSize',12,'FontName','Times');
hy = ylabel('\it{R}_s');
set(hy,'FontSize',12,'FontName','Times',
    'Rotation',0,'HorizontalAlignment','right');
hlege = legend('\it{r}_1','\it{r}_2',
    '\it{r}_3','\it{r}_4',2);
% 图例
set(gcf,'Color',[1,1,1]) % 设图形底色为白色
set(hline(1),'Color',[0,0,0],
    'LineStyle','-', 'LineWidth', 1.5)
set(hline(2),'Color',[0,0,1],
    'LineStyle',':', 'LineWidth', 2.5)
set(hline(3),'Color',[.1,.5,0],
    'LineStyle','-.', 'LineWidth', 1.5)
c4 = [1,0,0];
set(hline(4),'Color',c4, 'LineStyle',
    '--', 'LineWidth', 2.5)
set(hline(4), 'Marker','diamond', 'MarkerSize', 5,
    'MarkerEdgeColor',c4, 'MarkerFaceColor',c4)
set(hlege,'FontSize',11, 'FontName','Times')
% 设置图例(legend)的属性
h2 = get(gcf, 'Children');
hline = get(h2(2), 'Children');
```

假设某节能管理嵌入式系统失效概率  $p_s$  的估计值为:

$$p_s = F(p_1, p_2, \dots, p_n)$$

则失效概率  $p_s$  的先验分布如下:

$$f(p_s) = \text{Beta}(a_0, b_0) = \frac{p_s^{a_0-1} (1-p_s)^{b_0-1}}{B(a_0, b_0)}$$

失效概率  $p_s$  的数学期望如下：

$$E(p_s) = \int_0^1 p_s \text{Beta}(a_0, b_0) dp_s$$

在嵌入式系统失效概率  $p_s$  的数学期望情况下<sup>[2]</sup>，求解其满足最大熵原则的先验分布表达式如下：

$$\text{Max} \left\{ - \int_0^1 \text{Beta}(a_0, b_0) \ln(\text{Beta}(a_0, b_0)) dp_s \right\}$$

嵌入式系统失效概率  $p_s$  的后验期望如下：

$$\int_0^1 p_s \text{Beta}(a_0 + x, b_0 + n - x) dp_s$$

嵌入式系统失效概率  $p_s$  的后验期望就是系统失效概率的最小二次损失估计<sup>[8]</sup>，用其作为嵌入式系统当前失效概率的估计值<sup>[9]</sup>。

3 多模块可靠性测评方法

由于系统和模块之间可靠性估计存在一定的误差，所以需要进行系统级的可靠性测试，对系统可靠性进行估计、验证<sup>[10]</sup>。一般情况下，系统级的可靠性测试失效数据非常少，在利用 Bayes 方法进行系统级可靠性推断时，为了确定系统失效概率的先验分布，还需要进行模块测试和集成测试<sup>[11]</sup>。

表 1 失效概率  $p_s$  的共轭先验分布数值模拟

$p_s$	$f_{(1)}$	$f_{(2)}$	$f_{(3)}$	$f_{(4)}$
0.005	1	5.851492519	10.46221144	14.8411035
0.05	1	4.642685625	6.586106332	7.412659683
0.1	1	3.54294	3.835462841	3.294258114
0.15	1	2.662231875	2.165618448	1.397667506
0.2	1	1.96608	1.181116006	0.562949953
0.25	1	1.423828125	0.619448662	0.213815376
0.3	1	1.00842	0.310722774	0.075960984
0.35	1	0.696174375	0.148090177	0.024993112
0.4	1	0.46656	0.066512794	0.00752296
0.45	1	0.301970625	0.027862468	0.002039672
0.5	1	0.1875	0.010742188	0.000488281
0.55	1	0.110716875	0.003745569	0.000100533
0.6	1	0.06144	0.001153434	1.71799E-05
0.65	1	0.031513125	0.00030344	2.31815E-06
0.7	1	0.01458	6.49539E-05	2.29583E-07
0.75	1	0.005859375	1.04904E-05	1.49012E-08
0.8	1	0.00192	1.1264E-06	5.24288E-10
0.85	1	0.000455625	6.34315E-08	7.0063E-12
0.9	1	6E-05	1.1E-09	1.6E-14
0.95	1	1.875E-06	1.07422E-12	4.88281E-19
0.995	1	1.875E-11	1.07422E-22	4.88281E-34

由于共轭先验分布具有良好的数学表达，得到了广泛的应用，常见共轭先验分布，包括二项分布和泊松分布等。

假设嵌入式系统运行剖面失效概率为  $p$ ，且每个

输入执行都是相互独立的，在  $n$  个输入执行中失效数  $r$  是二项分布，那么，其每次输入失效概率  $p$  的共轭先验分布的表达式如下：

$$f(p) = \frac{p^{a-1} (1-p)^{b-1}}{B(a, b)}$$

失效概率  $p_s$  的共轭先验分布数值模拟结果如表 1 所示，系统失效概率  $p_s$  不同的先验分布曲线如图 3 所示。此时，系统失效概率  $p_s$  是一个非常小的值，它的分布应该集中在一个比较小的区间，Bayes 假设认为，此时  $p_s$  在整个区间呈均匀分布是背离客观实际的，在进行可靠性测评时所得出的结论是与实际情况不相符的。

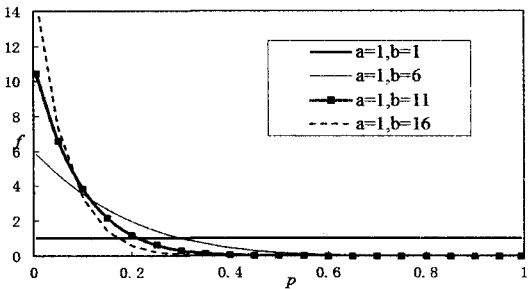


图 3 系统失效概率先验分布函数

在验证测试过程中，可以计算出对应的无失效验证测试用例量，表达式如下：

$$\int_0^{p_0} \frac{p^{a_0+j-1} (1-p)^{b_0+N_{j+1}-j-1}}{B(a_0+j, b_0+N_{j+1}-j)} dp \geq c$$

可以计算出满足最大熵原则的系统失效概率  $p_s$  的先验分布超参数  $a_0$  和  $b_0$ 。若系统的可靠性还未达到预定的可靠性设计指标，则需要进行系统级的可靠性增长测试。在增长测试阶段，若发现了一个失效，排错后还应判断测试是否需要继续进行。

4 结束语

嵌入式系统的可靠性测评方法，与嵌入式系统可靠性分配关系密切。为了实现嵌入式系统的设计目标，需要详细分析嵌入式系统，将其分解成为若干个基本元素。并考虑资源、成本和时间等限制条件，合理分配可靠性指标。虽然嵌入式系统可靠性分配的研究历史并不悠久，但已取得了许多成果，并将随着嵌入式系统可靠性研究的不断深入而迅速发展。

参考文献：

[1] 周源泉, 翁朝曦. 可靠性评定[M]. 北京: 科学出版社, 2005.

[2] 刘 斌, 李铁航. 软件可靠性测试及其评价[J]. 可靠性工程, 2003, 2(2): 88-90.

[3] Lyu M R. Software reliability engineering: a roadma[C]//

算出  $kkD_c$ , 攻击者将面临 ECDH 难题。

### 3.3 未知密钥共享安全

$Y_A, Y_B, Y_C$  是由可信中心为  $A, B$  和  $C$  所颁发的证书中得到的,  $\delta_A, \delta_B$  与  $\delta_C$  又包含了各用户的身份信息、时戳等, 可知消息被用户所绑定;  $C$  若认为会和  $F$  共享同一会话密钥, 还需从  $D_c$  中解出  $c$  和  $Y_c$  中解出  $x_c$ , 即攻击者能求解 ECDLP 难题。

### 3.4 临时密钥泄漏安全

当  $x_A$  和  $x_B$  泄漏给敌手后, 敌手就可伪装为用户  $C$ , 然后对截获的密文解密算出  $k_c, Q_c, D_A, D_B, D_c$ , 敌手不能计算密钥  $K$ , 因为  $a$  和  $b$  未知; 反之敌手能从  $Q_A, D_A$  求  $a$  和从  $Q_B, D_B$  求  $b$ 。同样地, 攻击者将面临 ECDLP 难题。

### 3.5 临时密钥泄漏安全

假设敌手获得了  $a, b, c$ , 攻击者就能计算出  $Q_A, Q_B, Q_C, D_A, D_B, D_C$ , 然后得到  $(P, x_A P, x_B P, x_C P)$ , 但是得不到  $kkD_c$ , 即共享密钥  $K$ 。反之, 攻击者将面临 ECDH 问题。

### 3.6 密钥不可控性

(1) 参数  $a, b$  和  $c$  都被共享密钥所包含, 协议未开始三方用户不能确定会话密钥;

(2) 用户  $A$  和  $B$  进行信息交互得到双方共享的密钥参数  $k$ , 用户  $A$  或  $B$  再把  $k$  作为一个参数与用户  $C$  进行信息交互, 得到三方共享密钥, 任何一方都不能单独得到会话密钥。

## 4 结束语

在现代社会中, 三方密钥协商的地位越来越高, 且在商业活动中运用越来越广泛。文中提出了一个可以认证的三方密钥协商协议, 能够抵抗各种攻击, 与无证书密码学的可认证三方密钥协议<sup>[11]</sup>相比具有较高的安全系数; 此外, 通过分析该协议仅仅使用了倍点运算和哈希运算, 各用户之间仅需要五次信息交互, 与新的三方密钥交换协议<sup>[12]</sup>相比具有较高的效率。通过分

析比较, 该协议能够很好地应用到当代社会的各种实践当中。

### 参考文献:

- [1] Diffie W, Hellman M. New Directions in Cryptography[J]. IEEE Trans. on Information Theory, 1976, 22(6): 644-654.
- [2] Joux A. A One-round protocol for tripartite Diffie-Hellman [C] // Proc of Algorithmic Number Theory Symposium. [s. l.]: Springer-Verlag, 2000.
- [3] Al-Riyami S S, Paterson K G. Tripartite authenticated key agreement protocols from pairings [M]. [s. l.]: Springer-Verlag, 2003.
- [4] Shim K. Efficient one-round tripartite authenticated key agreement protocol form the Weil pairing[J]. Electronics Letters, 2003(39): 208-209.
- [5] Al-Riyami S S, Paterson K G. Certificateless public key cryptography [C] // Proc of Advances in Cryptology2-Asiacrypt. [s. l.]: [s. n.], 2003.
- [6] 刘文刚, 李 斌, 何文星. 基于签密的高效可认证密钥协商协议[J]. 计算机工程, 2011, 37(2): 123-125.
- [7] 师鸣若, 姜中华. 一种无线认证密钥协商协议[J]. 计算机工程, 2009, 35(7): 142-143.
- [8] Abdalla M, Pointcheval D. Interactive Diffie-Hellman assumptions with applications to password-based authentication [C] // The 9th International Conference on Financial Cryptography. Berlin: Springer-Verlag, 2005: 341-356.
- [9] 王元元. 三方认证密钥交换协议研究[D]. 上海: 上海交通大学, 2009.
- [10] Stallings W. Cryptography and network security: principles and practices[M]. 3rd ed. London: Prentice Hall, Pearson Education International, 2000.
- [11] 陈家琪, 冯 俊, 郝 妍. 基于无证书密码学的可认证三方密钥协商协议[J]. 计算机应用研究, 2010, 27(5): 1902-1904.
- [12] 柳秀梅, 周福才, 刘广伟. 新的三方密钥交换协议[J]. 东北大学学报, 2009, 30(7): 976-979.

(上接第 155 页)

- Proceeding of 29th Int Conference on Software Engineering. Minneapolis: [s. n.], 2007.
- [4] Huang Chin-Yu. An improved decomposition scheme for assessing the reliability of embedded systems by using dynamic fault trees [J]. Reliability Engineering and System Safety, 2007, 92(10): 1403-1412.
- [5] 覃志东, 雷 航, 桑 楠, 等. 安全关键软件可靠性验证测试方法研究[J]. 航空学报, 2005, 26(3): 334-339.
- [6] Seija K S. Models for Dependability Assessment and Estimation [R]. [s. l.]: [s. n.], 2003: 100-110.

- [7] 陈火旺, 王 戟, 董 威. 高可信软件工程技术[J]. 电子学报, 2003, 31(1): 1933-1938.
- [8] 颜 炯, 王 戟, 陈火旺. 基于模型的软件测试综述[J]. 计算机科学, 2004, 31(2): 121-127.
- [9] 王儒敬, 白石磊, 毛雪岷. 大型知识库存储结构的研究[J]. 计算机工程, 2003, 29(21): 25-27.
- [10] 黄燕敏. 计算机技术[J]. 苏州工学院学报, 2000, 20(2): 78-80.
- [11] 於晓榛, 李 青. 基于数据仓库的决策支持系统的研究与应用[J]. 计算机与现代化, 2002(10): 32-34.