

容错分布式系统的维修策略研究

On Maintenance Policies of Fault-tolerant Distributed System

胡华平 金士尧

(国防科技大学计算机学院 长沙 410073)

容错, 分布式系统, 维修

TP338.607

摘要 Because the maintenance isn't considered deeply, not only system maintenance cost will be increased, but also the improvement of system performance (reliability, maintainability) is uncertain. In this paper, the reliability model of fault-tolerant distributed system constructed by 2D-TORUS is set up. After that, two kinds of age replacement policies (the minimum of economic lost and maximum availability) are studied.

关键词 Distributed system, Reliability, Maintenance policy

一、引言

许多实际系统在使用过程中,往往由于对维修性问题考虑不周,致使系统的维修费用增加;另一方面如果对系统进行过多的维修,不仅不能提高系统的可靠性和可用度,反而使系统的性能降低。因此系统采用何种维修策略,将关系到系统的性能和维修费用。随着计算机的飞速发展,其系统性能越来越好,价格越来越低;与此同时,计算机的可靠性也越来越高,如DEC公司提供的Alpha PCI 164单板机的MTBF ≥ 47900 小时(工作温度为40°C),其可用度大于0.9999。对于由高可靠性计算机组成的系统,如果再拘泥于一些维修策略,那将给系统增加不必要的维修费用,而且系统的可用度未必得到提高。本文针对由2D-TORUS网组成的容错分布式系统,开展维修策略研究。

二、系统的组成及可靠性模型的建立

1. 系统的组成

本系统的组成与体系结构见图1,它是一个紧耦合的具有容错结构的分布式系统。为了便于进行可靠性分析,将该系统划分为前端I/O节点机子系统、计算处理节点机子系统和后援节点机子系统等三个子系统。每个子系统的组成如下:

•前端I/O节点机子系统:由2个前端I/O节点

机和一备份节点机组成;

•计算处理节点机子系统:由9个计算处理节点机组成,每行由3个计算处理节点机组成;

•后援节点机子系统:由2个后援节点机组成。

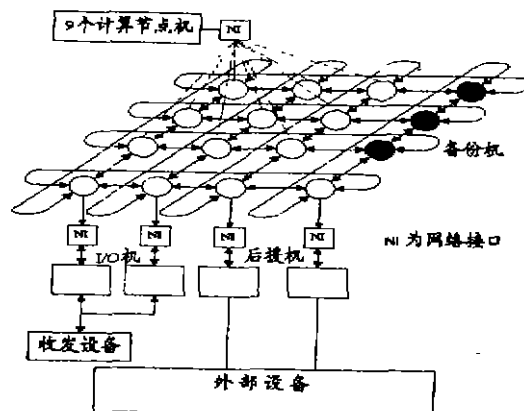


图1 系统的组成与体系结构

2. 可靠性模型的建立

在建立可靠性模型前,首先给出几点假设:

①系统的每个节点机(前端I/O节点机、计算处理节点机和后援节点机、备份节点机)只有两个状态,即工作和故障状态;

②单元的失效是统计独立的;

③组成系统的每个节点机的寿命分布为指数分布,其均值为 $1/\lambda$;故障节点机的修理时间也为指数

胡华平 博士,现为博士后,主要研究领域:计算机系统性能评价、复杂系统的建模与仿真、系统可靠性研究。金士尧 教授,博士生导师。

分布,其均值为 $1/\mu$,且修复如新;

④只分析节点机的可靠性,即认为软件、操作人员是完全可靠的。

现在讨论三种可靠性模型。

模型1 前端 I/O 节点机子系统的可靠性模型

该子系统的2个前端 I/O 节点机是双机动态备份;当有一前端 I/O 节点机发生故障时,可以由备份节点机代替故障前端 I/O 节点机进行工作。只有当前端 I/O 节点机和备份节点机中有2个或2个以上发生故障时,前端 I/O 节点机子系统才失效。该子系统可靠性框图见图2。

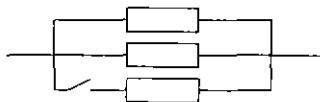


图2 前端 I/O 节点机子系统的可靠性框图

该子系统的可靠度和失效率分别为:

$$R(t) = \frac{A}{S_1 - S_2} \quad r(t) = \frac{4\lambda^2 B}{A}$$

其中: $A = S_1 e^{S_1 t} - S_2 e^{S_2 t}$; $B = e^{S_1 t} - e^{S_2 t}$

S_1, S_2 为下列方程的特征根:

$$S^2 + (4\lambda + \mu)S + 4\lambda^2 = 0$$

模型2 计算处理节点机子系统的可靠性模型

可将计算处理节点机子系统的可靠性模型建为2/3(G)表决,其主要原因有:①各计算处理节点机都运行独立的单机操作系统,它们之间不存在并行处理中的任务分配、调度、同步与通信。在完成任任务时,同行计算处理节点机存在着少量的通讯,不同行间的计算处理节点机均相互独立。因此只需分析某一行计算处理节点机的可用度,即可得到该子系统的可用度;②任务到达计算处理节点机子系统的任一处理节点机均需向同一行的计算处理节点机传送数据并发出计算要求,且认为该过程是完全可靠的(该假定是建立在紧耦合互连网络快速传输和富裕的计算节点处理能力的基础上);③当系统中有二个或二个以上的处理节点机故障时,系统才失效。该子系统的可靠性框图见图3。



图3 计算处理节点机子系统的可靠性框图

该子系统的可靠度和失效率分别为:

$$R(t) = \frac{A}{S_1 - S_2} \quad r(t) = \frac{6\lambda^2 B}{A}$$

其中: A, B 同前; S_1, S_2 为方程:

$$S^2 + (5\lambda + \mu)S + 6\lambda^2 = 0 \text{ 的特征根。}$$

模型3 后援节点机子系统的可靠性模型 由于后援节点机主要承担本系统的初起、服务过程中的系统管理、作业管理和网络管理、事后的档案管理及系统故障诊断等功能。该子系统的2个后援节点机构成双机动态备份,其可靠性框图见图4。

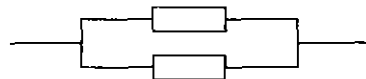


图4 后援节点机子系统的可靠性框图

该子系统的可靠度和失效率分别为:

$$R(t) = \frac{A}{S_1 - S_2} \quad r(t) = \frac{2\lambda^2 B}{A}$$

其中: A, B 同前; S_1, S_2 为方程:

$$S^2 + (3\lambda + \mu)S + 2\lambda^2 = 0 \text{ 的特征根。}$$

三、维修策略的研究

1. 维修策略

连续时间的基本维修策略主要有:年龄更换策略、成批更换策略、故障小修的周期更换策略、年龄维修策略、备用部件的预防维修策略、故障小修的周期维修策略等。由于计算机及其外部设备都极其昂贵,若采用故障更换的方法显然不合适,而采用故障维修的方法则是较为经济的维修策略。本文主要研究年龄维修策略。

年龄维修策略是指:当系统达到指定的年龄 T 仍然正常,则对系统进行预防维修,预防维修时间均值为 β_p 。若系统在指定的时间 T 之前发生故障,就立即进行事后维修,维修时间均值为 β_r ,图5为其示意图。



图5 年龄维修策略

$$\text{令 } a = \frac{C_p \beta_p}{(C_r \beta_r - C_p \beta_p)M + \beta_p \beta_r (C_r - C_p)}$$

$$b = \frac{\beta_r}{M(\beta_r - \beta_p)}$$

其中: C_p : 单位时间内系统的预防维修费用; C_r : 单位时间内系统的事后维修费用; M : 系统的平均无故障时间, $M = \int_0^\infty R(t)dt$ 。

由文[1]知:对于经济损失最小的年龄维修策略,若 $C_r \beta_r > C_p \beta_p$, $\beta_r > \beta_p$,且系统的失效率 $r(t)$ 是连续严格单调递增的,其是否存在最佳维修时间间隔 T^* 的判断为:

①若 $r(\infty) > a$, 则存在唯一的最佳 T^* , 使系统的经济损失最小;

②若 $r(\infty) \leq a$, 则 $T^* = \infty$, 且最小的经济损失为: $C(\infty) = C_0\beta_1/(M+\beta_1)$ 。

同样, 对于可用度最大的年龄维修策略, 其是否存在最佳维修时间间隔 T^* 的判断为:

①若 $r(\infty) > b$, 则存在唯一的最佳 T^* , 使系统的可用度最大;

②若 $r(\infty) \leq b$, 则 $T^* = \infty$, 且最大的可用度为: $A(\infty) = M/(M+\beta_1)$ 。

经验证, 本文所讨论的3个模型的失效率 $r(t)$ 均满足连续严格单调递增的条件。

2. 应用举例

假定: 预防维修时间 $\beta_1 = 1$ 小时, 其维修费用为 $C_0 = 100$ 元/小时; 事后维修时间 $\beta_2 = 4$ 小时, 其维修费用为 $C_1 = 400$ 元/小时。本文将分三种情况进行讨论(① $\lambda = 0.0005$ $\mu = 0.25$; ② $\lambda = 0.01$ $\mu = 0.25$; ③ $\lambda = 0.05$ $\mu = 0.25$), 对于经济损失最小和可用度最大的年龄维修策略, 各子系统是否存在最佳预防维修时间间隔的判断结果分别列于表1~表3。表中,

表1 最佳预防维修时间间隔的判定

($\lambda = 0.0005$ $\mu = 0.25$)

模型	$r(t)$	a	b	策略1	策略2
1	3.97×10^{-6}	4.23×10^{-6}	5.29×10^{-6}	不存在	不存在
2	5.94×10^{-6}	6.34×10^{-6}	7.92×10^{-6}	不存在	不存在
3	1.48×10^{-5}	2.12×10^{-5}	2.65×10^{-5}	不存在	不存在

表2 最佳预防维修时间间隔的判定

($\lambda = 0.01$ $\mu = 0.25$)

模型	$r(t)$	a	b	策略1	策略2
1	1.38×10^{-3}	1.47×10^{-3}	1.84×10^{-3}	不存在	不存在
2	2.01×10^{-3}	2.11×10^{-3}	2.65×10^{-3}	不存在	不存在
3	7.16×10^{-4}	7.44×10^{-4}	9.31×10^{-4}	不存在	不存在

表3 最佳预防维修时间间隔的判定

($\lambda = 0.05$ $\mu = 0.25$)

模型	$r(t)$	a	b	策略1	策略2
1	2.344×10^{-2}	2.32×10^{-2}	2.96×10^{-2}	存在	不存在
2	3.21×10^{-2}	3.12×10^{-2}	3.99×10^{-2}	存在	不存在
3	1.29×10^{-1}	1.32×10^{-1}	1.66×10^{-1}	不存在	不存在

策略1指经济损失最小的年龄维修策略; 策略2指可用度最大的年龄维修策略。

3. 结论

①对于策略1, 本文所讨论的三种情况, 仅有每个节点机的失效率和维修率为情况3($\lambda = 0.05$ $\mu = 0.25$)时, 才存在最佳预防维修时间间隔, 即才有采用预防维修的必要; 而对于其它情况, 则没有必要采用预防维修, 即只需对每个子系统采用事后维修, 就可使每个子系统的经济损失(维修费用)最小;

②对于策略2, 本文所讨论的三种情况, 均不存在最佳预防维修时间间隔, 即没有必要采用预防维修, 只需对每个子系统采用事后维修, 就可使每个子系统的可用度最大;

③对于本系统, 在目前计算机的可靠性和维修性的水平(非容错计算机的 MTBF ≥ 1080 小时, MTTR = 4 小时^[2], 通用机的可用度大于 0.99^[3])的情况下, 完全可以不对系统采用预防维修, 而只需采用事后维修就可使系统的维修费用最小或可用度最大。如果一味强调预防维修, 那将给系统增加不必要的维修费用, 而系统的可用度不但不会提高, 反而会降低。

参考文献

- [1] 胡华平, FMS 维修策略研究, 数理统计与应用概率, 11(1), 1996
- [2] 闵应骅, 容错二十五年, 计算机学报, 18(12), 1995
- [3] 国家自然科学基金委员会, 计算机科学技术, 科学出版社, 1994