

支持异常处理的软件系统可用性分析

潘 峰^{1,2}

(1 贵州民族大学 模式识别与智能系统省级重点实验室, 贵州 贵阳 550025;

2 贵州民族大学 计算机与信息工程学院, 贵州 贵阳 550025)

摘 要: 提出一种基于随机 Petri 网(Stochastic Petri Net, SPN)的支持异常处理的软件系统可用性建模与分析方法. 在建立支持异常处理的元结构 SPN 模型和支持异常处理的典型结构 SPN 模型的基础上, 给出了支持异常处理的软件系统可用度求解方法. 最后, 以某汽车厂零部件采购系统为例, 在建立其 SPN 模型的基础上, 分析了系统的可用度参数. 可以为软件系统异常处理的分析与设计提供理论参考.

关键词: 软件系统; 随机 Petri 网; 异常处理; 可用性

中图分类号: TP391

文献标识码: A

文章编号: 1000-7180(2013)08-0049-04

Availability Analysis of Software System Supporting Exception Handle

PAN Feng^{1,2}

(1 Guizhou Key Lab of Pattern Recognition & Intelligent Control, Guizhou Minzu University, Guiyang 550025, China;

2 School of Computer and Information Engineering, Guizhou Minzu University, Guiyang 550025, China)

Abstract: This paper presents a new availability analysis method of software system supporting exception handle (SSSEH) based on stochastic petri net (SPN). Based on constructing the primary structure SPN model supporting exception handle and the typical structure SPN model supporting exception handle, it gives the availability solving method of SSSEH. Finally, the SPN model of one component purchasing system of automobile factory is constructed, and its availability analysis is given. The work of this paper can provide theoretical basis for analysis, design and evaluation of SSSEH.

Key words: software system; stochastic petri net; exception; availability

1 引言

异常处理机制已经成为软件系统设计中不可缺少的重要组成部分, 文献[1]中的统计结果表明, 异常处理代码约占软件系统总体代码量的 10%, 可见异常处理机制为高可用性的软件系统提供了强有力的技术保障. 但是, 异常处理在长时间里并没有引起研究技术人员的重视, 这使得软件系统在运行过程中, 由于运行环境的动态不确定性以及服务资源的自治性和松耦合性, 更加容易出现各种各样的错误^[2-3]. 因此, 在软件系统开发过程中, 应当在总体设计阶段充分考虑异常处理机制的设计与规划, 从

而降低异常给软件系统可用性带来的影响. 传统的软件系统可用性分析方法不能很好地描述系统与时间相关的动态行为特性, 这样针对软件系统异常处理的分析、设计与评价就存在着一定的挑战.

随机 Petri 网^[4-5] (Stochastic Petri Net, SPN) 是一种形式化的图形建模与分析工具, 特别适用于软件系统异常处理的分析、设计与评价, 已经得到了众多学者的重视与研究^[6-9]. 本文以 SPN 为数学工具, 应用 SPN 技术研究支持异常处理的软件系统的可用性, 为软件系统异常处理的分析与设计提供理论支持.

收稿日期: 2012-10-27; **修回日期:** 2012-11-30

基金项目: 贵州省科学技术基金(黔科合 J 字 LKM[2011]18 号, 黔科合计 Z 字[2009]4002)

2 软件系统可用性

软件系统按照是否存在异常处理机制,可以分为可支持异常处理的软件系统和不可支持异常处理的软件系统.如果某一软件系统一旦出现异常,通过异常处理就可以恢复到正常工作状态,那么该软件系统是一个可支持异常处理的软件系统;反之,异常无法修复,则该软件系统是一个不可支持异常处理的软件系统.可见,软件系统的可用性这一概念是针对可支持异常处理的软件系统提出的.软件系统的可用性及其参数定义如下:

定义 1 软件系统的可用性.对于可支持异常处理的软件系统,在其工作经历“正常→异常→正常→异常”的循环过程中,系统所能实现正常工作的能力,即系统正常工作时间和总的运行时间之比,用可用度加以度量.

3 建模与分析方法

3.1 建模方法

3.1.1 支持异常处理的元结构 SPN 模型

图 1 所示为可支持异常处理的元结构 SPN 模型.模型中位置和变迁定义如下:位置 Pad 表示软件系统处于存在某种业务需求的状态;位置 Pus 表示可以为该业务需求提供服务的资源;位置 Pu 表示可以为该业务需求提供服务的资源处于正常工作状态;位置 Pee 表示可以为该业务需求提供服务的资源出现异常;位置 Pr 表示可以为该业务需求提供服务的资源处于待维修状态;位置 Pc 表示系统完成了该业务需求的服务.变迁 Tap 表示系统提出某种业务需求;变迁 Te 表示为该业务需求提供服务的资源以概率 $1-\beta$ 产生异常;变迁 Tn 表示为该业务需求提供服务的资源以概率 β 提供正常服务;变迁 Tes 表示为该业务需求提供服务的资源产生异常;变迁 Tr 表示对为该业务需求提供服务的资源进行维修;变迁 Tp 表示为该业务需求提供服务的资源可以提供正常服务.

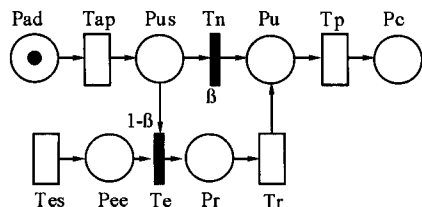


图 1 可支持异常处理的元结构 SPN 模型

3.1.2 可支持异常处理的串联结构 SPN 模型

图 2 所示为可支持异常处理的串联结构 SPN 模型,用以描述异常出现在有 $n(n \geq 2)$ 个组成单元的软件系统中,且所有异常全部通过单一的异常修复资源修复成功后,才能恢复正常工作的情况.模型中位置和变迁定义如下:位置 Pss 表示软件系统处于待开始工作状态;位置 $Pad_i (i=1,2,\dots,n)$ 表示软件系统中第 i 个组成单元处于存在某种分业务需求的状态;位置 $Pus_i (i=1,2,\dots,n)$ 表示软件系统中可以为第 i 个组成单元提供服务的资源;位置 $Pee_i (i=1,2,\dots,n)$ 表示软件系统中第 i 个组成单元处于产生异常状态;位置 Pr 表示软件系统中有某个组成单元异常,并处于待维修状态;位置 Pu 表示软件系统可以提供正常服务;位置 Pc 表示软件系统完成了相应服务.变迁 $Ts_i (i=1,2,\dots,n)$ 表示软件系统中第 i 个组成单元开始工作;变迁 $Tap_i (i=1,2,\dots,n)$ 表示软件系统中第 i 个组成单元产生某种分业务需求;变迁 $Tee_i (i=1,2,\dots,n)$ 表示软件系统中第 i 个组成单元产生异常;变迁 $Te_i (i=1,2,\dots,n)$ 表示可以为软件系统中第 i 个组成单元提供服务的资源以概率 $1-\beta_i$ 产生异常;变迁 $Tn_i (i=1,2,\dots,n)$ 表示可以为软件系统中第 i 个组成单元提供服务的资源以概率 β_i 提供正常服务;变迁 Tr 表示对为软件系统中各个组成单元的分业务需求提供服务的资源进行异常维修;变迁 Tp 表示为软件系统可以提供正常服务.

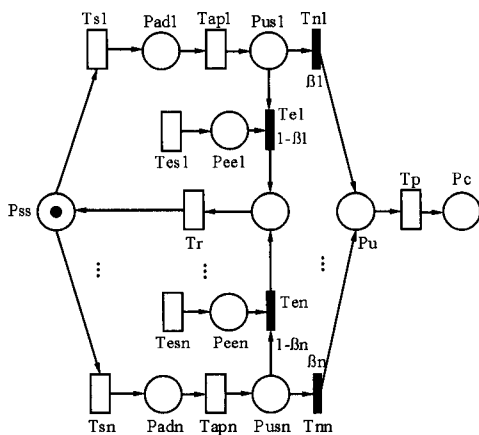


图 2 可支持异常处理的串联结构 SPN 模型

3.1.3 可支持异常处理的并联结构 SPN 模型

如图 3 所示为可支持异常处理的并联结构 SPN 模型,用以描述异常出现在有 $n(n \geq 2)$ 个组成单元的软件系统中,且每个组成单元的异常都是通过各自独立的异常修复资源修复成功后,才能恢复

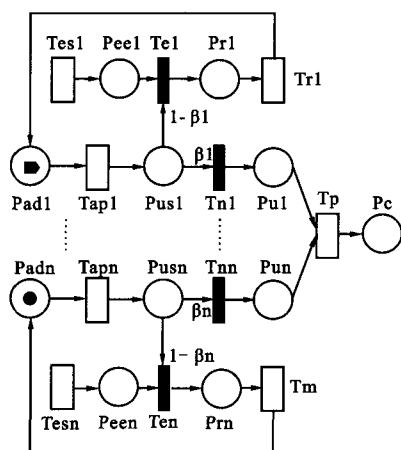


图 3 可支持异常处理的并联结构 SPN 模型

正常工作的情况。模型中位置和变迁定义如下:部分位置和变迁的命名与含义同可支持异常处理的串联结构 SPN 模型。此外,不同的有:位置 $Pr_i (i=1, 2, \dots, n)$ 表示软件系统中第 i 个组成单元处于待异常修复状态;位置 $Pu_i (i=1, 2, \dots, n)$ 表示为软件系统中第 i 个组成单元提供服务的资源处于正常工作状态;变迁 $Tr_i (i=1, 2, \dots, n)$ 表示对软件系统中第 i 个组成单元的异常进行修复。

3.2 可用度参数求解方法

应用随机 Petri 网技术对目标软件系统进行可用性建模后,便可以利用 SPN 模型与 Markov 链同构这一特性求解模型的可用度参数.

为便于分析,假设目标软件系统 SPN 模型有 $N+1$ 个状态,将这 $N+1$ 个状态分为两个子集合.其中,系统正常工作状态的子集合为 $S_n = \{s_0, s_1, \dots, s_k\}$;系统异常工作状态的子集合为 $S_e = \{s_{k+1}, s_{k+2}, \dots, s_N\}$.

令 $x_i(t) = P[X(t) = i]$ 是 t 时刻系统为状态 s_i 的概率 ($i = 0, 1, \dots, k, k+1, \dots, N$), 则 t 时刻系统为正常工作状态的概率向量为: $P_n(t) = [x_0(t), x_1(t), \dots, x_k(t)]$, 而 t 时刻系统为异常工作状态的概率向量为: $P_e(t) = [x_{k+1}(t), x_{k+2}(t), \dots, x_N(t)]$. 令系统从状态 s_i 转移到状态 s_j 的概率为 γ_{ij} , 可知:

$$\sum_{j=1}^N y_{ij} = 1 \quad (i=0, 1, \dots, k, k+1, \dots, N).$$

在相关参数定义完成后,给出系统可用度参数的求解计算式:

软件系统的可用度可以用软件系统在任意时刻 t 的正常工作状态 ($S_n = \{s_0, s_1, \dots, s_k\}$) 的概率. 当工作时间 t 足够长时, 软件系统的稳态可用度为状态 s_0 的稳态概率:

$$P_A(t) = \left(1 + \sum_{i=1}^n \frac{\lambda_i}{u_i}\right)^{-1} \quad (1)$$

式中, λ_i 和 μ_i 是软件系统中第 i 个组成单元的异常发生率和异常修复率.

4 实例研究

本文以某汽车厂零部件采购系统为例,将该汽车厂选择零部件供应商流程(图 4)作为研究对象,应用随机 Petri 网技术建立其可支持异常处理的 SPN 模型和不支持异常处理的 SPN 模型. 通过对比分析两者的可用性指标,验证本文方法的有效性.

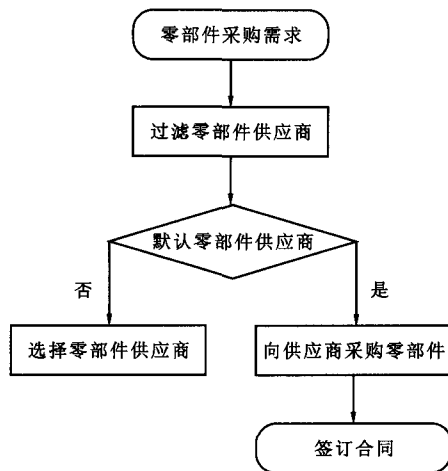


图 4 某汽车厂选择零部件供应商流程

4.1 SPN 模型建立

对照上述的某汽车厂选择零部件供应商流程,应用随机 Petri 网技术建立了其可支持异常处理的 SPN 模型(图 5)和不支持异常处理的 SPN 模型(图 6).

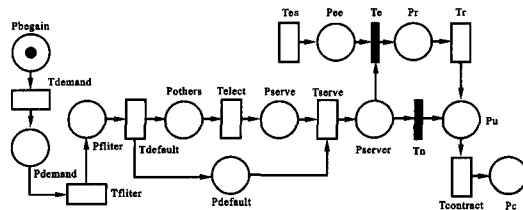


图 5 可支持异常处理的 SPN 模型

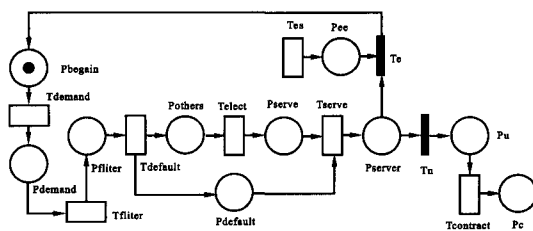


图 6 不支持异常处理的 SPN 模型

4.2 仿真及分析

SPNP6.0 软件包^[10]是美国杜克大学 Kishor S. Trivedi 教授领导的研究小组所研发的较成熟的随机 Petri 网建模与分析软件. 基于 SPNP6.0 软件包的建模与分析框架, 本文实现了汽车厂选择零部件供应商这一流程的可支持异常处理的 SPN 模型和不支持异常处理的 SPN 模型. 模型成功运行, 得到了两者的可用度变化曲线, 如图 7 所示.

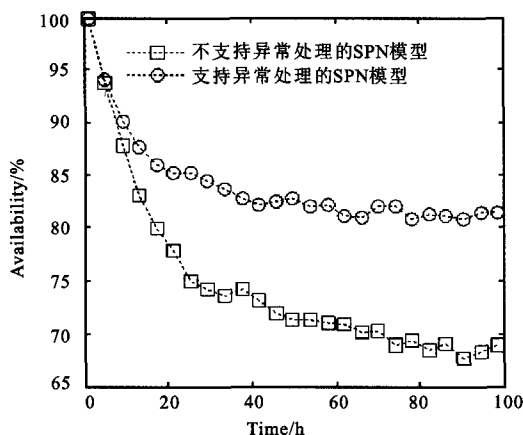


图7 系统可用度比较分析

由系统可用度比较分析图可知: 可支持异常处理的 SPN 模型的可用度曲线随着工作时间的增加下降速度缓慢, 到 40 h 开始趋于平缓, 最后为 80.3%. 而不支持异常处理的 SPN 模型的可用度曲线随着工作时间的增加下降速度较前者明显要快, 到 60 h 开始趋于平缓, 最后为 66.8%. 不难看出: 当该汽车厂零部件采购系统工作时间相同的情况下, 其可支持异常处理的 SPN 模型的可用度要明显优于不支持异常处理的 SPN 模型.

5 结束语

本文提出一种基于随机 Petri 网的支持异常处理的软件系统可用性建模与分析方法. 在建立支持异常处理的软件系统元结构和典型结构的 SPN 模型的基础上, 给出了支持异常处理的软件系统可用度求解方法. 选择某汽车厂零部件采购系统作为目标系统进行 SPN 建模, 分析求解了其可支持异常处

理的 SPN 模型和不支持异常处理的 SPN 模型, 通过比较两者的可用度参数, 验证了本文方法的有效性. 本文的工作为软件系统异常处理的分析与设计提供了新的思路.

参考文献:

- [1] Illard R M P, Murphy G C. Static analysis to support the evolution of exception structure in object-oriented systems[J]. ACM Transactions on Software Engand Methodology, 2003, 12(2): 1912-1921.
- [2] Jiang S J, Xu B W. Exception handling—an approach to improving software robustness[J]. Computer Science, 2003, 30(9): 169-172.
- [3] Lerner B S, Cheistov S, Osterweil L J, et al. Exception handling patterns for process modeling[J]. IEEE Transaction On Software Engineering, 2010, 36(2): 162-183.
- [4] 林闯. 计算机网络和计算机系统的性能评价[M]. 北京: 清华大学出版社, 2001: 185-192.
- [5] 林闯, 王元卓, 杨扬, 等. 基于随机 Petri 网的网络可信性分析方法研究[J]. 电子学报, 2006, 34(2): 322-332.
- [6] 杨志义, 张琛雨, 董云卫. AADL 软件容错系统建模与评估[J]. 计算机测量与控制, 2009, 17(4): 779-782.
- [7] 张静乐, 杨扬, 高昂, 等. 基于随机 Petri 网的柔性工作流可用性分析[J]. 计算机工程, 2010, 36(22): 22-25.
- [8] 张静乐, 杨扬, 曾明, 等. 支持异常处理的柔性工作流可信性分析[J]. 计算机科学, 2010, 37(4): 41-44.
- [9] 吴青, 应时, 贾向阳. 面向服务软件中基于着色 Petri 网的异常处理模型[J]. 计算机科学, 2011, 38(4): 170-174.
- [10] Ciaodo G, Muppala J, Trivedi K S. Manual for the SPNP package, version 6.0[D]. USA: Duke University, Department of Elec. Eng, 1999.

作者简介:

潘 峰 男, (1974-), 硕士, 副教授. 研究方向软件工程和 Petri 网理论.