基于随机 Petri网的网络可信赖性分析方法研究

林 闯[1],王元卓[2,1],杨 扬[2],曲 扬[1]
(1. 清华大学计算机科学与技术系,北京 100084; 2. 北京科技大学信息工程学院,北京 100083)

摘 要: 随着人们对计算机网络系统的依赖性的不断增强,网络系统的可信赖性研究变得越来越重要.本文首先对可信赖性的概念及其主要性能指标进行论述,并对系统可信赖性各种模型方法及求解特点作了分类比较.在此基础上研究了随机 Petri网 (SPN)对网络系统可信赖性建模分析的方法和步骤,着重研究了随机 Petri网描述系统的服务失效模型和容错模型,并给出了网络系统可信赖性分析中主要指标的计算方法.最后对于应用随机 Petri方法分析网络系统可信赖性时存在的问题以及研究现状作了分析和总结,并对今后研究的方向进行了展望.

关键词: 可信赖性; 容错; 随机 Petri网; 马尔可夫过程; 非马尔可夫过程
中图分类号: TP391.7 **文献标识码**: A **文章编号**: 0372-2112 (2006) 02-0322-11

Research on Network Dependability Analysis Methods Based on Stochastic Petri Net

LIN Chuang[1], WANG Yuan-zhuo[2,1], YANG Yang[2], QU Yang[1]
(1. Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China;
2. Information Engineering School, University of Science and Technology of Beijing, Beijing 100083, China)

Abstract: With people rely more on computer networks, the study on the dependability of networks is increasingly significant. First the paper provides insight about the main definitions and attributes related to dependability, and classifies and compares the general models for dependability. On the basis of the synthesis, the modeling and analysis methods using Stochastic Petri Net (SPN) for the network system dependability are mainly investigated. The service failure and fault tolerance SPN models and the calculating methods of main dependability attributes are examined. The existing problems and applications of SPN are concluded that concern the dependability of networks. And directions for future research are also indicated.

Key words: dependability; fault tolerance; stochastic Petri net; Markov; non-Markov

1 引言

系统能够提供可信赖服务的能力就是可信赖性.可信赖性是度量各种系统服务质量的重要指标,可信赖性问题极大的影响着系统的性能.对系统可信赖性问题的研究起源于 20世纪 30年代的美国军用系统的研制,并在美国的国防、航空、航天、电子等工业部门等到了应用.对系统可信赖性进行深入的分析研究是从 20世纪 40年代开始的并在近 30多年来日趋成熟,成为一门综合性和边缘性的应用学科.它的任务是研究系统或设备在设计和使用的各个阶段,定性与定量的分析、控制、评估和改善系统或设备的可信赖性,并在设计中达到可信赖性与经济性综合平衡.随着计算技术的普及,计算机系统应用日益广泛.由于计算机系统处理任务的多样化,计算机系统的工作环境普适化,计算机系统也越来越复杂,计算机系统面临的各种人为和非人为的威胁也越来越多.计算机系统能否正确、安全、高效地完成指定任务,即能否提供可信赖的服务能力,已成为人们关心的主要问题之一.

计算机网络是当前最复杂,规模最大,应用最广泛的计算机系统,并已成为信息基础设施最重要的组成部分.

收稿日期: 2005-10-10;修回日期: 2005-11-06
基金项目:国家自然科学基金 (No. 90412012);国家"九七三 重点基础研究发展规划项目基金 (No. 2003CB314804);国家自然科学基金委员会与香港研究资助局合作基金 (No. 60218003);高等学校博士学科点专项科研基金 (No. 20020003027);国家自然科学基金 (No. 60503052)

如何在网络复杂异构的环境下,提供一致的安全服务体系结构;如何在网络固有的脆弱性、人为的操作失误和管理漏洞以及网络攻击和破坏客观存在的状况下,保障系统服务的可信赖性,都是必须综合考虑的重要问题. 正如美国工程院院士 Patterson教授所指出的,过去的研究以追求高效行为为目标,而今天计算机系统需要建立高可信的网络服务,可信赖性必须成为可以衡量和验证的性能. 针对网络环境新特点,研究系统可信赖性,使其能够提供可信赖的 服务正在成为人们关注的焦点.

在可信赖性研究的发展过程中,为了得到各种可信赖性指标,人们提出了各种各样的可信赖性分析技术和建模工具,利用这些工具建立反映系统行为和性质的数学模型,在此基础上进行性能和可信赖性分析. 其中,随机 Petri网对系统的并发性、异步性和不确定性具有很强的动态分析能力,同时具有建模原语少、符合直观的图形表示等优点,它既能描述系统状态,又能表现系统行为,且全局的状态和行为不是最基本的概念,而是由局部的状态和行为组合得到的,特别适合于对系统建模和进行可信赖性分析.

本文的组织结构如下:第二部分对可信赖性的概念及其主要性能指标进行论述,并对系统可信赖性各种模型方法及求解特点作以分类比较,分析随机 Petri网建立系统可信赖性模型的优势;第三部分详细介绍随机 Petri网对描述网络系统的服务失效模型、容错模型的建模和求解方法;在第四部分中分析了随机 Petri网研究系统可信赖性时尚存在的问题以及研究现状;第五部分总结全文并展望下一步研究工作.

2　相关研究背景

2.1　可信赖性

1952年 Robert Lusser在 San Diego的一次论坛上首次提出了关于系统可信赖性的定义和参数. 1953年 Richard R Carhart对它作了概括,指出系统可信赖性 (dependability)是在一定的条件下,系统在一定的时间区间内完成一定功能的能力[1]. 在文献[2,3]中,可信赖性被进一步定义为,避免不可接受的频繁发生服务失效的能力. 在这里我们将可信赖性定义为系统在受到外部攻击或者由于人为误操作、环境影响以及硬件故障和软件 bug使得系统失效出现时,连续提供服务并在规定时间内恢复所有服务的能力.

永不失效的系统是不可能实现的,所以人们希望系统的失效概率足够低,以满足其应用需求,即系统的可信赖程度需要达到人们要求的水平. 我们认为可信的网络系统的行为及其结果是可以通过对其模型的求解来预期的,能够做到行为状态可监测,行为结果可评估,异常行为可控制. 具体而言,网络的可信赖性应该包括这样一些主要指标如图 1所示:可靠性 (Reliability)、可用性 (Availability)、可运行性 (Performability)、可维护性 (Maintainability)和可生存性 (Survivability)等[1,2],另外,MTTF (Mean Time To Failure)首次故障前平均时间;MTBF (Mean Time Between Fault)平均故障间隔时间;MTTR (Mean Time To Repair)平均故障时间也是可信赖性分析的重要指标.

可靠性[2]:提供正确服务的连续性,可以用 R(t)度量,一般认为系统在 0时刻正常工作的条件下,在 (0, t]时间区间内正常工作概率. 系统的失效被认为具有马尔科夫性.

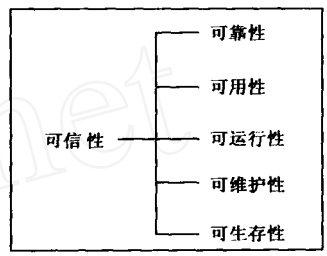

图 1　可信赖性研究的主要指标

$$R(t) = P\{X > t\} \quad (1)$$

同时可以用 1 - R(t)来计算系统的不可靠性.

可用性[2]:可以提供正确服务的能力,它是为可修复系统提出的,是可靠性和可维护性的综合描述. 对于不可修复系统可用性与可靠性相等. 根据可用性与时间的关系,可用性可分为瞬时可用性、稳态可用性、固有可用性.

(1)瞬时可用性 A(t):系统开始工作后,在任一时刻可提供服务的概率.

(2)稳态可用性 A_s:期望系统可用来执行有效服务的程度[4].

$$A_s = \lim_{t\to\infty} A(t) \quad (2)$$

(3)固有可用性 A_0:只考虑设备或系统可服务时间与故障及修复时间,而不考虑其他时间时的可用性,即

$$A_0 = MTBF/(MTBF + MTTR) \quad (3)$$

可维护性:调整、修复和容错的能力,一般可以认为是系统服务失效后在时间间隔 t内被修复的概率. 可表示为:

$$M(t) = P\{X \leq t\} \quad (4)$$

可运行性:对可失效系统性能的量化,可运行性分析通常把系统描述成一组结构状态,每个状态都对应着系统特定的运行能力,并且描述了这些状态之间是如何转换的[5]. 可运行性可表示为 P(L, t),即在 t时刻系统处于 L级别性能得概率. 当 t趋近于无穷时可获得系统的稳态可运行性.

可生存性还没有统一的定义,它是可用性概念的扩展和深化,在文献[6]中认为可生存性是指在遭受攻击、故障或意外事故时,系统能够及时地完成其关键任务的能力. 这里的"系统"有广泛的涵义,包括网络系统以及其他大规模系统.

它可以通过在发生故障后可用资源的比重来度量,假设资源 R受到故障的影响,则期望可生存性 E[R]是在所有出现故障的情况下可用资源的比重,百分比 r可生存性 Rr是资源 R不超过总资源的 r%的概率,零可生存性 R_0 表示资源完全不可用[7].

2.2　可信赖性分析方法

在可信赖性发展的过程中,为了对系统进行可信赖性

的定量和定性分析,人们提出了许多分析方法,它们在不同的层面,从不同的角度描述了系统的特性.这些分析方法主要可以归结为2类:一类是组合法(combinatorial models),另一类是状态法(state-space methods).表1是对这些可信赖性分析方法的归类[8,9].

表1 可信赖性分析方法

组合方法	可靠性框图法(RBD)	
	故障树分析方法(FTA)	
	故障模式影响分析法(FME)	
状态方法	基于马尔可夫过程的方法	马尔可夫回报模型分析法
		马尔可夫更新过程分析法
		补充变量分析法
	基于随机Petri网的方法	广义随机Petri网(GSPN)
		随机回报Petri网(SRN)
		扩展随机Petri网(ESPN)
		确定随机Petri网(DSPN)
		随机高级Petri网(SHLPN)
	基于进程代数的方法	随机进程代数(SPA)

组合法:

可靠性框图法(Reliability Block Diagrams, RBD):不但可以直观的表示系统各组件间的逻辑关系,而且还能描述系统随线形时间的变化情况[8].因此,它常被用来对系统的可靠性和可用性建模[10,11].

故障树分析法(Fault Trees Analysis, FTA)[12]:是用由各种逻辑门组成的树状的结构来表示基本器件与系统之间故障的逻辑关系,经常使用的逻辑门有与门、或门和k/n门.没有共享节点的故障树与可靠性框图法等价[11].

故障模式与效应分析法(Fault Mode Effect Analysis, FMEA):这是一种"自下向上"由因到果的逻辑归纳法,是一种定性的分析方法.

组合模型的方法对随机行为的表达能力有限,基于状态的随机方法可以表达更为复杂的模型关系(如文献[13]).它们的理论基础是概率论、随机过程和数理统计,并且在对其的研究过程中,常常需要考虑用到备种概率分布,如泊松分布、指数分布、威布尔分布等.

状态法:

Markov过程是前苏联数学家发现的,在1951年被引入到可信赖性的分析中来[1].马尔可夫回报模型(Markov Reward Model, MRM)[10]:它可以通过将连续时间马尔可夫链(CTMC)状态之间的转移赋以回报率来定义.

马尔可夫更新过程分析法[14],在马尔可夫过程、以及在半马尔可夫过程中选择合适的再生点,对于研究系统的可信赖性方法简便.

补充变量分析法:这是研究非马尔可夫型可修系统的一个重要方法,它是通过引进补充变量,使要讨论的问题变为一个广义的马尔可夫过程.然后,利用初始条件,建立微分方程,从而求出有关的可信赖性指标.

Petri网模型可以很好的描述系统的并行、异步、分布等特性.尤其是引入随机延迟时间后,所得到的随机Petri网(Stochastic Petri Net, SPN)[15]更是成为研究随机系统可信赖性的强有力的手段.有关随机Petri的情况,本文将在下节作详细介绍.

随机进程代数(SPA)[23]为性能评价提供了非常特殊的解决方案:它将组件进行的活动抽象为一个进程;而且能够通过等价定理自动化减状态空间,它主要用来描述和研究资源共享系统的可信赖性.由于SPA方法的理论基础与传统的形式化方法不同,因此这种方法有待于进一步完善.状态空间压缩、随机模型检测[24]是SPA当前的研究重点.

表2给出了组合法与状态法在描述能力、模型结构、计算量和约束条件几个方面的比较:

表2 组合方法与状态方法的比较

	组合方法	状态方法
描述能力	描述能力弱,但模型表达清晰,容易理解	描述能力强,但不容易理解
模型结构	简单	复杂
计算量	计算量小	计算量大
约束条件	基本事件之间应在统计意义上独立且基本事件间的逻辑关系确定	无独立条件约束,但需已知系统各状态的时间分布(一般为指数分布)

前面介绍并比较了各种可信赖性研究方法,本文主要研究基于随机Petri网的可信赖性分析方法,为了便于理解,下面将对随机Petri网作以简单介绍,详细情况请参阅文献[29, 51].

2.3 随机Petri网

随机Petri网以研究模型系统的组织结构和动态行为为目标,着眼于系统中可能发生的各种状态变化以及变化之间的关系.它描述的是系统的动态变化过程.Petri网模型以图形的方式来表示一个复杂系统,它的结构元素包括位置(Place)、变迁(Transition)和弧(Arc).位置用于描述可能的系统局部状态(条件或状况).变迁用于描述系统状态改变的事件.弧使用两种方法规定局部状态和事件之间的关系:他们引述事件能够发生的局部状态;由事件所引发的局部状态的转换.

在随机Petri网模型中,位置可能含有任意数量的标记(Token).随着事件的发生,标记可以在不同的位置中按照弧的方向流动,从而动态的描述了系统的不同状态.一个Petri网模型的动态行为是由它的实施规则(Firing rule)规定的.每个变迁有相应的输入位置和输出位置.输入位置定义为所有的与该变迁之间有弧连接并且弧的方向从位置到变迁的位置(相应弧称为输入弧).而输出位置与它的弧的方向与输入位置不同,它是从变迁到位置.如果一个变迁的每个输入位置中至少包含相应输入弧上标注数量的标记时,那么这个变迁就成为一个可实施的变迁.变迁的真正实施从它成为可实施起要经过一个随机的时间.

一个可实施的变迁的实施导致从它所有输入位置中清除相应输入弧上标注数量的标记,在它的每一个输出位置中产生相应输出弧上标注数量的标记.在输入位置中清除标记和在输出位置中产生标记是一个不可分割的完整操作.由于变迁的实施会使标记在位置中流动,因此在不同的时刻,标记在各个位置中的分布是不同的,我们定义这种不同的分布为标识 (Marking).标识就相当于系统所处的状态 (State).

在不断的研究过程中,随机 Petri网得到了很大的发展和扩充.如:可简化系统状态空间的广义随机 Petri网 (Generalized Stochastic Petri Net, GSPN)[16];变迁实施时间为一般分布的扩展随机 Petri网 (Extended Stochastic Petri Net, ESPN)[17];利用嵌入离散时齐马氏链的确定和随机 Petri 网 (Deterministic and Stochastic Petri Net, DSPN)[18];用回报形式表达系统性能测量的随机回报网 (Stochastic Reward Net, SRN)[19]以及将指数分布的变迁实施时间变量引入到高级 Petri网中的变迁集中的随机高级 Petri网 (Stochastic High level Petri Net, SHLPN)[37~39].

利用随机 Petri网的有关理论对容错系统的可信赖性问题进行建模,并通过随机 Petri网与马尔可夫过程同构的特性,可以求解容错系统的可信赖性参数.而直接使用马尔可夫模型,却很难对马尔可夫模型进行扩展.例如在实际系统中,一旦系统的资源增加或减少,相应的马尔可夫链的结构就可能会发生很大的变化,而在随机 Petri网模型中,只要通过增加相应位置中的标记数就可以建立相应的模型.并且随机 Petri网可以在一个系统模型的框架上采用图形化的方式完成系统的描述、可信赖性分析以及系统的验证和测试.这是其他的方法所不具备的功能.

另外,随机 Petri网在很多方面的发展已很完备,它已有很多成熟的、有效的软件工具,可大大简化使用者进行建模和求解的过程.如:ESPN, GreatSPN, SPNP, SURF-2, TOMSPIN, UltraSAN 等,因此,它是大型复杂网络系统可信赖性分析的有力工具[20].

3　随机 Petri网可信赖性分析方法

3.1　分析方法及主要步骤

网络作为一个非静态的开放的系统必须与人、环境以及其他系统等外在事物发生动态的关系.在不确定的、复杂的各种外部因素的影响下,网络系统不可能永远稳定、可靠地运行.分析网络系统的可信赖性先要建立系统的可信赖性模型,而建立可信赖性模型可以从以下的几个方面入手,首先要建立系统的性能模型,它描述了理想无失效发生时系统的结构和性能的情况,二是对可能出现失效的资源建立失效模型和容错模型.它用来描述部件失效的过程及失效后的反应.这其中引起网络服务失效的原因很多,可能是网络结构设计的问题;管理或操作中的问题;也可能是由于外来恶性攻击而造成的.最后将前面的两者相结合建立网络系统可信赖性模型,它描述了在一个特定的网络结构中某些资源失效后对整个系统所带来的影响,根据可信赖性模型计算各种可信赖性参数,就可综合分析一个网络系统的可信赖程度.

应用随机 Petri网分析系统可信赖性,可以按照以下步骤进行:

步骤 1:针对特定系统建立描述系统性能的 SPN 模型;

步骤 2:建立系统的容错 SPN 模型,它描述了资源的服务失效和修复的过程;其中可能发生失效的资源与前面性能模型的相应位置对应;

步骤 3:合并这两个模型生成系统可信赖性模型;

步骤 4:精化 SPN 模型结构,求出可达图及相应马尔可夫链;

步骤 5:计算各状态瞬态和稳态概率,从而求出各种可信赖性指标.

随机 Petri网描述系统功能结构和建立系统性能模型的方法可参阅 [29, 51],本文将重点研究服务失效模型和容错模型以及对其可信赖性指标的求解方法.

3.2　服务失效模型

服务失效模型描述了系统由正常服务状态到服务失效状态的变化过程中错误和故障发生的情况.下图列举了网络系统中发生服务失效的几种典型结构.复杂系统的失效情况,通常包含这些基本结构.

图 2～4分别描述了由于资源节点出现问题 (可能由于资源内部故障也可能由于外部的攻击),使得简单结构、串联结构和并联结构的系统发生服务失效的情况.其中,白色的长方形表示事件变迁,黑色的长方形为瞬时变迁. up_i 表示正常服务状态; $down_i$ 表示服务失效状态; p_i, q_i 表示某些中间状态; failure 表示引起服务失效的事件,它对应的失效速率为 λ_i, T 表示引起状最终态迁移的事件.

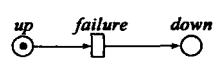

图 2　简单结构

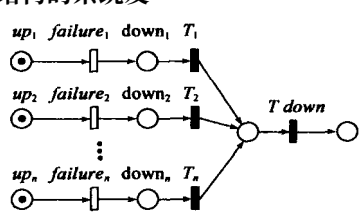

图 3　串联结构

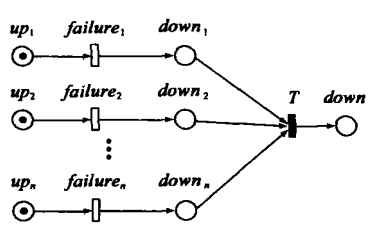

图 4　并联结构

另外,可以通过在变迁处设置不同的谓词,使得同样的模型描述不同的失效过程.如:在图 4中,如果 T处的谓词为 n - j < k(其中 n为部件总数, j为失效部件数),表示当正常部件小于 k时,服务失效;如果将变迁 T中的谓词表示

为 (n - j < s) (n - j > r),则表示当正常工作的部件大于 s 小于 r时,服务失效.

除了由于资源故障导致的服务失效外,系统结构设计中的错误以及对系统的某些操作也可能会导致系统的某些服务失效.如:图 5所示的死锁结构中 T_1、T_2 事件无法处于有效状态.图 6描述了由于两个服务同时启动,造成两个服务 t_1、t_3 全部失效;图 7描述了正在进行中的服务 t_1,资源被抢占致使服务失效的过程.

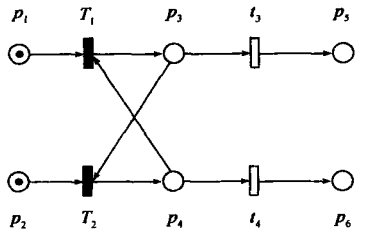

图 5 死锁结构

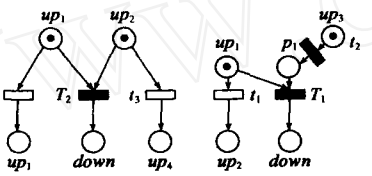

图 6 冲突结构 A 图 7 冲突结构 B

将服务失效模型放在具体的网络环境中,便得到了系统可信赖性的随机 Petri网模型,将其可达图中每条弧上标注的实施变迁 t_i 换成其平均实施速率 λ_i (或与标识相关 λ_i 的函数),则可得到与 SPN 模型同构的马尔可夫链 (MC),应用求解马尔可夫过程方法可对模型进行求解.

3.3 可修复系统容错模型

对于出现故障、错误而导致服务失效的系统,通常的容错方法是要经过修复才能恢复原来的工作.在可修复系统中,通常考虑的可信赖性模型是可信赖性增长模型.假设失效率或者失效强度单调地减小,并随时间的增加趋近于零.在文献 [21]中介绍了 S型模型,表示初始值随着可信赖性的增加而减小;文献 [20]介绍了超指数的模型,表示可信赖性增加并最终趋于稳定.

大多数的失效率模型假设系统行为是一个泊松过程,这些模型通常假设每个失效事件伴随着一个修复 恢复的过程,并且认为恢复与修复之间的关系可以在很大范围内变化.首先应该对两个极端情况做出限制:

(1)在每次失效发生后,对系统进行修复,而只有在修复之后系统才恢复正常工作能力.

(2)修复与失效之间的关系不是确定的,而是由一个特定随机过程所决定的.

这两种情况被认为分别与关键系统 (critical system) 和非关键系统 (non-critical systems)相关联.关键系统是指系统的故障往往会引起重大的生命、财产损失的系统[22],反之为非关键系统.最后,我们假设修复和恢复过程不是随时间变化的,对应的随机变量是随机同分布的.

3.3.1 单部件可修复系统模型 确定失效率模型是泊松过程[20],其可修复模型对应的是多状态马尔可夫链.下面给出了关键系统的 SPN 模型如图 8所示[20].图中失效变迁 $failure_{1,\cdots,r}$ 对应实施速率 $\lambda_{1,\cdots,r}$,互相独立,且 $\lambda_{1,\cdots,r}=\lambda_j$,$\lambda_j = f(m(C)) = m(C) + 1 - r$,其中 m(C)表示位置 C的标识数量,修复变迁 repaire对应的实施速率为 μ,其相应的马尔可夫链如图 9所示,其中 $U_1, U_2, \cdots, U_r$ 表示系统有效状态;$D_1, D_2, \cdots, D_r$ 表示系统的无效状态,假设在 r 个修复事件发生后,模型趋于一个泊松过程:失效发生的顺序是 $\{\lambda_1, \lambda_2, \cdots, \lambda_r\}$.进一步假设修复 恢复过程是一个以速率为 μ的泊松过程.

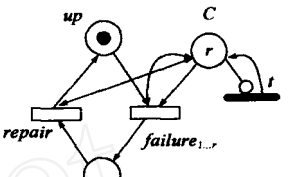

图 8 关键系统的 SPN模型

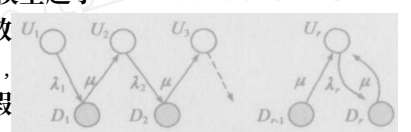

图 9 关键系统的多状态 MC

类似的可以得到非关键系统的 SPN 模型和相应的状态转移马尔可夫链分别如图 10、11所示.图中 v表示修复的速率,失效变迁 $failure_{1,\cdots,r}$ 对应实施速率 $\lambda_{1,\cdots,r}$ 互相独立,且 $\lambda_{1,\cdots,r}=\lambda_j$,$\lambda_j = f(m(NV)) = m(NV) + 1$,其中 m(NV)表示位置 NV 的标识数量,修复变迁 repaire 对应的实施速率为 μ

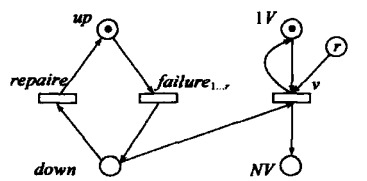

图 10 非关键系统的 SPN模型

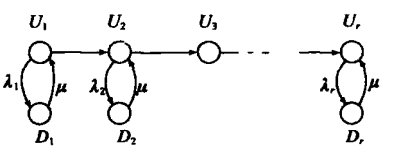

图 11 非关键系统的多状态 MC

3.3.2 多部件可修复系统模型 当系统各部件间相互随机独立时,可分别应用单部件修复模型建模组合求解.在大多数现实系统中,系统各部件在功能上明显的存在随机依赖性.这些依赖性可以由随机 Petri网进行模拟,实现服务过程中同步与协作.

下面我们在上节单部件可修复模型基础上,分别对关键系统多部件串联和并联的可修复系统的可信赖性模型进行说明.

(1)串联系统

组成串联系统的任何部件功能失效都将导致系统服务失效,而只有当所有部件正常工作时,系统才处于正常工作状态.设串联可修复系统有 n个部件组成,每个部件失效率和修复率分别为 $failure_i = \lambda_i$,$repaire_i = \mu_i$ (i = 1, 2, ⋯, n).设 X(t)为系统状态空间,则

$$X(t) = \begin{cases} 0, & \text{时刻 } t\text{系统正常工作} \\ i, & \text{时刻 } t\text{部件 } i\text{故障}, i = 1, \cdots, n\text{系统失效} \end{cases}$$

可得到随机 Petri模型如图 12所示,并通过分析状态转移的情况得到相应的马尔科夫链如图 13所示.

(2)并联系统

组成并联系统的部件中任何一个部件功能失效都不会导致系统功能的失效,而只有当超过系统正常运行所需要数量个部件功能失效时,系统才处于服务失效状态.假设在同一时刻没有两个或两个以上的部件失效,且任一时刻也不会有两个或多个部件被修复.并联可修复系统由 n个部件组成,为描述方便,设每个部件的失效率和修复率分别相同,且 $failure_i = \lambda$、$repaire_i = \mu$ 设 X(t)为系统的状态空间,则

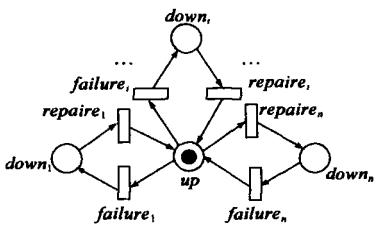

图 12　串联可修复系统的 SPN 模型

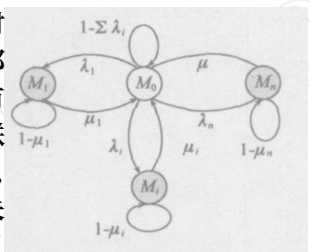

图 13 串联可修复系统的 MC

$$X(t)=\begin{cases} i, & i=1,\cdots,n-1,\text{时刻 } t\text{系统正常工作} \\ n, & \text{时刻 } t\text{系统处于服务失效状态} \end{cases}$$

可得到随机 Petri模型如图 14所示,并通过分析状态转移的情况得到相应的马尔科夫链如图 15所示.

3.4　冗余备份系统容错模型

对于关键系统,除了对故障资源要及时采取修复措施外,增加冗余备份资源是提高系统可用性最常采用的策略之一.这样可以使系统在出现故障的时候仍能维持正常功能,当工作部件发生故障后,可以用备份部件来代替有故障的部件而使系统能够维持正常工作.按备份部件所处状态的不同,冗余备份系统主要有三种形式:冷备份、温备份和热备份.冷备份是指备用部件处于完全不工作状态,并假设它的失效率为零.温备份系统指备用部件与主部件处于完全相同的工作状态下,但备用部件相对于主部件处于轻载荷工作状态,其失效率较主部件的小.而在热备份系统中,两者的失效率相同[25].

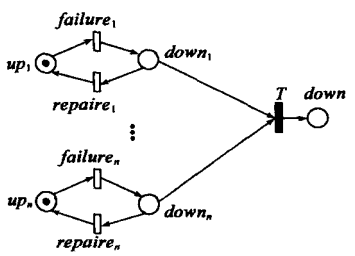

图 14　并联可修复系统的 SPN 模型

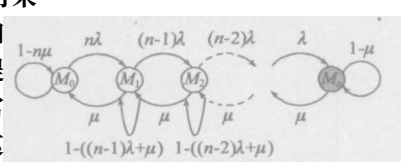

图 15　并联可修复系统的 MC

在实际的网络环境中可根据资源类型的不同,设置不同的冗余结构.如管理员服务器单元、数据库服务器单元和通信服务器单元为暖备份双机冗余系统,计算节点单元为 (k/n)表决冗余系统.双机冗余系统实际上也是 (1/2)表决冗余系统.因此,系统各单元部分的冗余容错模型均可归结为 (k/n)表决冗余系统.

在 k/n冗余备份系统分析方面,国内外许多学者已经作了一些研究,文献 [26]给出了一种即包含冷备份冗余和热备份冗余的 k/n系统可用性模型,该模型考虑了部件失效后立即进行维修的情况;文献 [27]给出了一种考虑在给定初始冷备份部件数、修复策略以及维修能力条件下的 k/n热备份冗余系统可用性模型.

下面我们用随机 Petri网描述通用 k/n冗余备份系统模型如下图所示,图 16是冷备份系统,图 17是温备份和热备份系统.

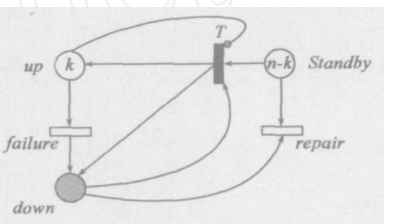

图 16　冷备份系统的 SPN 模型

此外,某些 k/n热备份冗余系统还备有 S个冷备份冗余部件,当系统的可用部件数量小于 k时,冷备份的部件可以代替工作,即该类系统属于一种热备份和冷备份共存的冗余系统,热备份冗余部件数即为 n - k并且某些 k/n系统在完成不同的阶段任务条件下 k可能是不同的.对于这类系统,系统的任务可用性不仅仅和热、冷备份冗余部件数和任务时间有关,还和系统经历的阶段任务的类型有关.

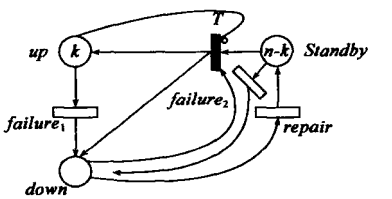

图 17　温备份、热备份系统的 SPN 模型

3.5　可信赖性参数求解

完成随机 Petri网对系统的可信赖性建模之后,便可根据可达图获得与 SPN 模型同构的 MC.假设 MC中可达标识集 $[M_0>$有 n个元素,即 MC有 n个状态.

定义状态转移矩阵 $Q=[q_{ij}]$,其中 Q 的非对角线上的元素 q_{ij},$(i\neq j)$可以这样获得:当从状态 M_i 到状态 M_j 有一条弧相连时,则弧上标注的速度即是 q_{ij}的值,如果没有弧从状态 M_i 到状态 M_j 相连时,则 $q_{ij}=0$. Q 的对角线上的元素 q_{ii}等于从状态 M_i 输出的各条弧上标注速率之和的负值.

设 MC中 n个状态的稳定状态概率是一个行向量 $\Pi=(\pi_1,\pi_2,\cdots,\pi_n)$,根据马尔可夫过程有下列线性方程组

$$\begin{cases} \Pi\times Q=0 \\ \sum_{i}^{n}\pi_i=1 \end{cases} \tag{5}$$

解此线性方程组,即可得每个可达标识的稳定概率 $P_i(t=\infty)=\pi_i(1\leq i\leq n)$.

另一方面,我们也可以直接列出所有平衡状态方程,对于任一标识 $M_i\in[M_0>$,所有 $M_j,M_k\in[M_0>$且 $M_i\in$

$[t_j > M_j, M_k \in [t_k > M_i$,则有方程

$$\left(\sum_k \lambda_k\right)_i = \sum_k \lambda_{k\ k} \tag{6}$$

显然,我们可以列 n - 1个齐次方程,含有 n个未知变量,因此可以用上式列出 n - 1个平衡状态方程,再加上方程 $\sum \lambda_j = 1$,即可求解每个可达标识的稳定概率. 在求得稳定概率的基础上,便可以进一步分析人们关心的稳定状态的可信赖性参数.

下面以图 12所示的串联可修复系统和图 14所示的并联可修复系统为例介绍可靠性、可用性、MTTR、MTBF以及可运行性的求解.

根据图 13的 MC及前诉方法可获得状态转移矩阵

$$Q = \begin{bmatrix} \Lambda & \lambda_1 & \cdots & \lambda_n \\ \mu_1 & -\mu_1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ \mu_n & 0 & \cdots & -\mu_n \end{bmatrix}$$

其中 $\Lambda = -\sum_i^n \lambda_i$,根据方程组 (4)可求得 $t \to \infty$时的稳态概率

$$\begin{cases} {}_0 = \left[1 + \sum_{i=1}^n \dfrac{\lambda_i}{\mu_i}\right]^{-1} \\ {}_i = {}_0 \dfrac{\lambda_i}{\mu_i}, \quad i = 1, \cdots, n \end{cases} \tag{7}$$

(1)可靠性

求解可靠性时,可不必求解方程 (1)的所有解,无论不可修复系统还是可修复系统,我们都可以假设系统有 n个状态,前 t个连续的正常工作状态是非吸收态,后 a个状态为吸收态 (故障态). 这样我们只需考虑系统的处于吸收状态时的可靠性. 即

$$R(t) = P_0(t) = \exp(\Lambda t) = \exp\left(-\sum_i^n \lambda_i\right) t \tag{8}$$

(2)MTTF

当部件失效服从指数分布时,$\lambda = \sum_i^n \lambda_i$ 则

$$MTTF = \int_0^\infty R(t)\,dt = \int_0^\infty \exp\left(-\sum_{i=1}^n \lambda_i t\right) dt = \lambda^{-1} \tag{9}$$

也可以用在 M_0 中驻留的时间表示.

(3)可维护性

为求得系统的可维护性 M(t),先定义系统的修复率 μ(t),它表示修理时间已达到某个时刻但尚未修复的资源,在该时刻后的单位时间内完成修复的概率,可用数学表示为

$$\mu(t) = \frac{1}{1 - M(t)} \frac{dM(t)}{dt} \tag{10}$$

则由式 (9)可得

$$M(t) = 1 - \exp\left(-\int_0^t \mu(t)\,dt\right) \tag{11}$$

当 μ(t)为常数时,式 (11)可写为

$$M(t) = 1 - \exp(-\mu t) \tag{12}$$

(4)MTTR、MTBF

系统的平均修复时间可表示为

$$MTTR = \lambda / \rho = \sum_{i=1}^n \lambda_i \Big/ \sum_{i=1}^n (\lambda_i / \mu_i) \tag{13}$$

其中,$\rho = \sum_i^n \rho_i$,为系统维修系数,$\rho_i = \lambda_i / \mu_i$ 为第 i个部件的维修系数.

平均故障间隔时间 MTBF可近似等于正常工作时间与在此段时间内故障次数之比,即

$$MTBF = t / N_f(t) \tag{14}$$

(5)可用性

系统的稳态可用性为状态 M_0 的稳定概率

$$A_s = {}_0 = \left(1 + \sum_{i=1}^n \frac{\lambda_i}{\mu_i}\right)^{-1} = \left(1 + \sum_{i=1}^n \rho_i\right)^{-1} = (1 + \rho)^{-1} \tag{15}$$

固有可用性

$$A_0 = MTBF / (MTBF + MTTR) = \left(\sum_{i=1}^n (\lambda_i / \mu_i) + 1\right)^{-1} \tag{16}$$

(6)可运行性

在图 14所示的并联系统中,系统的稳态可运行性 P(L)可由稳态时 n - L个部件处于失效状态的概率表示.

图 15的 MC对应的状态转移矩阵为

$$Q = \begin{bmatrix} -n\lambda & n\lambda & \cdots & 0 & 0 \\ \mu & -[\mu + (n-1)\lambda] & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & 0 & 0 \\ 0 & 0 & \cdots & -(\mu + \lambda) & \lambda \\ 0 & 0 & \cdots & \mu & -\mu \end{bmatrix}$$

根据方程组 (2)可解得 $t \to \infty$时的稳态概率

$$\begin{cases} {}_0 = \left(\sum_{m=0}^n (n!\ /\ (n-m)!)\ (\lambda/\mu)^m\right)^{-1} \\ {}_i = {}_0 ((n!\ /\ (n-i)!)\ (\lambda/\mu)^i), \quad i = 1, \cdots, n \end{cases} \tag{17}$$

则可运行性为

$$P(L) = {}_{n-L}, \quad L = 0, \cdots, n) \tag{18}$$

(7)可生存性

根据前面给出可生存性的定义和式 (16)的计算结果可以获得图 14所示系统的期望可生存性

$$E[R] = \sum_{i=0}^n \frac{n-i}{n} {}_i \tag{19}$$

同样,可以求得零可生存性和百分比 r可生存性

$$R_0 = {}_n \tag{20}$$

$$R_r = \sum_{i \le n \cdot r\%} {}_i \tag{21}$$

4 存在的问题分析

前面介绍了随机 Petri对系统可信赖性的建模和求解方法. 可以看出随机 Petri网是一种灵活有力的建模机制,在可信赖性建模方面也已形成了较为成熟的理论体系,但在实际应用中仍存在不少的局限性,主要有两方面:状态空间爆炸和变迁触发时间服从指数分布的假设

问题.

4.1 状态爆炸问题

随机 Petri网模型的状态空间大小随模型中位置、变迁等建模元素的增长呈指数级增长,导致所谓状态空间爆炸问题或维数灾难问题,严重限制着此类建模机制在现实中的应用.状态空间爆炸问题不仅关系到数值方法求解的可行性,而且影响到仿真方法分析的精确度.解决状态空间爆炸问题的一种主要途径是采用组合与分解的方法,组合与分解可以在网层进行[28],通过构建层次化模型,有助于理解系统各部分之间的交互关系,有助于开发模块化或基于组件的系统设计,层次化模型还可以更简洁地描述系统.对于每个独立子模型可单独求解,其结果被逐层传递到更高一级子模型,直至总模型.典型的方法如:状态截断法[30]、分层模型方案[31]、不动点重复法[32]以及混合方法[31]等.这种思想可以体现在不同的层面.

状态级的结块技术 (state level lumping)[33]已被广泛的使用,它是通过合并马尔可夫链的等价状态,减小状态空间的规模.状态空间被表示成子空间 Kronecker乘积的和,在子空间之间的转移率很小(接近无关)的情况下,用不动点重复法可求解模型[34],这类方法能给出较为准确的结果,但仅适用于那些不是太强连接的大型随机系统. Buchholz在文献[35]给出了一个算法,它的时间复杂度为 O(mn),空间复杂度为 O(m + n)其中 n是状态的数,m是转移数. Derisavi等人在文献[36]中提出了复杂度为 O(m logn)的 lumping算法,并给出了严格的证明.

模型级结块技术 (model level lumping)[9],在对系统建模的时,利用系统动态行为的对称性,将潜在马尔科夫链的状态空间化简为等价类空间,不需要产生完整的可达图,直接在等价类空间上进行计算.这样既保持了良好的模型特性和模型的可读性,又可以简化系统的状态空间,依照这种思想,文献[37～39]提出了随机高级 Petri网(SHLPN);后来又出现了着色随机 Petri网(CSPN)[40]、着色广义随机 Petri网(CGSPN)[41]和正规随机 Petri网[42]等.

具有乘积形式平稳分布的排队网络具有非常有效的求解方法.为了克服状态空间爆炸问题,很多文献研究了具有乘积形式解的随机 Petri网(Product-Form SPN)的求解方法,以及为不具有乘积形式解的随机 Petri网寻求近似的乘积形式解.文献[43]提出的方法不需产生可达图,直接根据模型结构判断是否存在乘积形式解;文献[44]给出了这类模型的完整特征;文献[45]说明可将满足一定结构条件的广义随机 Petri网转化为乘积形式随机 Petri网.另外,文献[63]介绍了将非乘积解随机 Petri网转化成乘积形式近似求解方法,使随机 Petri网的已有结论可以推广到更一般的情形,应用范围更广.

解决状态空间爆炸问题的其他途径主要有寻求性能指标的上下边界值[46]、利用分布式算法[47]以及忽略概率值较小的状态的约简方法等.

4.2 非马尔可夫随机 Petri网

指数分布特有的马尔可夫性能给随机 Petri网求解带来了很大的方便,但现实系统中存在大量活动,它们的持续时间为确定的或服从其他概率分布,勉强用指数分布来近似这些活动的非指数分布持续时间得到的结果往往不能准确反映真实情况.

非马尔可夫随机 Petri网 (Non-Markovian Stochastic Petri Nets, NMSPNs)[48]是用来描述非马尔可夫模型的,现在已有一些文献提出了一些分析 NMSPNs的技术.如:补充变量分析方法[49], Phase-type分布 (Phase-Type Distribution)近似方法[50],基于模型分解和迭代的近似性能分析技术[51],以及马尔可夫再生理论[52]. NMSPNs根据求解技术的不同可以分为扩展的随机 Petri网 (Extended Stochastic Petri Nets, ESPNs)[53],允许变迁的实施时间取确定值的确与随机 Petri网 (Deterministic and Stochastic Petri Nets, DSPNs)[54],含有 PH分布变迁的随机 Petri网 (Stochastic Petri Nets with Phase-Type Distributed Transitions, ESPs)[55],马尔可夫再生随机 Petri网 (Markov Regenerative Stochastic Petri Nets, MRSPNs)[56]等.实际上这也是 NMSPNs的演变过程,变迁的实施时间分布函数从指数分布扩展到确定和指数分布, PH分布,最后到更一般的情况,变迁的实施时间可取任意的概率分布[56],这种变迁叫一般变迁.

马尔科夫再生随机 Petri网可用来研究多相系统 (Multiple-Phased Systems, MPS)的可信赖性分析[57]. MPS的任务必须按一定的顺序执行,各任务的生命周期彼此不重叠.同时已有一些基于 DSPN和马尔可夫更新过程的针对多相系统的可信赖性建模和分析的工具,如 DEEM (DEpendability Evaluation of Multiple-phased systems)[58,59].

另一种较普遍采用的方法是辅助变量法[60],即在系统状态描述中加入一个连续变量,用于表示非指数变迁的相应时间,使得描述系统动态行为的随机过程仍然是马尔科夫随机过程.还可以采用连续时间或离散时间相型分布(Phase Type Distribution)近似各种非指数分布[62],通过在扩张的状态空间上定义的马尔科夫链近似原来的非马尔科夫随机过程,但这种方法会引起状态空间的急剧膨胀,增加了方程组求解的难度.

5 总结与展望

可信赖性研究作为一项重要的研究领域,正受到越来越多的关注.本文对可信赖性分析技术尤其是应用随机 Petri网研究网络系统的可信赖性进行了研究.文章首先给出了网络系统中可信赖性的定义,并对可信赖性分析中人们所关心的可用性、可靠性、可运行性、可维护性和可生存性等各项可信赖性指标作了介绍.并在此基础上对可信赖性分析技术进行了分类和总结.可信赖性分析技术主要有组合法和状态法两种,它们在描述能力、计算量、应用条件

和应用范围等方面都存在着自己的优势和不足.

与其他方法相比随机 Petri网对系统各个状态间的逻辑关系和动态变化过程具有极强的描述能力,尤其是对复杂的可修复系统进行建模时,随机 Petri网与传统的状态空间法相比较更实用、更简便、更清晰、可读性更强.本文介绍了随机 Petri网对网络系统可信赖性建模分析的方法和步骤,着重研究了随机 Petri网描述系统的服务失效模型和容错模型,并给出了网络系统可信赖性分析中主要指标的求解方法.随机 Petri网为大型复杂动态系统的可信赖性分析提供了很好的模型和求解方法,并在很多应用中都取得了很好的效果[63],具有广阔的应用前景,但仍存在一些有待解决的问题:

(1)如何将实际网络系统可信赖性问题化成可以用随机 Petri网描述和分析的问题,并通过随机 Petri网的求解结果获得更多人们关心的可信赖性指标.这依赖于设计者对网络结构的分析能力,以及对可信赖性问题和随机 Petri网理论的理解和掌握的程度.

(2)对造成网络系统中资源服务失效情况的分析,深入研究在复杂环境中可能导致资源失效的内部故障和外部攻击的情况及影响.

(3)如何将已有的可信赖性理论的优势体现在随机 Petri网模型中.研究随机 Petri网及其扩展形式与传统可信赖性研究方法之间的转换方法.

(4)在应用随机 Petri网分解压缩技术解决状态空间爆炸问题时,其误差分析、解的存在性以及解的收敛问题并没有得到理论上的证明,这种技术的理论支持尚待进一步研究.

(5)如何在网络系统可信赖性模型方法的研究中借鉴排队论的研究成果,将非乘积形式的随机 Petri网转化为乘积形式的随机 Petri网进行求解.

(6)增强随机 Petri网的模型能力,加强对非 Markov 过程性能模型的研究,寻求能够对非马尔可夫模型进行更为有效地模型和分析的方法[51].非马尔可夫过程中还有一类非常重要的问题,即自相似问题.目前,这一问题已成为网络可信赖性研究重点[64].

参考文献:

[1] Richard E Barlow. Mathematical theory of reliability: A historical perspective [J]. IEEE Trans on Reliability, 1984, 33(1): 16 - 20.

[2] Algirdas A, Jean-Claude Laprie, Brian Randell, Carl Landwehr. Basic concepts and taxonomy of dependable and secure computing [J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(1): 11 - 33.

[3] A Avizienis, J Laprie, B Randell, Fundamental Concepts of Dependability [R]. LAAS-CNRS, N01145, Apr. 2001.

[4] Gene J Schroeder, Marvin J Johnson. Complex availability: The new availability problem [A]. Reliability and Maintainability Symposium, 1990. Proc [C]. 1990. 268 - 274.

[5] G Bolch, S Greiner, H de Meer, K S Trivedi. Queueing Networks and Markov Chains [M]. New York: John Wiley & Sons, 1998.

[6] Ellison R, Fisher D, Linger R, et al. Survivable network systems-An emerging discipline [R]. Pittsburgh, Software Engineering Institute, Carnegie Mellon University, 1997.

[7] Yun Liu, Kishor S Trivedi. A General Framework For Network Survivability Quantification [M]. 3rd Polish-German Teletraffic Symposium, 2004.

[8] Manish Malhotra, Kishor S Trivedi. Power-hierarchy of dependability-model types [J]. IEEE Trans on Reliability, 1994, 43(3): 493 - 501.

[9] David M Nicol, William H Sanders, Kishor S Trivedi. model-based evaluation: From dependability to security [J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(1): 48 - 65.

[10] K S Trivedi. Probability and Statistics with Reliability, Queuing, and Computer Science Applications [M]. second ed. New York: John Wiley and Sons, 2001.

[11] M L Shooman. Probabilistic Reliability: An Engineering Approach [M]. seconded. Malabar, Fla: R. E. Krieger Publishing Co., 1990.

[12] W S Lee, D L Grosh, F A Tillman, C H Lie. Fault tree analysis, methods, and applications-A review [J]. IEEE Trans on Reliability, 1985, 43(3): 194 - 203.

[13] J K Muppala, M Malhotra, K S Trivedi. Markov Dependability Models of Complex Systems: Analysis Techniques, Reliability and Maintenance of Complex Systems, S. Ozekici, ed., Germany: Springer, 1996. 442 - 486.

[14] Andrea Bondavalli, Silvano Chiaradonna, Felicita Di Giandomenico, and Ivan Mura, Dependability Modeling and Evaluation of Multiple-Phased Systems Using DEEM, IEEE TRANSACTIONS ON RELIABILITY, 2004, 53(4): 509 - 522.

[15] LIN Chuang, Marinescu DC. Stochastichigh-level Petri nets and applications [J]. IEEE Transactions on Computers, 1988, 37(7): 815 - 825.

[16] Marsan M A, Conte G, et al. A class of generalized petri nets for the performance evaluation of multi processor system [J]. ACM Trans Computer Syst, 1984, 12(2): 93 - 122.

[17] J B Dugan, V Nicola, R Geist, K Trivedi. Extended stochastic petri nets: Applications and analysis [A]. Proc Conf Performance'84 [C]. 1985. 507 - 519.

[18] M A Marsan, G Chiola. On Petri nets with deterministic and exponentially distributed firing times [J]. Advances in Petri Nets, LNCS, vol 266, Springer, 1987: 132 - 145.

[19] Ciardo G, Blakemore A, Chimento P F, Muppala J K,

Trivedi K S. Automated generation analysis of Markov reward models using stochastic reward nets. In: Meyer C, Plemmons R J (ed.). Linear Algebra, Markov Chains, and Queueing Models, IMA Volumes in Mathematics and its Applications, Springer-Verlag, 1993, 48: 145 - 191.

[20] Laprie J-C, Kaaniche M, Kanoun K. Modeling computer systems evolutions: non-stationary processes and stochastic Petri nets-application to dependability growth, Petri Nets and Performance Models[A]. 1995, Proceedings of the Sixth International Workshop on 3-6 Oct [C]. 1995: 221-230.

[21] S Yamada, S Osaki. Software reliability growth modeling: models and assumptions[J]. IEEE Trans on Software Engineering, SE-11, 1985. 1431 - 1437.

[22] Papadopoulos Y, McDermid J A. The potential for a generic approach to certification of safety critical systems in the transportation sector[J]. Reliability Engineering and Systems Safety, 1999, 63(1): 47 - 66.

[23] LIN Chuang, WEI Ya Ya. Stochastic process algebras and stochastic petri nets[J]. Journal of software, 2002, 13(2): 203 - 213.

[24] H Hermanns, J-P Katoen, J Meyer-Kayser, M Siegle. Towards model checking stochastic process algebra[A]. W Grieskamp, T Santen, B Stoddart 2nd Int Conference on Integrated Formal Methods [C]. Dagstuhl: Springer, 2000, LNCS 1945. 420 - 439.

[25] JIANG L T, XUE G Z, YING R D, et al. Application of stochastic petri net to system availability analysis[J]. Journal of System Simulation, 2002, 14(6): 796 - 799.

[26] Frostig E, Levikson B. On the availability of R out of N repairable systems[J]. Naval Research Logistics, 2002, 49(5): 483 - 498.

[27] De Smidt-Destombes K S, Van der Heijden M C. On the availability of a k-out-of-N system given limited spares and repair capacity under a condition based maintenance strategy[J]. Reliability Engineering and System Safety, 2004, (83): 287 - 300.

[28] P Buchholz. A Hierarchical View of GCSPNs and Its Impact on Quantitative and Quantitative Analysis[J]. Parallel and Distributed Computing, 1992, 15: 207 - 224.

[29] LIN C. Stochastic Petri Nets and System Performance Evaluation [M]. Beijing: Tsinghua University Press, 2005. 1 - 137.

[30] D Chen, D Selvamuthu, D Chen, L Li, R R Some, A P Nikora, K Trivedi. Reliability and Availability Analysis for the JPL Remote Exploration and Experimentation System [A]. Proc Int'l Conf Dependable Systems and Networks[C]. 2002. 337 - 344.

[31] R A Sahner, K S Trivedi, A Puliafito. Performance and Reliability Analysis of Computer Systems: An Example-Based Approach Using the SHARPE Software Package [M]. Kluwer Academic Publishers, 1996.

[32] V Mainkar, K Trivedi. Sufficient conditions for existence of a fixed point in stochastic reward net-based iterative models[J]. IEEE Trans Software Eng, 1996, 22(9): 640 - 653.

[33] P Buchholz. Exact and ordinary lumpability in finite markov chains[J]. J Applied Probability, 1994, 31: 59 - 74.

[34] P Kemper. Numerical analysis of superposed GSPNs [J]. IEEE Transactions on Software Engineering, 1996, 22: 37 - 49.

[35] P Buchholz. Efficient computation of equivalent and reduced representations for stochastic automata[J]. Int'l J Computer Systems Science & Eng, 2000, 15(2): 93 - 103.

[36] S Derisavi, H Hermanns, W H Sanders. Optimal state-space lumping in markov chains[A]. Information Processing Letters[C]. Sept 2003. 87(6). 309 - 315.

[37] Lin C, Marinescu D C. Stochastic high level Petri nets and applications Computer Science Department [R]. Purdue University, CSD-TR-613, 1986.

[38] Lin C, Marinescu D C. On Stochastic high level petri nets[A]. In: Pro int Workshop on Petri Nets and Performance Models [C]. Madison, Wisconsin, USA, 1987. 34 - 39.

[39] Lin C, Marinescu D C. Stochastic high level petri nets and applications[J]. IEEE Trans Compute, 1988, 37(7): 815 - 825.

[40] Zenie A. Coloured stochastic petri nets[A]. In: Proc Int Workshop on Timed Petri Nets[C]. Torino, Italy, 1985. 262 - 271.

[41] Chiola G, Bruno G, Demaria T. Introducing a color formalism into generalized stochastic Petri nets[A]. In: Proc 9th European Workshop on Applications and Theory of Petri Nets[C]. Venezia, Italy, 1988. 202 - 215.

[42] Dutheillet C, Haddad S. Regular stochastic Petri nets [A]. In: Proc 10th European Wordshop on Applications and Theory of Petri Nets[C]. 1989.

[43] W Henderson, D Lucic, P G Taylor. A net level performance analysis of stochastic petri nets[J]. Journal of Australian Mathematical Soc Ser B, 1989, 31: 176 - 187.

[44] R J Boucherie. A Characterization of independence for competing markov chain with applications to stochastic petri nets[A]. In: Proc 5th International Workshop on Petri Nets and Performance Models[C]. 1993. 117 - 126.

[45] G Balbo, S C Bruell, M Sereno. On the relations between BCMP queueing networks and product form solu-

tion stochastic petri nets[A]. In Proc of the 10th International Workshop on Petri Nets and Performance Models[C]. 2003. 103 - 113.

[46] G Chiola, C Anglano, J Campos, et al. Operational analysis of timed petri nets and application to the computation of performance bounds[A]. In Proc 5th International Workshop on Petri Nets and Performance Models[C]. 1993. 128 - 137.

[47] S C Allmaier, M Kowarschik, G Horton. State space construction and steady state solution of GSPNs on a shard2memory multiprocessor[A]. In Proc of the 7th International Workshop on Petri Nets and Performance Models[C]. 1997. 112～121.

[48] LIN C, LI Y J, LIU X N. Analysis methods and applications of non-markovian stochastic petri nets[J]. Journal of system simulation, 2003, 15(s1): 71 - 75.

[49] R German. Markov regenerative stochastic Petri nets with general execution policies: Supplementary variable analysis and a prototype tool[J]. Performance Evaluation, 2000, 39: 165 - 188.

[50] A Horvath, A Puliafito, M Scarpa, M Telek. Analysis and evaluation of non-markovian stochastic petri nets[A]. In Computer Performance Evaluation, Modeling Techniques and Tools[C]. volume 1786 of LNCS, pages. Springer-Verlag, 2000. 171 - 187.

[51] LIN C. Performance Evaluation of Computer Networks and Computer Systems[M]. Beijing: Tsinghua University Press, 2001. 223 - 263.

[52] R German. Iterative analysis of Markov regenerative models[J]. Journal of Performance Evaluation, 2001.

[53] J B Dugan, K S Trivedi, R M Geist, V F Nicola. Extended stochastic Petri nets: Applications and analysis[A]. Performance[C]. 1984. 507 - 519.

[54] C Lindemann, G Shedler. Numerical analysis of deterministic and stochastic Petri nets with concurrent deterministic transitions[J]. Performance Evaluation, 1996, 23: 565 - 582.

[55] R Jones. Analysis of phase-type stochastic Petri nets with discrete and continuous timing. Technical Report NASA/CR-2000-210296[Z]. NASA Langley Research Center, Hampton, VA, USA, 2000.

[56] H Choi, V G Kulkarni, K S Trivedi. Markov regenerative stochastic Petri nets[J]. Performance Evaluation, 1994, 20: 337 - 357.

[57] Ivan Mura, Andrea Bondavalli. Markov regenerative stochastic Petri nets to model and evaluate phased mission systems dependability[J]. IEEE Transactions on Computer, 2001, 50(12): 1337 - 1352.

[58] Bondavalli A, Chiaradonna S, Di Giandomenico F, Mura I. Dependability modeling and evaluation of multiple-phased systems using DEEM. Reliability[J]. IEEE Transactions 2004, 53(4): 509 - 522.

[59] Andrea Bondavalli, Silvano Chiaradonna, Felicita Di Giandomenico, Ivan Mura. Dependability modeling and evaluation of multiple-phased systems using DEEM[J]. IEEE Transaction reliability, 2004, 53(4): 509 - 523.

[60] R German, C Lindemann. Analysis of stochastic Petri nets by the method of supplementary variables[J]. Performance Evaluation, 1994, 20: 317 - 335.

[61] R Jones, G Ciardo. On phased delay stochastic Petri nets: Definition and an application[A]. In Proc of the 9th International Workshop on Petri Nets and Performance Models[C]. 2001. 165 - 174.

[62] LIU D B, LIN C, LU W M. Product-form approximate solution for no-product-form solution stochastic petri nets[J]. Chinese Journal of Computer, 2001, 24(6): 588 - 595.

[63] M Dumitrescu. Stochastic petri nets architectural modules for power system availability proc[C]. Electronics, Circuits and System, 2002. 2. 745 - 748.

[64] W Willinger, R Govindan, S Jamin, V Panson, S Shenker. Scaling phenomena in the Internet: Critically examining criticality[J]. 2002, PNAS 2002 99 Suppl 1: 2573 - 2580.

作者简介:

林 闯 男,1948年出生于辽宁省,博士,清华大学计算机系教授,博士导师,计算机系主任,同时为 IFIP TC6 (Communication Systems)中国代表,IEEE高级会员,IEEE Transactions on Vehicular Technology编委,Journal of Parallel and Distributed Computing编委,Journal of Computer Science & Technology编委,《计算机学报》、《软件学报》、《电子学报》和《计算机研究与发展》编委,国家自然科学基金重大研究计划"网络和信息安全"的科学指导专家,主要研究领域为计算机网络,系统性能评价,安全分析,随机 Petri网. 曾在美国 Purdue大学、美国 Texas大学奥斯汀分校、香港科技大学、香港浸会大学和美国 Florida大学长期做研究工作,已在国内外一级期刊上和 IEEE Computer Society的学术年会上发表论文 210多篇,并在国内出版专著 3本. E-mail: Chlin@tsinghua.edu.cn.

王元卓 男,1978年生于黑龙江省,于 2004年 6月毕业于燕山大学计算机系获得计算机软件硕士学位,现为北京科技大学计算机应用专业在读博士研究生. 主要研究领域为计算机网络、系统性能评价、随机 Petri网、网格计算.