

基于贝叶斯网络的多阶段系统可靠性分析模型

刘 东^{1),2)} 张春元¹⁾ 邢维艳³⁾ 李 瑞¹⁾

¹⁾(国防科技大学计算机学院 长沙 410073)

²⁾(装备指挥技术学院国防科技重点实验室 北京 101416)

³⁾(中国华阴兵器试验中心 陕西 华阴 714200)

摘 要 针对多阶段系统(PMS)的可靠性评估问题,提出了一种基于贝叶斯网络(BN)的可靠性分析模型 PMS-BN. PMS-BN 模型首先为每个阶段构建各自的 BN,其结果命名为 phase-BN. 为了描述阶段之间的相关性,将所有 phase-BN 中表示同一部件但属于不同阶段的根节点用有向边连接,并且将所有 phase-BN 中的叶节点与一个新的表示 PMS 系统的节点用有向边连接,从而构建出用于刻画 PMS 系统的 BN,称之为 PMS-BN. 将各个阶段时间离散为 m 个时间段,利用 BN 推理算法获得 PMS 的可靠性参数. 通过 2 个实例详细阐述 PMS-BN 的建模过程. PMS-BN 模型为 PMS 可靠性分析提供了一种新的策略,能够方便地实施系统可靠度计算、故障诊断、重要度分析等应用. 若构建的 PMS-BN 满足所有非根节点均具有 2 个父节点,则 PMS 可靠度的求解过程仅需 $O(Nm^3)$ 的计算复杂度,其中 N 为非根节点的个数.

关键词 多阶段系统;贝叶斯网络;可靠性分析;计算复杂度;重要度分析

中图法分类号 TP302

Bayesian Networks Based Reliability Analysis of Phased-Mission Systems

LIU Dong^{1),2)} ZHANG Chun-Yuan¹⁾ XING Wei-Yan³⁾ LI Rui¹⁾

¹⁾(School of Computer, National University of Defense Technology, Changsha 410073)

²⁾(Key Laboratory of National Defense Technology, Academy of Equipment Command & Technology, Beijing 101416)

³⁾(China Huayin Ordnance Test Center, Huayin, Shaanxi 714200)

Abstract The paper presents a Bayesian networks (BN) framework for the reliability analysis of phased-mission systems (PMS), named PMS-BN model. A PMS consists of consecutive and non-overlapping time periods, with system configuration, success criteria, and component behavior varying from phase to phase. Firstly, each phase is represented by a BN framework, named phase-BN. Then, in order to figure the dependences across the phases, all the phase-BN are combined by connecting the root nodes that represent the same component but belong to different phases, and connecting the leaf nodes of phase-BN with a new node representing the whole PMS mission. The new constructed BN is called PMS-BN. In PMS-BN model, each phase time is divided into m segment, and the reliability analysis of PMS is performed by a discrete-time BN model acting on PMS-BN. Two examples are used to expatiate on the proposed approach. The PMS-BN based method provides a new efficient way to analyze the reliability of PMS, especially for those with dynamic phases. Moreover, it is also applicable to system diagnosis and sensitivity analysis. If all the non-root nodes in constructed PMS-BN own not more than 2 father nodes, the

computational complexity of evaluating the PMS reliability is $O(Nm^3)$, where N is the number of non-root nodes.

Keywords phased-mission systems; Bayesian networks; reliability analysis; computational complexity; sensitivity analysis

1 引言

多阶段系统(Phased-Mission System, PMS)包含多个连续不重叠的时间区域(或称为阶段),系统配置、成功标准以及部件行为在不同阶段中各不相同.在PMS中,不仅多个部件在同一阶段内存在相关性,而且同一部件在不同阶段之间也存在相关性.这种复杂相关性的存在造成了PMS可靠性分析的困难.

完全由静态阶段构成的PMS称为静态PMS,包含动态阶段的PMS称为动态PMS.目前,针对PMS的可靠性分析方法主要分成两类:基于组合模型的静态分析方法和基于状态空间的动态分析方法.

最简单的静态分析方法是部件分解法^[1].该方法将每个阶段内的部件分解为一系列统计独立的小部件,从而消除阶段间的相关性.然而,随着系统规模的增大,这种方法的复杂性呈指数增长.文献[2-3]提出了利用割集计算PMS可靠度的方法,通过对各阶段的割集进行不交化,并作概率求和,从而得到PMS的可靠度.割集方法是一种组合模型,具有简单、直观等特点,但仍然具有组合爆炸的隐患,因此该方法并不适合复杂系统.与基于割集的方法相比,BDD(Binary Decision Diagram, 二叉决策图)方法提供了一种快速求解静态PMS可靠度的机制,目前美国马塞诸州大学和弗吉尼亚大学正开展相关的研究工作.基于BDD的PMS可靠性分析方法将每个阶段的BDD利用阶段代数和前/后向阶段相关操作组合为整个系统的BDD(称为PMS-BDD),通过求解PMS-BDD得到PMS的可靠度^[4].目前,以PMS-BDD为基础的静态PMS研究主要集中在解决不完全错误覆盖(Imperfect Fault-Coverage, IPC)、阶段组合需求(Combinatorial Phase Requirement, CPR)^[5]、多模式失效(Multimode Failure)^[6]和共因失效(Common Cause Failure, CCF)^[7]等问题.

为了获得实用、可行的可靠性分析方法,人们通常对PMS进行各种假设,比如在静态PMS分析

中,通常假设PMS中各个部件的失效行为是相互独立且不可维修的.然而,对于阶段内各部件失效行为相互依赖的动态PMS,静态分析方法不能很好地加以处理,此时不得不采用基于状态空间的动态分析方法.

对于动态PMS,目前主要利用Markov链模型建模.Markov链模型是可靠性工程中有效的建模工具,其优点是能够正确描述阶段内各部件之间的依赖性以及部件跨阶段的依赖性.Markov链模型独立分析每个阶段的Markov链,而每个阶段的初始状态概率来源于上一个阶段的分析结果^[8].此外,也可将每个阶段的Markov链整合为单一的由状态空间组成的Markov链联合体,PMS的可靠度即为Markov链中所有工作状态的概率之和^[9].上述两种方法在本质上均是分阶段处理各自的Markov链,并由最后阶段的Markov链获得PMS的可靠性参数.文献[10-11]介绍了一种模块化方法,该方法将用于描述每个阶段的故障树(Fault Trees, FT)模块化,并以模块化后的每个模块作为模块基本事件(Modular Basic Event, MBE),并由MBE构建PMS的BDD.该方法在处理动态MBE时,则使用Markov链模型求解.由于系统状态规模随着系统部件数量增加呈指数增长,这导致Markov链模型的计算量非常庞大.

在动态分析方法中,通常假设PMS的阶段持续时间是确定的,阶段内的行为符合齐次马尔可夫过程特性.这些假设可以极大地简化PMS的可靠性分析.然而,对于实际中存在的不能满足上述假设的PMS,即具有随机分布的阶段持续时间和非指数分布行为的PMS,还需要采用其它分析方法.在有关这方面的研究中,文献[8]在阶段内随机过程是齐次马尔可夫过程的条件下推导了阶段持续时间分布为指数分布或一般分布的PMS任务可靠度计算公式.文献[12]针对阶段持续时间为随机分布、阶段内行为是非指数分布的PMS可靠性分析提出了基于五元组的分析模型.上述方法弱化了PMS可靠性分析中的假设条件,从而能够针对特殊的情况给出满足指定精度的分析结果,具有较强的适用性.与此

类似的研究还包括 Mura 等人提出的基于 Petri 网的 PMS 可靠性分析模型^[13-14],他们开发的 DEEP 建模工具综合了确定性分析、Markov 再生过程、随机 Petri 网等方法,并为 PMS 的可靠性分析提供了功能强大的集成环境。

除此之外, Monte Carlo 仿真方法为 PMS 的可靠性分析提供了另一种灵活的建模手段。仿真方法的理论基础是概率论中的基本定律——大数定律,该方法的应用范围从理论上说几乎没有什么限制^[15]。Murphy 等人开发的 Raptor 仿真工具^[15]可完成对 PMS 可靠性的仿真,但该工具所使用的仿真方法属于粗仿真(crude simulation),因此仿真效率较低。

总结目前有关 PMS 可靠性分析的研究工作,我们可以得出如下结论:

(1) 一般采用 BDD 及其扩展方法分析静态 PMS 的可靠性。BDD 方法是一种组合模型,具有快速建模、求解迅速等优点,其缺点是无法分析动态系统,并且只适用于非维修系统。

(2) 一般采用 Markov 链模型分析动态 PMS 的可靠性。Markov 链模型是描述随机过程的强有力工具。齐次 Markov 链模型的研究工作比较完善,具有成熟的理论基础和应用实例。Markov 链模型能够描述顺序失效、功能相关、储备等动态特性,并且可以对可维修系统建模。由于系统的状态空间会随着部件的数量呈指数变化,因此 Markov 链模型具有指数级的复杂度,在分析复杂系统时,将会面临状态空间爆炸问题。

(3) 静态分析方法与动态分析方法的结合可提高分析效率,这实际上是一种层次化的建模手段,能够充分利用两种分析方法的优点,避免各自的局限。例如,结合 Markov 链模型, BDD 方法仍旧能够对动态系统进行建模,其基本思想是:将系统中的动态部分封装为单个的模块,对单个模块利用 Markov 链模型分析,而以模块作为最基本的 BDD 分析单位^[11]。这种方法的优点是能够描述并求解动态随机过程,并可充分利用 BDD 的快速算法。

(4) 通过弱化模型假设条件,分析更一般条件下的 PMS 可靠性;或者为了避免复杂的 Markov 链求解过程,寻找新的建模方法。随着研究的不断深入,研究人员逐渐放宽对 PMS 的各种假设,开始关注系统在不满足齐次 Markov 链模型的条件下的可靠性建模方法。典型的情况是阶段内部的随机过程服从非指数分布,阶段持续时间为非确定的随机时

间。该问题可以通过基于状态空间的动态分析方法解决,例如 Markov 链模型^[8]和五元组分析模型^[12]。对于复杂的 PMS,当上述模型求解困难,以至于无法获得解析解和数值解时,通常采用 Monte Carlo 仿真方法模拟 PMS 的实际工作过程,利用统计参数作为可靠性分析结果。

本文的研究属于上述第 4 类工作,即为了避免复杂的 Markov 链求解过程,寻找新的 PMS 建模手段。通常来说,基于状态空间的动态分析方法最终需要求解复杂的状态方程(微分方程组),当 PMS 的阶段内随机过程服从非指数分布时,一般无法以解析的形式给出分析结果,此时需要求助于近似方法给出其数值结果。即便如此,当系统的规模庞大时,微分方程的近似求解也会异常困难,这使得 PMS 的可靠性分析变成纯粹的数学问题。此外,状态空间的规模会随着系统规模呈指数增长,其建模过程也将会变得烦冗、枯燥、易出错。

为了使可靠性分析过程真正落到系统的模型描述,而不是复杂数学问题的求解上,本文提出一种新的基于贝叶斯网络(Bayesian Networks, BN)的 PMS 可靠性分析模型 PMS-BN,其目的在于简化 PMS 可靠性分析的建模过程,减小模型的计算复杂度,并支持一般条件下的 PMS 系统(包括静态 PMS 和动态 PMS)分析。PMS-BN 模型将 PMS 描述为 BN,从而能够利用高效的计算方法求解 PMS 可靠性。利用 BN 特有的推理机制, PMS-BN 模型还适用于系统的故障诊断、重要度分析等更加复杂的应用。

本文将首先给出基于 BN 的可靠性分析原理。在此基础上,通过结合 BN 与 PMS,研究基于 BN 的 PMS 可靠性分析方法 PMS-BN。最后,本文将通过用例介绍 PMS-BN 在可靠度计算、故障诊断、重要度分析等领域中的应用。

2 贝叶斯网络及其在可靠性分析中的应用

BN 是一个有向无环图,其中的节点表示随机变量(在 BN 中,通常“节点”等同于“随机变量”),有向边表示条件独立关系。根节点是指不具有父节点的节点,叶节点指不具有子节点的节点,其它节点称为中间节点。对于由离散变量节点构成的 BN,根节点拥有先验概率表(Prior Probability Table, PPT),表中的数值表示根节点处于不同状态的概率;

非根节点拥有条件概率表(Conditional Probability Table, CPT),表中的数值表示在给定父节点取值组合的情况下,该节点处于不同状态的概率。

如果用节点和有向边表示系统的部件及其之间的关系,则 BN 刻画了系统中变量之间存在的条件独立关系,即节点在给定其父节点的前提下与其非后代节点条件独立^[16]. BN 揭示出所有变量的完全联合概率分布(Full Joint Probability Distribution, JPD),从而能够通过边缘化求解机制推理出所有与概率相关的问题(在给定一个或多个变量的前提下获得系统中其它变量的条件概率).变量之间条件独立关系的存在减少了确定 JPD 所需的参数,从而简化了系统中变量的概率模型.系统中所有变量 $\{X_1, X_2, \dots, X_n\}$ 的 JPD 可表示为

$$P[X_1, X_2, \dots, X_n] = \prod_{i=1}^n P[X_i | pa(X_i)] \quad (1)$$

其中, $pa(X_i)$ 表示节点 X_i 的父节点。

近年来, BN 模型在可靠性分析领域中的应用逐渐得到关注. 研究表明,无论在建模能力还是在分析能力上, BN 模型较故障树、可靠性框图等模型均具有显著的优势,并具有较小的复杂度^[16].

由于 PMS 系统的配置会在阶段的切换时刻发生变化,我们选择离散时间贝叶斯网络(Discrete-Time Bayesian Networks, DTBN)作为 PMS 的建模手段. 在 DTBN 中,根节点表示系统部件,中间节点表示一系列部件之间的相互关系,叶节点表示整个系统. DTBN 将系统任务时间离散为 m 个时间段. 若系统任务时间为 T ,则每个时间段的宽度为 $\Delta = T/m$. 相应的,每个节点具有 $m+1$ 个状态,每个状态表示节点在对应时间段内的行为. 例如,如果节点表示系统中的部件,则节点处于该状态表示部件在对应时间段内发生失效;如果节点表示门,则节点处于该状态表示门在对应时间段内产生输出. 系统的可靠度就是叶节点处于最后一个状态的概率。

复杂系统的 DTBN 中节点众多,节点之间的关联也会因系统的复杂行为而变得极其紧密. 然而,与基于状态空间的建模方法相比较, DTBN 模型将系统状态的转移映射到节点附带的条件概率表中,这种利用多个局部行为描述全局状态的变迁将会在很大程度上降低模型的复杂程度. 此外, DTBN 的推理方法具有直观、简洁的特点,易于用计算机实现快速分析和处理,避免了复杂微分方程的求解问题。

3 PMS-BN 可靠性分析模型

在本文中,对 PMS 系统给出以下假设:

(1) 部件或系统发生失效后不可修复. 由于 BN 是一种有向无环图,因此无法对可维修系统建模。

(2) 每个阶段的持续时间相等. 在本文中,每个阶段的持续时间被离散为多个时间段,从而将部件的工作过程表示为多个状态. 如果每个阶段的持续时间相等,可有利于 PPT 和 CPT 中状态概率的形式化表示. 事实上,本文的方法可以应用于阶段持续时间为任意值的 PMS,文末将会弱化这一假设,并指出这种情况下的处理方法。

(3) 任意阶段子任务的失败将导致整个 PMS 任务的失败. 大多数系统的正常运行需要经过多个连续的阶段,例如巡航导弹攻击任务可分为发射、惯性制导段、末制导段等阶段,太空飞行器本体从发射、运行、返回亦需经历不同的环境阶段等. 在不考虑阶段组合需求 CPR(即 PMS 系统具有多个任务,每个任务都需要组合不同的阶段配置)^[5]的情况下,这一假设符合实际系统的工作过程. 事实上,只需修改某些节点的 CPT,本文的方法将可以直接应用于 CPR 的分析. 文末将弱化这一假设,并指出这种情况下的处理方法。

3.1 PMS-BN 的生成方法

PMS 系统的每个阶段可以用 DTBN 表述,本文称这种用于表述阶段内部件相关性的 DTBN 为 phase-BN. 与 FT 类似, phase-BN 是 PMS 阶段内系统行为的一种表示方法,并可由每个阶段的 FT 转换得到. 例如, BN 中的根节点可以表示 FT 中的基本事件,中间节点表示 FT 中的各种静态/动态门以及与根节点具有依赖关系的基本事件,而叶节点则表示 FT 的顶事件. 有关将 FT 转换为 BN 的相关内容可参考文献[17].

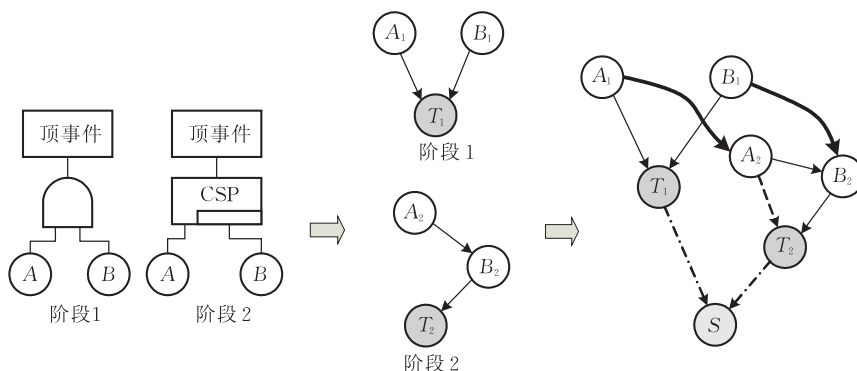
为了用 BN 描述整个 PMS 系统,通过如下两个步骤对 phase-BN 进行组合:

(1) 由于不同阶段间的同一部件是相关的,因此为了描述这种阶段之间的相关性,利用有向边连接那些位于不同阶段但属于同一部件的节点。

(2) PMS 的任务依赖于每个阶段子任务的执行情况,即一旦任何阶段失效, PMS 将会失效. 为了表示 PMS 任务和各个阶段子任务之间的相关性,构建一个新的节点表示整个 PMS 系统的任务,并用有向边连接 phase-BN 的叶节点和新的节点。

依照上述过程生成的 BN 即为 PMS-BN. 图 1 展示了一个 2 阶段 PMS 构建 PMS-BN 的过程, 其中第 2 个阶段由动态故障树 (Dynamic Fault Tree, DFT)^[18] 表示. 如图 1(a) 所示, 在第 1 阶段中, 部件 A 和 B 并联工作, 只有当 A 和 B 同时失效时, 系统才会失效. 在第 2 阶段中, 部件 B 作为 A 的冷

储备; 在 A 失效后, B 才开始工作; 只有当 A 和 B 均失效时, 系统才会失效. 两个阶段对应的 phase-BN 如图 1(b) 所示. 利用两个 phase-BN 生成的 PMS-BN 如图 1(c) 所示, 其中, $T_1(T_2)$ 代表阶段 1(2) 的顶事件, S 代表 PMS 系统.



(a) 两个阶段对应的DFT (b) 由DFT转换得到的phase-BN (c) PMS-BN

图 1 PMS-BN 的生成过程

在由 phase-BN 生成 PMS-BN 的过程中, 应当考虑如下特殊情况: 两个节点在 phase-BN 中条件独立, 但在 PMS-BN 中却具有相关性. 例如, 在第 2 阶段中, B 是 A 的冷储备, 因此该阶段的子任务状态原本只由 B 决定, 即第 2 阶段的 phase-BN 中, A_2 和 T_2 之间不存在有向边. 然而, 考虑到 B 有可能会在第 1 阶段中失效, 因此 T_2 的状态实际上是由 A_2 和 B_2 共同决定, 即 PMS-BN 中的 A_2 和 T_2 之间存在有向边, 这与第 2 阶段的 phase-BN 不同.

通常来说, 对于任意 3 个节点 X, Y 和 Z, 如果下述条件成立, 则应当在 PMS-BN 中用新的有向边连接 X 和 Z, 有向边的方向是由 X 指向 Z:

- (1) X, Y 和 Z 并不属于第 1 阶段, Y 在以前的阶段中曾经出现;
- (2) Y 是 X 的冷储备;
- (3) Z 是 Y 的冷储备, 或者 Z 表示 X 和 Y 的 CSP 门^[18].

3.2 PMS-BN 的可靠性分析方法

将每个阶段时间分为 m 个时间段, 从而整个任务时间分为 mn 个时间段, 其中 n 为阶段的个数.

在 PMS-BN 中, 第 1 阶段的部件节点具有 $m+1$ 个状态. 前 m 个状态表示部件在第 m 个时间段中失效, 而最后一个状态 (标识为 $m+1$) 表示部件在第 1 阶段中未发生失效. 与部件节点对应, 第 1 阶段的其它中间节点和叶节点同样具有 $m+1$ 个状态.

在剩余的阶段中, 每个部件具有 $m+2$ 个状态. 第 1 个状态表示部件在先前的阶段中已经失效, 用

0 标识. 接下来的 m 个状态表示部件在该阶段的第 m 个时间段中失效, 用 $(j-1)m+i$ 标识, 其中 i 是时间段编号, j 是阶段编号 ($0 < i \leq m, 1 < j \leq n$). 最后一个状态表示部件在该阶段中未发生失效, 用 $mj+1$ 标识. 与部件节点对应, 这些阶段的其它中间节点和叶节点同样具有 $m+2$ 个状态.

如果部件并未从第 1 阶段开始工作, 则该部件在第 1 次进入工作状态的那个阶段中具有 $m+1$ 个状态, 而在剩余的工作阶段中具有 $m+2$ 个状态.

PMS-BN 的叶节点具有 $(m+1)n$ 个状态. 前 m 个状态表示系统在第 1 阶段中的某个时间段内发生失效. 随后的 $(n-1)(m+1)$ 个状态被分为 $(n-1)$ 组, 每组对应一个阶段. 例如, 状态 $(m+1)$ 到 $m+(m+1)$ 表示系统在第 2 阶段内的行为, 其中, 状态 $m+1$ 表示系统在第 2 阶段开始时即发生失效, 随后的 m 个状态表示系统在对应的时间段内发生失效. 叶节点最后一个状态表示系统在任务时间内并未失效. 因此, PMS 的可靠度就是 PMS-BN 的叶节点处于最后一个状态的概率.

每个节点与其父节点之间的概率发生关系由对应的 CPT 描述, 从而 PMS 的可靠度可通过计算 PMS-BN 叶节点的后验概率得出. 由此可知, 第 1 阶段的每个节点的 CPT (对于根节点是 PPT) 具有 $m+1$ 个状态. 剩余阶段的节点的 CPT 具有 $m+2$ 个状态. 根据 BN 的结构, 每个节点具有 $k+1$ 维的 CPT (或者 PPT), 其中 k 是节点的父节点个数. 例如, 图 1 中 A_1, B_1, A_2 和 B_2 均具有 1 维的 PPT, 而

T_1, T_2 和 S 具有 3 维的 CPT.

假设所有部件的寿命服从指数分布,令 A 和 B 的失效率 $\lambda_A=\lambda_B=0.02\text{h}^{-1}$, 阶段内时间段的个数 $m=2$, 时间段长度 $\Delta=1\text{h}$, 则 A_1 或 B_1 的 PPT 可根据下式获得

$$\begin{aligned} Pr\{A_1=k\} &= F(k \cdot \Delta) = 1 - e^{-\lambda_A k \Delta}, \\ Pr\{A_1=3\} &= 1 - Pr\{A_1=1\} - Pr\{A_1=2\} \quad (2) \end{aligned}$$

其中, $k \leq 3$. 完整的 PPT 如表 1 所示.

表 1 $A_1(B_1)$ 的 PPT

$A_1(B_1)$	Pr
1	0.01980
2	0.01941
3	0.96079

如果部件在前一个阶段内失效,它将不能在后续阶段中继续工作. 因此,如果 A_1 的状态为 1 或 2, 则 A_2 处于状态 0 的概率为 1. 以部件 A 在第 $j-1$ 阶段不失效的前提下, A 在第 j 阶段中处于状态 i 的条件概率由下式计算:

$$\begin{aligned} P_{(A,i,j)} &= (Pr\{A \text{ 在 } [(j-1)m+i-1] \cdot \Delta, \\ &\quad ((j-1)m+i) \cdot \Delta \text{ 内失效}\}) / \\ &\quad (Pr\{A \text{ 在第 } j-1 \text{ 阶段未失效}\}) \\ &= (F(((j-1)m+i) \cdot \Delta) - \\ &\quad F(((j-1)m+i-1) \cdot \Delta)) / \\ &\quad (1 - F((j-1)m \cdot \Delta)) \quad (3) \end{aligned}$$

如果部件的寿命服从指数分布,则式(3)可整理为

$$\begin{aligned} P_{(A,i,j)} &= \frac{e^{-\lambda_A((j-1)m+i-1) \cdot \Delta} - e^{-\lambda_A((j-1)m+i) \cdot \Delta}}{e^{-\lambda_A(j-1)m \cdot \Delta}} \\ &= F(i \cdot \Delta) - F((i-1) \cdot \Delta) \quad (4) \end{aligned}$$

上式表明,部件在第 j 阶段中处于状态 i 的条件概率等于部件在第 1 阶段相应时间段内的先验概率,这是由于指数分布的无记忆性决定的. 因此,以 A_1 处于状态 3 作为前提, A_2 处于状态 3 的条件概率等于 A_1 处于状态 1 的先验概率,依次类推. 因此,有

$$Pr\{A_2=k|A_1=3\} = Pr\{A_1=k(\text{mod } m)\} \quad (5)$$

其中, $3 \leq k \leq 5$. A_2 的 CPT 如表 2 所示.

表 2 A_2 的 CPT

A_2	Pr		
	$A_1=1$	$A_1=2$	$A_1=3$
0	1	1	0
3	0	0	0.01980
4	0	0	0.01941
5	0	0	0.96079

由于 B_2 具有两个父节点 A_2 和 B_1 , 因此其 CPT 与 A_2 的 CPT 不同. 在第 2 阶段中, B 是 A 的冷储

备,只有在 A 失效之后, B 才开始工作. 除此之外, 如果 B 在第 1 阶段内失效,那么 B 在第 2 阶段也将不再工作. A 也同样具有类似的特性. 因此, B_2 的 CPT 将是一个 3 维表, 表中的数值依照下式填入:

$$\begin{aligned} Pr\{B_2=0|B_1=1 \text{ or } B_1=2\} &= 1, \\ Pr\{B_2=k|B_1=3, A_2=0\} &= Pr\{B_1=k(\text{mod } m)\}, \\ Pr\{B_2=g|B_1=3, A_2=3\} &= \\ Pr\{B_1=(g-1)(\text{mod } m)\}, \\ Pr\{B_2=5|B_1=3, A_2>3\} &= 1 \quad (6) \end{aligned}$$

其中, $3 \leq k \leq 5, 4 \leq g \leq 5$.

T_1 的 CPT 可以根据 A_1 和 B_1 的 AND 关系直接构建.

由于 T_2 与 A_2 和 B_2 连接, 因此其 CPT 是一个 3 维表. 如果 A 在第 1 阶段失效, 则 B 将在第 2 阶段开始时便进入工作状态, 而 T_2 的状态将由 B 确定; 如果 B 在第 1 阶段失效, 则 T_2 将只由 A 确定; 否则, T_2 将由 A_2 和 B_2 共同确定. T_2 的 CPT 中的数值依照下式填入:

$$\begin{aligned} Pr\{T_2=\max(k,g)|A_2=k, B_2=g, k=0 \text{ or } g=0\} &= 1, \\ Pr\{T_2=g|A_2=k, B_2=g\} &= 1 \quad (7) \end{aligned}$$

其中, $3 \leq k < g \leq 5$.

由于任意阶段子任务的失败将导致 PMS 的任务失败, 因此 S 的 CPT 可以根据 T_1 和 T_2 的 OR 关系构建:

$$\begin{aligned} Pr\{S=k|T_1=k, 1 \leq k \leq 2\} &= 1, \\ Pr\{S=3|T_1=3, T_2=0\} &= 1, \\ Pr\{S=g+1|T_1=3, T_2=g, 3 \leq g \leq 5\} &= 1 \quad (8) \end{aligned}$$

在 PPT 和 CPT 构建完毕之后, 节点 S 的状态 6 表示 PMS 未发生失效, 其概率即为 PMS 的可靠度. 本文利用开源 Matlab BNT 工具包^① 计算出图 1 中 PMS 在时刻 4h 的可靠度为 0.9951. 此外, 也可以通过计算 S 在任意状态的概率来计算系统在任意时刻的可靠度.

在上例中, 假设所有阶段时间相同, 而实际上, 本文中的方法可应用于具有不同阶段时间的 PMS (不满足假设 2). 此时可将每个阶段时间分为 $m_k = T_k/\Delta$ 个时间段, 其中 T_k 为第 k 个阶段的持续时间, Δ 为某一固定的时间长度.

当某一阶段子任务的失败并不导致整个 PMS 任务的失败时 (不满足假设 3), 可以更改 PMS-BN 叶节点的 CPT, 使之满足新条件下的阶段组合.

① <http://www.cs.ubc.ca/~murphyk/Software/BNT/bnt.html>

3.3 计算复杂度分析

如果仅仅计算 PMS 完成任务的概率(即 PMS 的可靠度),只需计算 PMS-BN 的叶节点 S 处于最后一个状态的概率,该过程的伪代码如下:

```
1. result=0;  
2. for  $s_1=1::N(pa_1(S))$   
3.   for  $s_2=1::N(pa_2(S))$   
4.     ...  
5.     for  $s_n=1::N(pa_n(S))$   
6.       result=result+Pr{ $S=mn+1 \mid pa_i(S)=s_i$ } ·  
            $\prod_{i=1}^n Pr\{pa_i(S)=s_i\}$ ,
```

其中, $N(pa_i(S))$ 表示节点 S 的第 i 个父节点的状态个数.对于本文的 PMS-BN,有

$$N(pa_i(S))=\begin{cases} m+1, & i=1 \\ m+2, & 1<i\leq n \end{cases}.$$

上述代码中的第 6 行是最内层的循环体,利用大 O 表示法表示的执行次数为 $O((m+1)(m+2)^{(n-1)})=O(m^n)$.

而构建 S 的 CPT 将需要填充一个具有 $(m+1)n$ 个状态的 $n+1$ 维表,表中具有的项的个数为 $O((m+1)n(m+1)(m+2)^{(n-1)})=O(nm^{(n+1)})$.为

了简化计算,只填充 S 的 CPT 的最后一行即可得到 PMS 的可靠度,此时,总的计算复杂度为 $O(m^n)$.

求解中间节点处于不同状态的概率需要构建完整的 CPT,所需的计算量为 $O(m^{(p+1)})$,其中 p 为中间节点的父节点的个数,将由系统的结构决定.如果 PMS-BN 中中间节点的最大父节点的个数为 p ,则求解 PMS-BN 可靠度所需的计算量应为 $O(m^n + Nm^{(p+1)})=\max(O(m^n), O(Nm^{(p+1)}))$,其中 N 为 PMS-BN 中非根节点的个数.

考虑计算复杂度表达式 $\max(O(m^n), O(Nm^{(p+1)}))$,在 $O(m^n)$ 中, n 实际上表示 PMS-BN 叶节点的父节点的个数,而 $O(Nm^{(p+1)})$ 的大小也主要取决于 p 的值,因此我们可以得出如下结论:父节点的个数将在很大程度上影响着 PMS-BN 模型的计算效率.因此,在构建 phase-BN 和 PMS-BN 时,应尽可能地以级联的方式将每个节点的父节点个数保持为 2,将可简化模型的复杂度.如图 2 所示,在将 4 输入 AND 门转换为 BN 时,最终的转换结果应当为如图 2(b)所示的由级联节点构成的 BN,而不是如图 2(c)所示的 BN.

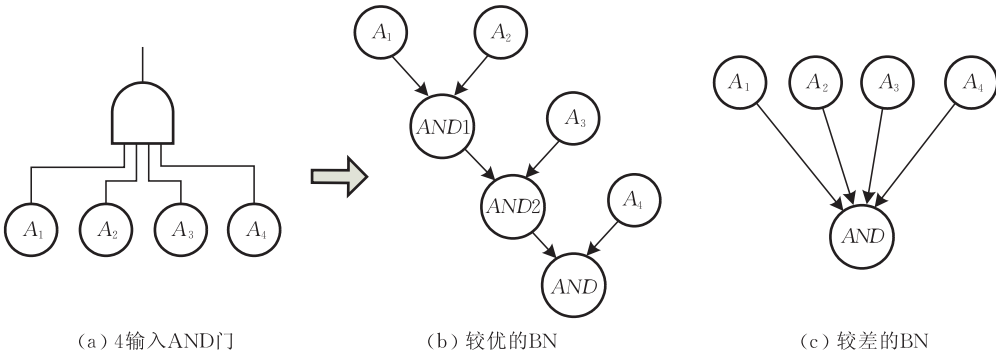


图 2 BN 的简化示例

在大多数情况下,系统的 PMS-BN 均可以构建满足上述要求的 BN 拓扑结构.此时,为了获得 PMS 可靠度,所需要的计算量将变为 $\max(O(m^n), O(Nm^{(p+1)}))=O(Nm^3)$.因此,PMS-BN 模型的计

算复杂度并不与系统规模呈指数增长关系.与 Markov 链模型相比较,后者状态空间为 2^q , q 为系统中所有变量的个数.两种可靠性分析模型的比较如表 3 所示.

表 3 PMS-BN 模型与 Markov 链模型 的比较

	建模过程	复杂度	可维修系统	求解算法	精确度
PMS-BN 模型	简单、直观	大多数情况 $O(Nm^3)$	不支持	简单的 DTBN 模型	近似解
Markov 链模型	复杂、易出错	$O(2^q)$	支持	复杂的微分方程	解析解或数值解

由表 3 可以看出,除了不支持可维修 PMS 的可靠性分析之外,PMS-BN 模型在建模过程、复杂度、求解算法等方面均较 Markov 链模型具有较大的优势.此外,PMS-BN 模型获得的可靠性分析结果的

精度由参数 m 确定, m 的值是计算精度与所消耗时间和空间的折中,这种折中为我们提供了一种灵活的解决方案.而求解 Markov 链模型则通常要求解复杂的微分方程,尽管可以通过各种简化方法加

快求解速度,但对于复杂系统的 Markov 链模型分析,则需要付出很大的时间和空间代价。

除了计算 PMS 可靠度之外,基于 PMS-BN 的建模方法还可以完成故障诊断、重要度分析等可靠性分析内容.这些内容的实现需要利用 BN 的后验概率推理,其复杂度取决于所采用的推理算法.一般来说,推理算法的复杂度主要由网络的拓扑结构和节点状态的个数(即时间段的个数 m)决定^[16].本文利用 BNT 工具中的连接树推理算法(junction tree inference algorithm)完成所有推理过程,其推理复杂度为 $O(d^\omega)$,其中, d 为最大变量值域空间的大小, ω 为 BN 对应的连接树中最大结点簇的大小^[19]. 如果将 PMS-BN 构建为级联的形式,则大多数情况下有 $d=m+2$, $\omega=3$,此时推理算法的复杂度为 $O(m^3)$,而与网络的规模(变量的个数)没有直接关系。

4 用例分析

4.1 用例 1

某一航空电子系统(Aviation Electric System, AES)的系统结构为分布式结构,如图 3 所示. AES 的搭载设备包括照相机(C)、姿态导航与控制子系

统(GNC,标识为 G)和冗余的计算机. 所有设备通过一对 CAN 总线连接. AES 的任务包含 3 个阶段. 总线 a (标识为 Na)和总线 b (标识为 Nb)在第 1 和第 3 阶段互为热储备,而在第 2 阶段则必须同时正常工作. 在第 1 阶段中,计算机 a (Oa)和计算机 b (Ob)构成温储备计算机子系统;只有计算机子系统或者 CAN 子系统或者 GNC 子系统失效,该阶段才会失效. 在第 2 阶段中, Oa 和 Ob 构成热储备计算机子系统;此外,该阶段还需要照相机完成地面拍照任务. 第 3 阶段与第 1 阶段类似,但在该阶段中, Oa 和 Ob 构成冷储备计算机子系统,即 Ob 是 Oa 的冷储备单元。

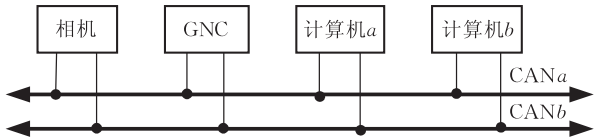


图 3 AES 的结构

AES 各个阶段的 FT 如图 4 所示,利用 FT 生成的 PMS-BN 如图 5 所示,其中的虚线是在由 FT 向 PMS-BN 的转化过程中填加的. 利用前文的分析方法为 PMS-BN 中的每个变量指派 PPT 或 CPT,该过程需考虑以下情况:

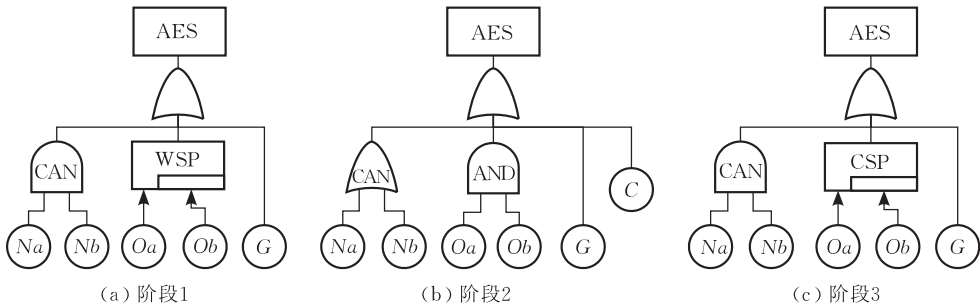


图 4 AES 每个阶段的故障树

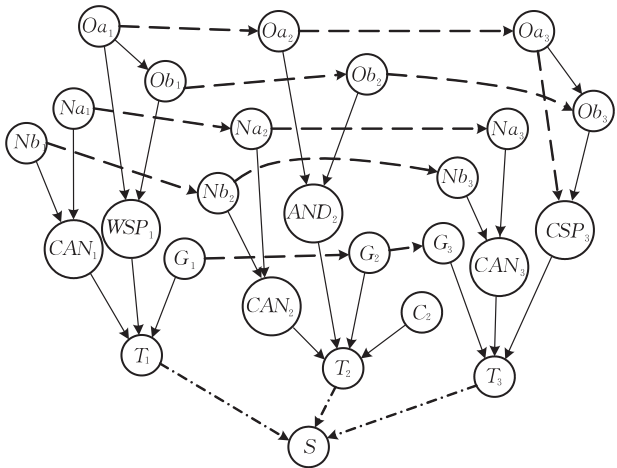


图 5 AES 的 PMS-BN

- (1) 当 Ob 作为温储备单元工作时,其失效率为正常失效率的 α 倍(称 α 为睡眠因子)。
- (2) 如果 Na 在第 2 阶段结束时仍未失效,那么可以确定 Na 在第 1 阶段并不失效,因此在给定 Na_2 的条件下, Na_1 与 Na_3 条件独立. 因此, Na_1 与 Na_3 之间不存在有向边. 其它部件的节点与此类似。
- (3) 在构建 PMS-BN 时,以级联节点的方式将每个节点的父节点个数保持为 2,将可简化 PMS-BN 的计算过程(图 5 所示为未简化的 PMS-BN)。
- (4) 在构建 PMS-BN 的过程中,考虑 Ob 在前 2 个阶段失效的情况,用 1 条有向边连接 Oa_3 和 CSP_3 。

4.1.1 可靠度的计算

假设 AES 中所有部件的寿命均服从指数分布,计算机、GNC、CAN 总线、照相机的失效率分别为 $\lambda_o=2.0\times10^{-5}\text{h}^{-1}$, $\lambda_G=3.0\times10^{-5}\text{h}^{-1}$, $\lambda_N=1.5\times10^{-5}\text{h}^{-1}$, $\lambda_C=5.0\times10^{-5}\text{h}^{-1}$. 温储备部件的睡眠因子 $\alpha=0.1$. 每个阶段需要 200h. 若 $m=10$, 利用 BNT 工具求解图 5 中的 PMS-BN, 得到 AES 在不同时刻的可靠度曲线如图 6 所示.

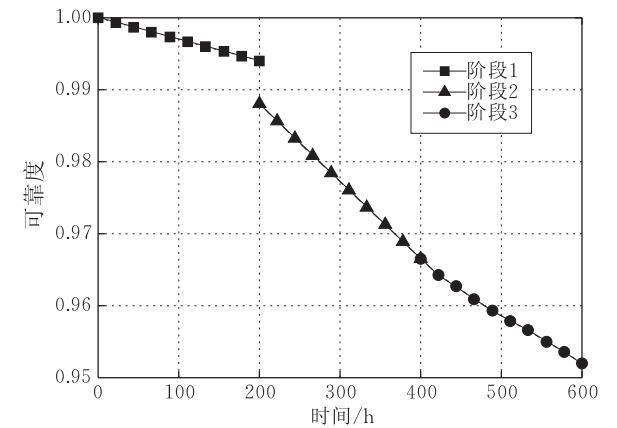


图 6 AES 在不同时刻的可靠度

由于 Na 和 Nb 在第 1 阶段组成一个并联系统, 因此如果两者之一发生失效, 那么系统在该阶段并不失效. 然而, 由于 Na 和 Nb 在第 2 阶段组成了一个串联系统, 因此只要任何一个部件失效, 系统将会失效. 这两个阶段的系统配置将会导致这样一种特殊的现象: 系统在第 2 阶段的开始时刻将比在第 1 阶段的结束时刻更容易失效, 即所谓的 PMS 潜在失效^[15]. 图 6 展示了这种潜在失效的示例——可靠度曲线在第 1 阶段结束时刻和第 2 阶段开始时发生了迅速的跳变.

AES 系统的单一 Markov 链模型^[9]中包含 25 个状态, 33 个状态转移, 利用 Matlab 工具的龙格-库塔算法解算 AES 系统的状态方程, 可以求得系统在第 3 阶段结束时的可靠度数值解为 $R_{\text{Markov}}=0.950861$, 计算过程耗时 0.047s. 对于不同的 m 值, 由 PMS-BN 计算出 AES 在第 3 阶段结束时的可靠度 $R_{\text{PMS-BN}}$ 以及与 R_{Markov} 的相对误差如表 4 所示. 由表 4 可以看出, 随着 m 的增加, $R_{\text{PMS-BN}}$ 的值逐渐趋近于数值解. 即使当 $m=5$ 时, $R_{\text{PMS-BN}}$ 与 $R_{\text{PMS-BN}}$ 的相对误差也保持在 1.5% 以内. 因此, 在实际应用时, 为了减小计算复杂度, 同时获得较高的计算精度, 可以令 $m=7$.

表 4 在不同 m 下利用 PMS-BN 模型计算的可靠度

m	可靠度 $R_{\text{PMS-BN}}$	消耗时间/s	相对误差
			$\left(\frac{ R_{\text{PMS-BN}}-R_{\text{Markov}} }{R_{\text{Markov}}}\times100\%\right)$
3	0.962690	0.017	1.24
5	0.961721	0.052	1.14
7	0.955821	0.732	0.52
8	0.952634	1.781	0.19
10	0.951987	9.394	0.12

4.1.2 故障诊断

故障诊断功能是 BN 优于其它可靠性分析方法的另一个特点. 利用 BN 进行系统的故障诊断, 即是在给定系统故障这一证据下, 分析各个部件发生失效的后验概率, 找到最可能导致系统故障的原因 (Most Probable Causes, MPC), 从而为系统设计和维护提供方法指导和理论依据.

对于 PMS-BN, 故障诊断过程不但可以确定哪些部件最可能发生失效, 还可确定部件在哪一时刻最可能发生失效. 基于贝叶斯网络的多阶段系统故障诊断过程包括以下步骤:

(1) 假设 PMS-BN 的叶节点 S 在时间段 p ($0 < p < mn+1$) 发生故障, 以此作为求解 PMS-BN 中其它节点后验概率的证据;

(2) 以 $S=p+(p \bmod m)=s$ 作为证据, 求出各个部件发生失效的后验概率 $Pr\{X_i \text{ 失效} | S=s\}=1-Pr\{X_i=im+1 | S=s\}$, 从而获得最可能导致 PMS 失效的部件 MPC.

(3) 设 X_i 为第 2 步得到的 MPC, 求 X_i 在各个时间段内发生失效的后验概率 $Pr\{X_i=k | S=s\}$.

对于图 5 所示的 PMS-BN, 令 $m=4, p=10$, 即以 $S=12$ 作为证据, 得到 AES 各个部件发生失效的后验概率如表 5 所示.

表 5 系统失效时各个部件失效的后验概率

部件	概率	部件	概率
Na_1	0	Ob_2	0.00718
Nb_1	0	G_2	0
Oa_1	0.00654	C_2	0
Ob_1	0.00065	Na_3	0.00410
G_1	0	Nb_3	0.00410
Na_2	0	Oa_3	0.02051
Nb_2	0	Ob_3	0.01308
Oa_2	0.01307	G_3	0.99018

由表 5 可知, 如果系统在第 10 个时间段内发生故障, 则最可能导致系统失效的部件是 GNC 子系统 (G_3). 在 PMS 失效的前提下, G_3 在各个时间段内失效的后验概率如表 6 所示.

表 6 系统失效时 GNC 子系统 G₃ 失效的后验概率

状态	后验概率
0	0
9	0
10	0.99014
11	0.00001
12	0.00001
13	0.00982

由表 6 可知,G₃最可能在第 10 个时间段内发生失效.

除了可以分析单个部件发生失效的后验概率之外,PMS-BN 模型还可以分析多个部件组合失效的后验概率,后者的分析方法与前者类似.

4.1.3 重要度分析

重要度分析使得设计人员可以确定每个系统部件的重要性.对具有较高重要度的部件进行可靠性改进,将会使系统的可靠性获得较大的提升.本文采用危害性重要度^[20]作为指标,利用 PMS-BN 分析 AES 中各个部件的重要度.部件 X 的危害性重要度定义为

$$I(X)=(Pr\{S|X\}-Pr\{S|\sim X\})\cdot \frac{Pr\{X\}}{Pr\{S\}} \quad (9)$$

其中,X 表示部件发生失效,~X 表示部件 X 完好,S 表示系统发生故障.由于 PMS 中不同阶段具有不同的结构,因此同一部件在不同阶段表现出不同的重要度.上式中,

$$Pr\{S|X_i\}=1-Pr\{\sim S|X_i\}$$
$$=1-\frac{Pr\{\sim S\}(1-Pr\{\sim X_i|\sim S\})}{1-Pr\{\sim X_i\}} \quad (10)$$

$$Pr\{S|\sim X_i\}=1-Pr\{\sim S|X_i\} \quad (11)$$

其中,1≤i≤n.由式(9)~(11)可得

$$I(X_i)=(Pr\{\sim S\}(1-Pr\{\sim X_i|\sim S\})+Pr\{\sim S|\sim X_i\}(1-Pr\{\sim X_i\}))/$$

$$(1-Pr\{\sim S\}) \quad (12)$$

对于 PMS-BN,有

$$Pr\{\sim X_i\}=Pr\{X_i=ij+1\} \quad (13)$$

$$Pr\{\sim S\}=Pr\{S=(m+1)n\} \quad (14)$$

其中,1≤j≤m.令 m=10,则 AES 在第 3 阶段结束时,根据式(12)~(14)得出的各个部件的重要度如表 7 所示.

表 7 部件在不同阶段的重要度

	Na	Nb	Oa	Ob	G	C
阶段 1	0.17981	0.17981	0.31707	0.24651	0.35909	—
阶段 2	0.18035	0.18035	0.39527	0.32471	0.36125	0.59730
阶段 3	0.23957	0.23957	0.47339	0.32472	0.36342	—

由表 7 可知,G 在第 1 阶段、C 在第 2 阶段、Oa 和 G 在第 3 阶段均具有较高的重要度,需要在部件设计时重点关注其可靠性的改进.

4.2 用例 2

对于如图 7 所示的 PMS 系统,由于系统共包含 16 个部件,因此其 Markov 链模型具有 2¹⁶ 个状态,此时利用系统状态方程求解可靠度参数将会异常复杂.而如果用 PMS-BN 刻画系统,级联各个根节点构成的 PMS-BN 将只需 59 个节点(包括:第 1 阶段 phase-BN 中的 27 个节点,第 2 阶段 phase-BN 中的 31 个节点,表示 PMS 的 1 个叶节点).当 m=6 时,利用 PMS-BN 模型计算该 PMS 的可靠度所耗时间仅为 8.5s.

5 结 论

本文提出了一种基于贝叶斯网络的多阶段系统可靠性分析模型 PMS-BN,旨在提供一种完善、高效的多阶段系统可靠性分析方法.PMS-BN 模型利

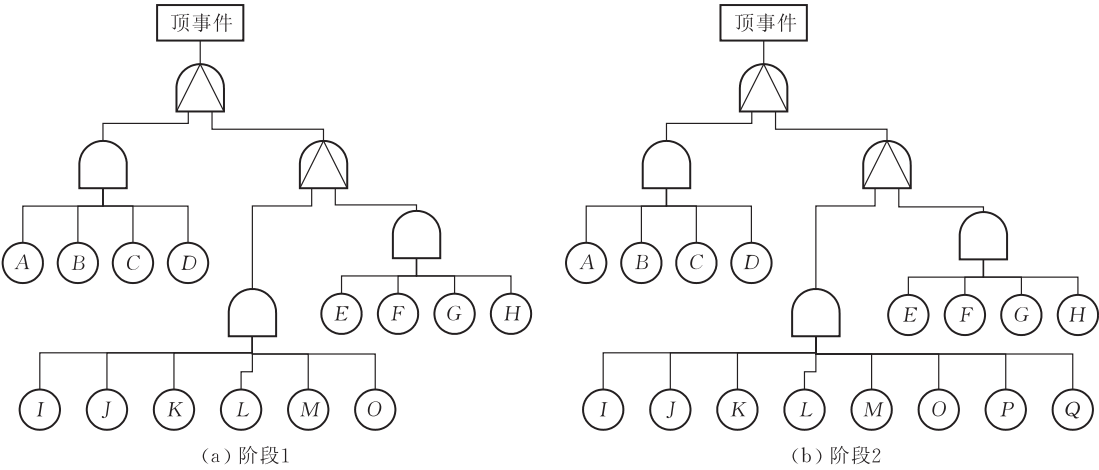


图 7 复杂 PMS 示例

用贝叶斯网络刻画多阶段系统,从而可以利用贝叶斯网络作为有力的建模和分析工具完成多阶段系统的可靠性分析.在进一步的工作中,我们将在 PMS-BN 模型中引入 IPC、CCF 等因素,拓展 PMS-BN 的建模能力.同时,考虑各种特殊应用,完成更为一般条件下的多阶段系统可靠性分析.

参 考 文 献

- [1] Esary J D, Ziehms H. Reliability analysis of phased missions//Proceedings of the Conference of Reliability and Fault Tree Analysis. Washington, USA, 1975: 213-236
- [2] Ma Y, Trivedi K S. An algorithm for reliability analysis of phased-mission systems. Reliability Engineering and System Safety, 1999, 66(2): 157-170
- [3] Somani A K, Trivedi K S. Phased-mission system analysis using Boolean algebraic methods//Proceedings of the ACM SIGMETRICS Conference on Measurement and Modeling of Computer Systems. Nashville, Tennessee, USA, 1994: 98-107
- [4] Zang X, Sun N, Trivedi K S. A BDD-based algorithm for reliability analysis of phased-mission systems. IEEE Transactions on Reliability, 1999, 48(1): 50-60
- [5] Xing L, Dugan J B. Analysis of generalized phased-mission system reliability, performance, and sensitivity. IEEE Transactions on Reliability, 2002, 51(2): 199-211
- [6] Tang Z, Dugan J B. BDD-based reliability analysis of phased-mission systems with multimode failures. IEEE Transactions on Reliability, 2006, 55(2): 350-360
- [7] Tang Z, Xu H, Dugan J B. Reliability analysis of phased mission systems with common cause failures//Proceedings of the Reliability and Maintainability Symposium. Alexandria, Virginia, USA, 2005: 313-318
- [8] Kim K, Park K S. Phased-mission system reliability under Markov environment. IEEE Transactions on Reliability, 1994, 43(2): 301-309
- [9] Dugan J B. Analysis of a hybrid voting algorithm for replicated file systems. Information and Software Technology, 1991, 33(4): 273-280
- [10] Ou Y, Meshkat L, Dugan J B. Multi-phase reliability analysis for dynamic and static phases//Proceedings of the Reliability and Maintainability Symposium. Seattle, Washington, USA, 2002: 404-410
- [11] Ou Y, Dugan J B. Modular solution of dynamic multi-phase systems. IEEE Transactions on Reliability, 2004, 53(4): 499-508
- [12] Mo Yu-Chang, Yang Xiao-Zong, Cui Gang et al. Mission reliability analysis of generalized phased mission systems. Journal of Software, 2007, 18(4): 1068-1076(in Chinese)
(莫毓昌, 杨孝宗, 崔刚等. 一般阶段任务系统的任务可靠性分析. 软件学报, 2007, 18(4): 1068-1076)
- [13] Mural I, Bondavalli A, Zang X et al. Dependability modeling and evaluation of phased mission systems: A DSPN approach//Proceedings of the 7th IFIP International Conference on Dependable Computing for Critical Applications. San Jose, California, USA, 1999: 319-337
- [14] Bondavalli A, Chiaradonna S, Giandomenico F D et al. Dependability modeling and evaluation of multiple-phased systems using DEEM. IEEE Transactions on Reliability, 2004, 53(4): 509-522
- [15] Murphy K E, Carter C M, Malerich A W. Reliability analysis of phased-mission systems: A correct approach//Proceedings of the Reliability and Maintainability Symposium. Orlando, Florida, USA, 2007: 7-12
- [16] Langseth H, Portinale L. Bayesian networks in reliability. Reliability Engineering and System Safety, 2007, 92(1): 92-108
- [17] Zhou Zhong-Bao, Zhou Jing-lun, Sun Quan et al. Dynamic fault tree analysis method based on discrete-time Bayesian networks. Journal of Xi'an Jiaotong University, 2007, 41(6): 732-736(in Chinese)
(周忠宝, 周经伦, 孙权等. 基于离散时间贝叶斯网络的动态故障树分析方法. 西安交通大学学报, 2007, 41(6): 732-736)
- [18] Dugan J B, Bavuso S, Boyd M. Dynamic fault tree models for fault tolerant computer systems. IEEE Transactions on Reliability, 1992, 41(3): 363-377
- [19] Tian Feng-Zhan, Zhang Hong-Wei, Lu Yu-Chang et al. Simplification of inferences in multiply sectioned Bayesian networks. Journal of Computer Research and Development, 2003, 40(8): 1230-1237(in Chinese)
(田凤占, 张宏伟, 陆玉昌等. 多模块贝叶斯网络中推理的简化. 计算机研究与发展, 2003, 40(8): 1230-1237)
- [20] Intellect. Reliability: A Practitioner's Guide. Beijing: Beihang University, 2003



LIU Dong, born in 1981, Ph. D.. His current research interests focus on real-time systems and fault-tolerance techniques.

ZHANG Chun-Yuan, born in 1964, professor, Ph. D. supervisor. His major research interests include high-performance computing and computer architecture.

XING Wei-Yan, born in 1980, M. S.. Her current research interests focus on the reliability analysis of complex systems.

LI Rui, born in 1977, Ph. D. candidate. His current research interests focus on computer architecture.

Background

The reliability analysis of Phased-Mission Systems (PMS) is different from that of normal systems, since the existence of more than one phase in PMS leads to some complexities which do not occur in a single phased-system. In PMS, dependences exist not only within a phase but also across the phases. The PMS reliability was investigated greatly in these ten years, and the research center lies in University of Virginia and Duke University, USA. There have been a variety of methodologies for the analysis of PMS, such as cut sets, binary decision diagrams (BDD) and Markov chain model. BDD based approaches provide an efficient way to analyze PMS. However, it is limited to the static systems (just like cut sets based models) and can not handle dynamic systems that are characterized by dynamic behaviors, such as function dependence, redundancy and sequential failure. Although Markov chain model is a powerful tool to handle dynamic systems, it has to confront the state explosion problem. Accordingly, it is a challenge to get an applicable and efficient method to analyze the general PMS that are

characterized by both static and dynamic behaviors.

The paper introduces Bayesian networks (BN) modeling into the reliability analysis of PMS, and presents a new model, named PMS-BN. PMS-BN provides a compact and intuitive way to analyze PMS with dynamic phases. In PMS-BN, the dependences within a phase and across the phases can be expressed easily by BN framework, and the reliability of PMS can be computed with less complexity compared by Markov chain model.

This research is supported by the National Natural Science Foundation of China (60673148, 60703073) and the National High Technology Research and Development Program (863 Program) of China (2006AA704302). The aim of the research is to establish a systematic method to analyze PMS, such as space information systems and aircraft systems. Until now, the research team has published more than 20 papers about the fault tolerant design and the reliability analysis of space information systems.