

通过升级实现韧性：一种基于图的卫星威胁响应 PACE 架构

Anouar Boumeftah*, Sarah McKenzie-Picot[†], Peter Klimas[†], Gunes Karabulut Kurt*

*Poly-Grames Research Center, Department of Electrical Engineering, Polytechnique Montréal, Montréal, QC, Canada

[†]NorthStar Earth & Space, Montréal, QC, Canada

{anouar.boumeftah, gunes.kurt}@polymtl.ca, {sarah.mckenzie-picot, peter.klimas}@northstar-data.com

摘要—卫星系统越来越面临来自干扰、网络攻击和电磁干扰的操作风险。传统的冗余策略往往无法应对动态的多向量威胁。本文介绍了一个基于设计的弹性框架，该框架植根于 PACE (Primary, Alternate, Contingency, Emergency) 方法论——最初为军事行动中的战术通信开发——并通过受 CVSS、DREAD 和 NASA 的风险矩阵等威胁评分框架启发的分层状态转换模型将其适应于卫星系统。我们定义了一个动态弹力指数来量化系统的适应性，并实现了三种 PACE 变体——静态、自适应和基于 softmax 的决策模型——以评估在各种干扰场景下的弹性。所提出的方法突出了轻量级、决策感知的备用机制在提高下一代太空资产生存能力和操作连续性方面的有效性。

Index Terms—卫星系统，冗余，PACE，赛博物理系统，决策建模，设计安全

I. 介绍

卫星系统面临着越来越不稳定的威胁环境，这种环境由自然现象和故意干扰共同塑造。随着对基于太空的通信、导航、地球观测和防御基础设施的依赖增加，轨道资产已成为全球网络中的关键且易受攻击的部分。威胁包括网络攻击、干扰、欺骗、电磁扰动以及跨越空地链路的级联故障。最近的事件突显了这些风险：2022 年 Viasat 网络攻击扰乱了欧洲 [1] 民用和军事服务，而 1962 年的 Starfish Prime 测试则展示了高空电磁脉冲 (EMP) 事件的广泛影响 [2]。

A. 背景及相关工作

卫星系统的韧性是指在硬件故障和恶意威胁存在的情况下维持基本功能的能力。最近的研究强调，虽然太空资产越来越成为网络攻击的目标，但许多系统仍然缺乏强大的、集成的韧性策略。Pavur 等。[3] 记

录了几十年来的卫星黑客事件，突显了该行业的脆弱性。Falco 等人。[4] 强调基于任务目标的动态需求的重要性。军事和国家太空政策现在强调韧性是容错和网络防御 [5] 的结合，要求卫星能够承受随机故障和蓄意攻击。在工程中，冗余仍然是主要策略，通常通过 N+1 方案或三模冗余 (TMR) 实现。然而，这些方法大多是静态的，在应对随机故障时有效，但在面对协调或适应性攻击时可能会失败。Sun 使用等。[6] 贝叶斯方法来评估卫星冗余的有效性，而 O' Halloran 使用等。[7] 提出了一个框架，用于在早期设计阶段分析赛博物理系统中的故障传播，强调使用图论指标识别正向、逆向和不耦合的传播路径。夏使用等。[8] 通过有向图方法扩展了这一研究，应用于受到攻击的复杂机电系统 (CMES)。虽然这些方法对随机故障有效，但它们主要是静态的，并假设威胁是被动的，因此对于适应性或协同攻击来说不太适用。从系统级角度来看，MILSATCOM DFARR 计划提供了设计经济实惠、有弹性的卫星通信系统的 [9] 见解。它对模块化波形和灵活的地空处理的关注反映了针对网络和干扰的韧性所采取的系统工程方法，并与促进分层保护以对抗动能、电子和基于软件威胁的新政策相一致。

B. 现有的威胁建模框架

威胁模型通常是一种形式化的抽象，定义了潜在的对抗和非对抗危害、系统漏洞，并建立了这些威胁得以实现的路径。威胁建模的应用不仅在于捕捉操作风险的范围和性质，还在于它在系统设计、部署以及本文所述的应急规划范围内促进了基于风险的决策制

定。NASA 的风险矩阵被广泛用于航空航天风险评估, 通过可能性和严重性来分类危害。在网络安全中, 诸如 CVSS (通用漏洞评分系统) 和 DREAD 等框架对漏洞和威胁进行评分。虽然 CVSS 量化了软件风险, 但 DREAD 则从潜在损害、可利用性等方面定性地排列威胁等级。应用于卫星时, 这些模型提供了有用的见解, 但仍未能充分融入到在轨决策制定中。Pavur 等。[3] 和 Falco 等。[4] 呼吁统一的威胁建模方法, 以弥合特定于空间的危害和网络安全风险评估之间的差距。与此互补的是, Jacobsen 和 Marandi 为无人驾驶飞行系统提供了一个量身定制的网络威胁分类法, 使用 STRIDE 来识别从欺骗到权限提升的各种漏洞。他们的方法提供了一种可迁移的卫星系统威胁建模框架——特别是在不断增长的自主或半自主空间平台领域中, 其中网络物理集成提出了类似的挑战 [10]。

尽管它们有价值, 现有的威胁模型通常被孤立应用, 并且与机载决策系统保持脱节。这限制了它们在需要快速适应的动态、竞争环境中发挥作用的能力。为了弥补这一差距, 第 III 节介绍了一种结构化的、具有决策意识的备选框架, 旨在支持在多种威胁条件下实现弹性的卫星操作。

C. PACE 方法论的起源

PACE 模型——主要、交替、偶然性和紧急情况——是由美国特种部队开发的, 旨在确保在受争议或退化环境中任务的连续性 [11]。它促进了一种独立备选方案的层级结构, 这些方案按照可行性和可靠性进行优先排序。虽然最初用于战术通信, 但现在 PACE 已被应用于高可靠性领域。在军事指挥与控制中, 它支持中断下的关键功能 [12]; 医疗系统使用它来排序紧急响应 [13]; 网络安全和基础设施安全局 (CISA) 将其应用于设计国家基础设施和应急操作的冗余通信框架 [14]。

D. 研究空白识别

传统冗余提高了容错能力, 但它是静态的, 并且专门针对随机独立故障进行设计。在竞争环境中, 这种设计对自适应或协同威胁失效, 通常导致共因故障, 所有冗余单元都被破坏 [15]。它们还增加了开销, 而没有保证抵御不断演变的风险的能力。最近的工作倡导了情境感知冗余。Jacobs 等。提出了可重构方案以适应环境压力 [15]; George 等。展示了在三模冗余和对称多处理之间切换的航天器架构 [16]。基于图的技术,

包括用于异常检测的知识图谱, 进一步支持系统级自适应性 [8], [17]。

这些研究指出了需要多层适应性策略的必要性。为此, 我们提出了一种受 PACE 规划概念启发的分层架构。我们的主要贡献是:

- 适应于军事的 PACE 韧性框架, 在竞争性轨道环境中应用于卫星操作。
- 设计一个以威胁驱动的决策树, 根据任务效用和运营成本选择最优的 PACE 备用层。
- 使用基于 softmax 的机制形式化动态转换, 以实现可追溯、奖励驱动的升级和恢复策略。
- 构建一个集成威胁可能性、运营成本和效用的系统级模型, 并通过蒙特卡罗模拟评估性能。
- 定义动态冗余效率指数 (DREI), 以量化不同策略中任务性能与回退成本之间的权衡。

本文的其余部分组织如下。第 II 节介绍系统模型和威胁场景。第 III 节介绍了基于图的 PACE 框架及其转换逻辑。第 IV 节定义了动态冗余效率指数 (DREI)。第 V 节概述了仿真设置和 PACE 变体。第 VI 节分析结果。第 VII 节总结关键发现并提出未来方向。

II. 系统和威胁概述

A. 威胁分类学跨越空间段

卫星威胁横跨三个操作领域: 空间、地面和链接段。虽然这种分割有助于风险评估, 但许多威胁向量跨越这些领域, 导致相互依赖或级联系统故障, 如第 II-C 节所述。

1) 空间段: 这包括易受硬件和软件攻击的机载系统 (图 1)。Willbold 等人。识别卫星固件中的缺陷, 例如未受保护的遥命令接口和缺失的访问控制, 这些可以允许持久性恶意软件或完全接管 [18]。Falco 等。进一步强调未经审查的商用现货 (COTS) 组件和供应链后门带来的风险 [19]。

2) 地面段: 地面部分包括任务控制、天线网络和云基础设施。关键风险包括网络分段薄弱、遗留遥测协议以及配置错误的 API [20]。攻击可能通过受损的门户发起, 并升级为未经授权的命令。先前的事件如 ROSAT 和 KA-SAT 证实了补丁不足和不安全接口如何导致整个系统中断 [19]。

3) 链段: 此部分涵盖了星地和星间链路 (ISLs), 这些链接极易受到射频 (RF) 威胁, 如干扰、欺骗和窃

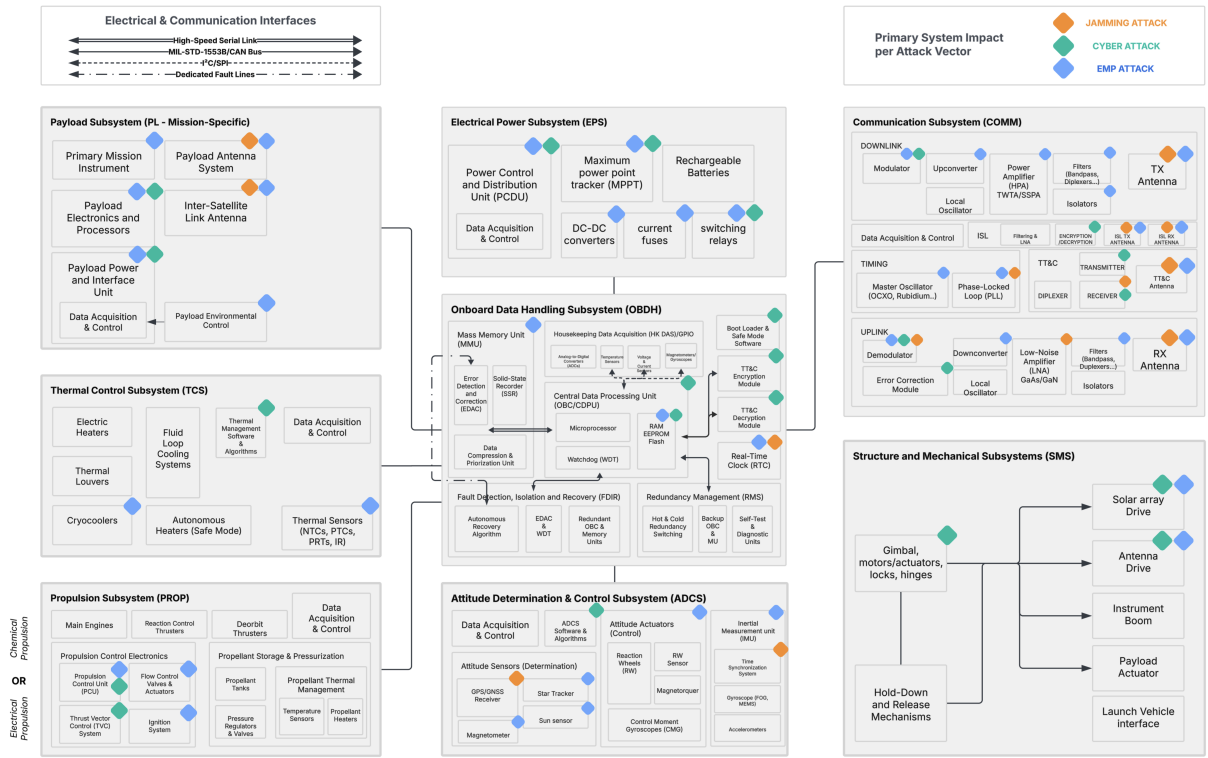


图 1: 系统级的卫星架构方块图。每个大方块表示一个主要子系统。彩色菱形标记指示了主要脆弱性攻击向量：干扰（橙色）、网络（蓝色）和电磁脉冲（绿色）。

听。Baselt 等。报告了广泛使用未加密的 SATCOM 链路 [21], 而 Morales-Ferre 等。表明 GNSS 欺骗可以破坏卫星的时间和定位功能 [22]。这些攻击可能会降低性能, 导致轨道误差或使上行链路劫持成为可能 [20]。

B. 系统级建模与影响分类学

系统级别的威胁映射在图 1 中突出了子系统对干扰、网络 and 电磁脉冲 (EMP) 威胁的脆弱性。我们重点关注三大类威胁: 信号干扰和欺骗攻击、网络攻击以及电磁脉冲 (EMP)。由于篇幅限制, 第 VI 节中的数值评估仅针对干扰场景。

1) 信号干扰和欺骗: 基于 RF 的干扰破坏卫星上行链路/下行链路, 而欺骗则将虚假信号注入控制回路。此类干扰可能导致操作模式降级或延迟 [20]。Morales-Ferre 等人。展示了 GNSS 对重放和 meaconing 攻击的脆弱性, 这威胁到轨道精度和时间同步, 特别是对于依赖导航的系统 [22]。

2) 网络攻击: 网络威胁针对卫星软件堆栈、固件和通信协议, 从而实现系统持久性破坏 [18]。ENISA 强调了卫星生命周期中的漏洞, 包括未加密的控制通道

和弱加密措施 [20]。德勤强调由于卫星互连性和地面站即服务 (GSaaS) 的应用导致网络风险增加 [23]。

3) 电磁脉冲 (EMP): 电磁脉冲事件同时通过引发破坏性的电涌威胁所有部分, 影响电力系统、电子设备和航空电子设备 [24]。使用商用现货电子产品的卫星特别容易发生锁存或烧毁。由于其立即且广泛的破坏潜力, 电磁脉冲被列为顶级非动能威胁之一 [20]。

C. 级联故障在子系统间的影响

跨段攻击可以引发系统范围的退化。伪造的链接可能会误导车载计算机 (OBCs), 而基于地面的入侵则会破坏固件并禁用安全防护措施。通过星间链路 (ISLs) 传播恶意软件的情况也已被证实 [25]。电磁脉冲可以同时干扰遥测、电源和控制系统。这些影响突显了需要建立能够隔离故障并保持关键功能的备用架构的重要性——这是基于 PACE 模型的核心目标。

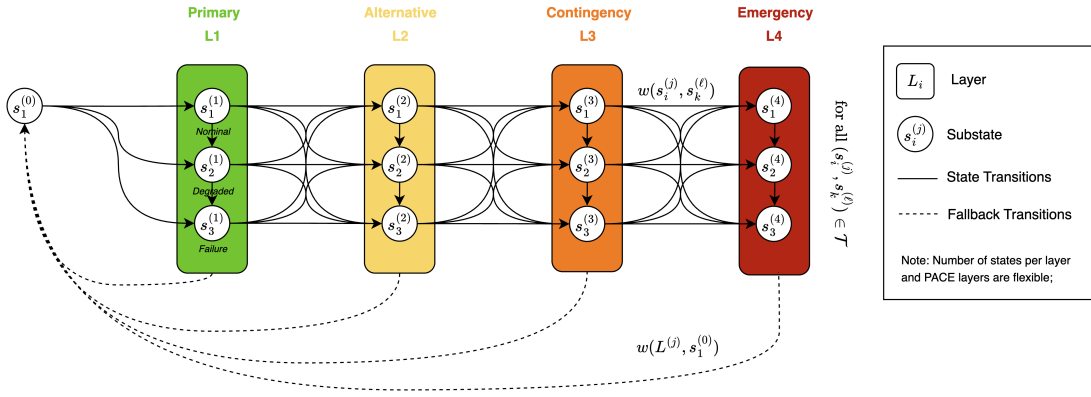


图 2: PACE 基于图的表示图

III. 提议的框架

A. 基于 PACE 的韧性模型

该模型将操作行为组织成四个韧性层次：**主要**（正常），**交替**（降级但功能正常），**偶然性**（压力下的生存能力）和**紧急情况**（最小操作或紧急信号）。每一层反映了任务效用与系统负担之间的权衡——平衡性能、风险承受能力和资源消耗。这些层次共同构成了一个模块化、自适应的结构，以实现优雅降级。转换由上下文感知指标和预定义阈值引导，以保持连续性 [12]。

B. 基于图的表示

如图 2 所示，我们将基于 PACE 的框架形式化为一个有向多层图 $G = (\mathcal{S}, \mathcal{T})$ ，其中：

- $\mathcal{S} = \bigcup_{i=1}^4 \{s_i^{(j)}\}$ 是跨越所有层次 $L_i \in \{P, A, C, E\}$ 的系统状态集
- $\mathcal{T} \subseteq \mathcal{S} \times \mathcal{S}$ 是状态之间的转换集合。

每个状态 $s \in \mathcal{S}$ 都与一个效用函数 $\omega(s)$ 和调整后的恢复潜力相关联。转换 $(s, s') \in \mathcal{T}$ 被注解为：

$$w(s, s') = (p(s, s'), c(s, s')) \quad (1)$$

其中 $p(s, s')$ 是从 s 转换到 s' 的概率，而 $c(s, s')$ 是相关的成本。

1) 状态定义和分层：每一层 L_i 包含一个固定数量的状态 $s_i^{(j)}$ ，代表操作可行性的程度。转换可能在同一层内发生（水平转换）或跨层发生（垂直转换）。以下规则适用：水平转换处理同一层内的退化或恢复；垂直转换表示在受到威胁时的回退或向上恢复，受成本和约束。

2) 转移概率和成本建模：转移权重是基于威胁可能性（NASA 风险矩阵，CVSS 评分）、运营成本（例如资源使用、任务损失、延误）以及系统动力学共同建模的，这些适应于环境因素如干扰强度、能量储备和任务阶段。由于页数限制，我们省略了威胁概率估计和转移模型的具体数值公式，尽管这些是作为我们的方法的一部分而开发出来的。

IV. 韧性评估指标

为了量化卫星系统在干扰下维持运行连续性的效果，我们引入了一个单一指标：动态冗余效率指数（DREI）。该指标捕捉了任务效用与随时间推移的备降或恢复转换成本之间的权衡。设 $\mathcal{S}$ 为 PACE 结构中所有系统状态的集合， $P_t(s)$ 为系统在时刻 t 处于状态 $s \in \mathcal{S}$ 的概率。每个状态 s 都与一个效用值 $\omega(s)$ 关联，并且状态之间的转换 (s, s') 在时间 t 产生成本 $c_t(s, s')$ 。我们定义调整后的效用 $\omega_t^*(s)$ 如下：

$$\omega_t^*(s) = \begin{cases} \omega(s) \cdot \kappa, & \text{if } s = \text{P_Nominal and } t > 0 \\ \omega(s), & \text{otherwise,} \end{cases} \quad (2)$$

其中 $\kappa > 1$ 是一个韧性奖励倍增器，强调了返回正常运行的重要性。

DREI 在时间 t 时计算为：

$$\text{DREI}_t = \frac{\sum_{s \in \mathcal{S}} \omega_t^*(s) \cdot P_t(s)}{C_t}. \quad (3)$$

这种表述奖励那些 (1) 恢复高效益状态，以及 (2) 无需承担过高的成本的韧性策略，使其适合用于评估如第 V-B 节中所述的能量感知回退或知情重新配置等动

态适应机制。高 DREI 值反映的是在不断演变的威胁下最大化系统效益同时最小化成本的配置。

V. 方法论

A. 仿真环境描述

为了评估提出的框架，我们使用时间步进、事件驱动模型模拟了一个具有代表性的信号干扰场景。卫星系统在图 1 中定义的操作约束和外部威胁下演化。每个时间步，环境更新能量储备、干扰强度 $J_t \in [0, 1]$ 和威胁活动，然后根据选定的 PACE 模型（静态、自适应或奖励优化）应用回退转换。每次转换都会带来概率成本并改变系统状态。在特定的时间步骤预定义危机加剧了威胁并通过层抑制、阻止转换或提高转换成本来模拟压力条件以测试恢复能力。

B. 实现了 PACE 变体

我们实现 PACE 框架的三个操作模型来评估环境意识和自适应决策对系统弹性的影响力。

1) 简单静态 PACE 模型：此基线使用从预计算的威胁分析中得出的固定转移权重。每个转移 $(s, s') \in \mathcal{T}$ 定义为：

$$w(s, s') = (p(s, s'), c(s, s')) \quad (4)$$

在每个时间步，系统以概率 p_{stay} 处于状态 s ；否则，它根据静态分布 $\{p(s, s')\}$ 进行转换。此非反应模型忽略了环境反馈，并用作基准。

2) 环境感知自适应 PACE 模型：此自适应模型根据实时条件调整转换，主要考虑干扰强度 J_t 和恢复并发性 $C \geq 1$ 。对于每个转换 (s, s') ，参数演化为：

$$p_t(s, s') = p(s, s') \cdot (1 + \lambda J_t) \quad (5)$$

$$c_t(s, s') = c(s, s') + \gamma J_t - \alpha(C - 1), \quad (6)$$

其中敏感度系数为 λ, γ, α 。

较高的 J_t 增加了退化状态的可能性，而同时恢复则降低了成本。不可行的转换被排除在外，并且在每个时间步骤中都从调整后的分布中抽取一个样本。

3) *Epsilon*-贪婪 MDP 启发的 PACE 模型：该模型采用了一种基于一奖励的决策规则，灵感来源于马尔可夫决策过程。每个有效的转换 (s, s') 都通过一个奖励 $R(s, s') = \omega(s') - c_t(s, s')$ 进行评分，其中 $\omega(s')$ 是目标状态的效用， $c_t(s, s')$ 是经过环境调整的成本。转换是通过一个 ϵ -贪婪策略选择的：以概率 ϵ ，随机选择

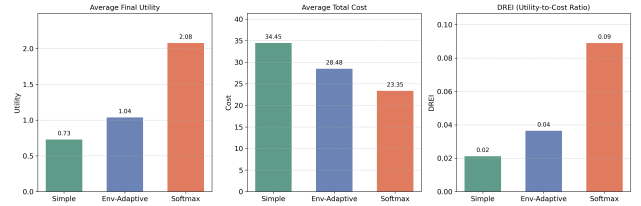


图 3: 平均最终效用（左），总累计成本（中）和 DREI（右）在所有试验中的 PACE 模型。

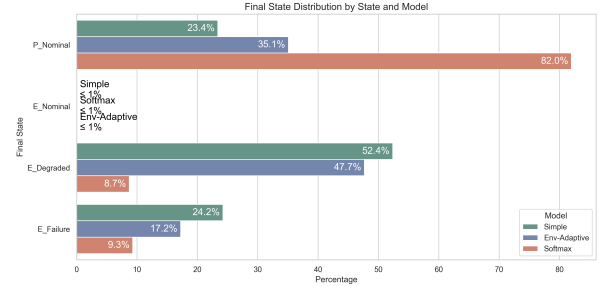


图 4: 最终状态分布显示了以正常、降级或故障状态结束的运行比例。

一个后继状态 $s' \in \mathcal{A}(s)$ （探索）；否则，选择最大化 $R(s, s')$ 的转换（开发）。

$$s \rightarrow s' \sim \begin{cases} \text{Uniform}(\mathcal{A}(s)) & \text{if } \epsilon \\ \arg \max_{s' \in \mathcal{A}(s)} R(s, s') & \text{otherwise.} \end{cases}$$

这种方法平衡了探索与利用，在偏好高效益、低成本转换的同时避免了局部最优。

对于每个 PACE 变体和干扰场景，我们执行 5000 次独立的蒙特卡洛试验，每次运行最多 $T = 12$ 个时间步。

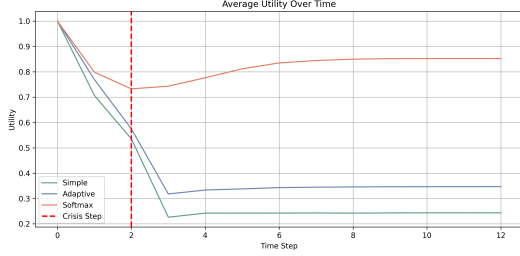
VI. 模拟结果与讨论

A. PACE 模型的比较性能

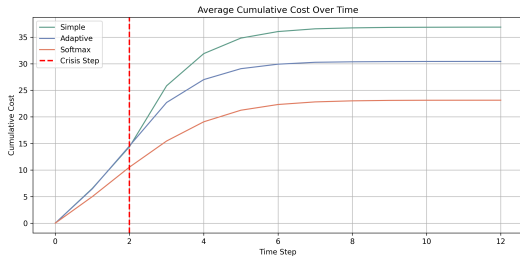
图 3总结了平均最终效用、总成本和 DREI。静态模型实现了 0.73 的效用，34.45 的成本，以及 0.02 的 DREI。自适应模型改善到 1.04 的效用，28.48 的成本，以及 0.04 的 DREI。Softmax 模型在各方面表现更优，达到了 2.08 的效用，23.35 的成本，以及 0.09 的 DREI——展示了跨指标的优越平衡。

图 4展示了最终状态分布。静态模型导致了 24.2% 的故障，52.4% 的退化状态和 23.4% 的正常状态。自适应

模型将故障减少到 17.2%，并将正常状态增加到 35.1%。softmax 模型最为稳健，实现了 82.0% 的正常状态，8.7% 的退化状态和 9.3% 的故障，突显了其在干扰下的鲁棒性。



(a) 时间平均效用。



(b) 随时间变化的平均累计成本。

图 5: 效用和成本的时间演化。红色虚线表示在第 2 时间步发生的危机事件。

图 5a 显示了随时间变化的平均效用。在第 2 个时间步长的危机之后，静态模型（降至 0.22）和自适应模型（降至 0.32）的效用急剧下降。softmax 模型逐渐恢复，在最后稳定在接近 0.85 的位置。图 5b 显示了累计成本。静态模型迅速累积成本，并饱和于大约 37 个单位。自适应模型趋于平稳，靠近 30 个单位，而 softmax 模型缓慢上升，仅达到 23 个单位。这些趋势表明，softmax 模型在危机后提供了更好的适应性和成本效率。softmax 模型的危机后恢复表明其在性能恢复方面具有更大的适应性，而其较慢且较低的成本累积则显示出在回退转换中提高了效率。

图 6 总结了总成本分布。柱状图（左面板）显示，静态模型的成本分布较宽且偏向较高值，反映出结果的巨大变异性。自适应模型的分布较窄，中心模式集中在 30 至 35 个单位之间。Softmax 模型产生的分布最为紧凑，集中在 20 到 25 个单位之间，表明成本较低且一致的结果。累积分布函数（CDF）（右面板）证实了这些趋势，softmax 曲线急剧上升，反映出低成本运行的

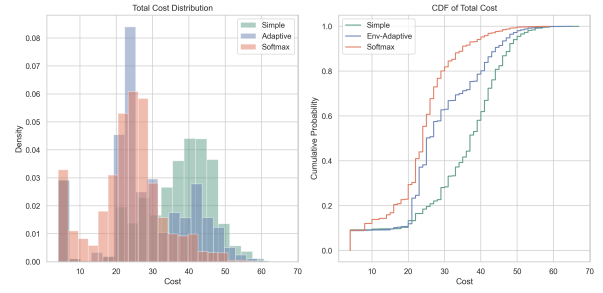


图 6: 总成本分布(左)和总成本的累积分布函数(CDF)(右)在不同模型中的情况。

紧密聚类，其次是自适应模型，然后是静态模型，其斜率最慢且成本变异性最高。

B. 关键见解与解读

结果突出了将环境反馈纳入备用策略的价值。虽然静态模型在应对动态干扰方面遇到困难，但自适应版本通过响应威胁级别显示出适度的改进。相比之下，softmax 模型表现得更加稳健——更有效地恢复效用同时保持较低的成本。不过，该框架有其局限性。我们的威胁场景被建模为离散事件，这简化了现实世界中中断的连续性质。捕捉更长期的依赖关系，例如持续干扰如何影响能耗或恢复可行性，将提高真实感。此外，从离线参数调优转向在线学习可以进一步改善实时鲁棒性。

VII. 结论

我们对三种 PACE 变体——静态、自适应和基于 softmax 的——进行的评估显示，传统的静态冗余在危机期间无法维持效用，通常会导致退化或失败状态。自适应模型通过环境意识提高了韧性，但在压力下仍然存在问题。基于 softmax 的模型始终优于其他两种模型，实现了更高的恢复率、更低的成本以及最高的韧性指数 (DREI)。

这些结果提供了三个关键见解：(1) 韧性需要实时适应动态威胁；(2) 轻量级、基于奖励的决策机制可以在不进行大量计算的情况下提供强大的性能；(3) 分层降级策略可以增强任务连续性并降低失败风险。

致谢

本工作部分得到了加拿大研究主席计划 (Tier 1) 的支持。作者也想向 NorthStar Earth & Space 团队表

示感谢, 包括 Narendra Gollu、Naron Phou、Noemi Giannichele、Yann Picard、Jean-Claude Leclerc、Srinivas Setty 等人, 感谢他们的讨论、技术见解和合作支持。

参考文献

- [1] K. A. Bingen, K. Johnson, and Z. Malekos Smith, “Russia threatens to target commercial satellites,” 2022.
- [2] A. Lele, “Remembering starfish prime,” *The Space Review*, 2024.
- [3] C. Pavur and I. Martinovic, “Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight,” *Proceedings of the IEEE Symposium on Security and Privacy*, 2022.
- [4] G. Falco and L. Boschetti, “Minimum requirements for space system cybersecurity – ensuring cyber access to space,” *IEEE Aerospace and Electronic Systems Magazine*, 2019.
- [5] A. Murat and *et al.*, “An overview of secure by design: Enhancing systems security through systems security engineering,” *IEEE Transactions on Dependable and Secure Computing*, 2023.
- [6] X. Sun and *et al.*, “A combined physics of failure and bayesian network reliability analysis method for complex electronic systems,” *IEEE Transactions on Reliability*, 2022.
- [7] J. O’ Halloran and *et al.*, “A graph theory approach to functional failure propagation in early complex cyber-physical systems design,” *Reliability Engineering & System Safety*, 2017.
- [8] W. Xia, Y. Wang, and Y. Hao, “Modeling failure propagation to analyze the vulnerability of the complex electromechanical systems under network attacks,” *Physica A: Statistical Mechanics and its Applications*, vol. 613, p. 128514, 03 2023.
- [9] M. Glaser, K. Greiner, B. Hilburn, J. Justus, C. Walsh, W. Dallas, J. Vanderpoorten, J.-C. Chuang, and C. Sunshine, “Protected milsatcom design for affordability risk reduction (dfarr),” in *MILCOM 2013 - 2013 IEEE Military Communications Conference*. IEEE, 2013, pp. 998–1003.
- [10] R. H. Jacobsen and A. Marandi, “Security threats analysis of the unmanned aerial vehicle system,” in *MILCOM 2021 - 2021 IEEE Military Communications Conference*. IEEE, 2021, pp. 316–320.
- [11] U.S. Department of the Army, *FM 6-02: Signal Support to Operations*, 2023.
- [12] —, *Army Techniques Publication 4-02.43: Army Health System Support to Special Operations Forces*, 2023, aTP 4-02.43.
- [13] T. Winniford, “Prioritizing resources: Pace yourself,” *EMS1*, 2025.
- [14] Cybersecurity and Infrastructure Security Agency, “Leveraging the pace plan in the emergency communications ecosystem,” 2023.
- [15] A. Jacobs, A. George, H. Lam, and H. Siegel, “Reconfigurable fault tolerance: A framework for environmentally adaptive fault mitigation in space,” *ACM Transactions on Reconfigurable Technology and Systems*, vol. 5, no. 4, pp. 1–30, 2012.
- [16] A. George, H. Quinn, and K. Morgan, “Hybrid, adaptive, reconfigurable fault tolerance (harft) for spaceflight computing,” in *2017 IEEE Aerospace Conference*. IEEE, 2017, pp. 1–10.
- [17] X. Yi, Y. Zhang, J. Li, and Q. Wang, “Application of knowledge graph technology with integrated feature data in spacecraft anomaly detection,” *Applied Sciences*, vol. 13, no. 19, p. 11024, 2023.
- [18] J. Willbold, M. Schloegel, M. Vögele, M. Gerhardt, T. Holz, and A. Abbasi, “Space odyssey: An experimental software security analysis of satellites,” *arXiv preprint arXiv:2305.20081*, 2023.
- [19] G. Falco and N. Boschetti, “A security risk taxonomy for commercial space missions.” American Institute of Aeronautics and Astronautics, 2021.
- [20] E. U. A. for Cybersecurity (ENISA), “Space threat landscape,” ENISA, Tech. Rep., 2025.
- [21] G. Baselt, J. Pavur, I. Martinovic, M. Strohmeier, and V. Lenders, “Security and privacy issues of satellite communication in the aviation domain,” in *14th International Conference on Cyber Conflict (CyCon 2022)*. NATO CCDCOE, 2022.
- [22] R. Morales-Ferre, V. Bouchereau, G. Daruis, and I. Henkel, “A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2830–2885, 2020.
- [23] Deloitte Insights, “Defending space systems against cyber threats,” *Deloitte Center for Government Insights*, 2024.
- [24] C. Kopp, “The electromagnetic bomb—a weapon of electrical mass destruction,” *Air & Space Power Journal*, 1996.
- [25] G. Falco, “When satellites attack: Satellite-to-satellite cyber attack, defense and resilience,” in *ASCEND*, 2020.