

题目编号：SH-04

针对航天智能算法可靠性与漏洞对抗解决方案挑战赛比赛方案

一、发榜单位

中国航天科技体系与创新研究院

二、题目名称

针对航天智能算法可靠性与漏洞对抗解决方案挑战赛

三、题目介绍

（一）题目背景

航天领域算法需满足小样本学习与高可靠性的双重特性，但其运行环境常面临强干扰、高实时性的极端条件，导致传统漏洞测试方法难以适用。现有测试方案存在计算资源消耗大（如对抗样本生成需海量迭代）、依赖完整训练数据集（航天数据获取成本高）等问题，难以满足快速定位漏洞的实际需求。因此，亟需开发一种低计算成本、低数据依赖、高漏洞发现率与高测试速度的航天算法漏洞检测方案，定位算法实际价值。

（二）技术需求

1. 计算效率优化

通过动态批处理、模型蒸馏等技术减少模型推理次数，目标是将单次测试需要模型的推理次数减少至 10^3 次以内，越低越

好。

2.数据依赖最小化

避免依赖完整训练数据集，提出基于迁移学习或增量学习的解决方案，仅需少量领域数据即可完成漏洞挖掘。数据需求 $\leq 10\%$ 原始数据，越低越好。

3.漏洞覆盖全面性

覆盖至少 3 类漏洞，并精准定位漏洞触发路径，定位准确率需 $\geq 85\%$ 。

通过聚焦航天领域高价值、低门槛、可落地的算法安全难题，参赛者需在创新性（如提出混合测试框架）与效率（如计算资源优化）之间取得平衡，最终成果将推动航天算法安全技术的产业化应用。

（三）技术意义

本题目聚焦航天领域算法漏洞测试，旨在突破高可靠性、小样本环境下的算法安全防护技术瓶颈，对解决我国航天领域“卡脖子”难题具有重要战略价值。当前，航天器控制、卫星通信等关键系统高度依赖复杂算法，但其面临对抗样本攻击等漏洞威胁时，传统测试方法存在计算资源消耗大、数据依赖性强、场景适配性差等缺陷，严重制约算法可靠性提升。通过构建低计算成本、高漏洞发现率的测试方案，本赛题将推动国产算法安全技术从“被动防御”向“主动免疫”转型，助力攻克极端环境（如高动态、强干扰）下算法鲁棒性提升等核心技术壁垒。

此外，本赛题成果可直接应用于航天器自主运行系统、星载 AI 故障诊断等场景，为我国航天装备的全生命周期安全保障提供技术支撑，减少对国外算法安全工具的依赖，有效维护国家空间信息安全。同时，通过推动算法漏洞检测技术的开源化与标准化，可赋能智能制造、工业控制等领域，为解决人工智能算法安全这一全球性难题贡献中国方案，助力实现高水平科技自立自强。

四、参赛对象

本题目只设学生赛道。

参赛对象为 2025 年 6 月 1 日以前正式注册的全日制非成人教育的各类高等院校在校专科生、本科生、硕士研究生、博士研究生（不含在职研究生），参赛人员年龄在 40 周岁以下，即 1985 年 6 月 1 日（含）以后出生。

同一作品不得同时参加第十九届“挑战杯”全国大学生课外学术科技作品竞赛（以下简称第十九届“挑战杯”竞赛）其他赛道的评比。

参赛对象可以团队或个人形式参赛，每个团队不超过 10 人，每件作品可由不超过 3 名指导教师进行指导。可以跨专业、跨学校、跨单位、跨地域组队，但同一团队所有成员均应符合本赛道相关年龄、身份要求。每件作品只可由 1 所高等院校作为参赛主体提交申报。

五、答题要求

1.作品形式

技术方案报告：需包含漏洞测试方法设计、模型案例分析、场景降级实现逻辑等，字数不少于 3000 字，需明确标注引用文献来源。

实验代码与模型：提供可复现的代码（推荐使用 PyTorch/TensorFlow 框架），并附模型架构说明（如基于大语言模型的漏洞检测模型）。

场景降级案例：需自行构造至少 3 个测试场景（如极端环境下的模型误判、长期运行参数漂移），并展示漏洞触发与修复过程。

2.技术内容

漏洞测试方法：需结合红蓝对抗机制，提出低计算成本、低数据依赖的解决方案，例如动态模糊测试与符号执行结合，或基于迁移学习的增量测试等。

模型案例：选择公开模型（如 BERT、YOLO）或自研模型，展示其在对抗样本攻击等场景下的漏洞表现，并对比传统方法（如 FGSM）的效率差异。

场景降级实现：需模拟航天、工业控制等领域的实际环境（如高实时、强干扰），通过代码注入或参数修改实现算法降级，并验证防御策略有效性。

3.创新性要求

避免使用已成熟技术（如传统黑盒攻击），聚焦 AI 驱动的漏洞发现（如基于大模型的代码语义分析）或动态防御机制（如模型水印与溯源）。

需明确说明是否依赖原始训练数据集，若依赖则需量化数据量需求（如 $\leq 10\%$ 原始数据）。

六、作品评选标准

（一）评选维度与权重

本评选标准从技术先进性（40%）、方案可行性（30%）、创新性（20%）、成果转化潜力（10%）四个维度综合评定，具体细则如下：

1. 技术先进性（40%）

① 计算效率

迭代次数限制：要求漏洞检测算法在 100 次迭代循环内发现有效漏洞（如对抗样本或参数漂移），对比传统方法（如 FGSM 需 10^5 次迭代）的效率提升需 $\geq 40\%$ 。

测试速度：单次完整测试（含漏洞生成、模型推理、结果分析）耗时需 ≤ 5 分钟，支持并行计算优化。

② 检测精度

漏洞覆盖度：需覆盖至少 3 类人工智能典型漏洞，且漏洞定位准确率 $\geq 85\%$ 。

2. 方案可行性（30%）

① 航天场景适配性

测评手段：需明确说明在航天典型环境下的测试方法。

数据依赖：若依赖原始训练数据集，需量化数据需求（如 $\leq 10\%$ 原始数据），并说明迁移学习或增量学习方案的有效性。

②工程可实施性

工具链完整性：提供开源代码或 SDK（支持 PyTorch/TensorFlow 框架），包含数据预处理、漏洞生成、测试执行与结果分析模块。

3.算法缺点评价指标（创新性补充，20%）

漏洞误判率：在正常输入中错误标记为漏洞的比例，需 $\leq 5\%$ 。

可解释性：需提供漏洞触发路径的可视化分析（如热力图、决策边界图），缺失则扣分。

（二）等次划分与评分细则

等次	技术先进性	方案可行性	创新性	成果转化
一等奖	≥ 35 分	≥ 25 分	≥ 15 分	≥ 8 分
二等奖	30-34 分	20-24 分	10-14 分	5-7 分
三等奖	25-29 分	15-19 分	5-9 分	2-4 分

评分说明：

创新性：聚焦动态模糊测试与符号执行结合、AI 驱动的漏洞语义分析等前沿方向，避免复用成熟技术（如传统黑盒攻击）。

成果转化：要求提交开源工具或行业标准草案（如漏洞检测 SDK 接口规范），推动航天企业实际应用。

七、作品提交时间

2025 年 5 月-8 月，参赛团队所在高校应组织学生参赛，安排专业人员给予指导，为参赛团队提供支持保障。

2025 年 8 月 15 日前，各参赛团队通过大赛申报系统提交作品，具体要求详见作品提交方式。

2025 年 8 月底前，由大赛组委会会同发榜单位共同完成初审，确定入围终审擂台赛的晋级作品和团队。

2025 年 9 月，发榜单位安排专门团队提供帮助和指导，各晋级团队完善作品，冲刺攻关参加终审擂台赛，角逐“擂主”。

八、参赛报名及作品提交方式

（一）报名方式

（1）参赛选手登录“挑战杯”官网 2025.tiaozhanbei.net，在“揭榜挂帅”擂台赛报名入口注册账号，登录大赛申报系统在线填写报名信息。报名信息提交后，下载打印系统生成的报名表。

（2）申报人在报名表对应位置加盖所在学校公章。

（3）将盖章版报名表扫描件上传至报名系统，等待系统审核。请参赛选手注意查看审核状态，如审核不通过，需重新提交。

（4）系统开放报名时间为 2025 年 5 月 30 日—6 月 30 日，逾期后系统将自动关闭报名功能。

（二）作品提交方式

申报作品（包括技术报告、实验代码与模型、测试数据及

案例、视频或其他展示形式提交的支持材料等）应统一打包压缩提交至大赛申报系统，压缩包命名方式为：申报人所在单位-申报人姓名-作品名称-联系电话（例如：XX 大学-张 XX-XX 方案-手机号）。

若压缩包过大，请同步以光盘刻录方式线下提交至发榜单位。以该种方式提交作品时，请一并提交 1 份报名系统中审核通过的参赛报名表（所有信息须与系统中填报信息严格保持一致）。邮寄方式请联络该榜题赛事服务团队（联系方式后附）。

九、赛事保障

赛事进行中，发榜单位可为参赛者提供技术指导与帮助、相应的研发平台与工具指导，助力参赛者提升参赛效率。如有需要请联络该榜题技术支持团队（联系方式后附）。

十、设奖情况及奖励措施

1. 设奖情况

该榜题设擂主 1 个、特等奖 5 个、一等奖 6 个、二等奖 8 个、三等奖 10 个。最终授奖数量视作品申报数量和质量情况，报组委会同意后动态调整。

2025 年“揭榜挂帅”擂台赛学生赛道获奖情况将按照一定分值计入第十九届“挑战杯”竞赛学校团体总分，具体分值以第十九届“挑战杯”竞赛章程为准。青年科技人才赛道获奖情况不纳入学校团体总分计分范围。

2. 奖励措施

“擂主”：设奖金 10 万元，颁发荣誉证书及奖杯。优先获得航天科技集团体系与创新研究院等单位的 1 年以上的带薪实习岗位，参与核心算法研发项目。就业支持方面，直接进入合作企业“联培生计划”，享受硕士/博士毕业生同等待遇。

特等奖：设奖金 1 万元，颁发荣誉证书及奖杯。优先获得航天科技集团体系与创新研究院等单位的 6 个月带薪实习岗位，参与核心算法研发项目。就业支持方面，直接进入合作企业“联培生计划”，享受硕士/博士毕业生同等待遇。

一等奖：设奖金 4000 元，颁发荣誉证书及奖杯。提供航天科技集团体系与创新研究院等单位 1 个月短期实训，接触控制算法漏洞测试场景。就业支持方面，提供绿色通道：在航天系统校园招聘中免笔试，直接进入面试环节。

二等奖/三等奖：设奖金 2000 元/1000 元，颁发荣誉证书及奖杯。

3. 奖金发放方式

获奖名单公示后 30 个工作日内，专班工作人员与获奖团队取得联系，启动奖金发放流程，将奖金一次性发放至获奖团队提供的银行卡中。实习/就业机会于赛后 1 年内落实。

十一、比赛专班联系方式

1. 专家指导团队

顾问专家：潘老师，联系电话：18910516879

顾问专家：林老师，联系电话：17816861463

负责比赛期间技术指导保障。

2. 赛事服务团队

联络专员：李老师，联系电话：18701778676

联络专员：尤老师，联系电话：18742593095

负责比赛期间组织服务及后期相关赛务协调联络。

3. 联系时间

比赛期间工作日（9:00-17:00）。

附：发榜单位简介

中国航天科技体系与创新研究院是中国航天科技集团有限公司所属以航天领域重大科技战略研究、重大体系工程项目论证、人工智能应用生态建设和前沿颠覆性研究为主的中央登记事业单位。