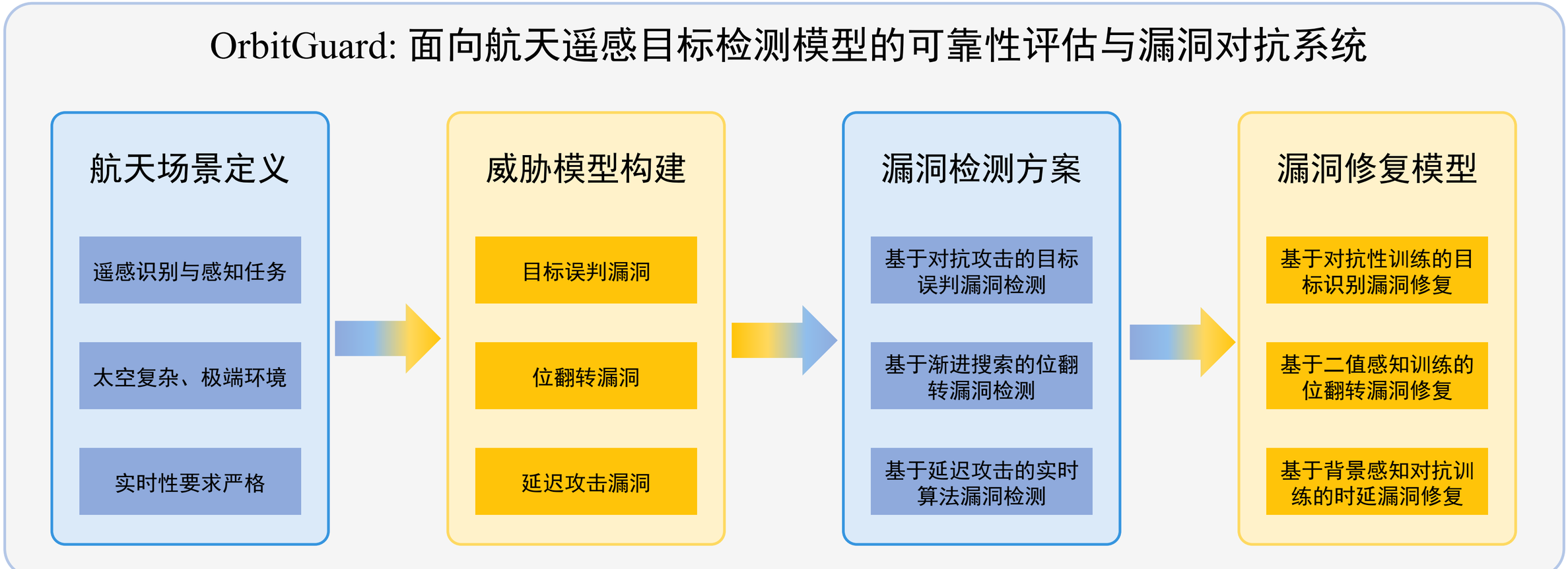
OrbitGuard: 面向航天遥感目标检测模型的可靠性评估与漏洞对抗系统
航天场景定义
遥感识别与感知任务
太空复杂、极端环境
实时性要求严格
威胁模型构建
目标误判漏洞
位翻转漏洞
延迟攻击漏洞
漏洞检测方案
基于对抗攻击的目标误判漏洞检测
基于渐进搜索的位翻转漏洞检测
基于延迟攻击的实时算法漏洞检测
漏洞修复模型
基于对抗性训练的目标识别漏洞修复
基于二值感知训练的位翻转漏洞修复
基于背景感知对抗训练的时延漏洞修复