Fuzzing-Guided Static Analysis: From a Reinforcement Learning Perspective

Dongjae Lee

2025.03.31

Abstract

Recent fuzzing research has evolved to conduct efficient fuzzing campaigns based on static analysis information. However, while fuzzing leverages static analysis, the reverse direction remains unexplored. I propose an approach to refine static analysis using fuzzing results and formulate it as a RL problem.

Modern fuzzing techniques (e.g., Directed Fuzzing) heavily rely on static analysis information to guide their fuzzing campaigns. However, the success of these campaigns can be significantly limited when static analysis produces imprecise results, often due to its dependence on human-designed heuristics.

The key insight is that fuzzing results provide ground truth about program behavior. This information could help refine static analysis in two ways: recovering information lost due to unsound analysis and eliminating spurious results from overly conservative analysis. This bidirectional relationship creates a positive feedback loop between static and dynamic analysis.

From RL perspective, static analysis results serve as a model of the actual environment, which is the concrete program. The fuzzer performs fuzzing by selecting appropriate policies (e.g., selective coverage, energy distribution) based on this model. After collecting sufficient fuzzing results, we can improve the model (static analysis results) based on that information. Fuzzing using the improved model would be more efficient than before.

This problem can be formulated as a model-based, off-policy RL problem. This formulation differs clearly from existing RL-based fuzzing research, which primarily considers the fuzzing process itself without static analysis. By combining knowledge from the existing RL field with insights from fuzzing and static analysis, I believe we can solve this problem.