DOI: 10.7544/issn1000-1239.ps20230701
60(7): 1431−1431, 2023

优化无人驾驶系统仿真模糊测试

沈学民

（滑铁卢大学　加拿大安大略省滑铁卢市）

无人驾驶系统的安全测试主要包括仿真测试和实景道路测试. 其中，仿真测试因其支持灵活配置虚拟驾驶场景而受到广泛关注. 仿真测试的核心挑战在于，如何在庞大的虚拟场景配置空间中搜索和发现容易导致安全事故的场景. 将模糊测试技术与仿真测试相结合，构建面向无人驾驶系统的仿真模糊测试技术是解决上述挑战的潜在方案之一.

复旦大学的杨珉教授团队撰写的“面向无人驾驶系统的仿真模糊测试：现状、挑战与展望”一文介绍了无人驾驶系统仿真模糊测试的基本架构，并梳理了此架构下的关键模块. 针对事故挖掘场景，该文剖析了各关键模块所面临的设计挑战，给出了对应的优化思路，并在主流无人驾驶系统上进行了可行性实验论证. 具体来说，该文包含以下 3 个主要贡献：

1. 提出了一种高质量种子场景的自动化构建方法，通过引入真实世界中车辆和行人的轨迹数据，自动化地构建了高质量的种子场景，解决了依赖个人经验的手工生成方式导致的种子场景质量不高的问题. 在 Apollo 系统上的测试结果表明，该种子场景构建方法在事故挖掘能力方面相较于现有工作最少提升了 203%.

2. 提出了一套基于事故主体和事故特性的分类体系，通过对挖掘到的大量事故场景进行相似性聚类，实现了准确的事故分类，同时避免了不必要的分析开销. 在涉及 50 种事故类型的 500 例事故场景的分类任务中，该体系的分类准确率远高于现有方案 AutoFuzz.

3. 提出了一种定制化的事故归因分析方法，通过实时地监控比对仿真场景中各元素的状态与无人驾驶系统的模块执行信息，有效识别事故主责模块. 实验结果表明，在 50 个事故场景中，该方法能正确地分析出其中 44 个缺陷所在的功能模块，平均用时 0.05 小时，相比人工分析的平均用时 4.4 小时，显著提高了事故归因效率.

仿真模糊测试对提升无人驾驶系统的安全性至关重要，而一套优秀的仿真模糊测试方法体系的形成往往需要经历长时间的研究与实践. 其原因是，对仿真模糊测试架构进行模块化拆解，需要深入理解仿真测试与模糊测试的关系和互相作用. 而针对各模块分别提出合理的优化方案，则需要系统性地掌握包括模糊测试、代码分析、编译优化、数据挖掘等在内的一系列基础知识. 该文对无人驾驶系统仿真模糊测试进行了深刻而全面的阐述，走出了具有启发性的一步. 这是源于作者团队过去 10 余年在软件应用程序漏洞挖掘与分析方面的长期探索和积累. 我相信，随着无人驾驶系统安全测试领域的不断发展，该文在学术研究和产业实践方面将会起到越来越重要的指引和推动作用.

评述专家：

沈学民，IEEE 通信学会主席，IEEE Fellow，加拿大滑铁卢大学杰出教授，加拿大工程院院士，加拿大工程研究院院士，加拿大皇家科学院院士，中国工程院外籍院士. 主要研究方向为无线通信网和车联网等.

亮点论文：

戴嘉润，李忠睿，张婉琪，张源，杨珉. 面向无人驾驶系统的仿真模糊测试：现状、挑战与展望 [J]. 计算机研究与发展，2023，60(7)：1433−1447. DOI: 10.7544/issn1000-1239.202330156