Systems and Computer Engineering
Carleton University
1125 Colonel By Drive
Ottawa, ON K1S 5B6

August 18, 2021

Position Available: M.A.Sc. Candidate

Reinforcement Learning for Security Testing of State Machine Models

A Master's-level research position on the topic of *Reinforcement Learning for Security Testing of State Machine Models* is available starting in January 2022.

Project Description

The rise of Machine Learning (ML) has been enabling new and improved ways to solve problems in many domains. This research project aims to employ ML to improve the testing of software systems, which accounts for approximately 50% of software development costs. More specifically, we investigate the application of Reinforcement Learning (RL), a subfield of ML, for effective and scalable testing of State Machine (SM) models, which have been extensively used in the development of software for Real-time Embedded (RTE) systems. We are particularly interested in applications related to the testing of security-critical systems. RL has shown great potential in various challenging areas, such as game playing and recommender systems. In the software engineering context, researchers have also reported promising results for RL applications in the testing of mobile applications, property based testing, and test selection and prioritization of regression tests. Inspired by this line of work, this project seeks to develop novel and timely methods that leverage RL techniques to efficiently exercise the SM models against a diverse set of inputs to maximize the likelihood of detecting faults and security vulnerabilities while keeping the costs manageable.

Project Keywords:

- reinforcement learning
- machine learning
- software testing
- security testing
- software engineering
- state machine models

Objective

The long-term objective of this research is to develop an effective and scalable solution to test SM models of RTE systems using RL techniques. The targeted systems are advanced RTE systems (e.g., control model of a self-driving car) with an input space so large that the application of any existing exhaustive testing techniques is infeasible. This MASc thesis contributes to this matter by addressing the following short-term objectives:

1. A reinforcement agent learns via interaction with an environment, through the use of feedback provided as observations (states) and rewards. Therefore, as the first objective, the testing of an SM model needs to be mapped to an RL problem. To address this, we seek to develop an efficient execution engine of SM models to provide the environment for executing test cases and a tool that takes SM models as input and generates an RL environment, i.e., a skeleton of an agent, and its interaction with the environment.
2. We aim to use the result of the first objective and advanced RL techniques to conduct a comprehensive analysis of how well the RL agent can perform in the testing of SM models using different configurations of RL techniques, reward functions, and state representations.

Related Literature References

[1] M. Bagherzadeh, N. Kahani, and L. Briand. Reinforcement learning for test case prioritization. IEEE Transactions on Software Engineering, pages 1-21, 2021.

[2] M. Pan, A. Huang, G. Wang, T. Zhang, and X. Li. Reinforcement learning based curiosity-driven testing of android applications. In Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis, pages 153–164, Association for Computing Machinery, New York, NY, USA, 2020.

[3] S. Reddy, C. Lemieux, R. Padhye, and K. Sen. Quickly generating diverse valid test inputs with reinforcement learning. In Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering, pages 1410–1421, Association for Computing Machinery, New York, NY, USA, 2020.

[4] A. S. Kalaji, R. M. Hierons, and S. Swift. Generating feasible transition paths for testing from an extended finite state machine (EFSM). In Proceedings of the 3rd International Conference on Software Testing, Verification, and Validation Workshops, pages 232-235, IEEE, 2010.

[5] J. Jaskolka. Recommendations for effective security assurance of software-dependent systems. In K. Arai, S. Kapoor, and R. Bhatia, editors, Intelligent Computing, SAI 2020, volume 1230 of Advances in Intelligent Systems and Computing, pages 511–531. Springer, Cham, 2020.

Desired Skills/Qualifications

Suitable candidates will have a Bachelor's degree in Software Engineering, Computer Science, or a related field. Ideal candidates will be self-motivated with an ability to work independently and to communicate effectively in a team environment. A background in machine learning, specifically reinforcement learning, and software testing is highly desirable. Experience with various security concepts, including security testing, is considered an asset.

All candidates must satisfy the Minimum Admission Requirements for Master's Programs at Carleton University. International candidates must also ensure that they satisfy the English as a Second Language Requirements. In all cases, these requirements will be strictly enforced when evaluating an application for admission.

Funding

Successful candidates for this position will be *eligible for funding* in the form of a research assistantship. Specific funding details are determined at the time of offer and consider numerous factors such as academic standing, research potential, availability of funds, eligibility for teaching assistantship and/or scholarships, etc.

Supervision

This position will be co-supervised by:

- Dr. Nafiseh Kahani (kahani@sce.carleton.ca), and
- Dr. Jason Jaskolka (jason.jaskolka@carleton.ca).

Host Research Institute Information

Carleton University is a public comprehensive university, founded in 1942, in Ottawa, Ontario, Canada. The research-intensive Faculty of Engineering and Design at Carleton University is recognized as one of Canada's leading institutions in the study and research of engineering, architecture, industrial design and information technology. Since the inception of engineering at Carleton in 1945, our experts have pushed the bounds of innovation and discovery. Carleton focuses on anticipating the needs of industry and society, and offers forward-thinking programs with real world application and produces research that is helping to shape our present and future. The Department of Systems and Computer Engineering is a recognized world-class institution in software engineering, computer systems engineering, communications engineering, and biomedical engineering. Together with the Department of Electronics, the Department of Systems and Computer Engineering constitutes one of the largest and most research-intensive centres for Electrical and Computer Engineering and Software Engineering education and research in Canada.

Application Instructions and Further Information

Interested applicants are to send a **CV** and **Statement of Interest** detailing your research interests, background, and experience by email to: kahani@sce.carleton.ca and jason.jaskolka@carleton.ca.

Application Deadline: Applications will be reviewed as they arrive until a suitable candidate is found.