Carnegie Mellon University
Computer Science Department

THESIS PROPOSAL

Deborah Katz

Identification of Software Failures in Complex Systems Using Low-Level Execution Data

Friday, December 7, 2018 – 2:30 p.m. – GHC 8102

Autonomous systems -- systems that are designed to react independently and without human supervision to various stimuli in the environment – are big, complex, and difficult for humans to supervise and are an increasingly large portion of the systems being developed and in use today.
In many of these systems, early knowledge of a fault would allow costly and safety-critical failures to be avoided.

My key insight is that I can look to typical program behavior as a basis for determining whether a program is operating within its normal parameters. To do this, I can record summaries of program behavior using low-level execution data to characterize each execution. By aggregating low-level execution data over many executions, I can create a picture of typical program behavior and suggest that a program behaving differently may be exhibiting unintended behavior. My techniques use the collected data as input to machine learning algorithms which build models of expected program behavior. I use these models to analyze individual program executions and make a prediction about whether the given execution represents typical behavior.

My core thesis is: Low-level execution signals recorded over multiple executions of a program or portion thereof can be used to create models that, in turn, can be used to evaluate whether signals from previously-unseen executions represent usual or unusual behavior. The combination of low-level instrumentation and models can provide useful evaluations with reasonable trade-offs between accuracy, intrusiveness, and efficiency.

To support this thesis I have conducted preliminary work. I have used dynamic binary analysis on small programs to construct supervised and unsupervised machine learning models to detect program executions that exhibit errors. I have instrumented simulations of the ArduPilot autonomous vehicle software to construct machine learning models to identify executions with errors.

I propose to conduct work evaluating novelty detection techniques on varied robotics programs. I further propose to refine my techniques for instrumenting program executions by evaluating trade offs in approaches to reduce overhead in instrumentation, a nontrivial problem because overhead can perturb execution paths in timing-sensitive programs. By reducing overhead but retaining meaningful information, I may be able to reach parts of programs previously unreachable by my instrumentation techniques.

I propose to evaluate the new work on several robotics and autonomous systems in simulation. I plan to evaluate accuracy in identifying program faults. I also plan to evaluate intrusiveness and efficiency of instrumentation and to evaluate the trade offs between these two sets of factors.

Thesis Committee:
Claire Le Goues, Chair
Phil Koopman
Dan Siewiorek
Eric Schulte, Grammatech, Inc.

Thesis Summary: https://www.cs.cmu.edu/~dskatz/dsk_proposal.pdf