ADSC
Illinois at Singapore Pte Ltd

SEMINAR NOTICE:

Verification of Embedded Simulink Models using Formal Methods

Nannan He

Post-Doctoral Research Assistant in
the Department of Computer Science
at Oxford University

TIME & LOCATION:

Illinois:
Tuesday, January 24 at 7:30 p.m.
Coordinated Science Lab - Room 238
ADSC Videoconference Room

Singapore:
Wednesday, January 25 at 9:30 a.m.
@ ADSC - Level 8, Fusionopolis,
Connexis North

Abstract:

Model-based design is a development methodology for modern software artifacts. The implementation of the system is either generated or derived manually from high-level models. The Matlab/Simulink language, developed by The MathWorks, has emerged as the predominant modeling formalism in many embedded applications, where a software glitch in these applications may result in high cost and considerable damage of reputation. Due to the safety-critical nature of these domains, defects in the software may put human lives at stake. Therefore, the effort to create appropriate test suites that exercise the implementation of the system according to certain coverage metrics, is substantial, and the execution of the test suites is time consuming.

In this talk, I focus on one kind of fault-based testing technique: mutation testing. Mutation testing works by injecting syntactic mutations into the model of interest, and then trying to derive test cases that can distinguish between the original and mutated models, and has proved effective for generating high-quality test suites for software systems. However, the lack of formal semantics for the Simulink language, the heavy use of floating-point arithmetic in Simulink models and the high complexity of mutation testing make mutation-based test case generation for Simulink a significant challenge.

In order to address the discussed challenges in the mutant-based test case generation (TCG) for Simulink models, we have designed precise and efficient test-case generation strategies. These TCG strategies are precise in the two senses. First, the use of bounded model checking and bit-precise modeling of floating-point calculations makes it possible to explore the behavior of Simulink models with high precision, taking intricate details such as the actual floating-point semantics of execution platforms into account. Secondly, we achieve the precise evaluation of mutation coverage by applying the k-induction method to equivalence checking of equivalent Simulink mutants. By combining white-box testing with formal concept analysis which exploits similarity measures on mutants, we are able to generate small sets of short test-cases that achieve high coverage on a collection of Simulink models from the automotive domain.

Biosketch:

Nannan He is a research assistant (post-doc) at the department of Computer Science (formally "Computing Laboratory") in Oxford University, UK. She received her doctoral degree in Computer Engineering in May 2009 at Virginia Tech, US. Her primary research interests include applied formal methods especially SAT/SMT based model checking, decision procedures and automatic abstraction, computer-aided software verification and security, model-based development and testing of embedded software.