PhD Defense Presentation

Wednesday, May 27, 2015
10:00am – 12:00pm

3105 Engineering Building

“AUTOMATED ADDITION OF FAULT-TOLERANCE VIA LAZY REPAIR AND GRACEFUL DEGRADATION”

By Yiyan Lin

Advisor: Sandeep Kulkarni
In this dissertation, we concentrate on the problem of automated addition of fault-tolerance that transforms a fault-intolerant program to be a fault-tolerant program. We solve this problem via model repair. Model repair is a correct-by-construct technique to revise an existing model so that the revised model satisfies the given correctness criteria, such as safety, liveness, or fault-tolerance. We consider two problems of using model repair to add fault-tolerance. First, even if a repaired model satisfies all correctness criteria, the model is hard to be realized as a valid program if the realizability constraints of underlying system cannot be preserved. Second, addition of fault-tolerance may fail if the program cannot fully recover after certain faults occur. In this dissertation, we propose a lazy repair approach that to address realizability issues in adding fault-tolerance. Additionally, we propose a technique to automatically add graceful degradation to a program, so that the program can recover with partial functionality if fully recovery is impossible.

Designing an efficient adding fault-tolerance algorithm for programs with realizability constraints is difficult. Existing adding fault-tolerance techniques address realizability issues in distributed programs by introducing heuristics. However, it is difficult to apply this heuristic-based approach to other domains, e.g., synchronous programs, cyber-physical programs, etc. It is because this approach is designed and optimized specifically for distributed programs in terms of the application of the heuristics. Additionally, the development of these heuristics is complicated. Hence, in this dissertation, we propose a more generic approach, i.e., lazy repair, to add fault-tolerance. It involves two steps. First, we only focus on repairing to obtain a model satisfies correctness criteria while ignoring realizability constraints. In the second step, we repair this model further by removing behaviors while ensuring that the desired specification is preserved. The lazy repair approach simplifies the process of developing heuristics, and provides a tradeoff in terms of the time saved in the first step and the extra work required in the second step. We demonstrate that lazy repair is applicable in the context of distributed systems, synchronous systems and cyber-physical systems.

Additionally, safety critical systems such as airplanes, automobiles and elevators always require high dependability even under harsh environment. However, existing adding fault-tolerance techniques may fail if the occurrence of faults break down some components of the system and prevent the system from fully recovery. In this scenario, it is still possible for a system to operate with remaining resources and deliver partial but core functionality, i.e., to display graceful degradation. In this dissertation, we propose a technique of adding fault-tolerance to a program with graceful degradation. In the absence of faults, such a program exhibits ideal behaviors. In the presence of faults, the program is allowed to recover with a reduced guarantee of original system requirements. This technique involves two steps. First, it automatically generates a program with graceful degradation based on the input fault-intolerant program. Second, it adds fault-tolerance to the output program from first step. We demonstrate that this technique is applicable in the context of high atomicity programs as well as low atomicity programs (i.e., distributed programs).