Department of Mathematics, Statistics and Computer Science
St. Francis Xavier University
Presents

Towards Distributed Model Checking of Real-time Systems

by

Dr. Hao Wang
Post-Doctoral Fellow
Department of Mathematics, Statistics and Computer Science
St. Francis Xavier University

March 20th, 2009 @ 2:15 in Annex 23a

This talk presents part of our progress on formal verification in distributed computing environment. *Model checking* is an automatic formal method which explores all possible states of a modeled system to verify whether the system satisfies a formally specified property. It became popularized in industrial applications, e.g., computer hardware and software. However, it suffers from the well-known problem of *state explosion*. One promising way to tackle this problem is to utilize the power of distributed computing. *DiVinE* is a distributed model checker which has been proved to achieve (much) better performance than its sequential counterpart, the well-known *SPIN* model checker.

Timed model checking, the method to verify real-time systems, is important in the model checking community. One problem with DiVinE and SPIN is that their modeling languages can *not* represent quantified time information. We have made some progress in the *Explicit-time Description Method*, which is intended to use ordinary (untimed) model checkers to realized timed model checking. Lamport has proposed an explicit-time description method with a clock-ticking process and a group of global variables for timing constraints. We propose a new method that does not rely on global variables; instead it uses rendezvous synchronization steps and timing constraints can be defined locally permitting a modular approach to system modeling. In addition, our method makes it possible to apply the explicit-time description method in some process-based languages without explicit global variables, e.g., *Communicating Sequential Processes* (CSP) and *Petri Nets*. Both Lamport's method and our method are implemented in DiVinE, which is (to our knowledge) the first time for which the explicit-time description methods have been implemented in a large-scale distributed model checker.

This research is supported partially by an ACEnet postdoctoral research fellowship and all experiments have been run on the ACEnet computing facilities.

Refreshments will be served before the talk in AX24A