NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

PH.D DEFENCE - PUBLIC SEMINAR

Title: **Improved symbolic model checking of real-time systems**

Speaker: Mr Nguyen Truong Khanh

Date/Time: 24 November 2014, Monday, 02:00 PM to 03:30 PM

Venue: Executive Classroom, COM2-04-02

Supervisor : Dr Dong Jin Song, Associate Professor, School of Computing

Abstract:

It is important to verify the correctness of real-time systems before launching them. Although there exist many studies on real-time model checking, it is worth noting that current techniques still encounter the state space explosion problem. The aim of this thesis is to study the symbolic model checking problems of real-time systems and to explore techniques to mitigate the state space explosion problem.

In the literature, the model checking technique based on binary decision diagrams (BDDs) has been shown to be successful in handling the state space explosion. However, the application of BDD-based model checking requires knowledge of BDDs and is difficult for hierarchical systems. Moreover, the performance of BDD-based model checking for real-time systems depends much on the encoding techniques and the magnitude of maximal clock constants. In the first part of this thesis, we present our encoding techniques for real-time systems. We propose to use only tick transitions to explicitly represent the timing requirements. This representation helps to reduce the problem of large maximal clock constants. Furthermore, our encoding techniques include a set of compositional encoding functions which compute the encoding of a system from the encodings of its subsystems. Thus, the encodings of hierarchical systems can be obtained easier by using our compositional encoding functions. Overall, our encoding techniques are general and have been applied to encode closed timed automata and Stateful Timed CSP modeling languages.

With regard to model checking algorithms, interesting problems are reachability analysis and emptiness checking. In the second part of the thesis, we aim to improve the current state-of-the-art algorithms by using the Lower Upper (LU) simulation relation. We prove that the simulation relation preserves not only the reachability but also the emptiness. We also show that symbolically computing the set of reachable states can be enhanced by applying the simulation relation. Specifically, the number of iterations to reach the fixpoint is reduced. The experimental results show that our approach improves significantly the performance.

Then, based on the automata theory that the model checking of linear temporal logic (LTL) properties can be done by checking the emptiness of timed Buchi automata, we extend our framework to support LTL properties.

In summary, the results of this thesis include two improved algorithms for the reachability analysis and the emptiness checking. In addition, a BDD framework is developed to support BDD-based model checking. Specifically, this framework improves the application and the extension of BDD-based model checking. We note that the application of this framework is not restricted to real-time verification. Other domains such as sensor networks and probabilistic models are further examples that can be benefited from our framework.