Model Checking and Testing of Concurrent Systems

Peng Wu

Directed by Prof. Huimin Lin

(Computer Software and Theory)

Abstract

This thesis is devoted to the formal analysis, verification and testing of concurrent systems based on symbolic transition graphs. The main contributions are:

1. A compositional framework is proposed for modeling network protocols using symbolic transition graphs. In this framework, a protocol entity is decomposed into a set of communicating sequential sub-tasks sharing a set of state variables. The model of the entity can then be synthesized from those decomposed sub-tasks in a parallel way. Moreover, the framework supports explicit message passing communication, which can naturally express the working mechanism of a network protocol. For mobile network protocols, the framework can also express dynamic network topologies without the need of introducing additional mobility facilities.
2. The concept of interoperability is defined in the context of the proposed framework. It is shown that interoperability is a sufficient condition to guarantee the deadlock freedom of a network protocol by the deadlock freedom of its sub-tasks. Furthermore, interoperability checking can be performed statically on a symbolic transition graph without referring to the global states of the network protocol under consideration.
3. A case study on Mobile IPv6 is conducted in the proposed framework. The study reveals that Mobile IPv6 can not always maintain binding coherency for mobile nodes and may result in unreachable or unstable routes: that is,\begin{enumerate}
   a) If a home agent acknowledges a *binding update* request from a mobile node before updating its local repository, then all datagrams captured during the

period of these two events will be forwarded to an outdated address;

   b) If a home agent acknowledges a *binding update* request from a mobile node after updating its local repository, then during the period of these two events, the mobile host is unstable in the sense that its roaming capability has not yet been enabled. Any datagram received during this period will be forwarded to the mobile node, of which the behavior is undefined in the specification of IPv6.

4. A first-order sequencing constraint logic(FOSCL) is proposed to represent test purposes for testing concurrent software. The logic incorporates temporal relationships among I/O events, as well as data dependency requirements between the event parameters of these events. Furthermore, an algorithm is developed to automatically generate symbolic test cases that can reflect both temporal relationships among I/O events, as well as data dependency requirements between these event parameters. Via symbolic test cases, test input data can be determined dynamically during interactions with the SUT. A case study shows the FOSCL-based test case generation can achieve transition coverage with smaller number of test steps.

Keywords:

Concurrent Systems, Model Checking, Network Protocol, Mobile IP, Model-Based Testing, Symbolic Test Case, First-Order Sequencing Constraint