Abstract

Web services have become increasingly pervasive in the development of today's enterprise applications, such as e-commerce application. Most workflow and business-to-business collaborative applications require the atomicity property of transaction in order to reach a mutually-agreed outcome. Atomicity ensures this outcome is observed consistently across all of the tasks within the application that comprises the business activity. The results of a task are typically made available before the overall business application or activity completes. The Web Service Atomic Transaction (WSAT) protocol is a framework for the coordination of web services between coordinator and participants during their executions. It provides consistent agreement that has the atomicity, on the outcome of distributed activities of web services. The WSAT protocol is based on Two-Phase Commit (2PC) protocol.

SPIN is a tool for analyzing the logical consistency of distributed systems, specifically of data communication protocols. It can be used in simulator or verifier modes. Given a model system specified in Promela, which is a modeling language, SPIN can either perform random simulations of the model system or analyze its behaviors. If the SPIN verifier encounters error of the system when analyzing, for example, violation of a constraint, we can read the error trace using guided simulation of the SPIN simulator and can conveniently visualize simulation runs. Due to these features, it is suitable to analyze the WSAT protocol by SPIN.

In this thesis, I analyze the WSAT protocol using SPIN. Firstly, I study the 2PC protocol, model it in Promela and verify its atomicity property by SPIN verifier. Then I study the WSAT protocol by its specification in TLA$^+$ by Leslie Lamport [3], together with the informal specification by the Organization for the Advancement of Structured Information Standards (OASIS). At last, the WSAT protocol is modeled in Promela and its correctness is verified by SPIN. Compared with the informal specification and the specification in TLA+, the model in

Promela is closer to the implementation. For an existing implementation, the gap between the implementation and Promela model may be smaller. If an implementation does not exist, the Promela model may provide better guidance for the implementation.

The major contribution of this thesis is the analysis of the WSAT protocol, in particular, the verification of its atomicity property.

Key words: 2PC, WSAT, SPIN, Promela, simulation, verification