Model Checking Lab

Meeting I: Preliminary discussion

Haidi Yue

Software Modeling and Verification Group

Oct. 14, 2010

Model Checking Lab

Aim

Application of Model Checking, learn how to use SPIN.

Tasks

Modeling and verification of distributed algorithms:

- Mutual exclusion protocol:
  Szymanskis protocol [Szy88, p. 621-626]
- Leader election protocol:
  Asymptotically optimal distributed consensus [BG98]
- Electronic commerce protocol:
  Modeling and Model Checking Mobile Phone Payment Systems [KS03]
  Model Checking Electronic Commerce Protocols [HJWW96]
- Routing algorithms:
  Automatized Verification of Ad Hoc Routing Protocols [WPP04]

Organization

Supervision

By appointment, haidi.yue@cs.rwth-aachen.de
If possible, send source code via E-Mail before the meeting

Group Work

Groups of two or three students work together.

Presentation / Competition

Competition between the different groups:

- Restrictions of the model?
- Reduction of the state space?
- Which properties can still be verified?

Requirements/Exam

Requirements

- A good understanding of the model checking approach.
- No experience with Spin or Promela required.

Exam

1. Evaluation after the first three introductory tasks: further participation only if completed successfully.
2. A final oral presentation of the results of the case study at the end of the term.

Schedule

Preliminary Schedule and Deadlines

- until 28.10.2010: Mutual exclusion
  First steps in Spin and Promela.
- until 11.11.2010: Byzantine consensus
  Advanced modeling of a byzantine consensus protocol.
- until 25.11.2010: E-commerce protocol
  Views based verification of a GSM E-commerce protocol.
- until 13.01.2011: Case Study
  Routing in Mobile Ad-Hoc networks.

Important

Start modeling the next model only if the last one is finished successfully.

Literature

About Spin and Promela

- http://spinroot.com/: freely download of SPIN, SPIN tutorial, Promela language reference.
- Gerard J. Holzmann The Spin Model Checker *Addison-Wesley, ISBN 0-321-22862-6. 2003.*

First Protocol Documentation

B. K. Szymanski. A simple solution to lamports concurrent programming problem with linear wait. *In Proceedings of the 2nd international conference on Supercomputing, p. 621-626, NY, USA, 1988.*