Verifying a Bounded Retransmission Protocol using VIS

Robert Meolic, Tatjana Kapus, Zmago Brezočnik
Faculty of Electrical Engineering and Computer Science
University of Maribor
Smetanova 17, SI-2000 Maribor, Slovenia
{meolic,kapus,brezocnik}@uni-mb.si

Contents:
1. Introduction
2. The Bounded Retransmission Protocol
3. Verification with model checking
4. Conclusion

Work supported by Ministry of Science and Technology,
Republic of Slovenia
Introduction

- **Communication protocol** is a basic control procedure to ensure efficient, correct, and smooth transfer of data between the systems.

- **Communication service** is the external behaviour that the protocol should have while interacting with a producer and a consumer.

- **Verifying** a communication protocol is the process of checking whether the protocol conforms to the service.

The protocol and the service have to be formally described.

- Here is the receiver of popular **alternating bit protocol**:

[Diagram of the alternating bit protocol]
The Bounded Retransmission Protocol

- **The BRP** delivers large data packets from a sender to a receiver through a lossy channel. The data packets consist of one or more chunks.

  ![Diagram of BRP](image)

- The rules for the **sender**:
  1. The acknowledgement does not arrive in time ⇒ send the same chunk again
  2. Too many unsuccessful attempts ⇒ abort sending of the data packet.

- The rule for the **receiver**:
  1. A new chunk is not received for a long time ⇒ abort receiving of the current data packet.

- Both the producer and the consumer have to get an indication whether the packet has been delivered successfully or not.

- Here is a schematic view of the whole BRP specification:
Verification with model checking

- Model checking is fully automatic verification method. It can be easily and efficiently implemented with BDDs.
- The properties are formally stated in some dialect of modal logic (we used CTL — Computation Tree Logic).
- CTL formulas are built from atomic propositions \((p)\), standard boolean operators \((!, *, +, \rightarrow)\), and temporal operators. Each temporal operator consists of a path quantifier \((A,E)\) and a temporal modality \((F,G,X,U)\).

\[
\begin{align*}
&\text{EG } p \\
&\text{AF } p
\end{align*}
\]

- Some examples of CTL formulas:
  - \(\text{AG } p\) — \(p\) is always valid
  - \(\text{!EF } p\) — \(p\) is never valid
  - \(\text{AG AF } p\) — \(p\) is valid infinitely often

- CTL formulas for BRP:
  - \(\text{AG}(Sout \rightarrow !EX E(!StartDelivering U Sout))\)
    After receiving an indication, producer cannot get another indication before the start of new delivery.
  - \(\text{AG}( ((Sout = I_{\text{NOK}}) \ast !FirstChunk) \rightarrow A(!Rout U (Rout = I_{\text{NOK}})) )\)
    If producer gets \(I_{\text{NOK}}\) when trying to deliver a non-first chunk, then consumer will get \(I_{\text{NOK}}\).
Conclusion

- We have successfully verified the BRP with a powerful, BDD-based, public domain verification tool VIS.
- We modeled the BRP with a hardware description language Verilog. Verilog is similar to familiar programming languages (IEEE standard since 1995). The whole Verilog description of the BRP is about 400 lines long including some comments.
- 12 CTL formulas were verified in 2 minutes on a HP 715/100 Workstation with 128 MB of RAM.

- **Advantages** of VIS and Verilog:
  - VIS is a reliable and capable model checker.
  - VIS has ability to produce counterexamples.
  - VIS can perform simulation of the model.
  - Verilog allows hierarchical description, nondeterminism, and realistic notion of time.

- **Drawbacks:**
  - Verilog does not support asynchronous communication between modules.

- **Further work:**
  - We intend to verify more complex protocols using VIS.
  - We are testing our model checker which also seems to be very efficient. Unfortunately, we do not have parser for Verilog yet, therefore we can not compare it to VIS.