Formal Verification and Implementation of a Distributed Diagnosis Protocol

Áron Sisak VI. Inf., aron@inf.bme.hu

Advisor: Péter Bokor, petbokor@mit.bme.hu
Department of Measurement and Information Systems

Distributed systems can be found almost everywhere nowadays. To assure their fault tolerance it is essential to use proper diagnostic protocols, i.e., to identify faulty units. *Distributed diagnostic* algorithms allow diagnosis without deploying a dedicated diagnostic unit (which inherently decreases fault tolerance as being a single-point-of-failure), however, they provide a challenge due to their complexity, in particular in creating a consistent view among fault-free nodes. The report presents the formal verification as well as an implementation of a distributed diagnostic protocol that has been recently developed in the DECOS project.

Formal verification proves based on a rigorous mathematical model that the system satisfies certain properties. In case of diagnosis, such a property would require that the diagnosis is sound, i.e. that all accused units are indeed faulty. Among various formal verification approaches we concentrate on *model checking*, mostly due to its automated nature. In our work, we use the SAL model checking framework.

Model checking suffers from state-space-explosion, i.e. it cannot handle models of exponential size. *Fault-tolerant* (distributed) protocols usually yield big state spaces, even if the number of the possible execution patterns is constrained by the fault model. Even small-sized systems (4-5 nodes) may lead to models of infeasible size. We utilize a novel *abstraction* technique to handle state space explosion, which exploits the inherent symmetry of distributed protocols to simplify the model.

The algorithm assumes a *hybrid fault model*, which defines different fault classes, so it can provide an enhanced fault-tolerance compared to fault models assuming only worst-case fault scenarios. The description of the diagnostic protocol does not contain precise information regarding the fault coverage of the algorithm; therefore based on results obtained from the model checker, we also derive the fault tolerance of the algorithm, i.e. the relation between the number of tolerated faults and nodes.

The DECOS diagnostic protocol has been developed considering the target platforms (regarding the fault model, communication between nodes, etc.). Such an architecture is the time-triggered cluster of TTTech, which implements the TTP communication protocol. We provide an *implementation* of the protocol on the TTTech cluster (at BME MIT), which we also utilize to test the results of the formal verification.

Literature:
1. Leonardo de Moura et al.: SAL 2, *volume 3114 of LNCS* (2004)
2. Serafini, M. et al.: On Exploiting Symmetry To Verify Distributed Protocols. *Fast abstract, The International Conference on Dependable Systems and Networks* (2006)
3. Kopetz H., Bauer G.: The Time-triggered Architecture. *Proceedings of the IEEE*, 91(1): 112–126, (2003)