Formal modeling and verification of distributed failure detectors

Muhammad Atif

The research theme during PhD is mainly to investigate the application of prominent formal verification techniques to failure-detection distributed algorithms where the system under consideration can be synchronous, asynchronous or partially synchronous. Performing formal analysis on distributed algorithms is still a challenge as the number of states grows exponentially with the number of concurrent/interactive system participants. We found that some papers claim to offer correct protocols while the details provided in these papers are insufficient to establish those claims and in some cases we could even disprove the claimed properties.

We formalize the specification of:

1. Accelerated heartbeat protocols
2. Consensus protocols in asynchronous distributed systems
3. Group membership protocols
4. Efficient algorithms to implement failure detectors in partially synchronous systems

We found that the accelerated heartbeat protocols proposed in [M.G. Gouda and T.M. McGuire, Accelerated Heartbeat Protocols, Proc. Of ICDCS'98], violated some natural and essential properties. We proved the results by giving counter examples and developed the techniques to address the time-triggered events in mCRL2 and investigated the correct time bounds for all the protocols.

Regarding consensus problem, we proved the correctness of the proposed algorithms where the failure detectors are unreliable (i.e., failure detectors may make mistakes). These algorithms are proposed in [T. Deepak Chandra and S. Toueg, Unreliable Failure Detectors for Reliable Distributed Systems, J. ACM, 1996].

For the group membership protocols proposed in [Y. Amir, D. Dolev, S. Kramer and D. Malki, Membership Algorithms for Multicast Communication Groups, Springer-Verlag, 1992], we found that the original specifications and the text explaining the protocols can be interpreted in different ways and even some natural interpretations contradict each other. Our formalization with respect to different interpretations showed the violation of claimed properties. So to resolve the ambiguities, we reconstructed the protocols and model-checked them.

For analyzing the algorithms proposed in [M. Larrea, S. Arevalo and A. Fernandez, Efficient Algorithms to Implement Unreliable Failure Detectors in Partially Synchronous Systems, Proc. of DISC'99], we applied symmetry reduction techniques. We found that every algorithm encounters a deadlock if there is a bounded (yet arbitrarily large) buffer in the communication channel between a pair of nodes. We propose fixes for deadlock avoidance and model check the proposed algorithm in UPPAAL, FDR2 and mCRL2. We also present a comparison of these three tools for model checking one of the given four protocols.