Safety Analyses with non-Markovian Stochastic Petri Nets – Extended Abstract

Felix Engelhard, Stefan Heller
DaimlerChrysler AG
REI / AA
{felix.engelhard, stefan.heller}@daimlerchrysler.com

Graham Horton
Universität Magdeburg
ISG
graham@sim-md.de

Within the last years, stochastic Petri nets have become more and more common for the modeling and analysis of different classes of systems ranging from performance analyses of communication systems over cost estimations in economical areas up to reliability and safety estimations for safety-critical systems. While in many cases the analysis of the models can be done with discrete event simulation, this is not the case when safety-critical issues are examined. The reason for this is, that simulation cannot guarantee that all states of the system are reached within the simulation run. As a safety-critical state is, if at all, hopefully only reached with a very small probability, very long simulation runs would be necessary to get at least a better confidence in the simulation results.

Therefore, in the case of safety-critical systems, an analytical solution is needed that takes into account the complete state space of the system under investigation. The challenges that emerge are twofold: First, the state space of realistic systems can be very large. Second, realistic models are usually non-Markovian, i.e., the distributions of the transitions are not only immediate or exponential, but typical reliability distributions as for example the Weibull distribution will occur. The aim of this paper is to present an analytical solution procedure for the handling of non-Markovian stochastic Petri nets.

When dealing with the analytical solution of stochastic Petri nets (SPNs), first of all the reduced reachability graph (RRG) has to be constructed that contains all reachable tangible markings of the system together with all possible transitions between those states. This RRG could be built directly from the SPN using a so-called on-the-fly elimination of vanishing markings. However, for the purpose of livelock detection, the full reachability graph has to be built up first explicitly. From this reachability graph the RRG is then build up by a post-elimination of all vanishing markings. To handle the state space explosion problem, a smart storage is needed to couple with realistic models. Within the last years, some symbolic storage structures as for example multi-valued decision diagrams (MDDs) or multi-terminal binary decision diagrams (MTBDDs) have been proposed for

the storage of such huge state spaces. However, these means are only useful and storage-efficient, if there is some structure in the system under investigation (e.g. independent subsystems). In realistic models, it is often the case that this special structure cannot be guaranteed. Therefore, we propose using a hard disk-based storage scheme for the RG and RRG to be able to cope with all possible models. A reduction algorithm has been developed for the transformation of the RG into the RRG that takes care of the disk-based storage and is able to deal with vanishing loops.

If the RRG has been constructed, the second step is the computation of state probabilities and derived measures as for example expected reward values. Many specialized solvers have been proposed within the last years to cope with such non-Markovian systems. However, the disadvantage of these solvers is, that up to now all of them impose strong limitations on the modeling capabilities. Therefore we propose a more universal approach - the use of phase type distributions. Phase type distributions, a superpositions of either geometric (in the discrete case [DPH]) or exponential (in the continous case [CPH]) phases, have been proven to be able to approximate any distribution arbitrarily well, at least theoretically. As experiments have shown that distributions that appear in reliability models can be more easily approximated using DPHs than CPHs, every distribution in the SPN is now approximated by a DPH. The RRG is now extended by incorporating the phase information, which means that a phase expanded RRG (PHRRG) has to be built up. Therefore, the state space explosion problem is increased. However, as the phase-expansion is performed in a very structured way, the symbolic storage techniques mentioned above can be used to store the PHRRG in a very compact form. When the PHRRG has been built up using DPHs, the only remaining step is to compute a transient or steady-state solution. Standard solution techniques as for example the Jacobi overrelaxation-method can be used for this purpose. The last step is finally to tranform the solution that has been computed for the PHRRG to a solution for the RRG by merging all PHRRG states that belong to the same RRG-marking. Therefore measures can be computed that are still connected with the underlying SPN and not only with the PHRRG which was only introduced to perform a Markovization. With the proposed analysis-procedure it is now possible to analytically solve non-Markovian SPNs that could not be analyzed by existing specialized analytical solvers because of their modeling complexity and that could no be analyzed by simulation because of their safety-criticality.

The complete analysis procedure that has been proposed here has been integrated into the tool Expect. Some example experiments will be given in the final paper.