Efficient Monitoring Techniques for Safety Critical Cyber-Physical Systems

Submitted by Aravinda Sistla on Sun, 10/07/2012 - 9:24pm. Contributor:
A. Prasad Sistla

Abstract

Correct functioning of cyber-physical systems is of critical importance. This is more so in the case of safety critical systems such as in medical or automotive applications. Since verification of correctness, in general, is infeasible and testing is not exhaustive, it is of critical importance to monitor such system during their operation and detect erroneous behaviors to be acted on.

The problem of designing monitors for safety critical cyber-physical systems is challenging since the correctness property to be monitored is specified on the evolution of system state over time which the monitor cannot directly observe; furthermore, the evolution of the system is probabilistic. The probabilities or randomness in the evolution of the system is due to uncertainties introduced by noise or due to other unpredictable events, such as component failures, modeled probabilistically. The inputs to the monitor are the outputs generated by the system. These may include some sensor outputs. By using these inputs the monitor needs to decide whether the system execution is correct or not.

The project has so far introduced two models for specifying the semantics of such cyber-physical sys- tems. The first model is the Hidden Markov System in which the states of the system are modeled as discrete states after quantization. For such systems the property to be monitored is specified by an automaton on in- finite strings. We defined two accuracy measures of a given monitor - acceptance and rejection accuracies. The accuracies capture percentage of false alarms and missed alarms, respectively. Using these concepts we defined two notions, called strong monitorability and monitorability. We gave exact characterizations when a system is strongly monitorable and monitorable with respect to a property. Based on these notions we developed techniques for monitoring, when the system to be monitored is specified by a probabilistic hybrid automaton and the property to be monitored is given by a deterministic hybrid automaton. We formulated a monitoring method that uses product automaton and estimates probabilities using particle filters. These monitoring techniques are implemented using Matlab and have been shown to be effective on examples.

We have also introduced Extended Hidden Markov Systems (EHMS) in which the state of the system is hybrid, i.e., has a continuous and discrete component. We extended the monitorability results to the EHMSes.

In order to implement monitors suggested by our theoretical analysis, a state estimation algorithm needs to be used. Even if in each discrete mode the cyber-physical system is linear, mode changes (discrete transitions) introduce nonlinearities. Furthermore, systems we consider have a large number of discrete modes, making traditional mode-estimation algorithms difficult to use. In our work we use particle filters to estimate the state of the system; the estimate is in turn used by the monitor. Due to a large number of discrete modes that the particle filter needs to detect, particle depletion represents a particular challenge. Traditionally, depletion calls for increasing number of particles to be used, increasing the computational cost of the particle filter. We use the invariances in the topology of the system stemming from asynchronous transitions to simplify the particle filter and thus dramatically reduce its computational time.

References

1. A. Sistla, M. ZVefran, and Y. Feng. Monitorability of stochastic dynamical systems. In *Computer Aided Verification*, pages 720-736. Springer, 2011
2. A. Sistla, M. ZVefran, and Y. Feng. Runtime monitoring of stochastic cyber-physical systems with hybrid state. In *Runtime Verification*, pages 276-293. Springer, 2012

Award ID: 1035914

Other available formats:

Efficient Monitoring Techniques for Safety Critical Cyber-Physical Systems

Automotive CPS Domains Hybrid Models Probabilistic and Statistical Verification Models of Computation Quantitative Verification Concurrency and Timing Testing Modeling Systems Engineering Critical Infrastructure Robotics Simulation Transportation Validation and Verification CPS Technologies Foundations National CPS PI Meeting 2012 2012 Poster Academia CPS PI MTG 12 Posters & Abstracts