2012 IEEE/ACM Third International Conference on Cyber-Physical Systems

Poster Abstract: Methods and Tools for Verification of Cyber-Physical Systems

Chris Myers Jian Wu, Zhen Zhang
University of Utah

Hao Zheng, Yingying Zhang
University of Utah University of South Florida

As chip technology scales, it is becoming possible to integrate multiple cores on a single chip which communicate using a *network-on-chip* (NoC) paradigm. One CPS application area that can leverage this is in automotive electronic systems which often require more than 50 *electronic control units* (ECUs) to operate everything from the entertainment system to the anti-lock breaks. Currently, each ECU is statically tied to specific sensors and actuators which means that processing power of each ECU cannot be shared, and when an ECU fails, it causes a malfunction in the corresponding sensor/actuator. With an NoC approach, it makes the mapping between ECUs and sensors/actuators flexible allowing for a sharing of processing power and enabling fault tolerance by having spare units.

However, an NoC must be carefully designed to avoid deadlock and be fault-tolerant while meeting latency and throughput goals. The key component of an NoC is the protocol that it employs to route packets between the processing elements. One approach, proposed by Glass/Ni, guarantees absence of deadlock while always being able to route around a single router that has failed. The idea is that particular "turns" in the routing grid are disallowed, and the routes are carefully chosen to ensure there is always an alternative path. This protocol, however, can deadlock in the situation where there is a single link failure. Yoneda et al. proposed a modified version of the protocol which introduces a mechanism to forward fault information, but this method still cannot consider link failures on the edges of the grid. We propose a new routing algorithm that is deadlock-free and guaranteed to route around any single link failure without extra hardware to forward the fault information.

CPS systems such as this NoC router design are complex, and the concurrent, timing, and stochastic behavior must be thoroughly verified. To address this challenge, we are developing a comprehensive methodology around a unified modeling formalism that supports all these aspects. The concurrent and timing behavior of this model are verified using improved versions of traditional model checking methods. The stochastic behavior is being verified using both statistical and stochastic model checking. More details are given below.

The verification of the NoC router design must be done at both the protocol and circuit levels. At the protocol level, one verification goal is to prove that it is deadlock-free. Since it is highly concurrent, it has a very large state space. One approach that we are exploring to deal with this state explosion is *partial order reduction* (POR) which avoids irrelevant concurrent interleavings. In particular, a new approach has been developed to compute more accurate and refined information that dramatically improves the POR's efficiency. For some examples, a 99 percent reduction in memory usage can be achieved. The second approach being considered is compositional minimization. This approach starts with system components and gradually constructs their state spaces, minimizes them, and then compose them together. At the end, a significantly reduced state space for the entire system can be constructed for verification. At the circuit level, it is necessary to verify that the circuit implementation works under all timing assumptions. The need to represent the timing in the states adds to the verification complexity. To address this issue, our timing analysis algorithm employs a compact symbolic state representation which has had promising results. To further improve the scalability of the verification tool to larger designs, we are currently investigating combinations of all of these approaches.

In order to determine the robustness of our NoC design, we are developing both statistical and stochastic model checking approaches. Statistical model checking employs stochastic simulation. In particular, we model the links in our router as having a probability of having a fault, and our method attempts to find the probability that a packet is unable to be routed to its destination. The challenge is that the probability of a link fault is extremely low, so an excessive number of simulations is required to determine our packet loss rate. To overcome this challenge, we are exploring *importance sampling* techniques to reduce the number of required runs. In stochastic model checking, Markov chain analysis is employed to determine the packet loss rate directly. The challenge with this method is to deal with the state explosion problem. To address this challenge, we plan to leverage the state space reduction techniques described earlier. The final challenge that we are trying to address is the determination of errors in a stochastic system such as our router. In conventional model checking, a single error trace can be reported while in stochastic model checking a set of traces must be reported that together exceed the acceptable probability of failure. Constructing such counterexample traces and presenting them to the user in a useful way to debug their design is an interesting area of future research.

978-0-7695-4695-7/12 $26.00 © 2012 IEEE
DOI 10.1109/ICCPS.2012.50