Eddy: a Parallel Framework for Model Checking?

Geof Sawaya (Robert Palmer, Robert M. Kirby, Ganesh Gopalakrishnan)
School of Computing, University of Utah

As society is increasingly dependent upon computer provided services for our well-being, including a full spectrum from aircraft navigation and air defense monitors to financial transactions, model checking is a tool for verifying the correctness of system behaviors and has traditionally been limited to verifying behaviors of small designs and mission-critical applications. The main limiting factors to model checking are time and available memory resources. We devised the Eddy framework to enable system designers to verify larger and more interesting behaviors by taking advantage of modern hardware architectures that use multiple concurrent machines, thereby making available more computation resources for verification tasks. We leverage modern computer architecture on two fronts: using multiple threads of execution on a single machine and multiple machines in a distributed computing environment. Each machine has a model checker thread and a thread that handles the communication between machines. The total memory available to Eddy is the sum of the memory of the machines in the distributed computing environment. We have used the Eddy framework successfully with the model checker Mur.

1. By utilizing Eddy we observe a linear increase in model checker speed and a manageable amount of memory overhead as we increase the number of machines in the distributed computing environment. The Eddy framework enabled us to perform verification of models that would otherwise be impossible on traditional architecture due to memory and time constraints.

Supported in part by NSF award CNS-0509379 and SPC Contract 2005-TJ-1318 and a grant from the Microsoft Corporation.

1 Eddy-Mur is being presented this year at SPIN ’06.