
Sampath Kannan

University of Pennsylvania
School of Engineering & Applied Science
Department of Computer & Information Science
200 S. 33rd St, Moore Building (GRW), Room 556
Philadelphia, PA 19104

U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

Approved for public release; distribution unlimited.

We have been developing formal methods for monitoring safety-critical real-time and reactive systems. In this project we are building on our expertise in the area of process-algebra-based specification and analysis of real-time systems as well as the paradigm of program checking which allows one to make rigorous statements about the correctness of program behavior rather than of the program itself.

To integrate these ideas we have implemented a prototype system (JavaMAC) for monitoring and checking Java programs. MAC takes a monitoring script provided by the user, the program, and a requirement specification and produces a) an instrumentation of the program to send variable update information to the monitoring and checking unit b) a script for transforming low level program variables to abstract events and c) a script for checking whether a sequence of events is consistent with the desired property. These scripts written in new languages we define (PEDL and MEDL respectively) are then used to produce other components that extract low-level information from the program, convert it to events and check that the sequence of events represents correct behavior. We have successfully tested our prototype on two applications --- micro air vehicles attaining a desired formation, and convergence of a network routing protocol.

We have done performance measurements on JavaMAC in an attempt to breakdown the overhead introduced by JavaMAC into its various components. Subsequently we have introduced several optimizations in JavaMAC to improve the performance.

Other research funded by this grant includes papers on probabilistic bisimulation and on low-overhead checking of the correctness of the output produced by programs for sorting and other "mathematically well-defined" tasks.

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UL

4

298-102
Journals:

Conferences:


Listing of all publications

-------------------------------


-------------------------------
Participating personnel:
Mahesh Viswanathan and Moonjoo Kim and Hee-Hwan Hwak were students who obtained their Ph.D.'s supported by this grant.
Oleg Sokolsky was a post-doctoral fellow supported by this grant. He has since taken up a position as Research Assistant Professor at the University of Pennsylvania.
Prof. Insup Lee and Prof. Sampath Kannan were supported by this grant.

Scientific Progress and Accomplishments
We have been developing formal methods for monitoring safety-critical real-time and reactive systems. In this project we are building on our expertise in the area of process-algebra-based specification and analysis of real-time systems as well as the paradigm of program checking which allows one to make rigorous statements about the correctness of program behavior rather than of the program itself.

To integrate these ideas we have implemented a prototype system (JavaMAC) for monitoring and checking Java programs. MAC takes a monitoring script provided by the user, the program, and a requirement specification and produces a) an instrumentation of the program to send variable update information to the monitoring and checking unit b) a script for transforming low level program variable values to abstract events and c) a script for checking whether a sequence of events is consistent with the desired property. These scripts written in new languages we define (PEDL and MEDL respectively) are then used to produce other components that extract low-level information from the program, convert it to events and check that the sequence of events represents correct behavior. We have successfully tested our prototype on two applications --- micro air vehicles attaining a desired formation, and convergence of a network routing protocol.

We have done performance measurements on JavaMAC in an attempt to breakdown the overhead introduced by JavaMAC into its various components. Subsequently we have introduced several optimizations in JavaMAC to improve the performance.

Other research funded by this grant includes papers on probabilistic bisimulation and on low-overhead checking of the correctness of the output produced by programs for sorting and other "mathematically well-defined" tasks.