REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE : 12/14/01	3. REPORT TYPE AND DATES COVERED Final Report ~~October 1998 – October 2001~~ 06Jul98-05Jul01

4. TITLE AND SUBTITLE
Checkers, Self-Testers, and Self-Correctors for Reactive Systems.

5. FUNDING NUMBERS
DAAG55-98-1-0393

6. AUTHOR(S)
Sampath Kannan

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
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

8. PERFORMING ORGANIZATION REPORT NUMBER
P – 35684MA

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U. S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
35683.1-CI

11. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12 a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12 b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

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.

14. SUBJECT TERMS

15. NUMBER OF PAGES
4

16. PRICE CODE

17. SECURITY CLASSIFICATION OR REPORT	18. SECURITY CLASSIFICATION ON THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

REPORT DOCUMENTATION PAGE (SF298)
(Continuation Sheet)

Journals:

O. Sokolsky, I. Lee, and H. Ben-Abdallah, Specification and Analysis of Real-Time Systems with PARAGON, Annals of Software Engineering, Vol. 7, 1999.

Conferences:

Y. Gertner, S. Kannan, T. Malkin, O. Reingold and M. Viswanathan, The Relationship Between Public-Key Encryption and Oblivious Transfer, FOCS Nov. 2000.

A. Philippou, I. Lee, and O. Sokolsky, Weak Bisimulation for Probabilistic Systems, Proceedings of CONCUR '00, August 2000.

K. Bhargavan, C.A. Gunter, M. Kim, I. Lee, D. Obradovic, O. Sokolsky, and M. Viswanathan, Formal Analysis of Network Simulations, Proceedings of the International Symposium on Software Testing and Analysis, August 2000.

L. Goldberg, M. Jerrum, S. Kannan, and M. Paterson, A Bound on the Capacity of Backoff and Ackknowledgement-Based Protocols, to appear Proc. ICALP '00.

R. Alur, J. Exposito, M. Kim, V. Kumar and I. Lee, Formal modeling and analysis of hybrid systems: A case study in multi-robot coordination, Proceedings of FM '99, September 1999.

J. Feigenbaum, S. Kannan, M. Strauss, and M. Viswanathan, An Approximate L^1 - Difference Algorithm for Massive Data Streams, Proc. Symp. On Foundations of Computer Science, New York, Oct. 1999, 501-511

R. Alur, S. Kannan, and S. La Torre, Polyhedral Flows in Hybrid Automata, Proc. Hybrid Systems: Computation and Control, 1999.

R. Alur, S. Kannan, and M. Yannakakis, Communicating Hierararchical State Machines, International Conference on Automata Languages and Programming, Prague 1999.

Insup Lee, S. Kannan, M. Kim, O. Sokolsky, M. Viswanathan, Runtime Assurance based on Formal Specifications, Proceedings of International Conference on Parallel and Distributed Processing Techniques and Applications, June 28-July1, 1999.

M. Kim, M. Viswathan, I. Lee, H.Ben-Abdellah, S. Kannan, and O. Sokolsky, Formally Specified Monitoring of Temporal Properties, Proceedings of the European Conference on Real-Time Systems, York, UK, June 9-11, 1999.

H.H. Kwak, I. Lee, A. Philipou, J. Y Chou and O. Sokolsky, Symbolic Schedulability Analysis of Real-time Systems, Proceedings of IEEE Real-Time Systems Symposium, December 1998.

Listing of all publications

I. Lee, S. Kannan, M. Kim, O. Sokolsky, and M. Viswanathan, "Runtime Assurance Based On Formal Specifications," International Conference on Parallel and Distributed Processing Techniques and Applications, June 28 - July 1, 1999.

M. Kim, M. Viswanathan, H. Ben-Abdallah, S. Kannan, I. Lee, and O. Sokolsky, "Formally Specified Monitoring of Temporal Properties", European Conference on Real-Time Systems, June 1999.

H. Ben-Abdallah, I. Lee, and O. Sokolsky, "Specification and Analysis of Real-Time Systems with PARAGON", Annals of Software Engineering, vol. 7 (1999), pp. 211-234.

O. Sokolsky, S. Kannan, M. Kim, I. Lee, and M. Viswanathan, "Steering of Real-Time Systems based on Monitoring and Checking," Workshop on Real-time Object-Oriented Dependable Systems, October 1999.

J.E. Hilger, I. Lee, and O. Sokolsky, "Comparative Analysis of Design Alternatives in Embedded Systems," IEEE Workshop on Real-Time Mission-Critical Systems, December 1999.

K. Bhargavan, C.A. Gunter, M. Kim, I. Lee, D. Obradovic, O. Sokolsky, and M. Viswanathan, "Formal Analysis of Network Simulations," xbInternational Symposium on Software Testing and Analysis, August 2000.

A. Philippou, I. Lee, and O. Sokolsky, "Weak Bisimulation for Probabilistic Systems," CONCUR'00, August 2000.

I. Lee, J.-Y. Choi, H.H. Kwak, A. Philippou, and O.Sokolsky, "A Family of Resource-Bound Real-time Process Algebras," International Conference on Formal Techniques for Networked and Distributed Systems, August 2001.

R. Alur, R. Grosu, I. Lee, and O. Sokolsky, "Compositional Refinement for Hierarchical Hybrid Systems," International Workshop on Hybrid Systems: Computation and Control, LNCS 2034, pp. 33-48. March 2001.

I. Lee, A. Philippou, and O. Sokolsky, "Formal Modeling and Analysis of Power-Aware Real-Time Systems," Workshop on Real-Time Embedded Systems, December 2001.

J. Feigenbaum, S. Kannan, M. Strauss, and M. Viswanathan, "An Approximate L1-Difference Algorithm for Massive Data Streams", to appear in SIAM J. Comput. (A preliminary version appeared in IEEE Symp. on Foundations of Computer Science (FOCS), 1999.

J. Feigenbaum, S. Kannan, M. Strauss, and M. Viswanathan, "Testing and spot-checking of data streams", to appear in Algorithmica. (A preliminary version appeared in ACM-SIAM Symp. On Disc. Algorithms (SODA) '00).

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.