

Lecture Notes in Computer Science  
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

2529

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Barcelona*

*Hong Kong*

*London*

*Milan*

*Paris*

*Tokyo*

Doron A. Peled Moshe Y. Vardi (Eds.)

# Formal Techniques for Networked and Distributed Systems – FORTE 2002

22nd IFIP WG 6.1 International Conference  
Houston, Texas, USA, November 11-14, 2002  
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany  
Juris Hartmanis, Cornell University, NY, USA  
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Doron A. Peled  
University of Warwick, Department of Computer Science  
Coventry, CV4 7AL, United Kingdom  
E-mail: [doron@dcs.warwick.ac.uk](mailto:doron@dcs.warwick.ac.uk)

Moshe Y. Vardi  
Rice University, Department of Computer Science  
6100 S. Main St., Houston, TX 77005, USA  
E-mail: [vardi@cs.rice.edu](mailto:vardi@cs.rice.edu)

Cataloging-in-Publication Data applied for

Bibliographic information published by Die Deutsche Bibliothek

Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliographie;  
detailed bibliographic data is available in the Internet at <http://dnd.ddb.de>.

CR Subject Classification (1998): C.2.4, D.2.2, C.2, D.2.4, D.2.5, D.2, F.3.1, D.4

ISSN 0302-9743

ISBN 3-540-00141-7 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York  
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

©2002 IFIP International Federation for Information Processing, Hofstrasse 3, A-2361 Laxenburg, Austria  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna e.K.  
Printed on acid-free paper SPIN: 10873162 06/3142 5 4 3 2 1 0

## Preface

The IFIP TC6 WG 6.1 Joint International Conference on Formal Techniques for Networked and Distributed Systems, FORTE 2002, was held this year at Rice University, Houston, Texas, on November 11–14. This annual conference provides a forum for researchers and practitioners from universities and industry to meet and advance technologies in areas of specification, testing, and verification of distributed systems and communication protocols. The main topics are:

- FDT-based system and protocol engineering.
- Semantical foundations.
- Extensions of FDTs.
- Formal approaches to concurrent/distributed object-oriented systems.
- Real-time and probability aspects.
- Performance modeling and analysis.
- Quality of service modeling and analysis.
- Verification and validation.
- Relations between informal and formal specification.
- FDT-based protocol implementation.
- Software tools and support environments.
- FDT application to distributed systems.
- Protocol testing, including conformance testing, interoperability testing, and performance testing.
- Test generation, selection, and coverage.
- Practical experience and case studies.
- Corporate strategic and financial consequences of using formal methods.

A total of 61 papers were submitted to FORTE 2002, and reviewed by members of the program committee and additional reviewers. The program committee selected 22 regular papers, two tool papers, and two posters for presentation at the conference. The program also included three tutorials and five invited talks.

FORTE 2002 would like to gratefully acknowledge the financial support received from HP, OFFIS, Microsoft Research, and Verisity. FORTE 2002 could not take place without the effort of the PC members, reviewers, and people participating in the local organization. The editors wish to thank all of them.

Doron A. Peled  
Moshe Y. Vardi

# Organization

FORTE 2002 was organized by the Department of Computer Science, Rice University, Houston, Texas.

## Executive Committee

**Program Chairs:** Doron A. Peled (University of Warwick, UK) and Moshe Y. Vardi (Rice University)

## Program Committee:

R. Alur	Univ. Pennsylvania, USA
D. Bjorner	Tech. Univ. Denmark
G. v. Bochmann	Univ. of Ottawa, Canada
T. Bolognesi	IEI, Italy
E. Brinksma	Univ. of Twente, The Netherlands
A. Cavalli	INT, France
S.T. Chanson	Hong Kong Univ.
P. Dembinski	IPI-PAN
H. Garavel	Inria, France
S. Gnesi	CNR-IEI, Italy
G.J. Holzmann	Bell Labs, USA
A. Hu	UBC Canada
C. Jard	IRISA-CNRS, France
G. Leduc	Univ. of Liege, Belgium
D. Lee	Bell Labs, China
I. Lee	Univ. Pennsylvania, USA
S. Leue	Univ. of Freiburg, Germany
L. Logrippo	Univ. of Ottawa, Canada
S. Mauw	Eindhoven, The Netherlands
K. McMillan	Cadence
M. Morley	Verisity
A. Muscholl	Univ. Paris 7, France
E. Najm	ENST, France
D. Peled	Univ. of Warwick, UK
A. Petrenko	CRIM, Canada
S. Smolka	Stony Brook, USA
R. Tenney	Univ. of Massachusetts, USA
K.J. Turner	Univ. of Stirling, UK
S.T. Vuong	Univ. of British Columbia, Canada
M.Y. Vardi	Rice University, USA
M. Yannakakis	Avaya Labs

VIII Organization

**Steering Committee:**

G. v. Bochmann	Univ. of Ottawa
E. Brinksma	Univ. of Twente
S. Budkowski	INT, France
G. Leduc	Univ. of Liege
E. Najm	ENST, France
R. Tenney	Univ. of Massachusetts
K.J. Turner	Univ. of Stirling

## Table of Contents

Encoding PAMR into (Timed) EFSMs . . . . .	1
<i>Manuel Núñez, Ismael Rodríguez</i>	
Submodule Construction for Specifications with Input Assumptions and Output Guarantees . . . . .	17
<i>Gregor v. Bochmann</i>	
Congruent Weak Conformance, a Partial Order among Processes . . . . .	34
<i>Ronald W. Brower, Kenneth S. Stevens</i>	
Symmetric Symbolic Safety-Analysis of Concurrent Software with Pointer Data Structures . . . . .	50
<i>Farn Wang, Karsten Schmidt</i>	
A Nested Depth First Search Algorithm for Model Checking with Symmetry Reduction . . . . .	65
<i>Dragan Bošnački</i>	
Protocol Techniques for Testing Radiotherapy Accelerators . . . . .	81
<i>Kenneth J. Turner, Qian Bing</i>	
System Test Synthesis from UML Models of Distributed Software . . . . .	97
<i>Simon Pickin, Claude Jard, Yves Le Traon, Thierry Jéron, Jean-Marc Jézéquel, Alain Le Guennec</i>	
Formal Test Purposes and the Validity of Test Cases . . . . .	114
<i>Peter H. Deussen, Stephan Tobies</i>	
Use of Logic to Describe Enhanced Communications Services . . . . .	130
<i>Stephan Reiff-Marganiec, Kenneth J. Turner</i>	
A Formal Venture into Reliable Multicast Territory . . . . .	146
<i>Carolos Livadas, Nancy A. Lynch</i>	
Modelling SIP Services Using CRESS . . . . .	162
<i>Kenneth J. Turner</i>	
Verifying Reliable Data Transmission over UMTS Radio Interface with High Level Petri Nets . . . . .	178
<i>Teemu Tynjälä, Sari Leppänen, Vesa Luukkala</i>	
Verifying Randomized Byzantine Agreement . . . . .	194
<i>Marta Kwiatkowska, Gethin Norman</i>	



Automatic SAT-Compilation of Protocol Insecurity Problems via Reduction to Planning .....	210
<i>Alessandro Armando, Luca Compagna</i>	
Visual Specifications for Modular Reasoning about Asynchronous Systems .....	226
<i>Nina Amla, E. Allen Emerson, Kedar S. Namjoshi, Richard J. Trefler</i>	
Bounded Model Checking for Timed Systems .....	243
<i>G. Audemard, A. Cimatti, A. Kornilowicz, R. Sebastiani</i>	
C Wolf – A Toolset for Extracting Models from C Programs .....	260
<i>Daniel C. DuVarney, S. Purushothaman Iyer</i>	
NTIF: A General Symbolic Model for Communicating Sequential Processes with Data .....	276
<i>Hubert Garavel, Frédéric Lang</i>	
Building Tools for LOTOS Symbolic Semantics in Maude .....	292
<i>Alberto Verdejo</i>	
From States to Transitions: Improving Translation of LTL Formulae to Büchi Automata .....	308
<i>Dimitra Giannakopoulou, Flavio Lerda</i>	
A Compositional Sweep-Line State Space Exploration Method .....	327
<i>Lars Michael Kristensen, Thomas Mailund</i>	
On Combining the Persistent Sets Method with the Covering Steps Graph Method .....	344
<i>Pierre-Olivier Ribet, François Vernadat, Bernard Berthomieu</i>	
Innovative Verification Techniques Used in the Implementation of a Third-Generation 1.1GHz 64b Microprocessor .....	360
<i>Victor Melamed, Harry Stuïmer, David Wilkins, Lawrence Chang, Kevin Normoyle, Sutikshan Bhutani</i>	
Mechanical Translation of I/O Automaton Specifications into First-Order Logic .....	364
<i>Andrej Bogdanov, Stephen J. Garland, Nancy A. Lynch</i>	
Verification of Event-Based Synchronization of SpecC Description Using Difference Decision Diagrams .....	369
<i>Thanyapat Sakunkonchak, Masahiro Fujita</i>	

A Distributed Partial Order Reduction Algorithm ..... 370  
*Robert Palmer, Ganesh Gopalakrishnan*

**Author Index** ..... 371