

Lecture Notes in Computer Science

2767

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer

Berlin

Heidelberg

New York

Hong Kong

London

Milan

Paris

Tokyo

Hartmut König Monika Heiner
Adam Wolisz (Eds.)

Formal Techniques for Networked and Distributed Systems – FORTE 2003

23rd IFIP WG 6.1 International Conference
Berlin, Germany, September 29 – October 2, 2003
Proceedings



Springer

Series Editors

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

Volume Editors

Hartmut König
Monika Heiner
Brandenburg University of Technology at Cottbus
Faculty of Mathematics, Natural Sciences and Computer Science
P. O. Box 10 13 44, 03013 Cottbus, Germany
E-mail: {koenig/mh}@informatik.tu-cottbus.de

Adam Wolisz
Technical University Berlin
TKN - Telecommunication Networks Group
Einsteinufer 25, 10587 Berlin, Germany
E-mail: wolisz@ee.tu-berlin.de

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

CR Subject Classification (1998): C.2.4, D.2.2, C.2, D.2.4-5, D.2, F.3, D.4

ISSN 0302-9743

ISBN 3-540-20175-0 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>

©2003 IFIP International Federation for Information Processing, Hofstrasse 3, 2361 Laxenburg, Austria
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Steingraber Satztechnik
Printed on acid-free paper SPIN 10930977 06/3142 5 4 3 2 1 0

Preface

This volume contains the proceedings of FORTE 2003, the 23rd IFIP TC 6/WG 6.1 International Conference on Formal Techniques for Networked and Distributed Systems, held in Berlin, Germany, September 29–October 2, 2003. FORTE denotes a series of international working conferences on formal description techniques (FDTs) applied to computer networks and distributed systems. The conference series started in 1981 under the name PSTV. In 1988 a second series under the name FORTE was set up. Both series were united to FORTE/PSTV in 1996. Two years ago the conference name was changed to its current form. The last five meetings of this long conference series were held in Paris, France (1998), Beijing, China (1999), Pisa, Italy (2000), Cheju Island, Korea (2001), and Houston, USA (2002).

The 23rd FORTE conference was especially dedicated to the application of formal description techniques to practice, especially in the Internet and communication domain. The scope of the papers presented at FORTE 2003 covered the application of formal techniques, timed automata, FDT-based design, verification and testing of communication systems and distributed systems, and the verification of security protocols. In addition, work-in-progress papers were presented which have been published in a separate volume.

The FORTE 2003 program consisted of 9 sessions, 2 work-in-progress sessions, and a working session on the practicability of formal description techniques. Three invited talks and a keynote speech gave an overview on actual results and experience in the application of formal description techniques in the Internet and communication domain. The conference was preceded by 3 half-day tutorials. The proceedings contain the 24 regular papers accepted and presented at the conference. They were selected from 55 submitted papers in a careful selection procedure based on the assessment of three referees for each paper. The proceedings also include the text of the invited talks of Manfred Broy, Jonathan Billington, and Jean-Pierre Courtiat.

FORTE 2003 was organized under the auspices of IFIP TC 6 by BTU Cottbus, the Brandenburg University of Technology Cottbus, and by TU Berlin, the Technical University of Berlin. It was supported by a number of partners including Microsoft, Telelogic, Bosch AG, the Deutsche Forschungsgemeinschaft (DFG), and the Berlin Marketing und Tourismus GmbH.

We would like to express our gratitude to the numerous people who contributed to the success of FORTE 2003. The reviewing process was one of the major efforts during the preparation of the conference. It was completed by experts from around the world. The reviewers are listed in these proceedings. Finally, we would like to thank the local organizers for the excellent running of the conference, especially Katrin Willhöft, Christian Noack, Sarina Gwiszcz, Joachim Paschke, Irene Ostertag, and Ronny Richter.

Our special thanks goes to Katrin Willhöft, Christian Noack, and Mario Zühlke from the BTU Cottbus for their hard work in organizing and preparing these proceedings.

September 2003

Hartmut König
Monika Heiner
Adam Wolisz

Organization

Conference Chairs

Hartmut König, *Brandenburg University of Technology Cottbus, Germany*
Monika Heiner, *Brandenburg University of Technology Cottbus, Germany*
Adam Wolisz, *Technical University of Berlin, Germany*

Steering Committee

Gregor v. Bochmann, *University of Ottawa, Canada*
Ed Brinksma, *Univ. of Twente, The Netherlands*
Stan Budkowski, *INT Evry, France*
Guy Leduc, *University of Liege, Belgium*
Elie Najm, *ENST, France*
Richard Tenney, *University of Massachusetts, USA*
Kenneth Turner, *University of Stirling, UK*

Technical Program Committee

T. Bolognesi, *IEI Pisa, Italy*
E. Borcoci, *University of Bucarest, Romania*
H. Bowman, *University of Kent, UK*
A. Cavalli, *INT Evry, France*
P. Dembinski, *IPI Warsaw, Poland*
R. Gotzhein, *Univ. of Kaiserslautern, Germany*
R. Groz, *INPG Grenoble, France*
U. Herzog, *Univ. of Erlangen, Germany*
T. Higashino, *Osaka University, Japan*
D. Hogrefe, *University of Göttingen, Germany*
G. J. Holzmann, *Bell Labs, USA*
C. Jard, *IRISA, France*
F. Khendek, *Concordia University Montreal, Canada*
M. Kim, *ICU Taejon, Korea*
P. Kritzinger, *University of Cape Town, South Africa*
H. Krumm, *University of Dortmund, Germany*
D. Lee, *Bell Labs, China*
M. Luukkainen, *University of Helsinki, Finland*
B. Müller-Clostermann, *University of Essen, Germany*
M. Nunez, *University of Madrid, Spain*

D. A. Peled, *University of Warwick, UK*
A. Petrenko, *CRIM Montreal, Canada*
K. Suzuki, *Advanced Comm. Coop., Japan*
Ü. Uyar, *City University of New York, USA*
J. Wu, *Tsinghua University, Beijing, China*
M. Y. Vardi, *Rice University Houston, USA*
N. Yevtushenko, *Tomsk State University, Russia*

Additional Reviewers

G. Bao, *Bell Labs Research, China*
M. ter Beek, *IEI Pisa, Italy*
S. Boroday, *CRIM, Canada*
J. Brandt, *University of Kaiserslautern, Germany*
J. Bredererke, *University of Bremen, Germany*
C. Chi, *Bell Labs Research, China*
A. Duale, *IBM, USA*
M. Ebner, *University of Göttingen, Germany*
M. Fecko, *Telcordia, USA*
D. de Frutos, *Universidad Complutense de Madrid, Spain*
X. Fu, *University of Göttingen, Germany*
R. Gotzhein, *University of Kaiserslautern, Germany*
R. Grammes, *University of Kaiserslautern, Germany*
H. Hallal, *CRIM, Canada*
R. Hao, *Bell Labs Research, China*
T. Hasegawa, *KDDI R&D Laboratories Inc., Japan*
J. Huo, *CRIM, Canada*
A. Idoue, *KDDI R&D Laboratories Inc., Japan*
Y. Ishihara, *Osaka University, Japan*
S. Kang, *Information and Communications University, Korea*
T. Karvi, *University of Helsinki, Finland*
K. Li, *Bell Labs Research, China*
L. Llana, *Universidad Complutense de Madrid, Spain*
N. López, *Universidad Complutense de Madrid, Spain*
S. Maag, *INT, France*
S. Maharaj, *University of Stirling, United Kingdom*
T. Massart, *Free University of Brussels (ULB), Belgium*
A. Mederreg, *INT, France*
A. Nakata, *Osaka University, Japan*
T. Ogishi, *KDDI R&D Laboratories Inc., Japan*
S. Prokopenko, *Tomsk State University, Russia*
S. Reiff-Marganec, *University of Stirling, United Kingdom*
I. Rodríguez, *Universidad Complutense de Madrid, Spain*
F. Rubio, *Universidad Complutense de Madrid, Spain*

C. E. Shankland, *University of Stirling, United Kingdom*
R. Soltwisch, *University of Göttingen, Germany*
J. Thees, *University of Kaiserslautern, Germany*
M. Tienari, *University of Helsinki, Finland*
V. Trenkaev, *Tomsk State University, Russia*
H. Ural, *University of Ottawa, Canada*
A. Ulrich, *Siemens, Germany*
E. Vieira, *INT, France*
G. Yang, *Bell Labs Research, China*
K. Yasumoto, *Nara Inst. Sci. Tech, Japan*
S. Yovine, *IMAG, Grenoble, France*

Organization Committee

Sarina Gwiszcs, *Brandenburg University of Technology Cottbus, Germany*
Christian Noack, *Brandenburg University of Technology Cottbus, Germany*
Irene Ostertag, *Technical University of Berlin, Germany*
Ronny Richter, *Brandenburg University of Technology Cottbus, Germany*
Katrín Willhöft, *Brandenburg University of Technology Cottbus, Germany*
Mario Zühlke, *Brandenburg University of Technology Cottbus, Germany*

Partners

BOSCH



Berlin Tourismus Marketing GmbH



Brandenburg University of Technology Cottbus



Microsoft®



Technische Universität Berlin

Telelogic

Table of Contents

UNIX STREAMS Generation from a Formal Specification	1
<i>Paweł Rychwański, Jacek Wytrębowicz</i>	
Specifying and Realising Interactive Voice Services	15
<i>Kenneth J. Turner</i>	
Vertical Reuse in the Development of Distributed Systems with FDTs	31
<i>Reinhard Gotzhein</i>	
Service-Oriented Systems Engineering: Modeling Services and Layered Architectures	48
<i>Manfred Broy</i>	
Validation of the Sessionless Mode of the HTTPR Protocol	62
<i>Paolo Romano, Milton Romero, Bruno Ciciani, Francesco Quaglia</i>	
Generation of All Counter-Examples for Push-Down Systems	79
<i>Samik Basu, Diptikalyan Saha, Yow-Jian Lin, Scott A. Smolka</i>	
Modeling and Model Checking Mobile Phone Payment Systems	95
<i>Tim Kempster, Colin Stirling</i>	
Behavioural Contracts for a Sound Assembly of Components	111
<i>Cyril Carrez, Alessandro Fantechi, Elie Najm</i>	
Automatic Verification of Annotated Code	127
<i>Doron Peled, Hongyang Qu</i>	
Combating Infinite State Using Ergo	144
<i>Peter Robinson, Carron Shankland</i>	
Numerical Coverage Estimation for the Symbolic Simulation of Real-Time Systems	160
<i>Farn Wang, Geng-Dian Hwang, Fang Yu</i>	
Discrete Timed Automata and MONA: Description, Specification and Verification of a Multimedia Stream	177
<i>Rodolfo Gómez, Howard Bowman</i>	
Can Decision Diagrams Overcome State Space Explosion in Real-Time Verification?	193
<i>Dirk Beyer, Andreas Noack</i>	
How Stop and Wait Protocols Can Fail over the Internet	209
<i>Jonathan Billington, Guy Edward Gallasch</i>	

Introducing Commutative and Associative Operators in Cryptographic Protocol Analysis	224
<i>Ivan Cibario Bertolotti, Luca Durante, Riccardo Sisto, Adriano Valenzano</i>	
A Lightweight Formal Analysis of a Multicast Key Management Scheme . .	240
<i>Mana Taghdiri, Daniel Jackson</i>	
Formal Security Policy Verification of Distributed Component-Structured Software	257
<i>Peter Herrmann</i>	
Towards Testing SDL Specifications: Models and Fault Coverage for Concurrent Timers	273
<i>Mariusz A. Fecko, M. Ümit Uyar, Ali Y. Duale</i>	
Concerning the Ordering of Adaptive Test Sequences	289
<i>Robert M. Hierons, Hasan Ural</i>	
Correct Passive Testing Algorithms and Complete Fault Coverage	303
<i>Arun N. Netravali, Krishan K. Sabnani, Ramesh Viswanathan</i>	
QoS Functional Testing for Multi-media Systems	319
<i>Tao Sun, Keiichi Yasumoto, Masaaki Mori, Teruo Higashino</i>	
Towards Testing Stochastic Timed Systems	335
<i>Manuel Núñez, Ismael Rodríguez</i>	
Formal Design of Interactive Multimedia Documents	351
<i>Jean-Pierre Courtiat</i>	
Progressive Solutions to a Parallel Automata Equation	367
<i>Sergey Buffalov, Khaled El-Fakih, Nina Yevtushenko, Gregor v. Bochmann</i>	
Type Abstraction in Formal Protocol Specifications with Container Types	383
<i>Joachim Thees</i>	
Decomposing Service Definition in Predicate/Transition-Nets for Designing Distributed Systems	399
<i>Hirozumi Yamaguchi, Gregor von Bochmann, Teruo Higashino</i>	
Towards an Efficient Performance Evaluation of Communication Systems Described by Message Sequence Charts	415
<i>Hesham Kamal Arafat Mohamed, Bruno Müller-Clostermann</i>	
Author Index	431