

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Kenji Suzuki Teruo Higashino
Keiichi Yasumoto Khaled El-Fakih (Eds.)

Formal Techniques for Networked and Distributed Systems – FORTE 2008

28th IFIP WG 6.1 International Conference
Tokyo, Japan, June 10-13, 2008
Proceedings

Volume Editors

Kenji Suzuki
The University of Electro-Communications
Department of Computer Science
1-5-1 Chofugaoka, Chofu-shi, Tokyo 182-8585, Japan
E-mail: suzuki@cs.uec.ac.jp

Teruo Higashino
Osaka University
Graduate School of Information Science and Technology
Department of Information Networking
Suita, Osaka 565-0871, Japan
E-mail: higashino@ist.osaka-u.ac.jp

Keiichi Yasumoto
Nara Institute of Science and Technology
Graduate School of Information Science
Ikoma, Nara 630-0192, Japan
E-mail: yasumoto@is.naist.jp

Khaled El-Fakih
Verimag – Université Joseph Fourier
Centre Equation, 2 rue de Vignate, 38610 Gières, France
E-mail: Khaled.Elfakih@imag.fr

Library of Congress Control Number: 2008927452

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

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743
ISBN-10 3-540-68854-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-68854-9 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media
springer.com

© IFIP International Federation for Information Processing 2008
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12278343 06/3180 5 4 3 2 1 0

Preface

This volume contains the proceedings of FORTE 2008, 28th IFIP WG6.1 International Conference on Formal Techniques for Networked and Distributed Systems. FORTE 2008 was held at the Campus Innovation Center in Tokyo, Japan during June 10–13, 2008. FORTE denotes a series of international working conferences on formal description techniques 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. In 2001 the conference changed the name to its current form. Recent conferences of this long series were held in Berlin (2003), Madrid(2004), Taipei(2005), Paris(2006), and Tallinn(2007).

As in the previous year, FORTE 2008 was collocated with TESTCOM/FATES 2008: the 20th IFIP International Conference on Testing of Communicating Systems (TESTCOM) and the 8th International Workshop on Formal Approaches to Testing of Software (FATES). The co-location of FORTE and TESTCOM/FATES fostered the collaboration between their communities. The common spirit of both conferences was underpinned by joint opening and closing sessions, invited talks, as well as joint social events.

This year we received 44 submissions. The Program Committee finally selected 19 full papers and 1 short paper for presentation at the conference. The special focus of FORTE 2008 was on formal approaches to new areas of networked and distributed systems such as ubiquitous, grid, and mobile computing systems, and also on the application of formal techniques to service-oriented architectures as well as security issues in networked systems. Together with the invited presentation by Wolfram Schulte from Microsoft Research, USA, the 20 accepted papers formed the very strong and high-quality program of FORTE 2008. In addition, the conference included two more invited presentations on behalf of TESTCOM/FATES by Yutaka Yasuda from KDDI Corporation, Japan and Paul Baker from Motorola, UK. A tutorial day preceded the conference.

It took tremendous efforts to organize this event. We would like to thank all the contributors for the success of FORTE 2008. In particular we are grateful to the Local Organization Chair, Tomohiko Ogishi from KDDI R&D Laboratories, who handled issues related to the conference venue, social events, and registration, and Takaaki Umedu from Osaka University, who managed the conference website and paper submission system. We also owe special thanks to all members of the FORTE 2008 Steering Committee, Program Committee, and co-reviewers for their support in selecting high-quality papers. Without these contributions, these proceedings would not exist. We thank the International Communications Foundation, Support Center for Advanced Telecommunications Technology Research, Foundation, Microsoft Research, and KDDI Corporation for their financial support, and Springer for publishing the proceedings.

Last but not least, we would also like to express our sincere appreciation to The University of Electro-Communications, Osaka University, Nara Institute of Science and Technology, Verimag, Université Joseph Fourier, and to all members of the Local Organization team for their continuous support of this conference.

March 2008

Kenji Suzuki
Teruo Higashino
Keiichi Yasumoto
Khaled El-Fakih

Conference Organization

General Chairs

Kenji Suzuki (The University of Electro-Communications, Japan)
Teruo Higashino (Osaka University, Japan)

Program Chairs

Keiichi Yasumoto (Nara Institute of Science and Technology,
Japan)
Khaled El-Fakih (Verimag, Université Joseph Fourier, France, and
American University of Sharjah, UAE)

FORTE Steering Committee

Gregor v. Bochmann (University of Ottawa, Canada)
John Derrick (University of Sheffield, UK)
Ken Turner (University of Stirling, UK)

Program Committee

Jiri Adamek (Charles University in Prague, Czech Republic)
Jonathan Billington (University of South Australia, Australia)
Gregor v. Bochmann (University of Ottawa, Canada)
Kirill Bogdanov (University of Sheffield, UK)
Mario Bravetti (University of Bologna, Italy)
Ana Cavalli (INT Evry, France)
Jose M. Colom (University of Zaragoza, Spain)
John Derrick (University of Sheffield, UK)
David de Frutos-Escrig (Complutense University of Madrid, Spain)
Reinhard Gotzhein (University of Kaiserslautern, Germany)
Susanne Graf (Verimag, France)
Serge Haddad (Lamsade-Paris Dauphine, France)
Teruo Higashino (Osaka University, Japan)
Dieter Hogrefe (University of Gottingen, Germany)
Gerard J. Holzmann (NASA/JPL, USA)
Claude Jard (ENS Cachan - Bretagne, France)
Ferhat Khendek (Concordia University, Canada)
Myungchul Kim (ICU, South Korea)
Hartmut Koenig (Brandenburg University of Technology, Germany)

David Lee (Ohio State University, USA)
Luigi Logrippo (University of Quebec - Outaouais, Canada)
Jose C. Maldonado (University of San Carlos, Brazil)
Elie Najm (ENST, France)
Masakatsu Nishigaki (Shizuoka University, Japan)
Manuel Nunez (Complutense University of Madrid, Spain)
Kazuhito Ohmaki (AIST, Japan)
Olaf Owe (University of Oslo, Norway)
Doron A. Peled (University of Warwick, UK)
Alexandre Petrenko (CRIM Montreal, Canada)
Jean-Francois Pradat-Peyre (Cedric-Cnam, France)
Wolfgang Reisig (Humboldt University, Germany)
Ichiro Satoh (NII, Japan)
Hiroyuki Seki (NAIST, Japan)
Jean-Bernard Stefani (Inria, France)
Kenji Suzuki (The University of Electro-Communications, Japan)
Stavros Tripakis (Cadence, USA)
Ken Turner (University of Stirling, UK)
Hasan Ural (University of Ottawa, Canada)
Juri Vain (Tallinn University of Technology, Estonia)
Farn Wang (National Taiwan University, Taiwan)
Jianping Wu (Tsinghua University, China)
Nina Yevtushenko (Tomsk State University, Russia)
Xia Yin (Tsinghua University, China)

Local Organization

Tomohiko Ogishi (KDDI R&D Laboratories Inc.) (Chair)
Takaaki Umedu (Osaka University)

Additional Reviewers

| | | |
|-------------------|---------------------|-----------------------|
| Saleh Al-Shadly | Irfan Hamid | Shin Nakajima |
| Cesar Andres | Chuanming Jing | Fernando Rosa-Velardo |
| Beatrice Berard | Einar B. Johnsen | Alper Sen |
| Faycal Bessayah | Guy-Vincent Jourdan | Soonuk Seol |
| Sergiy Boroday | Sungwon Kang | Andrey Shabaldin |
| Patricia Bouyer | Rajesh Karunamurthy | Natalia Shabaldina |
| Marius Bozga | Felix Klaedtke | Carron Shankland |
| David Cairns | Nimrod Lilith | Xingang Shi |
| Robert G. Clark | Lin Liu | Sebastian Schmerl |
| Arnaud Dury | Luis Llana | Martin Steffen |
| Lars-Ake Fredlund | Amel Mammar | Koichi Takahashi |
| Guy Gallasch | Mercedes G. Merayo | Min Tang |

Erik Tschinkel
Michael Vogel
Sebastian Vogel

Zhiliang Wang
Bachar Wehbi

Denis Wolf
Hirozumi Yamaguchi

Sponsoring Institutions

International Communications Foundation, Tokyo, Japan
Support Center for Advanced Telecommunications Technology Research,
Foundation, Tokyo, Japan
Microsoft Research, Redmond, USA
KDDI Corporation, Tokyo, Japan

Table of Contents

Invited Talk

| | |
|--|---|
| Model Generation for Horn Logic with Stratified Negation | 1 |
| <i>Ethan K. Jackson and Wolfram Schulte</i> | |

Abstraction

| | |
|---|----|
| Counterexample Guided Spotlight Abstraction Refinement | 21 |
| <i>Tobe Toben</i> | |
| An Experimental Evaluation of Probabilistic Simulation | 37 |
| <i>Jonathan Bogdoll, Holger Hermanns, and Lijun Zhang</i> | |
| An SMT Approach to Bounded Reachability Analysis of Model Programs | 53 |
| <i>Margus Veanes, Nikolaj Bjørner, and Alexander Raschke</i> | |

Verification

| | |
|--|----|
| Parameterized Tree Systems | 69 |
| <i>Parosh Aziz Abdulla, Noomene Ben Henda, Giorgio Delzanno, Frédéric Haziza, and Ahmed Rezine</i> | |
| Adapting Petri Nets Reductions to Promela Specifications | 84 |
| <i>C. Pajault, J.-F. Pradat-Peyre, and P. Rousseau</i> | |
| Verification of a Hierarchical Generic Mutual Exclusion Algorithm | 99 |
| <i>Souheib Baarir, Julien Sopena, and Fabrice Legond-Aubry</i> | |

Specification Framework I

| | |
|---|-----|
| Distributed Semantics and Implementation for Systems with Interaction and Priority | 116 |
| <i>Ananda Basu, Philippe Bidinger, Marius Bozga, and Joseph Sifakis</i> | |
| Checking Correctness of Transactional Behaviors | 134 |
| <i>Vincenzo Ciancia, Gian Luigi Ferrari, Roberto Guanciale, and Daniele Strollo</i> | |
| Specifying and Verifying Web Transactions | 149 |
| <i>Jing Li, Huibiao Zhu, and Jifeng He</i> | |

Application

| | |
|---|-----|
| Modelling and Analysing the Contract Net Protocol - Extension Using Coloured Petri Nets | 169 |
| <i>Jonathan Billington, Amar Kumar Gupta, and Guy Edward Gallasch</i> | |
| Program Repair Suggestions from Graphical State-Transition Specifications | 185 |
| <i>Farn Wang and Chih-Hong Cheng</i> | |
| Verifying Erlang Telecommunication Systems with the Process Algebra μ CRL | 201 |
| <i>Qiang Guo, John Derrick, and Csaba Hoch</i> | |

Specification Framework II

| | |
|---|-----|
| NQSL - Formal Language and Tool Support for Network Quality-of-Service Requirements | 218 |
| <i>Christian Webel, Reinhard Gotzhein, and Joachim Nicolay</i> | |
| Timed Mobile Ambients for Network Protocols | 234 |
| <i>Bogdan Aman and Gabriel Ciobanu</i> | |
| A Specification Framework for Earth-Friendly Logistics | 251 |
| <i>Ichiro Satoh</i> | |

Theory

| | |
|---|-----|
| A Hierarchy of Equivalences for Probabilistic Processes | 267 |
| <i>Manuel Núñez and Luis Llana</i> | |
| Multiset Bisimulations as a Common Framework for Ordinary and Probabilistic Bisimulations | 283 |
| <i>David de Frutos Escrig, Miguel Palomino, and Ignacio Fábregas</i> | |

Reliability of Networked Systems

| | |
|---|-----|
| Detecting Communication Protocol Security Flaws by Formal Fuzz Testing and Machine Learning | 299 |
| <i>Guoqiang Shu, Yating Hsu, and David Lee</i> | |
| Using SPIN to Detect Vulnerabilities in the AACS Drive-Host Authentication Protocol | 305 |
| <i>Wei Wang and Dongyao Ji</i> | |
| Protocol Modeling with Model Program Composition | 324 |
| <i>Margus Veanes and Wolfram Schulte</i> | |

| | |
|-------------------------------|-----|
| Author Index | 341 |
|-------------------------------|-----|