

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

TU Dortmund University, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

Erika Ábrahám Catuscia Palamidessi (Eds.)

Formal Techniques for Distributed Objects, Components, and Systems

34th IFIP WG 6.1 International Conference, FORTE 2014
Held as Part of the 9th International Federated Conference
on Distributed Computing Techniques, DisCoTec 2014
Berlin, Germany, June 3-5, 2014
Proceedings



Springer

Volume Editors

Erika Ábrahám
RWTH Aachen University, Informatik 2
Ahornstraße 55, 52074 Aachen, Germany
E-mail: abraham@informatik.rwth-aachen.de

Catuscia Palamidessi
Inria, Bâtiment Alan Turing, Campus de l'École Polytechnique
1, Rue Honoré d'Estienne d'Orves, 91120 Palaiseau, France
E-mail: catuscia@lix.polytechnique.fr

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-662-43612-7 e-ISBN 978-3-662-43613-4
DOI 10.1007/978-3-662-43613-4
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014939037

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© IFIP International Federation for Information Processing 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Foreword

In 2014, the 9th International Federated Conference on Distributed Computing Techniques (DisCoTec) took place in Berlin, Germany, during June 3–5. It was hosted and organized by the Technische Universität Berlin. The DisCoTec series, one of the major events sponsored by the International Federation for Information Processing (IFIP), included three conferences:

- COORDINATION 2014, the 16th International Conference on Coordination Models and Languages
- DAIS 2014, the 14th IFIP WG 6.1 International Conference on Distributed Applications and Interoperable Systems
- FORTE 2014, the 34th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components and Systems

Together, these conferences cover the complete spectrum of distributed computing subjects ranging from theoretical foundations over formal specification techniques to systems research issues.

Each day of the federated event began with a plenary speaker nominated by one of the conferences. The three invited speakers were:

- Frank Leymann (University of Stuttgart, Germany)
- Maarten van Steen (VU University Amsterdam, The Netherlands)
- Joachim Parrow (Uppsala University, Sweden)

There were also three satellite events, taking place on June 6–7:

1. The 5th International Workshop on *Interactions between Computer Science and Biology* (CS2BIO) with keynote lectures by Marco Pettini (Université de la Méditerranée, France) and Vincent Danos (University of Edinburgh, UK) and a tutorial by Jeffrey Johnson (Open University, UK)
2. The 7th Workshop on *Interaction and Concurrency Experience* (ICE) with keynote lectures by Kim Larsen (Aalborg University, Denmark) and Pavol Cerny (University of Colorado Boulder, USA)
3. The First International Workshop on *Meta Models for Process Languages* (MeMo) with keynote lectures by Joachim Parrow (Uppsala University, Sweden) and Marino Miculan (Università degli Studi di Udine, Italy)

This program offered an interesting and stimulating event for the participants. Sincere thanks go to the chairs and members of the Program Committees of the involved conferences and workshops for their highly appreciated effort. Moreover,

organizing DisCoTec 2014 was only possible thanks to the dedicated work of the Organizing Committee from TU Berlin, including Margit Russ, Kirstin Peters (also Publicity and Workshop Chair), and Christoph Wagner. Finally, many thanks go to IFIP WG 6.1 for providing the umbrella for this event, to EATCS and TU Berlin for their support and sponsorship, and to EasyChair for providing the refereeing infrastructure.

June 2014

Uwe Nestmann

Preface

This volume contains the proceedings of FORTE 2014, the 34th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components and Systems. FORTE 2014 took place June 3–5, 2014, as part of DisCoTec 2014, the 9th International Federated Conference on Distributed Computing Techniques. After 1996 in Kaiserslautern and 2003 in Berlin, this year the conference returned to Germany, in the heart of Europe, to the exciting, multi-faceted city of Berlin.

FORTE—since 2014 the heir to the original FORTE series, FMOODS series and joint FMOODS/FORTE conference series—is a forum for fundamental research on theory, models, tools, and applications for distributed systems, supporting the advance of science and technologies in this area. The conference encourages contributions that combine theory and practice and that exploit formal methods and theoretical foundations to present novel solutions to problems arising from the development of distributed systems. FORTE covers distributed computing models and formal specification, testing and verification methods. The application domains include all kinds of application-level distributed systems, telecommunication services, Internet, embedded and real-time systems, cyber-physical systems and sensor networks, as well as networking and communication security and reliability.

We received 55 abstracts, out of which 50 full papers were submitted for review. Each submission was reviewed by at least four Program Committee members. Based on the reviews and a thorough (electronic) discussion by the Program Committee, we selected 18 papers for presentation at the conference and for publication in this volume.

Joachim Parrow (Uppsala University, Sweden) was the keynote speaker of FORTE 2014. He is well-known in our community for his fundamental contribution to concurrency theory. In particular, he is one of the founding fathers of the π -calculus, and of the Fusion calculus. His team in Uppsala is the developer and the maintainer of the Mobility Workbench, a tool for manipulating and analyzing mobile concurrent systems. In his keynote speech, Joachim Parrow presented his recent work on the use of interactive theorem provers to validate frameworks of formalisms.

We would like to thank all who contributed to making FORTE 2014 a successful event in a constructive atmosphere: first of all the authors for submitting the results of their research to FORTE; the Program Committee and the additional reviewers for the reviews, efficient discussions, and a fair selection process; our invited speaker for enriching the program with his inspiring talk; the FORTE Steering Committee for taking care of the general needs and interests of the series; and of course the attendees of the event for their interest in the presentations and for the numerous constructive discussions. We benefited greatly

from the EasyChair conference management system, which we used to handle the submission, review, discussion, and proceedings preparation processes. We would also like to express our thank to the International Federation for Information Processing (IFIP), the European Association for Theoretical Computer Science (EATCS) and the Technische Universität Berlin for their great support. Last but not least, we are grateful to the DisCoTec General Chair Uwe Nestmann and all members of his local organization team at the University of Berlin for taking care of all the organizational issues.

June 2014

Erika Ábrahám
Catuscia Palamidessi

Organization

Program Committee

Erika Ábrahám (Co-chair)	RWTH Aachen University, Germany
Myrto Arapinis	University of Edinburgh, UK
Paul C. Attie	American University of Beirut, Lebanon
Dirk Beyer	University of Passau, Germany
Michele Boreale	University of Florence, Italy
Johannes Borgström	Uppsala University, Sweden
Roberto Bruni	University of Pisa, Italy
Pedro R. D'Argenio	Universidad Nacional de Córdoba, Argentina
Frank S. de Boer	LIACS/CWI, The Netherlands
Yuxin Deng	Shanghai Jiaotong University, China
Yliès Falcone	University of Grenoble, France
Daniele Gorla	Sapienza Università di Roma, Italy
Susanne Graf	CNRS/VERIMAG, France
Rachid Guerraoui	EPFL, Switzerland
Klaus Havelund	NASA/JPL, USA
Axel Legay	IRISA/Inria at Rennes, France
Jay Ligatti	University of South Florida, USA
Alberto Lluch Lafuente	IMT Lucca, Italy
Antonia Lopes	University of Lisbon, Portugal
Sjouke Mauw	University of Luxembourg, Luxembourg
Annabelle McIver	Macquarie University, Australia
Sebastian A. Mödersheim	Technical University of Denmark, Denmark
Peter Csaba Ölveczky	University of Oslo, Norway
Catuscia Palamidessi (Co-chair)	Inria Saclay, France
Doron Peled	Bar Ilan University, Israel
Anna Philippou	University of Cyprus, Cyprus
Sanjiva Prasad	Indian Institute of Technology Delhi, India
Sophie Quinton	Inria, France
Ana Sokolova	University of Salzburg, Austria
Heike Wehrheim	University of Paderborn, Germany

Additional Reviewers

Åman Pohjola, Johannes	Alvim, Mario S.	Arun-Kumar, S.
Aigner, Martin	Andric, Marina	Baldan, Paolo
Akshay, S.	Armstrong, Alasdair	Beggiato, Alessandro
Albright, Yan	Aronis, Stavros	Bensalem, Saddek

Table of Contents

Specification Languages and Type Systems

Type Checking Liveness for Collaborative Processes with Bounded and Unbounded Recursion	1
<i>Søren Debois, Thomas Hildebrandt, Tijs Slaats, and Nobuko Yoshida</i>	
Property Specification Made Easy: Harnessing the Power of Model Checking in UML Designs	17
<i>Daniela Remenska, Tim A.C. Willemse, Jeff Templon, Kees Verstoep, and Henri Bal</i>	
Formal Specification and Verification of CRDTs	33
<i>Peter Zeller, Annette Bieniusa, and Arnd Poetzsch-Heffter</i>	

Monitoring and Testing

Actor- and Task-Selection Strategies for Pruning Redundant State-Exploration in Testing	49
<i>Elvira Albert, Puri Arenas, and Miguel Gómez-Zamalloa</i>	
Efficient and Generalized Decentralized Monitoring of Regular Languages	66
<i>Yliès Falcone, Tom Cornebize, and Jean-Claude Fernandez</i>	
A Model-Based Certification Framework for the EnergyBus Standard . . .	84
<i>Alexander Graf-Brill, Holger Hermanns, and Hubert Garavel</i>	
Effectiveness for Input Output Conformance Simulation <i>iocos</i>	100
<i>Carlos Gregorio-Rodríguez, Luis Llana, and Rafael Martínez-Torres</i>	

Security Analysis

A Program Logic for Verifying Secure Routing Protocols	117
<i>Chen Chen, Limin Jia, Hao Xu, Cheng Luo, Wenchao Zhou, and Boon Thau Loo</i>	
Verifying Security Policies Using Host Attributes	133
<i>Cornelius Diekmann, Stephan-A. Posselt, Heiko Niedermayer, Holger Kinkel, Oliver Hanka, and Georg Carle</i>	
Denial-of-Service Security Attack in the Continuous-Time World	149
<i>Shuling Wang, Flemming Nielson, and Hanne Riis Nielson</i>	

Quantitative Information Flow under Generic Leakage Functions and Adaptive Adversaries	166
<i>Michele Boreale and Francesca Pampaloni</i>	
Uniform Protection for Multi-exposed Targets	182
<i>Roberto Vigo, Flemming Nielson, and Hanne Riis Nielson</i>	
Metrics for Differential Privacy in Concurrent Systems	199
<i>Lili Xu, Konstantinos Chatzikokolakis, and Huimin Lin</i>	

Bisimulation, Abstraction and Reduction

Dimming Relations for the Efficient Analysis of Concurrent Systems via Action Abstraction	216
<i>Rocco De Nicola, Giulio Iacobelli, and Mirco Tribastone</i>	
On the Step Branching Time Closure of Free-Choice Petri Nets	232
<i>Stephan Mennicke, Jens-Wolfhard Schicke-Uffmann, and Ursula Goltz</i>	
Coinductive Definition of Distances between Processes: Beyond Bisimulation Distances	249
<i>David Romero-Hernández and David de Frutos Escrig</i>	
Mechanizing the Minimization of Deterministic Generalized Büchi Automata	266
<i>Souheib Baarir and Alexandre Duret-Lutz</i>	
Formal Verification of Complex Properties on PLC Programs	284
<i>Dániel Darvas, Borja Fernández Adiego, András Vörös, Tamás Bartha, Enrique Blanco Viñuela, and Víctor M. González Suárez</i>	
Author Index	301