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
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 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 Inria Saclay, France

(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 Beggiauto, Alessandro
Albright, Yan Aronis, Stavros Bensalem, Saddek
Steering Committee

Chair
Jean-Bernard Stefani Inria, France

Elected Members
Frank S. de Boer LIACS/CWI, The Netherlands
Einar Broch Johnsen University of Oslo, Norway
Heike Wehrheim University of Paderborn, Germany

Rotating Members
2011–2014 Roberto Bruni University of Pisa, Italy
2011–2014 Juergen Dingel Queens’s University, Canada
2012–2015 Holger Giese University of Potsdam, Germany
2012–2015 Grigore Rosu University of Illinois at Urbana-Champaign, USA
2013–2016 Dirk Beyer University of Passau, Germany
2013–2016 Michele Boreale University of Florence, Italy
## Table of Contents

### Specification Languages and Type Systems

- **Type Checking Liveness for Collaborative Processes with Bounded and Unbounded Recursion** ........................................ 1  
  
  *Søren Debois, Thomas Hildebrandt, Tijs Slaats, and Nobuko Yoshida*

- **Property Specification Made Easy: Harnessing the Power of Model Checking in UML Designs** ........................................ 17  
  
  *Daniela Remenska, Tim A.C. Willemse, Jeff Templon, Kees Verstoep, and Henri Bal*

- **Formal Specification and Verification of CRDTs** ................. 33  
  
  *Peter Zeller, Annette Bieniusa, and Arnd Poetzsch-Heffter*

### Monitoring and Testing

- **Actor- and Task-Selection Strategies for Pruning Redundant State-Exploration in Testing** ....................................... 49  
  
  *Elvira Albert, Puri Arenas, and Miguel Gómez-Zamalloa*

- **Efficient and Generalized Decentralized Monitoring of Regular Languages** ...................................................... 66  
  
  *Yliès Falcone, Tom Cornebize, and Jean-Claude Fernandez*

- **A Model-Based Certification Framework for the EnergyBus Standard** .......................................................... 84  
  
  *Alexander Graf-Brill, Holger Hermanns, and Hubert Garavel*

- **Effectiveness for Input Output Conformance Simulation iocos** ................. 100  
  
  *Carlos Gregorio-Rodríguez, Luis Llana, and Rafael Martínez-Torres*

### Security Analysis

- **A Program Logic for Verifying Secure Routing Protocols** ................. 117  
  
  *Chen Chen, Limin Jia, Hao Xu, Cheng Luo, Wenchao Zhou, and Boon Thau Loo*

- **Verifying Security Policies Using Host Attributes** ................. 133  
  
  *Cornelius Diekmann, Stephan-A. Posselt, Heiko Niedermayer, Holger Kinkelín, Oliver Hanka, and Georg Carle*

- **Denial-of-Service Security Attack in the Continuous-Time World** ................. 149  
  
  *Shuling Wang, Flemming Nielson, and Hanne Riis Nielson*
Quantitative Information Flow under Generic Leakage Functions and Adaptive Adversaries ............................................. 166  
Michele Boreale and Francesca Pampaloni

Uniform Protection for Multi-exposed Targets ..................... 182  
Roberto Vigo, Flemming Nielson, and Hanne Riis Nielson

Metrics for Differential Privacy in Concurrent Systems .......... 199  
Lili Xu, Konstantinos Chatzikokolakis, and Huimin Lin

Bisimulation, Abstraction and Reduction

Dimming Relations for the Efficient Analysis of Concurrent Systems via Action Abstraction ............................................. 216  
Rocco De Nicola, Giulio Iacobelli, and Mirco Tribastone

On the Step Branching Time Closure of Free-Choice Petri Nets .... 232  
Stephan Mennicke, Jens-Wolfhard Schicke-Uffmann, and Ursula Goltz

Coinductive Definition of Distances between Processes: Beyond Bisimulation Distances ............................................. 249  
David Romero-Hernández and David de Frutos Escrig

Mechanizing the Minimization of Deterministic Generalized Büchi Automata ..................................................... 266  
Souheib Baarir and Alexandre Duret-Lutz

Formal Verification of Complex Properties on PLC Programs ...... 284  
Dániel Darvas, Borja Fernández Adiego, András Vörös, Tamás Bartha, Enrique Blanco Viñuela, and Víctor M. González Suárez

Author Index .......................................................... 301