Lecture Notes in Computer Science 7892

Dirk Beyer Michele Boreale (Eds.)

Formal Techniques for Distributed Systems

Joint IFIP WG 6.1 International Conference
FMOODS/FORTE 2013
Held as Part of the 8th International Federated Conference
on Distributed Computing Techniques, DisCoTec 2013
Florence, Italy, June 3-5, 2013, Proceedings

Springer

Volume Editors

Dirk Beyer
University of Passau
Department of Computer Science and Mathematics
Innstraße 31, 94032, Passau, Germany

Michele Boreale
Università di Firenze
Dipartimento di Statistica, Informatica, Applicazioni (DiSIA)
Viale Morgagni, 65, 50134 Florence, Italy

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-38591-9 e-ISBN 978-3-642-38592-6
DOI 10.1007/978-3-642-38592-6
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013938531

CR Subject Classification (1998): F.3, D.2.4, F.1, D.2, F.4, I.2.2-3, D.3, C.2, C.3

LNCS Sublibrary: SL 2 – Programming and Software Engineering

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 2013, the 8th International Federated Conference on Distributed Computing Techniques (DisCoTec) took place in Florence, Italy, during June 3–6. They were hosted and organized by the Università di Firenze. The DisCoTec series of federated conferences, one of the major events sponsored by the International Federation for Information processing (IFIP), included three conferences:

- The 15th International Conference on Coordination Models and Languages (Coordination)
- The 13th IFIP International Conference on Distributed Applications and Interoperable Systems (DAIS)
- The 2013 IFIP Joint International Conference on Formal Techniques for Distributed Systems (33rd FORTE/15th FMOODS)

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

Each of the first three days of the federated event began with a plenary speaker nominated by one of the conferences. The three invited speakers were: Tevfik Bultan, Department of Computer Science at the University of California, Santa Barbara, USA; Gian Pietro Picco, Department of Information Engineering and Computer Science at the University of Trento, Italy; and Roberto Baldoni, Department of Computer, Control and Management Engineering "Antonio Ruberti", Università degli Studi di Roma "La Sapienza", Italy. In addition, on the second day, there was a joint technical session consisting of one paper from each of the conferences. There were also three satellite events:

1. The 4th International Workshop on Interactions Between Computer Science and Biology (CS2BIO) with keynote talks by Giuseppe Longo (ENS Paris, France) and Mario Rasetti (ISI Foundation, Italy)
2. The 6th Workshop on Interaction and Concurrency Experience (ICE) with keynote lectures by Davide Sangiorgi (Università di Bologna, Italy) and Damien Pous (ENS Lyon, France)
3. The 9th International Workshop on Automated Specification and Verification of Web Systems (WWV) with keynote talks by Gerhard Friedrich (Universität Klagenfurt, Austria) and François Taïani (Université de Rennes 1, France)

I believe that this program offered each participant an interesting and stimulating event. I would like to thank the Program Committee Chairs of each conference and workshop for their effort. Moreover, organizing DisCoTec 2013 was only possible thanks to the dedicated work of the Publicity Chair Francesco Tiezzi (IMT Lucca, Italy), the Workshop Chair Rosario Pugliese (Università di Firenze, Italy), and the members of the Organizing Committee from Università di Firenze: Luca Cesari, Andrea Margheri, Massimiliano Masi, Simona Rinaldi, and Betti Venneri. To conclude I want to thank the International Federation for Information Processing (IFIP) and Università di Firenze for their sponsorship.

June 2013 Michele Loreti

Preface

This volume contains the proceedings of the 2013 IFIP Joint International Conference on Formal Techniques for Distributed Systems (33^{rd} FORTE/15^{th} FMOODS). The joint conference is the result of merging the two international conferences Formal Techniques for Networked and Distributed Systems (FORTE) and Formal Methods for Open Object-Based Distributed Systems (FMOODS). The city of Florence, Italy, was selected as the conference venue, taking place during June 3–5, 2013. This edition of the conference was organized as part of the 8th International Federated Conference on Distributed Computing Techniques (DisCoTec).

The FORTE/FMOODS conference series represents a forum for fundamental research on theory, models, tools, and applications for distributed systems. 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/FMOODS 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, as well as networking and communication security and reliability.

We received a total of 49 full paper submissions for review (10 were withdrawn before review). Each submission was reviewed by at least three members of the Program Committee (papers that were co-authored by a PC member received four reviews). Based on high-quality reviews, and a thorough (electronic) discussion by the Program Committee, we selected 20 papers for presentation at the conference and for publication in this volume.

Tevfik Bultan, University of California, Santa Barbara (USA), was the keynote speaker of FORTE/FMOODS 2013. He is well-known in our community for his work on dependability of Web-service-based systems and their automated verification. Tevfik Bultan's keynote, entitled "Analyzing Interactions of Asynchronously Communicating Software Components," gave an overview of "choreography" specifications and their realizability; an abstract of the keynote is included in this proceedings volume.

We would like to thank all who contributed to making FORTE/FMOOD 2013 a successful event: first of all, the authors, for submitting their fine research results; the Program Committee, for an efficient discussion and a fair selection process; the invited speaker; and of course the attendees of FORTE/FMOODS 2013! We are also grateful to the DisCoTec general chair, Michele Loreti, and all members of his local-organization team at the Università di Firenze. Thank you!

June 2013

Dirk Beyer
Michele Boreale

Organization

Program Committee

Sven Apel	University of Passau, Germany
Saddek Bensalem	VERIMAG, France
Dirk Beyer	University of Passau, Germany
Michele Boreale	Università di Firenze, Italy
Tevfik Bultan	University of California at Santa Barbara, USA
Luis Caires	Universidade Nova de Lisboa, Portugal
Mariangiola Dezani-Ciancaglini	Università di Torino, Italy
Juergen Dingel	Queen's University, Canada
Simon Gay	University of Glasgow, UK
Holger Giese	University of Potsdam, Germany
Kim Guldstrand Larsen	Aalborg University, Denmark
Arie Gurfinkel	Software Engineering Institute, USA
Matthew Hennessy	Trinity College Dublin, Ireland
Paola Inverardi	Università dell'Aquila, Italy
Alan Jeffrey	Bell Labs, USA
Joost-Pieter Katoen	RWTH Aachen University, Germany
Vladimir Klebanov	Karlsruhe Institute of Technology, Germany
Axel Legay	IRISA/INRIA at Rennes, France
Matteo Maffei	Saarland University, Germany
Uwe Nestmann	TU Berlin, Germany
Mauro Pezz	University of Lugano, Italy
Corneliu Popeea	TU Munich, Germany
Sophie Quinton	TU Braunschweig, Germany
Jan Rutten	CWI, The Netherlands
Geoffrey Smith	Florida International University, USA
Jaco Van De Pol	University of Twente, The Netherlands
Helmut Veith	Vienna University of Technology, Austria
Martin Wirsing	Ludwig Maximilians University of Munich, Germany
Nobuko Yoshida	Imperial College London, UK
Gianluigi Zavattaro	Università di Bologna, Italy

Additional Reviewers

Ancona, Davide
Autili, Marco
Berger, Martin
Bocchi, Laura
Bravetti, Mario
Cerone, Andrea
Combaz, Jacques
Delahaye, Benoit
Delange, Julien
Di Giusto, Cinzia
Di Pierro, Alessandra
Dyck, Johannes
Elrakaiby, Yehia
Fahrenberg, Uli
Fossati, Luca
Ghafari, Naghmeh
Giachino, Elena
Graf, Susanne
Jansen, Christina
Jongmans, Sung-Shik T. Q.
Kammueller, Florian
Koutavas, Vasileios
Kroiß, Christian
Lanese, Ivan
Ledesma-Garza, Ruslan
Loreti, Michele
Neumann, Stefan
Noll, Thomas
Nouri, Ayoub
Padovani, Luca
Peters, Kirstin
Posse, Ernesto
Pous, Damien
Proenca, Jose
Pérez, Jorge A.
Rensink, Arend
Schneider, Sven
Spaccasassi, Carlo
Tivoli, Massimo
Trefler, Richard
V. Gleissenthall, Klaus
Vigliotti, Maria
Vogel, Thomas
Volpato, Michele
Wong, Peter
Wätzoldt, Sebastian

Steering Committee

Jean-Bernard Stefani	(Chair, elected member)
Frank de Boer	(Elected member)
Einar Broch Johnsen	(Elected member)
Heike Wehrheim	(Elected member)
John Hatcliff	(Rotating member, 2010–2013)
Elena Zucca	(Rotating member, 2010–2013)
Roberto Bruni	(Rotating member, 2011–2014)
Juergen Dingel	(Rotating member, 2011–2014)
Holger Giese	(Rotating member, 2012–2015)
Grigore Rosu	(Rotating member, 2012–2015)

Table of Contents

Invited Talk

Analyzing Interactions of Asynchronously Communicating Software Components 1
Tevfik Bultan

Session 1: Verification

Formal Analysis of a Distributed Algorithm for Tracking Progress 5
Martín Abadi, Frank McSherry, Derek G. Murray, and Thomas L. Rodeheffer

A Case Study in Formal Verification Using Multiple Explicit Heaps 20
Wojciech Mostowski

Parameterized Verification of Track Topology Aggregation Protocols 35
Sergio Feo-Arenis and Bernd Westphal

Session 2: Types

Monitoring Networks through Multiparty Session Types 50
Laura Bocchi, Tzu-Chun Chen, Romain Demangeon, Kohei Honda, and Nobuko Yoshida

Semantic Subtyping for Objects and Classes 66
Ornela Dardha, Daniele Gorla, and Daniele Varacca

Polymorphic Types for Leak Detection in a Session-Oriented Functional Language 83
Viviana Bono, Luca Padovani, and Andrea Tosatto

Session 3: Testing

Passive Testing with Asynchronous Communications 99
Robert M. Hierons, Mercedes G. Merayo, and Manuel Núñez

Input-Output Conformance Simulation (iocos) for Model Based Testing 114
Carlos Gregorio-Rodríguez, Luis Llana, and Rafael Martínez-Torres

Session 4: DisCoTec Joint Session

Model Checking Distributed Systems against Temporal-Epistemic Specifications 130
Andreas Griesmayer and Alessio Lomuscio

Session 5: Model Checking

Formal Verification of Distributed Branching Multiway Synchronization Protocols 146
Hugues Evrard and Frédéric Lang

An Abstract Framework for Deadlock Prevention in BIP 161
Paul C. Attie, Saddek Bensalem, Marius Bozga, Mohamad Jaber, Joseph Sifakis, and Fadi A. Zaraket

Bounded Model Checking of Graph Transformation Systems via SMT Solving 178
Tobias Isenberg, Dominik Steenken, and Heike Wehrheim

Session 6: Automata

Verification of Directed Acyclic Ad Hoc Networks 193
Parosh Aziz Abdulla, Mohamed Faouzi Atig, and Othmane Rezine

Transducer-Based Algorithmic Verification of Retransmission Protocols over Noisy Channels 209
Jay Thakkar, Aditya Kanade, and Rajeev Alur

Asynchronously Communicating Visibly Pushdown Systems 225
Domagoj Babić and Zvonimir Rakamarić

Session 7: Distribution and Concurrency

A Timed Component Algebra for Services 242
Benoît Delahaye, José Luiz Fiadeiro, Axel Legay, and Antónia Lopes

Probabilistic Analysis of the Quality Calculus 258
Hanne Riis Nielson and Flemming Nielson

May-Happen-in-Parallel Based Deadlock Analysis for Concurrent Objects 273
Antonio E. Flores-Montoya, Elvira Albert, and Samir Genaim

Session 8: Security

Lintent: Towards Security Type-Checking of Android Applications 289
Michele Bugliesi, Stefano Calzavara, and Alvise Spanò

Honesty by Typing 305
Massimo Bartoletti, Alceste Scalas, Emilio Tuosto, and Roberto Zunino

Author Index 321