

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

Madhu Sudan

Microsoft Research, Cambridge, 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

John Hatcliff Elena Zucca (Eds.)

Formal Techniques for Distributed Systems

Joint 12th IFIP WG 6.1 International Conference, FMOODS 2010
and 30th IFIP WG 6.1 International Conference, FORTE 2010
Amsterdam, The Netherlands, June 7-9, 2010
Proceedings

Volume Editors

John Hatcliff

Kansas State University, Computing and Information Sciences

234 Nichols Hall, Manhattan, KS 66502, USA

E-mail: hatcliff@ksu.edu

Elena Zucca

DISI, University of Genova

Via Dodecaneso 35, 16146 Genova, Italy

E-mail: zucca@disi.unige.it

Library of Congress Control Number: Applied for

CR Subject Classification (1998): D.2, D.2.4, I.2.2, D.3, F.3, F.4, I.2.3

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743

ISBN-10 3-642-13463-7 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-13463-0 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.com

© IFIP International Federation for Information Processing 2010

Printed in Germany

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

Printed on acid-free paper 06/3180

Foreword

In 2010 the international federated conferences on Distributed Computing Techniques (DisCoTec) took place in Amsterdam, during June 7-9. It was hosted and organized by the Centrum voor Wiskunde & Informatica.

DisCoTec conferences jointly cover the complete spectrum of distributed computing subjects ranging from theoretical foundations to formal specification techniques to practical considerations. The 12th International Conference on Coordination Models and Languages (Coordination) focused on the design and implementation of models that allow compositional construction of large-scale concurrent and distributed systems, including both practical and foundational models, run-time systems, and related verification and analysis techniques. The 10th IFIP International Conference on Distributed Applications and Interoperable Systems in particular elicited contributions on architectures, models, technologies and platforms for large-scale and complex distributed applications and services that are related to the latest trends in bridging the physical/virtual worlds based on flexible and versatile service architectures and platforms. The 12th Formal Methods for Open Object-Based Distributed Systems and 30th Formal Techniques for Networked and Distributed Systems together emphasized distributed computing models and formal specification, testing and verification methods.

Each of the three days of the federated event began with a plenary speaker nominated by one of the conferences. The first day Joe Armstrong (Ericsson Telecom AB) gave a keynote speech on Erlang-style concurrency, the second day Gerard Holzmann (Jet Propulsion Laboratory, USA) discussed the question “Formal Software Verification: How Close Are We?”. The third and last day Joost Roelands (Director of Development Netlog) presented the problem area of distributed social data. In addition, there was a joint technical session consisting of one paper from each of the conferences and an industrial session with presentations by A. Stam (Almende B.V., Information Communication Technologies) and M. Verhoef (CHESS, Computer Hardware & System Software) followed by a panel discussion.

There were four satellite events: the Third DisCoTec Workshop on Context-Aware Adaptation Mechanisms for Pervasive and Ubiquitous Services (CAM-PUS), the First International Workshop on Interactions Between Computer Science and Biology (CS2BIO) with keynote lectures by Luca Cardelli (Microsoft Research - Cambridge, UK) and Jérôme Feret (INRIA and École Normale Supérieure - Paris, France), the First Workshop on Decentralized Coordination of Distributed Processes (DCDP) with a keynote lecture by Tyler Close (Google), and the Third Interaction and Concurrency Experience Workshop with keynote lectures by T. Henzinger (IST, Austria) and J.-P. Katoen (RWTH Aachen University, Germany).

I hope this rich program offered every participant interesting and stimulating events. It was only possible thanks to the dedicated work of the Publicity Chair Gianluigi Zavattaro (University of Bologna, Italy), the Workshop Chair Marcello Bonsangue (University of Leiden, The Netherlands) and the members of the Organizing Committee, Susanne van Dam, Immo Grabe, Stephanie Kemper and Alexandra Silva. To conclude I want to thank the sponsorship of the International Federation for Information processing (IFIP), the Centrum voor Wiskunde & Informatica and the Netherlands Organization for Scientific Research (NWO).

June 2010

Frank S. de Boer

Preface

This volume contains the proceedings of the IFIP International Conference on Formal Techniques for Distributed Systems. The conference was organized as the joint activity of two conferences: FMOODS (Formal Methods for Open Object-Based Distributed Systems) and FORTE (Formal Techniques for Networked and Distributed Systems). FMOODS/FORTE was part of the federated conference event DisCoTec (Distributed Computing Techniques) 2010, which also included the 12th International Conference on Coordination Models and Languages (COORDINATION) and the 10th IFIP International Conference on Distributed Applications and Interoperable Systems (DAIS).

The goal of FMOODS/FORTE is to provide a forum for fundamental research on theory and applications of distributed systems. The conference emphasizes the use of a variety of techniques for development of concurrent and distributed systems including model-based design, component and object technology, type systems, formal specification and verification, and formal approaches to testing.

The conference encourages contributions that combine theory and practice in application areas of telecommunication services, Internet, embedded and real-time systems, networking and communication security and reliability, sensor networks, service-oriented architecture, and Web services.

The FMOODS/FORTE 2010 program consisted of 13 regular and 6 short papers. These papers were selected by a 30-member Program Committee (PC) from among 38 submissions. Each paper was assigned to at least four PC members for a detailed review. Additional expert reviews were solicited if the reviews of a paper had diversified assessments or the reviewers indicated low confidence. The final decision of acceptance was based on a 10-day online discussion of the PC. The selected papers constituted a strong program of stimulating and timely topics in the areas of formal verification, algorithms and implementations, modeling and testing, process algebra and calculus, and analysis of distributed systems.

FORTE traces its heritage back to the Protocol Specification, Testing and Verification (PSTV) conference first held in 1981 in Teddington, UK. Since that first meeting, PSTV has evolved into FORTE and now into FMOODS/FORTE and this year's conference in Amsterdam was the 30th meeting in the conference series. To highlight this milestone, this year's DisCoTec plans to include a special celebration reflecting on the progress of the community since 1981 and on challenges for the future.

In the first PSTV meeting in 1981, Gerard Holzmann published a paper containing his early views of what would become the SPIN model checker. We were pleased to note this special work in the history of FORTE by featuring Dr. Holzmann as the keynote speaker of FMOODS/FORTE 2010 as part of this special celebration of PSTV - FORTE - FMOODS history.

We are deeply indebted to the PC members and external reviewers for their hard and conscientious work in preparing 154 reviews. We thank Frank de Boer, the DisCoTec General Chair, for his support, and the Steering Committees of FMOODS and FORTE for their guidance. Our gratitude goes to the authors for their support of the conference by submitting their high-quality research works. We thank the providers of the conference tool EasyChair that was a great help in organizing the submission and reviewing process.

June 2010

John Hatcliff
Elena Zucca

Organization

Program Chairs

John Hatcliff
Elena Zucca

Kansas State University, USA
University of Genoa, Italy

Program Committee

Gregor v. Bochmann
Paulo Borba
Mario Bravetti
Ana Cavalli
John Derrick
Mariangiola Dezani
Juergen Dingel
Dieter Hogrefe
Valerie Issarny
Claude Jard
Einar Broch Johnsen
Ferhat Khendek
David Lee
Jay Ligatti
Luigi Logrippo
Antonia Lopes
Peter Mueller
Uwe Nestmann
Manuel Núñez
Olaf Owe
Alexandre Petrenko
Frank Piessens
Arnd Poetzsch-Heffter
Martin Steffen
Ken Turner
Martin Wirsing
Keiichi Yasumoto
Nobuko Yoshida

University of Ottawa, Canada
Federal University of Pernambuco, Brazil
University of Bologna, Italy
INT Evry, France
University of Sheffield, UK
University of Turin, Italy
Queens University, Kingston, Ontario, Canada
University of Göttingen, Germany
INRIA, France
ENS Cachan - Bretagne, France
University of Oslo, Norway
Concordia University, Canada
The Ohio State University, USA
University of South Florida, USA
University of Quebec - Outaouais, Canada
University of Lisbon, Portugal
ETH, Switzerland
Technical University of Berlin, Germany
Complutense University of Madrid, Spain
University of Oslo, Norway
CRIM Montreal, Canada
Katholieke Universiteit Leuven, Belgium
University of Kaiserslautern, Germany
University of Oslo, Norway
University of Stirling, UK
LMU Munich, Germany
Nara Institute of Science and Technology,
Japan
Imperial College London, UK

Additional Referees

Suzana Andova	Toqeer Israr	Ernesto Posse
Lucian Bentea	Juliano Iyoda	Cristian Prisacariu
Lorenzo Bettini	Bart Jacobs	Ismael Rodriguez
Sergiy Boroday	Willy Jimenez	Fernando Rosa-Velardo
Florent Bouchy	Ioannis Kassios	Jan Schäfer
Roberto Bruni	Christian Kissig	Rudolf Schlatte
Marco Carbone	Ilham Kurnia	Sven Schneider
Corina Cirstea	Felipe Lalanne	Jens Schönborn
Ferruccio Damiani	David Lee	Adenilso Simao
Dominique Devriese	Ugo de' Liguoro	Carron Shankland
Mustafa Emre Dincturk	Luis Llana	Jan Smans
Jose Pablo Escobedo	Savi Maharaj	Fausto Spoto
Pietro Ferrara	Thi Mai Thuong Tran	Volker Stolz
David de Frutos-Escrig	Francisco Martins	Dries Vanoverberghe
Simon Gay	Tiago Massoni	Mahesh Viswanathan
Nils Gesbert	Alexandre Mota	Frederic Vogels
Rohit Gheyi	Akio Nakata	Neil Walkinshaw
Qiang Guo	Luca Padovani	Yannick Welsch
Yating Hsu	Miguel Palomino	Hirozumi Yamaguchi
Iksoon Hwang	Andrew Phillips	Gianluigi Zavattaro

Table of Contents

Invited Talk

Formal Software Verification: How Close Are We? (Abstract)	1
<i>Gerard J. Holzmann</i>	

Formal UML Modeling

Exploiting the Hierarchical Structure of Rule-Based Specifications for Decision Planning	2
<i>Artur Boronat, Roberto Bruni, Alberto Lluch Lafuente, Ugo Montanari, and Generoso Paolillo</i>	
Reactive Semantics for Distributed UML Activities	17
<i>Frank Alexander Kraemer and Peter Herrmann</i>	

Components and Architecture

Statistical Abstraction and Model-Checking of Large Heterogeneous Systems	32
<i>Ananda Basu, Saddek Bensalem, Marius Bozga, Benoît Caillaud, Benoît Delahaye, and Axel Legay</i>	
Formal Semantics and Analysis of Behavioral AADL Models in Real-Time Maude	47
<i>Peter Csaba Ölveczky, Artur Boronat, and José Meseguer</i>	
Testing Probabilistic Distributed Systems	63
<i>Robert M. Hierons and Manuel Núñez</i>	
Specification and Testing of E-Commerce Agents Described by Using UIOLTSS	78
<i>Juan José Pardo, Manuel Núñez, and M. Carmen Ruiz</i>	
Testing Attribute-Based Transactions in SOC	87
<i>Laura Bocchi and Emilio Tuosto</i>	

Joint DisCoTec Session

Grouping Nodes in Wireless Sensor Networks Using Coalitional Game Theory	95
<i>Fatemeh Kazemeyni, Einar Broch Johnsen, Olaf Owe, and Ilanko Balasingham</i>	

Timed Process Algebra

Forgetting the Time in Timed Process Algebra: Timeless Behaviour in a Timestamped World 110
Anton Wijs

Theory and Implementation of a Real-Time Extension to the π -Calculus 125
Ernesto Posse and Juergen Dingel

Timed and Hybrid Automata

Fuzzy-Timed Automata 140
F. Javier Crespo, Alberto de la Encina, and Luis Llana

Model Checking of Hybrid Systems Using Shallow Synchronization 155
Lei Bu, Alessandro Cimatti, Xuandong Li, Sergio Mover, and Stefano Tonetta

Program Logics and Analysis

Heap-Dependent Expressions in Separation Logic 170
Jan Smans, Bart Jacobs, and Frank Piessens

Static Type Analysis of Pattern Matching by Abstract Interpretation 186
Pietro Ferrara

Reasoning about Distributed Systems

On-the-Fly Trace Generation and Textual Trace Analysis and Their Applications to the Analysis of Cryptographic Protocols 201
Yongyuth Permpoontanalarp

On Efficient Models for Model Checking Message-Passing Distributed Protocols 216
Péter Bokor, Marco Serafini, and Neeraj Suri

Logics for Contravariant Simulations 224
Ignacio Fábregas, David de Frutos Escrig, and Miguel Palomino

Author Index 233