Formal Techniques for Distributed Objects, Components, and Systems

Alexey Gotsman, Ana Sokolova

▶ **To cite this version:**

Alexey Gotsman, Ana Sokolova. Formal Techniques for Distributed Objects, Components, and Systems: 40th IFIP WG 6.1 International Conference, FORTE 2020, Held as Part of the 15th International Federated Conference on Distributed Computing Techniques, DisCoTec 2020, Valletta, Malta, June 15–19, 2020, Proceedings. Springer International Publishing, LNCS-12136, 2020, Lecture Notes in Computer Science, 978-3-030-50085-6. 10.1007/978-3-030-50086-3 . hal-03283230

HAL Id: hal-03283230

https://inria.hal.science/hal-03283230

Submitted on 9 Jul 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Lecture Notes in Computer Science 12136

Founding Editors

Gerhard Goos
Karlsruhe Institute of Technology, Karlsruhe, Germany
Juris Hartmanis
Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino
Purdue University, West Lafayette, IN, USA
Wen Gao
Peking University, Beijing, China
Bernhard Steffen
TU Dortmund University, Dortmund, Germany
Gerhard Woeginger
RWTH Aachen, Aachen, Germany
Moti Yung
Columbia University, New York, NY, USA

More information about this series at http://www.springer.com/series/7408

Alexey Gotsman · Ana Sokolova (Eds.)

Formal Techniques for Distributed Objects, Components, and Systems

40th IFIP WG 6.1 International Conference, FORTE 2020
Held as Part of the 15th International Federated Conference on Distributed Computing Techniques, DisCoTec 2020
Valletta, Malta, June 15–19, 2020
Proceedings

Springer

Editors
Alexey Gotsman
IMDEA Software Institute
Pozuelo de Alarcón, Spain

Ana Sokolova
University of Salzburg
Salzburg, Austria

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-50085-6 ISBN 978-3-030-50086-3 (eBook)
https://doi.org/10.1007/978-3-030-50086-3

LNCS Sublibrary: SL2 – Programming and Software Engineering

© IFIP International Federation for Information Processing 2020
The chapter "Conformance-Based Doping Detection for Cyber-Physical Systems" is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/). For further details see license information in the chapter.
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.
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.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

The 15th International Federated Conference on Distributed Computing Techniques (DisCoTec 2020) took place during June 15–19, 2020. It was organized by the Department of Computer Science at the University of Malta, but was held online due to the abnormal circumstances worldwide affecting physical travel.

The DisCoTec series is one of the major events sponsored by the International Federation for Information Processing (IFIP). It comprises three conferences:

- The IFIP WG 6.1 22nd International Conference on Coordination Models and Languages (COORDINATION 2020)
- The IFIP WG 6.1 20th International Conference on Distributed Applications and Interoperable Systems (DAIS 2020)
- The IFIP WG 6.1 40th International Conference on Formal Techniques for Distributed Objects, Components and Systems (FORTE 2020)

Together, these conferences cover a broad spectrum of distributed computing subjects, ranging from theoretical foundations and formal description techniques to systems research issues. As is customary, the event also included several plenary sessions in addition to the individual sessions of each conference, that gathered attendants from the three conferences. These included joint invited speaker sessions and a joint session for the best papers from the respective three conferences.

Associated with the federated event, two satellite events took place:

- The 13th International Workshop on Interaction and Concurrency Experience (ICE 2020)
- The First International Workshop on Foundations of Consensus and Distributed Ledgers (FOCODILE 2020)

I would like to thank the Program Committee chairs of the different events for their help and cooperation during the preparation of the conference, and the Steering Committee and Advisory Boards of DisCoTec and their conferences for their guidance and support. The organization of DisCoTec 2020 was only possible thanks to the dedicated work of the Organizing Committee, including Davide Basile and Francisco "Kiko" Fernández Reyes (publicity chairs), Antonis Achilleos, Duncan Paul Attard, and Ornela Dardha (workshop chairs), Lucienne Bugeja (logistics and finances), as well as all the students and colleagues who volunteered their time to help. Finally, I would like to thank IFIP WG 6.1 for sponsoring this event, Springer's *Lecture Notes in Computer Science* team for their support and sponsorship, EasyChair for providing the reviewing framework, and the University of Malta for providing the support and infrastructure to host the event.

June 2020 Adrian Francalanza

Preface

This volume contains the papers presented at the 40th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2020), held as one of three main conferences of the 15th International Federated Conference on Distributed Computing Techniques (DisCoTec 2020), during June 15–19, 2020, online due to the coronavirus pandemic.

FORTE is a well-established forum for fundamental research on theory, models, tools, and applications for distributed systems, with special interest in:

- Software quality, reliability, availability, and safety
- Security, privacy, and trust in distributed and/or communicating systems
- Service-oriented, ubiquitous, and cloud computing systems
- Component- and model-based design
- Object technology, modularity, and software adaptation
- Self-stabilization and self-healing/organizing
- Verification, validation, formal analysis, and testing of the above

The Program Committee received a total of 25 submissions, written by authors from 18 different countries. Of these, 11 papers were selected for inclusion in the scientific program. Each submission was reviewed by at least three Program Committee members with the help of 10 external reviewers in selected cases. The selection of accepted submissions was based on electronic discussions via the EasyChair conference management system.

As program chairs, we actively contributed to the selection of the keynote speakers of DisCoTec 2020 (which due to the conference being held online are not all confirmed at the time of writing).

This year DisCoTec also includes a Tutorial Day of six invited tutorials. This volume includes the following tutorial papers:

- Parameterised Verification with Byzantine Model Checker
- Typechecking Java Protocols with [St] Mungo

We wish to thank all the authors of submitted papers, all the members of the Program Committee for their thorough evaluations of the submissions, and the external reviewers who assisted the evaluation process. We are also indebted to the Steering Committee of FORTE for their advice and suggestions. Last but not least, we thank the DisCoTec general chair, Adrian Francalanza, and his organization team for their hard, effective work in providing an excellent environment for FORTE 2020 and all other conferences and workshops, despite of the pandemic troubles.

June 2020

Alexey Gotsman
Ana Sokolova

Organization

Program Committee

Marco Bernardo	University of Urbino, Italy
Nathalie Bertrand	Inria, France
Marco Carbone	IT University of Copenhagen, Denmark
Andrea Corradini	University of Pisa, Italy
Cezara Dragoi	Inria and ENS, France
Constantin Enea	Université Paris-Diderot, France
Javier Esparza	TU Munich, Germany
Alexey Gotsman	IMDEA Software Institute, Spain
Philipp Haller	KTH, Sweden
Bart Jacobs	KU Leuven, Belgium
Radha Jagadeesan	DePaul University, USA
Akash Lal	Microsoft Research, India
Mohsen Lesani	University of California, Riverside, USA
Stephan Merz	Inria, France
Antoine Miné	Sorbonne Université, France
Koko Muroya	RIMS Kyoto University, Japan
Catuscia Palamidessi	Inria and LIX, France
Kirstin Peters	TU Darmstadt, Germany
Tatjana Petrov	University of Konstanz, Germany
Vincent Rahli	University of Birmingham, UK
Ana Sokolova	University of Salzburg, Austria
Tyler Sorensen	Princeton University and University of California, Santa Cruz, USA
Marielle Stoelinga	TU Twente, The Netherlands
Sara Tucci-Piergiovanni	CEA LIST, France
Nikos Tzevelekos	Queen Mary University of London, UK
Viktor Vafeiadis	MPI-SWS, Germany
Josef Widder	TU Vienna and Interchain, Austria

Additional Reviewers

Pranav Ashok
Stephanie Delaune
Maribel Fernandez
Ernst Moritz Hahn
Yu-Yang Lin
Marco Romanelli
Ocan Sankur
Alceste Scalas
Jacopo Soldani
Stefano Tognazzi

Contents

Full Papers

Strategy Synthesis for Autonomous Driving in a Moving Block Railway System with Uppaal Stratego 3
Davide Basile, Maurice H. ter Beek, and Axel Legay

Towards Bridging Time and Causal Reversibility 22
Marco Bernardo and Claudio Antares Mezzina

Defining and Verifying Durable Opacity: Correctness for Persistent Software Transactional Memory 39
Eleni Bila, Simon Doherty, Brijesh Dongol, John Derrick, Gerhard Schellhorn, and Heike Wehrheim

Conformance-Based Doping Detection for Cyber-Physical Systems 59
Rayna Dimitrova, Maciej Gazda, Mohammad Reza Mousavi, Sebastian Biewer, and Holger Hermanns

On Implementable Timed Automata 78
Sergio Feo-Arenis, Milan Vujinović, and Bernd Westphal

Deep Statistical Model Checking. 96
Timo P. Gros, Holger Hermanns, Jörg Hoffmann, Michaela Klauck, and Marcel Steinmetz

Trace Equivalence and Epistemic Logic to Express Security Properties 115
Kiraku Minami

Derivation of Heard-of Predicates from Elementary Behavioral Patterns 133
Adam Shimi, Aurélie Hurault, and Philippe Queinnec

Probabilistic Timed Automata with One Clock and Initialised Clock-Dependent Probabilities 150
Jeremy Sproston

A Formal Framework for Consent Management 169
Shukun Tokas and Olaf Owe

Tutorials

Tutorial: Parameterized Verification with Byzantine Model Checker 189
Igor Konnov, Marijana Lazić, Ilina Stoilkovska, and Josef Widder

Typechecking Java Protocols with [St]Mungo 208
A. Laura Voinea, Ornela Dardha, and Simon J. Gay

Short Paper

Towards a Hybrid Verification Methodology for Communication Protocols (Short Paper) 227
Christian Bartolo Burlò, Adrian Francalanza, and Alceste Scalas

Author Index 237