

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, 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


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


Ezio Bartocci · Yliès Falcone (Eds.)

Lectures on Runtime Verification

Introductory and Advanced Topics

Editors

Ezio Bartocci 
TU Wien
Vienna
Austria

Yliès Falcone 
Université Grenoble Alpes, Inria,
Laboratoire d'Informatique de Grenoble
Grenoble
France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-75631-8 ISBN 978-3-319-75632-5 (eBook)
<https://doi.org/10.1007/978-3-319-75632-5>

Library of Congress Control Number: 2018933096

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer International Publishing AG, part of Springer Nature 2018

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.

Cover illustration: Automata-based and rewrite-based runtime verification. Created by Yliès Falcone. Used with permission.

Printed on acid-free paper

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



Preface

Runtime verification (RV) is a lightweight, yet rigorous, formal method for the monitoring and analysis of the runtime behavior of software and hardware systems. RV complements classic exhaustive verification techniques (such as model checking and theorem proving) with a more practical approach that analyzes a single execution trace of a system. At the price of a limited execution coverage, RV can give very precise information on the runtime behavior of the monitored system. RV is now widely employed in both academia and industry both before system deployment, for testing, verification, and debugging purposes, and after deployment to ensure reliability, safety, robustness, and security.

The interest in this field of research has grown since 2001 when the first international workshop on RV was organized. This venue has occurred each year since then, becoming a conference in 2010. In 2014, we initiated the International Competition on Runtime Verification (CRV) with the goal of fostering the comparison and evaluation of software runtime verification tools. In the same year, an European scientific network for the Cooperation in Science and Technology (COST) on “Runtime Verification Beyond Monitoring (ARVI)” was approved and funded within the European framework program Horizon 2020. ARVI currently includes the participation of scientists from 26 European countries and Australia. In 2016, together with other partners of ARVI, we also started to organize the first of a series of schools on RV. Our aim is to train researchers from academia and industry introducing them first to the basic concepts and then to the advanced topics in this exciting research area.

The idea of this volume originated from the need to have a book for students to support their training with several tutorials on different aspects of RV. The volume has been organized in seven chapters and the topics covered include an introduction on runtime verification, dynamic analysis of concurrency errors, monitoring events that carry data, runtime error reaction and prevention, monitoring of cyber-physical systems, runtime verification for decentralized and distributed systems, and an industrial application of runtime verification techniques in financial transaction systems.

Each paper has been reviewed by two reviewers and the editors. The editors would like to thank the reviewers: Thomas Arts, Ebru Aydin Gol, Andreas Bauer, Christian Colombo, Raymond Hu, Jan Kofron, Zhaodan Kong, Laura Nenzi, Gordon Pace, Rahul Purandare, Giles Reger, Oleg Sokolsky, Shmuel Ur.

November 2017

Ezio Bartocci
Yliès Falcone

Contents

Introduction to Runtime Verification	1
<i>Ezio Bartocci, Yliès Falcone, Adrian Francalanza, and Giles Reger</i>	
Discovering Concurrency Errors	34
<i>João M. Lourenço, Jan Fiedor, Bohuslav Křena, and Tomáš Vojnar</i>	
Monitoring Events that Carry Data	61
<i>Klaus Havelund, Giles Reger, Daniel Thoma, and Eugen Zălinescu</i>	
Runtime Failure Prevention and Reaction	103
<i>Yliès Falcone, Leonardo Mariani, Antoine Rollet, and Saikat Saha</i>	
Specification-Based Monitoring of Cyber-Physical Systems: A Survey on Theory, Tools and Applications	135
<i>Ezio Bartocci, Jyotirmoy Deshmukh, Alexandre Donzé, Georgios Fainekos, Oded Maler, Dejan Ničković, and Sriram Sankaranarayanan</i>	
Runtime Verification for Decentralised and Distributed Systems	176
<i>Adrian Francalanza, Jorge A. Pérez, and César Sánchez</i>	
Industrial Experiences with Runtime Verification of Financial Transaction Systems: Lessons Learnt and Standing Challenges	211
<i>Christian Colombo and Gordon J. Pace</i>	
Author Index	233