

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

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

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Farn Wang (Ed.)

Formal Techniques for Networked and Distributed Systems – FORTE 2005

25th IFIP WG 6.1 International Conference
Taipei, Taiwan, October 2-5, 2005
Proceedings



Springer

Volume Editor

Farn Wang
National Taiwan University
Department of Electrical Engineering
1, Sec. 4, Roosevelt Rd., Taipei, Taiwan 106, ROC
E-mail: farn@cc.ee.ntu.edu.tw

Library of Congress Control Number: 2005932939

CR Subject Classification (1998): C.2.4, D.2.2, C.2, D.2.4-5, D.2, F.3, D.4

ISSN	0302-9743
ISBN-10	3-540-29189-X Springer Berlin Heidelberg New York
ISBN-13	978-3-540-29189-3 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 is a part of Springer Science+Business Media

springeronline.com

© 2005 IFIP International Federation for Information Processing, Hofstrasse 3, 2361 Laxenburg, Austria
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11562436 06/3142 5 4 3 2 1 0

Preface

FORTE (Formal Techniques for Networked and Distributed Systems) 2005 was sponsored by Working Group 6.1, Technical Committee 6 (TC6) of the International Federation for Information Processing (IFIP). The conference series started in 1981 under the name PSTV (Protocol Specification, Testing, and Verification). In 1988, a second series under the name FORTE was started. Both series merged to FORTE/PSTV in 1996. The conference name was changed to FORTE in 2001. During its 24-year history, many important contributions have been reported in the conference series. The last five meetings of FORTE were held in Pisa (Italy), Cheju Island (Korea), Houston (USA), Berlin (Germany), and Madrid (Spain).

The 25th FORTE was held from Sunday to Wednesday, October 2–5, 2005 on the beautiful campus of the National Taiwan University (NTU), Taipei, Taiwan, ROC. The scope covered formal description techniques (MSC, UML, Use cases, ...), semantic foundations, model-checking, SAT-based techniques, process algebras, abstractions, protocol testing, protocol verification, network synthesis, security system analysis, network robustness, embedded systems, communication protocols, and several promising new techniques. In total, we received 88 submissions and accepted 33 regular papers and 6 short papers. All submissions received three reviews. The final program also included 3 keynote speeches, respectively by Prof. Amir Pnueli, Dr. Constance Heitmeyer, and Prof. Teruo Higashino, and 3 tutorials, respectively by Prof. Rance Cleaveland, Dr. Constance Heitmeyer, and Prof. Teruo Higashino. The proceedings also include the text of the keynote speeches. In addition, there were social events, including a reception, a banquet, and an excursion.

FORTE 2005 was co-located with ATVA (Automated Technology for Verification and Analysis) 2005 with a two-day overlap. Prof. Amir Pnueli was the joint keynote speaker. The participants of FORTE 2005 and ATVA 2005 also enjoyed a joint banquet/reception and a joint excursion.

FORTE 2005 was organized under the auspices of IFIP TC 6 by the Department of Electrical Engineering, NTU. It was generously supported by the National Science Council, Taiwan, ROC; the Ministry of Education, Taiwan, ROC; the Institute of Information Science, Academia Sinica, Taiwan, ROC; the Center for Information and Electronic Technologies, NTU; the Graduate Institute of Communication Engineering, NTU; and the Computer and Information Networking Center, NTU.

We would like to thank the Steering Committee members of FORTE for all their suggestions, guidance, and assistance. We also owe a lot to all the Program Committee members and reviewers for their effort in compiling rigorous reviews. Prof. Manuel Nunez deserves special thanks for unselfishly passing on his experience as organizer of FORTE 2004. We would also like to thank Prof. Jin-Fu Chang, Prof. Chuan Yi Tang, Prof. Wanjiun Liao, Prof. Sy-Yen Kuo, Prof. Ming-Syan Chen, Dr. Churn-Jung Liao, and Dr. Ching-Tarn Hsieh for their assistance. Finally special thanks go to Ms. Lih-Chung Lin, Ms. Tz-Hua Chen, Mr. Rong-Shiung Wu, and Mr. Zawa Chu for their energetic and careful planning in the local arrangements and webpage management.

Organization

Steering Committee

Gregor v. Bochmann (Canada) Tommaso Bolognesi (Italy)
John Derrick (UK) Guy Leduc (Belgium)
Ken Turner (UK)

General Chair

Jin-Fu Chang (Taiwan)

Program Chair

Farn Wang (Taiwan)

Program Committee

Gregor v. Bochmann (Canada)	Tommaso Bolognesi (Italy)
Mario Bravetti (Italy)	Ana Cavalli (France)
Jin Song Dong (Singapore)	Khaled El-Fakih (UAE)
Colin Fidge (Australia)	David de Frutos-Escrig (Spain)
Reinhard Gotzhein (Germany)	Constance Heitmeyer (USA)
Holger Hermanns (Germany)	Teruo Higashino (Japan)
Dieter Hogrefe (Germany)	Gerald J. Holzmann (USA)
Ching-Tarng Hsieh (Taiwan)	Claude Jard (France)
Myungchul Kim (Korea)	Hartmut Koenig (Germany)
David Lee (USA)	Chin-Laung Lei (Taiwan)
Wanjiun Liao (Taiwan)	Churn-Jung Liao (Taiwan)
Huimin Lin (China)	Nancy Lynch (USA)
Elie Najm (France)	Manuel Nunez (Spain)
Kenji Suzuki (Japan)	Alex Petrenko (Canada)
Ken Turner (UK)	Chuan Yi Tang (Taiwan)
Farn Wang (Taiwan)	Hasan Ural (Canada)
Tomohiro Yoneda (Japan)	Hsu-Chun Yen (Taiwan)

Additional Reviewers

Akira Idoue Alessandro Fantechi Alex Groce
Arnaud Dury Baptiste Alcalde Bassel Daou and Daniel Amyot

Carlos Gregorio -Rodríguez	Carron Shankland	Clara Segura
Claudio Guidi	Claudio Sacerdoti Coen	Constantin Werner
Dario VIEIRA	Dong Wang	Dongluo Chen
Elisangela Rodrigues-Vieira	Fabio Martinelli	Fida Dankar
Guoqiang Shu	Hesham Hallal	Hidetoshi Yokota
Hong PAN	Ingmar Fliege	Ismael Rodriguez
Jalal Kawash	Jiale Huo	Jian Liu
Jinzhi Xia	Joachim Thees	Jun Lei
Jun Sun	Keqin Li	Li Jiao
Lijun Zhang	Luis Llana	Manuel Mazzara
Marco Zibull	Maurice ter Beek	Mercedes G. Merayo
Michael Ebner	Miguel Palomino	Natalia Lopez
Nicola Tonellotto	O. Marroquin-Alonso	Ping Hao
Rene Soltwisch	Robert Clark	Roberto Gorrieri
Roberto Lucchi	Rüdiger Grammes	Rui Xue
Salvatore Rinzivillo	Sam Owre	Savi Maharaj
Sebastian Schmerl	Serge Boroday	Soonuk Seol
Stefania Gnesi	Stephan Schröder	Stephane Maag
Sungwon Kang	Takashi Kitamura	Thomas Kuhn
Tomohiko Ogishi	Toru Hasegawa	Wenhui Zhang
Xinxin Liu	Yolanda Ortega-Mallén	Yuan Fang Li
Yutaka Miyake		

Sponsoring Institutions

National Science Council, Taiwan, ROC

Ministry of Education, Taiwan, ROC

Institute of Information Science, Academia Sinica, Taiwan, ROC

Center for Information and Electronic Technologies, NTU

Graduate Institute of Communication Engineering, NTU

Computer and Information Networking Center, NTU

Table of Contents

KEYNOTE SPEECHES

Ranking Abstraction as Companion to Predicate Abstraction <i>Ittai Balaban, Amir Pnueli, Lenore D. Zuck</i>	1
Developing High Quality Software with Formal Methods: What Else Is Needed? <i>Constance Heitmeyer</i>	13
A Testing Architecture for Designing High-Reliable MANET Protocols <i>Teruo Higashino, Hirozumi Yamaguchi</i>	20

REGULAR PAPERS

A Composition Operator for Systems with Active and Passive Actions <i>Stefan Strubbe, Rom Langerak</i>	24
A Formal Semantics of UML StateCharts by Means of Timed Petri Nets <i>Youcef Hammal</i>	38
A Hierarchy of Implementable MSC Languages <i>Benedikt Bollig, Martin Leucker</i>	53
Combining Static Analysis and Model Checking for Systems Employing Commutative Functions <i>A. Prasad Sistla, Min Zhou</i>	68
Fast Generic Model-Checking for Data-Based Systems <i>Dezhuang Zhang, Rance Cleaveland</i>	83
Logic and Model Checking for Hidden Markov Models <i>Lijun Zhang, Holger Hermanns, David N. Jansen</i>	98
Proving $\forall\mu$ -Calculus Properties with SAT-Based Model Checking <i>Bow-Yaw Wang</i>	113
Ad Hoc Routing Protocol Verification Through Broadcast Abstraction <i>Oskar Wibling, Joachim Parrow, Arnold Pears</i>	128

Discovering Chatter and Incompleteness in the Datagram Congestion Control Protocol	
<i>Somsak Vanit-Anunchai, Jonathan Billington, Tul Kongprakaiwoot</i>	143
Thread Allocation Protocols for Distributed Real-Time and Embedded Systems	
<i>César Sánchez, Henny B. Sipma, Venkita Subramonian, Christopher Gill, Zohar Manna</i>	159
A Petri Net View of Mobility	
<i>Charles A. Lakos</i>	174
Modular Verification of Petri Nets Properties: A Structure-Based Approach	
<i>Kais Klai, Serge Haddad, Jean-Michel Illié</i>	189
An Improved Conformance Testing Method	
<i>Rita Dorofeeva, Khaled El-Fakih, Nina Yevtushenko</i>	204
Resolving Observability Problems in Distributed Test Architectures	
<i>J. Chen, R.M. Hierons, H. Ural</i>	219
Automatic Generation of Conflict-Free IPsec Policies	
<i>Chi-Lan Chang, Yun-Peng Chiu, Chin-Laung Lei</i>	233
A Framework Based Approach for Formal Modeling and Analysis of Multi-level Attacks in Computer Networks	
<i>Gerrit Rothmaier, Heiko Krumm</i>	247
Model Checking for Timed Statecharts	
<i>Junyan Qian, Baowen Xu</i>	261
Abstraction-Guided Model Checking Using Symbolic IDA* And Heuristic Synthesis	
<i>Kairong Qian, Albert Nymeyer, Steven Susanto</i>	275
Modeling and Verification of Safety-Critical Systems Using Safecharts	
<i>Pao-Ann Hsiung, Yen-Hung Lin</i>	290
Structure Preserving Data Abstractions for Statecharts	
<i>Steffen Helke, Florian Kammüller</i>	305
Amortised Bisimulations	
<i>Astrid Kiehn, S. Arun-Kumar</i>	320
Proof Methodologies for Behavioural Equivalence in DPI	
<i>Alberto Ciaffaglione, Matthew Hennessy, Julian Rathke</i>	335

Deriving Non-determinism from Conjunction and Disjunction <i>Naijun Zhan, Mila Majster-Cederbaum</i>	351
Abstract Operational Semantics for Use Case Maps <i>Jameleddine Hassine, Juergen Rilling, Rachida Dssouli</i>	366
ArchiTRIO: A UML-Compatible Language for Architectural Description and Its Formal Semantics <i>Matteo Pradella, Matteo Rossi, Dino Mandrioli</i>	381
Submodule Construction for Extended State Machine Models <i>Bassel Daou, Gregor V. Bochmann</i>	396
Towards Synchronizing Linear Collaborative Objects with Operational Transformation <i>Abdessamad Imine, Pascal Molli, Gérald Oster, Michaël Rusinowitch</i>	411
Designing Efficient Fail-Safe Multitolerant Systems <i>Arshad Jhumka, Neeraj Suri</i>	428
Hierarchical Decision Diagrams to Exploit Model Structure <i>Jean-Michel Couvreur, Yann Thierry-Mieg</i>	443
Computing Subgraph Probability of Random Geometric Graphs: Quantitative Analyses of Wireless Ad Hoc Networks <i>Chang Wu Yu, Li-Hsing Yen</i>	458
Formalising Web Services <i>Kenneth J. Turner</i>	473
From Automata Networks to HMSCs: A Reverse Model Engineering Perspective <i>Thomas Chatain, Loïc Hélouët, Claude Jard</i>	489
Properties as Processes: Their Specification and Verification <i>Joel Kelso, George Milne</i>	503

SHORT PAPERS

Epoch Distance of the Random Waypoint Model in Mobile Ad Hoc Networks <i>Yueh-Ting Wu, Wanjiun Liao, Cheng-Lin Tsao</i>	518
Automatic Partitioner for Behavior Level Distributed Logic Simulation <i>Kai-Hui Chang, Jeh-Yen Kang, Han-Wei Wang, Wei-Ting Tu, Yi-Jong Yeh, Sy-Yen Kuo</i>	525

Expressive Completeness of an Event-Pattern Reactive Programming Language	
<i>César Sánchez, Matteo Slanina, Henny B. Sipma, Zohar Manna</i>	529
Formalizing Interoperability Testing: Quiescence Management and Test Generation	
<i>Alexandra Desmoulin, César Viho</i>	533
Formal Description of Mobile IPv6 Protocol	
<i>Yujun Zhang, Zhongcheng Li</i>	538
Incremental Modeling Under Large-Scale Distributed Interaction	
<i>Horst F. Wedde, Arnim Wedig, Anca Lazarescu, Ralf Paaschen, Elisei Rotaru</i>	542
The Inductive Approach to Strand Space	
<i>Yongjian Li</i>	547
Compositional Modelling and Verification of IPv6 Mobility	
<i>Peng Wu, Dongmei Zhang</i>	553
Author Index	557