

# FORMAL METHODS FOR DISTRIBUTED SYSTEM DEVELOPMENT

**FORTE / PSTV 2000**

*IFIP TC6 WG6.1 Joint International Conference on  
Formal Description Techniques for Distributed Systems  
and Communication Protocols (FORTE XIII) and  
Protocol Specification, Testing and Verification (PSTV XX)  
October 10-13, 2000, Pisa, Italy*

*Edited by*

**Tommaso Bolognesi**

*Consiglio Nazionale delle Ricerche (CNR)  
Istituto di Elaborazione dell'Informazione (IEI)  
Italy*

**Diego Latella**

*Consiglio Nazionale delle Ricerche (CNR)  
Istituto CNUCE  
Italy*



---

KLUWER ACADEMIC PUBLISHERS

BOSTON / DORDRECHT / LONDON

---

**Distributors for North, Central and South America:**

Kluwer Academic Publishers  
101 Philip Drive  
Assinippi Park  
Norwell, Massachusetts 02061 USA  
Telephone (781) 871-6600  
Fax (781) 871-6528  
E-Mail <kluwer@wkap.com>

**Distributors for all other countries:**

Kluwer Academic Publishers Group  
Distribution Centre  
Post Office Box 322  
3300 AH Dordrecht, THE NETHERLANDS  
Telephone 31 78 6392 392  
Fax 31 78 6546 474  
E-Mail <services@wkap.nl>



Electronic Services <<http://www.wkap.nl>>

---

**Library of Congress Cataloging-in-Publication Data**

IFIP TC6 WG6.1 Joint International Conference on Formal Description Techniques for Distributed Systems and Communication Protocols and Protocol Specification, Testing and Verification (2000 : Pisa, Italy)

Formal methods for distributed system development : October 10-13, 2000, Pisa, Italy / FORTE/PSTV 2000, IFIP TC6 WG6.1 Joint International Conference on Formal Description Techniques for Distributed Systems and Communication Protocols and Protocol Specification, Testing and Verification ; edited by Tommaso Bolognesi, Diego Latella.

p. cm. — (IFIP ; 55)

Includes bibliographical references.

ISBN 0-7923-7968-3 (alk. paper)

1. Electronic data processing—Distributed processing—Congresses. 2. Formal methods (Computer science)—Congresses. I. Bolognesi, Tommaso. II. Latella, Diego. III. Title. IV. International Federation for Information Processing (Series) ; 55.

QA76.9.D5 I33845 2000

004'.36—dc21

00-061057

---

Copyright © 2000 by International Federation for Information Processing.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, mechanical, photo-copying, recording, or otherwise, without the prior written permission of the publisher, Kluwer Academic Publishers, 101 Philip Drive, Assinippi Park, Norwell, Massachusetts 02061.

*Printed on acid-free paper.*

Printed in the United States of America.

## Contents

Contributors	ix
Preface	xi
Programme Committee and Referees	xiii
Acknowledgements	xv

### Part One

#### VERIFICATION AND THEOREM PROVING

1. Formal Verification of the TTP Group Membership Algorithm <i>H. Pfeifer</i>	3
2. Verification of a Sliding Window Protocol Using IOA and MONA <i>M. A. Smith, N. Klarlund</i>	19
3. A Priori Verification of Reactive Systems <i>M. Majster-Cederbaum, F. Salger, M. Sorea</i>	35

### Part Two

#### TEST GENERATION

4. From Rule-based to Automata-based Testing <i>K. Etessami, M. Yannakakis</i>	53
5. Integrated System Interoperability Testing with Applications to VOIP <i>N. Griffeth, R. Hao, D. Lee, R. K. Sinha</i>	69
6. On Test Derivation from Partial Specifications <i>A. Petrenko, N. Yevtushenko</i>	85

### **Part Three**

#### **MODEL CHECKING - THEORY**

- |    |   |     |
|----|---|-----|
| 7. | Compositionality for Improving Model Checking<br><i>A. Santone</i>                                | 105 |
| 8. | A Model Checking Method for Partially Symmetric Systems<br><i>S. Haddad, J.-M. Ilié, K. Ajami</i> | 121 |

### **Part Four**

#### **MODEL CHECKING - APPLICATIONS**

- |     |   |     |
|-----|---|-----|
| 9.  | Specification and Verification of Message Sequence Charts<br><i>D. Peled</i>  | 139 |
| 10. | A State-Exploration Technique for Spi-Calculus<br>Testing Equivalence Verification<br><i>L. Durante, R. Sisto, A. Valenzano</i> | 155 |
| 11. | Verification of Consistency Protocols via Infinite-State<br>Symbolic Model Checking<br><i>G. Delzanno</i>                       | 171 |

### **Part Five**

#### **MULTICAST PROTOCOL ANALYSIS AND SIMULATION**

- |     |  |     |
|-----|--|-----|
| 12. | Systematic Performance Evaluation of Multipoint Protocols<br><i>A. Helmy, S. Gupta, D. Estrin, A. Cerpa, Y. Yu</i>                 | 189 |
| 13. | Simulating Multicast Transport Protocols in Estelle<br><i>J. Templemore-Finlayson, E. Borcoci</i>                                  | 205 |
| 14. | Generation of Realistic Signalling Traffic in an ISDN<br>Load Test System using SDL User Models<br><i>T. Steinert, G. Roessler</i> | 219 |

### **Part Six**

#### **EXHAUSTIVE AND PROBABILISTIC TESTING**

- |     |  |     |
|-----|--|-----|
| 15. | Satisfaction up to Liveness<br><i>U. Ultes-Nitsche</i> | 237 |
|-----|--|-----|

16. Testing IP Routing Protocols - From Probabilistic Algorithms to a Software Tool 249  
*R. Hao, D. Lee, R. K. Sinha, D. Vlah*

**Part Seven**

**HARDWARE SPECIFICATION, IMPLEMENTATION AND TESTING**

17. Verifying and Testing Asynchronous Circuits using LOTOS 267  
*J. He, K. J. Turner*
18. Hardware implementation of Concurrent Periodic EFSM's 285  
*H. Katagiri, M. Kirimura, K. Yasumoto, T. Higashino, K. Taniguchi*
19. Modeling Distributed Embedded Systems in Multiclock ESTEREL 301  
*B. Rajan, R. K. Shyamasundar*

**Part Eight**

**FORMAL SEMANTICS**

20. Compact Net Semantics for Process Algebras 319  
*M. Bernardo, M. Ribaud, N. Busi*
21. A Concise Compositional Statecharts Semantics Definition 335  
*M. von der Beeck*
22. Implementing CCS in Maude 351  
*A. Verdejo, N. Martí-Oliet*

**Part Nine**

**INVITED PAPERS ON VERIFICATION AND SECURITY**

23. From Refutation to Verification 369  
*J. Rushby*
24. Process Algebraic Analysis of Cryptographic Protocols 375  
*M. Boreale, R. De Nicola, R. Pugliese*
25. A Logic of Belief and a Model Checking Algorithm for Security Protocols 393  
*M. Benerecetti, F. Giunchiglia, M. Panti, L. Spalazzi*

## Preface

The 20<sup>th</sup> anniversary of the IFIP WG6.1 Joint International Conference on Formal Methods for Distributed Systems and Communication Protocols (FORTE XIII / PSTV XX) was celebrated by the year 2000 edition of the Conference, which was held for the first time in Italy, at Pisa, October 10-13, 2000. In devising the subtitle for this special edition -- 'Formal Methods -- Implementation Under Test' -- we wanted to convey two main concepts that, in our opinion, are reflected in the contents of this book. First, the early, pioneering phases in the development of Formal Methods (FM's), with their conflicts between evangelistic and agnostic attitudes, with their over-optimistic applications to toy examples and over-skeptical views about scalability to industrial cases, with their misconceptions and myths..., all this is essentially over. Many FM's have successfully reached their maturity, having been 'implemented' into concrete development practice: a number of papers in this book report about successful experiences in specifying and verifying real distributed systems and protocols. Second, one of the several myths about FM's -- the fact that their adoption would eventually eliminate the need for testing -- is still quite far from becoming a reality, and, again, this book indicates that testing theory and applications are still remarkably healthy.

A total of 63 papers have been submitted to FORTE/PSTV 2000, out of which the Programme Committee has selected 22 for presentation at the Conference and inclusion in the Proceedings. The central themes of this book are the theory and practice of distributed system Verification (with Model Checking playing a predominant role), and Testing. Several papers deal with the analysis of communication protocols, and some of them address, in particular, multicast protocols. Other papers deal with the

specification, implementation and testing of hardware systems. The issue of formal semantics is also covered, but to a lesser extent than in past editions of the Conference, as a further indication of the shift of emphasis from the definition to the application of FM's. Three internationally recognized speakers, namely Rocco De Nicola, Fausto Giunchiglia, and John Rushby, have provided invited contributions on Verification and on Security protocols: these are collected in the last part of the book.

The Conference has been complemented by two tutorial/advanced seminar tracks including a total of six presentations:

- E. Allen Emerson: Model Checking.
- Jan Tretmans: Specification based testing with formal methods -- from theory via tools to applications.
- Marta Kwiatkowska: Modelling and verification of probabilistic real time systems using probabilistic timed automata.
- Hartmut Koenig, Peter Langendoerfer: Automated Derivation of Efficient Implementations from Formal Protocol Specifications.
- R. Gotzhein, E. Börger, A. Prinz: Abstract State Machines and their Applications.
- C. Petitpierre: Bridging the Gap Between Formal Methods and the Implementation Process.

Finally, a multidisciplinary Satellite Workshop -- 'Formal Methods Elsewhere' -- was held on October 10, devoted to applications of FM's to areas other than communication protocols and distributed systems, such as physics, chemistry, biology, social sciences, arts and humanities, music. After two decades, FM's are perhaps ready to spread out of their native territory and, at the turn of the millenium, invade new exciting areas of research, for a wider exploitation of the huge intellectual investment behind their definition.

*Tommaso Bolognesi*  
*Diego Latella*