Manuel Núñez Zakaria Maamar
Fernando L. Pelayo Key Pousttchi
Fernando Rubio (Eds.)

Applying Formal Methods: Testing, Performance, and M/E-Commerce

LNCS 3236

FORTE 2004 Workshops The FormEMC, EPEW, ITM
Toledo, Spain, October 2004
Proceedings

Springer

Manuel Núñez Zakaria Maamar
Fernando L. Pelayo Key Pousttchi
Fernando Rubio (Eds.)

Applying Formal Methods: Testing, Performance, and M/E-Commerce

FORTE 2004 Workshops The FormEMC, EPEW, ITM
Toledo, Spain, October 1-2, 2004
Proceedings

Springer

Volume Editors

Manuel Núñez
Universidad Complutense de Madrid
Departamento de Sistemas Informática y Programacion
E-mail: mn@sip.ucm.es

Zakaria Maamar
Zayed University
College of Information Systems
E-mail: zakaria.maamar@zu.ac.ae

Fernando L. Pelayo
Universidad de Castilla-La Mancha
Departamento de Informatica
E-mail: fpelayo@info-ab.uclm.es

Key Pousttchi
University of Augsburg
Business Informatics and Systems Engineering
E-mail: key.pousttchi@wiwi.uni-augsburg.de

Fernando Rubio
Universidad Complutense de Madrid
Dept. Sistemas Informáticos y Programación
E-mail: fernando@sip.ucm.es

Library of Congress Control Number: 200112846

CR Subject Classification (1998): D.2, C.2.4, F.3, D.4, C.4, K.4.4, C.2

ISSN 0302-9743
ISBN 3-540-23169-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by DA-TeX Gerd Blumenstein
Printed on acid-free paper SPIN: 11324263 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3236

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Preface

This volume contains the refereed proceedings of the first edition of three workshops colocated with the International Conference on Formal Techniques for Networked and Distributed Systems (FORTE). The workshops took place in Toledo (Spain) on the 1st and 2nd of October of 2004, and they dealt with different topics related to the application of formal methods. The names of the workshops were the following:

- TheFormEMC: 1st International Workshop on Theory Building and Formal Methods in Electronic/Mobile Commerce
- EPEW: 1st European Performance Engineering Workshop
- ITM: 1st International Workshop on Integration of Testing Methodologies

In total, the calls for papers of the workshops attracted 62 high-quality submissions. The program committees of the workshops selected 27 papers after a rigorous review process in which every paper was reviewed by at least three reviewers. In these proceedings, the papers are grouped according to the workshop they belong to. In addition to the selected papers, there was a keynote speech by Prof. Rob Pooley, from the Heriot-Watt University, UK.

We want to express our gratitude for their financial support both to the Universidad de Castilla-La Mancha and to the Junta de Comunidades de Castilla-La Mancha. Besides, we are in debt to all the authors who submitted high-quality papers to the workshops: Without their effort and interest, it would have been impossible to organize the workshops. We would also like to thank the program committee members of the three workshops for their collaboration during the reviewing process. Last, but not least, we would like to thank the organizers of each of the workshops for their fine work.

In the next pages of this preface, the main characteristics of each of the workshops are described. We hope that these proceedings will be interesting not only for the workshop attendants, but also for a wider community of researchers working on the application of formal methods.

October 2004

Manuel Núñez
Zakaria Maamar
Fernando L. Pelayo
Key Pousttchi
Fernando Rubio

TheFormEMC

Electronic commerce (e-commerce) places new demands not only on support and delivery information technology, but also on the way business processes have to be designed, implemented, monitored, and maintained. Reliability, efficiency, scalability, and fault-tolerance are among the features that have to be embedded into e-commerce processes. Initially, research focused on how to deal with the technical issues. However, the increasing challenges of deploying reliable, efficient, secure, and fault-tolerant applications have highlighted the added value of having theoretical foundations and rigorous formal methods for specifying and validating the design of such applications. In addition, new possibilities extend *static* systems with mobility capabilities. In this sense, the TheFormEMC workshop tried to get together researchers working on theoretical aspects that can be applied to e-commerce and m-commerce systems.

The TheFormEMC workshop attracted 16 high-quality submissions from 9 different countries. The multidisciplinary nature of e-commerce and m-commerce technologies presents challenges for evaluating technical papers. The program committee comprised of experts from several disciplines selected 8 papers after a rigorous double-blind review process in which every paper was reviewed by at least three reviewers.

Program Committee Chairs

Key Pousttchi	University of Augsburg, Germany
Zakaria Maamar	Zayed University, UAE
Manuel Núñez	Universidad Complutense de Madrid, Spain

Organizing Committee Chair

Bettina Bazijanec	University of Augsburg, Germany

Program Committee

Djamel Benslimane	Université Claude Bernard Lyon 1, France
Mario Bravetti	University of Bologna, Italy
Sviatoslav Braynov	State University of New York at Buffalo, USA
Milena M. Head	McMaster eBusiness Research Centre, Canada
Lyes Khelladi	CERIST, Algeria
Birgitta Koenig-Ries	Technical University of Munich, Germany
Winfried Lamersdorf	University of Hamburg, Germany
Franz Lehner	University of Regensburg, Germany
Natalia López	Universidad Complutense de Madrid, Spain
Wathiq Mansoor	Zayed University, UAE
Ismael Rodríguez	Universidad Complutense de Madrid, Spain
Klaus Turowski	University of Augsburg, Germany
Pallapa Venkataram	Indian Institute of Science Bangalore, India
Peter Wurman	North Carolina State University, USA

EPEW

EPEW is a new European forum for the presentation of all aspects of performance modelling and analysis of computer and telecommunication systems. The EPEW workshop attracted 36 high-quality submissions from 15 different countries. The program committee comprised of experts from several disciplines selected 14 papers after a rigorous review process in which every paper was reviewed by at least three reviewers. The 14 accepted papers cover a broad range of topics including performance modelling and analysis of computer systems and networks, performance engineering tools, formal modelling paradigms and methods for performance prediction.

Program Committee Chair

Fernando López Pelayo (Universidad Castilla-La Mancha, Spain)

Program Committee

J. Bradley (Imperial College, UK)
M. Bravetti (U. Bologna, Italy)
J. Campos (U. Zaragoza, Spain)
F. Cuartero (UCLM, Spain)
K. Djemame (U. Leeds, UK)
D. de Frutos (UCM, Spain)
N. Georganas (U. Ottawa, Canada)
S. Gilmore (U. Edinburgh, UK)
H. Hermanns (U. Saarland, Germany)
D.D. Kouvatsos (U. Bradford, UK)
K.G. Larsen (U. Aalborg, Denmark)
M. Núñez (UCM, Spain)
L. Orozco (UCLM, Spain)
R.J. Pooley (U. Heriot-Watt, UK)
R. Puigjaner (U. Illes Balears, Spain)
M. Silva (U. Zaragoza, Spain)
N. Thomas (U. Durham, UK)
V. Valero (UCLM, Spain)

Additional Reviewers

A. Argent-Katwala
S. Bernardi
D. Cazorla
S. Galmes
C. Guidi
P. Harrison
L. Kloul
L. Llana
N. López
R. Lucchi
C. Pérez Jiménez
M. Ribaudo
I. Rodríguez
F. Rubio
F. Tricas

Organizing Committee Chair

Fernando Cuartero Gómez (Universidad Castilla-La Mancha, Spain)

Organizing Committee

Enrique Arias
Antonio Bueno
Emilia Cambronero
Diego Cazorla
Gregorio Díaz
Natalia López
Hermenegilda Macià
Encarnación Moyano
Juan José Pardo
María L. Pelayo
Fernando Rubio
Mª Carmen Ruiz

ITM

Even though testing activities are considered to be rather important, we have to overcome the problem that different testing communities use different methods. We may roughly identify two testing communities: testing of software, and testing of communicating systems. Until very recently, research had been carried out with almost no interactions between these two communities, even though they have complementary know-how. The ITM workshop has born to help find a synthesis between the different techniques developed by each community.

The ITM workshop attracted 10 high-quality submissions from 7 different countries. The program committee selected 5 papers after a rigorous review process in which every paper was reviewed by at least three reviewers. The papers present a well-balanced view of testing technologies, combining both theoretical and practical issues.

Program Committee Chair

Manuel Núñez (Universidad Complutense de Madrid, Spain)

Program Committee

A. Bertolino (ISTI-CNR, Italy)
R. Castanet (LABRI, France)
A. Cavalli (GET-INT, France)
F. Cuartero (UCLM, Spain)
R. Dssouli (Concordia U., Canada)
J. Grabowski (Göttingen, Germany)
R. Hierons (Brunel U., UK)
T. Higashino (Osaka, Japan)
D. Hogrefe (Göttingen, Germany)
P. Le Gall (Evry, France)
D. Lee (Bell Laboratories, USA)
M. Núñez (UCM, Spain)
F. Ouabdesselam (IMAG, France)
M. Pezzè (Milano Bicocca, Italy)
J. Tretmans (Nijmegen, Netherlands)
F. Rubio (UCM, Spain)
I. Schieferdecker (FOKUS, Germany)
H. Ural (Ottawa, Canada)
U. Uyar (CUNY, USA)
J. Wegener (DaimlerChrysler, Germany)
N. Yevtushenko (Tomsk State U., Russia)

Additional Reviewers

D. Chen
A. En-Nouaary
L. Frantzen
X. Fu
N. López
S. Papagiannaki
I. Rodríguez
Z. Wang
T. Willemse

Organizing Committee Chair

Fernando Rubio (Universidad Complutense de Madrid, Spain)

Organizing Committee

Alberto de la Encina
Mercedes Hidalgo
Natalia López
Olga Marroquín
Juan José Pardo
Ismael Rodríguez
Fernando Rubio
María del Carmen Ruiz

Lecture Notes in Computer Science

For information about Vols. 1–3160

please contact your bookseller or Springer

Vol. 3274: R. Guerraoui (Ed.), Distributed Computing. XIII, 465 pages. 2004.

Vol. 3273: T. Baar, A. Strohmeier, A. Moreira, S.J. Mellor (Eds.), <<UML>> 2004 - The Unified Modelling Language. XIII, 449 pages. 2004.

Vol. 3271: J. Vicente, D. Hutchison (Eds.), Management of Multimedia Networks and Services. XIII, 335 pages. 2004.

Vol. 3270: M. Jeckle, R. Kowalczyk, P. Braun (Eds.), Grid Services Engineering and Management. X, 165 pages. 2004.

Vol. 3266: J. Solé-Pareta, M. Smirnov, P.V. Mieghem, J. Domingo-Pascual, E. Monteiro, P. Reichl, B. Stiller, R.J. Gibbens (Eds.), Quality of Service in the Emerging Networking Panorama. XVI, 390 pages. 2004.

Vol. 3263: M. Weske, P. Liggesmeyer (Eds.), Object-Oriented and Internet-Based Technologies. XII, 239 pages. 2004.

Vol. 3260: I. Niemegeers, S.H. de Groot (Eds.), Personal Wireless Communications. XIV, 478 pages. 2004.

Vol. 3258: M. Wallace (Ed.), Principles and Practice of Constraint Programming – CP 2004. XVII, 822 pages. 2004.

Vol. 3256: H. Ehrig, G. Engels, F. Parisi-Presicce, G. Rozenberg (Eds.), Graph Transformations. XII, 451 pages. 2004.

Vol. 3255: A. Benczúr, J. Demetrovics, G. Gottlob (Eds.), Advances in Databases and Information Systems. XI, 423 pages. 2004.

Vol. 3254: E. Macii, V. Paliouras, O. Koufopavlou (Eds.), Integrated Circuit and System Design. XVI, 910 pages. 2004.

Vol. 3253: Y. Lakhnech, S. Yovine (Eds.), Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems. X, 397 pages. 2004.

Vol. 3250: L.-J. (LJ) Zhang, M. Jeckle (Eds.), Web Services. X, 300 pages. 2004.

Vol. 3249: B. Buchberger, J.A. Campbell (Eds.), Artificial Intelligence and Symbolic Computation. X, 285 pages. 2004. (Subseries LNAI).

Vol. 3246: A. Apostolico, M. Melucci (Eds.), String Processing and Information Retrieval. XIV, 332 pages. 2004.

Vol. 3245: E. Suzuki, S. Arikawa (Eds.), Discovery Science. XIV, 430 pages. 2004. (Subseries LNAI).

Vol. 3244: S. Ben-David, J. Case, A. Maruoka (Eds.), Algorithmic Learning Theory. XIV, 505 pages. 2004. (Subseries LNAI).

Vol. 3242: X. Yao, E. Burke, J.A. Lozano, J. Smith, J.J. Merelo-Guervós, J.A. Bullinaria, J. Rowe, P. Tiňo, A. Kabán, H.-P. Schwefel (Eds.), Parallel Problem Solving from Nature - PPSN VIII. XX, 1185 pages. 2004.

Vol. 3241: D. Kranzlmüller, P. Kacsuk, J.J. Dongarra (Eds.), Recent Advances in Parallel Virtual Machine and Message Passing Interface. XIII, 452 pages. 2004.

Vol. 3240: I. Jonassen, J. Kim (Eds.), Algorithms in Bioinformatics. IX, 476 pages. 2004. (Subseries LNBI).

Vol. 3239: G. Nicosia, V. Cutello, P.J. Bentley, J. Timmis (Eds.), Artificial Immune Systems. XII, 444 pages. 2004.

Vol. 3238: S. Biundo, T. Frühwirth, G. Palm (Eds.), KI 2004: Advances in Artificial Intelligence. XI, 467 pages. 2004. (Subseries LNAI).

Vol. 3236: M. Núñez, Z. Maamar, F.L. Pelayo, K. Pousttchi, F. Rubio (Eds.), Applying Formal Methods: Testing, Performance, and M/E-Commerce. XI, 381 pages. 2004.

Vol. 3232: R. Heery, L. Lyon (Eds.), Research and Advanced Technology for Digital Libraries. XV, 528 pages. 2004.

Vol. 3229: J.J. Alferes, J. Leite (Eds.), Logics in Artificial Intelligence. XIV, 744 pages. 2004. (Subseries LNAI).

Vol. 3225: K. Zhang, Y. Zheng (Eds.), Information Security. XII, 442 pages. 2004.

Vol. 3224: E. Jonsson, A. Valdes, M. Almgren (Eds.), Recent Advances in Intrusion Detection. XII, 315 pages. 2004.

Vol. 3223: K. Slind, A. Bunker, G. Gopalakrishnan (Eds.), Theorem Proving in Higher Order Logics. VIII, 337 pages. 2004.

Vol. 3222: H. Jin, G.R. Gao, Z. Xu, H. Chen (Eds.), Network and Parallel Computing. XX, 694 pages. 2004.

Vol. 3221: S. Albers, T. Radzik (Eds.), Algorithms – ESA 2004. XVIII, 836 pages. 2004.

Vol. 3220: J.C. Lester, R.M. Vicari, F. Paraguaçu (Eds.), Intelligent Tutoring Systems. XXI, 920 pages. 2004.

Vol. 3219: M. Heisel, P. Liggesmeyer, S. Wittmann (Eds.), Computer Safety, Reliability, and Security. XI, 339 pages. 2004.

Vol. 3217: C. Barillot, D.R. Haynor, P. Hellier (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2004. XXXVIII, 1114 pages. 2004.

Vol. 3216: C. Barillot, D.R. Haynor, P. Hellier (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2004. XXXVIII, 930 pages. 2004.

Vol. 3215: M.G.. Negoita, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems. LVII, 906 pages. 2004. (Subseries LNAI).

Vol. 3214: M.G.. Negoita, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems. LVIII, 1302 pages. 2004. (Subseries LNAI).

Vol. 3213: M.G.. Negoita, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems. LVIII, 1280 pages. 2004. (Subseries LNAI).

Vol. 3212: A. Campilho, M. Kamel (Eds.), Image Analysis and Recognition. XXIX, 862 pages. 2004.

Vol. 3211: A. Campilho, M. Kamel (Eds.), Image Analysis and Recognition. XXIX, 880 pages. 2004.

Vol. 3210: J. Marcinkowski, A. Tarlecki (Eds.), Computer Science Logic. XI, 520 pages. 2004.

Vol. 3209: B. Berendt, A. Hotho, D. Mladenic, M. van Someren, M. Spiliopoulou, G. Stumme (Eds.), Web Mining: From Web to Semantic Web. IX, 201 pages. 2004. (Subseries LNAI).

Vol. 3208: H.J. Ohlbach, S. Schaffert (Eds.), Principles and Practice of Semantic Web Reasoning. VII, 165 pages. 2004.

Vol. 3207: L.T. Yang, M. Guo, G.R. Gao, N.K. Jha (Eds.), Embedded and Ubiquitous Computing. XX, 1116 pages. 2004.

Vol. 3206: P. Sojka, I. Kopecek, K. Pala (Eds.), Text, Speech and Dialogue. XIII, 667 pages. 2004. (Subseries LNAI).

Vol. 3205: N. Davies, E. Mynatt, I. Siio (Eds.), UbiComp 2004: Ubiquitous Computing. XVI, 452 pages. 2004.

Vol. 3203: J. Becker, M. Platzner, S. Vernalde (Eds.), Field Programmable Logic and Application. XXX, 1198 pages. 2004.

Vol. 3202: J.-F. Boulicaut, F. Esposito, F. Giannotti, D. Pedreschi (Eds.), Knowledge Discovery in Databases: PKDD 2004. XIX, 560 pages. 2004. (Subseries LNAI).

Vol. 3201: J.-F. Boulicaut, F. Esposito, F. Giannotti, D. Pedreschi (Eds.), Machine Learning: ECML 2004. XVIII, 580 pages. 2004. (Subseries LNAI).

Vol. 3199: H. Schepers (Ed.), Software and Compilers for Embedded Systems. X, 259 pages. 2004.

Vol. 3198: G.-J. de Vreede, L.A. Guerrero, G. Marín Raventós (Eds.), Groupware: Design, Implementation and Use. XI, 378 pages. 2004.

Vol. 3195: C.G. Puntonet, A. Prieto (Eds.), Independent Component Analysis and Blind Signal Separation. XXIII, 1266 pages. 2004.

Vol. 3194: R. Camacho, R. King, A. Srinivasan (Eds.), Inductive Logic Programming. XI, 361 pages. 2004. (Subseries LNAI).

Vol. 3193: P. Samarati, P. Ryan, D. Gollmann, R. Molva (Eds.), Computer Security – ESORICS 2004. X, 457 pages. 2004.

Vol. 3192: C. Bussler, D. Fensel (Eds.), Artificial Intelligence: Methodology, Systems, and Applications. XIII, 522 pages. 2004. (Subseries LNAI).

Vol. 3191: M. Klusch, S. Ossowski, V. Kashyap, R. Unland (Eds.), Cooperative Information Agents VIII. XI, 303 pages. 2004. (Subseries LNAI).

Vol. 3190: Y. Luo (Ed.), Cooperative Design, Visualization, and Engineering. IX, 248 pages. 2004.

Vol. 3189: P.-C. Yew, J. Xue (Eds.), Advances in Computer Systems Architecture. XVII, 598 pages. 2004.

Vol. 3188: F.S. de Boer, M.M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), Formal Methods for Components and Objects. VIII, 373 pages. 2004.

Vol. 3187: G. Lindemann, J. Denzinger, I.J. Timm, R. Unland (Eds.), Multiagent System Technologies. XIII, 341 pages. 2004. (Subseries LNAI).

Vol. 3186: Z. Bellahsène, T. Milo, M. Rys, D. Suciu, R. Unland (Eds.), Database and XML Technologies. X, 235 pages. 2004.

Vol. 3185: M. Bernardo, F. Corradini (Eds.), Formal Methods for the Design of Real-Time Systems. VII, 295 pages. 2004.

Vol. 3184: S. Katsikas, J. Lopez, G. Pernul (Eds.), Trust and Privacy in Digital Business. XI, 299 pages. 2004.

Vol. 3183: R. Traunmüller (Ed.), Electronic Government. XIX, 583 pages. 2004.

Vol. 3182: K. Bauknecht, M. Bichler, B. Pröll (Eds.), E-Commerce and Web Technologies. XI, 370 pages. 2004.

Vol. 3181: Y. Kambayashi, M. Mohania, W. Wöß (Eds.), Data Warehousing and Knowledge Discovery. XIV, 412 pages. 2004.

Vol. 3180: F. Galindo, M. Takizawa, R. Traunmüller (Eds.), Database and Expert Systems Applications. XXI, 972 pages. 2004.

Vol. 3179: F.J. Perales, B.A. Draper (Eds.), Articulated Motion and Deformable Objects. XI, 270 pages. 2004.

Vol. 3178: W. Jonker, M. Petkovic (Eds.), Secure Data Management. VIII, 219 pages. 2004.

Vol. 3177: Z.R. Yang, H. Yin, R. Everson (Eds.), Intelligent Data Engineering and Automated Learning – IDEAL 2004. XVIII, 852 pages. 2004.

Vol. 3176: O. Bousquet, U. von Luxburg, G. Rätsch (Eds.), Advanced Lectures on Machine Learning. IX, 241 pages. 2004. (Subseries LNAI).

Vol. 3175: C.E. Rasmussen, H.H. Bülthoff, B. Schölkopf, M.A. Giese (Eds.), Pattern Recognition. XVIII, 581 pages. 2004.

Vol. 3174: F. Yin, J. Wang, C. Guo (Eds.), Advances in Neural Networks - ISNN 2004. XXXV, 1021 pages. 2004.

Vol. 3173: F. Yin, J. Wang, C. Guo (Eds.), Advances in Neural Networks – ISNN 2004. XXXV, 1041 pages. 2004.

Vol. 3172: M. Dorigo, M. Birattari, C. Blum, L. M. Gambardella, F. Mondada, T. Stützle (Eds.), Ant Colony, Optimization and Swarm Intelligence. XII, 434 pages. 2004.

Vol. 3171: A.L.C. Bazzan, S. Labidi (Eds.), Advances in Artificial Intelligence – SBIA 2004. XVII, 548 pages. 2004. (Subseries LNAI).

Vol. 3170: P. Gardner, N. Yoshida (Eds.), CONCUR 2004 - Concurrency Theory. XIII, 529 pages. 2004.

Vol. 3166: M. Rauterberg (Ed.), Entertainment Computing – ICEC 2004. XXIII, 617 pages. 2004.

Vol. 3163: S. Marinai, A. Dengel (Eds.), Document Analysis Systems VI. XI, 564 pages. 2004.

Vol. 3162: R. Downey, M. Fellows, F. Dehne (Eds.), Parameterized and Exact Computation. X, 293 pages. 2004.

Table of Contents

III ITM

Formal Analysis of the Internet Open Trading Protocol

Chun Ouyang and Jonathan Billington

Computer Systems Engineering Centre
School of Electrical and Information Engineering
University of South Australia, SA 5095, AUSTRALIA
{Chun.Ouyang,Jonathan.Billington}@unisa.edu.au

Abstract. The Internet Open Trading Protocol (IOTP) is an electronic commerce (e-commerce) protocol developed by the Internet Engineering Task Force (IETF) to support online trading activities. The core of IOTP is a set of financial transactions and therefore it is vitally important that the protocol operates correctly. An informal specification of IOTP is published as Request For Comments (RFC) 2801. We have applied the formal method of Coloured Petri Nets (CPNs) to obtain a formal specification of IOTP. Based on the IOTP CPN specification, this paper presents a detailed investigation of a set of behavioural properties of IOTP using state space techniques. The analysis reveals deficiencies in the termination of IOTP transactions, demonstrating the benefit of applying formal methods to the specification and verification of e-commerce protocols.

1 Introduction

Electronic commerce (e-commerce) applications are susceptible to failures if the underlying protocols are not properly designed and analysed. These failures could result in financial loss to any participant, e.g., commercial traders, financial institutions or consumers. However, ensuring the correctness of complex e-commerce protocols is a difficult task and informal methods are inadequate. Formal methods [6] are necessary for the construction of unambiguous and precise models that can be analysed to identify errors and verify correctness before implementation. Application of formal methods will lead to more reliable and trustworthy e-commerce protocols [16].

An important example of an e-commerce protocol is the Internet Open Trading Protocol (IOTP) [5] developed by the Internet Engineering Task Force (IETF) to support trading activities over the Internet. It is also referred to as a shopping protocol [3, 10] which encapsulates different payment systems such as Secure Electronic Transaction (SET) [18] and Mondex [11]. The specification of IOTP, Request For Comments (RFC) 2801 [4], is the largest RFC developed by IETF spanning 290 pages. The RFC contains an informal narrative description of IOTP, and so far no complete implementation of IOTP exists [17, 7]. The development of IOTP is still in an early stage and can therefore benefit from the use of formal methods to verify its functional correctness.

M. Núñez et al. (Eds.): FORTE 2004 Workshops, LNCS 3236, pp. 1–15, 2004.

We apply Coloured Petri Nets (CPNs) [8] to model and analyse IOTP. CPNs are a formal modelling technique that combines the graphical notation of Petri nets with the power of abstract data types allowing data and control flow to be visualised. CPNs have been used successfully for protocol modelling and analysis for 2 decades [2]. Babich and Deotto [1] provide a recent survey comparing this approach with the other main approaches. CPN models are executable and can be analysed using state spaces to detect errors such as deadlocks. We use a tool called Design/CPN [12] for constructing and analysing our CPN models.

In previous work [14], we developed a hierarchical formal specification of IOTP and briefly mentioned some initial analysis results. In contrast, this paper describes our analysis approach in detail. With the state space generated from the CPN model, we investigate and formally reason about a set of desired properties of IOTP (e.g., correct termination). The analysis reveals errors in the current design.

The paper is organised as follows. Section 2 gives an introduction to IOTP's basic concepts and procedures. Section 3 describes the IOTP CPN specification, with focus on its hierarchical structure. Section 4 presents a detailed investigation of several desired properties of IOTP. Finally, we conclude this paper and discuss future work in Sect. 5.

2 The Internet Open Trading Protocol

IOTP [4] focuses on consumer-to-business e-commerce applications. It defines five *trading roles* to identify the different roles that organisations can assume while trading. These are *Consumer*, *Merchant*, *Payment Handler* (a bank), *Delivery Handler* (a courier firm) and *Merchant Customer Care Provider*. The core of IOTP is an *Authentication* transaction and five payment-related transactions named *Purchase*, *Deposit*, *Withdrawal*, *Refund* and *Value Exchange*. Each transaction comprises a sequence of message exchanges between trading roles.

Document Exchanges and Transactions. IOTP defines a set of document exchanges as building blocks for implementation of transactions. These are: *Authentication*, *Brand Dependent Offer*, *Brand Independent Offer*, *Payment*, *Delivery*, and *Payment-and-Delivery*. An Authentication transaction consists of just an Authentication (document) exchange. A Purchase transaction comprises an optional Authentication, an Offer (either a Brand Dependent Offer or a Brand Independent Offer), and then, a Payment exchange, a Payment followed by a Delivery exchange, or a Payment-and-Delivery exchange. A Deposit, Withdrawal, or Refund transaction starts with an optional Authentication, an Offer, and a Payment exchange. Finally, a Value Exchange transaction begins with an optional Authentication followed by an Offer and two Payment exchanges in sequence.

Below, we consider an example of a Purchase transaction which comprises an Authentication, a Brand Dependent Offer, and a Payment followed by a Delivery exchange. Figure 1 shows a possible sequence of messages exchanged between the four trading roles involved in the transaction.

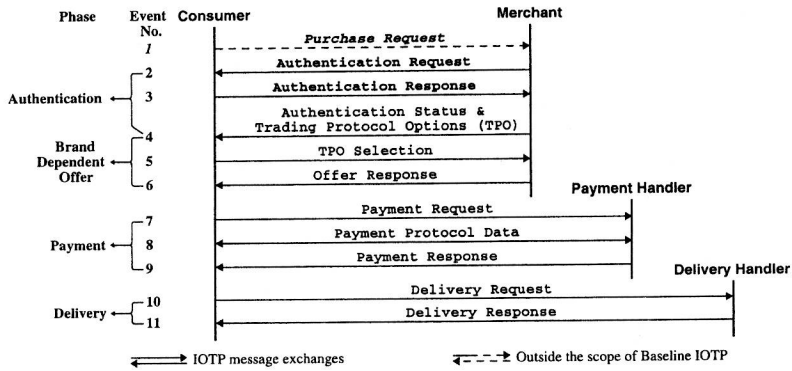

Fig. 1. A possible sequence of message exchanges in a Purchase transaction

In the beginning, the Consumer decides to buy goods, and sends a Purchase Request (event 1) to the Merchant. This event initiates a Purchase transaction, however it is not part of Baseline IOTP.

Upon receiving the Purchase Request, the Merchant starts an Authentication document exchange (events 2-4) to verify the *bona fides* of the Consumer. In IOTP's terminology, the Merchant acts as the *Authenticator* and the Consumer the *Authenticatee*. At first, an Authentication Request is issued by the Merchant (event 2), specifying the authentication algorithm to be used. As a result, the Consumer replies with an Authentication Response containing the authentication data obtained using the above algorithm (event 3). After verifying the Consumer's response, the Merchant generates an Authentication Status indicating that the authentication is successful (see event 4).

Once the authentication completes, the Merchant continues to a Brand Dependent Offer document exchange (events 4-6) by providing the Consumer a list of Trading Protocol Options (TPO). This includes the available payment methods and associated payment protocols. The message combining the TPO and the above Authentication Status is then sent to the Consumer (event 4). The Consumer chooses one of the options, and sends it back as a TPO Selection (event 5). The Merchant uses the selection to create and send back an Offer Response (event 6), which contains details of the goods to be purchased together with payment and delivery instructions.

Next, a Payment document exchange starts between the Consumer and the Payment Handler (events 7-9). After checking the Offer Response for purchase details, the Consumer sends the Payment Handler a Payment Request (event 7). The Payment Handler checks the Payment Request, and if valid, the payment is conducted using Payment Protocol Data exchanges (events 8) as determined by the encapsulated payment protocol (e.g., SET). After the payment protocol data exchange has finished, the Payment Handler sends a Payment Response (event 9) containing the payment result (e.g., receipt).

Finally, a Delivery document exchange is carried out between the Consumer and the Delivery Handler (events 10-11). After checking the Payment Response, the Consumer sends the Delivery Handler a Delivery Request (event 10). The Delivery Handler schedules the delivery and sends the Consumer a Delivery Response (event 11) containing details of the delivery, and possibly the actual delivery if the goods are electronic (e.g., an e-journal).

Also, it should be mentioned that event 5 in the above scenario may or may not take place in an Offer exchange, which results in the distinction between a Brand Dependent Offer and a Brand Independent Offer. The Brand Dependent Offer occurs when the Merchant offers some additional benefit (e.g., price discount) in the Offer Response *depending* on the specific *payment brand* (e.g., VISA or MasterCard) chosen in the Consumer's TPO Selection. In the Brand Independent Offer, the Offer Response is *independent* of the *payment brand* selected by the Consumer. In this case, the Merchant does not require the Consumer's TPO Selection before the Offer Response can be generated. IOTP defines a combined TPO and Offer Response message to be used in the Brand Independent Offer.

Transaction Cancellation and Error Handling. These are two important procedures related to IOTP transactions. A transaction may be cancelled by any trading role engaged in that transaction. For example, in the Purchase transaction shown in Fig. 1, the Merchant would cancel the transaction if the Consumer's Authentication Response has failed. Error handling is concerned with how trading roles handle technical errors and exceptions that occur during a transaction. For example, in Fig. 1, the Merchant may re-send the TPO upon a time-out when expecting the Consumer's TPO Selection. A Cancel message is used for transaction cancellation and an Error message for reporting errors.

3 A Formal Specification of IOTP

RFC 2801 [4] contains an informal narrative description of IOTP and suffers from ambiguities and incompleteness. We have created a CPN model of IOTP to obtain a formal specification of IOTP that truly reflects the intent of its RFC specification. When ambiguities and gaps are detected, assumptions are made to clarify the ambiguities and fill in the gaps. A detailed description of this formal specification of IOTP is presented in [14]. Figure 2 shows the *hierarchy page* for the IOTP CPN model. It provides an overview of the *pages* (modules) constituting the model. There are 31 pages organised into four hierarchical levels. An arc between two pages indicates that the destination page is a *subpage* (submodule) of the source page. The four-level hierarchy of the IOTP CPN model provides a logical structure that can be validated against RFC 2801.

The first (top) level presents an abstract view of IOTP on one page, namely IOTP_TopLevel. It has four subpages: Consumer, Merchant, PHandler and DHan-