

CONTESSA Meeting, April 2003

José Meseguer

Computer Science Department
University of Illinois at Urbana-Champaign

Introduction

The **CONTESSA** project focuses on **CON**text **S**ensitive **S**ystem **A**daptivity.

The problems of distributed system adaptation and composition are hard, fundamental, and lack of adequate technology is currently a big stumbling block in software engineering.

These problems must be considered at many different, yet related, levels and aspects. This is a perfect candidate for a multidisciplinary research project. In CONTESSA, the following disciplines are brought together:

Introduction (II)

- Agents/Actors
- Reflective Middleware
- Mobile Computing
- Network Protocols and Security
- Formal Models and Formal Analysis

In particular, in the CONTESSA Project, **formal models** provide the **conceptual glue** helping us **develop new concepts** and techniques, and also allowing **early prototyping and validation** of new designs and mechanisms.

Project Meetings and Collaborations

The following general meetings have taken place, including this last one:

- Kickoff Meeting, Upenn, June 02
- PI Meeting, Washington Univ. October 02
- Project Review Meeting, UPenn, April 02

These meetings have helped us refine the original goals of the project, and have led to a number of interesting collaborations:

Project Meetings and Collaborations (II)

- NRL/UIUC collaboration (ongoing) on using Maude to implement the Multiset Rewriting formalism used at NRL and in SPYCE to specify and analyze cryptographic protocols
- Penn/UIUC collaboration on the Sectrace protocol specification
- UCI/SRI/UIUC collaboration on formal models of reflective middleware
- UIUC (both PIs) collaboration on new models for distributed probabilistic systems

Some Papers

1. M. Clavel, J. Meseguer and M. Palomino, *Reflection in Membership Equational Logic, Horn Logic with Equality, and Rewriting Logic*, in *Proc. WRLA 2002, International Workshop on Rewriting Logic and its Applications* (Pisa, Italy, September 2002) Elsevier ENTCS, Vol. 71, 2000.
2. S. Eker, J. Meseguer, and A. Sridharanarayanan, *The Maude LTL Model Checker*, with, in *Proc. WRLA 2002, International Workshop on Rewriting Logic and its Applications* (Pisa, Italy, September 2002) Elsevier ENTCS, Vol. 71, 2000.
Fok, C.L., and Roman, G.-C., A Lightweight Coordination Model for Mobile Computing, TR

WUCSE-02-32, Washington University, St. Louis, MO, 2002.

3. *Handorean, R., Julien, C., Roman, G.-C., Coordination Middleware Supporting Rapid Deployment of Ad Hoc Mobile Systems, to appear in Proc. of the ICDCS Workshop on Mobile Computing Middleware, 2003.*
4. *Huang, Q., Lu, C., and Roman, G.-C., Mobicast: Just-in-Time Multicast for Sensor Networks under Spatiotemporal Constraints, to appear in Proc. of the 2nd Intl. Workshop on Information Processing in Sensor Networks, 2003.*
5. *Julien, C., Roman, G.-C., and Huang, Q., Declarative and Dynamic Context Specification Supporting Mobile Computing and Ad Hoc Networks, TR WUCSE-03-13, Washington University, St. Louis, MO, 2003.*

6. *N. Kumar, K. Sen, J. Meseguer, and G. Agha, Probabilistic Rewrite Theories: Unifying Models, Logics, and Tools, Manuscript, CS Department, UIUC, March 2003.*
7. *Sebastian Gutierrez-Nolasco, Nalini Venkatasubramanian. A Reflective Middleware Framework for Communication in Dynamic Environments, IFIP International Conference on Distributed Objects and Applications, 2002.*
8. *Sebastian Gutierrez-Nolasco, Nalini Venkatasubramanian Reachability Snapshots in the Presence of Failures: An Exercise in Protocol-Service Composition, IEEE Dependable Systems and Networks Workshop on Dependable Middleware, 2002.*
9. *Sebastian Gutierrez-Nolasco, Nalini*

Venkatasubramanian and Carolyn Talcott A Semantic Model for Adaptive Communication, Technical Report, UC Irvine, 2003.

10. *Qi Han, Sebastian Gutierrez-Nolasco, Nalini Venkatasubramanian. Reflective Middleware for Integrating Network Monitoring with Adaptive Object Messaging, Submitted for publication, 2003.*
11. *J. Meseguer, Software Specification and Verification in Rewriting Logic, to appear in Proc. 2002 Marktoberdorf Summer School on "Models Algebras and Logics of Engineering Software, 2003.*
12. *J. Meseguer and C. Talcott, Semantic Models for Distributed Object Reflection, in Proc. 16th European Conference on Object-Oriented Programming, ECOOP*

2002 (Málaga, Spain, June 2002) Springer Lecture Notes in Computer Science, Vol. 2374, 2002, pages 1–36.

13. *Nalini Venkatasubramanian, Carolyn Talcott and Gul Agha. A Formal Model for Reasoning about Adaptive QoS-enabled middleware, in revision (ACM TOSEM), early version at Formal Methods Europe, 2001.*
14. *Jehan Wickramasuriya, Qi Han and Nalini Venkatasubramanian. A Directory Enabled Middleware Framework for Distributed Systems, in IEEE Workshop on Real-time Distributed Systems, 2003.*
15. *Jehan Wickramasuriya, Nalini Venkatasubramanian, Carolyn Talcott. Multilevel Access Control for Environments with Object and Node Mobility, under*

submission. Early version appeared as poster paper in IFIP DOA 2002.

16. *Qi Han, Nalini Venkatasubramanian. Aggregation Based Information Collection for Mobile Environments, Journal of High Speed Networking, Special Issue on Mobility 2002.*
17. *Qi Han, Nalini Venkatasubramanian. Addressing Timeliness/Accuracy/Cost Tradeoffs in Information Collection for Dynamic Environments, submitted for publication.*
18. *Shivajit Mohapatra, Nalini Venkatasubramanian. PARM: Power-Aware Reconfigurable Middleware, IEEE International Conference on Distributed Computing Systems, ICDCS 2003.*

Today's Schedule (Morning)

- 9:40-10:30 Sectrace Design, Implementation and Experiments, Alwyn Goodloe and Michael McDougall, UPenn
- 10:30-11:00 Formal Specification of Sectrace, Mark-Oliver Stehr, UIUC
- 11:00-11:20 Coffee Break
- 11:20-12:00 Probabilistic Modeling and Formal Analysis of Networked Embedded Systems, Gul Agha and Koushik Sen, UIUC
- 12:00-1:00 Lunch

Today's Schedule (Afternoon)

- 12:30-1:10 Project Overview, Dan Siewiorek, CMU
- 1:10-1:50 Composability Issues in Adaptive Reflective Middleware for Dynamic Environments Nalini Venkatasubramanian and Sebastian Gutierrez-Nolasco, UC Irvine
- 1:50-2:20 Formal Specification of Group Communication Middleware, Mark-Oliver Stehr, UIUC
- 2:20-2:40 Coffee Break
- 2:40-3:20 Declarative Context Specifications Supporting Mobile Computing, Gruia-Catalin Roman and Christine Julien, Washington Univ.
- 3:20-4:00 General Discussion

Concluding Remarks

Today's presentations have given a snapshot of current research in the CONTESSA project. Not all advances were covered; other advances are reported in the papers distributed or are work in progress. In summary we have shown:

- Work Connecting Theory and Practice
- Interesting Synergies
- Formal Modeling and Analysis Tools
- System Implementations

Connecting Theory and Practice

For example:

- theorems and formal analysis of Sectrace
- applying probabilistic rewrite theories and runtime verification to networked embedded systems
- formal models of reflective middleware
- formal model of contexts for mobility

Interesting Synergies

For example:

- between new network security protocol design and formal modeling and analysis in Maude
- between massively distributed embedded systems and new formal probabilistic methods and tools
- between work at UCI, UIUC, and Washington Univ. on reflective middleware and mobility, and different formal models for them

Formal Modeling and Analysis Tools

- Maude
- the Maude LTL Model Checker
- the Maude ITP, Church-Rosser Checker, Termination Checker, and KB Completion and Coherence Completion Tools
- Real-Time Maude
- PMaude

System Implementations

- The above Maude formal tools
- Sectrace
- Probabilistic distributed protocols for networked embedded systems
- Reflective middleware systems
- The Lime and Limon mobile systems