Project Number:	IST-2001-33100
Project Acronym:	PROFUNDIS
Title :	Proofs of Functionality for Mobile Distributed Systems

Periodic Progress Report Year 4

Preparation date:	June 29, 2005
Classification:	Public
Contract start date	1 January 2002
Duration:	3 years
Project co-ordinator:	Joachim Parrow
Partners:	Univ. Uppsala, Sweden Univ. Pisa, Italy INRIA, France Univ. FFCT, Portugal

Contents

PROFUNDIS:
Periodic Progress Report Year 4

June 29, 2005

1 Executive Summary

PROFUNDIS is a FET GC project with the main goal to advance the state of the art of formal modelling and verification techniques to the point where key issues in mobile distributed systems can be treated rigorously and with considerable automatic support. The partners are Uppsala (co-ordinator), Lisbon, INRIA and Pisa. In this Periodic Progress Report we present the developments in Year 4 (2005).

Overall PROFUNDIS has been successful and reached all the major scientific goals. Inevitably there are small discrepancies in comparison to the plan we made three and a half years ago. In some areas we have fewer results than hoped, and in some we have progressed farther than envisaged.

Originally the project was planned to last three years, terminating 31/12/2004. However we had initial problems in recruiting researchers and the work was a bit delayed. Therefore we were granted a four month extension, terminating 30/4/2005. The report here only covers this extension. The accompanying Final Report describes the outcome of the entire project. Another related document is the Technology Implementation Plan.

The extension period has run without incidents. Project resources are now spent, and we have conducted 6% more than the planned manmonths. Scientific and dissemination goals have been met, with an additional 9 peer-reviewed published papers. During the period we have done the final project review, with a satisfactory outcome.

2 Work progress overview

We here elaborate on the objectives of year 4, on the progress made and on how it compares to plan. We report on activities in man months per Work Package.

2.1 Specific objectives for year 4

The specific objectives for year 4 can be broken down onto the three scientific Work Packages as follows.

2.1.1 WP1: Models

The overall goal of this Work Package is to develop a comprehensive automata-like model that supports effective techniques to specify and verify properties of network applications. In the last period of the Profundis project we continued enriching with new features the models and the proof techniques we develop. Moreover, we experimented with our verification toolkits. Indeed, the research was active on all of the three tasks of WP1.

2.1.2 WP2: Specifications

The objectives of WP2 in Year 4 are to continue some of the work going on in Year 3, namely on the spatial-logic model-checker and case studies, spatial logics with quantitative information and types for spatial properties.

2.1.3 WP3: Types

This Work Package deals with formal type systems for our calculi and logics. The work in year 4 was planned to consist in polishing the results from 2004, writing some journal papers, and preparing the first draft of Y. Deng's PhD thesis.

2.2 Overview of progress, comparison to plan and assessment of results

2.2.1 WP1

The three tasks of WP1 have proceeded according to plans with a small discrepancy in Task 1.3. Hereafter, we will briefly comment on the results of each of the three tasks of WP1.

Task 1.1: Automata with Operations and Substitutions Symbolic semantics is a well established syntax-based approach approach to finite state verification of nominal calculi. An alternative class of models for nominal calculi are the so-called syntax-free models where names are explicitly dealt with regardless of the syntactic structure of the calculi. History Dependent automata (HD-automata in brief) are examples of syntax-free models of nominal calculi. As pointed out in the previous PPRs these two lines of research (symbolic semantics and HD automata) were developed independently. A main result of the last period of the project consists in integrating together the two approaches. The technical contribution of our research is the development of a coalgebraic framework for the Fusion calculus equipped with the symbolic semantics. Our main result here is that the coalgebraic description of the minimisation algorithm for HD-automata smoothly extends to handle the Fusion calculus and behaves in accordance with the symbolic semantics: bisimilar processes are mapped together by the morphisms yielding the minimal HD-automaton. As a beneficial side effect, this also provides a bisimulation checker for Fusion calculus.

The integration of syntax-based and syntax-free models of nominal calculi in a coalgebraic setting is indeed a main result of the Profundis project.

Task 1.2: Proof Techniques The π-calculus with data terms (πT) extends the pure π-calculus by data constructors and destructors and allows data to be transmitted between agents. We present a new type of encoding and prove it to be fully abstract with respect to may-testing equivalence. To our knowledge this is the first result of its kind, for any calculus enriched with data terms. It has particular importance when representing security properties since attackers can be regarded as may-test observers. Full abstraction proves that it does not matter whether such observers are formulated in π or πT, both are equally expressive in this respect. The technical new idea consists of achieving full abstraction by encoding data as table entries rather than active processes, and using a firewalled central integrity manager to ensure data security.

It has long been known how to encode such data types in π, but until now it has been open how to make the encoding fully abstract, meaning that two encodings (in π) are semantically equivalent precisely when the original πT agents are semantically equivalent.

Task 1.3: Prototype and Case Studies As pointed out in the previous PPR, the Profundis group in Pisa has established a collaboration with an indus-

trial partner – Telecom Italia Lab (TILAB) . Together with the TILAB group, the Pisa Profundis Group has exploited some of the toolkits of the PWeb to verify functional and non-functional properties of the PARLAY-X infrastructure. The main contribution here is the complete specification of the PARLAY-X framework in a dialect of the of the π-calculus. This is a substantial amount of research and experimentation but that has not yet led to a scientific publication.

2.2.2 WP2

Task 2.1 (Logics for systems with spatial and temporal structure Progress has been made on the study of types for spatial properties and results are expected soon, but no publication is available yet. A paper has been published on a modal logic which quantitative modalities. The logic has been exploited as basis to define a spatial logic with quantitative information.

Task 2.2 (Expressiveness) No activity was planned for this period.

Task 2.3 (Tools and case studies) the development of the spatial-logic model-checker continued with the implementation of new functionalities and further examples.

2.2.3 WP3

During 2005 the main work has been about polishing the results produced during 2004. Notably, two journal papers have been prepared, a first draft of Deng's PhD thesis (funded by Profundis to work on WP3) has been made ready.

A few new results and conference papers have however been produced, in the topic of access control policies based on stack inspection.

In conclusion, the work has gone very much according to plans.

2.3 Activities per Work Package

We here give the tables indicating the effort spent in man months on the different Work Packages.

2.3.1 Project total

TOTAL	Year 4 Planned		Year 4 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	0	0	7	4	82	54	110	58
FFCT	0	0	13	12	135	99	103	63
INRIA	0	0	6	6	69	69	69	69
PISA	0	0	13	8	95	54	120	83
Total	0	0	39	30	381	276	402	273

The total effort is very close to plan: 106% of the planned total work and 99% of the planned work directly paid by the PROFUNDIS contract. Work in Uppsala and Pisa has been above plan, and in FFCT below plan.

2.3.2 WP1

WP1	Year 4 Planned		Year 4 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	0	0	6	4	46	32	88	53
FFCT	0	0	0	0	42	33	10	2
INRIA	0	0	1	1	18	18	14	14
PISA	0	0	10	8	59	34	78	60
Total	0	0	17	13	165	117	190	129

The overall efforts of WP1 (including the the four months extension) amounts to an additional 12% of what planned in the TA for the three years. Hence, the activities of WP1 have progressed basically as planned. An important deviation from what was specified in the TA concerns the activities planned in Lisbon. The work in Lisbon has been significantly less than planned. However, this has been compensated by much work done in Uppsala and Pisa.

2.3.3 WP2

WP2	Year 4 Planned		Year 4 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	0	0	0	0	15	11	5	5
FFCT	0	0	13	12	72	54	76	54
INRIA	0	0	1	1	18	18	17	17
PISA	0	0	1	0	15	9	16	9
Total	0	0	15	13	120	92	114	85

As noted in the last report, there is less work than expected in Uppsala due to reordering of priorities. The initial difficulty felt by Lisbon in hiring people was overcome at the end of the project.

2.3.4 WP3

WP3	Year 3 Planned		Year 3 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	0	0	0	0	15	11	10	0
FFCT	0	0	0	0	18	12	14	7
INRIA	0	0	4	4	30	30	35	35
PISA	0	0	2	0	18	11	23	14
Total	0	0	6	4	81	64	82	56

Figures are globally as expected, less work in Uppsala and Lisbon being compensated by additional effort at Pisa and INRIA.

2.3.5 WP4: Management

WP4	Year 4 Planned		Year 4 Actual		Cumulative Planned		Cumulative Actual	
	Tot	Paid	Tot	Paid	Tot	Paid	Tot	Paid
UU	0	0	1	0	6	0	7	0
FFCT	0	0	0	0	3	0	3	0
INRIA	0	0	0	0	3	3	3	3
PISA	0	0	0	0	3	0	3	0
Total	0	0	1	0	15	3	16	3

Activities are according to plan.

2.4 Reviewer comments

In their report on the second and third years of PROFUNDIS the reviewers had no particular comments or requests for a change of plan. We have continued the case studies and workpackage interactions started in Year 2 (as described in the PPR for year 2).

3 Project management and coordination

Project management and coordination has been conducted without any friction. There have been no conflicts within the consortium. There have been no contractual issues. Since this is an extension period no general PROFUNDIS meetings have been conducted. A steering committee meeting was held in Edinburgh, April 2005.

4 Information dissemination and exploitation of results

4.1 Web presence

1. `http://www.it.uu.se/profundis` is the project main web page. It includes:
   - A main page with synopsis of overview and pointers to all other resources.
   - A project overview, related projects, and a list of official (yearly) progress reports.
   - A list of meetings, with links to files for each meeting.
   - A list of visits.
   - A list of events, with links to the main web page of each event.
   - A list of publications reporting the work done within the project.
   - Links to all delivered software.
2. `http://jordie.di.unipi.it:8080/pweb` is a web site for the distributed PROFUNDIS tools. Here the tools STA, pi-compiler, Reducer, MWB and Trust can be accessed in a general framework.
3. `http://www.cmi.univ-mrs.fr/~vvanacke/trust.html` is a web site for the TRUST tool.
4. `http://jordie.di.unipi.it:8080/mihda` is the web site of the HD-Reducer
5. `http://rep1.iei.pi.cnr.it/projects/JACK/hal.html` is the web site for the HAL tool.
6. `http://www.it.uu.se/research/group/mobility/mwb` is the web site for the MWB tool.
7. `http://www.dsi.unifi.it/~boreale/tool.html` is the web site of the STA tool.

8. `http://www-ctp.di.fct.unl.pt/SLMC` is the web site of the Spatial Model Checker (SLMC) tool.

9. `http://perso.ens-lyon.fr/damien.pous/gcpan` is a web site for the the abstract machine for the execution of Safe Ambients.

4.2 Visits between members of the project

In April 2005, Daniel Hirschkoff and Damien Pous (Lyon) visited Davide Sangiorgi (Bologna).

4.3 Visits and talks by project members outside PROFUNDIS

At the European Joint Conferences on Theory and Practice of Software (ETAPS) with associated workshops, several PROFUNDIS researchers participated. Among them, the following gave presentations.

1. Y. Deng presented "Axiomatizations for Probabilistic Finite-State Behaviors"

2. K. Yemane presented " A Unifying Model of Variables and Names"

3. U. Montanari gave the invited talk "Model Checking for Nominal Calculi"

4. M. Buscemi presented "A general name binding mechanism"

Appendix : Publications and reports

Reviewed Publications

[1] Michael Baldamus, Joachim Parrow, and Björn Victor. A fully abstract encoding of the π-calculus with data terms. In *Proceedings of ICALP'05*, LNCS. Springer, 2005.

[2] Massimo Bartoletti, Pierpaolo Degano, and Gianluigi Ferrari. Enforcing secure service composition. In *IEEE Computer Security Foundation Workshop, to appear*, 2005.

[3] Massimo Bartoletti, Pierpaolo Degano, and Gianluigi Ferrari. History-based access control with local policies. In *FOSSACS 2005*, volume 3441 of *Lectures Notes in Computer Science*. Springer, 2005.

[4] L. Caires and E. Lozes. Elimination of quantifiers and undecidability in spatial logics for concurrency. *Theor. Comput. Sci.*, 2005. Accepted for publication.

[5] S. Dantchev and F.D. Valencia. On infinite csp's. In *Proc. Third International CP'05 Workshop on Modelling and Reformulating CSP's*, 2005.

[6] Rocco DeNicola, Gianluigi Ferrari, Ugo Montanari, Rosario Pugliese, and Emilio Tuosto. A process calculus for qos-aware applications. In *Coordination 2005*, volume 3454 of *Lectures Notes in Computer Science*. Springer, 2005.

[7] Gianluigi Ferrari, Ugo Montanari, Emilio Tuosto, Björn Victor, and Kidane Yemane. Modelling fusion calculus using hd-automata. In *To appear in In First Conference on Algebra and Coalgebra in Computer Science CALCO'05*, LNCS. Springer, 2005.

[8] Alberto Lluch-Lafuente and Ugo Montanari. Quantitative μ-calculus and ctl defined over constraint semirings. In *QAPL (2005)*, Electronic Notes in Computer Science, pages 1–30. Elsevier, 2005.

[9] Marino Miculan and Kidane Yemane. A unifying model of variables and names. In *Proceedings of FoSSaCS 2005*, Lecture Notes in Computer Science. Springer Verlag, April 2005.

Papers Submitted for Publication, Reports, Drafts

[10] Y. Deng and D. Sangiorgi. Ensuring termination by typability. Submitted, 2005.