Information Societies Technology (IST) Programme

Future and Emerging Technologies - Open Domain

Project acronym: Advance

Project full title:

Advanced Validation Techniques
for Telecommunication Protocols

Contract no: IST-1999-29082

Deliverable 19

Progress Report

Year 3 : October 2002 - January 2004

Date of preparation: January 2004

Contributors: all groups

Edited by: Ahmed Bouajjani, University of Paris 7

Part A
Executive summary

1 Work progress and achievements

The main achievements obtained during the third year of the project are the following:

1.1 Symbolic reachability analysis of extended automata

1. Development of widening techniques on automata-based symbolic representation structures (NDDs and RVAs) and their use in the verification of infinite-state models such as counter automata and timed/hybrid automata.

2. Development of a generic framework for the abstract analysis of systems of communicating pushdown automata, a natural model for concurrent programs with recursive procedure calls. The proposed framework allows to combine the automata-based techniques for symbolic reachability analysis of pushdown automata with abstract interpretation in order to compute abstractions of sets of computations paths.

1.2 Verification of parametrized networks and dynamic systems

1. Improvements of the algorithmics behind the different approaches for computing transitive closures in regular model-checking (state-space collapsing techniques on transducers, or widening techniques on automata-based representations).

2. Development of powerful methods for the verification of both safety and liveness properties of parametrized networks of processes (including probabilistic systems) combining abstraction, proof methods, and model-checking techniques.

3. Design of (tree automata-based) symbolic reachability analysis of programs with dynamic creation of processes and procedure calls modeled by means of a special kind of term rewrite systems (Process Rewrite Systems).

4. Design of a framework for the abstract analysis of programs with dynamic creation of processes and procedure calls, extending the framework defined for communicating pushdown automata (mentioned in the previous subsection) to the case of dynamic systems.

5. Design of new specification and verification techniques for programs with dynamic memory (creation and deletion of objects, pointer manipulation, etc).

1.3 Tool development and integration

An important effort has been devoted to the improvement and the development of new techniques in our tools.

1. New developments in the algorithmics for symbolic reachability analysis in the tool LASH by implementing widening techniques on automata. Release of the new library of RVA (automata-based representation for the first-order arithmetics over reals and integers without multiplication).

2. Improvement and development of new libraries for symbolic representation of different classes of arithmetical constraints in the tool TReX (new library for parametric different bound matrices, parametric interval constraints). New release of TReX.

3. Integration in TReX of external libraries for interval constraints and upward-closed constraints (developed by the university of Brussels). These libraries are being integrated in the implementation of new reachability analysis procedures where different representations are used at different level of abstraction during the same analysis, and where the level of abstraction is refined by need (*lazily*) when false counterexamples are detected during the search. Also, the new RVA library developed by Liège is being used by the group of Paris in the implementation of new reachability analysis techniques, in particular for the model of unbounded timed Petri nets with urgency constraints.

4. Development of a new version of TLV where combinations of abstraction, proof, and (regular) model checking techniques can be done. The new tool uses a connection to the PVS theorem prover developed at SRI.

5. Improvement of the integration of the tools RMC and TLV for the verification of parametrized networks in the common IF-based verification environment.

1.4 Cases studies and experimentations

We have used our tools in several experimentations with nontrivial case studies. These experimentations show the applicability of our techniques and tools, and show also their complementarity.

1.4.1 Parametric constraint synthesis

We have been able to synthesize automatically the constraints relating several parameters of two complex protocols which guarantee their correction w.r.t. significant properties.

1. Parametric analysis of the PGM protocol has been carried out automatically using the tool TReX.

2. Parametric analysis of the IEEE1394 Root Contention Protocol using the tool LASH.

1.4.2 Automatic verification of parametrized algorithms

Several experiments have been carried out with the new TLV version tool. These experiments concern the verification of liveness properties of nontrivial parametrized algorithms such as the Lehman and Rabin's Courteous Philosophers algorithm. The verification of such properties is beyond the scope of the other tools in the project (such as LASH or TReX).

2 Dissemination of results

2.1 Publications

Results obtained by our project have been published/presented this year (or have been accepted for publication) in the following international conferences (in chronological ordering) and journals:

- Intern. Conf. on Tools and Algorithms for the Construction and Analysis of Systems *TACAS'03*, March 2003, Warsaw, Poland,

- *FOSSACS'03*, April 2003, Warsaw, Poland,

- Intern. Conf. on Computer Aided Verification *CAV'03*, July 2003, USA,
- Intern. Symp. on Computer Science Logic *CSL'03*, August 2003, Vienna, Austria,
- Intern. Conf. on Concurrency Theory *CONCUR'03*, September 2003, Marseilles, France,
- Intern. Workshop on Partial Evaluation and Semantics-Based Program Manipulation *PEPM'03*, San Diego, USA,
- Intern. Symp. of Formal Methods Europe *FME'03*, September 2003, Pisa, Italy,
- Intern. Conf. on Foundations of Software Technology and Theoretical Computer Science *FST&TCS'03*, December 2003, Mumbay, India,
- Inter. Workshop on Verification, Model Checking, and Abstract Interpretation *VMCAI'04*, January 2004, Venicia, Italy,
- Intern. Symp. on Principles of Programming Languages *POPL'04*, January 2004, Venicia, Italy.
- Intern. Conf. on Tools and Algorithms for the Construction and Analysis of Systems *TACAS'04*, March 2004, Barcelona, Spain.
- Intern. Journal of Foundations of Computer Science *JFCS*, World Scientific Pub.,
- Intern. Journal on Software Tools for Technology Transfer *STTT*, Springer Pub.

2.2 Seminar and Workshop organization:

- The last meeting of the project was organized as an open workshop with the invited speakers: Shaz Quadeer (Microsoft research), John Rushby (SRI), Jean-François Raskin (Univ. of Brussels),
- France Telecom R&D (Yves-Marie Quemener) has presented the results obtained in the ADVANCE project in the framework of the annual presentation of the research done in the field of security analysis of software. The presentation took place in December 2003, The attendence was coposed of FT R&D experts in security, researchers and ingeneers in the "Direction de la Scurit" of the FT R&D group, ingeneers from the "Centre National de Scurit Informatique" of the "Direction of Information Systems" of France Telecom, and also from Orange Suisse.
- A presentation of the results of ADVANCE by the participants of the project is planned in the framework of "College France Telecom" in the second trimester of 2004. "College France Telecom" consists of seminars organized by France Telecom R&D each year for the leading managers of France Telecom. The seminar of 2004 will be on the subject of "Formal Methods for the Dependability of Software Systems".

3 Coordination and Management

3.1 Internal meetings, visits, and cooperations

- Two project meetings (march 2003, and January 2004),
- Axel Legay from Liège visited Paris, collaboration between Paris (Ahmed Bouajjani) and Liège (Axel Legay and Pierre Wolper),

- Axel Legay from Liège visited Uppsala, collaboration between Liège (Axel Legay) and Uppsala (Parosh Abdulla and Marcus Nilsson)
- Ahmed Bouajjani visited Grenoble (Yassine Lakhnech),
- Invitation of Markus Müller-Olm (from Dortmund) by Paris, coopération with Ahmed Bouajjani and Tayssir Touili,
- Invitation of Barbara König (from Stuttgart) by Paris.

3.2 Management of the project

The table below describes the manpower (Paid/Non paid persons-months effort) used by the partners of the project.

Participant	**WP1**	**WP2**	**WP3**	**Total**
(**UP7**)	15 / 5	12 / 5	1 / 2	28 / 12
(**F-Telecom**)	3	2	1	6
(**Liège**)	7.9 / 1.4	3.1 / 2.0	0/0.4	11 / 3.8
(**UEdin**)	10/3	2/1	0/0	12/4
(**Uppsala**)	8/5	4/1	0/1	12/7
(**UJF**)	8	8	1	17
(**Weizmann**)	6/1.5	4.6/1.3	0 / 0.5	10.6 / 3.3
	57.9/15.9	35.7/10.3	3/3.9	96.6/30.1

There was no major deviations from the expected effort defined in the original proposal. France Telecom spent more effort than planned (6 instead of 4) since they have started an activity in the third year around the verification of security properties in dynamic software systems. This increase in the effort compensates the fact that they have spent 6 months in two last years instead of the planned 8 months.

Part B

Achievements per Working Package

1 WP1: Methods and tools

1.1 Task T1.1: Abstraction

1.1.1 Liveness properties for parametrized networks

In [APZ03, PA03, FPPZ04], powerful methods for the verification of parametrized networks of processes have been defined, implemented, and experimented on nontrivial examples. Theses methods are based on combining abstraction techniques with proof principles and model-checking algorithms.

1.1.2 Resource management systems

In [BHV03], decidability results are established concerning the model-checking of parametric networks of processes competing for a set of shared resources. These results are based on cut-off properties allowing to reduce parametric verification problems to finite numbers of finite-state model-checking problems. This study was motivated by a case study furnished by Ericsson.

1.1.3 Multicast protocols

In [EM03], cut-off properties are established for the parametric verification of a class of multicast protocols with tree-like topologies. This study was motivated by the PGM case study furnished by France Telecom.

1.1.4 Communicating pushdown systems

In [BET03], a generic approach to the static analysis of concurrent programs with procedures is developped. Programs are modeled as communicating pushdown systems. This work proposes an algebraic framework for defining abstractions (upper approximations) of sets of computation paths, combining automata theoretic techniques with algorithms for solving systems of polynomial inequations in Kleene algebras.

1.1.5 Verification of Java code

Abstraction techniques combined with model-checking techniques have been used in France Telecom R & D to analyse security properties (absence of illegal access to critical methods) on Java programs.

1.2 Task T1.2: Symbolic methods

1.2.1 Regular Model Checking

In [AJNd03], several improvements of the earlier techniques are developed, leading to a simpler theoretical framework as well as to a more efficient algorithm for computing transitive closures of regular transducers.

In [BLW03], a widening technique on finite-word automata is introduced and used in the automata-based symbolic reachability analysis of (integer) counter systems. This work is extended to the case of infinite-word automata in [BLW04] and applied to the reachability analysis of timed/hybrid systems (systems with real valued variables).

The proposed techniques are shown to be more powerful in some cases than the existing acceleration techniques for numerical models (extended automata with integer/real valued variables) based on computing transitive closures of single operations (guarded commands).

1.2.2 Process Rewrite Systems

The paper [BT03] introduces new symbolic reachability analysis techniques for a class of models (based on term rewrite systems) for programs with dynamic creation of concurrent processes and recursive procedure calls. The considered models, called Process Rewrite Systems (PRS), subsume pushdown automata and Petri nets. Our techniques allow to define automata-based techniques for the verification of significant classes of programs. These techniques unify and generalize the existing techniques concerning this kind of models.

1.2.3 Systems with dynamic memory

The paper [BIL03] introduces a logic allowing to specify heap properties of programs with dynamic memory structure and address decidability issues related to the verification of such properties.

1.2.4 Tool development

Several teams have devoted a important effort in the implementation of the new developed techniques and algorithms:

1. The group of Liège has improved the LASH tool by implementing *hybrid acceleration* techniques which allow to tackles the analysis of heterogeneous systems modeled by finite-state machines extended with unbounded integer variables and unbounded real clocks. In particular, the widening techniques proposed in the papers [BLW03, BLW04] have been implemented and shown to be efficient w.r.t. the existing techniques.

2. A new release of the tool TReX has been produced with a modular architecture designed in order to be able to integrate easily new libraries of symbolic representations and corresponding procedures for state-space exploration/generation.

3. The group of Uppsala has considerably improved the efficiency of his tool RMC by implementing new techniques for Regular Model Checking published in [AJNd03].

4. The group of Weizmann Inst. has developed a new version of TLV allowing the combination of abstraction, proof, and model-checking techniques (finite-state model checking as well as regular model checking for infinite-state verification). The tool is connected to the PVS theorem prover.

1.3 Task T1.3: Efficient state-space exploration

The paper [Ios03] addresses the problem of verifying dynamic concurrent systems. Efficient model checking techniques are defined for these systems based on symmetry and partial-order reductions.

2 WP2: Integration of tools and Experimentations

2.0.1 Tasks T2.1/T2.2: Common language and interface/Integration of tools

- Improvement of the integration of the tools TLV and RMC in the common verification environnement. The improvement consists on taking into account a larger fragment of the IF language allowing to specify parametrized networks of processes.

Examples of parametrized systems such as mutual exlusion protocols of Burns, Szymanski, Peterson, etc, can be described in the common language which can be handled by both tools.

- Libraries for the representation of various specific classes of arithmetical constraints have been integrated in TReX (essentially, libraries for handling upward-closed sets, and interval constraints). The RVA library developed by LASH is also being used in a prototype which will be part of the next release of TReX (allowing the analysis of timed Petri nets with urgent transitions).

2.1 Task T2.3: Experimentations and case studies

This year the effort concerning this task was to show the applicability of our symbolic reachability analysis techniques in parametric analysis of significant case studies, and in particular in automatic synthesis of parameter constraints, and in checking liveness properties for parametrized algorithms. In all cases, the obtained results are the state-of-the-art in the verification of the considered systems.

2.1.1 PGM

The team of Paris devoted an important effort in improving the tool TReX in order to tackle the case PGM case study. The team was able to extend the result obtained in the second year by (1) deriving accurate constraints on the parameters which guarantee the correctness w.r.t. non trivial properties [BS03, ADV04], and (2) using TReX in order to generate automatically these constraints [ADV04].

2.1.2 IEEE Root Contention Protocol

The group of Liège considered the case study of the IEEE Root Contention Protocol. Starting from a model which was previousely designed and studied by the group of Paris, the group was able to use LASH for (1) the generation of the state-space of a model of the RCP which can be used for checking various properties such as reachability of specific control points, deadlocks, etc., and (2) the synthesis of parameter constraints allowing to satisfy some relevant safety properties [ADV04].

2.1.3 Parametrized algorithms

The team of Weizmann Inst. tackled the verification of several nontrivial examples of parametrized algorithms such as mutual exlusion protocols, and systems with shared resources. They have been able to prove automatically difficult properties (liveness properties) for nontrivial instances of such systems [APZ03, PA03, FPPZ04].

3 WP3: Project management / assessment

3.1 Task T3.1: Management and coordination

See the Executive Summary (Part A of the report).

3.2 Task T3.2: Assessment and quality control

3.2.1 Self-assessment criteria

We consider the self-assessment criteria defined in the technical annex describing the work in the project.

1. **Production of theoretical and applied results on methodology and validation techniques:** The evaluation criteria used for this work are the technical level and its scientific value, (selectivity of the conferences and journals), the relevance to the project and the proved and/or potential wide range of applications, and the quality of the dissemination (scientific quality and level of diffusion of the conferences and journals, variety of addressed communities). We consider that a minimal contribution of each (academic) participant should be at least one high quality publication per year.

2. **Construction of validation tools and their integration:** We consider as minimal success criterion the production of a validation environment where validation techniques for *infinite-state extended automata* (e.g. automata with counters, clocks, and FIFO-channels) are available. Further steps we intend to reach consists in the extension of this environment in order to deal also with (1) *parametrized systems* (e.g., networks with unbounded number of components, parametric timed automata, etc), and (2) *dynamic networks* and *mobile processes*. Those are highly exploratory (and hence risky) steps. We will consider as a success any progress toward the development of new methods, techniques, and prototype tools for dealing with these kinds of systems.

3. **Applications and experimentations:** We consider as minimal success criterion showing the application of our techniques and tools to nontrivial cases. The main success criterion we consider here is the power of our methods, techniques, and tools from the *qualitative* point of view: showing that our approach allows to tackle in a systematic way classes of systems that are, by nature, beyond the scope of the existing approaches. The second criterion we consider is the power of our techniques from the *quantitative* point of view: showing that our techniques allow to deal with cases of important sizes. The main objective of our work on case studies is indeed to experiment and to evaluate our techniques and tools according to the criteria above.

3.2.2 Achievements in the third year of the project

Results on methodology and validation techniques: The research has produced both theoretical and applied works with high technical level and scientific value. The main results obtained this year concern (1) new techniques for regular model checking improving the applicability and the efficiency of the existing tools, (2) new algorithms for parametrized networks (networks of timed automata, multicast protocols, systems for shared resources management, etc) and dynamic systems (multithreaded programs, concurrent programs with dynamic memory, etc), (3) new methods for the verification of liveness properties of parametrized networks based on combining abstraction, proof, and model-checking techniques.

We consider that the quality of the obtained results is quite satisfactory, and that our objectives for this year concerning the production of verification methods and algorithms (especially for parametrized and dynamic systems) were realized.

Construction of validation tools and their integration: We have extended the capabilities of the our tools and released new versions with improved performances and range of applications. The effort of this year concern the following points:

- The tools TReX and LASH have been upgrated by the implementation of new libraries of symbolic representation and new algorithms for symbolic reachability analysis.
- The tool TLV has also been improved by integrating abstraction, proof, and model-checking techniques, using a connection to the tool PVS (developed at SRI).
- The tools TLV and RMC for the verification of parametrized systems have been connected to the IF environment through interfaces with the IF language.

The improvements and the new developments introduced in our tools allowed to tackle complex verification problems and nontrivial cases studies.

Applications and experimentations: An important effort has been devoted this year to the parametric analysis of complex protocols and algorithms. The main achievements are:

- Automatic synthesis using TReX of constraints on the parameters of the PGM protocol allowing to guarantee the full recovery property. These constraints are quite complex and involve parameters such as the size of the buffers, the propagation delays, the rate of losses in the channels, etc.
- Parametric analysis of the IEEE1394 route contention protocol using LASH. This analysis required the extension of LASH with new representation structures allowing to deal simultaneously with integer and real variables. This work is a continuation of an earlier analysis which was performed using TReX (in the first year of the project).
- Automatic verification of non trivial parametrized algorithms including probabilistic algorithms such as Lehman and Rabin's Courteous Philosophers algorithm. This was possible using the powerful approach developed in TLV based on combining abstraction, proof, and model-checking techniques.

Carrying out these experimentations allowed to improve significantly our tools and to develop new methods and verification techniques.

3.3 Task T3.3: Dissemination and transfer activities

Publications: We have published and/or presented our results in major conferences related to the topics of the project: CAV, TACAS, CONCUR, CSL, POPL, FME, FSTTCS, FOSSACS, PEPM, VMCAI. These conferences target several different research communities such as formal methods, computer-aided verification, concurrency theory, abstract interpretation, static analysis, software validation, programming languages, automata, logic, etc. All the articles produced in our project can be found at:

`http://www.liafa.jussieu.fr/~haberm/ADVANCE/main.html`

Seminar and Workshop organization:

- The last meeting of the project was organized as an open workshop with the invited speakers: Shaz Quadeer (Microsoft research), John Rushby (SRI), Jean-François Raskin (Univ. of Brussels),
- France Telecom R&D (Yves-Marie Quemener) has presented the results obtained in the ADVANCE project in the framework of the annual presentation of the research done in the field of security analysis of software. The presentation took place in December 2003, The attendence was coposed of FT R&D experts in security, researchers and ingeneers in the "Direction de la Scurit" of the FT R&D group, ingeneers from the "Centre National de Scurit Informatique" of the "Direction of Information Systems" of France Telecom, and also from Orange Suisse.
- A presentation of the results of ADVANCE by the participants of the project is planned in the framework of "College France Telecom" in the second trimester of 2004. "College France Telecom" consists of seminars organized by France Telecom R&D each year for the leading managers of France Telecom. The seminar of 2004 will be on the subject of "Formal Methods for the Dependability of Software Systems".

References

[ADV04] ADVANCE. Case studies: PGM protocol, IEEE1394 root contention protocol. Technical report, University of Pari7 and France Telecom R&D, 2004.

[AJNd03] Parosh Aziz Abdulla, Bengt Jonsson, Marcus Nilsson, and Julien d'Orso. Algorithmic improvements in regular model checking. In *Proc.* 15^{th} *Int. Conf. on Computer Aided Verification (CAV'03)*, volume 2725 of *Lecture Notes in Computer Science*, 2003.

[APZ03] T. Arons, A. Pnueli, and L. Zuck. Parameterized verification by probabilistic abstraction. In *Proc. Intern. Conf. on Foundations of Software Science and Computation Structures (FOSSACS'03)*, volume 2620 of *Lecture Notes in Computer Science*, 2003.

[BET03] Ahmed Bouajjani, Javier Esparza, and Tayssir Touili. A generic approach to the static analysis of concurrent programs with procedures. In *30th Symp. on Principles of Programming Languages (POPL'03)*, pages 72–73. ACM Pub., 2003. Full version in the Intern. Journal of Foundations of Computer Science, volume 14, No 4, August 2003.

[BHV03] Ahmed Bouajjani, Peter Habermehl, and Tomas Vojnar. Verification of parametric concurrent systems with prioritized fifo resource management. In *Proc.* 14^{th} *Int. Conf. on Concurrency Theory (CONCUR'03)*, volume 2761 of *Lecture Notes in Computer Science*, pages 174–190, 2003.

[BIL03] M. Bozga, R. Iosif, and Y. Lakhnech. Storeless Semantics and Alias Logic. In *Proceedings of PEPM'03 Workshop - Partial Evaluation and Semantics-Based Program Manipulation*, SIGPLAN. ACM, 2003.

[BLW03] Bernard Boigelot, Axel Legay, and Pierre Wolper. Iterating transducers in the large. In *Proc.* 15^{th} *Int. Conf. on Computer Aided Verification (CAV'03)*, volume 2725 of *Lecture Notes in Computer Science*, pages 223–235, 2003.

[BLW04] Bernard Boigelot, Axel Legay, and Pierre Wolper. Omega-regular model checking. In *Proc. TACAS '04,* 10^{th} *Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems*, Lecture Notes in Computer Science, 2004.

[BS03] Marc Boyer and Mihaela Sighireanu. Synthesis and Verification of Constraints in the PGM Protocol. In *FME'03*, volume 2805 of *Lecture Notes in Computer Science*, 2003.

[BT03] Ahmed Bouajjani and Tayssir Touili. Reachability Analysis of Process Rewrite Systems. In *Proc. Intern. Conf. on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'03)*, Lecture Notes in Computer Science, Mumbai, India, 2003.

[EM03] J. Esparza and M. Maidl. Simple representative instantiations for multicast protocols. In *Proc. TACAS '03,* 9^{th} *Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems*, volume 2619 of *Lecture Notes in Computer Science*, pages 128–142, 2003.

[FPPZ04] Y. Fang, N. Piterman, A. Pnueli, and L. Zuck. Liveness with invisible ranking. In G. Levi and B. Steffen, editors, *Proc. of the $5^t h$ workshop on Verification, Model Checking, and Abstract Interpretation*, Lecture Notes in Computer Science, 2004. To appear.

[Ios03] Radu Iosif. Symmetry reductions for model checking of concurrent dynamic software. *Software Tools for Technology Transfer, STTT*, 2003.

[PA03] A. Pnueli and T. Arons. TLPVS: A PVS-based LTL verification system. In Nachum Dershowitz, editor, *Verification–Theory and Practice: Proceedings of an International Symposium in Honor of Zohar Manna's 64th Birthday*, volume 2772 of *Lecture Notes in Computer Science*, pages 601–628, 2003.