Information Society
Technologies

ARTIST2 – Year 1 Review

Grenoble, October 3rd-4th, 2005

Platform

Platform for Testing and Verification

Activity leader : Kim G Larsen (Aalborg U, DK)

Outline of the Presentation

Industrial Needs and Experience

Year 1 Activities

- 18 month objectives

- Achievements and ongoing work

- Interaction and Building Excellence Between Partners

18 Month Perspective

- Work planned for the next 18 months

Industrial Needs and Experience

❖ **INDUSTRIAL NEEDS:**

30-40% of production time is currently spend
on elaborate, ad-hoc testing

➢ The potential of existing/improved
testing methods and tools is enormous

➢ Especially important and **challenging** for embedded systems

❖ **AIM**

➢ Continued effort: on development of tools owned by cluster participants.

➢ Easy overview: of academic state-of-the-art tools, there domain of applicability, features, successful applications, etc.

➢ Increase scalability: Price of PC-cluster technology is going down and should be utilized in scaling up verification and analysis of models.

➢ Coordination: Realization of a European Verification Grid.

Activities – T&V Platform
18 month objective

Original

❖ **A. Testing and Verification Server:**

➢ **T0+06:**
Evaluation of main testing and verification tools wrt maturity for integration.

➢ **T0+18:**
Installed and configured (virtual) server containing main testing and verification tools, e.g.:
  – SPIN, SMV, UPPAAL, Kronos, Blast, TorX, TGV, FAST, CADP, IF
  – HyTech, visualSTATE, TAU, LASH, EMTCC, Rapture, ..

❖ **B. Parallel and Distribution Model Checking (PDMC):**

➢ **T0+6:**
Evaluation of tools currently supporting PDMC on local PC-clusters.

➢ **T0+18:**
Design of coordination layer for integrating PDMC methods.

❖ **C. European Test and Verification GRID**

➢ **T0+6:**
Preevaluation of UPPAAL running on NORDUGRID

➢ **T0+18:**
Design of GRID infrastructure with links to national as well as European GRID activities.

Year 1 activities
Achievements & Ongoing Work

❖ **Work on individual tools:**

➢ New version of TGV (based on on-the-fly enumerative algorithms) linked to the IF toolbox (Verimag) has been developed using STL libraries (in place of CADP libraries) (IRISA)

➢ Extensions of real-time model checker UPPAAL with C-code (Aalborg)

➢ Development of IF tool-suit (Verimag)

➢ Support of the verification tool LASH and hosts powerful servers dedicated to verification (CFV)

➢ Linking between MoDEST/MOTOR and UPPAAL (Twente/Aalborg)

➢ DiVinE (Brno) has been extended with a Promela front-end for SPIN compatible distributed model checking.

➢ Development of UPPAAL Cora for optimal planning and scheduling (Aalborg)

➢ Development of UPPAAL Tron for real-time testing (Aalborg)

➢ Development of TIMES for schedulability analysis (Uppsala)

Year 1 activities
Achievements & Ongoing Work

❖ **Work on Web-based Repository of Tools:**

YAHODA, Verification Tools Database

Year 1 activities
Achievements & Ongoing Work

❖ **Work on Web-based Repository of Tools:**

YAHODA, Verification Tools Database

Year 1 activities

❖ **W**
D
C

Year 1 activities
Achievements & Ongoing Work

❖ **Work on Parallel and Distributed Model Checking**

➤ Application of Distributed UPPAAL
to Leader Election Algorithm for
Mobile Ad-hoc Networks by
Leslie Lamport (1 year effort).

(1,2,0,1)

(2,1,0,1)
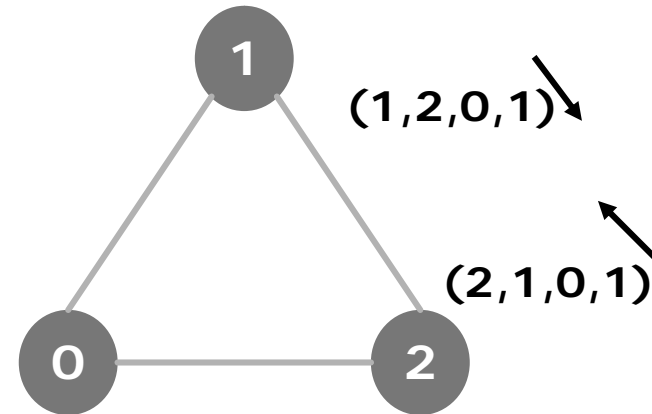
(id,dest,id.lead,id.hops)

Leslie Lamport

```
All,

Thanks for the spec.
It seems to run fine.
As expected, it's 2
or 3 orders of
magnitude faster than
TLC.  I'm wondering
if your algorithms
could be  used for
checking specs
written in a higher
level  language like
TLA+.
```

Year 1 activities
Interaction & Building Excellence

❖ Tutorials and tool presentations given at several conferences, workshops and schools: *eg*

  ➢ Embedded World Nürnberg

  ➢ ARTIST2 summerschool

  ➢ RTSS05

  ➢ TECS06

❖ Several exchange visits between Brno and Aalborg University.

❖ Steering committee membership and invited presentations at PDMC workshop (ICALP2005).

18 Month Perspective
Work Planned for the next 18 months

❖ Extend Yahoda Database with testing tools and links to repository for case studies.

❖ Continue effort on individual tools.

❖ Extend parallel and distributed model checking capabilities from safety to liveness properties.

❖ Initiative effort on Parallel and Distributed Methods for Verification and Performance Evaluation
with European Teams outside the cluster
November 16-17, 2005,
INRIA Rhone-Alpes (Grenoble) .

Jiri Barnat (Masaryk Univ. Brno)
Gerd Behrmann (Aalborg Univ.)
Stefan Blom (Univ. of Innsbruck)
Jeremy Bradley (Imperial College)
Lubos Brim (Masaryk Univ. Brno)
Ivana Cerna (Masaryk Univ. Brno)
Hubert Garavel (INRIA Rhone-Alpes)
Boudewijn Haverkort (Univ. Twente)
Christophe Joubert (INRIA Rhone-Alpes)
Josva Kleist (Aalborg Univ.)
William Knottenbelt (Imperial College)
Martin Leucker (TU Munich)
Radu Mateescu (INRIA Rhone-Alpes)
Jaco van de Pol (CWI)
Michael Weber (Aachen and CWI)
X (Twente U)

Activities – T&V Platform
18 month objective

Modified

❖ **A. Testing and Verification Server:**

➢ **T0+06:**
Evaluation of main testing and verification tools wrt maturity for integration.

➢ **T0+18:**
~~Installed and configured (virtual) server containing main testing and verification tools~~
Link from Yahoda to easy downloadable versions of **mature** and **stable** versions of tools with links to common repository of successful case studies.

❖ **B. Parallel and Distribution Model Checking (PDMC):**

➢ **T0+6:**
Evaluation of tools currently supporting PDMC on local PC-clusters.

➢ **T0+18:**
(Initiate) Design of coordination layer for integrating PDMC methods.

❖ **C. European Test and Verification GRID**

➢ **T0+6:**
Preevaluation of UPPAAL running on NORDUGRID

➢ **T0+18:**
Design of GRID infrastructure with links to national as well as European GRID activities.

END

☺ ☺☺☺

Schedule & Milestones

Joint Cluster Meeting (w. parallel sessions) medio December

Quantitative Testing & Verification

A. Foundation for black-box testing of real-time systems established
   T0+6:
   a. Soundness and limit-completeness
   b. Metric for coverage.
   T0+18:
   a. ~~Computability and Complexity of learnability.~~
   b. Robustness and Implementability

B. Improved tools for quantitative analysis with experimental evaluation
   T0+6:
   a. Improved symbolic datastructures
   b. Heuristics for efficient guiding
   T0+18:
   a. Abstraction methods
   b. Comparison with (MI)LP and OR
   c. Stochastic Model Checking
   d. Controller Synthesis

C. Industrial case studies.
   T0+6:
   Collection of case studies on web.
   T0+18:
   Classification of case studies

Verification of Security Properties

A: Cryptographic protocols
   T0+6:
   a. A common language for security protocols
   b. A publicly available data base of security protocols and their analysis (attacks, proofs, assumptions/properties,...)
   T0+18:
   a. A validation tool set that is accessible via the web.
   b. Two industrial case studies that are already available.

B: Certification technology and virtual machine validation
   T0+6:
   A methodology for certification of the levels EAL6 and EAL7 of the common criteria.
   T0+18:
   A (prototype) tool set for certification of the levels EAL6 and EAL7 of the common criteria.

Testing & Verification Platform

A. Testing and Verification Server:
   T0+06:
   Evaluation of main testing and verification tools wrt maturity for integration.
   T0+18:
   ~~Installed and configured (virtual) server~~
   Links to mature/stable versions

B. Parallel and Distribution Model Checking (PDMC):
   T0+6:
   Evaluation of tools currently supporting PDMC on local PC-clusters.
   T0+18:
   (Initiate) design of coordination layer for integrating PDMC methods.

C. European Test and Verification GRID
   T0+6:
   Preevaluation of UPPAAL running on NORDUGRID
   T0+18:
   Design of GRID infrastructure