Projet IOP
Intégration d'outils à CosyVerif

Étienne André, Fabrice Kordon, Alban Linard, Laure Petrucci

Etienne.Andre@univ-paris13.fr, Fabrice.Kordon@lip6.fr, Alban.Linard@lsv.ens-cachan.fr,
Laure.Petrucci@lipn.univ-paris13.fr

11 juin 2014

CosyVerif

Motivation

Dissemination of Verification Tools

- Application of formal methods to dedicated cases studies
- Towards technological transfer to industry
- Tools organised around formalisms

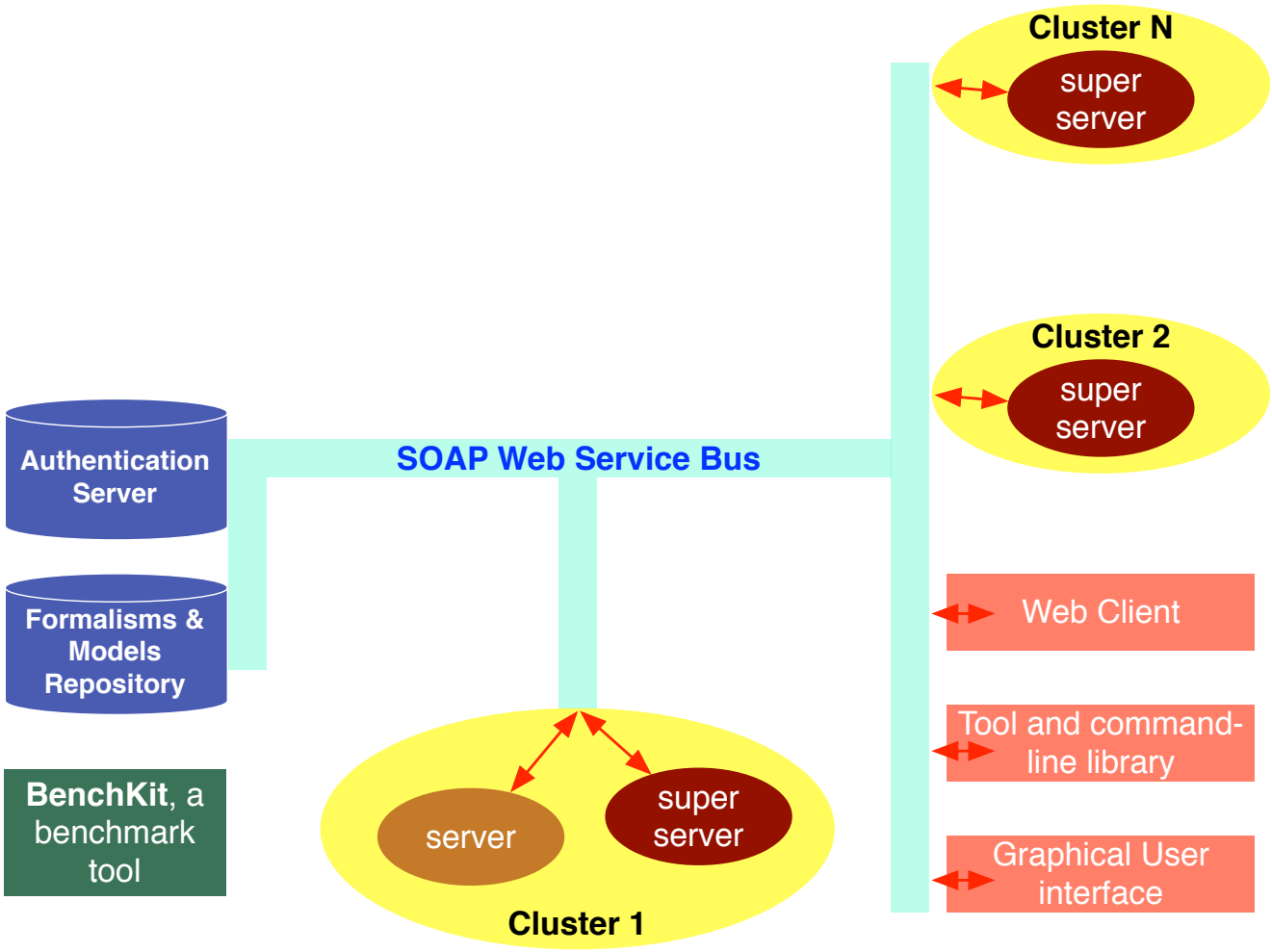
Academics $\neq$ Developers 

- Need to share effort (platform, interfaces, distribution mechanisms)
- Need to share definitions (typically formalisms)
- Coordinated effort to better handle a complex context of interrelated formal notations
  - Variants of Petri nets
  - Variants of automata
  - etc.

Principles of the *CosyVerif* platform

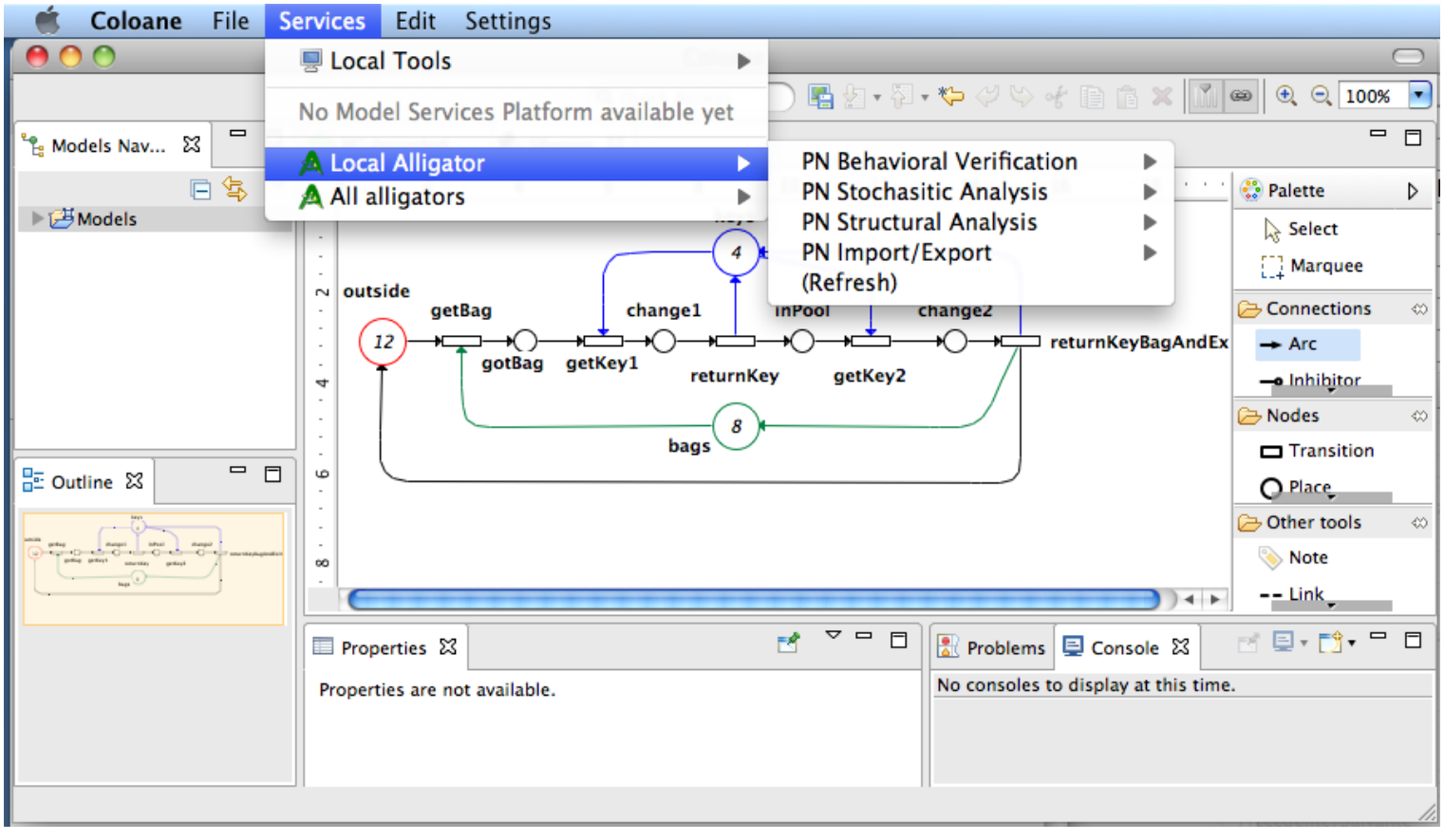
- Distributed and open [AHHKLLP13]
  - Developed at ENS Cachan, Paris 13, UPMC, etc.
- Supports different families of formalisms
  - automata
  - Petri nets
- 12 concrete formalisms
- 2-layered XML-based description language: [ABDHHKLP13]
  - FML, Formalism Markup Language (modelling language description)
  - GrML, Graph Markup Language (actual model description)
- Reuse of existing formalisms
- Open to new tool contributions
- Tools invoked through web services transparent to the user
- Graphical user interface: Coloane
- Repository of models

The *CosyVerif* Architecture



The *Coloane* User Interface

The *Coloane* User interface (Graphical client)



Command-line client is also available for script-based access to tools

Formalisms and Tools

Formalisms	Tools	
Petri Nets	PROD (Univ. Helsinki, Symmetric nets)	
	PNXDD (LIP6, Symmetric nets)	[Kordon et al., 2012]
	Crocodile (LIP6, Symmetric nets w. bags)	[Colange et al., 2011]
	Cunf (LSV, P/T nets)	[Baldan et al., 2012]
	Cosmos (LSV, Stochastic Petri nets)	[Ballarini et al., 2011]
	GreatSPN invariants (Univ. Torino, P/T nets)	
	Helena (LIPN, HL nets)	[hel, 2014]
	ModGraph (LIPN, HL nets)	[Lakos and Petrucci, 2004]
	ObsGraph (LIPN, HL nets)	[Klai and Ochi, 2012]
	Structural bounds (LIP6, P/T nets)	
	Unfold into P/T nets (LIP6, Symmetric nets)	
	Various exports (LIP6, P/T nets)	
Automata	Imitator (LIPN, Timed automata)	[André et al., 2012]
	Modgraph (LIPN, Synchronised automata)	[Lakos and Petrucci, 2004]

Goal of the GDR GPL Project

Goals

1. Integrate more tools into the *CosyVerif* platform
2. Establish an integration procedure that will benefit for other tools to be integrated in *CosyVerif*

Use of the fundings: 2 interns hired:

- Henoc Khouilla (LIPN)
- Idrissa Sokhona (LIP6)

Integration of GreatSPN

Tool for invariant computation for Petri nets

Status before the work

- Not integrated, but integrated into CPN-AMI (ancestor of *CosyVerif*)

Work achieved

- Integrating the functions of the tool (Place invariants, Transition invariants, Minimal syphon, Minimal traps)
- Translating the internal *CosyVerif* format into the one of CPN-AMI, thus enabling the reuse of the previous translators
- Testing and benchmarking was done to access the new integration's results compared to ones provided by CPN-AMI

Integration of ModGraph

Tool for construction and analysis of modular state spaces [Lakos and Petrucci, 2004]

Status before the work

- Previously integrated in *CosyVerif*, but it provided only a poor user interface

Work achieved

- Upgrade the ModGraph service to the latest version of the tool;
- Enhance the user interface provided by the service.

Integration of ObsGraph

BDD-based tool implementing a verification approach for workflows using Symbolic Observation Graphs [Haddad et al., 2004, Klai and Ochi, 2012]

Status before the work

- Previously integrated in *CosyVerif*, but it provided only a poor user interface

Work achieved

- Upgrade the ObsGraph service to the latest version of the tool;
- Enhance the user interface provided by the service;
- Upgrade the service by interaction with the tool developer, for instance the addition of new services above the ObsGraph tool.

Integration of Helena

Explicit state model checker (a High-level Petri net is used for models) [hel, 2014]

Status before the work

- Not integrated

Work achieved

- First attempt to the integration of Helena in *CosyVerif*
- A prototype was obtained, but not polished enough to be released yet. (Integrating Helena is difficult because a translation from the *CosyVerif* model format to Helena's one must be defined.)

Teaching Experience Report

[A., Kordon, Petrucci, 2014]

Univ. Pierre & Marie Curie

- course attended by 25 students
- students had to provide a small individual project as homework
- only issue (first practical session only, since patch was then provided): misuse of the permissions leading to a crash, due to Eclipse embedded libraries for Coloane
- students downloaded the bundle and provided their project on time

Univ. Paris 13

- course attended by 20 students
- anonymous aftercourse evaluation
- 87% satisfied or very satisfied by their experience

Recent and Ongoing Evolutions

- Asynchronous tool invocation
  - Get the result later (e.g. by email)
- Federation of servers and use of clusters
  - Enable load balancing
- Repository of formalisms and models
- Command-line version of the underlying platform

Future Evolutions

- Enhanced interaction between tools
  - Output of a tool as input of another one
- Handling semantics (bridges between formalisms)
  - Also allows system simulation
- Handling heterogeneous models (mixing different formalisms)

Future Evolutions

- Enhanced interaction between tools
  - Output of a tool as input of another one
- Handling semantics (bridges between formalisms)
  - Also allows system simulation
- Handling heterogeneous models (mixing different formalisms)

Try it!

http://cosyverif.org/

Bibliography

References I

(2014).
Helena.
http://lipn.univ-paris13.fr/~evangelista/helena/.

André, É., Barbot, B., Démoulins, C., Hillah, L. M., Hulin-Hubard, F., Kordon, F., Linard, A., and Petrucci, L. (2013).
A modular approach for reusing formalisms in verification tools of concurrent systems.
In Groves, L. and Sun, J., editors, *15th International Conference on Formal Engineering Methods (ICFEM'13)*, volume 8144 of *Lecture Notes in Computer Science*, pages 199–214. Springer.

André, É., Fribourg, L., Kühne, U., and Soulat, R. (2012).
IMITATOR 2.5: A tool for analyzing robustness in scheduling problems.
In *Formal Methods*, volume 7436 of *Lecture Notes in Computer Science*, pages 33–36. Springer.

André, É., Hillah, L.-M., Hulin-Hubard, F., Kordon, F., Lembachar, Y., Linard, A., and Petrucci, L. (2013).
CosyVerif: An open source extensible verification environment.
In Liu, Y. and Martin, A., editors, *18th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS'13)*, pages 33–36. IEEE Computer Society.

André, É., Kordon, F., and Petrucci, L. (2014).
Teaching formal methods: Experience at UPMC and UP13 with CosyVerif.
In *Proceedings of the 25th EAEEIE annual International Conference (EAEEIE'14)*. IEEE Computer Society.
To appear.

References II

Baldan, P., Bruni, A., Corradini, A., König, B., Rodríguez, C., and Schwoon, S. (2012).
Efficient unfolding of contextual Petri nets.
Theoretical Computer Science, 449:2–22.

Ballarini, P., Djafri, H., Duflot, M., Haddad, S., and Pekergin, N. (2011).
HASL: An expressive language for statistical verification of stochastic models.
In *VALUETOOLS*, pages 306–315.

Colange, M., Baarir, S., Kordon, F., and Thierry-Mieg, Y. (2011).
Crocodile: A symbolic/symbolic tool for the analysis of symmetric nets with bags.
In *ICATPN*, volume 6709 of *Lecture Notes in Computer Science*, pages 338–347. Springer.

Haddad, S., Ilié, J.-M., and Klai, K. (2004).
Design and evaluation of a symbolic and abstraction-based model checker.
In *ATVA*, pages 196–210.

Klai, K. and Ochi, H. (2012).
Modular verification of inter-enterprise business processes.
In *eKNOW*, pages 155–161.

Kordon, F., Linard, A., Buchs, D., Colange, M., Evangelista, S., Lampka, K., Lohmann, N., Paviot-Adet, E., Thierry-Mieg, Y., and Wimmel, H. (2012).
Report on the model checking contest at Petri Nets 2011.
ToPNoC, V:121–140.

References III

Lakos, C. and Petrucci, L. (2004).
Modular analysis of systems composed of semiautonomous subsystems.
In *ACSD*, pages 185–196. IEEE Computer Society.