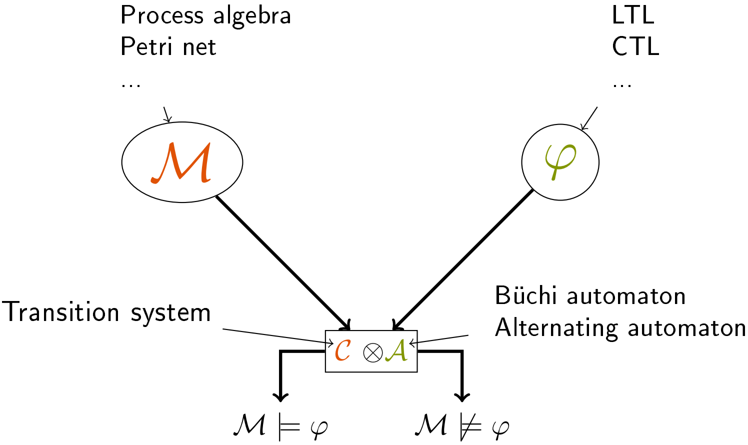
Cosmos: Evolution of a Statistical Model Checking Platform

Benoît Barbot[1], Paolo Ballarini[2]

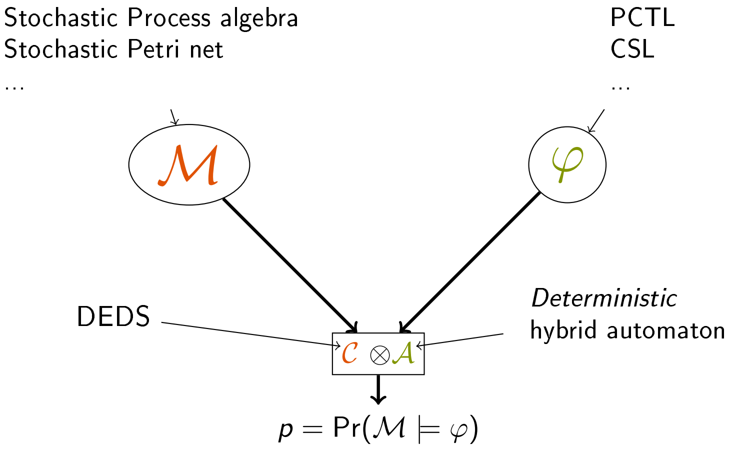
[1] Université Paris-Est Créteil Val de Marne, [2] Université Paris Saclay

Friday, 12 November, TOSME21

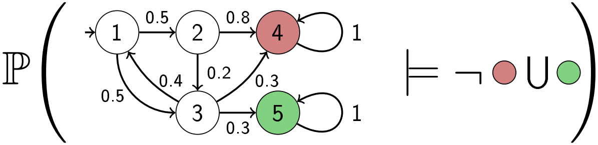
Model Checking



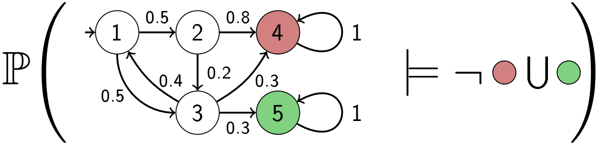
Model Checking for Stochastic Systems



Numerical vs Statistical Approaches



Numerical vs Statistical Approaches



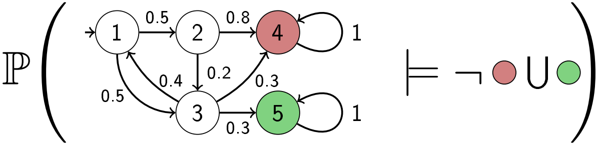
Numerical Model Checking

$$\begin{pmatrix} -1 & 0.5 & 0.5 & 0 & 0 \\ 0 & -1 & 0.2 & 0.8 & 0 \\ 0.4 & 0 & -1 & 0.3 & 0.3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$\Downarrow$$

$$x_1 = 0.2368$$

Numerical vs Statistical Approaches



Statistical Model Checking

$1 \to 2 \to 4$ **x**

$1 \to 3 \to 1 \to 3 \to 5$ ✓

$1 \to 3 \to 4$ **x**

$1 \to 3 \to 1 \to 3 \to 1 \to 2 \to 4$ **x**

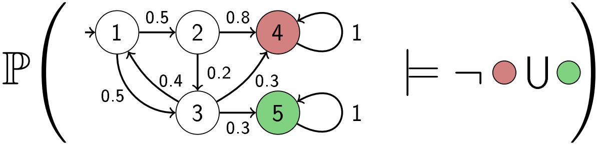
$1 \to 2 \to 3 \to 5$ ✓

...

$\Downarrow$

$x_1 \in [0.19, 0.26]$

Numerical vs Statistical Approaches



Numerical Model Checking

$$\begin{pmatrix} -1 & 0.5 & 0.5 & 0 & 0 \\ 0 & -1 & 0.2 & 0.8 & 0 \\ 0.4 & 0 & -1 & 0.3 & 0.3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$\Downarrow$$

$$x_1 = 0.2368$$

Statistical Model Checking

$1 \rightarrow 2 \rightarrow 4$ ✗
$1 \rightarrow 3 \rightarrow 1 \rightarrow 3 \rightarrow 5$ ✓
$1 \rightarrow 3 \rightarrow 4$ ✗
$1 \rightarrow 3 \rightarrow 1 \rightarrow 3 \rightarrow 1 \rightarrow 2 \rightarrow 4$ ✗
$1 \rightarrow 2 \rightarrow 3 \rightarrow 5$ ✓
...

$$\Downarrow$$

$$x_1 \in [0.19, 0.26]$$

Numerical vs Statistical Approaches

Numerical approach

- Precise value (but prone to numerical errors)
- Strong probabilistic hypotheses
- Memory space proportional to the size of the stochastic process

Numerical vs Statistical Approaches

Numerical approach

- Precise value (but prone to numerical errors)
- Strong probabilistic hypotheses
- Memory space proportional to the size of the stochastic process

Statistical approach

- Confidence interval: probabilistic framing
- Small memory space
- Easy to parallelise
- Weak probabilistic hypotheses (only an operational semantic)
- Requires fully stochastic models
- Rare events problem

Numerical vs Statistical Approaches

Numerical approach

- Precise value (but prone to numerical errors)
- Strong probabilistic hypotheses
- Memory space proportional to the size of the stochastic process

Statistical approach

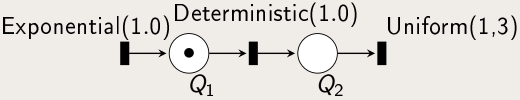
- Confidence interval: probabilistic framing
- Small memory space
- Easy to parallelise
- Weak probabilistic hypotheses (only an operational semantic)
- Requires fully stochastic models
- Rare events problem

Hybrid approaches

Combine both approaches; usually using stochastic bounds

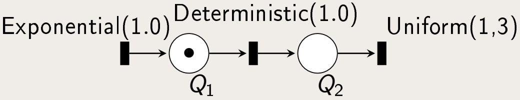
Generalised Stochastic Petri Net with General Distribution

Example Description (Tandem Queues)



Generalised Stochastic Petri Net with General Distribution

Example Description (Tandem Queues)

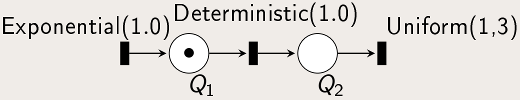


Description

- A Petri net; defines state space, events and transitions.
- After a transition is enabled the time before firing is distributed according to the distribution.
- The next event is the transition with smallest firing time.

Generalised Stochastic Petri Net with General Distribution

Example Description (Tandem Queues)



Description

- A Petri net; defines state space, events and transitions.
- After a transition is enabled the time before firing is distributed according to the distribution.
- The next event is the transition with smallest firing time.

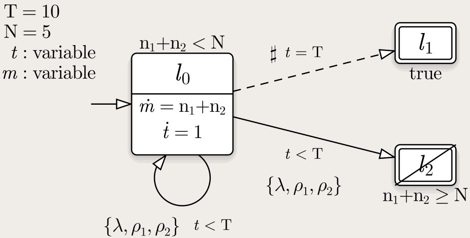
Extensions

- Petri net with inhibitor arcs, marking dependant valuation.
- Coloured Petri net

Specification Language

Linear Hybrid Automaton (LHA)

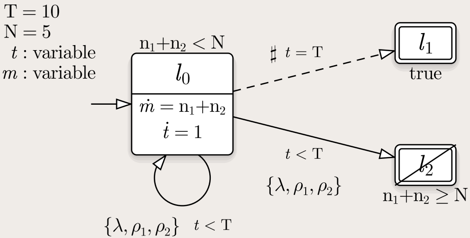
- An automaton labelled by set of Petri net transitions or #.
- A set of variables with flows.
- Assignment of variable.
- Linear guard and invariant.



Specification Language

Linear Hybrid Automaton (LHA)

- An automaton labelled by set of Petri net transitions or $\#$.
- A set of variables with flows.
- Assignment of variable.
- Linear guard and invariant.



HASL formula

- An LHA
- An expression over variables of the automaton, to compute complex indexes on *accepted* paths.

Cosmos a statistical model checking tool

Development History

- 2009-2012 Joint work LACL and LSV : initial work
  $\Rightarrow$ Hilal Djafri thesis
- 2011-2014 LSV : handling of rare events
  $\Rightarrow$ Benoît Barbot thesis
- 2015-2018 Joint work LACL, LIP6, LSV, IRT SystemX : simulation of hybrid systems for autonomous vehicles
  $\Rightarrow$ Yann Duplouy thesis
- 2015– Joint work LACL, University of Oxford, Verimag : Uniform sampling of timed languages

Cosmos 1/2

Description: a command-line tool

- Input model: a Generalised Stochastic Petri Net with extension
- Input specification: HASL formulas
- Input: Statistical Parameters
- Output: Probabilistic framing of values of HASL formulas

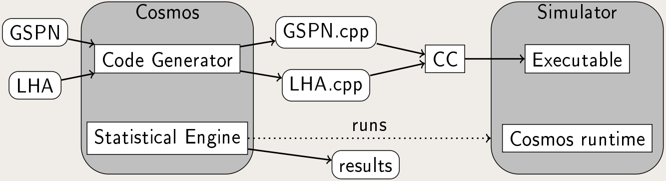
Cosmos 1/2

Description: a command-line tool

- Input model: a Generalised Stochastic Petri Net with extension
- Input specification: HASL formulas
- Input: Statistical Parameters
- Output: Probabilistic framing of values of HASL formulas

Architecture

- Contains 25 Kloc of C/C++ and OCaml under GPLv2
- Generates code implementing the synchronisation GSPN/LHA
- Distributes simulation



Cosmos 2/2

Features

- Static and Sequential statistical methods: Chernoff-Hoeffding, Chow-Robbins, Gaussian, SPRT
- Several input formats: GrML, Marcie, PNML, Prism
- Several compatible editing tools: Coloane, GreatSPN Editor, Snoopy
- Fast thanks to structural analysis of Petri nets and code generation
- Low memory footprint
- Various possible outputs

Cosmos 2/2

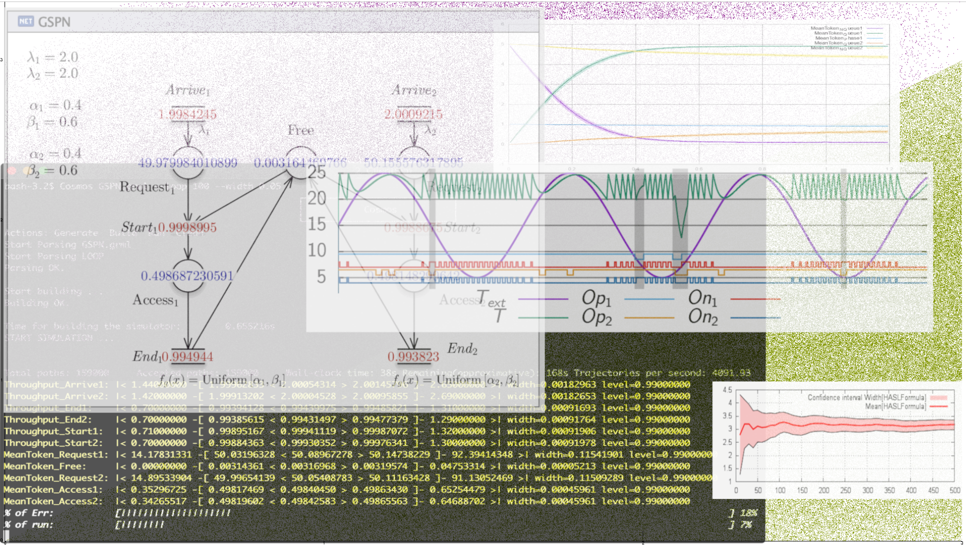
Features

- Static and Sequential statistical methods: Chernoff-Hoeffding, Chow-Robbins, Gaussian, SPRT
- Several input formats: GrML, Marcie, PNML, Prism
- Several compatible editing tools: Coloane, GreatSPN Editor, Snoopy
- Fast thanks to structural analysis of Petri nets and code generation
- Low memory footprint
- Various possible outputs

Extensions

- Handling of Rare Events with importance sampling
- Uniform sampling for timed automata
- Hardware in the loop simulation
- Simulation of hybrid models: Simulink

Cosmos Output



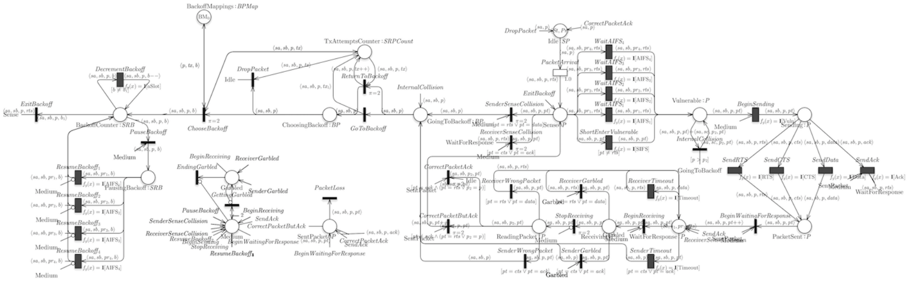
Performance Evaluation of Models

- Waiting Queues [*PT, RareEvents*]
- Databases, Philosophers, Peterson [*Coloured*]
- Flexible Manufacturing Systems [*PT*]
- Molecular Signalling Pathway [*PT, RareEvents*]
- Computation with DNA [*PT*]
- Human Heart and Pacemaker System [*Hybrid model*]
- Autonomous Vehicles [*Hybrid model*]

Modelling of IEEE 802.11 Wireless network

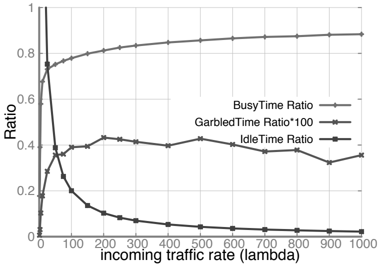
Modelling as a Stochastic Coloured Petri Net [ValueTools19]

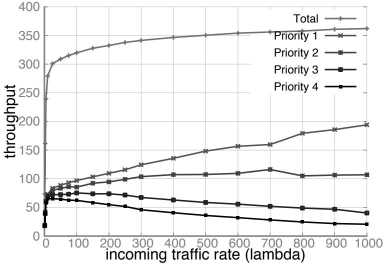
- WiFi with priorities
- Random backoff
- Colored Petri Net
- Large color class



Modelling of IEEE 802.11 Wireless network

Throughput and busytime with increasing loads.





Conclusion

Cosmos

- Fast and lightweight statistical model checker.
- Rich classes of input models.
- Rich specification language.
- Modular and open source.

Conclusion

Cosmos

- Fast and lightweight statistical model checker.
- Rich classes of input models.
- Rich specification language.
- Modular and open source.

cosmos.lacl.fr/publis.html

Cosmos Home Description Installation Tutorial Publications Documentation Extensions PetriNet Editor

Publications on Cosmos

1. B. Barbot, B. Bérard, Y. Duplouy and S. Haddad. Integrating Simulink Models into the Model Checker Cosmos. *In* Proceedings of the 39th International Conference on Applications and Theory of Petri Nets (PETRI NETS'18), pages 363-373, Bratislava, Slovakia, June 2018, LNCS. Springer.
2. P. Ballarini, B. Barbot, M. Duflot, S. Haddad and N. Pekergin. HASL: A New Approach for Performance Evaluation and Model Checking from Concepts to Experimentation. Performance Evaluation 90, pages 53-77, 2015.
3. P. Ballarini, H. Djafri, M. Duflot, S. Haddad and N. Pekergin. COSMOS: a Statistical Model Checker for the Hybrid Automata Stochastic Logic. *In* QEST'11, pages 143-144. IEEE Computer Society Press, 2011.
4. P. Ballarini, H. Djafri, M. Duflot, S. Haddad and N. Pekergin. HASL: An Expressive Language for Statistical Verification of Stochastic Models. *In* VALUETOOLS'11, pages 306-315. 2011.

Publications using Cosmos

5. B. Barbot, B. Basset T. Dang. Generation of Signals under Temporal Constraints for CPS Testing.. In *Proceedings of NASA Formal Methods 19*,To appear, 2019.
6. P. Ballarini, B. Barbot, N. Vasselin. Performance modelling of access control mechanisms for local and vehicular wireless networks.. In *Proceedings of the 12th EAI International Conference on Performance Evaluation Methodologies and Tools, VALUETOOLS 2019, pages 111 118. ACM*, 2019.
7. B. Barbot, B. Bérard, Y. Duplouy, and S. Haddad. Statistical model-checking for autonomous vehicle safety validation. In *SIA Simulation Numérique*, 2017.
8. P. Ballarini, M. Beccuti, Enrico Bibbona, Andras Horvath, Roberta Sirovich, Jeremy Sproston. Analysis of Timed Properties Using the Jump-Diffusion Approximation. *In* proceedings of the 14th European Performance Engineering Workshop (EPEW 2017). 2017.
9. B. Barbot, N. Basset, M. Beunardeau and M. Kwiatkowska. Uniform Sampling for Timed Automata with Application to Language Inclusion Measurement. *In* QEST'16, volume 9826 of Lecture Notes in Computer Science, pages 175–190. Springer, 2016.
10. B. Barbot, M. Kwiatkowska, A. Mereacre and N. Paoletti. Building Power Consumption Models from Executable Timed I/O Automata Specifications. *In* HSCC'16, pages 195–204. ACM, 2016.2016.
11. B. Barbot, M. Kwiatkowska, A. Mereacre and N. Paoletti. Estimation and verification of hybrid heart models for personalised medical and wearable devices. *In* CMSB'15, volume 9308 of LNCS, pages 3-7. 2015.
12. P. Ballarini and M. Duflot. Applications of an expressive statistical model checking approach to the analysis of genetic circuits. In *Theoretical Computer Science*, Elsevier, DOI, 06/2015.
13. B. Barbot, S. Haddad, M. Heiner and C. Picaronny. A Rare Event Method Applied to Signalling Cascades. International Journal on Advances in Systems and Measurements 8(1-2), 2015.
14. B. Barbot and M. Kwiatkowska. On Quantitative Modelling and Verification of DNA Walker Circuits Using Stochastic Petri Nets. *In* ICATPN'15, LNCS 9115, pages 1-32. Springer, 2015.
15. P. Ballarini, Analysing oscillatory trends of discrete-state stochastic processes through HASL statistical model checking. *In* STTT, 17(4):505–526, 2015.
16. B. Barbot, S. Haddad, M. Heiner and C. Picaronny. Rare Event Handling in Signalling Cascades. *In* SIMUL'14, pages 126-131. XPS, 2014.
17. P. Ballarini, E. Gallet, P. Le Gall, and M. Manceny. Formal analysis of the Wnt/beta-catenin pathway through statistical model checking. *In* proceedings of 6th Int. Symposium On Leveraging Applications of Formal Methods, Verification and Validation (ISOLA), 2014, pag. 193-207.
18. G. Amparore, P. Ballarini, M. Beccuti, S. Donatelli and G. Franceschinis. Expressing and computing passage time measures of gspn models with hasl. *In* proceedings