A & T: Stochastic Analysis (v1)
Second Year Report

UT, all CRs

May 3, 2004

AMETIST DELIVERABLE 2.4.a

Project acronym: AMETIST
Project full title: Advanced Methods for Timed Systems
Project no.: IST-2001-35304

1 Introduction

This is the Ametist second year's deliverable of Task 2.4.a on Stochastic Analysis. The aim of the Task is the integration of techniques for the analysis of timed systems with those for stochastic systems.

Whereas formal verification focuses on the absolute correctness of systems, in practice such rigid notions are hard, or even impossible, to guarantee. Instead, systems are subject to various phenomena of stochastic nature, such as message loss or garbling, unpredictable environments, faults, and delays. Correctness thus is of a less absolute nature. Accordingly, instead of checking whether system failures are impossible a more realistic aim is to establish, for instance, whether "the chance of shutdown occurring is at most 0.01%". Similarly, the question whether a distributed computation terminates becomes "does it eventually terminate with probability 1?". These queries can be checked using *stochastic* model checking, an automated technique for validating stochastic models.

Stochastic model checking is based on conventional model checking, since it relies on reachability analysis of the underlying transition system, but must also entail the calculation of the actual likelihoods through appropriate numerical methods. In addition to the qualitative statements made by conventional model checking, this provides the possibility to make quantitative statements about the system. Stochastic model checking uses extensions of temporal logics with probabilistic operators, affording the expression of these quantitative statements. Prominent examples of such extensions for CTL are PCTL and CSL.

Stochastic model checking is typically based on discrete-time and continuous-time Markov chains (DTMCs and CTMCs, respectively), or discrete-time and continuous-time Markov decision processes (MDPs and CTMDPs, respectively). Whereas Markov chains are fully stochastic, Markov decission processes allow for nondeterminism. The former models are intensively used in performance and dependability analysis, whereas MDPs are of major importance in stochastic operations research and automated planning in artificial intelligence. Extensions of model checking to stochastic models originate from the mid 1980s, first focusing on 0-1 probabilities, but later also considering quantitative properties. During the last decade, these methods have been extended, refined and improved, and – most importantly – significant work on software tools has been carried out, partly as part of Ametist. With the currently available technology, models of 10^6 – 10^7 states can be successfully checked.

In the first two years of Ametist, contributions have been made to the following issues related to the verification of stochastic aspects:

- **Model-checking of discrete probabilistic systems.** Algorithms have been developed for discrete-time probabilistic models to accommodate for the incorporation of cost aspects for DTMCS and MDPs [2], and to allow for parametric and precise analysis for DTMCs [13].
- **Model-checking of probabilistic timed systems.** Algorithms have been developed for continuous-time probabilistic models, such as CTMCs [4], CTMDPs [5], and have been extended with state costs [16].
- **Abstraction techniques for probabilistic timed systems.** Various abstraction techniques necessary to reduce the size of the probabilistic system to be verified have been studied. Weak simulation has been considered for CTMS [8, 6] and its relationship with weak simula-

tion for DTMCs formally compared [7]. Abstraction techniques for MDPs include branching bisimulation [3], strong simulation [12] and partial order reduction [11].

- **Tools.** Software tools implementing model-checking algortihms and/or reduction techniques have been developed to support automatic verification of probabilistic models, viz. ETMCC [17] for DTMCs and CTMCs, and Rapture [19] for MDPs. Three tools have been added to the CADP toolbox to enable both functional and performance evaluation within the same framework [18, 15]. Finally, a real-time and a probabilistic model-checker have been combined for the verification of a probabilistic timed protocol [14].

- **Case studies.** The developed verification techniques have been applied to analyse systems exhibiting stochastic behaviour: protocols in ad-hoc networks [9], a timed randomized contention protocol [14], and, most importantly, the Axxom case study on scheduling of lacquer production [10].

- **Stochastic scheduling.** The problem of scheduling under stochastic uncertainty has been addressed in [1] analysing a special case of CTMDP, and in [20] using stochastic integer programming.

A more detailed summary of these contributions is given in the remainder of this report. Part of the reported work has been funded from other sources than the Ametist project, but all of the reported work is strongly related to Ametist in terms of relevance of the results, as well as the involved researchers.

The achievements in the field of stochastic analysis are of very high quality and leading-edge internationally. This not only applies to the theoretical and algorithmic results, but also to tool-development. For the third year of the Ametist project, research will mainly focus on models that combine non-determinism with random timing.

2 Model-checking of discrete probabilistic systems

2.1 Discrete-time rewards model-checked

A model-checking approach for analyzing discrete-time Markov reward models is presented in [2]. For this purpose, the temporal logic probabilistic CTL is extended with reward constraints. This allows to formulate complex measures – involving expected as well as accumulated rewards – in a precise and succinct way. Algorithms to efficiently analyze such formulae are introduced. The approach is illustrated by model-checking a probabilistic cost model of the IPv4 zeroconf protocol for distributed address assignment in ad-hoc networks.

2.2 Symbolic and parametric model-checking of discrete-time Markov chains

A language-theoretic approach to symbolic model checking of PCTL over DTMCs is presented in [13]. The probability with which a path formula is satisfied is represented by a regular expression. A recursive evaluation of the regular expression yields an exact rational value when transition probabilities are rational, and rational functions when some probabilities are left unspecified as parameters of the system. This allows for parametric model checking by evaluating the regular expression for different parameter values, for instance, to study the influence of a lossy channel in the overall reliability of a randomized protocol.

3 Model-checking of probabilistic timed systems

3.1 Continuous-time Markov chains

A branching temporal logic for expressing real-time probabilistic properties on CTMCs and approximate model checking algorithms for this logic are presented in [4]. The logic, an extension of the continuous stochastic logic CSL of Aziz et al., contains a time-bounded until operator to express probabilistic timing properties over paths as well as an operator to express steady-state probabilities.

It is shown that the model checking problem for this logic reduces to a system of linear equations (for unbounded until and the steady-state operator) and a Volterra integral equation system (for time-bounded until), and that the problem of model-checking time-bounded until properties can be reduced to the problem of computing transient state probabilities for CTMCs. This allows the verification of probabilistic timing properties by efficient techniques for transient analysis for CTMCs such as uniformization. Finally, it is shown that a variant of lumping equivalence (bisimulation), a well-known notion for aggregating CTMCs, preserves the validity of all formulas in the logic.

3.2 Continuous-time Markov decision processes

A continuous-time Markov decision process (CTMDP) is a generalization of a continuous-time Markov chain in which both probabilistic and nondeterministic choices co-exist. [5] presents an efficient algorithm to compute the maximum (or minimum) probability to reach a set of goal states within a given time bound in a *uniform* CTMDP, i.e., a CTMDP in which the delay time distribution per state visit is the same for all states. It also shows that these probabilities coincide for (time-abstract) history-dependent and Markovian schedulers that resolve nondeterminism either deterministically or in a randomized way. A special case of CTMDP is used to solve the problem of scheduling under probabilistic temporal uncertainty in [1].

3.3 Markov models with rewards

Model checking has been introduced as an automated technique to verify whether functional properties, expressed in a formal logic like computational tree logic (CTL), do hold in a formally-specified system. In recent years, we have extended CTL such that it allows for the specification of properties over finite-state CTMCs. Computational techniques for model checking have been developed and successfully applied in the dependability context.

Further work in this area has recently led to the continuous stochastic reward logic (CSRL), a logic to specify measures over CTMCs extended with a reward structure (so-called Markov reward models). Well-known performability measures, most notably also Meyer's performability distribution, can be easily defined with CSRL. However, using CSRL it is possible to specify performability measures that have not yet been addressed in the literature, hence, for which no computational procedures have been developed yet. This paper [16] presents a number of computational procedures to perform model checking of CSRL over finite Markov reward models, thereby stressing their computational complexity (time and space) and applicability from a practical point of view (accuracy, stability). A case study in the area of ad hoc mobile computing under power constraints shows the merits of CSRL and the new computational procedures.

4 Abstraction techniques for probabilistic systems

4.1 Weak equivalences and preorders

Weak simulation for continuous-time Markov chains. A simulation preorder for CTMCs is considered in [8] and [6]. The simulation preorder is a conservative extension of a weak variant of probabilistic simulation on fully probabilistic systems, i.e., DTMCs.

The main result of [8] is that the simulation preorder preserves safety and liveness properties expressed in continuous stochastic logic (CSL), a stochastic branching-time temporal logic interpreted over CTMCs. Despite the second-order quantification in its definition, [6] presents a polynomial-time algorithm to compute the weak simulation preorder of a finite CTMC.

Branching bisimulation for discrete alternating models. Three equivalence relations that abstract from internal actions in the alternating model of Hansson are studied in [3].

The first equivalence is branching bisimilarity. Branching bisimilarity is a well-known and generally accepted equivalence for non-probabilistic systems. For probabilistic systems, it has only been studied in a different semantic setting.

The second equivalence is based on schedulers that induce maximal probabilities. It is shown that this second notion coincides with branching bisimilarity. This means that it is not necessary to consider a potentially infinite set of schedulers for branching bisimilarity, but that it suffices to consider only special schedulers. On the basis of these results, an algorithm can be defined to decide the notion of branching bisimilarity.

The third notion of equivalence is based on trace equivalence. Additional information is added to the graphs, in terms of colours that are added as labels to the nodes of these graphs. The colours are used to code for the branching behavioural potentials of a system in a node. It is shown that this extra information can be used to exactly capture the notion of branching bisimilarity. This third characterisation gives a nice alternative characterisation of branching bisimilarity that is not based on the notion of schedulers. A similar result was obtained by van Glabbeek and Weijland for the simpler setting of non-probabilistic systems.

Comparative branching-time semantics. Various semantics in the branching-time spectrum of discrete-time and continuous-time Markov chains are presented in [7]. Strong and weak bisimulation equivalence and simulation pre-orders are covered and are logically characterised in terms of the temporal logics PCTL and CSL. Apart from presenting various existing branching-time relations in a uniform manner, the contributions are: (i) weak simulation for DTMCs is defined, (ii) weak bisimulation equivalence is shown to coincide with weak simulation equivalence, (iii) logical characterisation of weak (bi)simulations are provided, and (iv) a classification of branching-time relations is presented, elucidating the semantics of DTMCs, CTMCs and their interrelation.

4.2 Reduction techniques

Reduction and Refinement Strategies for Probabilistic Analysis. An approach for model checking quantitative reachability properties of MDPs based on simulation preorders is presented in [19]. In this approach, properties are analyzed on abstractions rather than directly on the given model. Such abstractions are expected to be significantly smaller than the original model, and may safely refute or accept the required property. Otherwise, the abstraction is refined and the process repeated. As the numerical analysis involved in settling the validity of the property is more costly than the refinement process, the method profits from applying such numerical analysis on smaller state spaces. The method is significantly enhanced by a number of novel strategies: a strategy for reducing the size of the numerical problems to be analyzed by identification of so-called essential states, and heuristic strategies for guiding the refinement process.

Partial Order Reduction for MDPs. Partial order reduction has been used to alleviate the state explosion problem in model checkers for nondeterministic system. The method relies on exploring only a fragment of the full state space of a program that is enough to assess the validity of a property. Partial order reduction for probabilistic programs represented as MDPs is presented in [11].

The proposed technique preserves probabilistic quantification of reachability properties and is based on partial order reduction techniques for (non-probabilistic) *branching* temporal logic. It is also shown that techniques for (non-probabilistic) linear temporal logics are not correct for probabilistic reachability and that in turn this method is not sufficient for probabilistic CTL. Moreover, it is conjectured that the reduction technique also preserves maximum and minimum probabilities of next-free LTL properties.

5 Tools

5.1 ETMCC

Markov chains are widely used in the context of performance and reliability modeling of systems of various nature. Model checking of such chains with respect to a given (branching) temporal logic formula has been proposed for both the discrete and the continuous time setting. This paper [17] describes a prototype model checker for discrete and continuous-time Markov chains, the Erlangen–Twente Markov Chain Checker (ETMCC), where properties are expressed in appropriate extensions of CTL. The general benefits of this approach are illustrated and the structure of the tool is discussed. Furthermore successful application of the tool to some examples are reported, highlighting lessons learned during the development and application of the tool.

5.2 CADP

Considering functional correctness and performance evaluation in a common framework is desirable, both for scientific and economic reasons. The CADP toolbox, originally designed for verifying the functional correctness of LOTOS specifications, can also be used for performance and dependability analysis [15]. Three new tools (named BCG_STEADY, BCG_TRANSIENT, and DETERMINATOR) have been added to the CADP toolbox. The approach taken [18] fits well within the existing architecture of CADP, which doesn't need to be altered to enable performance evaluation.

5.3 Rapture

Rapture [19] is a tool for the verification of quantified reachability properties over MDPs. The originality of the tool is to provide two reduction techniques that limit the state space explosion problem: automatic abstraction and refinement algorithms, and a so-called essential states reduction. Several case-studies illustrate the usefulness of these techniques.

6 Case studies

6.1 Synthesis and stochastic assessment of schedules for lacquer production

MoDeST modeling language pairs modeling features from stochastic process algebra and from timed and probabilistic automata with light-weight notations such as exception handling. It is supported by the Motor tool, which facilitates the execution and evaluation of MoDeST specifications by means of the discrete event simulation engine of the Moebius tool. [10] describes the application of MoDeST Motor and Moebius to a highly nontrivial case. The effect of faulty behavior on a hard real-time scheduling problem from the domain of lacquer production is investigated. The scheduling problem is first solved using the timed model-checker Uppaal. The resulting schedules are then embedded in a MoDeST failure model of the lacquer production line, and analyzed with the discrete event simulator of Moebius. This approach allows one to assess the quality of the schedules with respect to timeliness, utilization of resources, and sensitivity to different assumptions about the reliability of the production line.

6.2 Cost-Optimisation of the IPv4 Zeroconf Protocol

The tradeoff between reliability and effectiveness for the IPv4 Zeroconf protocol, a protocol dedicated to the self-configuration of IP network interfaces, is investigated in [9]. The protocol is modelled as a simple stochastic model with costs, where reliability is measured in terms of the probability to avoid an address collision after configuration, while effectiveness is viewed as the average penalty perceived by a user. From an analytical expression for the user penalty derived from the model, optimal configuration parameters of the network can be obtained, restricting to those parameters which are under the control of a consumer electronics manufacturer. In particular it is shown that minimal cost and maximal reliability are qualities that cannot be achieved at the same time. A simpler model of the protocol has been considered to model-check using rewards in [2] and parametrically in [13].

6.3 Automatic Verification of the IEEE 1394 Root Contention Protocol

This article [14] reports on the automatic verification of timed probabilistic properties of the IEEE 1394 root contention protocol combining two existing tools: the real-time model-checker Kronos and the probabilistic model-checker Prism. The system is modelled as a probabilistic timed automaton. Kronos is first used to perform a symbolic forward reachability analysis to generate the set of states that are reachable with non-zero probability from the initial state, and before the deadline expires. This information is then encoded as an MDP to be analyzed with Prism. This technique is applied to compute the minimal probability of a leader being elected before a deadline, for different deadlines, and to study the influence on this minimal probability, of using a biased coin, and considering different wire lengths.

7 Stochastic scheduling

7.1 Optimal scheduling under temporal uncertainty

The problem of scheduling under two types of temporal uncertainty, set-based and probabilistic is addressed in [1]. For the former appropriate optimality criteria are defined and an algorithm for finding optimal scheduling strategies using a backward reachability algorithm for timed automata is developed. Probabilistic uncertainty is dealt with solving a special case of CTMDP. All results have been implemented and a preliminary assessment of the merits of each approach is provided.

7.2 Real-time scheduling using stochastic integer programming

The contribution [20] deals with scheduling problems of flexible chemical batch processes with a special emphasis on their real-time character. This implies not only the need for sufficiently short response times, but in particular the burden of incomplete knowledge about the future. To solve such problems, the application of two-stage stochastic integer programming techniques on moving horizons is proposed. They reflect the need for immediately applicable decisions and the potential of later recourse actions to cope with realized uncertainties. In addition to the classical expected value objective, simple measures of risk can be included. Motivated by an example process, some essential modelling prerequisites are discussed. As an important first step, the master scheduling problem is studied and a number of master scheduling models are presented. Large mixed-integer linear problems arise, which are well-suited for a dual decomposition approach. Numerical experiments with a problem-specific solution algorithm demonstrate the applicability of the method to real-world problems.

References

[1] Y. Abdeddam, E. Asarin, and O. Maler. On optimal scheduling under uncertainty. In H. Garavel and J. Hatcliff, editors, *Proc. TACAS*, volume 2619 of *LNCS*. Springer, 2003. Available from World Wide Web: `http://www-verimag.imag.fr/~maler/Papers/uncertain.ps`.

[2] Suzana Andova, H. Hermanns, and Joost-Pieter Katoen. Discrete-time rewards model-checked. In *Formal Modelling and Analysis of Timed Systems (FORMATS 2003)*, Marseille, France, 2003. Lecture Notes in Computer Science, Springer-Verlag. Available from World Wide Web: `http://fmt.cs.utwente.nl/publications/files/417_AHK03.ps`.

[3] Suzana Andova and Tim Willemse. Equivalences for silent transitions in probabilistic systems, 2004. Submitted to QEST.

[4] C. Baier, B. Haverkort, H. Hermanns, and J.-P. Katoen. Model-checking algorithms for continuous-time Markov chains. In *IEEE Transactions on Software Engineering*, volume 29, pages 524–541, 2003. Available from World Wide Web: `http://fmt.cs.utwente.nl/publications/files/399_116221.pdf`.

[5] C. Baier, B. Haverkort, H. Hermanns, and J.-P. Katoen. Efficient computation of time-bounded reachability probabilities in uniform continuous-time Markov decision processes. In *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, Barcelona, Spain, 2004. Lecture Notes in Computer Science, Springer-Verlag. Available from World Wide Web: `http://fmt.cs.utwente.nl/publications/files/420_ctit_tr_03_50.pdf`.

[6] C. Baier, H. Hermanns, and J.-P. Katoen. Probabilistic weak simulation is polynomially decidable. *Information Processing Letters, Vol. 89, Issue: 3*, pages 123–252, 2004.

[7] C. Baier, H. Hermanns, J.-P. Katoen, and Verena Wolf. Comparative branching-time semantics for Markov chains. In *Concurrency Theory (CONCUR)*, pages 492–507, Marseille, France, 2003. Lecture Notes in Computer Science, Vol. 2761, Springer-Verlag. Available from World Wide Web: `http://fmt.cs.utwente.nl/publications/files/404_BHKW03.ps`.

[8] Christel Baier, Joost-Pieter Katoen, Holger Hermanns, and Boudewijn Haverkort. Simulation for continuous-time Markov chains. In L. Brim, P. Jancar, M. Kretinsky, and A. Kucera, editors, *Concurrency Theory*, volume 2421 of *Lecture Notes in Computer Science*, pages 338–354. Springer-Verlag, 2002. Available from World Wide Web: `http://link.springer.de/link/service/series/0558/papers/2421/24210338.pdf`.

[9] H. Bohnenkamp, P. van der Stok, H. Hermanns, and F.W. Vaandrager. Cost-optimisation of the IPv4 zeroconf protocol. In *Proceedings International Performance and Dependability Symposium (IPDS),* San Fransisco. IEEE CS Press, 2003. Available from World Wide Web: `http://www.cs.kun.nl/ita/publications/papers/fvaan/IPDS.html`. To appear.

[10] H.C. Bohnenkamp, H. Hermanns, R. Klaren, A. Mader, and Y.S. Usenko. Synthesis and stochastic assessment of schedules for lacquer production. Submitted to QEST'04.

[11] Pedro R. D'Argenio and Peter Niebert. Partial order reduction on concurrent probabilistic programs, 2004. Available from World Wide Web: `http://www.cmi.univ-mrs.fr/~dargenio/papers/DArgenio-Niebert-submitted.ps.gz`. Submitted for publication.

[12] P.R. D'Argenio, B. Jeannet, H.E. Jensen, and K.G. Larsen. Reduction and refinement strategies for probabilistic analysis. In H. Hermanns and R. Segala, editors, *Proceedings of Process Algebra and Probabilistic Methods. Performance Modeling and Verification. Joint International Workshop, PAPM-PROBMIV 2001,* Copenhagen, Denmark, Lecture Notes in Computer Science. Springer-Verlag, 2002. Available from World Wide Web: `http://www.cs.famaf.unc.edu.ar/dargenio/papers/papm-probmiv2002.ps.gz`.

[13] C. Daws. Symbolic and parametric model-checking of discrete-time Markov chains, 2004. Available from World Wide Web: `http://ametist.cs.utwente.nl/INTERNAL/PUBLICATIONS/UTPublications/daws-qest04.ps.gz`. Submitted to QEST'04.

[14] C. Daws, M. Kwiatkowska, and G. Norman. Automatic verification of the IEEE 1394 root contention protocol with KRONOS and PRISM. *Software Tools for Technology Transfer*, 5(2–3):221–236, 2004. Available from World Wide Web: `http://ametist.cs.utwente.nl/INTERNAL/PUBLICATIONS/UTPublications/daws-STTT04.ps.gz`.

[15] H. Garavel and H. Hermanns. On combining functional verification and performance evaluation using CADP. In L. Eriksson and P. Lindsay, editors, *FME 2002: International Symposium of Formal Methods Europe*, volume 2391 of *LNCS*, pages 410–429. Springer, 2002. Available from World Wide Web: `http://www.inrialpes.fr/vasy/Publications/Garavel-Hermanns-02.html`.

[16] B. Haverkort, L. Cloth, H. Hermanns, J.-P. Katoen, and C. Baier. Model-checking performability properties. In *International Conference on Dependable Systems and Networks (DSN)*, pages 103–112. IEEE CS Press, 2002. Available from World Wide Web: `http://computer.org/proceedings/dsn/1597/15970103abs.htm`.

[17] H. Hermanns, J.-P. Katoen, J. Meyer-Kayser, and M. Siegle. A tool for model-checking Markov chains. *Int. Journal on Software Tools for Technology Transfer*, 4(2):153–172, 2003. Available from World Wide Web: `http://link.springer.de/link/service/journals/10009/bibs/3004002/30040153.pdf`.

[18] Holger Hermanns and Christophe Joubert. A set of performance and dependability analysis components for CADP. In *Proceedings TACAS 2003*, 2003. Available from World Wide Web: `http://www.inrialpes.fr/vasy/Publications/Hermanns-Joubert-03.html`.

[19] B. Jeannet, P.R. D'Argenio, and K.G. Larsen. Rapture: A tool for verifying Markov Decision Processes. In I. Cerna, editor, *Tools Day'02,* Brno, Czech Republic, Technical Report. Faculty of Informatics, Masaryk University Brno, 2002. Available from World Wide Web: `http://www.cs.famaf.unc.edu.ar/dargenio/papers/tools-day-concur2002.ps.gz`.

[20] G. Sand and S. Engell. Modelling and solving real-time scheduling problems by stochastic integer programming. *Computers and Chemical Engineering*, 2004. Available from World Wide Web: `http://ametist.cs.utwente.nl/INTERNAL/PUBLICATIONS/DORTMUNDPublications/CCE04.pdf`. (to appear).