

Probabilistic model checking of stochastic hybrid systems by abstraction: application to Air Traffic Management

Alessandro D’Innocenzo and Maria D. Di Benedetto

Department of Electrical and Information Engineering, Center of Excellence DEWS
University of L’Aquila, Italy

The introduction of new Air Traffic Management (ATM) procedures is a necessary condition for achieving safety and efficiency objectives requested by the increasing air traffic. In the past, the Air Traffic Controller (ATC) and the pilots had access to different data, and the responsibility of changes in procedures and operations were totally delegated to the ATC. The introduction of the next generation of ATM systems forecasts the use of ground and on-board integrated surveillance systems, which guarantee a cooperation between the ATC and the pilots. Moreover, new technologies provide broadcast communication of an aircraft position in the airspace, thus enabling the possibility of decentralization of decision making from the ATC to the pilot. These are the enabling technologies for development of a plethora of applications, such as the Airborne Separation Assistance System (ASAS) [1], which aims to improve efficiency of air traffic management procedures by a decentralization of responsibility among the ATC and the pilots. The more advanced ASAS application is the Airborne Self Separation (ASEP) [2], which aims to a total shift of responsibility to the pilots flying in a specified airspace. Within this airspace, the pilots are responsible of maintaining safety separation with the other aircraft using the on board surveillance system. These new concepts are a potential solution to the increasing air traffic density expected in the future years, and forecast an increase of safe air traffic from three to six times the current air traffic. The main problem is providing guarantee that the new air traffic procedures are sufficiently safe. Modeling, simulation and formal analysis and validation of new ATM procedures is an important and necessary step for the development of ATM systems. In the context of the iFly project, our research focuses on development of novel concepts and technologies for addressing the issues discussed above, in order to provide automatic tools for the ATM systems under development and standardization.

However, the dynamical analysis of high-dimensional, stochastic models poses a number of challenges. When direct analysis of the model under study is impaired by its sheer complexity, automatic verification and algorithmic control design procedures are essential. An approach that is used to cope with this scalability issue is that of *abstraction*: a system with smaller (possibly finite) state space is obtained, which is *equivalent* to the original system [3]. Equivalence is usually defined by the notions of language equivalence and bisimulation [4], [5]. Often though the (exact) notions of language equivalence

and bisimulation are quite restrictive, since they require a perfect correspondence between the trajectories of the original system and those of its abstraction. To address this potential limitation, *approximate* notions of system equivalence [6], [3], [7], [8], [9] have been recently developed. According to this relaxed approach, a proper metric is introduced to quantify the distance between the trajectories of the original system and those of the approximate abstraction.

Currently, the research on abstraction techniques for dynamical systems has two general goals. The first objective is that of *proving the existence of a finite abstraction*: given a model within a class of systems (e.g. timed [10] or hybrid automata, stable linear or non-linear systems), does there always exist an equivalent finite abstract model, or an approximately equivalent one? The second goal is that of *developing abstraction algorithms*: given a model, synthesize an algorithm that terminates in finite time, which constructs a finite (approximate) abstraction of the model. Algorithms that can be refined as needed are particularly useful as they allow tuning the level of approximation.

Abstraction techniques have also been adapted to probabilistic models. For instance, notions of bisimulation for classical discrete Markov processes have been developed in [11], [12], [13]. Abstraction techniques have been applied to discrete-space, continuous-time models [14]. In [15], classes of continuous-time Markov Processes are studied with time-abstraction techniques. In [9] a notion of approximate bisimulation has been proposed for jump linear stochastic systems. Weak approximations of continuous-time probabilistic models as locally-consistent Markov Chains have been introduced by [16], and are tailored to hybrid models in [17], [18]. Categorical notions of bisimulation are discussed in [19]. Notice that they are different than the present work in that they derive no explicit approximation bound.

In this talk we illustrate new results (introduced in [20]) on approximate abstractions of discrete-time stochastic hybrid systems (DTSHS). This model encompasses a number of other classes of stochastic hybrid models. We introduce a procedure to construct an approximate abstraction of a DTSHS. The procedure involves the partition of the state space and the approximation of the transition laws of the DTSHS over the partition sets. The abstraction is interpreted as a Markov set-Chain (MSC) [21], namely a Markov Chain where the transition probabilities are compact intervals (rather than just real

values). MSC are useful as they comprise both stochastic and non-deterministic parts. By posing some continuity assumptions on the DTSHS model, we derive explicit and tunable bounds on the error between the probability distribution of the abstracted model (the MSC) and that of the original model (the DTSHS, considered over the partition sets), for each time instant (and, in particular, in steady-state). The adjustability of the error bounds allows successive refinements of the abstraction procedure. Moreover, given proper assumptions on the ergodicity of the original DTSHS, it is possible to construct in finite time an approximate abstraction with arbitrary precision. The precision quantifies the distance between the stationary distributions. A finite-time algorithm is introduced to achieve this.

As an application of these concepts, we propose to apply a methodology (introduced in [22]) for formal reasoning based on stochastic hybrid systems theory, that provides a powerful framework to analyze multi-agents stochastic models of ATM procedures. We propose the use of automatic tools for verifying probabilistic properties of ATM scenarios. In particular, we propose to use PCTL logic to define probabilistic properties of interest (we refer to [23] and references therein for a survey on PCTL). Recently, formal verification of stochastic models has been transformed from an academically attractive discipline to a research effort prone to yield industrially relevant applications, and tools for probabilistic model checking have been developed: we propose the use of PRISM [24], [25], [26] for automatic verification of PCTL properties on ATM procedures. Figure 1 illustrates the main phases of the verification algorithm we propose. In the first block, a detailed

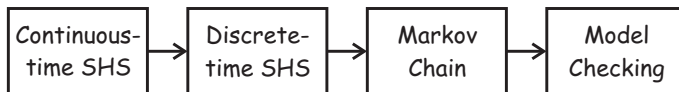


Fig. 1. Verification algorithm flow.

continuous-time stochastic model of the ATM procedure (e.g. a stochastic model of the aircraft dynamics) is defined, using the mathematical framework of continuous time Stochastic Hybrid Systems (ct-SHS). This model can be discretized with respect to the time variable, thus obtaining a discrete time SHS (dt-SHS). We refer to [27] and references therein for the formal definition of discrete and continuous time SHSs. In the third block, a Markov Chain abstraction of the model is obtained using the abstraction procedure proposed in [20]. This abstraction procedure is essentially a partition of the state space, which depends on a tunable parameter δ (the width of the partition grid). The reason for using this abstraction is that it provides an approximation of the original system, and it can be used to perform automatic model checking using the tool PRISM. The results of the model checking verification directly apply to the original system, modulo an approximation error ϵ . This approximation error ϵ can be chosen a-priori, by modifying the parameter $\delta(\epsilon)$ of the abstraction procedure from dt-SHS to Markov Chain.

REFERENCES

- [1] J.-M. Loscos, "Asas:towards new cooperation based on airborne spacing," *Revue Technique de la DTI, ISSN 776-1239*, December 2005.
- [2] "D6.1b qualitative risk assessment for asep-itp, v.1.0," ASSTAR Projects, Tech. Rep., 01 February 2007.
- [3] Antoine Girard and George J. Pappas, "Approximation metrics for discrete and continuous systems," *IEEE Trans. on Automatic Control*, vol. 52(5), pp. 782–798, 2007.
- [4] R. Alur, T. Henzinger, G. Lafferriere, and G. Pappas, "Discrete abstractions of hybrid systems," *Proceedings of the IEEE*, vol. 88(2), pp. 971–984, July 2000.
- [5] G. Pappas, "Bisimilar linear systems," *Automatica*, vol. 39(12), pp. 2035–2047, December 2003.
- [6] A. Girard and George J. Pappas, "Approximate bisimulation relations for constrained linear systems," *Automatica*, 2008, accepted for publication.
- [7] T. A. Henzinger, R. Majumdar, and V. Prabhu, "Quantifying similarities between timed systems," in *Proceedings of the Third International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS)*, ser. Lecture Notes in Computer Science, vol. 3829. Springer Verlag, 2005, pp. 226–241.
- [8] A. Julius and G. Pappas, "Approximate equivalence and approximate synchronization of metric transition systems," in *Proceedings of the 45th IEEE Conference on Decision and Control, San Diego, CA, USA*, December 2006.
- [9] A.A. Julius and G.J. Pappas, "Approximate abstraction of stochastic hybrid systems," *IEEE Trans. Automatic Control*, 2008, provisionally accepted.
- [10] R. Alur and D. Dill, "A theory of timed automata," *Theoretical Computer Science*, vol. 126, pp. 183–235, 1994.
- [11] K. Larsen and A. Skou, "Bisimulation through probabilistic testing," *Information and Computation*, vol. 94, pp. 1–28, 1991.
- [12] J. Desharnais, A. Edalat, and P. Panangaden, "Bisimulation for labeled Markov processes," *Information and Computation*, vol. 179, no. 2, pp. 163–193, 2002.
- [13] H. Hermanns, *Interactive Markov Chains, and the Quest for Quantified Quality*, ser. Lecture Notes in Computer Science. Springer Verlag, 2002, vol. 2428.
- [14] C. Baier, J. Katoen, H. Hermanns, and V. Wolf, "Comparative branching-time semantics for Markov chains," *Information and Computation*, vol. 200, no. 2, pp. 149–214, 2005.
- [15] N. Wolovick and S. Johr, "A characterization of meaningful schedulers for continuous-time Markov decision processes," in *FORMATS*, ser. Lecture Notes in Computer Science, E. Asarin and P. Bouyer, Eds., vol. 4202. Springer, 2006, pp. 352–367.
- [16] H. J. Kushner, *Approximation and Weak Convergence Methods for Random Processes with Applications to Stochastic Systems Theory*. Cambridge, Massachusetts: MIT Press, 1984.
- [17] X. Koutsoukos, "Optimal control of stochastic hybrid systems based on locally consistent Markov decision processes," *International Journal of Hybrid Systems*, vol. 4, pp. 301–318, 2004.
- [18] M. Prandini and J. Hu, "A numerical approximation scheme for reachability analysis of stochastic hybrid systems with state-dependent switchings," in *In Proc. IEEE Int. Conf. Decision and Control*, New Orleans, LA, Dec. 2007, pp. 4662–4667.
- [19] M. Bujorianu, J. Lygeros, and M. Bujorianu, "Bisimulation for general stochastic hybrid systems," in *Hybrid Systems: Computation and Control*, ser. Lecture Notes in Computer Science, M. Morari and L. Thiele, Eds. Springer Verlag, 2005, vol. 3414, pp. 198–214.
- [20] A. D’Innocenzo, A. Abate, M. Di Benedetto, and S. Sastry, "Approximate abstractions of discrete-time controlled stochastic hybrid systems," in *Proceedings of the 47th IEEE Conference of Decision and Control*, Cancun, MX, December 2008, pp. 221–226.
- [21] H. J. Hartfiel, *Markov set-Chains*, ser. Lecture Notes in Mathematics. Springer-Verlag Berlin Heidelberg, 1998, vol. 1695.
- [22] M. D. Benedetto, G. Di Matteo, and A. D’Innocenzo, "Stochastic validation of atm procedures by abstraction algorithms," *Submitted to: 4th International Conference on Research in Air Transportation ICRAT 2010 - Budapest, Hungary*, 2010.
- [23] M. Kwiatkowska, G. Norman, and D. Parker, "Stochastic model checking," in *Formal Methods for the Design of Computer, Communication and Software Systems: Performance Evaluation (SFM07)*, ser. Lecture Notes in Computer Science, M. Bernardo and J. Hillston, Eds. Springer, 2007, vol. 4486 (Tutorial Volume), pp. 220–270, to appear.
- [24] A. Hinton, M. Kwiatkowska, G. Norman, and D. Parker, "PRISM: A tool for automatic verification of probabilistic systems," in *Proc. 12th International Conference on Tools and Algorithms for the Construction*

- and Analysis of Systems (TACAS'06)*, ser. LNCS, H. Hermanns and J. Palsberg, Eds., vol. 3920. Springer, 2006, pp. 441–444.
- [25] M. Kwiatkowska, G. Norman, and D. Parker, “Prism: Probabilistic model checking for performance and reliability analysis,” *ACM SIGMETRICS Performance Evaluation Review*, 2009.
- [26] “www.prismmodelchecker.org.”
- [27] A. Abate, M. Prandini, J. Lygeros, and S. Sastry, “Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems,” *Automatica*, 2007, accepted for publication.