V for Verification: Intelligent Algorithm of Checking Reliability of Smart Systems

Anna Lukina

Cyber-Physical Systems Group
Technische Universität Wien
Treitlstrasse 3/3, Vienna, Austria
anna.lukina@tuwien.ac.at

Introduction

Cyber-physical systems (CPS) are intended to receive information from the environment through sensors and perform appropriate actions using actuators of the controller.

In the last years world of intelligent technologies has grown in an exponential fashion: from cruise control to smart ecosystems. Next we are facing the future of CPS involved in almost every aspect of our lives bringing higher comfortability and efficiency. Our goal is to help smart inventions adjust to this highly uncertain environment and guarantee safety for its inhabitants.

The physical environment renders the problem of CPS verification extremely cumbersome. Due to a wealth of uncertainties introduced by physical processes, the system is best described by stochastic models. Approximate prediction techniques, such as Statistical Model Checking (SMC), have therefore recently become increasingly popular (Grosu and Smolka 2005; Clarke and Zuliani 2011). As a result, verification of a CPS boils down to quantitative analysis of how close the system is to reaching bad states (safety property) or desired goal (liveness property).

Controlling the systems, that is, computing appropriate response actions depending on the environment, involves probabilistic state estimation, as well as optimal action prediction, i.e., choosing the best next step by simulating the future. In my thesis, I develop a novel intelligent algorithm addressing existing deficiencies of SMC such as poor prediction of rare events (RE) and sampling divergence.

Motivation

Verification. We motivate *the verification question* by the challenges associated with automatic control for unmanned vehicles, in particular flying drones. First, we would like to use flying drones simulation models in order to investigate the verification question of their safety. It is essential that the following properties are satisfied for flying drones:

– Drones do not collide, crash into flying objects or people.

– Stochastic environmental changes are correctly addressed.

– Probability of RE (e.g., flipping over, diverging from the goal) is estimated with high confidence.

Control. After we estimate the probability of such RE, it is only logical to address the control question by developing a policy that guarantees that the system avoids RE, satisfying the requirements above. *The control question* I am addressing is motivated by nature itself (Chazelle 2012), namely, by flocks of birds organizing into V-formations while traveling long distances. Every bird-like agent in our model (Grosu et al. 2014) moves in 2-dimensional space locally governed by the same control law. Any agent in the flock can detect the positions and velocities of all other agents through sensors, and given this information, the agent's controller calculates an optimal acceleration for it: $\overline{x}_i(t), \overline{v}_i(t)$ and $\overline{a}_i(t)$ are the vectors of 2-dimensional positions, velocities, and accelerations, respectively, of bird i at time t, $1 \leq i \leq N$, for a fixed number of birds N. the following equations model the behavior of bird i in discrete time with $\overline{a}_i(t)$ as controlled variables $\forall\ i = \{1, \ldots, N\}$: $\overline{x}_i(t+1) = \overline{x}_i(t) + \overline{v}_i(t+1)$, $\overline{v}_i(t+1) = \overline{v}_i(t) + \overline{a}_i(t)$.

Ultimately, we would like to synthesize an algorithm providing analytical guarantees of agents getting into a V-formation starting from a random configuration using a flying drones simulation model and statistical model checking. Particle Swarm Optimization (PSO) (Kennedy and Eberhart 1995) is a promising approach to address this problem. It uniformly distributes the particles in space and adjusts their velocities to lead the swarm to satisfying a given property while using a random factor in the adjustment rule in order to explore the space.

On the one hand, a V-formation provides the birds with a clear view of the front field and visibility of their lateral neighbors. On the other hand, the latter is of great importance to flocking birds for saving energy from the free lift as a beneficial effect of the upwash region generated off the trailing edge of wings of the birds in front of them (Weimerskirch et al. 2001). We believe this approach can lead to a breakthrough discovery in developing energy-efficient and reliable autonomous technologies.

Achievements and Planned Research

First and foremost, we strive to obtain a better understanding of the challenges we face when dealing with currently

existing CPS. By doing so, we will be able to predict their behavior in extreme cases and give guidance to the future generation of smart technologies.

In 2015-2016 together with R. Grosu, E. Bartocci, S. A. Smolka, K. Kalajdzic, and C. Jegourel we developed a novel framework of feedback control for SMC of CPS. The approach tackles an increasingly important problem of RE by combining two advanced sequential Monte-Carlo methods: Importance Sampling (ISam) (Kahn 1955) and Importance Splitting (ISpl), originally developed for statistical physics (Kahn and Harris 1951). These techniques have recently been adopted by the robotics (Russell and Norvig 2010) and SMC communities (Jégourel, Legay, and Sedwards 2012; 2013).

In the proposed framework, ISam estimates the current system state and the current level, and ISpl controls the execution of the CPS based on this information. Both techniques depend on the model identified during a preliminary, learning stage. The algorithm may be applied to the approximate analysis of any complex probabilistic program whose monitoring is feasible through appropriate instrumentation, but whose model derivation is infeasible through static analysis techniques (due to e.g. sheer size or complicated transitions). This collaborative work successfully resulted in publication (Kalajdzic et al. 2016).

Current and Anticipated Progress

Recently, I have worked on testing existing centralized Model Predictive Control (MPC) (Garca, Prett, and Morari 1989) to bird flocking optimization problem proposed in (Yang et al. 2016). After adjusting original algorithm for parallel execution I conducted $10,000$ experiments on a 16-core machine. Analyzing accumulated statistical data I estimated the performance of the algorithm as being too low to be considered reliable. As a result, I have focused on possible directions for improvement:

– Tunning parameters or discovering substitutes for PSO.

– Modifying MPC routine.

My thorough investigation resulted in developing a novel adaptive receding-horizon synthesis algorithm for optimal plans bringing an arbitrary dynamic process to a stable state. Experimental results proved reliability improvement by at least 40% and ten-fold average execution time decrease. I consider control of a dynamic system as a memoryless decision process. The algorithm performs adaptive splitting into monotonically decreasing levels of optimization by taking advantage of intelligent space exploration with numerous runs of PSO and selective importance-based resampling. When stabilized and tested this algorithm has a great potential to be applied for a wider range of optimization problems.

In October 2016 I submitted a paper introducing my algorithm to the 23rd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'17). I now consider its application to drones. By February 2017 I expect to prepare a paper for submission to the 56th IEEE Conference on Decision and Control (CDC'17).

References

Chazelle, B. 2012. Natural algorithms and influence systems. *Commun. ACM* 55(12):101–110.

Clarke, E., and Zuliani, P. 2011. Statistical model checking for cyber-physical systems. In *Proc. of the 9th International Symposium on Automated Technology for Verification and Analysis (ATVA'11)*, volume 6996 of *LNCS*, 1–12. Springer.

Garca, C. E.; Prett, D. M.; and Morari, M. 1989. Model predictive control: Theory and practice – a survey. *Automatica* 25(3):335–348.

Grosu, R., and Smolka, S. 2005. Monte Carlo model checking. In *Proc. of the 11th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'05)*, volume 3440 of *LNCS*, 271–286. Springer-Verlag.

Grosu, R.; Peled, D.; Ramakrishnan, C.; Smolka, S. A.; Stoller, S. D.; and Yang, J. 2014. Using statistical model checking for measuring systems. In *Proc. of the International Symposium On Leveraging Applications of Formal Methods, Verification and Validation (ISoLA'14)*, 223–238. Springer Berlin Heidelberg.

Jégourel, C.; Legay, A.; and Sedwards, S. 2012. Cross-entropy optimisation of importance sampling parameters for statistical model checking. In *Proc. of the 24th International Conference (CAV'12)*, 327–342.

Jégourel, C.; Legay, A.; and Sedwards, S. 2013. Importance Splitting for Statistical Model Checking Rare Properties. In *Proc. of the 25th International Conference on Computer Aided Verification (CAV'13)*, 576–591. Springer-Verlag.

Kahn, H., and Harris, T. E. 1951. Estimation of particle transmission by random sampling. *National Bureau of Standards applied mathematics series* 12:27–30.

Kahn, H. 1955. Use of different monte carlo sampling techniques. *Rand Corporation*.

Kalajdzic, K.; Jégourel, C.; Lukina, A.; Bartocci, E.; Legay, A.; Smolka, S. A.; and Grosu, R. 2016. Feedback Control for Statistical Model Checking of Cyber-Physical Systems. In *Proc. of the International Symposium Leveraging Applications of Formal Methods, Verification and Validation: Foundational Techniques (ISoLA'16)*, LNCS, 46–61. Springer.

Kennedy, J., and Eberhart, R. 1995. Particle swarm optimization. In *Proc. of 1995 IEEE International Conference on Neural Networks*, 1942–1948.

Russell, S., and Norvig, P. 2010. *Artificial Intelligence: A Modern Approach*. Prentice-Hall, 3rd edition.

Weimerskirch, H.; Martin, J.; Clerquin, Y.; Alexandre, P.; and Jiraskova, S. 2001. Energy saving in flight formation. *Nature* 413(6857):697–698.

Yang, J.; Grosu, R.; Smolka, S. A.; and Tiwari, A. 2016. Love Thy Neighbor: V-Formation as a Problem of Model Predictive Control (Invited Paper). In *Proc. of the 27th International Conference on Concurrency Theory (CONCUR'16)*, volume 59 of *LIPIcs*, 4:1–4:5. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.