High-assurance provably correct controller synthesis of aerospace cyber-physical systems using Bayesian model checking

Sumit Kumar Jha, EECS Department, University of Central Florida, Orlando, FL
Steven L. Drager, High-Assurance Systems Branch, Air Force Research Laboratory, Rome, NY
Brent Miller, EECS Department, University of Central Florida, Orlando, FL

The U.S. Congress has recently mandated [1, 2] the integration of Unmanned Aerial Systems (UAS) into the U.S. airspace protocols and recommended that the Federal Aviation Administration consider granting UAS licenses more broadly (to public entities and commercial institutions) as early as 2015. It has been estimated that the proposed changes in the regulatory framework will lead to as many as 7,500 unmanned aerial systems in the U.S. airspace over a period of five years.

The development of autonomous unmanned aerial vehicles will provide an opportunity for cost-effective transportation and surveillance that does not require constant oversight by expert, well-trained and expensive human pilots. A fundamental concern in the use of such unmanned aerial systems is the assured safe and correct functioning of these devices. It is widely recognized that even a few accidents involving UAS can quickly shape an adverse public opinion, and hence delay the pervasive adoption of unmanned aerial systems for several years. Thus, there is an urgent need for designing provably correct high-assurance controllers for such autonomous unmanned aerial systems.

Traditionally, autonomous aerial vehicles have employed PID (proportional-integral-derivative) and model predictive controllers (MPC). Both of these approaches [3-5] use online computations to make course corrections in the flight of autonomous UAS; these computations are simple enough that they could be performed in a real-time manner using off-the-shelf single-core 100 MHz or more embedded and consumer-grade processors. Modern unmanned aerial systems can carry high-performance 10 Gigaflop Field Programmable Gate Arrays (FPGAs) and other modern high-performance low-power multi-core processors, and the newer wireless standards have enabled wireless communication with bandwidth as high as 500 Mbit/sec. Thus, there is a gap between the availability of processing and communication capacity, and the ability of existing control algorithms to leverage these recent hardware advances.

We envision a scenario where we employ Bayesian model checking [6, 7] of detailed computational modeling of the aerodynamics of unmanned aerial systems against a suite of probabilistic complex safety and performance specifications to discover optimal control strategies for the provably safe flight of autonomous UAS. The desired trajectory of an autonomous UAS can be described using linear spatiotemporal logic; the same specification framework can be used to encode safety constraints such as minimal distance from fixed geographical structures and other aerial systems. The probabilistic version of the linear spatiotemporal logic can be used to describe performance requirements such as minimization of fuel costs, maximization of speed, or the guarantee of sustained flight using low-power solar power systems. We need to investigate an aerospace version of probabilistic linear spatiotemporal logic and the automated synthesis of such specifications automatically and transparently from geo-spatial trajectories and airspace protocols.

Bayesian model checking [8-10] has been successively employed to verify hardware, software, biological and cyber-physical systems, and has been shown to be a very competitive statistical model checking algorithms that requires a small number of simulation samples to verify complex computational stochastic models. We envision the invention of high-performance Bayesian model checking algorithm that can employ information on the cost of performing simulations and the cost of a potential failure of the unmanned aerial system to determine a control strategy that provably minimizes the value-at-risk of the combined validation and deployment phases of the unmanned aerial system.

We conjecture that such a verified control strategy will create high-assurance unmanned aerial systems that can be readily and safely deployed. Further, their rapid adoption will not only accelerate our economic growth but also address problems of socio-economic inequity such as the existence of food deserts. We believe that the successful design of high-assurance provably correct UAS will bring the same revolution of equal access in the physical world that the Internet has brought in the world of information. The use of unverified controllers and systems would make the UAS technology vulnerable to adverse public opinion and potential rejection as a technology that is not mature for civilian use.

References

1. Modernization, F., *Reform Act of 2012.* Public Law, 2012: p. 112-95.
2. Mulligan, J., *Legal and Policy Issues in the FAA Modernization and Reform Act of 2012.* Issues in Aviation Law and Policy, 2012. **11**(3).
3. Shan, D., et al. *PID Parameters Tuning Based on Self-Adaptive Hybrid Particle Swarm Optimization Algorithm*. in *Proceedings of the International Conference on Information Engineering and Applications (IEA) 2012*. 2013. Springer.
4. Visioli, A., *Practical PID control*. 2006: Springer.
5. Garcia, C.E., D.M. Prett, and M. Morari, *Model predictive control: theory and practice—a survey.* Automatica, 1989. **25**(3): p. 335-348.
6. Jha, S.K. and C.J. Langmead, *Exploring behaviors of stochastic differential equation models of biological systems using change of measures.* BMC bioinformatics, 2012. **13**(Suppl 5): p. S8.
7. Jha, S.K., et al., *A Bayesian approach to model checking biological systems*, in *Computational Methods in Systems Biology* 2009. p. 218-234.
8. Clarke, E.M. and P. Zuliani, *Statistical model checking for cyber-physical systems*, in *Automated Technology for Verification and Analysis*. 2011, Springer. p. 1-12.
9. Zuliani, P., A. Platzer, and E.M. Clarke. *Bayesian statistical model checking with application to Simulink/Stateflow verification*. in *Proceedings of the 13th ACM international conference on Hybrid systems: computation and control*. 2010. ACM.
10. Jha, S.K., *Model validation and discovery for complex stochastic systems*, in *Computer Science Department*2010, Carnegie Mellon University: Pittsburgh.