Control Theory and Technology
https://doi.org/10.1007/s11768-020-00008-w

LETTER

Recent advances on formal methods for safety and security of cyber-physical systems

Xiang Yin[1,2] · **Shaoyuan Li**[1,2]

Received: 21 September 2020 / Accepted: 21 September 2020

Cyber-physical systems (CPSs) are engineering systems with both computational and physical components [1]. Typical CPSs include energy systems, transportation systems, autonomous vehicles, etc. CPSs are usually hybrid involving complex interactions of continuous dynamics with discrete logics. The development of controller design and verification algorithms for such complex systems are crucial and challenging tasks. Ever-increasing demands for safety and security of CPSs put stringent constraints on their analysis and design, and necessitate the use of formal model-based approaches. In recent years, we have witnessed a substantial increase in the use of formal techniques for the verification and design of safety–critical and security-sensitive CPSs [2].

Due to the complex functionalities of safety–critical CPSs, ensuring safety is extremely challenging. In particular, since CPSs involve both continuous and discrete dynamics, safety not only requires that the low-level physical trajectory is within constrained regions, e.g., the value of the state should never exceed a threshold, but also requires that the high-level behavior of the system satisfies some desired specifications, e.g., executing a set of tasks in a right order. However, existing control theory mainly focuses on simple low-level specifications such as stability. To describe functional safety of the high-level behaviors of CPSs, more rich specification languages, such as regular languages and linear temporal logics (LTL), are needed. Also, security-related attacks are increasingly becoming pervasive in safety–critical cyber-physical systems; such security vulnerabilities related to information leaks in CPSs are extremely difficult to discover and mitigate as the interaction between the embedded control software and the physical environment exposes numerous attack surfaces for malicious exploitation.

To enforce complex specifications for safety–critical cyber-physical systems, one of the most popular approaches developed in the past 50 years is the abstraction-based approach, which consists of the following steps: 1) abstract the original infinite continuous system as a finite symbolic system; 2) synthesize a supervisory controller based on the symbolic model to enforce desired specifications; 3) refine the symbolic controller synthesized to control the original system. To construct the symbolic model, a typical approach is to discretize the state-space to induce a finite quotient system. The key here is to establish certain relationship between the original system and its abstraction. In the seminal work of [3], the notion of approximate bi-simulation relation was proposed to capture the equivalence of two models with guaranteed abstraction error; this idea was further extended to the notion of alternating bi-simulation relation for the purpose of control [4]. Recently in [5], a more unified relation called feedback refinement relation was proposed. Compositional approaches have also been developed to compute finite abstractions for large-scale interconnected CPSs [6].

When the symbolic model and the original system are related (usually guaranteed by the abstraction procedure), the synthesized symbolic controller can be refined back to control the original system. To synthesize such feedback controllers for complex specifications based on symbolic models, many synthesis techniques are developed by both the computer science community in the context of the reactive synthesis (RS) and by the control engineering community in the context of the supervisory control theory (SCT). The essences of the RS and the SCT are very similar; both of them consider a game between the decision-maker and the environment (disturbances or adversaries). The main difference between the RS and the SCT is that the RS considers open systems with I/O properties, while the SCT considers specific plants [7]. One of the most significant recent developments in the RS is the concept of GR(1) synthesis

✉ Xiang Yin
yinxiang@sjtu.edu.cn

[1] Department of Automation, Shanghai Jiao Tong University, Shanghai 200240, China

[2] Key Laboratory of System Control and Information Processing, Ministry of Education, Shanghai 200240, China

Published online: 02 November 2020

[8]. By considering a restrictive but still expressive enough sub-class of LTL formulae, the synthesis complexity can be reduced tremendously from 2EXP to polynomial time. GR(1) synthesis has became a very successful and popular tool in the design of logic controller for autonomous robots [9]. In the context of the SCT, one of the major breakthroughs in the past 5 years is the synthesis of supervisors under imperfect information. In the series works of Yin and Lafortune [10–12], a uniform framework for synthesizing partially observation supervisory controllers was proposed; this framework is applicable to a large class of properties including both functional safety and information-flow security.

Although formal methods provide algorithmic and correct-by-construction procedures for the certification and enforcement of safety, the main challenging is the curse of dimensionality. In particular, in abstraction-based approach aforementioned, the size of the symbolic model grows exponentially fast as the dimension of the underlying system grows. Furthermore, controller synthesis for some classes of specifications is also computationally difficult, e.g., the general LTL synthesis problem is 2EXP as mentioned. Therefore, how to mitigate the computational complexity is the central topic in this area in the past years. To tackle this challenging, abstraction-free approaches have also been drawing considerable attention. One of the most important abstraction-free formal synthesis techniques developed recently is the use of control barrier functions (CBFs). In [13], where the notion of CBF was first proposed, the authors proposed to use CBF to achieve physical safety such that the dynamic trajectory is always within a safe set. Quadratic programming is used to obtain optimal control inputs satisfying safety constraints. More recently, the idea of CBF was further leveraged to achieve more complex specifications described by temporal logics. For example, in [14], the authors propose how to construct CBFs for signal temporal logic (STL) specifications. In [15], CBFs are used to enforce LTL specifications for stochastic systems. Another recently developed approach for mitigating computational complexity is to use data-driven methods. Along this line, reinforcement learning techniques have been introduced to the framework of formal synthesis. For example, in [16, 17], the authors propose new safe RL algorithms that learn control policies with safety and complex formal specifications guarantees.

Compared with safety that is usually related to the actually behavior of the system, security and privacy are usually related to the information flow of the system, i.e., the information released by the dynamic system to the outside world. Formal techniques have also been applied to the verification and synthesis of information-flow security for CPSs. One of the most widely adopted formal information-flow security properties is the notion of opacity. Roughly speaking, opacity is a confidentiality property that captures the plausible deniability of the secret behavior. Readers are referred to the recent survey [18] for more details. The notion of opacity was originally applied to security for symbolic systems. Recently, this concept has been extended to CPSs with continuous dynamics. For example, in [19, 20], opacity for linear systems was investigated. In [21], the authors provided a new approximate simulation relation that preserves opacity. Hence, existing techniques for finite systems can be leveraged to verify opacity for incremental stable nonlinear systems with infinite states.

We briefly presented some recent advances in formal methods for safety and security of CPSs, which have been tremendously successful in the past 50 years. However, most of the existing formal methods depend heavily on system models and suffer from the very high computational complexity. An important future direction in formal methods for CPSs is to leverage results from data-driven methods to improve the scalability of the computation procedures and to relax the dependency on precise system models.

References

1. Alur, R. (2015). *Principles of Cyber-physical Systems*. Cambridge: MIT Press.
2. Belta, C., Yordanov, B., & Gol, E. A. (2017). *Formal Methods for Discrete-time Dynamical Systems* (Vol. 89). Berlin: Springer.
3. Girard, A., & Pappas, G. J. (2007). Approximation metrics for discrete and continuous systems. *IEEE Transactions on Automatic Control, 52*(5), 782–798.
4. Zamani, M., Pola, G., Mazo, M., & Tabuada, P. (2011). Symbolic models for nonlinear control systems without stability assumptions. *IEEE Transactions on Automatic Control, 57*(7), 1804–1809.
5. Reissig, G., Weber, A., & Rungger, M. (2017). Feedback refinement relations for the synthesis of symbolic controllers. *IEEE Transactions on Automatic Control, 62*(4), 1781–1796.
6. Meyer, P. J., Girard, A., & Witrant, E. (2017). Compositional abstraction and safety synthesis using overlapping symbolic models. *IEEE Transactions on Automatic Control, 63*(6), 1835–1841.
7. Ehlers, R., Lafortune, S., Tripakis, S., & Vardi, M. Y. (2017). Supervisory control and reactive synthesis: a comparative introduction. *Discrete Event Dynamic Systems, 27*(2), 209–260.
8. Bloem, R., Jobstmann, B., Piterman, N., Pnueli, A., & Sa'ar, Y. (2012). Synthesis of reactive (1) designs. *Journal of Computer and System Sciences, 78*(3), 911–938.
9. Kress-Gazit, H., Lahijanian, M., & Raman, V. (2018). Synthesis for robots: Guarantees and feedback for robot behavior. *Annual Review of Control, Robotics, and Autonomous Systems*, *1*, 211–236.
10. Yin, X., & Lafortune, S. (2016). A uniform approach for synthesizing property-enforcing supervisors for partially-observed discrete-event systems. *IEEE Transactions on Automatic Control, 61*(8), 2140–2154.
11. Yin, X., & Lafortune, S. (2016). Synthesis of maximally permissive supervisors for partially-observed discrete-event systems. *IEEE Transactions on Automatic Control, 61*(5), 1239–1254.

12. Yin, X., & Lafortune, S. (2017). Synthesis of maximally-permissive supervisors for the range control problem. *IEEE Transactions on Automatic Control, 62*(8), 3914–3929.
13. Ames, A. D., Xu, X., Grizzle, J. W., & Tabuada, P. (2016). Control barrier function based quadratic programs for safety critical systems. *IEEE Transactions on Automatic Control, 62*(8), 3861–3876.
14. Lindemann, L., & Dimarogonas, D. V. (2019). Control barrier functions for signal temporal logic tasks. *IEEE Control Systems Letters, 3*(1), 96–101.
15. Jagtap, P., Soudjani, S., & Zamani, M. (2020). Formal synthesis of stochastic systems via control barrier certificates. *IEEE Transactions on Automatic Control*. https://doi.org/10.1109/TAC.2020.3013916.
16. Fulton, N., & Platzer, A. (2018). Safe reinforcement learning via formal methods. *32nd AAAI Conference on Artificial Intelligence,* (pp. 6485–6492). New Orleans, LA.
17. Li, X., Serlin, Z., Yang, G., & Belta, C. (2019). A formal methods approach to interpretable reinforcement learning for robotic planning. *Science Robotics*, *4*(37),
18. Lafortune, S., Lin, F., & Hadjicostis, C. N. (2018). On the history of diagnosability and opacity in discrete event systems. *Annual Reviews in Control, 45,* 257–266.
19. An, L., & Yang, G. H. (2020). Opacity enforcement for confidential robust control in linear cyber-physical systems. *IEEE Transactions on Automatic Control, 65*(3), 1234–1241.
20. Ramasubramanian, B., Cleaveland, R., & Marcus, S. I. (2020). Notions of centralized and decentralized opacity in linear systems. *IEEE Transactions on Automatic Control, 65*(4), 1442–1455.
21. Yin, X., Zamani, M., & Liu, S. (2020). On approximate opacity of cyber-physical systems. *IEEE Transactions on Automatic Control*. https://doi.org/10.1109/TAC.2020.2998733.

Xiang Yin was born in Anhui, China, in 1991. He received the B.Eng degree from Zhejiang University in 2012, the M.Sc. degree from the University of Michigan, Ann Arbor, in 2013, and the Ph.D. degree from the University of Michigan, Ann Arbor, in 2017, all in Electrical Engineering. Since 2017, he has been with the Department of Automation, Shanghai Jiao Tong University, where he is an Associate Professor. His research interests include formal methods, discrete-event systems and cyber-physical systems. Dr. Yin also received the IEEE Conference on Decision and Control (CDC) Best Student Paper Award Finalist in 2016. He is the co-chair of the IEEE CSS Technical Committee on Discrete Event Systems. He is also a member of the IEEE CSS Conference Editorial Board.

Shaoyuan Li was born in Hebei, China, in 1965. He received the B.Sc. and M.Sc. degrees in Automation from the Hebei University of Technology, Tianjin, China, in 1987 and 1992, respectively, and the Ph.D. degree from Nankai University, Tianjin, in 1997. Since 1997, he has been with the Department of Automation, Shanghai Jiao Tong University, Shanghai, China, where he is currently a Professor. His current research interests include model predictive control, dynamic system optimization, and cyber-physical systems. He is the vice-president of the Chinese Association of Automation.