IEEE Control Systems Society
Technical Committee on Discrete Event Systems

Newsletter **October 2024**

Editor: Xiang Yin
Chair, IEEE CSS Technical Committee on DES
Associate Professor
Department of Automation, Shanghai Jiao Tong University
SEIEE Building 2-443, Dongchuan Rd 800, Shanghai, 200240, China

Phone: (+86) 021-34204022
Email: yinxiang@sjtu.edu.cn
Website: http://xiangyin.sjtu.edu.cn

Welcome to the 2024 October issue of the newsletter, also available online at
https://ieeecss.org/tc/discrete-event-systems/newsletters

Editorial

You are welcome to submit new items to the newsletter (topics including schools, workshops, sessions, conferences, journals, books, software, positions). Also please encourage relevant colleagues and students to subscribe to this newsletter.

- To **submit a new item**, please email to yinxiang@sjtu.edu.cn.
- To **subscribe**, please email to yinxiang@sjtu.edu.cn.
- To **unsubscribe**, please reply to this email with the subject line UNSUBSCRIBE.

Contents

1 Selections of Journal Publications

Contributed by: Xiang Yin (yinxiang@sjtu.edu.cn)

1.1. Discrete Event Dynamic Systems Theory and Applications

Volume: 34, Issue: 3, September 2024

- **An extremum timed extended reachability graph for temporal analysis of time Petri nets**
  Authors: Jiazhong Zhou ; Dimitri Lefebvre ; Zhiwu Li
  Abstract: In this paper, a type of graph, called an extremum timed extended reachability graph, is designed to abstract the temporal specifications and represent the feasible trajectories of time Petri nets. This graph improves the timed extended reachability graph recently proposed for time Petri nets (Lefebvre. Discrete Event Dynamic Systems 29(1):31–56. (2019); Zhou et al. IEEE Trans Autom Control 67(7):3693–3698. (2022)) by replacing the earliest-firing policy with a more general policy. In detail, when a transition is preselected for the next firing, the firing can be delayed for a certain period after its minimal residual time has elapsed, rather than immediately firing once its minimal residual time has elapsed. Then, a sampled timed extended reachability graph is designed, wherein, for a transition preselected to fire next, a finite number of time points within a time interval, starting at minimal residual time and ending at maximal residual time, are selected as the firing time instants for the preselected transition. Furthermore, a special case of the sampled timed extended reachability graph, called an extremum timed extended reachability graph that details only the minimal and maximal residual times of the transitions, is also proposed. For a feasible sequence, the corresponding feasible trajectories with minimal and maximal durations are easy to compute with this graph. Thus, an end-to-end delay of a feasible sequence can be obtained by directly searching the graph. Finally, the scheduling of a typical flexible manufacturing system illustrates the advantages and applications of the proposed approach.
- **A tropical-algebraic method for the control of timed event graphs with partial synchronization**
  Authors: Germano Schafaschek ; Laurent Hardouin ; Jörg Raisch
  Abstract: This paper studies a scenario in which the occurrence of one or more events in a discrete event system is subject to external restrictions which may change unexpectedly during run-time. The system is modeled as a timed event graph (TEG) and, in this context, the presence of the aforementioned external restrictions has become known as partial synchronization (PS). This phenomenon arises naturally in several applications, from manufacturing to transportation systems. We develop a formal and systematic method to compute optimal control signals for TEGs in the presence of PS, where the control objective is tracking a given output reference as closely as possible and optimality is understood in the widely-adopted just-in-time sense. The approach is based on the formalism of tropical semirings — in particular, the min-plus algebra and derived semiring of counters. We claim that our method expands modeling and control capabilities with respect to previously existing ones by tackling the case of time-varying PS restrictions, which, to the best of our knowledge, has not been dealt with before in this context.
- **Diagnosability and attack detection for discrete event systems under sensor attacks**
  Authors: Feng Lin ; Stéphane Lafortune ; Caisheng Wang
  Abstract: This paper extends the theory of diagnosability by investigating fault diagnosis in discrete event systems under sensor attacks using finite-state automata as models. It assumes that an attacker has compromised the communication channel between the system's sensors and the diagnostic engine. While the general attack model utilized by the attacker has been previously studied in the context of supervisory control, its application to fault diagnosis remains unexplored. The attacker possesses the capability to substitute each compromised observable event with a string from an attack language. The attack model incorporates event insertion and deletion, as well as static and dynamic attacks. To formally capture the diagnostic engine's ability to identify faults in the presence of the attacker, a novel concept called CA-diagnosability is introduced. This extends the existing notions of CA-controllability and CA-observability. A testing procedure for CA-diagnosability is developed, and its correctness is proven. Some sufficient conditions for CA-

diagnosability that can be easily checked are also proposed and proved. The paper then investigates conditions under which the role of an attacker can be reverted from malicious to benevolent, that is, to help the diagnoser to diagnose faults. The paper further applies diagnosability theory to investigate conditions under which the presence of the attacker can be detected.

Back to the contents

1.2. IEEE Transactions on Automatic Control

Volume: 69, Issue: 10, October 2024

- **Bounded Synthesis and Reinforcement Learning of Supervisors for Stochastic Discrete Event Systems With LTL Specifications**
  Authors: Ryohei Oura ; Toshimitsu Ushio ; Ami Sakakibara
  Abstract: In this article, we consider supervisory control of stochastic discrete event systems (SDESs) under linear temporal logic specifications. Applying the bounded synthesis, we reduce the supervisory synthesis to the problem of satisfying a safety condition. First, we consider a directed controller that allows at most one controllable event to be enabled. We assign a negative reward to the unsafe states and introduce an expected return with a state-dependent discount factor. We compute a winning region and a directed controller with the maximum satisfaction probability using a dynamic programming method, where the expected return is used as a value function. Next, we construct a permissive supervisor via the optimal value function. We show that the supervisor accomplishes the maximum satisfaction probability and maximizes the reachable set within the winning region. Finally, for an unknown SDES, we propose a two-stage model-free reinforcement learning method for efficient learning of the winning region and the directed controllers with the maximum satisfaction probability. We also demonstrate the effectiveness of the proposed method by simulation.
- **Verification of Hyperproperties for Dynamical Systems via Barrier Certificates**
  Authors: Mahathi Anand ; Vishnu Murali ; Ashutosh Trivedi ; Majid Zamani
  Abstract: Hyperproperties are system properties that require quantification over multiple execution traces of a system. Hyperproperties can express several specifications of interest for cyber–physical systems—such as opacity, robustness, and noninterference—which cannot be expressed using linear time properties. This article presents for the first time a discretization-free approach for the formal verification of discrete-time dynamical systems against hyperproperties. The proposed approach involves the decomposition of complex hyperproperties into several verification conditions by exploiting the automata-based structures corresponding to the complements of the original specifications. These verification conditions are then discharged by synthesizing so-called augmented barrier certificates , which provide certain safety guarantees for the underlying system. For systems with polynomial-type dynamics, we present a sound procedure to synthesize polynomial-type augmented barrier certificates by reducing the problem to sum-of-squares optimizations. We demonstrate the effectiveness of our proposed approaches on two physical case studies against two important hyperproperties: initial-state opacity and initial-state robustness.
- **Hybrid Control Barrier Functions for Continuous-Time Systems**
  Authors: Mathias Marley ; Roger Skjetne ; Andrew R. Teel
  Abstract: Control barrier functions (CBFs) enable constraint satisfaction in controlled dynamical systems, by mapping state constraints into state-dependent input constraints. This article investigates the use of hybrid CBF formulations for constraint satisfaction in continuous-time systems. Augmenting CBFs with logic variables enables solving control problems that are not solvable by continuous, or even discontinuous, control. Examples include robust deadlock resolution for vehicles moving in the presence of bounded obstacles, and robust obstacle avoidance for nonholonomic vehicles required to maintain a nonzero forward speed. A recursive procedure for constructing hybrid high-order CBFs is proposed, thereby extending hybrid CBFs to systems with high-order safety constraints. The theoretical results are illustrated by several examples.
- **Relative Q-Learning for Average-Reward Markov Decision Processes With Continuous States**

Authors: Xiangyu Yang ; Jiaqiao Hu ; Jian-Qiang Hu
Abstract: Markov decision processes (MDPs) are widely used for modeling sequential decision-making problems under uncertainty. We propose an online algorithm for solving a class of average-reward MDPs with continuous state spaces in a model-free setting. The algorithm combines the classical relative Q-learning with an asynchronous averaging procedure, which permits the Q-value estimate at a state–action pair to be updated based on observations at other neighboring pairs sampled in subsequent iterations. These point estimates are then retained and used for constructing an interpolation-based function approximator that predicts the Q-function values at unexplored state–action pairs. We show that with probability one the sequence of function approximators converges to the optimal Q-function up to a constant. Numerical results on a simple benchmark example are reported to illustrate the algorithm.

- **Noninterference Analysis of Bounded Petri Nets Using Basis Reachability Graph**
Authors: Ning Ran ; Jingyao Nie ; Aiwen Meng ; Carla Seatzu
Abstract: In this article, we deal with two problems related to security and privacy of bounded Petri nets, namely, noninterference analysis and enforcement. A system could be monitored by different types of users, high-level and low-level users, who have access to different information even if both know the structure of the system. Low-level users can observe only the occurrence of a subset of events. On the contrary, high-level users can observe the occurrence of all the events affecting the system dynamics. A system is said noninterferent if low-level users cannot infer the occurrence of those events that are observable only by high-level users. In this article, we deal with the problems of analysis and enforcement of a particular noninterference property, namely, strong nondeterministic noninterference (SNNI). In particular, we show that, under the assumption of acyclicity of the high-level subnet, the notions of basis marking and basis reachability graph allow to solve the problems of SNNI analysis and enforcement with clear advantages in terms of computational complexity since they prevent exhaustive marking enumeration.

- **Concealability Analysis for Current-State Opacity Enforcement via Editing Functions**
Authors: Kun Peng ; Yufeng Chen ; Carla Seatzu ; Zhiwu Li ; Alessandro Giua
Abstract: This article focuses on the problem of enforcing current-state opacity of a discrete event system via editing functions. In more detail, the observation exposed to an intruder is modified, either erasing or inserting some observations, so as to guarantee that the intruder is not able to discover the predefined secret. The notion of concealability, which formalizes the possibility of maintaining the secret hidden, is introduced starting from defining some illegal states on a particular structure called joint observer. An algorithm for the analysis of concealability is proposed. Finally, an online procedure to make the system opaque is proposed by selecting an editing function.

- **Event Concealment and Concealability Enforcement in Discrete Event Systems Under Partial Observation**
Authors: Wei Duan ; Christoforos N. Hadjicostis ; Zhiwu Li
Abstract: In this article, we investigate event concealment and concealability enforcement in discrete event systems modeled as nondeterministic finite automata under partial observation. Given a subset of secret events in a given system, concealability holds if the occurrences of all secret events remain hidden to a curious observer (an eavesdropper). When concealability of a system does not hold, we analyze how a defensive function, placed at the interface of the system with the eavesdropper, can be used to enforce concealability by manipulating the observations generated by the system using event deletions, insertions, or replacements. The defensive function is said to be C -enforcing if, following the occurrence of secret events and regardless of earlier and subsequent activity generated by the system, it can always deploy a strategy to manipulate observations and conceal the secret events perpetually. We propose a polynomial complexity construction for obtaining one necessary and one sufficient condition for C -enforceability.

- **Optimal Communication and Control Strategies in a Cooperative Multiagent MDP Problem**
Authors: Sagar Sudhakara ; Dhruva Kartik ; Rahul Jain ; Ashutosh Nayyar
Abstract: The problem of controlling cooperative multiagent systems under different models of information sharing among agents has received significant attention in the recent literature. In this

article, we consider a setup where rather than committing to a fixed and nonadaptive information sharing protocol (e.g., periodic sharing or no sharing, etc.), agents can dynamically decide at each time step whether to share information with each other and incur the resulting communication cost. This setup requires a joint design of agents' communication and control strategies in order to optimize the tradeoff between communication costs and the control objective. We first show that agents can ignore a big part of their private information without compromising the system performance. We then provide a common-information-approach-based solution for the strategy optimization problem. This approach relies on constructing a fictitious partially observable markov decision process (POMDP) whose solution (obtained via a dynamic program) characterizes the optimal strategies for the agents. We extend our solution to incorporate time-varying packet-drop channels and constraints on when and how frequently agents can communicate.

Back to the contents

1.3. Automatica

Volume: 168, October 2024

- **Robust Q-learning algorithm for Markov decision processes under Wasserstein uncertainty**
  Authors: Ariel Neufeld ; Julian Sester
  Abstract: We present a novel Q-learning algorithm tailored to solve distributionally robust Markov decision problems where the corresponding ambiguity set of transition probabilities for the underlying Markov decision process is a Wasserstein ball around a (possibly estimated) reference measure. We prove convergence of the presented algorithm and provide several examples also using real data to illustrate both the tractability of our algorithm as well as the benefits of considering distributional robustness when solving stochastic optimal control problems, in particular when the estimated distributions turn out to be misspecified in practice.

Back to the contents

1.4. IEEE Transactions on Systems, Man, and Cybernetics: Systems

Volume: 54, Issue: 10, October 2024

- **Supervisor Synthesis Using Labeled Petri Nets for Forbidden State Specifications**
  Authors: Yihui Hu ; Ziyue Ma ; Ruotian Liu ; Maria Pia Fanti ; Zhiwu Li
  Abstract: This research focuses on the forbidden state problem in the framework of labeled Petri nets (LPNs), i.e., to design a supervisor for a plant modeled by an LPN such that the closed-loop system cannot reach a set of predefined forbidden markings and does not contain any deadlock. Different from the traditional control scheme, the supervisor derived by this work can not only observe the observable transitions, but also the quiescence information. First, a new structure named an extended basis reachability graph (EBRG) is introduced to describe the reachability space of an LPN without computing all reachable markings. Based on an EBRG, a basis observer is then excogitated to represent the behavior of an LPN. Some states in the basis observer are defined as bad states and control-induced deadlocks, which relates to the undesirable behavior of the plant. Finally, an algorithm is introduced to compute a supervisor based on the basis observer. The consideration of system quiescence provides extra information on the marking estimation of the closed-loop system such that certain disabled transitions are re-enabled. Consequently, the developed supervisor in this article is generally more permissive than those do not observe the quiescence.

Back to the contents

1.5. IEEE/CAA Journal of Automatica Sinica

Volume: 11, Issue: 10, October 2024

- **Hierarchical Controller Synthesis Under Linear Temporal Logic Specifications Using Dynamic Quantization**
  Authors: Wei Ren ; Zhuo-Rui Pan ; Weiguo Xia ; Xi-Ming Sun

Abstract: Linear temporal logic (LTL) is an intuitive and expressive language to specify complex control tasks, and how to design an efficient control strategy for LTL specification is still a challenge. In this paper, we implement the dynamic quantization technique to propose a novel hierarchical control strategy for nonlinear control systems under LTL specifications. Based on the regions of interest involved in the LTL formula, an accepting path is derived first to provide a high-level solution for the controller synthesis problem. Second, we develop a dynamic quantization based approach to verify the realization of the accepting path. The realization verification results in the necessity of the controller design and a sequence of quantization regions for the controller design. Third, the techniques of dynamic quantization and abstraction-based control are combined together to establish the local-to-global control strategy. Both abstraction construction and controller design are local and dynamic, thereby resulting in the potential reduction of the computational complexity. Since each quantization region can be considered locally and individually, the proposed hierarchical mechanism is more efficient and can solve much larger problems than many existing methods. Finally, the proposed control strategy is illustrated via two examples from the path planning and tracking problems of mobile robots.

Back to the contents

2 Conferences

Contributed by: Xiang Yin (yinxiang@sjtu.edu.cn)

2.1 **2024 IEEE Conference on Decision and Control (CDC)**
Milan, Italy, December 16-19, 2024.
https://cdc2024.ieeecss.org/

2.2 **2025 ACM International Conference on Hybrid Systems: Computation and Control (HSCC)**
Irvine, California, USA, May 6-9, 2025.
https://hscc.acm.org/2025/

2.3 **2025 IEEE International Conference on Robotics and Automation (ICRA)**
Atlanta, USA, May 19-23, 2025.
https://2025.ieee-icra.org/

2.4 **2025 Annual Learning for Dynamics Control Conference (L4DC)**
Ann Arbor, Michigan, USA, June 4-6, 2025.
https://sites.google.com/umich.edu/l4dc2025/

2.5 **2025 European Control Conference (ECC)**
Thessaloniki, Greece, June 24-27, 2025.
https://ecc25.euca-ecc.org/

2.6 **2025 American Control Conference (ACC)**
Denver, Colorado, USA, July 8-10, 2025.
https://acc2025.a2c2.org/

2.7 **2025 International Conference on Automation Science and Engineering (CASE)**
Los Angeles, California, USA, August 17-21, 2025.
https://2025.ieeecase.org/

2.8 **2025 IEEE Conference on Control Technology and Applications (CCTA)**
San Diego, California, USA, August 25-27, 2025.
https://ccta2025.ieeecss.org/

2.9 **2025 IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)**
Porto, Portugal, September 9-12, 2025.
https://etfa2025.ieee-ies.org/

2.10 **2025 International Conference on Systems, Man, and Cybernetics (SMC)**
Vienna, Austria, October 5-8, 2025.
https://www.ieeesmc2025.org/

Back to the contents

3 Books

3.1 Cybersecurity of Discrete Event Systems—From Smart Attacks to Resilient Defence

Author: Rong Su, Nanyang Technological University.

Description: This book describes analysis and control against smart cyberattacks in discrete event systems (DES), modelled by regular languages or finite-state automata. “Smart attacks" cannot be detected by the supervisor until an irreversible process towards ensured damage occurs. An attack may be conducted either in the observation channel (i.e., the input of the supervisor) or in the command channel (i.e., the output of the supervisor), or both simultaneously. Therefore, defense strategies against these attacks are urgently needed. This book provides an overview of the latest theories and includes empirical examples to illustrate concepts and methods. By centering on what information is available and how such information is used, the readers are provided with methods to evaluate the cyber vulnerability of a given system and to design a resilient supervisor against relevant smart attacks. By focusing on a conceptual introduction and systematic analysis, this book provides a solid theoretical foundation for future exploration by researchers and graduate students who are interested in cybersecurity research, not necessarily limited to those in the DES community. Readers are recommended to have a background in formal language theory.

Additional information on the book can be found at
https://www.routledge.com/Cybersecurity-of-Discrete-Event-Systems-From-Smart-Attacks-to-Resilient
Su/p/book/9781032368108?srsltid=AfmBOor9fqjhOR7YfMgGE8coz0rHXF6YyKhoucc7UzqYlY9GhcWpQBg3,
where an inspection copy is possible for educational institutions.

3.2 Graph-Theoretical Methods in Systems Theory and Control

Author: Jan Lunze, Ruhr-University, Germany

Description: The book describes for numerous scenarios how to use the structural properties of a system represented by a graph to simplify modelling, analysis, and design tasks. For example, block diagrams and coupling graphs can be used to decompose systems, automata graphs to analyse discrete-event systems and Markov chains, structure graphs to find generic properties of linear systems or communication graphs to design networked control systems. The book includes many examples derived from diverse fields of application, exercises with solutions and MATLAB scripts to implement graph-theoretical methods for systems analysis.

Additional information on the book can be found at
www.editionmora.de/gmsc

The book is produced as “print-on-demand" and can be ordered directly at the printer:
https://publish.bookmundo.de/books/349971

3.3 Safe Autonomy with Control Barrier Functions: Theory and Applications

Authors: Wei Xiao, Christos G. Cassandras, and Calin Belta

Description: The book presents the concept of Control Barrier Function (CBF), which captures the evolution of safety requirements during the execution of a system and can be used to enforce safety. Safety is central to autonomous systems since they are intended to operate with minimal or no human supervision. The book includes both theoretical and application perspectives on how safety can be guaranteed. It explains how the CBF approach is computationally efficient and can easily deal with nonlinear models and complex constraints used in a wide spectrum of applications, including autonomous driving, robotics, and traffic control. Safety guarantees can be integrated into the operation of such autonomous systems, including typical safety requirements that involve collision avoidance, technological system limitations, and bounds on real-time executions. Adaptive and event-driven approaches for safety are also discussed for time-varying execution bounds and noisy dynamics, as well as for systems with unknown dynamics.

Additional information on the book can be found at
https://link.springer.com/book/10.1007/978-3-031-27576-0
where an eBook version can also be downloaded (free for some educational institutions).

Back to the contents

4 Software Tools

4.1 Eclipse ESCET™ version 5.0 release

The Eclipse Supervisory Control Engineering Toolkit (Eclipse ESCET) project provides a model-based approach and toolkit for the development of supervisory controllers. It includes the languages CIF, Chi and ToolDef. ESCET, initially developed by Eindhoven University of Technology, is since January 2020 an Eclipse Foundation open-source project. More information can be found on the toolkit's website at https://www.eclipse.dev/escet/.

In October 2024, ESCET version 5.0 has been released and can be downloaded from https://www.eclipse.dev/escet/download.html. he main changes in this version are

- Annotations are now a stable CIF language feature.
- The CIF data-based synthesis tool now has a new 'Exploration strategy' option, featuring not only regular fixed edge order and the workset algorithm, but also a new third strategy: the saturation strategy. This new saturation strategy improves the performance of reachability computations. On average, for the CIF benchmark models, synthesis performance is improved 14.5 times, although the results differ per model. Saturation is now the new default exploration strategy. The 'Edge workset algorithm' option is no longer supported.
- The CIF controller properties checker now computes bounded response differently, using the execution scheme, which improves the performance of the check, and generally leads to lower bounds. Furthermore, the CIF controller properties checker now uses the saturation strategy for reachability computations, improving the performance of the non-blocking under control check.
- Several improvements to the (still experimental) new CIF PLC code generator have been included. The CIF code generator now generates code that adheres to the execution scheme prescribed by the CIF controller properties checker (see point above). As a result of this, some parts of the generated code are now in a different order.
- The CIF to mCRL2 transformer has been re-implemented and is now based on first linearizing the CIF specification. For recursive process call, now only the assigned variables are included, not all variables, and the arguments are named rather than positional, which reduces the model size and improves readability. No more summations, nor location pointers (sorts) for automata with only one location, are generated. See release notes for detailed changes in the CIF to mCRL2 transformer.

The full ESCET release notes, including links to the language specific release notes and release notes from previous versions, are available from https://www.eclipse.dev/escet/release-notes.html.

Back to the contents