Summary & Enabling Capabilities

UF UNIVERSITY of FLORIDA

Duke UNIVERSITY

TEXAS The University of Texas at Austin

UC SANTA CRUZ

Summary

- Center of Excellence faced with the challenge of laying the groundwork for assured autonomous operation in contested environments

Year 1 Outcomes

- Developed several key enabling theoretical cornerstones for continued development (see subsequent slides)
- Continue to integrate with AFRL research staff (internships, summer faculty fellows, joint publications, alumni joining AFRL), look to leverage and expand facilities and we look forward to new opportunities (DURIP, joint AFRL/AACE workshop)
- Continue to establish collaborations and investigate problems at the boundaries (joint publications, setting stage for joint workshops, student swaps) – hard to maintain RT boundaries
- Dissemination of research outcomes (publications, webpage, workshops, conference sponsorship/branding) – exceptional creativity and productivity

Enabling Capabilities

RT1

- Development of hybrid systems models/frameworks and generalizations of previous analysis methods that provide foundations for the integration of information dynamics and physical dynamics, e.g., intermittent information, inclusion of logic, and opportunistic learning
- Generation of tools to assure invariance and safety for nonlinear, nonsmooth, hybrid systems using nonsmooth barrier certificates satisfying sufficient conditions that are also necessary
- Formulation of a preliminary categorical framework for geometric analysis of systems with nonsmooth and hybrid dynamics
- Development of a framework for the formulation of optimization problems for hybrid systems and for the control of hybrid systems using model predictive control

Enabling Capabilities

RT2

- Advances in adaptive control methods (ICL – eliminating PE, time-varying parameters)
- RL-based ADP: Breaking down the barriers to computational constraints (sparse learning, StaF), including state constraints (barrier function), and for a broader class of systems (hybrid)
- Advances in control synthesis: sampling-based optimal control synthesis method (STyLuS* - Scalable Temporal Logic Synthesis), that can provably find solutions to problems with 10^800 states

Enabling Capabilities

RT3 & 4

- Establishing bounds on scalability and robustness (intermittency and asynchrony)
- Formulation of distributed algorithms for synchronization and estimation under intermittency
- Examining underlying assumptions related to attack behaviors, classifying, and detecting such behaviors
- Investigating role of learning in control over network (connections to RT2)
- Envisioning innovative applications (SwarmShield)

Enabling Capabilities

RT5

- Security-aware planning for autonomous systems using of-the-shelf model-checking tools - such plans provide strong mission guarantees even in the presence of attacks (e.g., sensor spoofing, false-data inject
- Developing foundation for a design framework that enables quantifiable tradeoffs between Quality-of-Control guarantees in the presence of attacks, and required system resources
- Introduced a general framework for analysis of discrete-event control systems in the presence of attacks (on sensors, actuators, communication, control software), as well as techniques and an open-source tool for synthesis of attack-resilient supervisory controllers with strong performance guarantees even under attack
- We show how hyperproperties, which capture the relationship between multiple executions simultaneously in time, as well as our probabilistic verification techniques enable safety even with uncertainties

Enabling Capabilities

RT6

- Developed a method for agents that interact with an environment to learn an unknown reward function with potential variations in the reward function due to an adversary
- constrained policy synthesis in multi-agent stochastic environments modeled by MDP to hundreds of agents with thousands of states for each (related to contributions in RT2)
- Developed a framework for reasoning about secure machine learning systems by abstracting the learning system problem setting to examine how to create adaptive systems for contested environments
- Developed an algorithm for privacy-preserving policy synthesis to take actions in an MDP while keeping its transition probabilities private