Collaborative Research: CPS: Small: An Integrated Reactive and Proactive Adversarial Learning for Cyber-Physical-Human Systems

Kyriakos G. Vamvoudakis (kyriakos@gatech.edu, http://kyriakos.ae.gatech.edu)
Daniel Guggenheim School of Aerospace Engineering, Georgia Institute of Technology
Zhong-Ping Jiang (zjiang@nyu.edu, https://engineering.nyu.edu/faculty/zhong-ping-jiang)
Tandon School of Engineering, New York University

1. Robustness and resilience analysis under DoS attacks

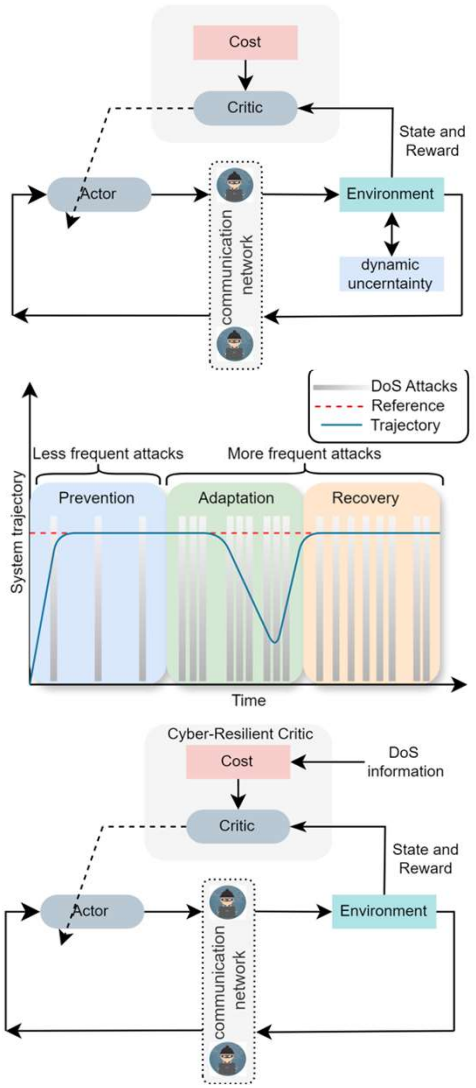
- Developed a resilient RL framework for partially linear systems facing parametric/dynamic uncertainties and DoS attacks. The controller learns from input-state data in real time under DoS attacks by leveraging policy iteration and adaptive dynamic programming.
- Through an integrated analysis using small-gain theory and identifying explicit constraints on DoS duration, the global asymptotic stability under DoS attacks is guaranteed.
- By incorporating the internal model principle with reinforcement learning, the proposed method ensures reference tracking under DoS attacks and system uncertainties.

2. Active learning-based control design under DoS attacks

- Proposed a reinforcement learning-based control scheme, integrating switching systems theory and adaptive dynamic programming under DoS attacks.
- Using known DoS patterns, a resilient controller is designed to maintain nominal performance and mitigate disruptions.
- As DoS patterns evolve, the controller is reconfigured in real time to preserve effectiveness under changing attack conditions.
- The reconfigured controller restores system performance by continuously refining policies and leveraging newly acquired data.

3. Adversarially Robust Pursuit-Evasion Games with Asymmetric and Incomplete Information

- Developed two separate customized receding horizon control-based differential games for the pursuer and evader such that the derived policies are both optimal and robust to the asymmetric game scenario.
- There is no need for an equal extent of knowledge among the agents, thereby enabling the disadvantaged player to achieve its objective despite the information discrepancy.



4. Learning-based in the Presence of Sparse and Adversarially Corrupteed Rewards

- Developed a model-free learning-based intelligent optimal tracking framework for UAVs that allows intermittency in rewards and control policies.
- Test the efficiency of the proposed learning-based controller on a real-world quadrotor in challenging experiments.

Key challenges:

- Adversarial components on CPS can sabotage power grids, transport systems, or medical devices, disrupting essential services.
- Ensuring stability and adversarial robustness under parametric and dynamic uncertainties, maintaining global asymptotic stability.
- Continual adaptation to evolving DoS patterns demands real-time policy updates using reinforcement learning and adaptive dynamic programming
- Rapid controller reconfiguration and continuous policy refinement are crucial for restoring and sustaining performance post-disruption.
- Experimental validation in microdrones using learning with sparse and adversarially corrupted rewards.

Broader Impact

1. Strengthen public confidence in autonomous systems by showcasing robust cyber-resilience.
2. Use efficient autonomous technology to reduce pollution, optimize resource utilization, and safeguard public health
3. Develop interdisciplinary courses and gather feedback to nurture expertise in resilient, cost-effective autonomy.

Scientific impact

1. Elevates robust reinforcement learning for handling DoS attacks under uncertain conditions.
2. Proposes new theoretical insights using small-gain and switching systems theories for global asymptotic stability.
3. Demonstrates real-time adaptive policy reconfiguration under varying DoS attacks.
4. Combines small-gain theory, switching systems theory, and RL, expanding applications in cybersecurity and control engineering.

Award ID#: CPS-2227185, CPS-2227153