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

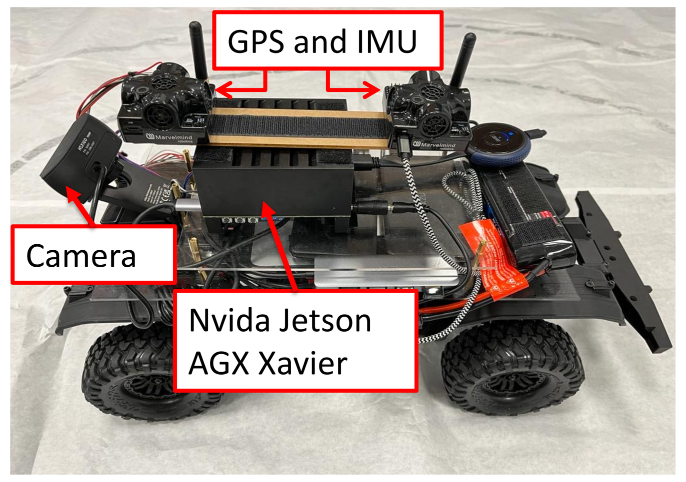
Prof. Kyriakos G. Vamvoudakis (kyriakos@gatech.edu, http://kyriakos.ae.gatech.edu)
Daniel Guggenheim School of Aerospace Engineering, Georgia Institute of Technology
Prof. Zhong-Ping Jiang (zjiang@nyu.edu, https://engineering.nyu.edu/faculty/zhong-ping-jiang)
Tandon School of Engineering, New York University

1. Learning-based Automated Lane Changing Control in Mixed Traffic

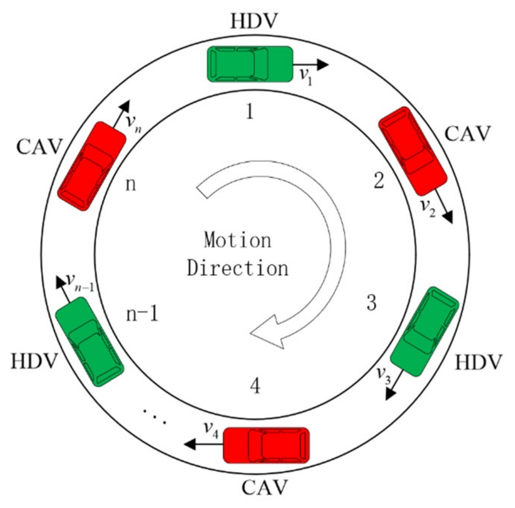
- A learning-based optimal control method employing adaptive dynamic programming (ADP) to create a near-optimal lane-changing controller using real-time input-state data of autonomous vehicles (AV).
- Treats AV dynamics as a linear parameter-varying system, using gain scheduling combined with ADP techniques to generate a learning-based
- A data-driven decision algorithm for safe lane changes, validated through MATLAB and SUMO simulations.

2. Experimental Study for Learning-Based Automated Lane Changing Control

- Developed a cost-effective, safe, and time-efficient learning-based control policy for AV lane-changing, leveraging real-time sensor data processed by an NVIDIA Jetson board, proven in lab tests with future aims for real-world trials.



3. Data-driven optimal control of connected vehicles in mixed traffic

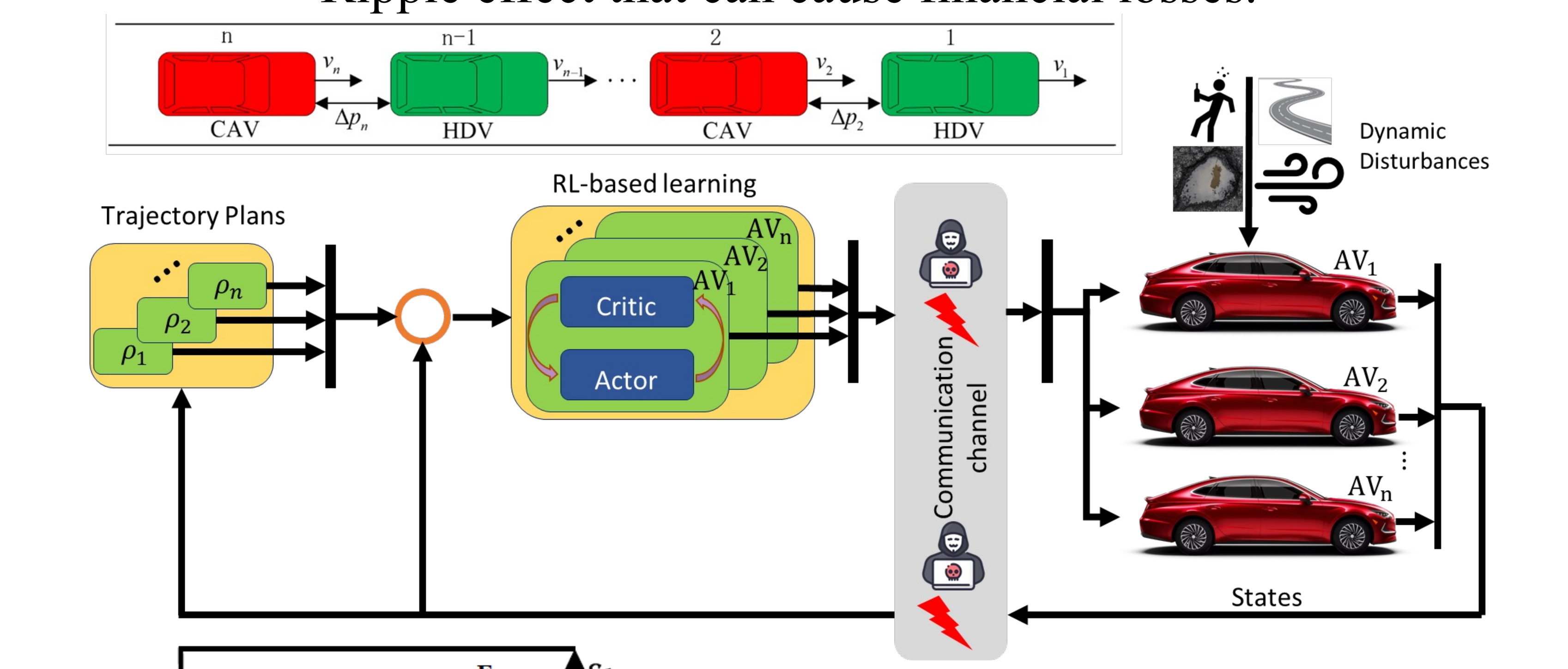


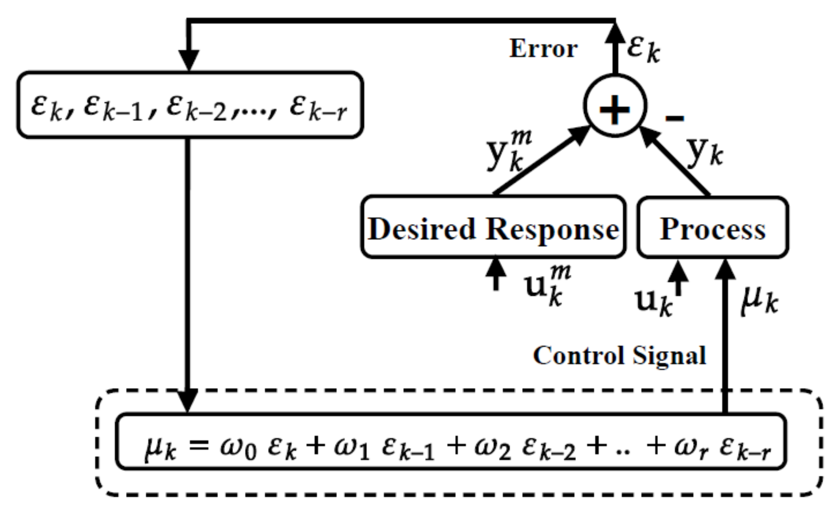
- Stabilization: minimizing $\int_0^{\infty} x^T Qx + u^T Ru\, dt$
- Disturbance attenuation: minimizing $\max_{w} \int_0^{\infty} x^T Qx + u^T Ru\, dt - \gamma w^T w\, dt$

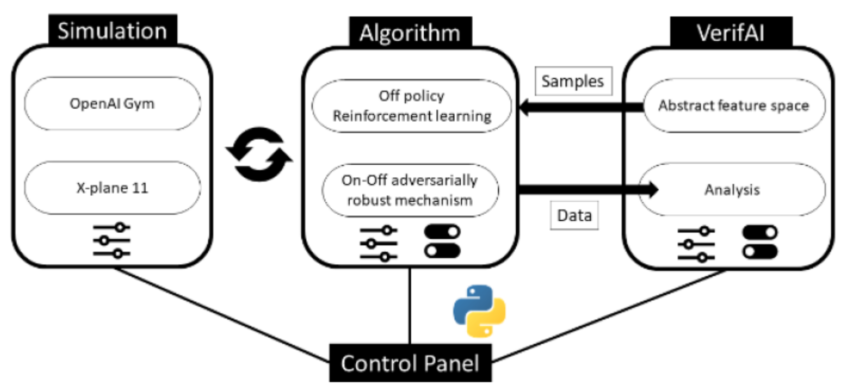
- A "reduced" system for the stabilizability on a ring road.
- Policy iteration for stabilization and L_p string stability
- Value iteration for disturbance attenuation.

Challenges:

- Emergence of heterogeneous cyber-physical-human systems
- Learning optimal controllers for trajectory tracking and disturbance rejection in face of cyber attacks.
- RL decision making mechanisms:
  - Self-adaptation - Self-healing - Self-optimization
- Sabotage of vehicle's RL governed control systems leads to;
  - Traffic jams, pollution, and accidents
  - Ripple effect that can cause financial losses.







Scientific impact

1.Model the intricate dynamics of human-AV interactions.
2.Use intermittent, robust reinforcement learning to reduce cyber attacks.
3.Simplify IoT redundancies through efficient reinforcement learning designs.
4.Create a new balance for safety, efficiency, and reliability in mixed traffic.
5.Develop instant, safe decision-making for autonomous agents with human integration.

Broader Impact

1.Boost trust in autonomous tech with ethical, safe human-machine interactions.
2.Apply autonomous tech in cities and healthcare to cut pollution and protect health.
3.Create interdisciplinary courses on efficient, cost-effective autonomous systems and gather student feedback.

4. Adversarial Motion Planning using Gaussian Process Classification

- Proposed Adversarial RRT-QX, a motion planning algorithm to allow a player agent to navigate a multi-agent environment while simultaneously identifying and avoiding potential adversaries attempting to intercept it.
- The algorithm additionally includes ways to identify non-adversarial independent agents to avoid unnecessary replanning or the freezing robot problem

5. Online Fixed-Time Reinforcement Learning for Safety Verification using Reachability Analysis

- A safety-critical control problem is addressed using reachability analysis and design a reinforcement learning-based mechanism for learning online and in fixed-time the solution to the safety-critical control problem.
- Safety is ensured by determining a set of states for which there does not exist an admissible control law generating a system trajectory reaching a set of forbidden states at a user-prescribed time instant.

6. Online Vehicle-Following Projection Mechanism Using Reinforcement Learning

- Ease of implementation in a digital environment such as microprocessors.
- Ability to utilize measurements of the process without incorporating any explicit dynamical information in the underlying strategy.
- Capability to solve model-following problems with high-order error dynamics using feasible adaptive strategies.
- Enabling simultaneous multi-objective optimization of the model-following and strategy adaptation performances.

7. Verification of Adversarially Robust Reinforcement Learning Mechanisms in Aerospace Systems

- This work integrates an RL algorithms to solve optimal control problems, an adversarial mitigation mechanism, a moving target defense framework, and a VerifAI toolkit.
- Then, we provide a testing framework to verify the robustness of closed-loop RL mechanisms.
- The verification test-bed framework is applied to an X-plane 11 Cessna 172 to successfully evaluate and verify the reliability of off-policy RL.

Award No.#: CNS-2227185 / CNS-2227153