Modeling cloud-controlled cyber-physical system resilience using a reinforcement-learning cart-pole testbed

Md Imran Jahid Khan, Mohammad Rahman, Fan Wu
Department of Computer Science, Tuskegee University

BACKGROUND

- Many modern infrastructures rely on cloud-controlled cyber-physical system (CPS) architectures.
- Cloud-based control improves operational efficiency, scalability, and computational capability, but it also increases exposure to cybersecurity threats.
- Adversarial conditions such as environmental stress and cyber-related threats, including sensor spoofing, signal interference, and data integrity degradation, may disrupt system control loops.
- Understanding how learning-enabled controllers behave under cyber and environmental stress is therefore essential for improving CPS resilience.

RESEARCH GOAL

Investigate how environmental stress and cyber disturbances affect the resilience of a reinforcement-learning–controlled cart-pole CPS.

METHODOLOGY

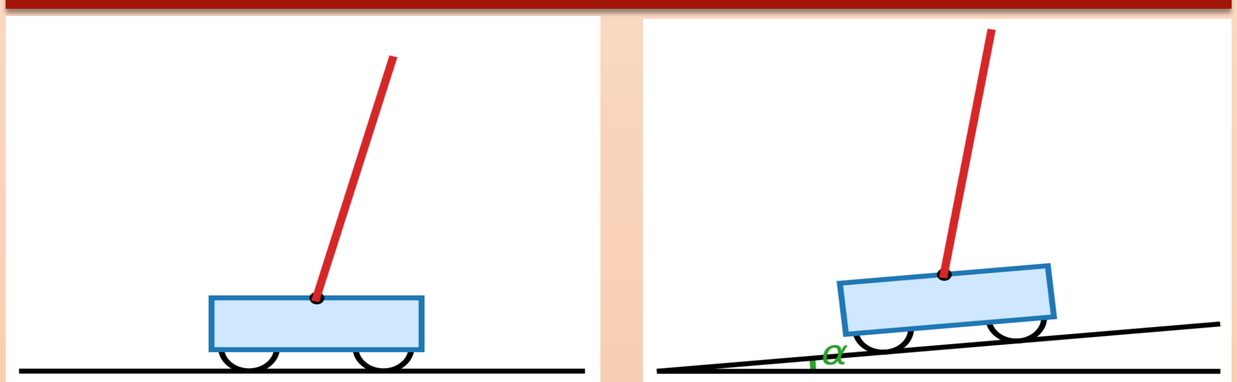

Figure 1: Cart-Pole Testbed under Horizontal and Inclined Surface

- **Model:** Cart–pole system simulated as a cloud-controlled CPS.
- **Controller:** Q-learning used to stabilize the pole via discrete control actions.
- **Experimental Conditions:** Baseline (α = 0), inclined surface (α = 0.1, 0.2 rad).
- **Adversarial Conditions:** Gaussian observation noise (σ = 0.006) added to state observations to simulate cyber disturbances.
- **Performance Metrics:** Learning curves, pole angle dynamics, and mean survival time.

Mean Survival Time, $MST = \frac{1}{N}\left(\sum_{i=1}^{N} L_i\right)\Delta t$

Here, L_i = Number of steps before failure in episode i
N = Total number of episodes
Δt = Simulation timestep = 0.02 s

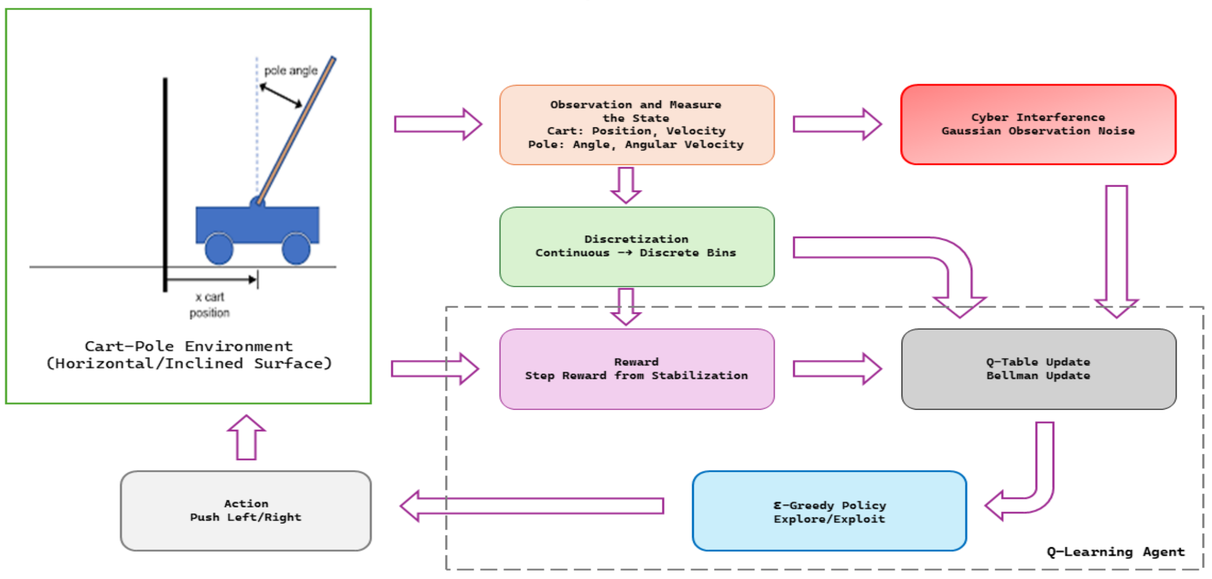

Figure 2: Q-Learning Workflow for Cart-Pole Stabilization

SIMULATION RESULTS

Learning Performance

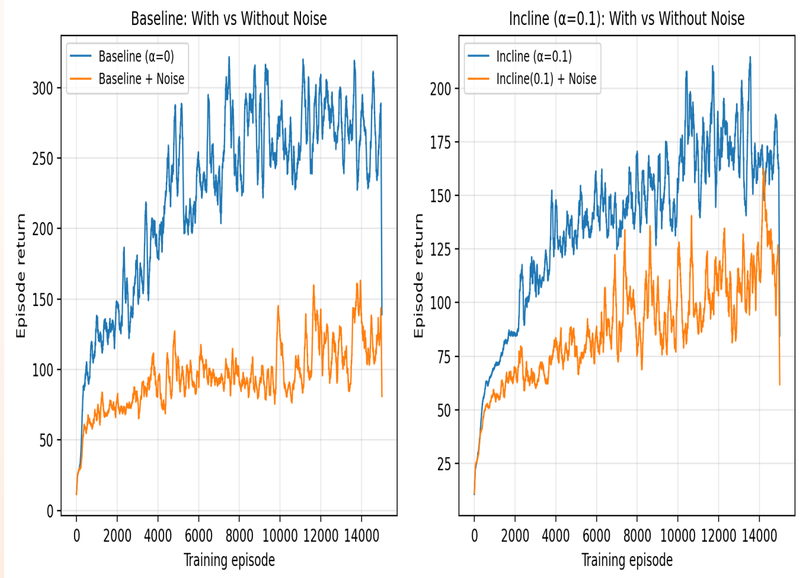

Figure 3: Effect of Observation Noise on Learning Performance

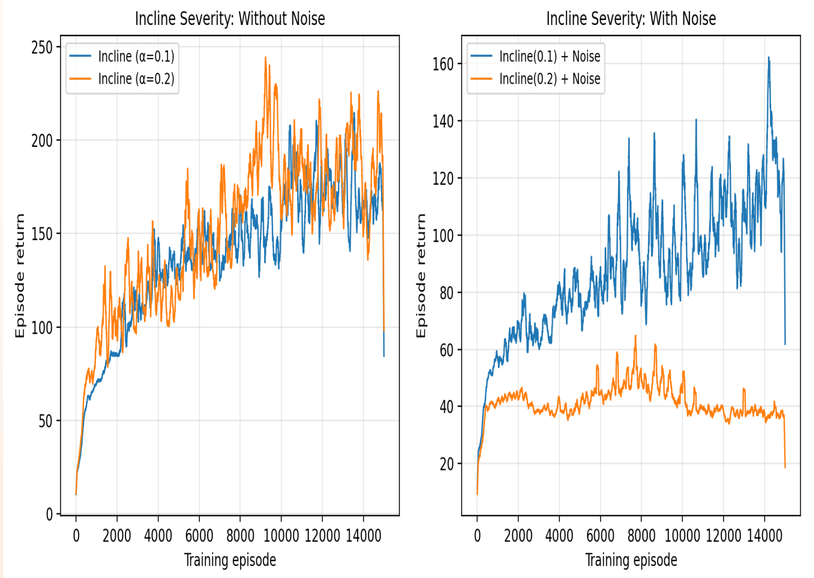

Figure 4: Effect of Surface Inclination on Learning Performance

System Stability

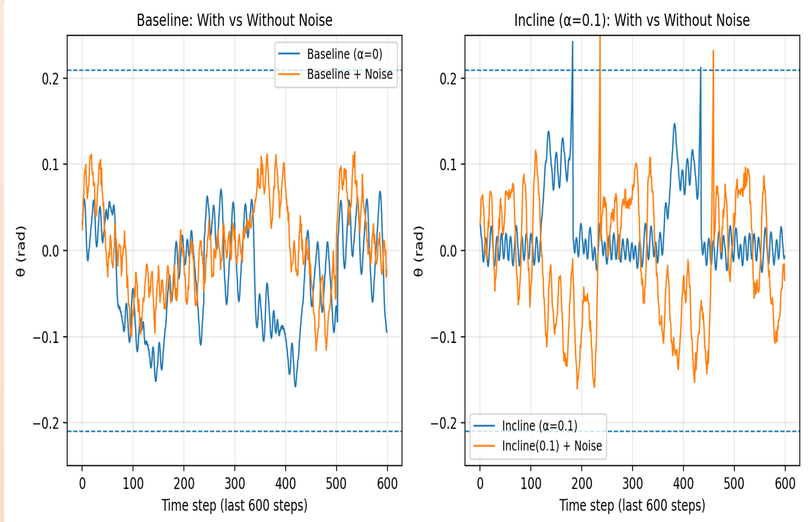

Figure 5: Pole Stability With vs Without Cyber Interference

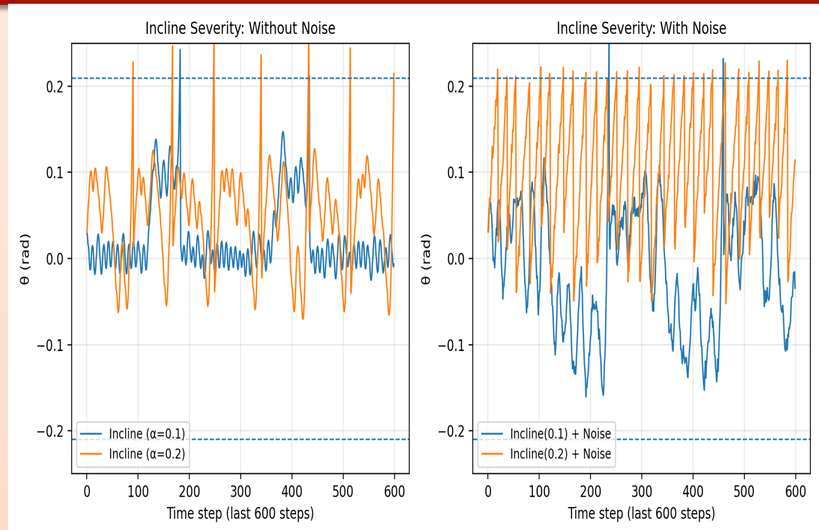

Figure 6: Pole Stability Under Different Surface Inclinations With & Without Cyber Interference

Resilience Summary

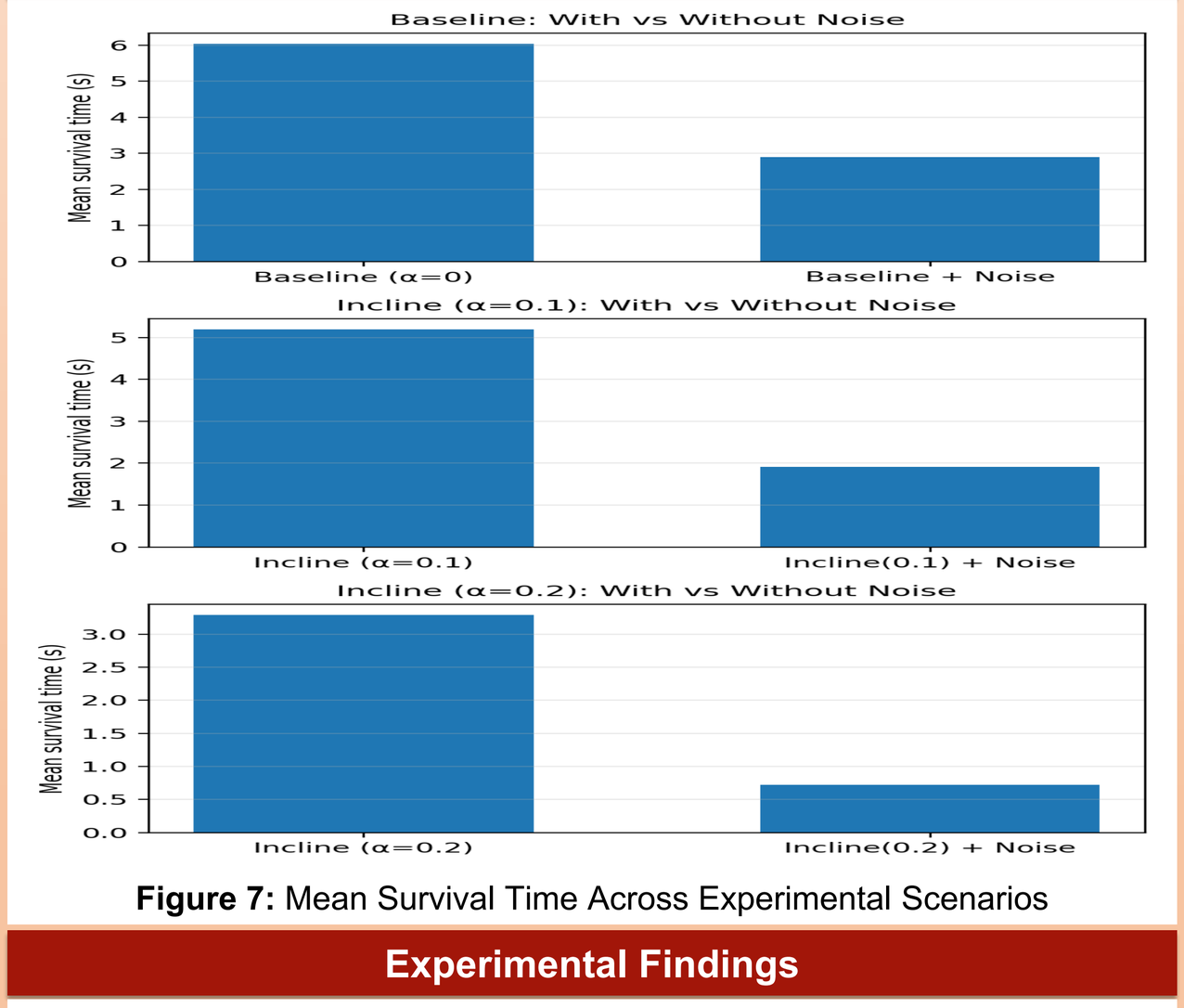

Figure 7: Mean Survival Time Across Experimental Scenarios

Experimental Findings

- RL stabilizes the cloud-controlled CPS under nominal conditions.
- Surface inclination alone has limited impact on system stability.
- Observation noise significantly degrades control performance.
- Cyber interference affects CPS stability more strongly than environmental stress.

ACKNOWLEDGMENT

This work is partially supported by the National Science Foundation (NSF) under Awards #2100134, #2209637, #2234911, and #2417608. The views expressed are those of the authors and not necessarily of the NSF.

REFERENCE

Yu, Z., Gao, H., Cong, X., Wu, N., & Song, H. H. (2023). *A survey on cyber–physical systems security*. **IEEE Internet of Things Journal, 10**(24), 21670–21686. https://doi.org/10.1109/JIOT.2023.3289625