CERIAS

The Center for Education and Research in Information Assurance and Security

Learning Adversarial Attacks on Adaptive Traffic Signal Control Systems Under Cooperative Perception

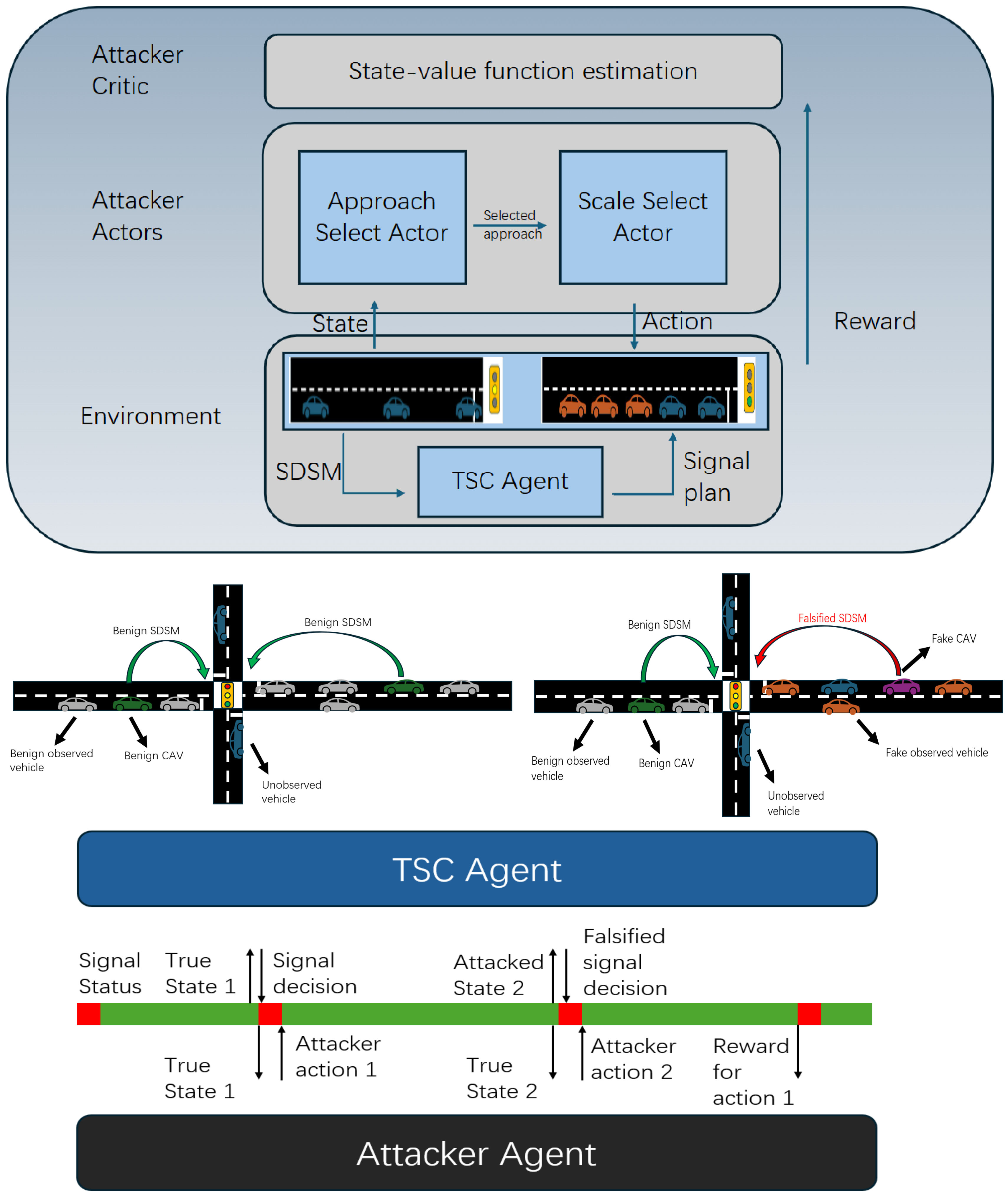
Wangzhi Li[1] , Tianheng Zhu[1], and Yiheng Feng[1]

1. Lyles School of Civil Engineering, Purdue University

Introduction

- ➢ The cooperative perception environment enabled by connected and automated vehicles (CAVs) can effectively enhance overall data collection efficiency.
- ➢ Cooperative perception-based traffic signal control (TSC) systems can further improve mobility at intersections but may suffer from potential cyber attacks.
- ➢ A deep reinforcement learning-based black-box adversarial attack framework is proposed and showed effectiveness against a learning-based traffic signal control model.

Threat Model



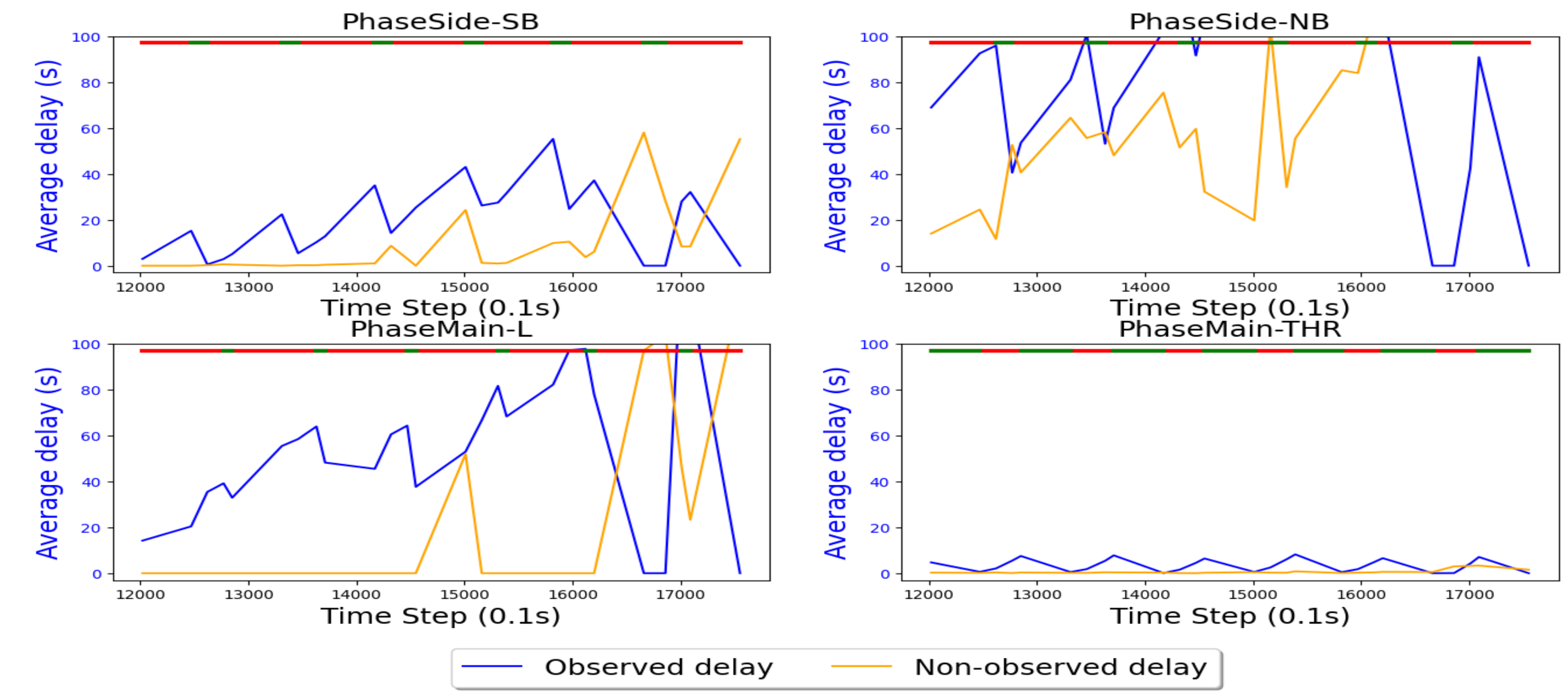
Target learning-based TSC

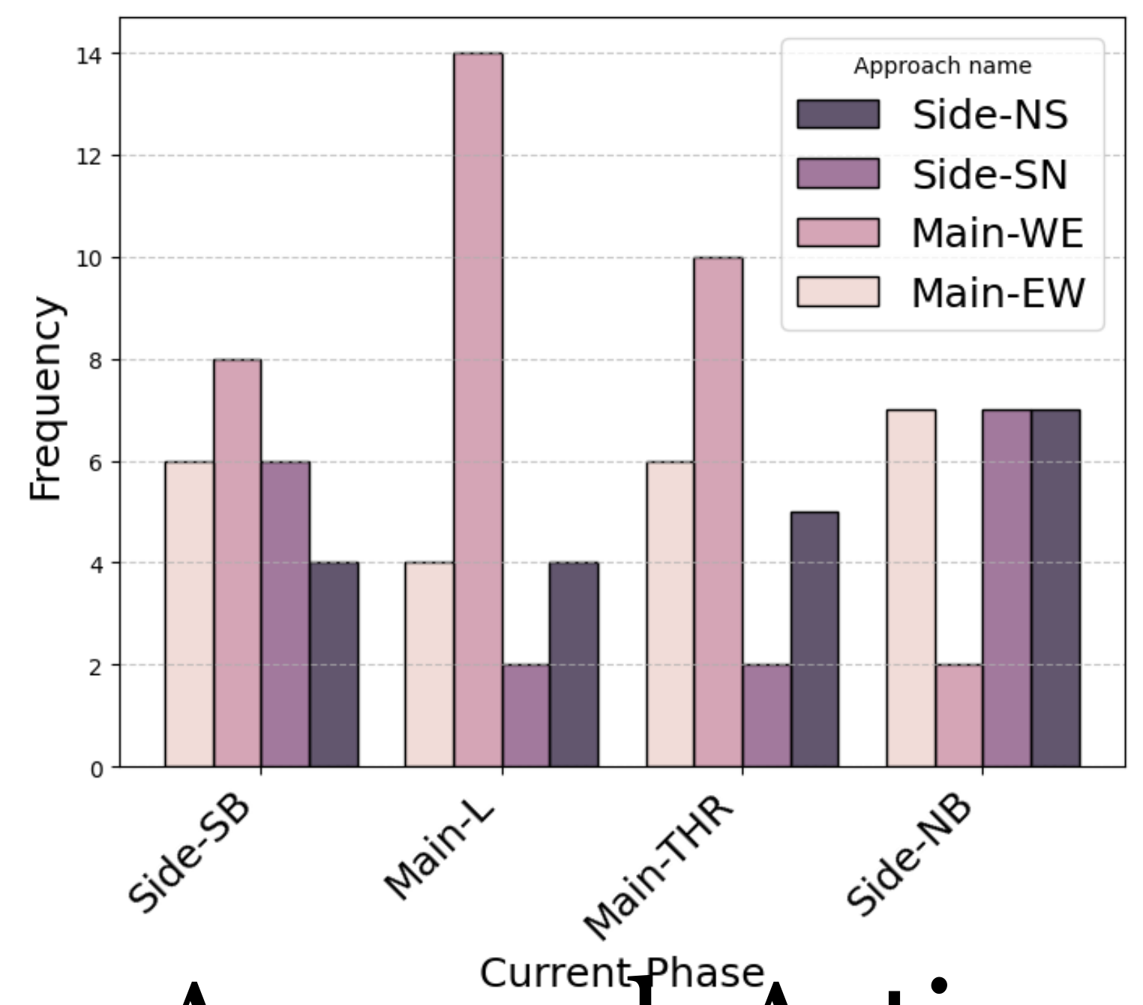
- ➢ State: **number of vehicles** on each segment; **average speed difference** of vehicles on each segment; index of current phase; duration of current phase.
- ➢ Action: continue the current phase or switch to the next phase. Phase sequence is given.
- ➢ Reward: weighted sum of scaled average delay per vehicle and a phase-switching penalty.

Attacker Agent

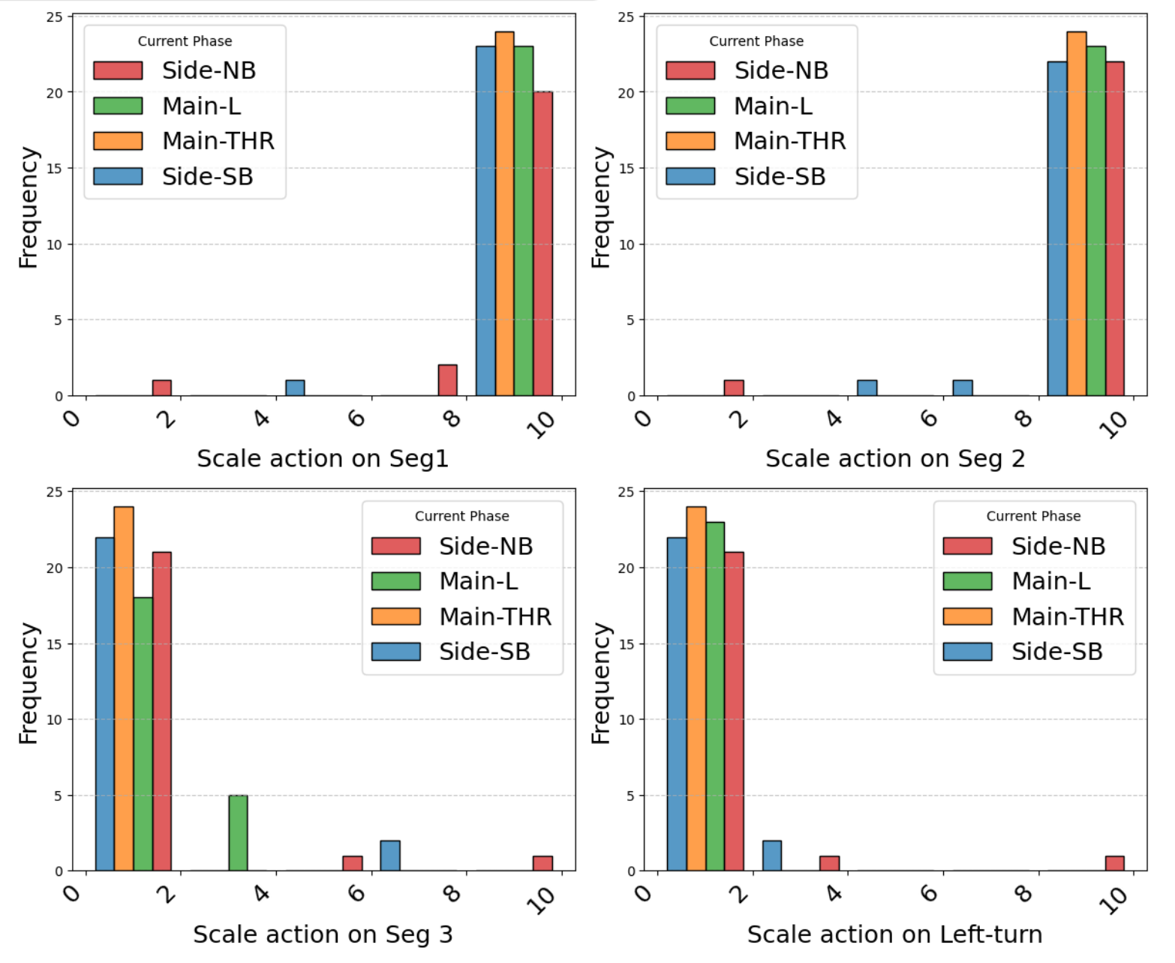
- ➢ State: same as the target TSC system
- ➢ Approach Action: an array of probabilities representing chance of **selecting the approach**, respectively
- ➢ Scale Action: numbers within 0 and 1 representing the percentage of the maximum number of **added vehicles to each segment.**
- ➢ Reward: weighted sum of attack performance and cost. Total vehicle delay and number of added fake vehicles.

Result Analysis





Approach Action



Scale Action

PURDUE UNIVERSITY

CERIAS