ADAPTIVE ADVERSARIAL VIDEOS ON ROADSIDE BILLBOARDS: DYNAMICALLY MODIFYING TRAJECTORIES OF AUTONOMOUS VEHICLES

By: Naman Patel, Prashanth Krishnamurthy, Siddharth Garg, Farshad Khorrami

Published: 2019 IEEE/RSJ International Conference on Intelligent Robots and Systems

Presented By: Brandon Ellis

WAIT, WHO ARE YOU?

- Brandon Ellis
- Masters Student
- Security x HCI
- Improve SOC analyst experience

SO, WHY ARE YOU HERE?

"Adaptive Adversarial Videos on Roadside Billboards: Dynamically Modifying Trajectories of Autonomous Vehicles"

or

"using a billboard to crash your car"

Background Information

The Paper

- Overview
- Attack
- Results
- Conclusion

Discussion

Adaptive Adversarial Videos on Roadside Billboards: Dynamically Modifying Trajectories of Autonomous Vehicles

BACKGROUND INFORMATION

DEEP NEURAL NETWORKS

- Deep Neural Network (DNN)
- Incorporation in Autonomous Devices
- Implements End-to-End Control Policy for Navigation

SOMEONE ATTACKS DNN

- DNNs for Classification & Object Detection
- Vulnerable to Adversarial Perturbations
- Closest Work used Static Attack
- DNNs are Fragile

Adaptive Adversarial Videos on Roadside Billboards: Dynamically Modifying Trajectories of Autonomous Vehicles

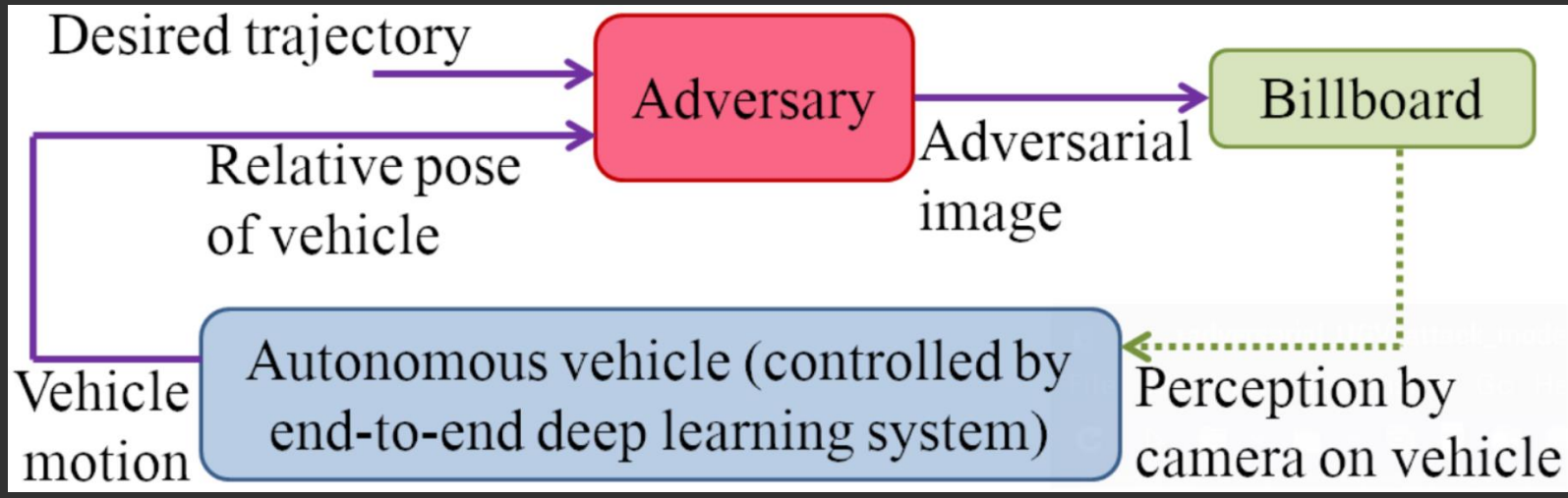
THE PAPER

THE PAPER

- Dynamic Attack
- Targeting Autonomous Vehicle's DNN Controller
- Utilizes Billboard with Camera
- Able to Direct Vehicle
- Resilient to Environmental Conditions
- Tested via Simulator

THE EXPERIMENT

- Simulator
- Assumptions
- Objective
- Experiment



DID IT WORK?

Scenario 1

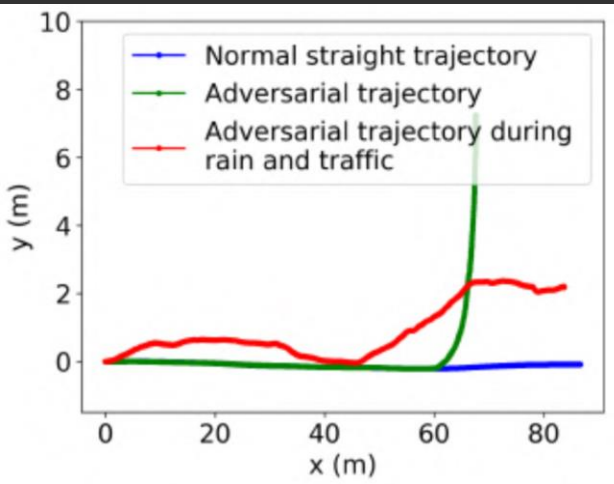
- Vehicle is Moving Straight
- Attacker Tries to Cause Left Turn
- Tested in Clean Environment
- Tested in Heavy Rain with Traffic
- Successful Results – Required Dynamic Video

Scenario 2

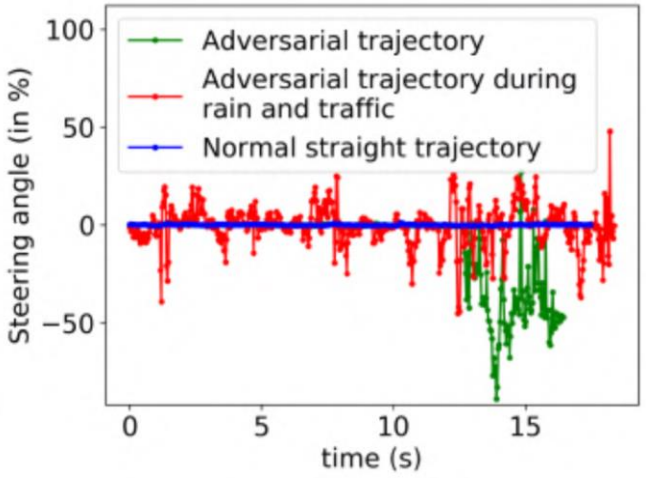
- Vehicle is Turning Right
- Attacker Tries to Keep Car Going Straight
- Tested in Clean Environment
- Tested in Low Light
- Successful Results – Required Static Image Only

DID IT WORK?

Scenario 1

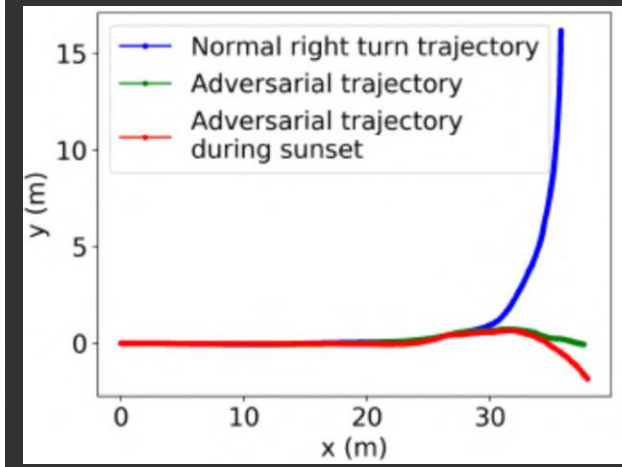


Trajectory

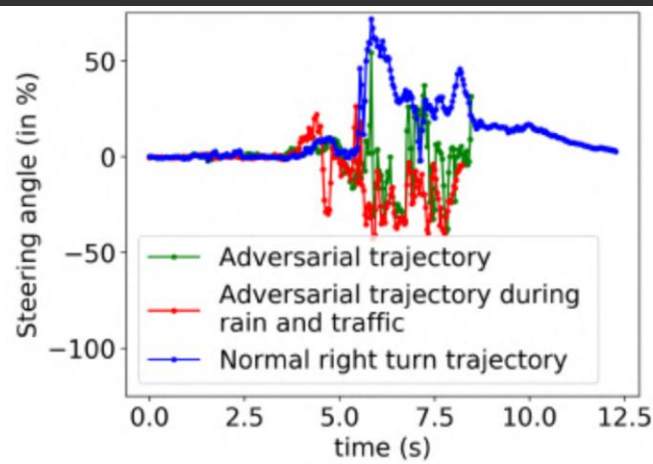


Steering

Scenario 2

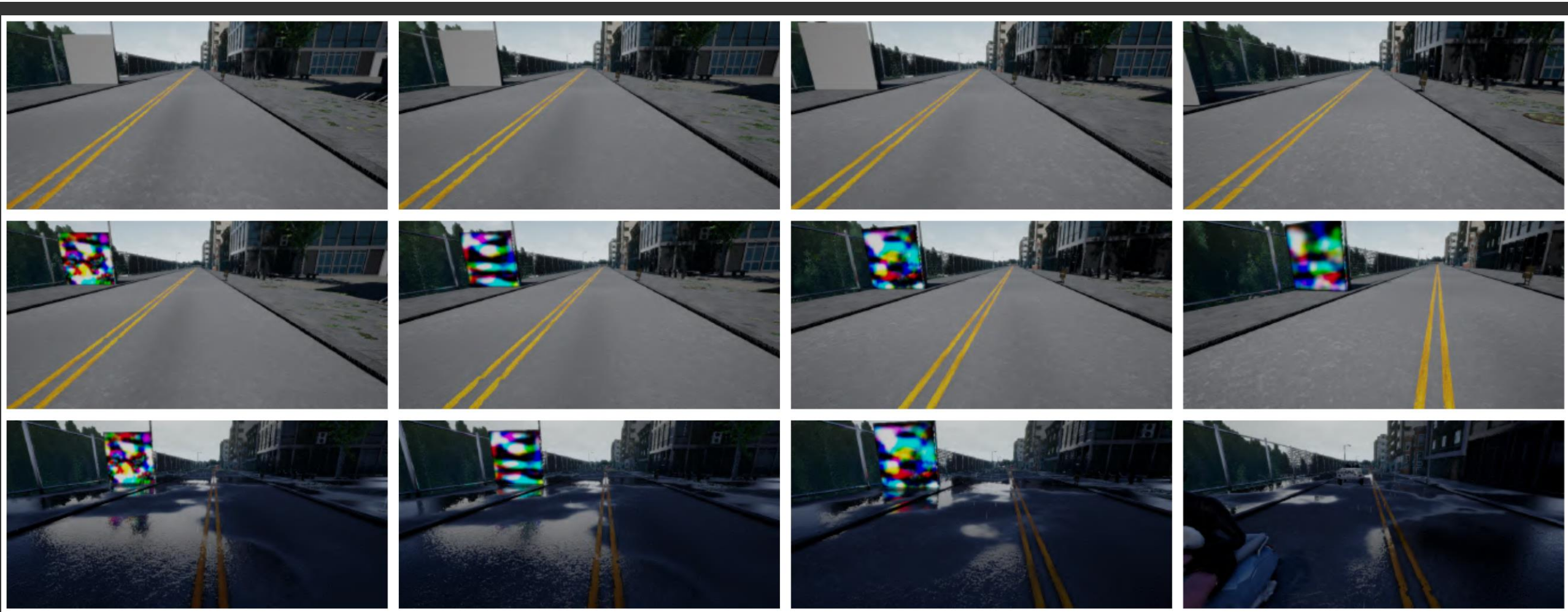


Trajectory

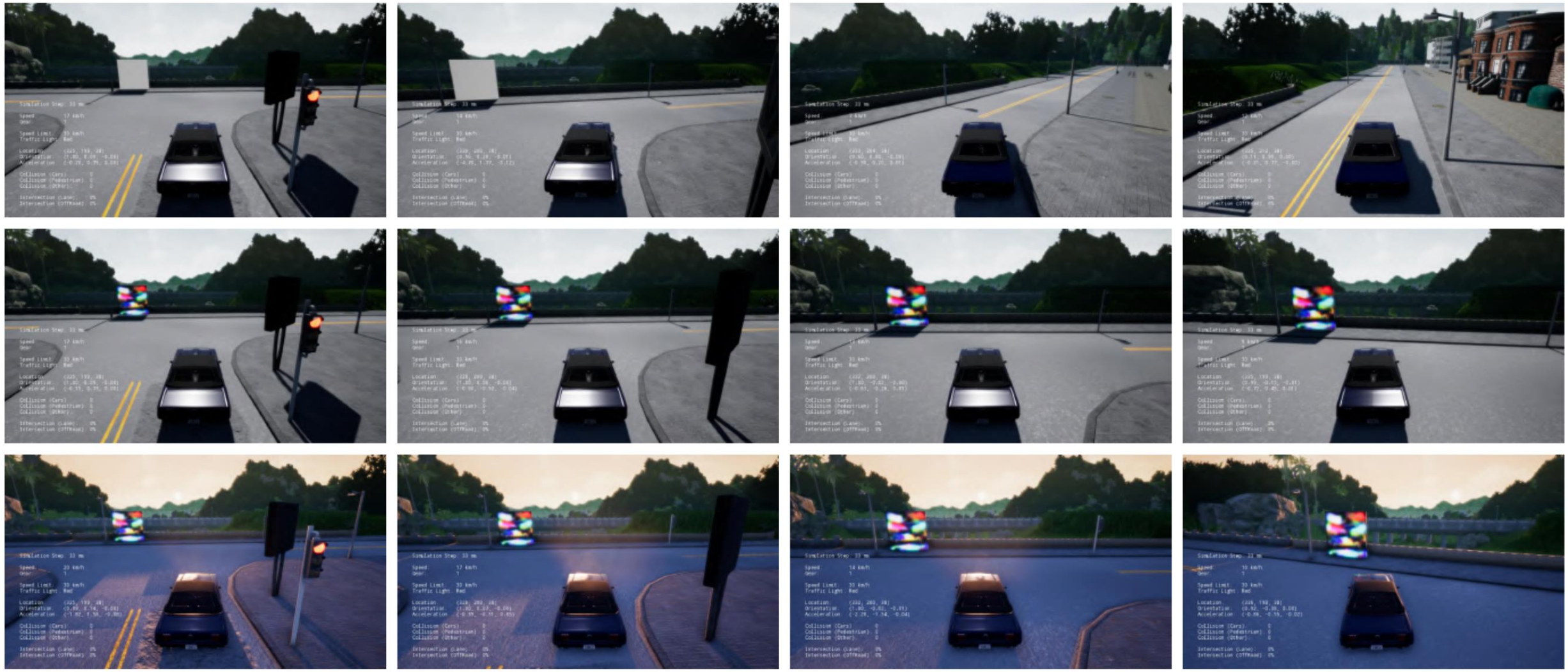


Steering

SIMULATION EXAMPLE



SIMULATION EXAMPLE



CONTRIBUTIONS

- Framework to Enable Attacks in Dynamic Environment
- Methodology for Adversarial Perturbation Generation
- Data Generation Policy for Iterative Attack
- Environmentally Robust Attack

CONCLUSIONS

- Launched Attack in Simulated Environment
- Conducted Two Separate Attack Scenarios
- Successful Under Different Environmental Conditions
- Soft Accept, But…

Adaptive Adversarial Videos on Roadside Billboards: Dynamically Modifying Trajectories of Autonomous Vehicles

DISCUSSION

DISCUSSION

- Scenario Testing
- Environmental Testing
- Attack Scenarios