2024 - AI - X6J-YHB - Discovering Adversarial Driving Maneuvers against Autonomous Vehicles - lucky061681@gmail.com - Ruoyu Song

CERIAS
The Center for Education and Research in Information Assurance and Security

Discovering Adversarial Maneuvers against Autonomous Vehicle

Ruoyu Song, Muslum Ozgur Ozmen, Hyungsub Kim, Raymond Muller, Z. Berkay Celik, Antonio Bianchi

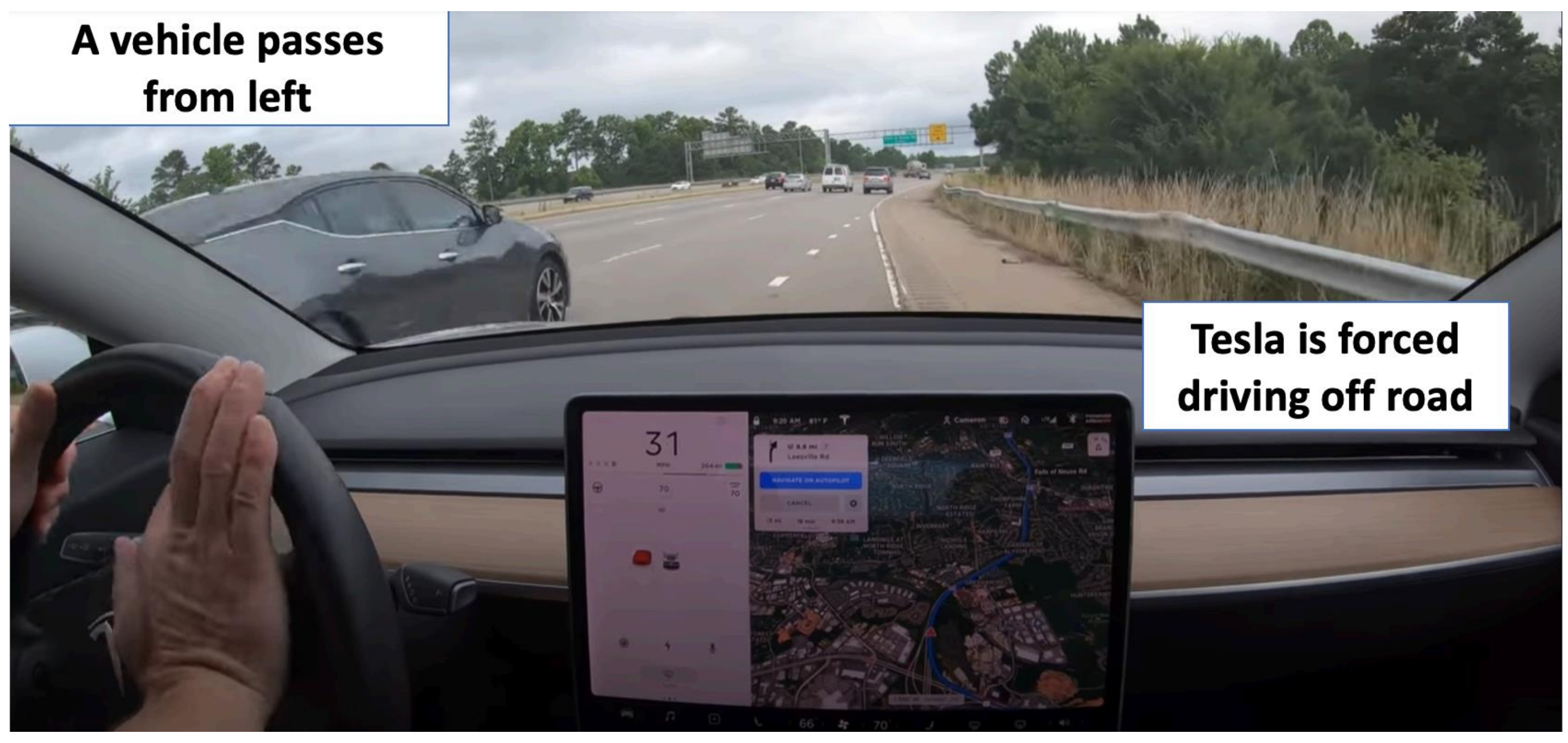
Purdue University

1. Motivation

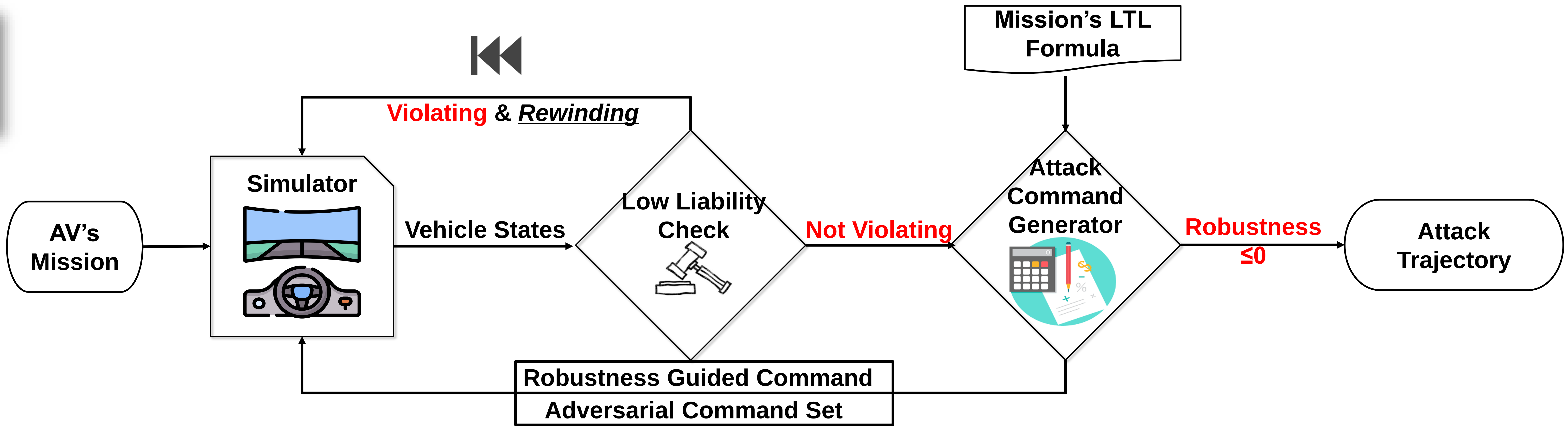
Problem: 1. Autonomous Vehicle (AV) performs poorly to abnormal driving maneuvers.

2. The adversarial maneuvers generated by prior work do not prevent adversaries from having legal liability for the attack.

Example: Real-world driving behavior causing the Tesla autopilot to steer off the road, forcing the operator to intervene. While this behavior could be defined as “aggressive” or “inconsiderate”, it does not look intentionally malicious.

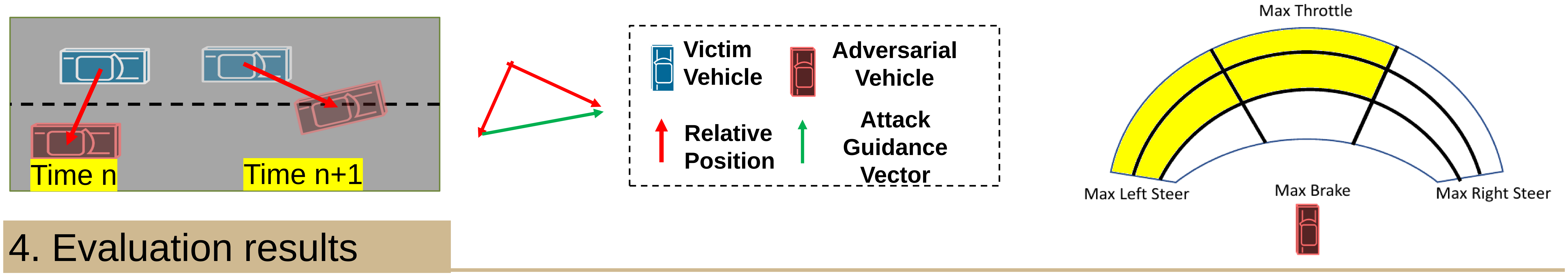


2. Acero Overview



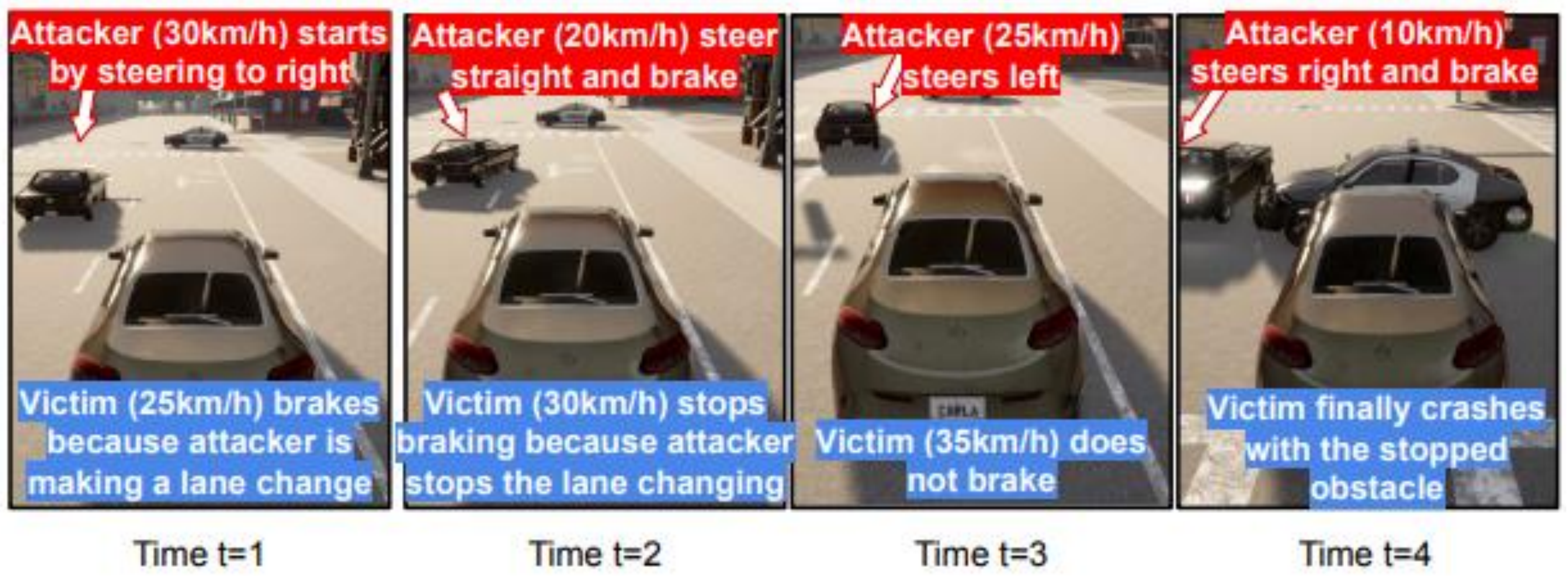
Solution: **ACERO** [1] generates adversarial maneuvers that deviate the AV from its mission. To ensure the attacker’s safety, maintain low liability, and preserve the practicality of the attack, we design seven formally verifiable physical constraints to enforce on adversarial maneuvers.

3. Trajectory Generation



4. Evaluation results

- **Datasets**: Two driving software (openpilot and Autoware) in the CARLA simulator.
- **Results**: **ACERO** discovered 219 attacks against openpilot and 122 attacks against Autoware. 73.3% of these attacks cause the victim to collide with a third-party vehicle, pedestrian, or static object.


Attacker (30km/h) starts by steering to right
Victim (25km/h) brakes because attacker is making a lane change
Time t=1
Attacker (20km/h) steer straight and brake
Victim (30km/h) stops braking because attacker stops the lane changing
Time t=2
Attacker (25km/h) steers left
Victim (35km/h) does not brake
Time t=3
Attacker (10km/h) steers right and brake
Victim finally crashes with the stopped obstacle
Time t=4

[1] **Ruoyu Song,** Muslum Ozgur Ozmen, Hyungsub Kim, Raymond Muller, Z. Berkay Celik, Antonio Bianchi "Discovering Adversarial Driving Maneuvers against Autonomous Vehicles." *32nd USENIX Security Symposium (USENIX Security 23)*. 2023.