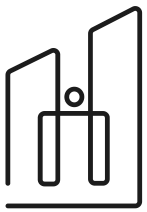
Analysing Adversarial Threats to Rule-Based Local-Planning Algorithms for Autonomous Driving

Andrew Roberts[1], Mohsen Malayjerdi[2], Mauro Bellone[2], Olaf Maennel[3], Ehsan Malayjerdi[1]

VehicleSec 2023

IseAuto - Autonomous Driving Research Lab
(https://iseauto.taltech.ee/en/



Funded by the European Union

Main idea of our study

- Local-planning is an essential function for navigation and achievement of journey/mission – security of algorithms is a developing space.
- A lack of robustness to adversarial threats in one or many of the local-planning modules can lead to unsafe Autonomous Driving (AD) behaviour.
- What if an attacker directly targeted the algorithm responsible for generating safe trajectories?
- Can the attack be conducted in a stealthy manner?

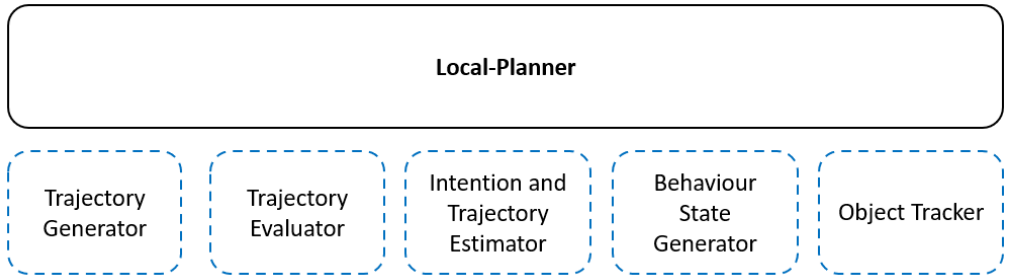


Figure 1: Local-Planning Algorithm

Figure 2: iseAuto Autonomous Vehicle Shuttle

Funded by the European Union

Trajectory Generation and Evaluation

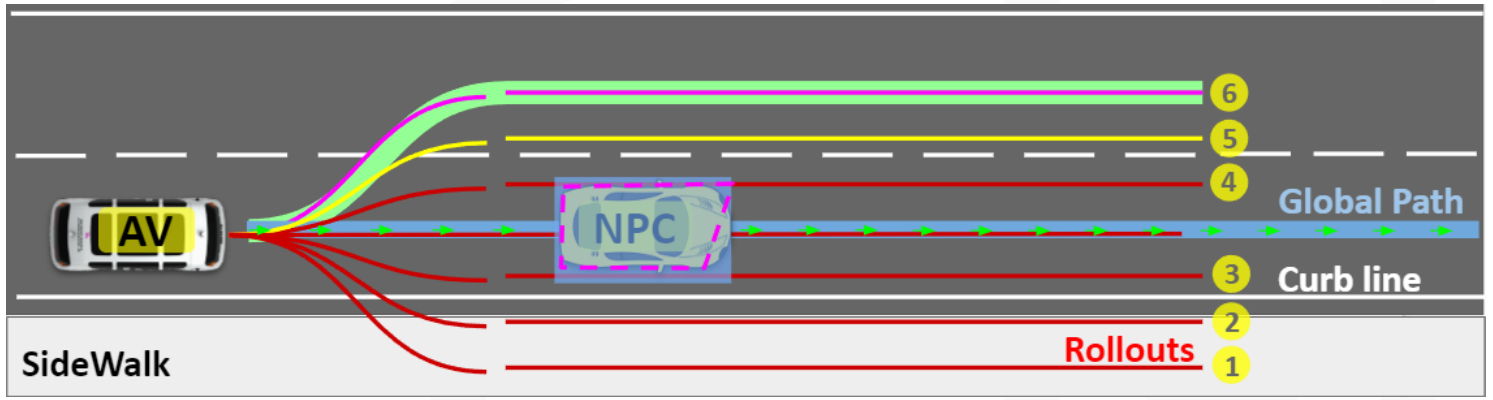


Figure 3: Local-Planning Trajectory Generation

$$C = \begin{bmatrix} w_{cent} \\ w_{trans} \\ w_{longColl} \\ w_{latColl} \\ w_{vis} \end{bmatrix} \cdot \begin{bmatrix} C_{cent} \\ C_{trans} \\ C_{longColl} \\ C_{latColl} \\ C_{vis} \end{bmatrix}^T$$

Figure 4: Cost-Function Algorithm for Local-Planning

Funded by
the European Union

Threat Model

- **Attack Case 1: Position Offset**
  - Manipulation of Current_Pose Data: Longitudinal and Latitudinal position.
  - Deviations range from minimal to 1meter.

- **Attack Case 2: Message Time-Delay**
  - Delay in the communication of sensed pose data to the cost-function algorithm.

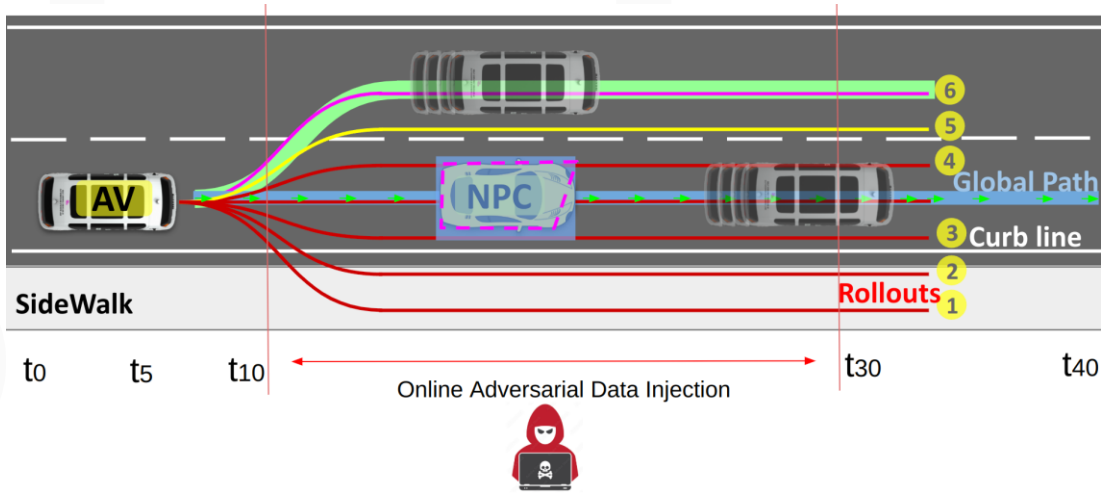


Figure 5: Attack Test Case

Funded by the European Union

Experimental Setup

- **Attack Case 1: Position Offset**
  - Test Case 1a – 1c Lateral Pose Deviation. (0.16%, 0.33%, 0.5%)
  - Test Cas 1d – 1f Longitudinal Pose Deviation. (0.33%, 0.66%, 1.0%)

- **Attack Case 2: Message Time-Delay**
  - Test Case 2a – 2c Time-Delay. (0.3sec, 0.6sec. 1.0sec)

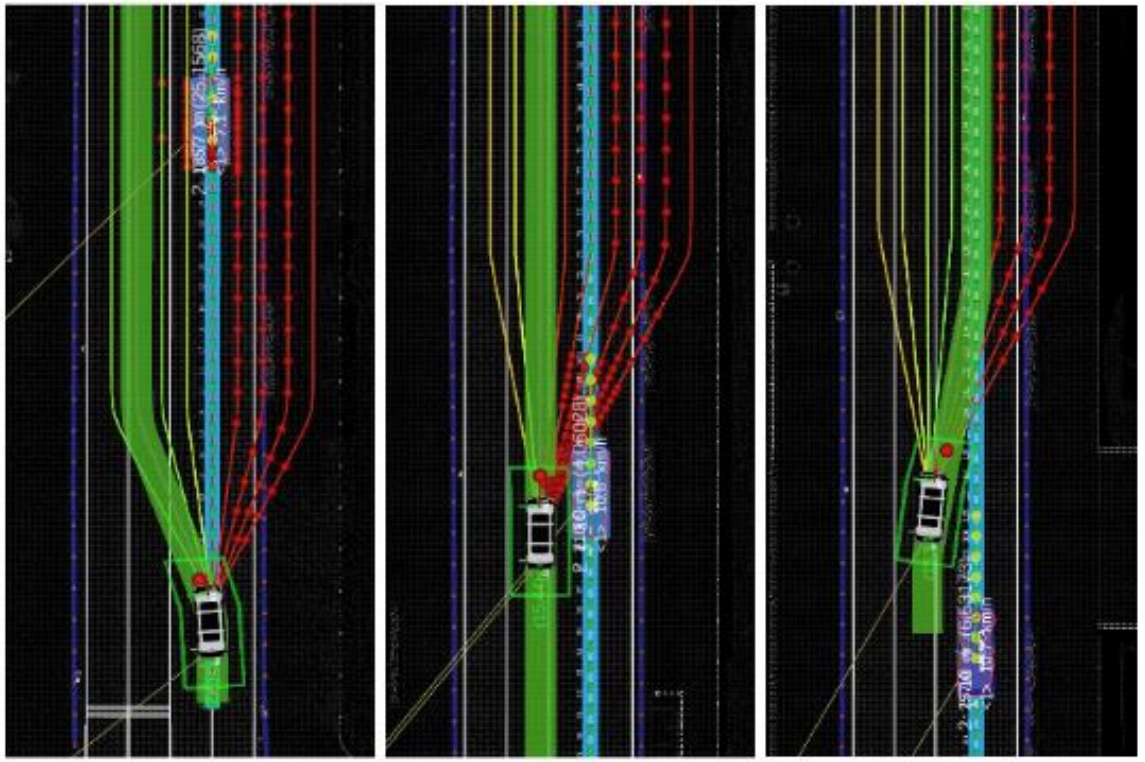
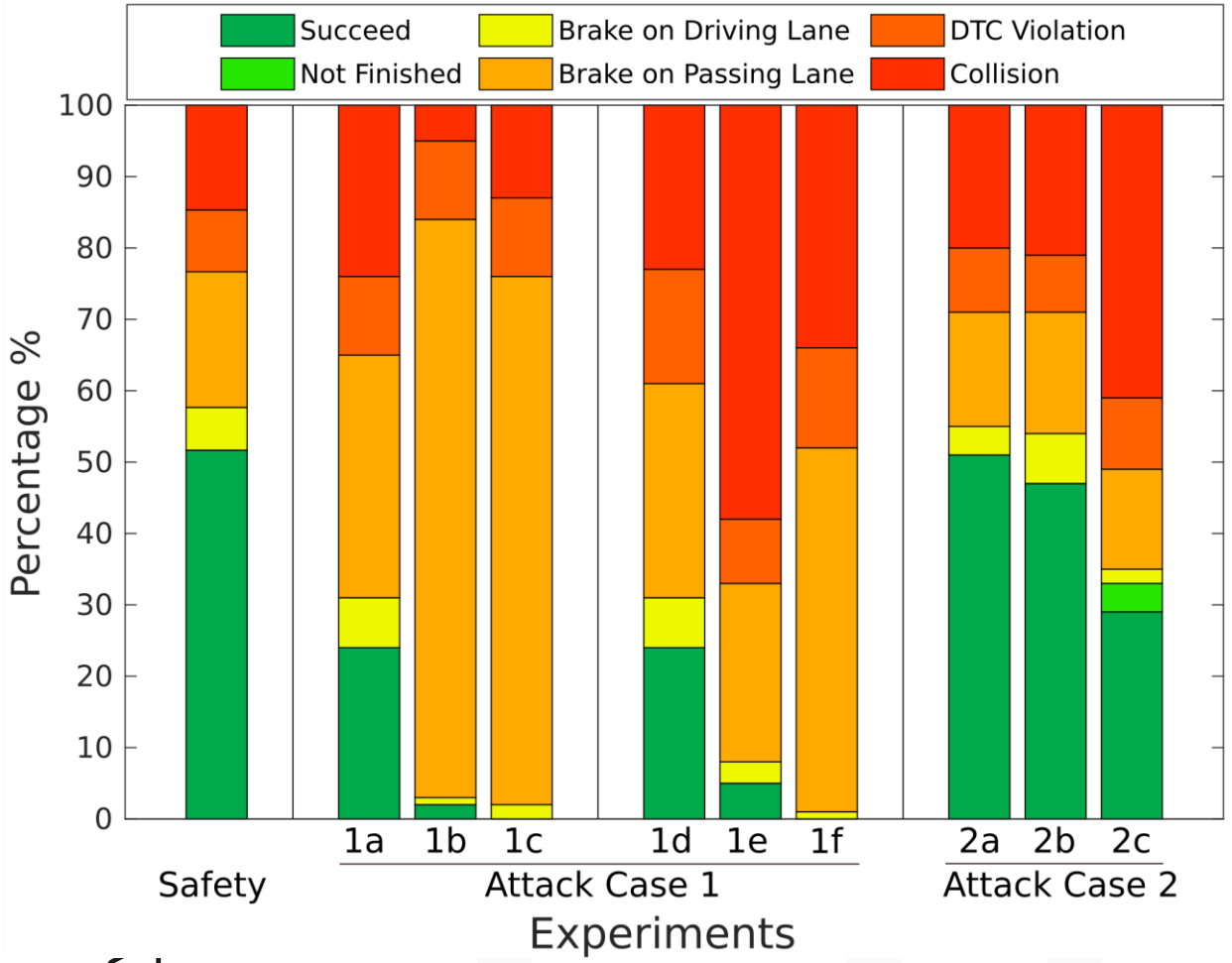


Figure 6: Low-Fidelity Simulation of AV Overtaking Manoeuvre

Funded by the European Union

Results



- Small deviations of the Pose data can substantially impact safe AD driving behaviour.
- The higher deviation results in the AV being stuck in the passing lane, this is due the dramatic change in lateral pose.
- Greater Time-Delay of Pose Data impacts Trajectory Generation.

Figure 7: Experiment Test Results

Funded by the European Union

Results

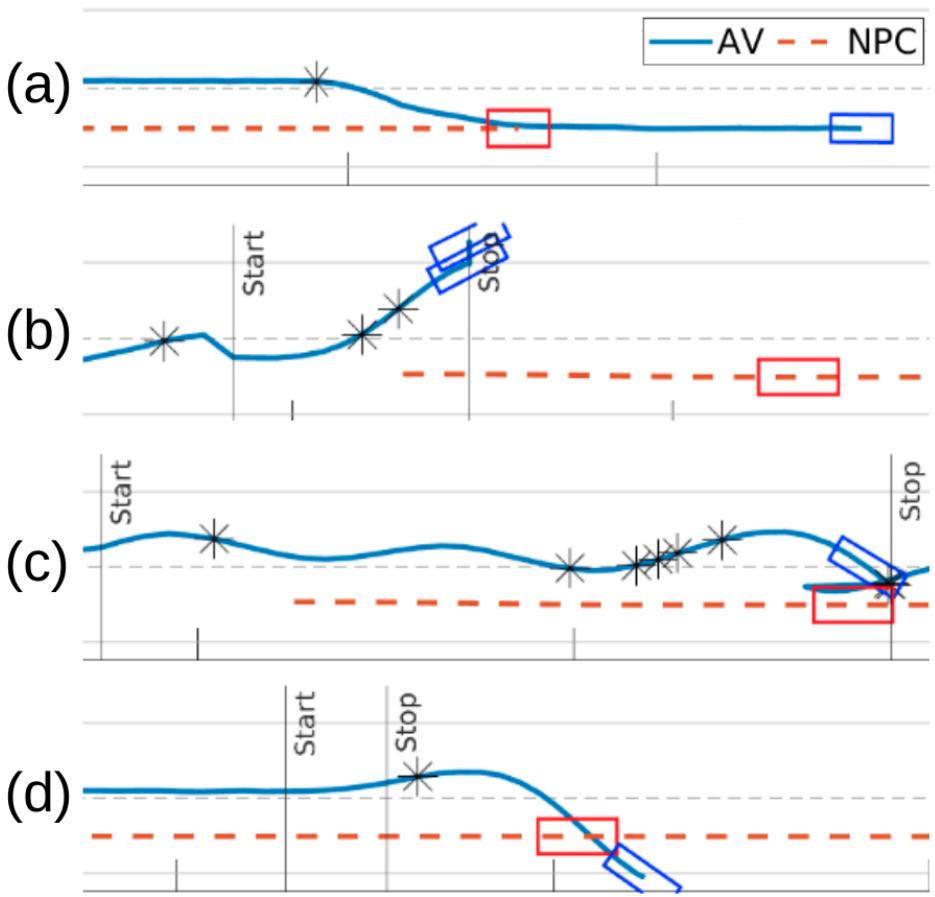


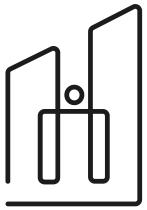
Figure 8: Experiment Test Results Trajectory Behaviour

- Small deviations to lateral pose result in a fluctuation of the cost of different rollouts which cause greater lane transitions as the cost function causes the AV to choose a route based on minimum cost.
- The higher deviation results in a higher occurrence of breaking activity and hitting the curb.
- The time-delay of the pose data to the local-planning nodes results in a loss of localisation and the greater delay the greater impact on the cost calculation which in turn causes uncertainty for the behaviour selector/decision-making.

Funded by
the European Union

Discussion

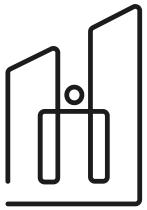
- Minor pose deviation attacks, where the deviation is a range of 20 to 25cm offer a good starting point to mutate adversarial data for further attacks based on this range.
- Delays in sensed-data input flowing to the local-planning modules of greater than 1 second increase the rate of mission failure and safety violations. Given that 1 message is broadcast every 20 milliseconds, 1 second represents around 50 messages, and a delay of this magnitude is also likely to be more observable.



Funded by
the European Union

Conclusion

- Local-planning cost-function is sensitive to adversarial data manipulation that introduces deviations to the lateral and longitudinal values.
- Small deviations of the pose data input, which are below the threshold of normal noise, affect AD safe driving behaviour.
- Trajectory Generation was robust against limited delays in message communication.
- It is possible to mutate malicious input to develop greater stealth attacks.
- Future work should focus on monitoring solutions to such attacks.



Funded by
the European Union

Thank you!

FinEst Centre
for Smart Cities

Funded by
the European Union

FinEst Twins project is funded by two grants: the European Union´s Horizon 2020 Research and Innovation Programme, under the grant agreement No. 856602, and the European Regional Development Fund, co-funded by the Estonian Ministry of Education and Research, under grant agreement No 2014-2020.4.01.20-0289.