Demo: SlowTrack: Increasing the Latency of Camera-Based Perception in Autonomous Driving Using Adversarial Examples

Chen Ma[1⋆] Ningfei Wang[2⋆] Qi Alfred Chen[2] Chao Shen[1]
⋆These authors contributed equally [1]Xi'an Jiaotong University [2]University of California, Irvine

***Abstract*—In Autonomous Driving (AD), real-time perception is a critical component responsible for detecting surrounding objects to ensure safe driving. While researchers have extensively explored the integrity of AD perception due to its safety and security implications, the aspect of availability (real-time performance) or latency has received limited attention. Existing works on latency-based attack have focused mainly on *object detection*, i.e., a component in camera-based AD perception, overlooking the entire camera-based AD perception, which hinders them to achieve effective system-level effects, such as vehicle crashes. In this paper, we propose SlowTrack, a novel framework for generating adversarial attacks to increase the execution time of camera-based AD perception. We propose a novel two-stage attack strategy along with the three new loss function designs. Our evaluation is conducted on four popular camera-based AD perception pipelines, and the results demonstrate that SlowTrack significantly outperforms existing latency-based attacks while maintaining comparable imperceptibility levels. Furthermore, we perform the evaluation on Baidu Apollo, an industry-grade full-stack AD system, and LGSVL, a production-grade AD simulator, with two scenarios to compare the system-level effects of SlowTrack and existing attacks. Our evaluation results show that the system-level effects can be significantly improved.**

I. Introduction

In this Demo, we focuse on the security of Autonomous Driving (AD) vehicles, particularly the camera-based perception system used for real-time detection of environmental objects. Previous studies have explored the integrity of these systems, highlighting vulnerabilities that could lead to safety hazards. However, the aspect of system availability, crucial for safety, has received less attention. Traditional availability analyses often overlook the complete AD perception pipeline, which includes both object detection and tracking.

We introduce a novel framework, SlowTrack, which is the first to investigate availability-based adversarial attacks across the entire AD perception pipeline. This approach differs from previous ones that targeted only object detection and thus had limited impact on system-level effects. SlowTrack emphasizes increasing latency in the AD perception process, exploiting both object detection and tracking stages. The research includes theoretical analysis of tracking algorithms and proposes a two-stage attack strategy. The effectiveness of SlowTrack is demonstrated through experimental evaluation on four state-of-the-art AD perception pipelines, showing significantly increased latency and higher rates of system-level effects such as vehicle crashes in simulations.

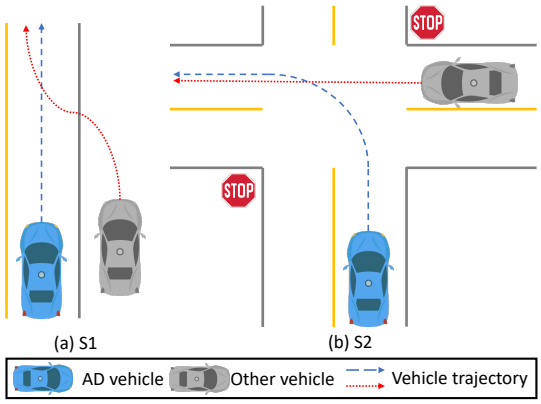

Fig. 1. Two scenarios for simulation evaluation setup on system-level effects.

II. Demonstration Plan

Demonstration of the tracking results. We will demonstrate the tracking results visually on a driving video dataset to show how SlackTrack introduce the high latency into AD [1].

Demonstration of system-level effects in simulation. To measure system-level effects, we adopt a simulation-centric evaluation using LGSVL and Baidu Apollo with the Borregas Ave map and the Lincoln2017MKZ AD vehicle with default configuration. The two scenairos are shown in Fig. 1. We will demonstrate the system-level attack effect, i.e., vehicle crashes [1] with both prior attacks and our SlowTrack showing improvements in system-level effectiveness.

Acknowldgments

This work was supported by National Key R&D Program of China (2020AAA0107702); the NSF under grants CNS-1929771, CNS-2145493, and CNS-1932464; USDOT UTC Grant 69A3552348327; National Natural Science Foundation of China (U21B2018, 62161160337, 62132011, 62376210, 62006181, U20B2049); Shaanxi Province Key Industry Innovation Program (2021ZDLGY01-02); and Fundamental Research Funds for the Central Universities under grant (xtr052023004, xtr022019002).

References

[1] C. Ma, N. Wang, Q. A. Chen, and C. Shen, "SlowTrack: Increasing the Latency of Camera-Based Perception in Autonomous Driving Using Adversarial Examples," in *Proceedings of AAAI*, 2024.

Symposium on Vehicles Security and Privacy (VehicleSec) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-7-6
https://dx.doi.org/10.14722/vehiclesec.2024.25015
www.ndss-symposium.org