Poster: 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
ershang@stu.xjtu.edu.cn ningfei.wang@uci.edu alfchen@uci.edu chaoshen@xjtu.edu.cn

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.e., the vehicle crash rate of SlowTrack is around 95% on average while existing works only have around 30%.

I. Main content

This research [1] is recently published in AAAI 2024. The original abstract and author list are shown above. We post the paper links with arXiv version[1].

II. Acknowledgments

We would like to thank Ziwen Wan, Yunpeng Luo, Tong Wu, Xinyang Zhang, and the anonymous reviewers for their valuable and insightful feedback. This research was supported in part 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). Chao Shen and Qi Alfred Chen are the corresponding authors.

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.

[1]https://arxiv.org/abs/2312.09520