Weaponizing Infrared Against Lane Detection Systems in Autonomous Vehicles*

Hyunmin Ju, Sangmin Woo, Dohyun Kim, Weonji Choi, and Yongdae Kim

KAIST, Daejeon, South Korea
{hyunmin.ju, wsm723, dohyunjk, wec69, yongdaek}@kaist.ac.kr

1 Introduction

These days, autonomous vehicles primarily utilize cameras for lane detection, and nearly all modern vehicles are equipped with lane detection capabilities. This study presents an attack method on infrared-based lane detection systems, leveraging vulnerabilities including the absence of infrared filters in autonomous vehicle cameras and excessive sensitivity of lane detection systems. Building upon previous work that demonstrated attacks using IR to generate fake objects [4] and attacks that induced lane departure through crafted perturbations exploiting the hypersensitivity of lane detection systems [1], we utilize infrared (IR) lasers to create fake lanes that are invisible to the human eye but detectable by autonomous vehicle cameras. This approach induces lane detection algorithms to misinterpret these fake lanes as real lanes. Through experiments in both digital and physical domain, we demonstrate attack scenarios that affect the safety of autonomous vehicles, including path deviation and failure to maintain lane centering.

2 Evaluation

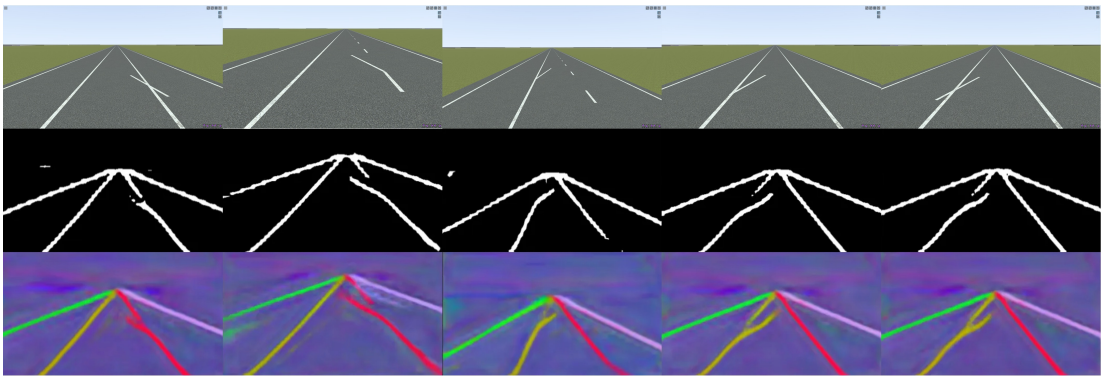

Figure 1: Digital Domain - AS 1

We design two attack scenarios (AS). The first is malicious lane extension, which creates fake lanes at the end of real lanes or through real lanes. The second is inter-lane injection, which inserts a single fake lane between existing lanes. In the digital domain, we design custom road environments using RoadRunner by MathWorks, and for both AS1 and AS2, the LaneNet [2] algorithm recognized fake lanes as real lanes. In the physical domain, we implement scenarios by projecting IR lasers onto miniature-scaled tracks, and successfully execute attacks for both AS1 and AS2, with both LaneNet and LaneATT [3] algorithms misidentifying fake lanes as real lanes.

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-61, December 16-18, 2025, Sapporo, Japan.

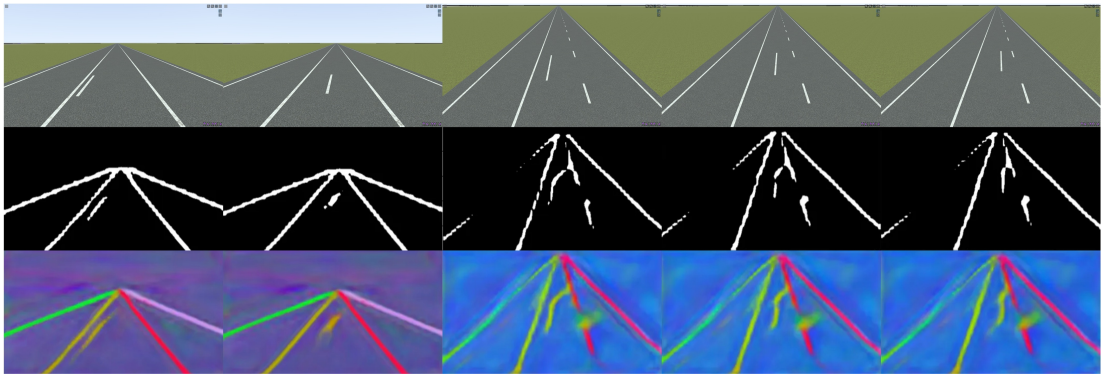

Figure 2: Digital Domain - AS 2

3 Conclusion

In this work, we present a new stealthy attack method that deceives the lane detection module of autonomous vehicles using infrared lasers. We design two attack scenarios: malicious lane extension, which creates fake lanes extending from or crossing through real lanes, and inter-lane injection, which inserts fake lanes between existing lanes. Our experiments demonstrate successful attacks in both digital and physical domains. In the digital domain using RoadRunner by MathWorks, the LaneNet [2] algorithm misidentifies fake lanes as real lanes for both attack scenarios. In the physical domain with miniature-scaled tracks and IR laser projection, both LaneNet and LaneATT [3] algorithms are successfully deceived, validating the effectiveness of our attack method.

For future work, we will refine our attack methodology based on digital domain experimental results, focusing on optimizing angle and distance parameters to enhance the robustness of physical domain experiments. Additionally, we will extend our evaluation beyond LaneNet and LaneATT to include parameter-based lane detection algorithms, analyzing how attacks can be optimized for each algorithmic category. Furthermore, we plan to conduct experiments on actual vehicles equipped with vision-based lane detection systems to demonstrate that vehicles perceive infrared as effectively as visible light, revealing significant vulnerabilities in the infrared spectrum.

References

[1] Pengfei Jing, Qiyi Tang, Yuefeng Du, Lei Xue, Xiapu Luo, Ting Wang, Sen Nie, and Shi Wu. Too good to be safe: Tricking lane detection in autonomous driving with crafted perturbations. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3237–3254, 2021.

[2] Davy Neven, Bert De Brabandere, Stamatios Georgoulis, Marc Proesmans, and Luc Van Gool. Towards end-to-end lane detection: an instance segmentation approach. In *2018 IEEE intelligent vehicles symposium (IV)*, pages 286–291. IEEE, 2018.

[3] Lucas Tabelini et al. Keep your eyes on the lane: Real-time attention-guided lane detection. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, 2021.

[4] Wei Wang, Yao Yao, Xin Liu, Xiang Li, Pei Hao, and Ting Zhu. I can see the light: Attacks on autonomous vehicles using invisible lights. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1930–1944, 2021.