A Realistic Multi-Modal Attack for LiDAR Systems*

Minjae Lee, Jiho Bae, Ungsik Kim, and Suwon Lee†

Gyeongsang National University, South Korea
{wjdchs0129, dream_cacao_jh, blpeng, leesuwon}@gnu.ac.kr

Abstract

Existing adversarial attacks on LiDAR-based perception systems often generate physically implausible point clouds that are easily detectable by human observers. To address this, we propose a realistic multi-modal LiDAR attack method that generates stealthy and realistic adversarial point clouds. By leveraging both the intrinsic properties of the LiDAR sensor and semantic information from camera images, proposed method minimizes visual artifacts from point addition and deletion, creating attacks that can deceive not only machine learning models but also human inspection.

Keywords: LiDAR Security, Adversarial Attack, Autonomous Driving

1 Introduction

The robustness of autonomous driving systems is challenged by their vulnerability to adversarial attacks, prompting defensive studies like anomaly detection. Current LiDAR attacks, which primarily add [1] or delete points [2], often ignore the sensor's physical properties, such as vertical resolution and scan range. This oversight generates physically implausible data that, while capable of misleading a system, is easily detected by human observers and thus fails to achieve true stealth. To address this, our paper proposes a realistic and stealthy attack methodology. By simulating real-world physics and sensor principles, our approach aims to create attacks that can deceive both machine perception and human visual inspection.

2 Methodology

2.1 Sensor Analysis and Pre-processing

To generate physically plausible adversarial points, we first extract foundational information from the sensors. We analyze the intrinsic properties of the LiDAR sensor, such as its vertical resolution and scan range, and extract global features from the original point cloud to understand its overall context. Concurrently, we perform semantic segmentation on the corresponding camera image to obtain pixel-level semantic information. This step is crucial for ensuring that manipulated points are semantically consistent with their surrounding environment.

2.2 Attacks based on Physical Constraints and Fusing Process

Point Addition Attack. This branch builds upon existing point addition techniques but incorporates the sensor's vertical resolution and scan range as constraints. Furthermore, by referencing the semantic segmentation map from the camera, points are generated only in

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

†Corresponding author

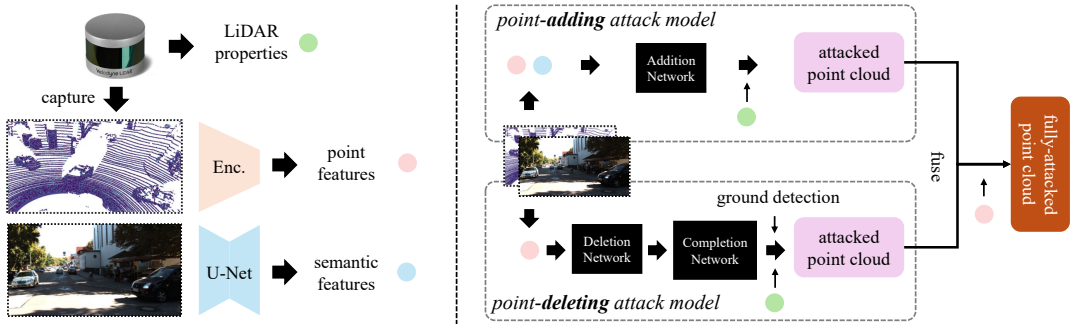

Figure 1: Overall process of proposed method. Each branch is processed independently, and the results are fused to create a single, coherent adversarial point cloud.

locations where an object could plausibly exist, thereby maximizing the attack's realism.
Point Deletion Attack. This branch aims to remove an object by deleting its corresponding points. The key challenge is to naturally reconstruct the void left behind. To achieve this, we perform 'empty space completion' by utilizing the LiDAR completion method and LiDAR sensor's properties. This process reconstructs the occluded background with physically valid points, effectively minimizing any traces of the deletion.
Fusing Adversarial Point Clouds. A simple combination of the outputs from the addition and deletion branches can create unnatural artifacts at their boundaries. To resolve this, we fuse the global features of the original data (from Section 2.1) with the local features from each branch. This feature fusion process seamlessly integrates the results of both attacks, producing a single, coherent, and natural-looking adversarial point cloud.

3 Conclusion

We proposed a realistic multi-modal LiDAR attack method to address the physical implausibility of existing LiDAR attacks. By incorporating sensor characteristics and semantic camera data, our method can generate highly stealthy adversarial point clouds designed to bypass both anomaly detection models and human inspection. This work highlights a new class of sophisticated, realistic security threats for autonomous systems.

Acknowledgment

This research was supported by the Regional Innovation System & Education(RISE) program through the RISE Center, Gyeongsangnam-do, funded by the Ministry of Education(MOE) and the Gyeongsangnam-do Provincial Government, Republic of Korea. (2025-RISE-16-001)

References

[1] Mazen Abdelfattah, Kaiwen Yuan, Z Jane Wang, and Rabab Ward. Adversarial attacks on camera-lidar models for 3d car detection. In *2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pages 2189–2194. IEEE, 2021.

[2] Yulong Cao, S Hrushikesh Bhupathiraju, Pirouz Naghavi, Takeshi Sugawara, Z Morley Mao, and Sara Rampazzi. You can't see me: Physical removal attacks on {lidar-based} autonomous vehicles driving frameworks. In *32nd USENIX security symposium (USENIX Security 23)*, pages 2993–3010, 2023.