Poster: Intensity-Aware Chosen Pattern Injection LiDAR Spoofing Attack

Ozora Sako†, Takami Sato‡, Yuki Hayakawa†, Ryo Suzuki†, Kazuma Ikeda†, Rokuto Nagata†,
Qi Alfred Chen‡, and Kentaro Yoshioka†
†Keio University; ‡University of California, Irvine

***Abstract*—Autonomous vehicles employ LiDAR-based systems for 3D object detection to monitor their environment. Addressing potential security threats to these systems is vital for ensuring safety. Previous studies have demonstrated how injecting false point clouds into LiDAR data can deceive 3D object detectors. However, while these studies often replicate the shape of objects almost perfectly, the intensity of these injected point clouds tends to be unnaturally high compared to real objects. Consequently, we find that many of these injected objects remain undetected by common 3D object detectors. In this paper, we present a novel LiDAR spoofing attack that is aware of intensity levels. This method injects objects with intensity similar to that of actual objects, greatly improving the success of attacks on object detectors compared to previous techniques.**

I. Introduction

A. Motivation

LiDAR (Light Detection and Ranging) is a crucial sensor in autonomous driving systems. It scans the surrounding environment in three dimensions and generates a point cloud (X) for each distance measurement.

$$X = \{(x_i, y_i, z_i, int_i)\} \in \mathbb{R}^{n\times 4} \tag{1}$$

Here, n is the number of points, (x_i, y_i, z_i) represents i-th point's 3D location, and int_i represents i-th point's intensity. LiDAR spoofing attacks present a notable security challenge for LiDAR systems, since these attacks disrupt accurate measurements by transmitting deceptive laser signals to the sensor [1]–[3]. While past works have verified both object injection and removal attacks in this context, in this study, we specifically focus on the Chosen Pattern Injection (CPI) attack. This approach involves introducing objects that closely replicate real ones into the detection system, thereby misleading 3D object detectors.

B. Related Works

In prior research, Chosen Pattern Injection (CPI) attacks have been validated through physical experiments [2], [3]. These studies illustrated the feasibility of precisely injecting coordinates (x_i, y_i, z_i) from a pre-recorded point cloud into LiDARs. Furthermore, they demonstrated that the injected point cloud can mislead a 3D object detector, causing it to recognize an object that does not exist.

C. Research Gap

While traditional studies have been nearly perfect in mimicking the "shape" of real objects with LiDAR spoofing attacks, a significant gap exists in replicating the "intensity." Given the objective of altering the victim LiDAR's measurement data, injected point clouds often possess unnaturally high intensity. Consequently, the intensity of these injected objects is significantly higher than that of real objects. Since such high-intensity objects are not found in nature, there is a high likelihood that they will not be correctly recognized by 3D object detectors that take intensity into account.

D. Threat Model

The objective of our attack is to introduce malicious points into a mechanical LiDAR system, thereby causing errors in its 3D object detection capabilities. To achieve the aforementioned attack goal, we assume the adversary has the following capabilities as in [2]: LiDAR parameter awareness, white-box object detector, and physical attack capability.

II. Attack design

A. Attack Framework

Our CPI attack framework operates as follows: Initially, a photodiode (PD) captures legitimate laser pulses emitted by the target LiDAR and forwards these as triggers to a function generator (FG). The FG then creates signals that control the attack laser pulses. In the final step, a laser diode (LD) emits these false laser pulses back towards the target LiDAR.

B. Attack Methodology

Traditional CPI attacks often encounter a challenge where the intensity of the injected point cloud is unnaturally high, resulting in potential non-detection by object detectors. In this study, we introduce an intensity-aware CPI (ICPI) attack, which is tailored to replicate the intensity of the injected point cloud so that it aligns with that of a real point cloud. ICPI enables to deceive object detectors that also consider intensity in their detection process. The intensity of point clouds measured by the VLP-16 indicates objects' reflectivity (ρ) and takes values from 0 to 255. Normal objects like cars and people, which are diffuse reflectors, typically have point cloud intensities ranging from 0 to 100. However, in typical LiDAR spoofing methods [2], [3], the aim is to overwrite the data of the targeted LiDAR with as a strong laser as possible. As a result, the intensity of the spoofed points often reaches the maximum values (250-255). Such high-intensity objects do not naturally exist, increasing the likelihood that the object detector will not recognize them as shown in Figure 1.

To decrease the intensity of point clouds measured by VLP-16, we focus on the returning power of the signal (P_r) and the distance from the LiDAR to the point clouds (R). Firstly, since the intensity is proportional to the P_r as shown in (2) [4], we enlarge the beam diameter of the attack laser and weaken its power, as shown in Figure 2.

$$intensity \propto P_r \tag{2}$$

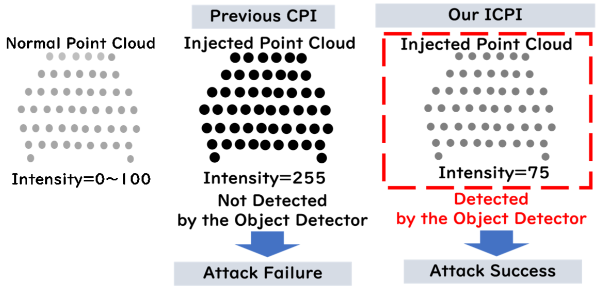


Fig. 1: Overview of our ICPI attack concept

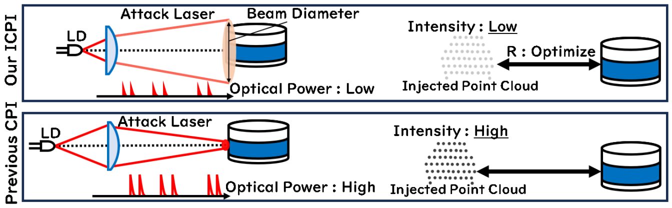


Fig. 2: Overview of our ICPI attack methodology

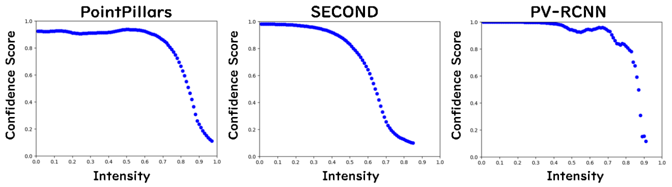


Fig. 3: The correlation between intensity and detection confidence scores for each detector

Also, VLP-16 features compensation for intensity based on distance R to return consistent results for the same surface (details undisclosed) [5]. To decrease intensity, we optimize the distance R from the LiDAR to the injected points and exploit the compensation as shown in Figure 2.

III. Experiment

First, we established that objects injected with unnaturally high intensity, similar to past studies, are not detected by 3D object detectors considering intensity. To test various scenarios, we used car data from the widely-used KITTI dataset in prior research. We selected three frames closely resembling actual attack scenarios. We tested with popular detectors used in previous studies (PointPillars, SECOND, PV-RCNN), utilizing implementations from OpenPCDet. To assess the impact of intensity, we varied the intensity of car point clouds from minimum to maximum values and measured the detection confidence scores relative to these intensity changes. All detectors showed higher detection rates with lower intensity point clouds as shown in Figure 3, which is likely correlated with the actual intensity distribution of car data. Therefore, it became clear that to increase the success rate of CPI attacks against these object detectors, the intensity of the injected point clouds must be reduced.

Subsequently, we executed physical experiments for the ICPI attack to assess the feasibility of injecting point clouds with an intensity similar to real objects. We employed the VLP-16 LiDAR, consistent with its use in prior research. According to our methodology, we adjusted the optical power of the attack laser and observed the resulting changes in intensity when varying the distance R between the LiDAR and the point clouds. By reducing the optical power of the attack laser and optimizing the distance from the LiDAR to the point clouds, we managed to lower the intensity to approximately 60-75. This finding indicates that the ICPI attack can inject point clouds with an intensity level sufficient to deceive detectors, affirming its potential effectiveness in spoofing attacks.

TABLE I: Detection Confidence Score Comparison

	No Attack	Previous CPI	Our ICPI
Intensity	4	255	75
Detection Confidence Score	0.4804	0.1683	0.4218

Finally, we compared the detection scores of object detectors using both traditional and proposed methods. We altered the intensity of car point clouds contained in a single frame of the nuScenes dataset. The intensities were adjusted to match those of the traditional method and the intensities obtained from our physical experiments. Results are shown in Table I. When the intensity was set according to the traditional CPI method, the detection confidence score was 0.1683. However, when set to the intensity level of our ICPI method, the detection confidence score closely matched that of the original point clouds, achieving a score of 0.4218. This result highlights the enhanced effectiveness of the ICPI method in deceiving object detectors.

IV. Conclusion

In previous CPI attack studies, while the shape of the injected objects could almost perfectly mimic real objects, there was a gap in that the intensity of the injected point clouds was unnaturally high and did not accurately replicate real objects. To address this gap, we propose an intensity-aware CPI (ICPI) attack in this paper. By adjusting the laser optics and the injection distance, we demonstrated that the intensity of the injected point clouds can be controlled to closely resemble that of real objects. Furthermore, our findings indicate that ICPI is effective in deceiving object detectors that consider intensity, effectively closing the gap identified in prior research.

Acknowledgements

This research was supported in part by the JST CREST JPMJCR23M4, JST PRESTO JPMJPR22PA, Amano Institute of Technology, NSF CNS-2145493, CNS-1929771, CNS-1932464, and USDOT UTC Grant 69A3552348327.

References

[1] Y. Cao, S. H. Bhupathiraju, P. Naghavi, T. Sugawara, Z. M. Mao, and S. Rampazzi, “You Can’t See Me: Physical Removal Attacks on LiDAR-based Autonomous Vehicles Driving Frameworks,” in *USENIX Security Symposium*, 2023.

[2] Z. Jin, X. Ji, Y. Cheng, B. Yang, C. Yan, and W. Xu, “Pla-lidar: Physical laser attacks against lidar-based 3d object detection in autonomous vehicle,” in *2023 IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 1822–1839.

[3] T. Sato, Y. Hayakawa, R. Suzuki, Y. Shiiki, K. Yoshioka, and Q. A. Chen, “LiDAR Spoofing Meets the New-Gen: Capability Improvements, Broken Assumptions, and New Attack Strategies,” in *Network and Distributed System Security Symposium (NDSS)*, 2024.

[4] R. A. Hewitt and J. A. Marshall, “Towards intensity-augmented slam with lidar and tof sensors,” in *2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 2015, pp. 1956–1961.

[5] J. Guo, P. V. K. Borges, C. Park, and A. Gawel, “Local descriptor for robust place recognition using lidar intensity,” *IEEE Robotics and Automation Letters*, vol. 4, no. 2, pp. 1470–1477, 2019.

Poster: Intensity-Aware Chosen Pattern Injection LiDAR Spoofing Attack

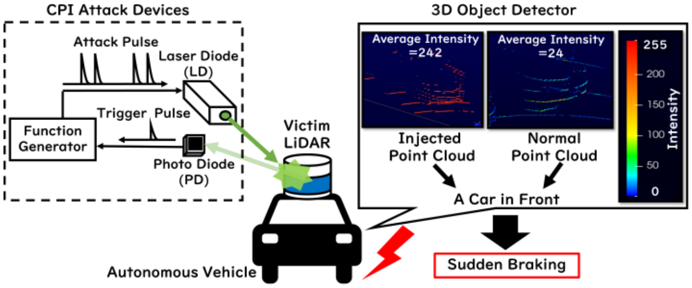
Ozora Sako[1], Takami Sato[2], Yuki Hayakawa[1], Ryo Suzuki[1], Kazuma Ikeda[1], Rokuto Nagata[1], Qi Alfred Chen[2], Kentaro Yoshioka[1]

[1] Keio University [2]University of California, Irvine

Introduction

LiDAR Spoofing

- A notable security challenge for LiDAR systems
- Disrupts accurate measurements by transmitting deceptive laser signals

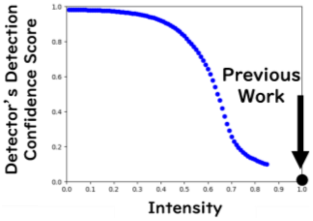


Thread Model：CPI (Chosen Pattern Injection) Attack

- Injecting point cloud that do not physically exist into LiDAR
- Inducing sudden braking in autonomous vehicles

Previous Work [1]

- Mimicking the "shape" of real objects
- Failing to replicate the "intensity" of normal point cloud



Research Gap

Objects with excessively high intensity are not included in the point cloud dataset, and the object detector fails to recognize the injected points

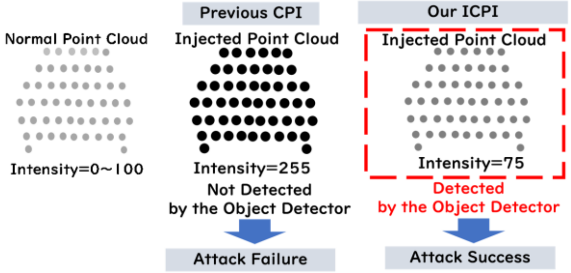
Our Contribution

- Reveal the influence of point cloud intensity on object detectors
- Introduce the Intensity-Aware CPI which enhances the attack success rate

Attack Design

Attack Concept

- High-intensity point clouds may go undetected by the object detector
- We propose an Intensity-Aware CPI (ICPI), replicating the intensity of injected point clouds to match the actual point cloud intensity
- Significantly enhance the attack success rate



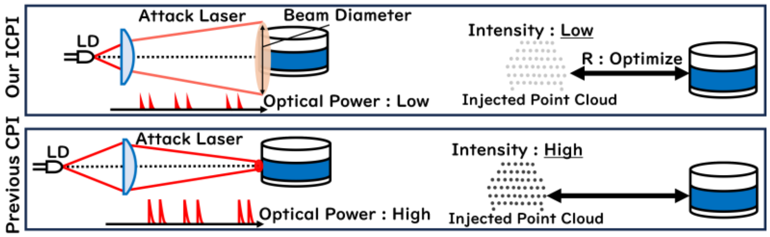
Attack Methodology

- The intensity is proportional to the returning power of the signal（P_r）

- Enlarging the beam diameter and weakening the power of the attack laser

- VLP-16 features a compensation for intensity based on distance（R）

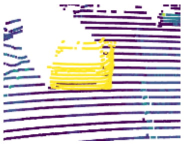
- Optimizing the distance (R) to exploit the compensation



Experiment

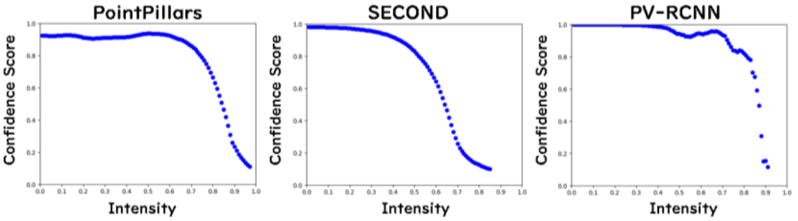
①Investigation into the Impact of Intensity on Object Detection

- Chose a frame from KITTI datasets
- Selected the target vehicle and adjusted its point cloud intensity from minimum to maximum
- Evaluated detection confidence scores using object detectors



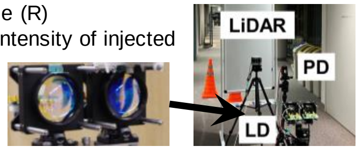
Target Point Cloud

Finding 1 : High-Intensity Value of Point Clouds Decreases the Detection Rate

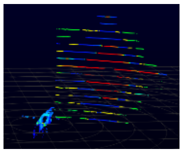


② Physical Measurement of the ICPI Attack

- Adjusting the power of the attack laser and distance (R)
- Measuring the intensity of injected point cloud



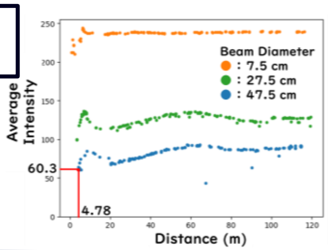
Physical Experiment Setup



Injected Point Cloud

Finding 2：The Proposed Method Enables Lowering the Intensity of Injected Point Clouds

- Reducing the power of the attack laser by enlarging the beam diameter lowers the intensity
- Optimizing the distance（R）lowers the intensity
- We managed to lower the intensity to 60 - 75



③ Evaluation on Object Detectors

- Chose a frame from nuScenes datasets
- Selected target vehicle, adjusted its intensity to the previous CPI's intensity and our ICPI's intensity
- Evaluated detection confidence scores using object detectors (SECOND)

Finding 3 : Our Method Enables More Effective Attacks on Detectors

Table 1 : Detection Confidence Score Comparison

	No attack	Previous CPI	Our ICPI
Intensity	4	255	75
Detection Confidence Score	0.4804	0.1683	0.4218

Conclusion

- Prior research had issues with unnaturally high intensity of the injected point cloud
- We propose an ICPI attack to fill this gap
- Initial experiments demonstrate that our method has higher attack success rates

Discussion

- **Defense：** Sensor fusion
- **Future Work：** Conducting attacks with multiple LiDARs and in real-world scenarios

[1]: Takami Sato et al., *LiDAR Spoofing Meets the New-Gen: Capability Improvements, Broken Assumptions, and New Attack Strategies*. In NDSS 2024.