Poster: Towards Practical LiDAR Spoofing Attack against Vehicles Driving at Cruising Speeds

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

***Abstract*—LiDAR (Light Detection and Ranging) is an essential sensor for autonomous driving (AD). Due to its critical safety implications, recent studies have explored its security risks and exposed the potential vulnerability against LiDAR spoofing attacks, which manipulate measurement data. Nevertheless, deploying LiDAR spoofing attacks against driving AD vehicles still has significant technical challenges. The current state-of-the-art attack can be successful only at $\leq$5 km/h. Motivated by this, we design novel tracking and aiming methodology and conduct a feasibility study to explore the actual practicality of LiDAR spoofing attacks against AD vehicles at cruising speeds. In this poster, we report our initial results demonstrating that our object removal attack successfully makes the targeted pedestrian undetectable with $\geq$90% success rates in a real-world scenario. Finally, we discuss the current challenges and our future plans.**

I. Introduction

The research and development of Autonomous Driving (AD) are rapidly growing year by year. One of the major drivers of the growth is enabled by LiDAR (Light Detection and Ranging) sensors, especially for over Level 4 AD. However, recent studies have posed the safety and security risks of LiDAR due to its sensitivity to ambient light noises and malicious laser emission, which is known as LiDAR spoofing attack [1]. The malicious lasers of LiDAR spoofing attacks can overwrite the legitimate measurements. Meanwhile, prior work predominantly focuses on stational lab-level setups or dynamic but impractical low-speed setups [2] even though they discuss the safety implications of their attacks against AD systems. Motivated by this, we design a novel tracking and aiming methodology to precisely emit attack lasers against the victim vehicle driving at cruising speeds (e.g., 35 km/h).

In this poster, we report our recent progress on the feasibility study attacking a fast-driving vehicle with our novel tracking and aiming system called Moving Vehicle Spoofing system (MVS system). We demonstrate that our attack can successfully remove a pedestrian from object detection results with $\geq$90% success rate in the real-world scenario that a victim vehicle is approaching at 35 km/h from 45 m away. This result implies potential serious security risks against AD vehicles. Finally, we discuss our findings, limitations, and future plans.

II. Background and Related Works

A. LiDAR Spoofing Attacks

LiDAR spoofing attacks [1]–[4] manipulate the distance measurements of LiDAR sensing by overwriting the legitimate lasers with higher-power malicious lasers. The attacks can be categorized into two distinct types. *1) Object Injection Attacks:* This type of attack injects ghost objects that do not actually exist. *2) Object Removal Attacks:* These attacks are designed to make actual objects undetected by object detectors.

B. Prior Attempt to Attack Driving Vehicles

To date, there has been no successful demonstration of LiDAR spoofing attacks on AD vehicles driving at operational speeds. We call this type of attack the Moving Vehicle Spoofing attack (MVS attack). Prior attempt [2]–[4] claims the potential attack effectiveness of the MVS attacks with digital-space simulations and physical-world experiments. However, there are some critical research gaps to be successful MVS attacks (e.g., lack of real-time and long-range detection and tracking system, real-world feasibility of aiming).

III. Methodology

To overcome critical research gaps in prior attempts, we design a MVS system; which is a novel attacking system with the IR-camera-based detection and tracking system, with an aiming system equipped with high-precision servo motor and arrayed laser diodes.

A. Overview of MVS System

Figure 1 illustrates the our MVS system. We generally follow the same optical components and electronics akin to the ones that previous studies [1]–[4] used in static or low-speed setup. Our major improvements focus on the devices to accurately track and aim fast-moving targets.

1) Real-Time and Long-Range Detection and Tracking System: To localize the target LiDAR, RGB cameras are typically employed to capture and feed images directly into an object detector [2], [3]. However, at distances exceeding 20 m, the LiDAR occupies an extremely small portion of the camera's field of view (FOV), typically just a few pixels. This significantly hinders the object detector's ability to extract meaningful features from the camera image. To address this challenge, we design a novel spoofer system with an infrared (IR) camera. Our system directly captures the emitted IR lasers from the target LiDAR. This enables accurate location detection of the LiDAR even at long-range distances.

2) Handling Image Flickering: The major challenge of our IR-camera-based detection is that the IR camera cannot always detect the laser trace emitted by the LiDAR, which scans each direction at around 10 Hz. This image flickering prevents the stable tracking of target LiDAR without any countermeasures. To address this, we design an object detection architecture fed multiple frames in the channel dimension. As the IR camera feeds grayscale images at every frame, we use three consecutive latest frames for the single detection. This design significantly improves detection stability even under image flickering.

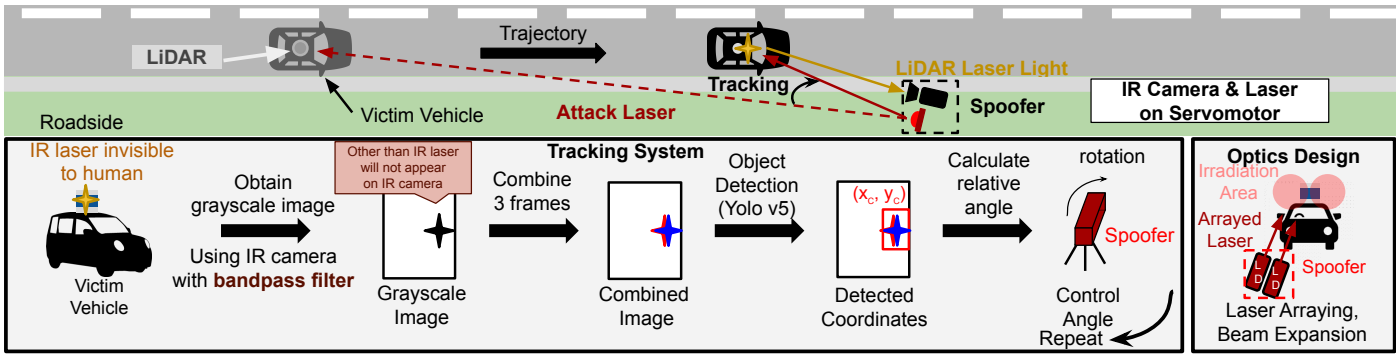


Fig. 1: Overview of our MVS system and improvements on optics design.

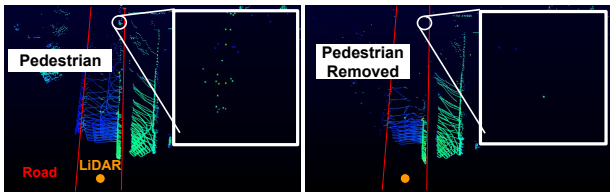


Fig. 2: An example of LiDAR point clouds visible from a vehicle moving at 35 km/h.

TABLE I: Point-level success rate of our tracking removal attack with different threshold levels of removal percentage(RP).

	Success Rate(%)						
	All Distances			>10 m			
Speed	RP(%)	100%	>90%	>80%	100%	>90%	>80%
10 km/h		71.0	87.1	92.7	75.2	91.7	98.2
35 km/h		70.0	84.3	87.1	75.0	90.6	93.8

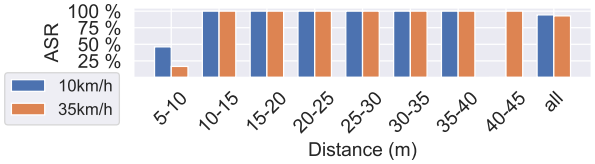


Fig. 3: Attack success rate (ASR) of MVS attack on livox detection. At 10 km/h, 40-45 m is blank as there are no results.

3) Stable and High-Precision Spoofer Design: In the context of long-range spoofing attacks, even minimal detection errors can amplify, resulting in substantial inaccuracies. This issue is further compounded when dealing with rough road surfaces, as these conditions induce vibrations in the vehicle body, leading to potential perturbations of the target LiDAR. We address this challenge by expanding the laser irradiation area as much as possible and achieved a total beam area that is about 110 times larger than that in prior work [4].

IV. Evaluation

A. Real-World MVS Attack Evaluations

Experimental Environment and Attack Methodology. Assuming a roadside attack scenario, we position the spoofer 2 m from the edge of the driving lane. The victim vehicle commenced its approach from a distance of approximately 40 m from this pedestrian. Moreover, to explore how different driving speeds affect the MVS attack's difficulty, we conducted experiments with the car moving at two speeds: 10 km/h and 35 km/h. For the method of attack, we specifically chose HFR attack [1]. HFR attack is notably potent and versatile, capable of targeting a wide range of LiDAR models. In our experiments, we set the HFR laser pulse frequency to 400 kHz.

Point Cloud Based Results. Figure 2 shows the point cloud data captured by a victim LiDAR while driving at 35 km/h, both with and without the attack. Notably, the disappearance of the pedestrian's point cloud, initially located 40 m away, evidences the efficacy of our MVS attack upon executing a removal attack. In Table I, we present the removal rate of the point cloud of the target person for each speed during the MVS attack. Remarkably, for distances greater than 10 meters, the removal rate exceeded 90 % in more than 90 % of the frames, indicating a high level of consistency in our attack.

Object Detector Based Results. To assess the effectiveness of our MVS attack at the object detector level, we processed the point cloud data obtained during the attack through the Livox Detection System. Figure 3 shows the attack success rate (ASR) for each distance at each speed, defining success as instances where the object was not detected by the system. The object detector was successfully deceived in more than 90 % of the frames during the MVS attack at both 10 km/h (94.4 %) and 35 km/h (92.9 %).

V. Concluding Remarks and Future Plans

In this poster, we presented an MVS system capable of launching an attack on cruising vehicles. We demonstrated that our attack can successfully remove a pedestrian from object detection results with $\geq$ 90% success rate in the real-world scenario. In the future, we plan to expand our evaluation scope to dive deeper into the threat of MVS attacks.

Acknowledgements

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

References

[1] 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 *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2024.

[2] 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.

[3] Y. Cao, J. Ma, K. Fu, R. Sara, and M. Mao, "Automated Tracking System for LiDAR Spoofing Attacks on Moving Targets," in *Proc. Workshop Automot. Auto. Vehicle Secur.(AutoSec)*, 2021, p. 1.

[4] Z. Jin, J. Xiaoyu, Y. Cheng, B. Yang, C. Yan, and W. Xu, "PLA-LiDAR: Physical Laser Attacks against LiDAR-based 3D Object Detection in Autonomous Vehicle," in *IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 710–727.

Poster: Towards Practical LiDAR Spoofing Attack against Vehicles Driving at Cruising Speeds

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

Research Gaps for LiDAR Spoofing Attack against Driving Vehicles (MVS Attacks)

– Prior attempt claims the potential attack effectiveness of the MVS attack
But there are 2 critical research gaps to be effective against AD vehicles driving at cruising speeds.

1) Lack of Real-Time and Long-Range Detection

– Not shown clear feasibility of MVS attacks to fast-moving targets coming from a far distance due to **limitations of the spoofer**
– To obtain the accurate location of the target AD, **high-performance detection and tracking** are required.

2) Real-World Feasibility of Aiming and Laser Emitting Device

– Almost all attacks are only evaluated against vehicle driving at low speed and close range
– Unclear whether their systems are effective against fast-moving vehicles at long range, primarily from the perspective of **aiming**

	Attack on moving target	Relative Speed	Attack from roadside	Attack types: Injection	Attack types: Removal	Maximum attack range
Ours	✓	≤35 km/h	✓	-	✓	∼ 45 m
Cao et al. 2023	✓	≤5 km/h	-	-	✓	∼ 10 m
Cao et al. 2021	✓	≤0.4 km/h	-	✓	-	∼ 4 m
Jin et al. 2023	✓	0 km/h (running parallel)	-	✓	✓	∼ 15 m

Low Speed

Close Range

Moving Vehicle Spoofing (MVS) System : Our Improved Spoofer System for MVS Attack

1) Detection at Long Ranges and Independent of LiDAR Models

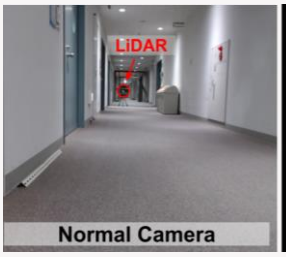
– **IR vision-based** detection system allows to detect a distant LiDAR
– **Same detection model** can be used to detect multiple LiDAR models.

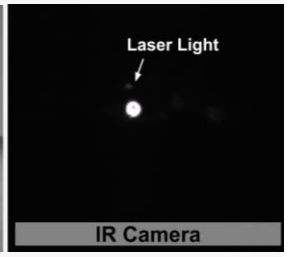
2) Robust to Image Flickering

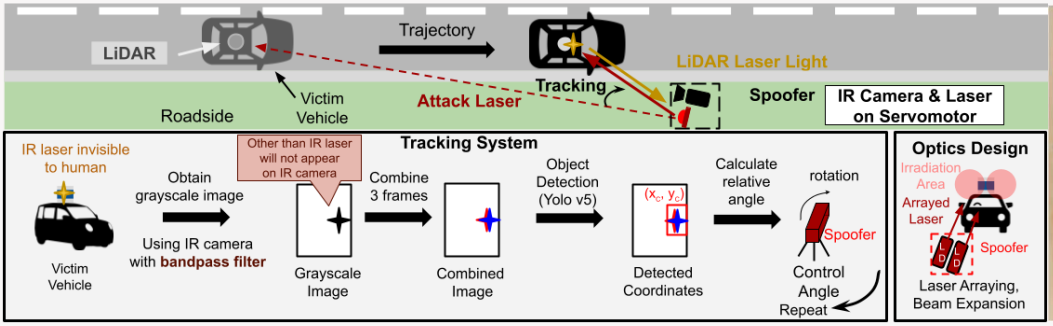
– LiDAR scans each direction at 10 Hz → IR camera cannot always detect the laser ☹
– **Detection architecture fed multiple frames** improves detection stability under flickering ☺

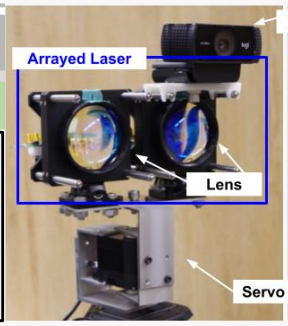
3) High Tracking Stability

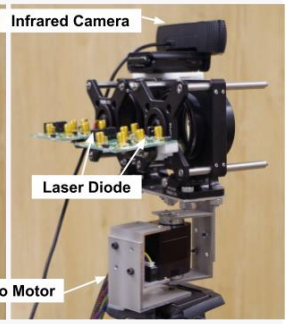
– **Arrayed laser** enhances the stability of tracking against driving vehicles





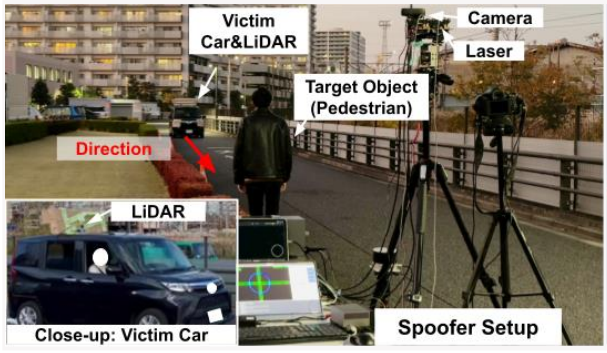


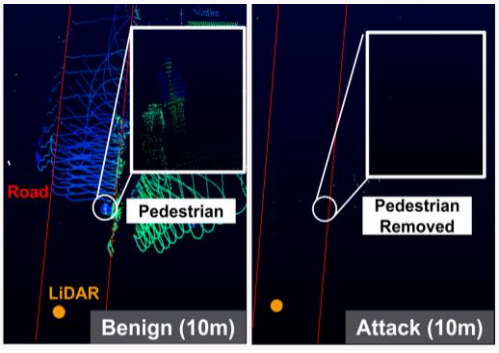


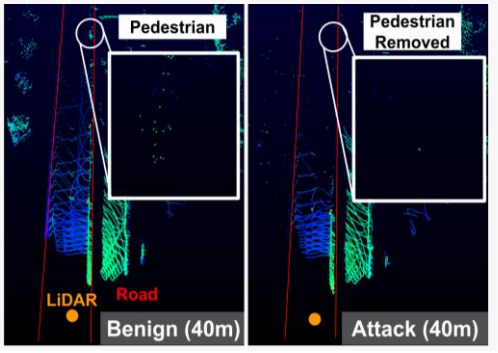


Attack Demos (Roadside Scenario)

MVS attack against vehicles driving at 35 km/h

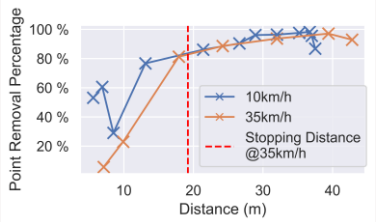




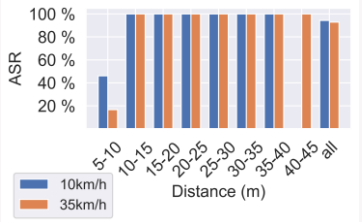


Quantitative Analysis

– **Point cloud based results**



– **Object detector based results**



Conclusion & Future Plans

– **Presented MVS system capable of launching an attack on cruising vehicles approaching 35 km/h**
– Will evaluate MVS attacks on vehicles traveling at **higher speeds**
– Plan to conduct tests on **multiple LiDAR models**
– Plan to propose **defense mechanisms** for AD systems utilizing LiDAR