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

Takami Sato*†, Ryo Suzuki*‡, Yuki Hayakawa*‡, Kazuma Ikeda‡, Ozora Sako‡, Rokuto Nagata‡,
Qi Alfred Chen†, Kentaro Yoshioka‡
†University of California, Irvine, Department of Computer Science
‡Keio University, Department of Electronics and Electrical Engineering

***Abstract*—LiDAR plays an essential role in autonomous driving (AD) even though the vulnerability to spoofing attacks is widely known. This threat has not been regarded as a serious risk yet because deploying LiDAR spoofing attacks against driving AD vehicles still has significant technical challenges, particularly in accurately aiming at the LiDAR of a moving AV from the roadside. This demo shows videos of our recent efforts to explore the possibility of attacking vehicles driving at cruising speed.**

I. Introduction

LiDAR plays an inevitable role in recent autonomous driving (AD). However, recent studies have posed security risks against LiDAR spoofing attacks [1], [2]. However, prior work demonstrated the attacks only on impractical low-speed setups (e.g., at most 5 km/h [2]). Motivated by this, we are investigating the possibility of LiDAR spoofing attacks against driving vehicles. In this demo, we report our recent efforts to evaluate more practical LiDAR spoofing attacks and our attempts to attack vehicle driving at cruising speeds (35 km/h).

II. Attack Design

We will demonstrate 2 LiDAR spoofing attacks:
HFR attack [3] emits periodic pulses between 400 kHz and 5 MHz at the victim LiDAR to overwrite all legitimate lasers of the victim LiDAR. The major advantage of the HFR attack over prior work [1], [2] is no requirement to know online information from the victim LiDAR, and thus we consider that this attack has high feasibility even for the moving vehicles.
A-HFR attack [4] is an extension of the HFR attack. A-HFR attack can achieve 5 times higher frequency than the HFR attack. A-HFR attack boosts the frequency when scanning the target object, and idles the attack in the other time to avoid overheating. While this attack needs to know when LiDAR scans which object roughly, it is much less information to know from the victim than prior work [1], [2].

III. Demonstration

We plan to play the attack videos of our indoor and outdoor driving experiments in this demo session.

A. Indoor Experiments

Fig.2 shows the attack demonstration of the HFR and A-HFR attacks on an anonymized LiDAR, which has state-of-the-art pulse fingerprinting technology to authenticate its own laser. As shown, the prior HFR attack does not work on the LiDAR because its attack frequency is not enough to bypass the authentication [3]. On the other hand, the A-HFR attack can completely remove the attack target.

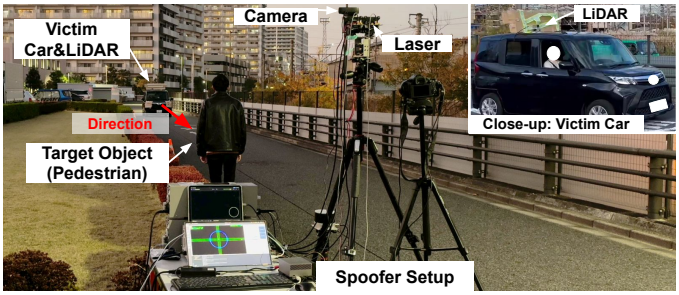

Fig. 1: Experimental setup of the outdoor driving scenario.

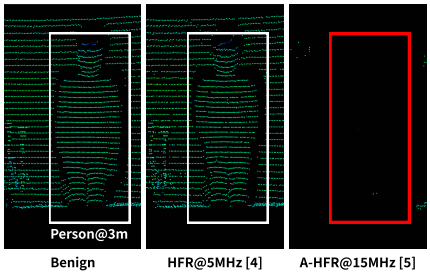

Fig. 2: Demo of the HFR and A-HFR attacks on a LiDAR with fingerprinting.

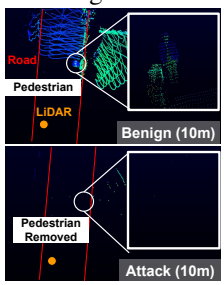

Fig. 3: Attack in outdoor experiment

B. Outdoor Driving Experiments

We deployed the HFR attack against a vehicle at 35 km/h speed. As shown in Fig. 1, we position the spoofer 2 m from the edge of the driving lane. We target a person standing 5 m. The victim vehicle is approaching 40 m away. Fig. 3 shows that the HFR attack can completely make the pedestrian undetected from 40 m away to 10 m away.

References

[1] 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 Security and Privacy*, 2023.

[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*, 2023.

[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," 2024.

[4] Y. Hayakawa, T. Sato, R. Suzuki, K. Ikeda, O. Sako, R. Nagata, Q. A. Chen, and K. Yoshioka, "WIP: An Adaptive High Frequency Removal Attack to Bypass Pulse Fingerprinting in New-Gen LiDARs," *VehicleSec*, 2024.

*co-first authors

Symposium on Vehicles Security and Privacy (VehicleSec) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-7-6
https://dx.doi.org/10.14722/vehiclesec.2024.25018
www.ndss-symposium.org