Demo: Automated Tracking System For LiDAR Spoofing Attacks On Moving Targets

Yulong Cao*, Jiaxiang Ma*, Kevin Fu*, Rampazzi Sara† and Morley Mao*
* {yulongc, mmmjx, kevinfu, zmao}@umich.edu, University of Michigan, Ann Arbor, MI, USA
† srampazzi@ufl.edu, University of Florida, Gainesville, FL, USA

***Abstract*—Recent studies have demonstrated that LiDAR sensors are vulnerable to spoofing attacks, in which adversaries spoof fake points to fool the car's perception system to see nonexistent obstacles. However, these attacks are generally conducted on static or simulated scenarios. Therefore, in this demo, we perform the first LiDAR spoofing attack on moving targets. We implemented a minimal tracking system integrated with the spoofer device to perform laser-based attacks on Lidar sensors. The demo shows how it is possible to inject up to 100 fake cloud points under three different scenarios.**

I. Introduction

Advanced driver-assistance (ADA) systems used in autonomous vehicles leverage LiDAR sensors technology for obstacle detection. Prior research has shown that spinning LiDARs are vulnerable to laser spoofing attacks. In particular, Cao et al. [4] demonstrated how to selectively inject fake points to a LiDAR in order to fool the LiDAR-based perception system of autonomous vehicles into perceiving nonexistent obstacles. Such LiDAR spoofing attacks can lead to dangerous automatic emergency maneuvers such as steering or activate the brakes that may injure passengers, other vehicles, and pedestrians. However, these attacks were demonstrated in static scenarios (e.g. the LiDAR sensor in a fixed position). Thus, it is unclear whether such attacks can be successfully performed if the victim's vehicle is moving. In order to investigate this scenario, we designed and built a minimal automated tracking system (see Figure 1) integrated to an optimized version of the spoofer device developed by Cao et al. [4] to perform laser attacks in dynamic settings (e.g. moving robotic systems). The developed tracker is composed of a LI-USB30-AR023ZWDR camera [1] to detect the LiDAR location and a pan-tilt system PTX-ATX18 [2] to automatically aim a 905 nm pulsed laser diode with integrated driver. In this demonstration, we verify the feasibility of the laser spoofing attack in dynamic settings. The developed tracking system can be used in future studies to investigate LiDAR spoofing attacks in real-world scenarios.

II. Tracking System Overview

We adopted the SSD Inception v2 COCO model [3] to detect the LiDAR location. We trained the model using a custom dataset consisting of 320 LiDAR images publicly available, captured with different scenarios. To further increment the size of the dataset, we used standard image data augmentations techniques such as horizontal flipping and random crop. The model achieves a mean average precision (mAP) of 0.8 at intersection over union (IOU) of 0.5 in the test set. To predict a smoother bounding box of the LiDAR over continuous frames, we implemented the SORT model [5] to track the LiDAR using the prediction results of the object detector. We then extracted the spatial coordinates of the LiDAR based on the camera parameters to calculate the pan-tilt system movement for aiming the laser to the target direction keeping the LiDAR sensor at the center of the camera frame.

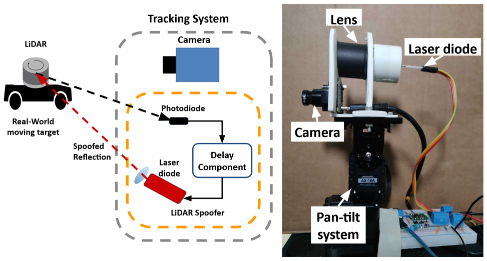

Fig. 1. Spoofing attack overview with laser integrated to the pan-tilt system.

III. Demonstration

We performed the laser spoofing attack demonstration[1] tracking a Velodyne VLP-16 PUCK on top of a Neato Botvac D85 Robot while proceeding on a straight line in three different indoor scenarios: (1) at the maximum robot speed of 0.11 m/s, (2) up to 4 meter away from the spoofer, and (3) under different environmental light conditions. In all the scenarios the spoofer device were able to continuously spoof up to 100 fake points, confirming the feasibility of the attack on moving targets.

Acknowledgment

This research was funded by NSF Grants CNS-2031077 and CNS-1930041, and awards from Facebook and UM MCity.

References

[1] "LIUSB30AR023ZWDR Datasheet," https://www.leopardimaging.com/.

[2] "PhantomX Robot Turret Kit," https://www.trossenrobotics.com/.

[3] "TensorFlow 1 Detection Model Zoo," https://github.com/tensorflow/-models/blob/master/research/-object_detection/g3doc/tf1_detection_zoo.md.

[4] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial sensor attack on lidar-based perception in autonomous driving," in *ACM SIGSAC CCS*, 2019.

[5] N. Wojke, A. Bewley, and D. Paulus, "Simple online and realtime tracking with a deep association metric," in *IEEE ICIP*, 2017.

Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021
25 February 2021, Virtual
ISBN 1-891562-68-1
https://dx.doi.org/10.14722/autosec.2021.23019
www.ndss-symposium.org

[1] Demo videos available at https://sites.google.com/view/lidarspoofingattack