Poster: Blinding Lights: Attacking Traffic Sign Recognition Through Adversarial Flickering of Streetlights

Alkim Domeke, Pedram MohajerAnsari, Mert D. Pesé
Clemson University
{adomeke, pmohaje, mpese}@clemson.edu

***Abstract*—Ensuring the security of autonomous vehicles (AVs) remains a paramount concern for researchers dedicated to enhancing traffic safety. This poster introduces a novel adversarial example for compromising AV perception systems. It details an attack method where flickering of streetlights, induced by a high-powered laser, causes misclassification of traffic signs. The practicality, legality, and stealthiness of this approach are emphasized, highlighting a significant vulnerability in AV systems.**

I. Introduction

This research focuses on the vulnerability of the perception systems to adversarial attacks, particularly in traffic sign recognition. We propose a legal, stealthy, and practical attack by manipulating streetlight flickering using a common laser pointer, presenting a significant challenge to AV security.

II. Attack Design and Methodology

We targeted LED streetlight sensors, increasingly prevalent in the U.S. [1], by inducing flicker with high-powered lasers to disrupt AV camera frames. Our lawful and reversible approach leverages ubiquitous LED lighting [2] and was tested in CARLA for frequencies that affect typical AV cameras [3]. Laser parameters and the attack model are depicted in Fig. 1. Our experiments used modified urban settings in CARLA, with different weather conditions at night to minimize interference from other light sources, applying advanced detection algorithms like Faster R-CNN with Inception Resnet V2 for their efficiency and precision in AV contexts.

III. Experimental Results

Results show flickering frequency, distance, and weather impact on sign recognition accuracy, with graphs highlighting misdetection risks. As seen in Table I, safety implications were analyzed by vehicle deceleration and an average driver's response time to assess stopping before a STOP sign. However, if reaction time of the driver is above the average value due to factors such as age or common distractions like texting, safety dangers surge as the available time for deceleration shortens.

IV. Interpretation of Results

Table I uses color codes for deceleration to indicate attack severity on AV stop times: green for safe, orange for compromised, and red for critical stop scenarios. The simulations tested the attack's robustness across different weather conditions and laser frequencies, measuring success by the drop in cutting-edge traffic sign detection algorithms' confidence levels. As detailed in Table II, adverse weather conditions were found to amplify the attack's impact and analysis on frequency revealed that a 60 Hz flicker rate proved most effective.

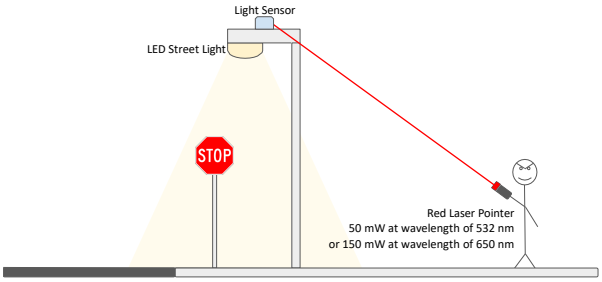

Fig. 1. Laser Attack Setup on Streetlights

TABLE I
Deceleration (a) for Different D_{Total} and v_i with $t_{\text{reaction}} = 1.5$ seconds

Distance	Initial Speeds					
	10 km/h	20 km/h	30 km/h	40 km/h	50 km/h	60 km/h
10 m	2.58	5.16	7.74	10.33	12.92	15.50
30 m	0.68	1.36	2.04	2.73	3.41	4.09
50 m	0.41	0.81	1.21	1.61	2.01	2.41

TABLE II
Mean Confidence of Attack Model by Weather Condition and Frequency

Weather	Mean Confidence	Frequency (Hz)	Mean Confidence
Clear	0.31	0.5	0.15
Cloudy	0.01	5.0	0.07
Rain	0.06	30.0	0.08
Wet	0.13	60.0	0.06

References

[1] New data shows LED streetlights reduce electricity costs. (Apr 2023). Retrieved from https://www.roadsbridges.com/roadway-lighting/news/11004364/new-data-shows-led-streetlights-reduce-electricity-costs
[2] Digital Pressworks. (Oct 2022). Dealing with Street Lights. Retrieved from https://www.digitalpressworks.com/dealing-with-street-lights/
[3] EETimes and EETimes. (Mar 2016). ADAS Front Camera: Demystifying Resolution and Frame-Rate. EE Times. Retrieved from https://www.eetimes.com/adas-front-camera-demystifying-resolution-and-frame-rate/

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.2024.25022
www.ndss-symposium.org