Data Management Plan

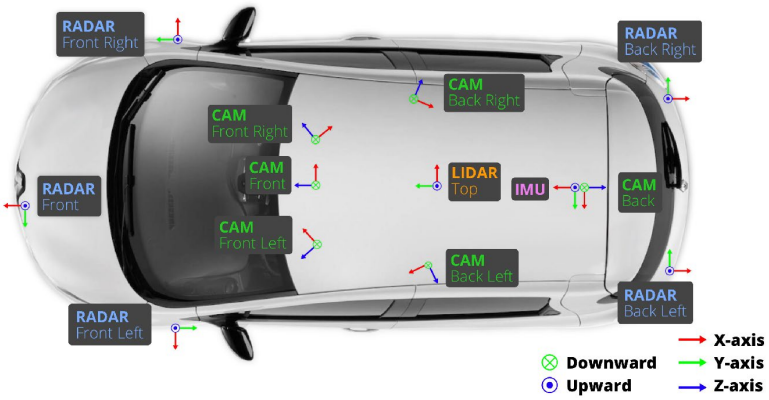
Project Title:	Identifying and Patching Vulnerabilities of Camera-LiDAR Based Autonomous Driving Systems
PI Name and Contact:	Name: Cihang Xie Title: Assistant Professor Affiliation: UC Santa Cruz Phone: 424-320-1038 Email: cixie@ucsc.edu
Submission Date:	January 31, 2025
Version:	1.0
Project Performance Period	January 1, 2024 – December 31, 2024

Project Summary

Autonomous driving systems rely on advanced perception models to interpret their surroundings and make real-time driving decisions. Among these, Bird's Eye View (BEV) perception has emerged as a critical component, offering a unified 3D representation from multi-camera and sensor inputs. While BEV-based models have gained traction in industry-leading platforms like Tesla Autopilot, their security vulnerabilities remain largely underexplored in adversarial machine learning research. This study provides a multi-dimensional security analysis of BEV perception models, focusing on adversarial threats in both vision-only and multi-sensor fusion architectures. We examine the susceptibility of state-of-the-art models—including BEVDet, BEVDet4D, DAL, and BEVFormer—to adversarial attacks targeting their detection and decision-making capabilities. Unlike traditional adversarial research that primarily misleads perception models at the classification level, this study investigates real-world attack scenarios where adversaries can manipulate perception to cause practical disruptions, such as inducing traffic congestion or triggering unsafe vehicle behaviors. Our findings reveal significant security risks in BEV-based perception, with both vision-only and sensor-fusion models vulnerable to adversarial perturbations. Attack transferability across architectures further highlights the urgency of developing robust defense mechanisms to ensure the reliability of self-driving technology. This work underscores the need for adversarially resilient perception models to safeguard the future of autonomous driving.

1. Data Description

The data we collected are sensor data and object annotations collected from CARLA's built-in simulated environment. The sensor data we collected includes photos captured by 6 RGB cameras and RADAR signals captured by 4 LiDAR sensors. These sensors are implemented by the following layout.



The object annotations include the categories and bounding boxes for every pedestrian and vehicle that appears in the RGB images.

2. Data format and metadata standards

RGB images are stored as JPG images, and LiDAR data are stored as raw binary. Bounding boxes are stored as NumPy arrays in directories named by category names. Instead of the raw data described above, we mainly used preprocessed data, which were converted into the same format as the NuScenes dataset. Please refer to this link (https://www.nuscenes.org/nuscenes#data-format) for more information. Both the raw and converted data will be shared and available for open access.

All of this data is stored on our servers during the research.

3. Access Policies

We will upload the data to an online storage service, e.g. Google Drive, Huggingface, with open access. All ones with the URL should be able to access it.

4. Policies and Provisions for Re-use, Redistribution, Derivatives

As all the data are collected in a simulated CARLA environment, there shall be no ethical or copyright concerns.

5. Plans for Archiving and Preservation of Access and Data Integrity

All the data we collected via the CARLA simulator during the research will be submitted to the TraCR committee for future publication and long-term access.

6. Change Log

Version	Date	Description
1.0	02/09/2025	Init