ROS File Analysis

Venkata Gowtham Gottimukkala

Computer & Information Science & Engineering, University of Florida
v.gottimukkala@ufl.edu

Introduction

Perception is a crucial component of autonomous vehicles (AVs), using sensors such as cameras and LiDARs to understand the driving environment. Previous research[1] has focused on the security of perception systems due to their impact on road safety. In this project, we propose a pipeline for analyzing data in the event of a physical removal attack (PRA)[1] on an AV system. PRA is a laser-based spoofing technique that selectively removes LiDAR point cloud data of genuine obstacles at the LiDAR sensor level effectively creating gaps in the data. The aim of our pipeline is to automatically compute and visualize the variations in the data when such an attack happens. It does this by combining multiple data sources into a common frame of reference and using the Intersection over Union method to determine the overlap between the predictions and the actual data.

To accomplish this, we will use the Autoware[2] framework, which is built on top of ROS[3]. Autoware provides all of the necessary functions for driving autonomous vehicles, including localization, object detection, route planning, and control. ROS[3] is a publish/subscribe system that enables nodes to exchange messages about data at different levels of abstraction. Autoware[2] subscribes to the point cloud data (from the LiDAR) published by ROS[3], performs euclidean clustering, and publishes the predicted object clusters.

Methodology and Pipeline

The pipeline is implemented using Python and is evaluated using the public KITTI[4] dataset, which provides LiDAR and Image data captured from the real world. Figure 2 shows the input, output and modules involved in the pipeline. In addition to the modified LiDAR raw data (after PRA attack described in Figure 1), the pipeline is also given the output of Autoware's object clustering. The pipeline then converts the data that are in different spatial coordinate frames to a common frame of reference allowing for a comparison of the predictions and ground truth. The output of the pipeline is a CSV file containing the raw data and predicted cluster data paths, along with the computed IoU.

Figure 3 is the output of the pipeline visualizing the modified LiDAR raw data, Autoware predictions on it and the computed IoU.

UF Herbert Wertheim College of Engineering
UNIVERSITY of FLORIDA

Physical Removal Attack (PRA)

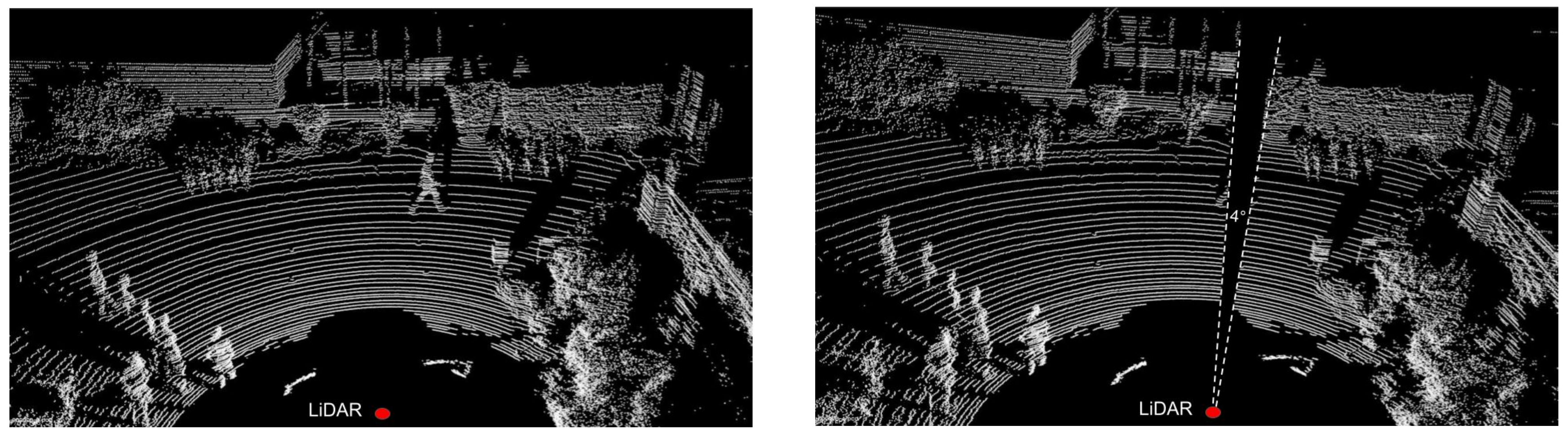

Figure 1. PRA[1] aiming to remove the walking pedestrian in front of the vehicle with an attack angle of 4 degrees.

Pipeline Flow Diagram

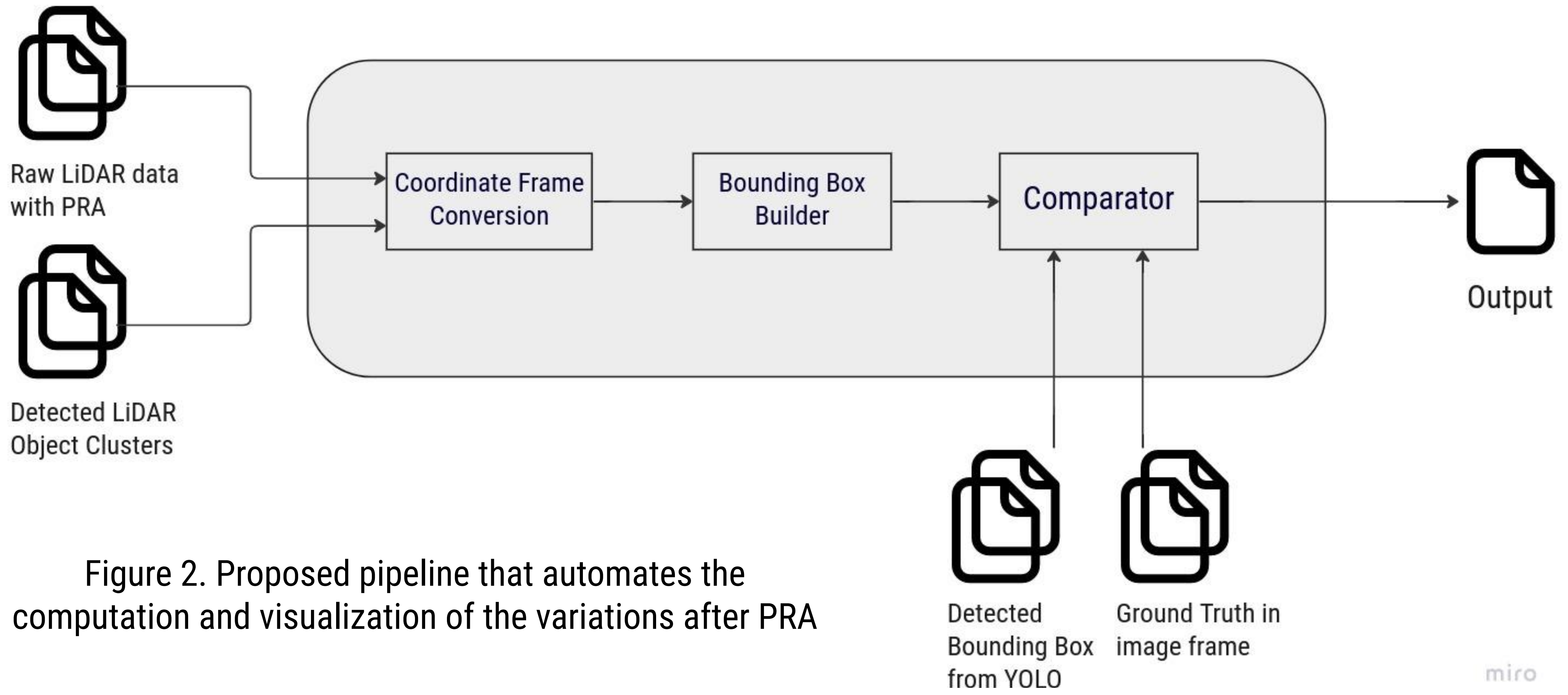
Raw LiDAR data with PRA
Detected LiDAR Object Clusters
Coordinate Frame Conversion
Bounding Box Builder
Comparator
Output
Detected Bounding Box from YOLO
Ground Truth in image frame
miro

Figure 2. Proposed pipeline that automates the computation and visualization of the variations after PRA

Comparision

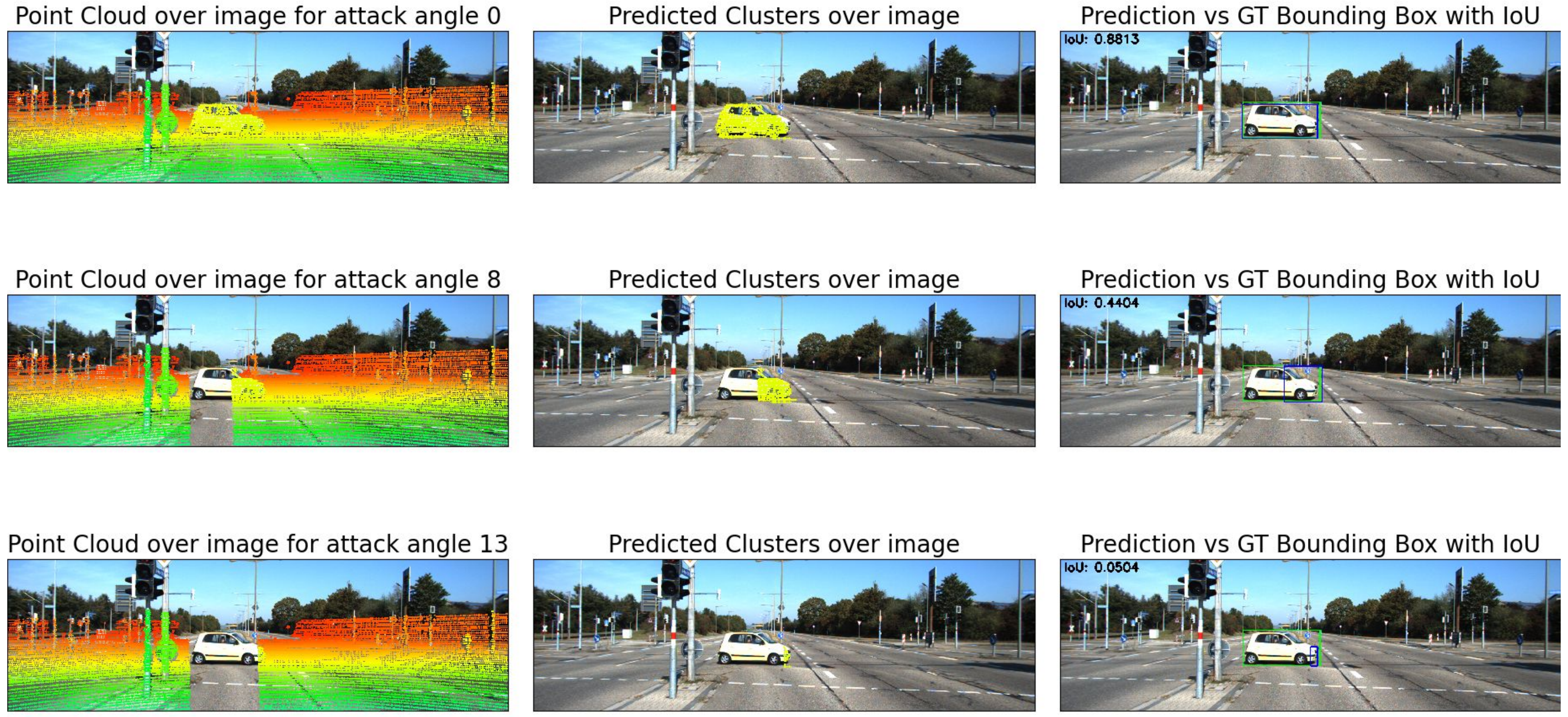
Point Cloud over image for attack angle 0
Predicted Clusters over image
Prediction vs GT Bounding Box with IoU
IoU: 0.8813
Point Cloud over image for attack angle 8
Predicted Clusters over image
Prediction vs GT Bounding Box with IoU
IoU: 0.4404
Point Cloud over image for attack angle 13
Predicted Clusters over image
Prediction vs GT Bounding Box with IoU
IoU: 0.0504

Figure 3. Pipeline output on a frame with one vehicle obstacle and PRA with different attack angles

Results

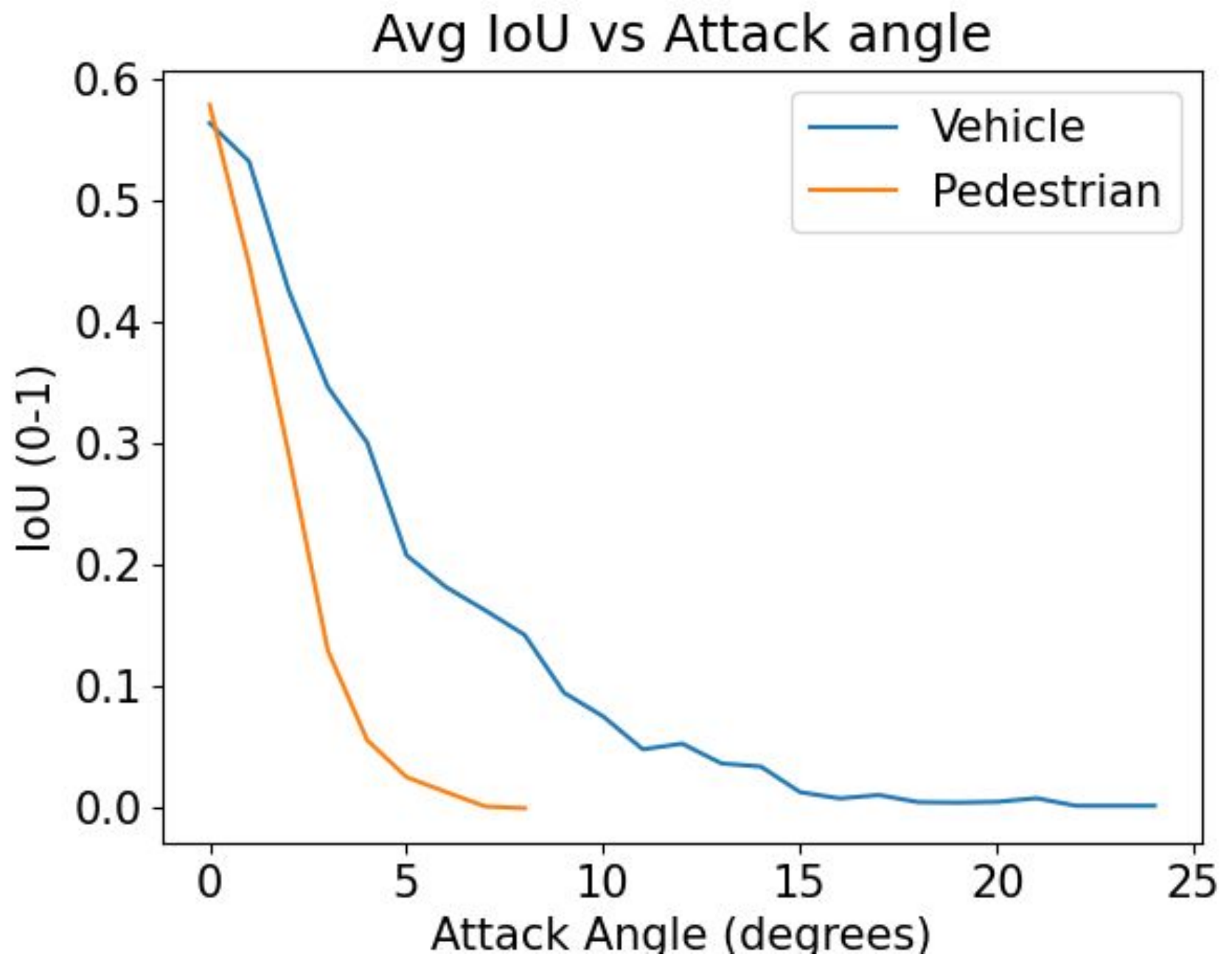

Figure 4. Average Intersection over Union metric vs attack angle used for the physical removal attack

As shown in Figure 4, we plot the attack angle against the average IoU for two different obstacles: vehicle and pedestrian. The Intersection over Union metric is the lowest i.e. the obstacle is completely removed for attack angles 24 and 7 for the vehicle and pedestrian obstacles, respectively.

Conclusion and Future Work

Our analysis shows the variations between the predictions and the ground truth when a physical removal attack (PRA) occurs on the LiDAR data. The pipeline provides modules for coordinate frame conversion, filtering LiDAR data points based on bounding box coordinates, generating bounding boxes, calculating the IoU, and building ROS bags from .bin and .pcd point cloud data. These modules successfully automate the analysis and visualization of variations that occur during attacks when given ROS bags as input.. In the future, this pipeline can be used to analyze other types of attacks on information channels within the ROS framework.

References

1. Yulong Cao, S. Hrushikesh Bhupathiraju, Pirouz Naghavi, Takeshi Sugawara, Z. Morley Mao, and Sara Rampazzi. You can't see me: Physical removal attacks on lidar-based autonomous vehicles driving frameworks. In 32nd USENIX Security Symposium (USENIX Security 23), 2023.
2. https://github.com/autowarefoundation/autoware
3. ROS: Robot operating system. http://www.ros.org/.
4. Geiger, A., Lenz, P., Stiller, C., & Urtasun, R. (2012). Are we ready for autonomous driving? The KITTI vision benchmark suite. In Conference on Computer Vision and Pattern Recognition (pp. 3354-3361).