

Full length article

LiDAR point cloud transmission: Adversarial perspectives of spoofing attacks in autonomous driving

Tariq Hussain^{a,b}, Muhammad Nawaz Khan^{c,*}, Bailin Yang^{a,b,*}, Razaz Waheeb Attar^d, Ahmed Alhomoud^e

^a School of Computer Science and Technology, Zhejiang Gongshang University, Hangzhou 310018, China

^b School of Statistics and Mathematics, Zhejiang Gongshang University, Hangzhou 310018, China

^c Department of Smart Security, Gachon University, Seongnam 13120, Republic of Korea

^d Management Department, College of Business Administration, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

^e Department of Computer Sciences, Faculty of Computing and Information Technology, Northern Border University, Rafha 91911, Saudi Arabia

ARTICLE INFO

Keywords:

LiDAR
Point cloud compression
Security
Spoofing attacks
Autonomous vehicles
False positive and true positive
Average precision
CARLA

ABSTRACT

LiDAR technology uses laser light to illuminate the surrounding area and detect 3D objects. Calculates different features such as distance, shape, height, and direction of objects, ultimately generating comprehensive 3D maps by collecting cloud points. They are frequently used in autonomous vehicles, robotics, forestry, archaeology, and environmental monitoring. LiDAR is important in autonomous vehicles for recognizing objects, pedestrians, and other vehicles, allowing them to make judgments to prevent collisions and ensure human safety. The LiDAR systems are generally robust; they are not immune to certain types of security attacks that could compromise the integrity of the signals and may affect the accuracy of the data. If the signal is compromised, the system could incorrectly interpret the environment, resulting in erroneous object recognition, incorrect obstacle avoidance decisions, or inaccurate environment mapping. As a result, it can lead to serious consequences, such as property damage, accidents, or dangerous driving conditions. To address these security challenges and establish better security mechanisms for LiDAR systems, we have proposed a novel technique for detecting and avoiding all possible spoofing attacks on LiDAR signals. Initially, the system identifies potential spoofing attacks, and as a preventive measure, it employs an optimized path strategy. This strategy ensures safe crossings and autonomous navigation while avoiding obstacles along the vehicle's route. The main aim is to identify the spoofed objects, suitably map the 3D presentation of the objects, and properly navigate autonomous vehicles with an optimized path selection in the automatic driving system. The proposed system is validated in different scenarios, and the experimental results demonstrate a success rate of 94.57% in true positive and false positive rates, indicating the effectiveness of the system. The average precision rate of 0.95 further supports its performance. The strength of the system was confirmed by testing it with different intersection over union (IoU) rates in different situations and closely looking at the attacker's success rate.

1. Introduction

LiDAR (Light Detection and Ranging) (*LiD*) is an advanced remote sensing technology that uses laser light to accurately measure distances and create complex 3D maps of its surrounding area and objects (Bhupathiraju et al., 2023; Coops et al., 2021; Roriz et al., 2021). The main aim is to create transportation systems that promote safety, resilience, and responsiveness. Most of the autonomous vehicles (AV) in development include a variety of cameras, sensors, GPS, radar, LiDAR, and an onboard processing unit. All of these systems work together to map the location and surroundings of the vehicle in a 3D point cloud (3DX) (Cao et al., 2023; Qiao and Zulkernine, 2023).

LiD works by broadcasting laser light pulses and calculating how long the reflected light returns from the 3D object (O_{3b}). It helps detect the actual distance between different objects in the surroundings and properly map them as real-world objects. It is recommended to create a comprehensive and precise 3D map of its surroundings (Beck et al., 2023).

Its working principle is similar to that of radar technology but uses laser beams instead of radio waves, which create more precise images O_{3b} . It is normally used to measure a million distances from sensors to surface points. It operates at remarkable speed, efficiently calculating the distances between *LiD* and O_{3b} . There are three main components:

* Corresponding authors.

E-mail addresses: uom.tariq@gmail.com (T. Hussain), muhammadnawaz@gachon.ac.kr (M.N. Khan), ybl@zjgsu.edu.cn (B. Yang).

<https://doi.org/10.1016/j.cose.2025.104544>

Received 7 October 2024; Received in revised form 15 April 2025; Accepted 23 May 2025

Available online 1 July 2025

0167-4048/© 2025 Elsevier Ltd. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

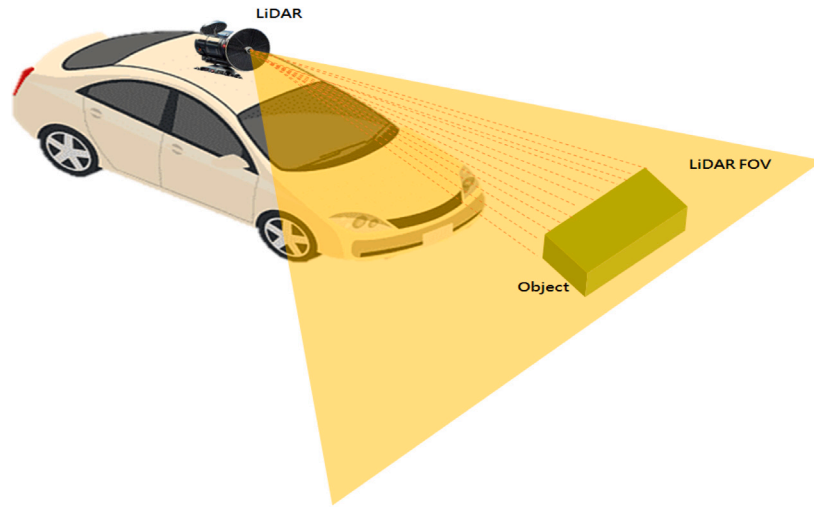


Fig. 1. LiDAR communication with FOV & 3D-Object detection.

(1) Laser light: *LiD* emits pulsed light waves of laser directed at the object. Subsequently, these light pulses bounce back onto the surface and are detected by the scanner. (2) Scanner: The emitted light will bounce off an object and return to the sensor. The scanner within the sensor is carefully adjusted to detect these reflected light waves. (3) GPS Receiver: After the scanner identifies the light, the device's GPS receiver calculates the light's distance traveled. By measuring the time it takes for light to reflect and return, a detailed map of the location dimensions of the objects is created (Zhou et al., 2023; Sun et al., 2023; Li et al., 2023).

LiD Technology's capacity to deliver precise and thorough 3D mapping and distance measurements makes it useful in a variety of sectors, including surveying and mapping, urban planning and infrastructure, forestry and agriculture, archaeology and cultural heritage, meteorology, floodplain mapping, mining and quarrying, etc. Zhang et al. (2020a) and Li et al. (2021a). It is also used in *AV*, drone technology, and cell phones. *AV* Technology has changed significantly and has been largely influenced by *LiD*. The precision and accuracy of *LiD* data have revolutionized navigation, autonomous driving, and pilot asset systems within the *AV* industry. In Fig. 1, *LiD* – *sen* has been shown with *LiD* – *FOV*, *O_{3b}* (Schepis et al., 2023). Although *AV* technology has improved efficient and safe communication, improved safety, and increased comfort, it also opens the door to various types of attacks and threats (Vishnu et al., 2023; Sun et al., 2020a; Zhu et al., 2021). The point cloud is *LiD*, a critical component of *AV* systems and is essential to detect and perceive the environment. However, growing connections *AV*s create opportunities for attackers to exploit vulnerabilities (Wang et al., 2023). Sending false and incorrect data by spoofing the signals to the cloud point can lead to severe incidents or collisions (Shafique et al., 2021; Airlangga and Liu, 2023). In this situation, an attacker could alter the *LiD* data to mislead the *AV*'s perception system (Cao et al., 2023; Qiao and Zulkernine, 2023). These attacks might include sending deceptive signals to confuse other vehicles on the road or creating false objects to compromise the integrity of the communication network, among them *AV*s. To address these security challenges, in this research work, we have proposed a novel method to identify the spoofing attacks of *LiD* signals and adequately manage them so that we *AV*s can avoid these spoofing attacks by introducing an optimized path selection procedure. The main contributions of the proposed work are as follows:

- To analyze scenario-based spoofing attacks and find out how to compromise authentic *LiD* data for various purposes that can divert or delay transmissions, which can cause the point-cloud system to have erroneous data.

- To analyze the specific spoofing attack with all possible capabilities and challenges. Subsequently, assess the attack's impact on the same scenario.
- To verify the efficiency of the proposed mechanism using the *CARLA* simulators by testing it against established defense mechanisms for cloud point spoofing, a new improved path optimization strategy has been introduced to effectively mitigate the identified threat and avoid it on the *AV*s route.

The rest of the paper is arranged as follows: Section 2 is Related Work in *LiDAR*-Based Approaches; Section 3 is the Internet of Autonomous Vehicles; Section 4 is the Threat Model for Spoofing Attacks; Section 5 is the Impact of the Spoofing Attacks; Section 6 is Problem Definition; Section 7 is Optimal Path Selection for Collision Avoidance; and Section 8 is Evaluation of the System. Finally, we have concluded the paper in Section 9.

2. Related work in *LiDAR*-based techniques

A significant challenge with *LiD*-based *AV*s lies in their susceptibility to different spoofing attacks. This attack diverts the *AV* system's perception for many reasons. This can lead to false perceptions of obstacles, inaccurate distance calculations, and disruptions in the navigation system. This spoofing poses safety risks; the *AV* may make incorrect decisions based on compromised sensor data, potentially resulting in accidents.

Cao et al. (2019) investigate the security of *LiD*-based imaging systems in *AV*s, specifically the susceptibility of such systems to spoofing attacks. The study demonstrates that indiscriminately applying *LiD* spoofing is insufficient owing to machine learning-based object identification procedures, and it is based on an investigation into strategically directed spoof attacks using optimization methodologies. The main drawback identified in this system is the inability to blindly apply *LiD* spoofing to achieve the goal of fooling the machine learning-based object detection process. This limitation prompts the need for a more sophisticated approach, leading to the exploration of strategically controlled spoofed attacks. Cao et al. (2023) proposed another scheme that focuses on a novel risk called Physical Removal Attacks (PRA), which use laser-based spoofing techniques to selectively remove authentic *LiD* point cloud data from obstacles, misleading *AV*s'. Assesses the influence of fusion models and driving decisions, indicating the essential need for improved defense tactics to counter such attacks. However, in this scheme, the vulnerability of PRA, in which laser-based spoofing techniques selectively remove actual *LiD* point cloud data

from obstacles. This vulnerability confuses *AV* obstacle sensors, causing them to fail to detect and identify obstacles accurately.

Sun et al. (2020a) analyze the vulnerability of *LiD*- perception based on *AV* systems for spoofing attacks. The study identifies that hidden occlusion patterns in *LiD* point cloud make them *AV*s vulnerable; the study offers the first black-box spoofing attack with a mean success rate of 80% in all target models. A defense method, CARLO, is suggested to use occlusion patterns as permanent characteristics to lower the average attack success rate. It also suggests SVF, a universal architecture for robust *LiD*-based detection, which reduces the average attack success rate. But in this scheme, an attacker can exploit neglected occlusion patterns in *LiD* point clouds by selectively transmitting laser pulses to the sensor, which enables successful black-box spoofing attacks. You et al. (2021) suggested a comprehensive approach called 3D Temporal Consistency Check (3D-TC2) that detects spoofing attacks by exploiting motion as a physical invariant. A rough prototype implementation shows promising performance with an overly high attack detection rate. However, 3D-TC2 may face challenges in scenarios where the motion of genuine objects is limited or restricted, and it could be influenced by various environmental factors, potentially impacting its robustness. However, the model may be less successful without detailed data on potential limitations, ecological dependencies, or conditions.

Alheeti et al. (2022) proposed a defensive approach that uses machine learning, primarily decision trees, to detect and prevent spoofing threats. The suggested approach effectively detects *LiD* spoofing attempts, improving the security of *AV* systems. The scheme may be less successful if detailed data is not provided. Chandalvala et al. suggested a data-hiding method that uses 3D Quantization Index Modulation (QIM) to protect raw data from *LiD*. Detects tampering in the *LiD* data and identifies the precise location that has been tampered with. The approach detects and localizes insider data-altering attempts, such as false target insertion (FTI) and valid target deletion (VTD). However, the scheme is an adverse response to a rapidly changing object or shape. Another scheme proposed by Cheng et al. (2020) for a semifragile data-hiding technique uses 3D quantization index modulation (QIM) for real-time integrity verification and tamper detection in *LiD* data. The method inserts a binary watermark in the sensing layer, enabling integrity verification and tamper detection at the decision-making unit. The scheme is complex and takes a long time to calculate FOI and TOD.

Jakobsen et al. (2023) explore the growing prevalence of fully *AV*s and the critical need for robust perception models that combine *LiD* camera data through multisensor fusion (MSF). The difficulty of ensuring dependability under unanticipated real-world conditions is highlighted, as is the rising security consideration related to potential sensor attacks. However, this scheme accepts the need for more robust defenses and an understanding of the complexity of attacks; greater complexity alone may not be adequate in the *AV* system. Jin et al. (2023) investigate the possibility of affecting *LiD*-based 3D object identification by adding adverse point clouds using lasers. They inject adverse point clouds with specified forms into the victim *LiD* by using a dedicated laser source. It explores four types of attacks: hiding, creating based on records, optimization-based hiding, and optimization-based creation.

Hallyburton et al. (2022) proposed a scheme in which the vulnerability of camera-*LiD* fusion in *AV*s to *LiD* spoofing attacks was discovered, discovering robustness against classic attacks while revealing a unique attack. This recently discovered attack is very successful across various perception algorithms and designs, showing its stealth and the ability to compromise the system *AV*'s tracking module over time. Mahima et al. (2023) explore the effect of class-wise point distribution on adversarial robustness, emphasizing the significant susceptibility of ground-level points to perturbation attacks. The examination of attack technique transferability reveals significant resistance in networks based on point data representation. It also improves the study of adversarial situations to *LiD*-based 3D semantic segmentation using

three *LiD* point-based adversarial attack methods on networks built using the SemanticKITTI dataset.

Tu et al. (2020) address the challenge of creating ubiquitous 3D-threatening objects that deceive *LiD* detectors. The approach is illustrated by placing an attacker object on the roof of a target car, which successfully conceals the vehicle from the *LiD* detectors. It covers attack findings for numerous detectors with different point cloud input representations. Abdelfattah et al. (2021) proposed a universal and physically realizable adversarial attack for several *LiD* camera model types and an analysis and comparison of their vulnerability to these attacks. The goal of installing a single hostile item with a distinguishing form and texture on an automobile is to enable it to elude detection. Based on the widely recognized KITTI benchmark, the adversarial object obtained a detection evasion rate.

Li et al. (2021c) present a *LiD* point cloud generated by moving vehicle trajectories that present privacy issues because of adversarial spoofing trajectories. These are vulnerable to wireless attacks and might leave safety-critical items undetected or incorrectly positioned for deep network perception. Liu and Park (2021) address the impact of perception error attacks (PEAs) *AV*s and introduce a countermeasure named LIFE (*LiD* and image data fusion for detecting perception errors). LIFE utilizes advanced machine learning and computer vision algorithms to analyze the consistency between camera image data and *LiD* data, providing a robust defense against PEA. Rieken and Maurer (2020) demonstrate an essential weakness in present *LiD*-based perception structures to show how neglecting occlusion and distance patterns in point clouds exposes *AV*s to black-box spoofing attacks. To address this weakness, they suggested SVF architecture shows promise in improving durability by significantly reducing the mean success rate of spoofing attacks.

The abovementioned schemes aim to detect and prevent spoofing attacks in the Lidar-based *AV* system. It is important to note that each technique is from a unique perspective rather than focusing solely on countering physical attacks on the *LiD* signal. This emphasizes the need for a comprehensive and multifaceted approach to address the diverse challenges of ensuring the security of *AV* systems. In this research, our novel approach involves conducting comprehensive security analyses specifically tailored for *LiD*-based schemes. The threat model encompasses various types of *LiD*-based active spoofing and jamming signals, including diverting signals, eavesdropping, bad data manipulation, and denial of service (DoS) attacks. Our scheme addresses spoofing-specific attacks such as reflection spoofing, replay spoofing, signal jammed spoofing, object mimicry spoofing, and false return spoofing. In the next section, the Internet of Vehicles will be discussed.

Motivation: *LiD* Point cloud is used mainly in many real-time applications of smart transportation systems, such as *AV*s, where accurate 3D mapping is created. For more secure communication, fast and accurate object detection is always needed due to quick-changing scenarios. If there is delay and latency in object detection, it can cause severe consequences in navigation failure and road accidents, directly affecting safety applications. To make *LiD* data trusted and secure, there is always a mechanism for detecting false objects and exploring hidden objects. In this research work, we have explored the specific attack scenario of spoofing an attack on the *LiD* point cloud data. The proposed technique works on the detection of spoofed objects that mislead the point cloud for incorrectly packaged and spoofed objects. It also proposed a mechanism for optimizing the selection of routes on real-time objects on the road side or passing over another *AV* in congested roadside traffic.

3. Internet of autonomous vehicles

Navigation on public roads involves dealing with various conditions and obstacles, including pedestrians, other vehicles, road rotation, traffic signals, bicycles, etc. To operate safely under such conditions, an *AV* must have human vision capabilities and be able to see obstacles

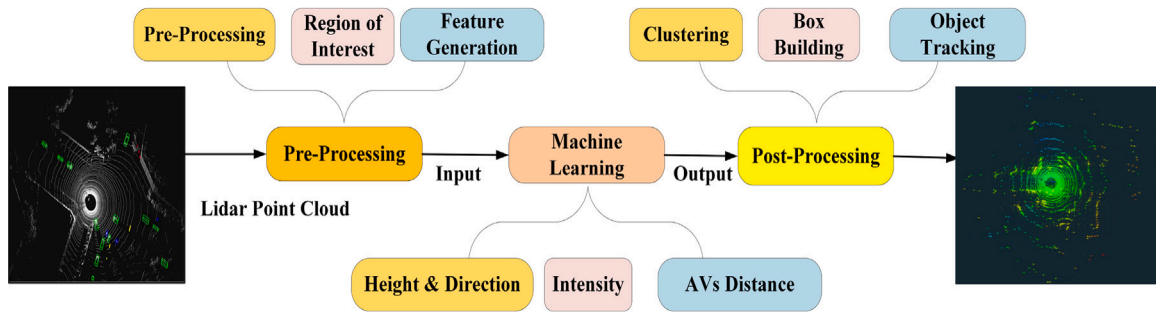


Fig. 2. LiDAR-based perception in Baidu Apollo.

Table 1
Symbol table.

Symbol	Meaning
θ	Angle of elevation
$\overline{Dis}$	Distance B/W objects
I_{oV}	Internet of vehicle
$V2V$	Vehicle to vehicle
O_{3b}	3D-object
O'_{3b}	Spoofed 3D-object
AV_n	Any autonomous vehicle
LiD_{sen}	LiDAR-Sensor
HT	Altitude
CAM_n	Camera
$3DX$	3D point cloud
$3DX'$	Adversal 3D point cloud
F_x, F_y, F_z	3D cartesian coordinate
M_{ch}	Machine learning model
AT_n	Any spoofing attack
X_{in}	Input matrix
X'_{in}	Adversal input matrix
$\Phi(n)$	Mapping function from 3D to 2D
H_{max}	Maximum height of O_{3b}
H_{avg}	Average height of O_{3b}
I_{max}	Maximum intensity of O_{3b}
I_{avg}	Average intensity of O_{3b}
DR_{3b}	Direction of O_{3b}
X_{Fx}	Input feature matrix
X'_{Fx}	Spoofed input feature matrix
N_{pt}	No of point in cell/ROI
N'_{pt}	Spoofed no of point in cell

on the road. Having these vehicles to check lanes and obstacles on the road is a big challenge for the *AV* industry. Researchers have addressed this challenge by combining multiple sensor technologies to produce detection systems that work like human vision and even far exceed it.

The model used LiD_{sen} for the acquisition and navigation of data on any map is summarized in Fig. 2 and is based on Baidu Apollo (Zhang et al., 2020a; Jeong and Choi, 2024). In the preprocessing stage, the unfiltered LiD data in the point cloud are converted to absolute coordinates. Then, using HDM_{ap} data to apply a region of interest (ROI) filter, creating a feature matrix " X_{max} " ($8 \times 512 \times 512$), mapping the filtered 3D point cloud within a given range to 512×512 cells, and extracting 8 features per cell to feed into the machine learning model. In the machine learning phase, a deep neural network (DNN) (Ravindran et al., 2020; Li et al., 2021b) receives the feature matrix " X_{max} " as input and produces several output metrics for each cell, including the probability that each cell will be an obstacle. In the post-processing phase of the connected network, the clustering method identifies cells whose abjectness values are more significant than a predetermined threshold (0.5 by default). Following a 0.1 average positive value threshold filter, the tracker integrates successive frames to produce a perception output LiD that includes tracked obstacles and additional speed and acceleration, and the builder reconstructs the boundary boxes of $3DX$. The Apollo system makes driving decisions using data on perceived obstacles, such as their locations, shapes, and types (Feng

and Zhang, 2022; Fan et al., 2018). The planning module creates future driving paths and actions, including stopping, changing lanes, and turning, after additional processing of the perceptual output to estimate future trajectories of detected obstacles. The different symbols used in this article and their relevant meanings are shown in Table 1.

4. Threat model for spoofing attacks

Consider a scenario in which an object *AV* collects data from LiD_{sen} for object detection and mapping as it moves along the roadside. LiD_{sen} emits laser beams that interact with surrounding objects. The laser light is transmitted and subsequently reflects off surfaces, creating a detailed point cloud representation of the environment, as shown in Fig. 3. The point cloud data is then processed and used for different actions by the system. Point Cloud serves as a comprehensive map, capturing the spatial information of objects in the vehicle's vicinity to determine the location, shape, and movement of various objects in the environment. To analyze and check the contents of these data packets, an *AV* can identify roadside obstacles, pedestrians, and other vehicles on the road, determine their exact positions, and anticipate their movements. All this happens in real time, and using this data, *AV* makes informed decisions about its route, speed, and overall trajectory, ensuring a safe and efficient journey. The following are some of the attacks that may occur in systems based on LiD_{sen} :

4.1. Attack scenario

Often, LiD -based attacks manipulate or deceive LiD_{sen} by introducing false or misleading data. This can happen by confusing the LiD system's perception of the environment and causing it to misinterpret the surroundings. In executing an attack (AT_n), various scenarios may be considered based on the specific objectives of the attacker. In these scenarios, the attacker aims to achieve control by deploying a diversion or jamming the laser beam. The attacker launches an object on the premise of an attempt AV_n to incorrectly position O_{3b} and divert its location. Any location may be carefully chosen to target areas such as pedestrian or human crossings and intersections, where the trajectory would be most significant AV_n , and the data captured on the top or front view is distorted. The transmitter differentiates echoes from other incoming signals using a specific waveform. This implies that the attacker must first collect the ping waveform to launch the attack. The attacker may now attack by sending the signal back to the victim's LiD after obtaining the waveform of the sensor because the victim vehicle finds it difficult to differentiate between real and fake signals (Cao et al., 2019; Petit et al., 2015).

4.2. Spoofing by reply attack

The attacker can launch a device that can do many things, such as absorb the signal, broadcast a stronger beam of laser signals, divert the signal, and delay the signal when an attacker introduces a device equipped with a photodiode, a delay module, and a laser source, as

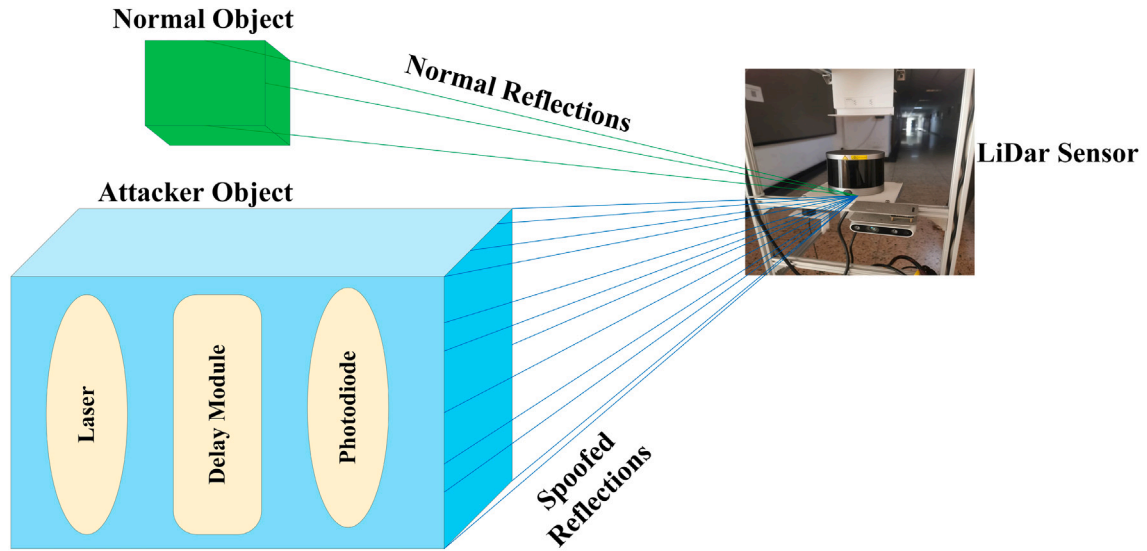


Fig. 3. LiDAR with an Attacker device & Normal device reflections.

shown in Fig. 3. In this diagram, a LiD_{sen} broadcasts a laser beam into the surroundings, and the reflection back of this light creates 3D maps at $3DX$. The attacker device has three main modules: a photodiode, a delay module, and a laser source. Here is how these components might work. A photodiode is a light-sensitive device that can detect incoming LiD signals from objects and their surroundings (Cao et al., 2019; Jin et al., 2024). Here, a photodiode will capture the legitimate LiD signals. The delay module adds a temporal delay to the captured signals. By doing so, the attacker can manipulate the timing of the signals before retransmitting them. The laser source is used to generate laser signals that mimic legitimate LiD signals. These signals, which are delayed by the delay module, are then emitted back into the environment by laser. As the reflected light at the cloud point calculates the distance, the signal delay marks the object away from it LiD . The delay points the objects away from their original position, and the LiD system maps them somewhere else from their original position. This spoof attack might trick them LiD_{sen} into detecting reflections from original objects to an imaginary or nonexistent object or confuse the timing and position of observed items. A spoofed reply attack can mislead LiD_{sen} by generating fake obstacles, manipulating distance estimates, or interfering with the accuracy of environmental mapping (Guesmi and Shafique, 2024).

4.3. Spoofing by absorbing all signals

An attacker device can absorb or ingest all signals and create vacant spaces in the vicinity to confuse or mislead the actual objects. This can happen by selectively blocking or modifying the signals detected by the LiD . It may eliminate the reflection of laser signals sent out by the LiD . This type of interference can be part of a spoofing attack aimed at disrupting the accurate perception of the environment by the LiD system (Hu et al., 2024). Signs are absorbed using materials or coatings that absorb or scatter the laser signals, preventing them from reaching the intended places. By intentionally absorbing LiD signals, the attacker generates places where the sensor detects insufficient reflections, resulting in misleading blank spaces or blind spots in the LiD data. The LiD_{sen} may misinterpret the absence of reflections as wide areas or nonexistent objects, potentially leading to navigation problems in applications such as in our case of AV_n (Khan et al., 2024).

4.4. Spoofing by tempering the signals

Signal tampering involves altering the properties of LiD signals to mislead or affect the LiD_{sen} 's perception of their surroundings.

Tampering may involve changing the angle of elevation, intensity, and direction to alter the speed of the object. Tampering can create virtual obstacles or objects in LiD data that do not exist in the real world. Hiding or reducing the view of actual objects results in blind spots or lapses in LiD perception (Li et al., 2021c; Dasgupta et al., 2025).

4.5. Spoofing by jamming signals

Jamming in LiD signals refers to deliberate attempts to interrupt the system, whether with the attacker's intention or accidentally by other LiD systems working concurrently. This purposeful interference poses significant risks, particularly in applications like AV , where accurate and reliable LiD data is critical for navigation and obstacle recognition (Rigó et al., 2024). This process creates electromagnetic signals or interference in the same band of frequencies as the LiD system. This may disrupt the consistent transmission and reception of laser pulses, causing inaccurate distance measurements and the development of incorrect maps. Objects partially or entirely hidden by occluding components may not be correctly detected, compromising the safety and reliability of applications such as AV_s (Hu et al., 2024).

4.6. Occlusion of signals

Occlusion happens when objects or obstacles restrict the LiD_{sen} 's line of sight to the target surface. It prevents them LiD from immediately "seeing" or identifying surfaces hidden by other objects. As a result, they can provide incomplete maps of the surroundings, with information hidden behind occluding obstacles (Usmani et al., 2022). The occluded locations can produce shadows in the LiD data, resulting in inaccurate representations of the environment in $3DX$. These shadows may cause gaps or lower point density in the LiD point cloud, affecting the accuracy and authenticity of the acquired 3D map (Schneider et al., 2010).

4.7. Saturation of signal attack

Using a high-intensity signal to drive a sensor — like a LiD_{sen} — beyond its upper detection threshold is known as a saturation attack. This unexpectedly causes a denial-of-service (DoS) problem by making the sensor unable to reflect the changes in the input signal accurately. Because it uses light as a medium to overwhelm the sensor, this type of attack is also known as a blinding attack when it comes to LiD . Saturation attacks are effective because they are difficult to avoid and

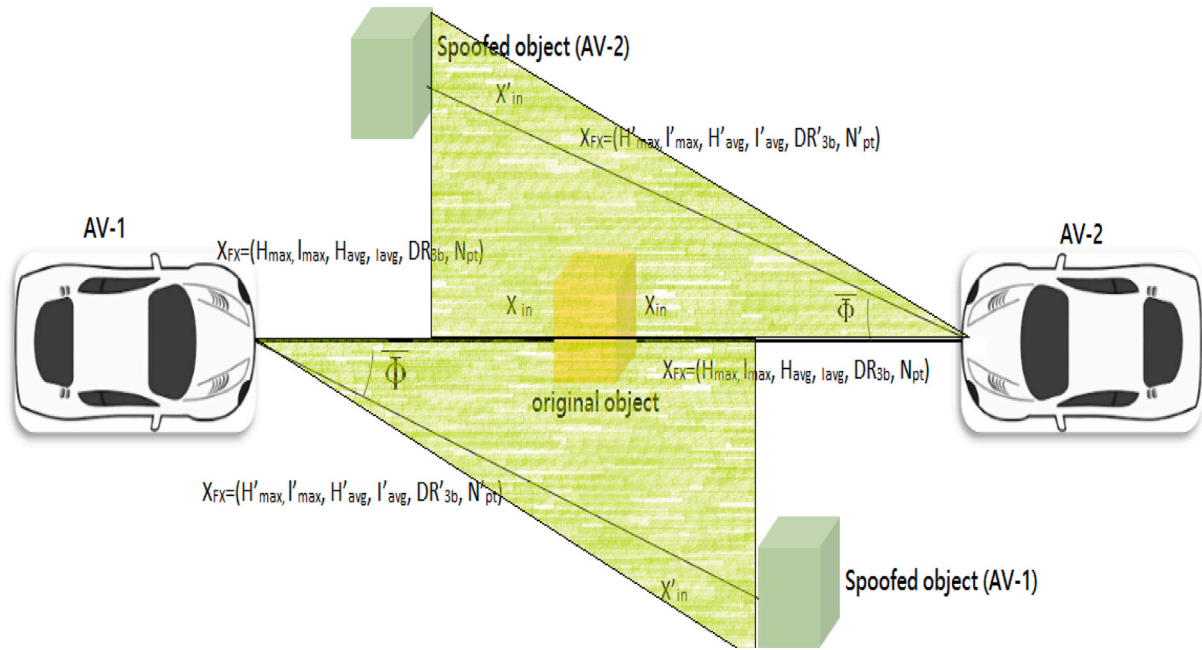


Fig. 4. LiDAR data with an original & spoofed object with two AVs.

can be challenging to prevent when detected. Since *LiD* works in the safe wavelength of infrared light in the eyes, human drivers and pedestrians may not be aware of such attacks (Shin et al., 2017).

5. Impact of the spoofing attacks

These attacks change the object's orientation, size, distance, speed, and intensity. These parameters confuse the system in creating a clear perception of 3D modeling and can cause serious damage to AV systems. The following are the main properties that have changed due to the above attacks:

5.1. Change the distance of the object

In the replay spoofing attack, the attacker device reflects the same light with a delay in return, which causes the mapping of the observed object to increase in distance. This process involves altering the perceived range or proximity of the object detected by the system. As mentioned, the time it takes to emit laser beams and measure their return after hitting objects provides accurate distance measurements. The delay or false reflections of the signal can mislead autonomous systems relying on cloud points for environmental perception. These adjustments may result in incorrect object location estimations, which might risk user safety in applications such as AV_n .

5.2. Change the altitude of the object

In altitude spoofing, the altitude of an object is altered from its original to a spoofed position, which refers to manipulating the object's perceived height or vertical location as detected by the sensor. When calculating the altitude of an object, the LiDAR produces laser beams and monitors how long it takes for the beams to return after striking objects. An attacker can trick the LiDAR system into thinking that the object is at a different height than it is by changing the latency or timing of these signals. This manipulation may be used for various objectives, including escaping detection, creating an incorrect mapping of the surroundings, and injecting errors into the system's view of the environment.

5.3. Object hiding

Hiding objects AVs is more dangerous in spoofing attacks due to its potential consequences because detecting a spoofed object may make AVs come to a complete stop. The failure to detect a real object poses a greater risk, significantly increasing the probability of a fatal collision. The perception of 3DX is treated as if there is no object, while there is a real object. The attacker follows such a mechanism that all laser beams are absorbed in the surface, and this absorption causes no reflection. The object is then invisible, and it causes serious consequences. In these attacks, the vehicle's sensors are manipulated to either misinterpret or entirely miss crucial objects in the surroundings. As a result, they AV may not be aware of the presence of obstacles, pedestrians, or others AVs, increasing the chances of a collision or other safety-critical incidents. Unlike spoofing attacks, which involve presenting false information to the target LiD_{sen} , object-hiding attacks directly compromise the AV ability to perceive and respond to its environment accurately, making them potentially more dangerous in real-world driving scenarios.

5.4. Change the intensity of the signals

Abrupt changes in intensity can play a vital role in object detection and environmental perception. Intensity is used mainly to distinguish between different materials and surfaces. Any abrupt changes may lead to misinterpretations, affecting the accuracy of object detection and mapping at 3DX. It can also interrupt the categorization process, compromising the ability of AVs to recognize and categorize objects in their surroundings efficiently. As a result, AV's capacity to make judgments based on accurate sensor data may be compromised.

5.5. Change the direction of an object

The LiD_{sen} uses laser beam reflections to evaluate an object's position and mobility. If the direction of a moving object changes abruptly, *LiD* may have issues effectively tracking the object's trajectory and predicting its future path. This can lead to mistakes in the recognition of the dynamic environment AV's, which limits its ability to make precise decisions about navigation.

6. Problem definition

Data LiD_{sen} are collected 3DX with original object detection and spoofed object detection. The AV system marks both spaces as objects; one is near, and the other is far from the point of observation. At the same time, other AV s are also on the premises, and the same object is observed at the original and another location. The original matrix has x_{in} values, while the spoofed object is x'_{in} the input matrix AV_1 such that the same AV_2 marks the original matrix, x_{in} and the spoofed object is another location with x'_{in} values. For both AV s, the original points remain the same, while the spoofed points are marked on two separate plates. From this, they 3DX mapped the original object as a legitimate point and marked it as the original object. After finding the original and spoofed object points 3DX, we can apply different models to map and navigate the whole scenario with original and spoofed objects. This scenario is mapped in Fig. 4.

From the above spoofing attacks and their effect on the overall environment, we can formulate the problem of any AT_n by representing some mathematical notation. The machine learning models that are more effective and efficient in obtaining any O_{3b} object mapping and modeling 3DX are mentioned in Xiao et al. (2018b,a) and Cheng et al. (2020), and we also optimized them for our proposed strategy.

$$LiD_n(X_{in} \oplus X'_{in}; M_{ch}) \quad X'_{in} \in \Phi(3DX'[3DX' \in AT_n] \& X_{in} = \Phi X_{in}) \quad (1)$$

where $LiD_n(M_{ch})$ is the actual attack LiD_{sensor} X_{in} is an input matrix, X'_{in} is an adverse input matrix, M_{ch} is machine learning (DNN), or AT_n is a spoofing attack. Other notations have already been explained in Table 1. After launching any of the adversaries AT_n explained above, we can formulate any of the above adversaries in the form of the equation. The difference between O_{3b} and O'_{3b} should be identified, as should the mapping of these objects on a 3DX. Using the merging function to compare these objects 3DX, the objects are first analyzed with the input matrix X_{in} . The $\Theta(n)$ extracts the preprocessing values from the matrix X_{in} in 3DX. This process includes three sub-processes. First, coordinate the transformation of the image O_{3b} , then filter the region of interest (ROI), then filter it, and finally, extract the input feature matrix. The first two steps have a minor impact on SDX' , while the coordinate transformation step has no effect since it transforms 3DX' along with 3DX. Only ROI the filtering step was used; it excludes 3D point cloud elements situated outside the road when viewed from above.

All other parameters for extracting the model are H_{avg} , I_{avg} , H_{max} , I_{max} and DR_{3b} . They X'_{in} are combined by an operation $\oplus$ to compare with X_{in} . Some parameters, such as direction and distance, are fixed before applying these values. We can obtain, see in Eq. (2):

$$x'_{in} = x_{in} \oplus X_{FX} = \begin{bmatrix} N_{pt} + N'_{pt} \\ (H_{avg} \cdot N_{pt} + H_{avg} \cdot N'_{pt}) / N_{pt} + N'_{pt} \\ \text{Max}(H_{max}, H'_{max}) \\ (I_{avg} \cdot N_{pt} + I'_{avg} \cdot N'_{pt}) / N_{pt} + N'_{pt} \\ \Sigma I_{max} \cdot 1(H_{max} = \text{max}(H_{max}, H'_{max})) \end{bmatrix} \quad (2)$$

Now, in this stage, the legitimate and spoofed points in the LiD data are found, and the real and spoofed objects are differentiated with clear dimensions. The algorithm 1 is used to launch $ATT_{spoofed}$ in LiD_{sen} to successfully compromise the system and change the perception of the system in 3DX.

7. Optimal path selection for collision avoidance

After extracting the original points for object creation, with its inherent features like N_{pt} , H_{avg} , H_{max} , I_{avg} , I_{max} and DR_{3b} for comparison with the spoofed object at 3DX. They are compared with AV_1 values for fake objects like N'_{pt} , H'_{avg} , H'_{max} , I'_{avg} , I'_{max} and DR'_{3b} . The 3D map

Algorithm 1 Adversarial Attack on AV s

- 1: Assume the presence of an attacker AT_{AV} aiming to manipulate AV s' perception. AV_i in AV s from i to j
- 2: Collect data X_{in} in LiD_{sen} and CAM_i for AV_i .
- 3: Apply the perception model M_{ch} to get the initial perception $P_{initial}$ for AV_{i-j} .
Adversarial parameter change in height, shape, speed, intensity, and direction
- 4: Generate adversarial inputs:
 - Change height: H'_{avg} , H'_{max} .
 - Alter shape: Modify the 3D object O_{3b} shape.
 - Adjust speed: V_{AV_i} .
 - Modify direction: DR_{AV_i} .
- 5: Formulate an adversarial input matrix X'_{in} based on the changes.
- 6: Apply the adversarial input X'_{in} to the perception model M_{ch} for AV_i .
- 7: Obtain the adversarial perception P_{adv} for AV_i .
- 8: Evaluate the impact of the adversarial changes on AV_i 's perception.
- 9: Compare P_{adv} with $P_{initial}$ for AV_i and assess the success of the attack.

of the scenario 3DX clearly shows the original and spoofed objects. It is necessary to avoid the original object and others AV s and to follow a safe route for each AV . To optimize the process of avoiding obstacles AV s on the road, the Frenet frame (Li et al., 2022; Huang et al., 2023; Li and Zhang, 2020) is used. This focuses on the formulation with a calculated path boundary function L_p . The Frenet frame is a coordinate system commonly used in extracting the parameters for AV s motion, especially in the context of trajectory planning and optimization. It is a coordinate system that describes the position of a point such as (AV s) in terms of its longitudinal position along a reference path, its lateral position perpendicular to the reference path, and its orientation angle. This frame is particularly useful for describing the motion of vehicles along a curved path.

$$\begin{aligned} f(L_p(sp)) &= v_{L_p} * \int L(sp)^2 d(sp) + v_{L_{p'}} * \int L'(sp)^2 d(sp) + v_{L_{p''}} \\ &* \int L''(sp)^2 d(sp) + v_{L_{p'''}} \\ &* \int L'''(sp)^2 d(sp) + v_{obs} * \int L(sp) - 0.5 \\ &* (L_p(sp)_{min} + (L_p(sp)_{max}))^2 d(sp) \end{aligned} \quad (3)$$

This equation is necessary to satisfy the constraints:

$$L_{sp} \in L_p(sp),$$

forall $sp \in [0, sp_{max}]$. We employ a strategy that divides the path into segments to efficiently develop and solve an optimization issue while evaluating if specific requirements are satisfied in actual settings. To do this, the path function L_p is divided into discrete points depending on the spatial parameter sp and a certain degree of detail Δ (SP). These locations allow us to adjust the form of the path and approximately judge if the requirements are met (Zhang et al., 2020a, 2019). The main objective is to reduce the one-dimensional function to the level of its second-order derivative. We then employ constant third-order derivative terms to connect discrete positions efficiently. The discrete path function L_p with the derivative values can be calculated by changing from point to point concerning sp , as shown in Table 2. These points control how AV can move and avoid obstacles or objects in its lane on the road.

Between each pair of consecutive points, a constant third-order term L'''_p is used to connect them. This can be calculated in order of L_p as:

$$L'''_{i \rightarrow i+1} = (L''_{i+1} - L''_i) / \Delta sp \quad (4)$$

Table 2

Table for different points.

Initial	First	2nd	n-1	n+1
L_0	L_1	L_2	L_{n-1}	L_{n+1}
L'_0	L'_1	L'_2	L'_{n-1}	L'_{n+1}
L''_0	L''_1	L''_2	L''_{n-1}	L''_{n+1}
L'''_0	L'''_1	L'''_2	L'''_{n-1}	L'''_{n+1}

Some extra points will be needed for the connected path from 1st and 2nd-order derivatives in between, i and $i+1$; it can be expressed as:

$$L'_{i+1} = L'_i + \int_0^{sp} L'''_{i \rightarrow i+1} d(sp) = (L'_i + L'''_{i \rightarrow i+1}) * \Delta sp \quad (5)$$

$$L'_{i+1} = L'_i + \int_0^{sp} L''(sp) d(sp) = L'_i + L'_i * \Delta sp + 1/2 * L'''_{i \rightarrow i+1} d(sp)^2 \quad (6)$$

$$L_{i+1} = L_i + \int_0^{sp} L'(sp) d(sp) \quad (7)$$

$$L_{i+1} = L_i + L'_i * \Delta sp + 1/2 * L''_i * (\Delta sp)^2 + 1/6 * L'''_{i \rightarrow i+1} * (\Delta sp)^3 \quad (8)$$

To ensure the complete path between all these objects and between AVs, we can find out the values of path optimization while L_i , L'_i and $L'''_i \in [0, n+1]$. They ensure the path optimization constraints like no collision and other safety precautions.

$$\begin{aligned} \hat{f}(L(sp)) &= V_{LP} * \sum_{i=1}^{n+1} L_i^2 + V'_{LP} * \sum_{i=1}^{n+1} L_i'^2 + V''_{LP} * \sum_{i=1}^{n+1} L_i''^2 + V'''_{LP} \\ &* \sum_{i=1}^{n+1} ((L''_{i+1} - L''_i) / \Delta sp) \\ &V_{obs} * \sum_{i=1}^{n+1} (L_i - 0.5 * (L_{min} + L_{max}))^2 \end{aligned} \quad (9)$$

Kinematic feasibility (Polack et al., 2017; Cui et al., 2020) refers to whether a motion or trajectory follows the physical limits and limitations of the kinematics of a system. Kinematics explains an object's motion without considering the forces that create it. It includes characteristics such as location, velocity, and acceleration. It guarantees that the intended motion or trajectory is consistent with the mechanical design, joint restrictions, and other kinematic constraints of AVs. It analyzes whether a proposed motion is physically viable for a particular system while adhering to its inherent restrictions. The frame conversion equations determine the curvature of a single point in a route as the following equation:

$$C = \frac{(L'' + (\dot{C}_{rL} + C_{rL}'') \tan \Delta \theta) \cos^2 \Delta \theta}{(1 - C_{rL}) + \frac{C_r}{\cos \Delta \theta (1 - C_{rL})}} \quad (10)$$

C_r and C'_r are the curvatures, and $\Delta \theta$ is the angle difference for AV, the front direction, and the direction of movement at the point r . After applying the optimization process, both AV_1 and AV_2 follow a path that not only escapes the real objects on the way but also each other on the safe side, as shown in Figs. 5, 6. In which both AV_1 and AV_2 change their position concerning 3DX, and at each value of L_n , the value is mapped in the 3D-map.

Throughout the process, from data collection to processing and decision-making regarding potential adversaries, an algorithm is proposed 2. This algorithm systematically guides LiD_{sen} in collecting data, redirects them to authentic and spoofed objects, and uses various models for perception and navigation. Instructs the system on how to detect and respond to possible threats. It also provides a systematic framework to maintain the accuracy of the data and the reliability of perception based on LiD in AVs.

Algorithm 2 LiD_{sen} Data Processing Algorithm

- 1: Collect LiD_{sen} data at 3DX with original and spoofed object detection
- 2: AV system marks both spaces as objects: one near and one far from 3DX.
- 3: AVs are present on the premises: $\forall AV_i$ to AV_j . X_{in} in the range $[0, 1]$
- 4: The original matrix is X_{in} values Spoofed object is the X'_{in} in AV_1 AV_2 , original matrix is X_{in} and spoofed is at another location with X'_{in} values
- 5: 3DX maps the original object as a legitimate point.
- 6: Find original and spoofed object points at 3DX.
- 7: Apply different models to map and navigate the scenario with original and spoofed objects.
- 8: Formulate the problem, of any AT_n : $LiD_n(X_{in} \oplus X'_{in}; M_{ch})X'_{in} \in \Phi(3DX'[3DX] \in AT_n) \wedge X_{in} = \Phi X_{in}$
- 9: Launch AT_n to formulate adversaries in equation form.
- 10: Identify the difference between O_{3b} and O'_{3b} and map these objects on 3DX.
- 11: Use a merging function to compare objects at 3DX with the input matrix X_{in} .
- 12: Extract pre-processing values from the matrix X_{in} at 3DX using $\Phi(n)$:
 1. $O_{3b}(F_x, F_y, F_z)$: Coordinates
 2. Region of interest (ROI) filtering.
 3. Input feature matrix extraction X_{in} .
- 13: Minor impact on 3DX' for the first two steps; no effect on the coordinate transformation step.
- 14: ROI Filtering excludes 3D point cloud elements outside the road when viewed from above.
- 15: Extract the model parameters: H_{avg} , I_{avg} , H_{max} , I_{max} , and DR_{3b} .
- 16: Combine X'_{in} using the operation $\oplus$ for comparison with X_{in} :

$$x'_{in} = x_{in} \oplus X_{Fx} = \begin{bmatrix} N_{pt} + N'_{pt} \frac{H_{avg} \cdot N_{pt} + H'_{avg} \cdot N'_{pt}}{N_{pt} + N'_{pt}} \\ \max(H_{max}, H'_{max}) \frac{I_{avg} \cdot N_{pt} + I'_{avg} \cdot N'_{pt}}{N_{pt} + N'_{pt}} \\ \sum I_{mx} \cdot \mathbb{I}\{H_{mx} = \max(H_{mx}, H'_{mx})\} \end{bmatrix}$$
- 17: Find legitimate and spoofed points in the LiD data and differentiate between real and spoofed objects.

8. Evaluation of the system

The proposed approach is likely to be recommended to mitigate spoofing attacks on the LiD_{sen} . The scheme is tested with some basic parameters to check its applicability in real-time AVs systems. The scenario has been developed in CARLA (Dosovitskiy et al., 2017; Deschaud, 2021) and tested for different parameters. These parameters are well known in the simulations AVs and are constantly checked for system navigation and 3D mapping. Table 3 mentions the simulation parameters, meaning, and the values concerned.

8.1. True positive and true negative rate

The proposed mechanism effectively recognizes fake objects on the roadside or along the road AVs. The system achieves a success rate of up to 94.57% through repeated experimentation. This indicates the system's ability to differentiate between actual and fake objects 3DX, demonstrating its good performance and dependability in situations involving AVs navigating highways. In Fig. 7, false positive and false negative values are assigned and mapped when there are one AV,

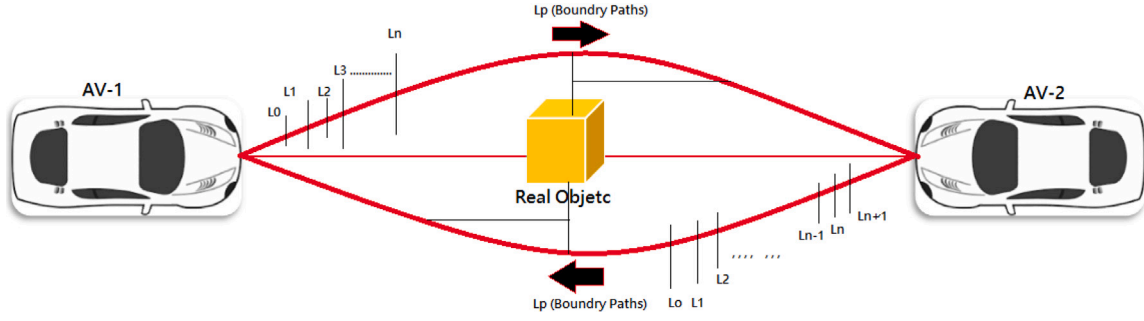


Fig. 5. Optimized path selection for two AVs with avoiding the object on the way.

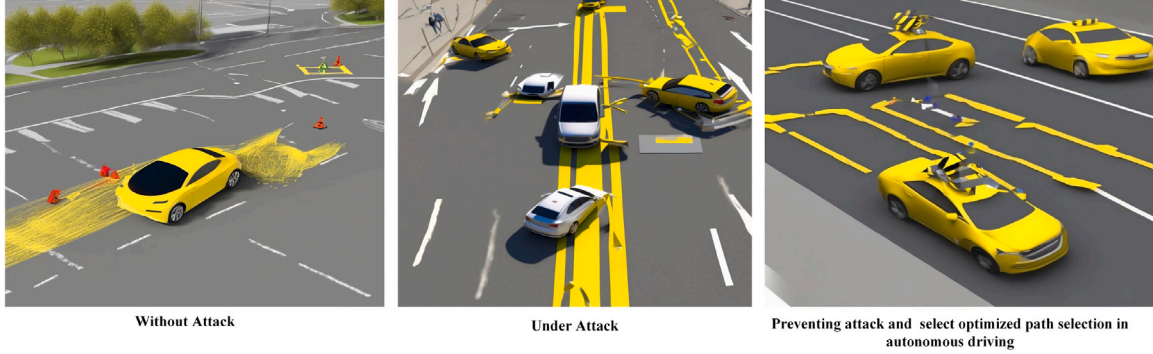


Fig. 6. Optimized path selection for AVs.

Table 3
Simulations parameters.

Parameters	Symbols	Values/Units
Laser wavelength	λ	1550 nm
Attenuation	α	0.567 dB/km
Launch power value	ρ	8 dBm
Maximum range	R_{mx}	50 m
Minimum range	R_{mn}	1, 1.5, 3 m
Pulse shape	SH	RRC
Non-linear coefficient	γ	1.45 1/W/km
Modulation	MD	16.8 QAM
Max. & Min. horizontal angles	θ	180, -180 degrees
Resolution (H)	R_N	0.17 degree
Horizontal divergence	H_d	0.334 rad
Vertical divergence	V_d	0.0072 rad
Signal cutoff	S_{CT}	1.22 m
Max. & Min. vertical angles	θ	11.4, -30.6
Polarization	P_n	dual
Diameter of receiver	D_m	40 cm

two AVs, and three AVs experiments. In this figure, the evaluation of two detection techniques involves examining the receiver operating characteristic (ROC) curves during the detection phase, especially in scenarios where there are one, two, and three AVs attackers. ROC Curves are visual representations of the trade-off between true positive rates (detection > 90%) and false positive rates (detection > 90%), showing the performance of the schemes across various threshold values. However, in the one-AV scenario, the detection rate is low and increases with increasing numbers of AVs because the system better navigates the perception at 3DX with a larger number of LiD_{sen} . After a series of experiments with a repeatability rate of 10, we have found an average of all of these experiments and mapped these values in Fig. 8. Performance evaluation is further quantified using the area under-curve (AUC), a valuable tool to measure the overall effectiveness of object detection techniques. This complete evaluation provides its ability to detect fake objects and how they respond to changing numbers of

attacks AVs. It also includes information about their stability on the same path and its effect on irregular objects.

8.2. Average precision (AP) and intersection over union (IoU) and recall in detecting spoofed objects

These parameters are used 3DX in the collected data for accurate object detection and combinations of different frames. The ability of AP to detect false objects is evaluated using several scenarios involving different numbers of AVs. The average precision data gives a thorough assessment of the detection system's performance, taking into account both accuracy and recall. All these parameters test the system's ability to maintain accurate and reliable detection capabilities. In Fig. 9, three scenarios are mapped to verify the precision accuracy of the data in 3DX, and these values vary from scenario to scenario. In one-AV, precision is 0.85, in two-AVs, the value is about 0.92, and in three-AVs, the bar hits 0.95. This means that these values gradually increase. The red line in the figure is the average of all these values, and it hits 0.95, proving the effectiveness of the proposed techniques.

IoU value is also an important metric for assessing segmentation models since it extracts the model of an object from other objects in the same frame. In the mathematical expressions, we quantify the intersection between the ground-truth real object and the predicted or fake object. This can mathematically be represented in our case as:

$$IoU = (|O_{3b-1} \cap O_{3b-2}|) / |O_{3b-1} \cup O_{3b-2}| \quad (11)$$

This equation can also be written for binary values as:

$$IoU = (TP) / (TP + FN + FP) \quad (12)$$

For detecting the rate of an object, we have mapped the three experiments in Fig. 10. In essence, the values IoU are a quantitative measure of the spatial agreement between the expected and ground-truth bounding boxes, which helps in evaluating object identification performance. A high IoU of 0.96 indicates a precise match between the fake and real bounding boxes, implying accurate detection. A different

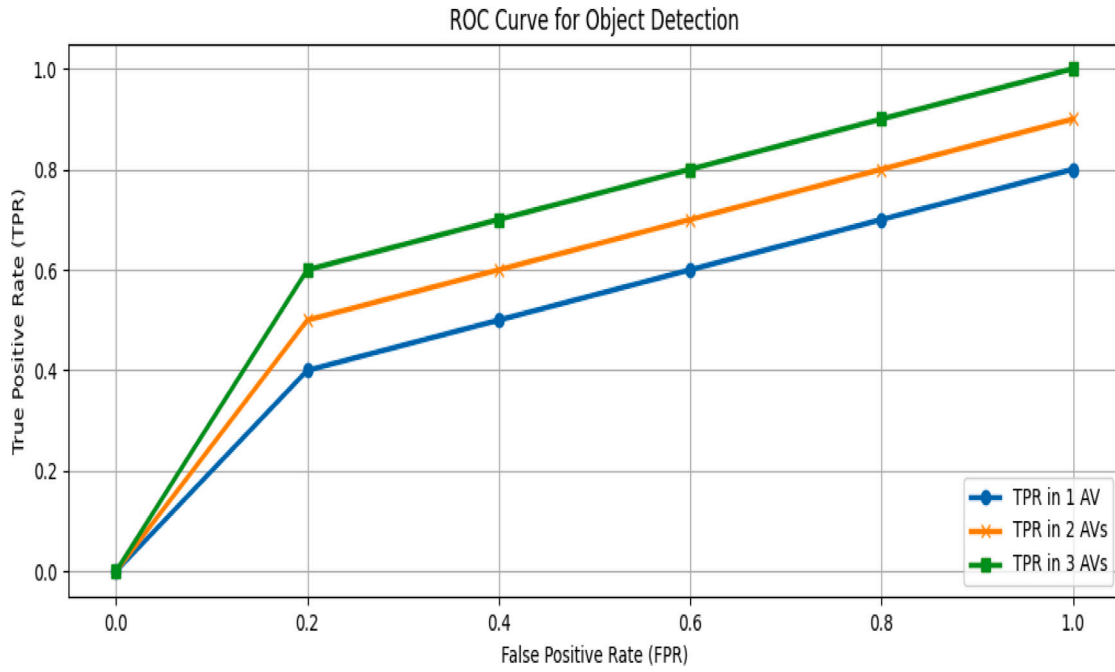


Fig. 7. Detection rate of the spoofed object in the presence of 1 AV, 2 AVs, & 3 AVs.

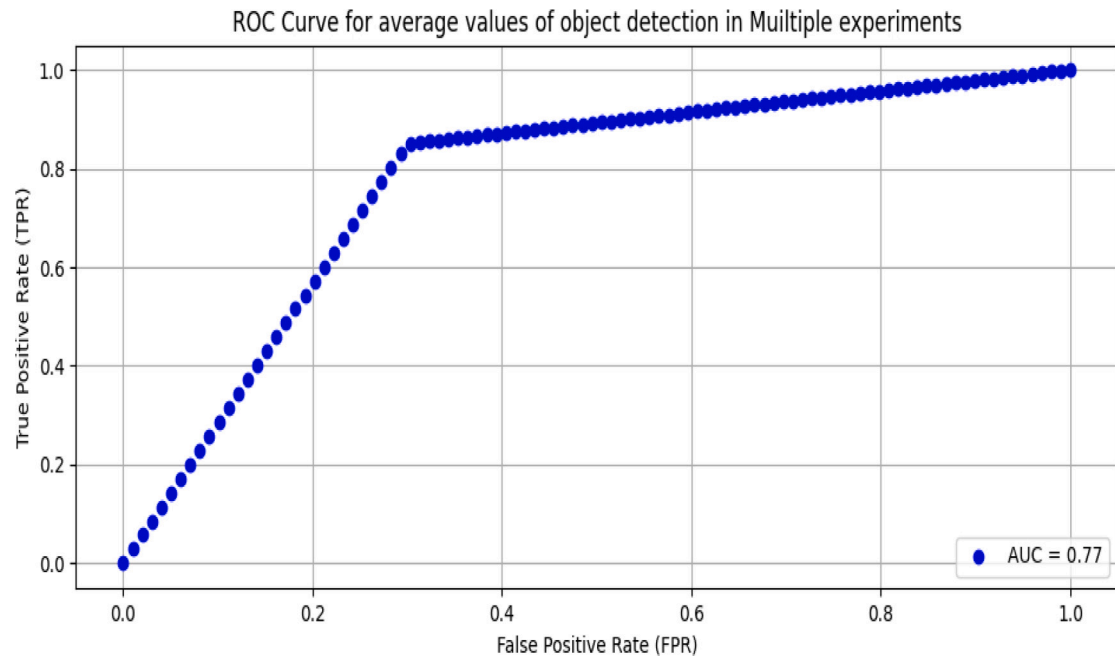


Fig. 8. Average detection rate after applying the same experiment with 10 repeatability.

object with an IoU of 0.74 shows significant but not complete overlap, indicating good but somewhat less precise identification. However, an IoU of 0.43 suggests a lower degree of position, indicating that this item may be detected less accurately.

Check the IoU values for both regular and irregular objects that are positioned in front of an experiment AV. Different numbers of AVs are deployed in the same scenario, and the values of IoU are measured. The results, as shown in Fig. 11, showed a noteworthy trend: As the number of AVs increases, the corresponding values of IoU decrease. These values suggest that the spatial alignment or overlap between the predicted and ground-truth bounding boxes is minimized with the

fake presence of an object. The minimum value challenges accurately detecting objects in scenarios involving multiple AVs.

Fixing the threshold IoU for different objects and finding the performance detection rate for cyclists and pedestrians, AVs was evaluated. The graphs showing the values of IoU and the recall rates for each category show the behavior in each case. For pedestrian identification, the scenario $IoU = 0.5$ showed that recall levels changed with distance (0, 50, 100, and 200 points). In particular, the recall values depended on the number of recorded points, suggesting that the degree of detail collected by LiD_{sen} might impact the detection mode's performance. In a parallel analysis, cyclist detection scenarios with $IoU = 0.7$ evaluate the effect of distance and $3DX$ on recall. Original recall patterns were

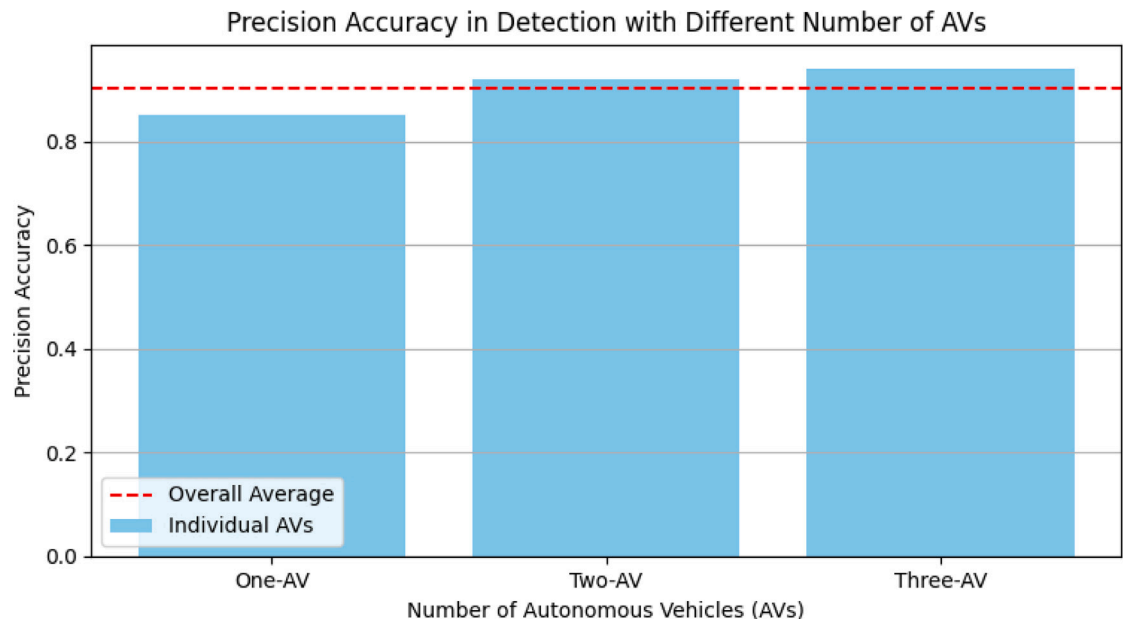


Fig. 9. Average precision in detection of fake objects with different numbers of AVs.

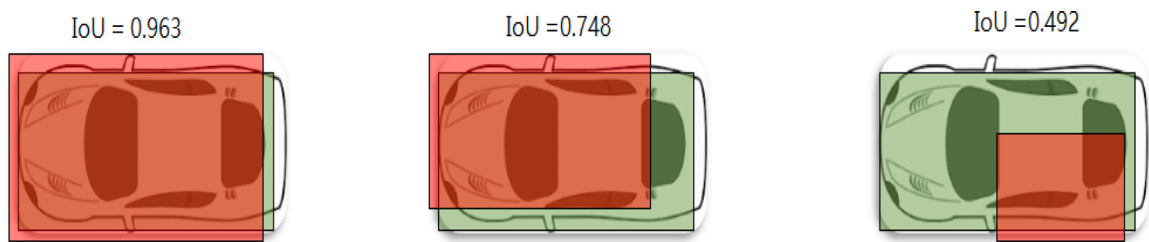


Fig. 10. IoU values for detection rate at three case.

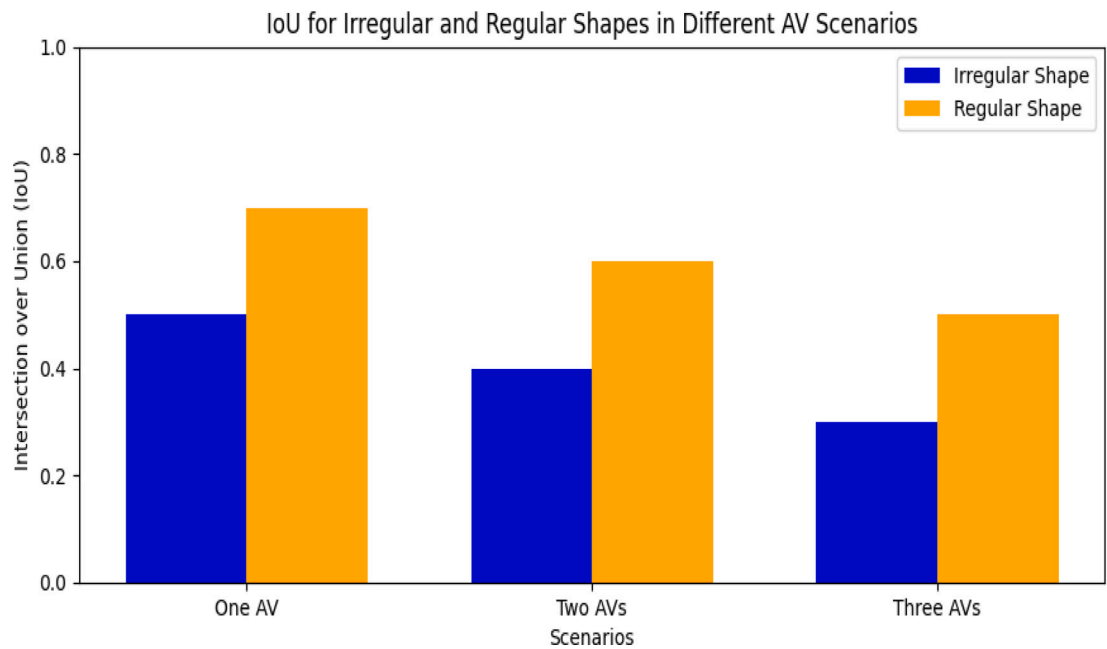


Fig. 11. IoU for Regular & Irregular shapes in different numbers of AVs.

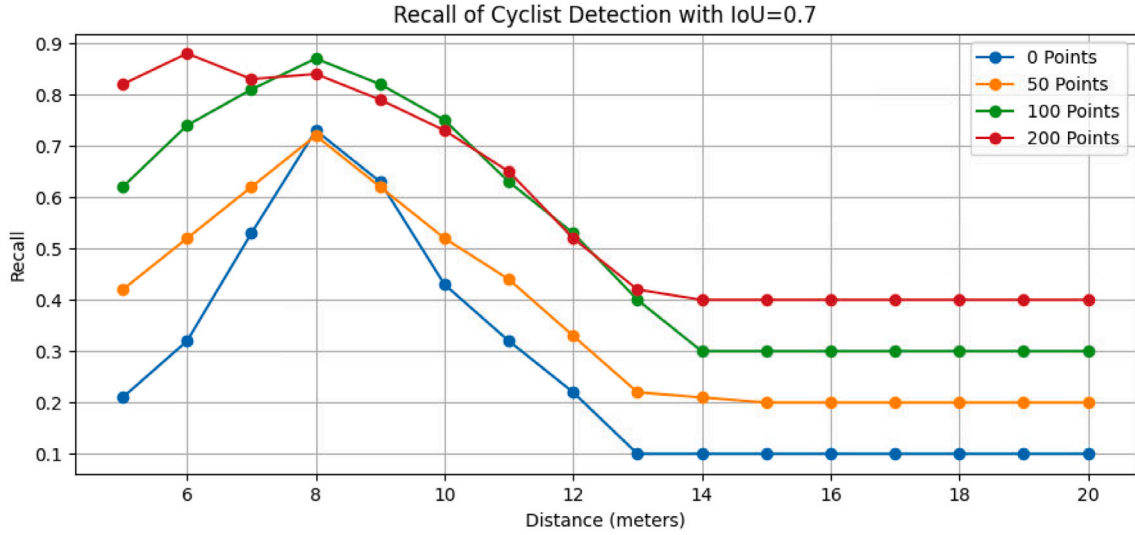


Fig. 12. IoU = 0.7 for cyclist with different points.

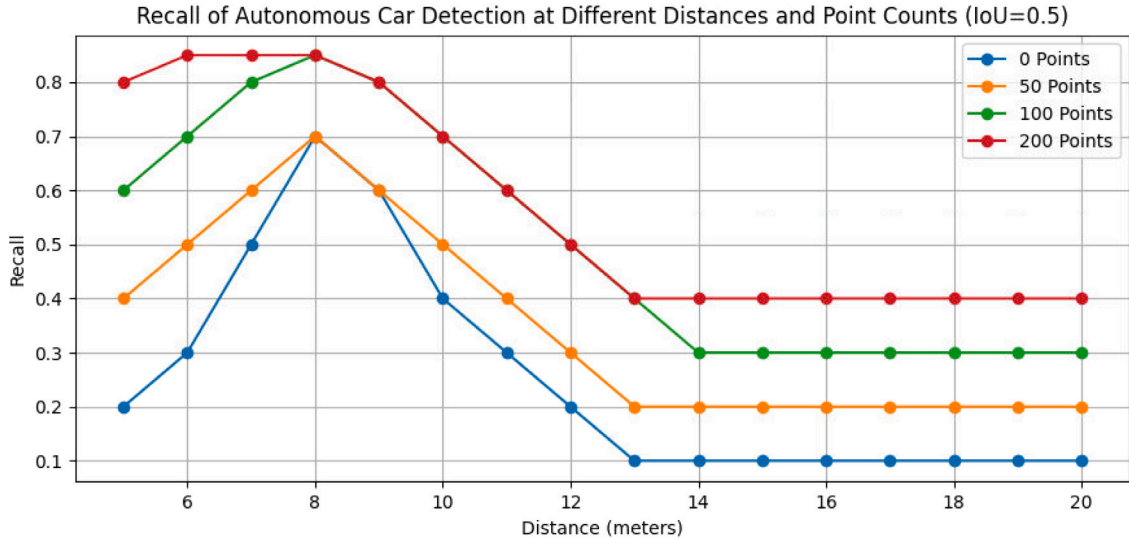


Fig. 13. IoU = 0.5 for cyclist with different points.

shown with modifications that indicate changes in the detection model or environmental variables, as shown in Fig. 12. In general, we observed that the recall values improved as the number of points sampled increased. However, the interaction of parameters such as distance and *IoU* threshold added difficulties, illustrating the importance of precise parameter adjustment to obtain maximum efficiency (see Fig. 13).

Similarly, the analysis was extended to pedestrian detection with *IoU* = 0.7, revealing novel findings. The study of multiple *IoU* thresholds revealed that differences in *IoU* and distance impacted pedestrians and recognition of *AV* in comparable ways. For pedestrian detection with *IoU* = 0.7, it was found that as distance increased, the recall decreased for various counts of points (0, 50, 100, and 200 points). Furthermore, differences in recall values indicated vulnerability to the number of sampled points, as shown in Fig. 14. In the same way, the analysis was extended to *AVs* detection with *IoU* = 0.7, and the recall patterns showed a constant reduction as the distance from the sensor increased. The differences in recall values emphasized the importance of sampling locations in gathering reliable information about the environment, particularly at increasing distances, as shown in Fig. 14.

8.3. Attacker Success Rate (ASR)

The ASR is a metric normally used to quantify an attacker's success against any system. Here, we have mapped the attacker's success rate at different points in these experiments. Mathematically, it *ASR* is calculated as:

$$ASR = \frac{\text{No. of Successful } ATT_{spoofed}}{\text{Total No. of } ATT_{spoofed} \text{ Attempts}} \times 100$$

We have analyzed our system by measuring *ASR* with different thresholds, which provided insights into *LiD*'s sensitivity to adversarial attacks. The graphical depiction demonstrated the dependency of *ASR*'s on various attack thresholds, which helped to comprehend the system's robustness against spoofing attempts. In Figs. 15 and 16, the calculation *ASR* is calculated with different threshold values on the x-axis, while the y-axis shows the related *ASR*. Fig. 17 is the actual position of the original and spoofed object over time. As threshold values increase, this indicates a higher accuracy in spoofing efforts. It also shows a relationship between the attacker's effectiveness in tricking the victim *LiD_{sen}* and the thresholds used. The changing values in the graph also show the system's sensitivity to spoofing attacks at various degrees of

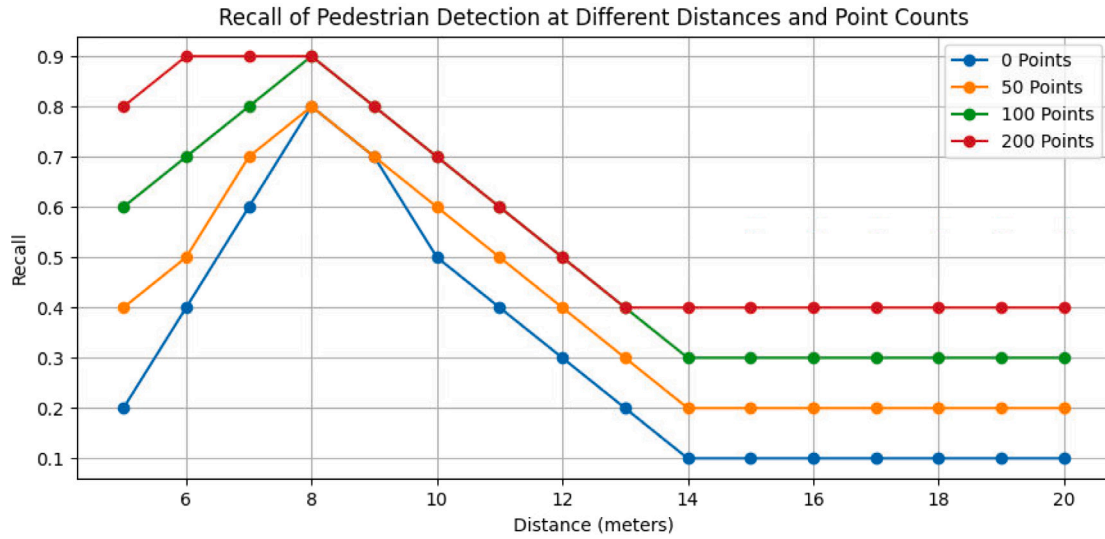


Fig. 14. IoU = 0.7 for pedestrian at different points.

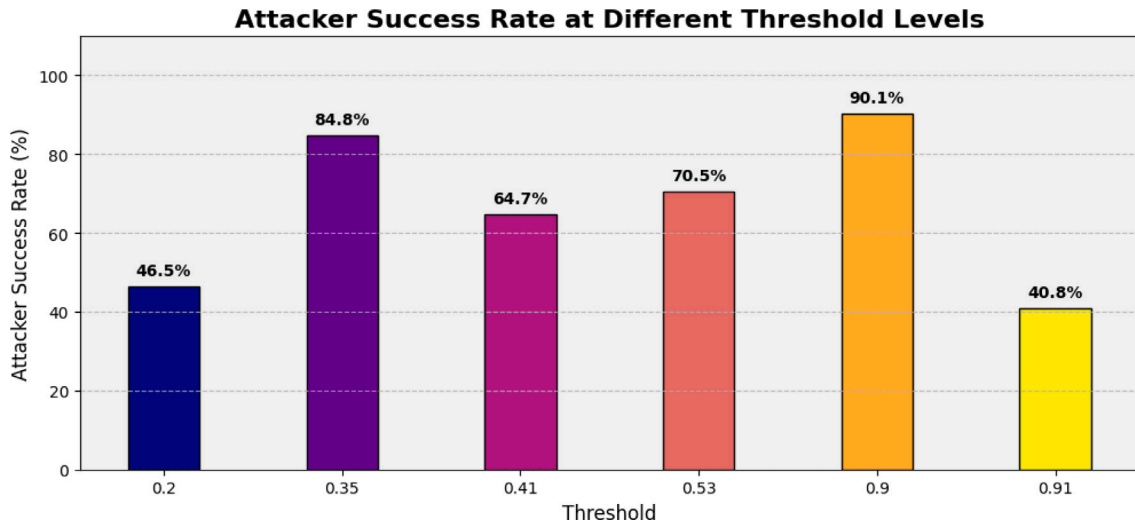


Fig. 15. Attacker success rate in different thresholds.

complexity, as it indicates vital insights to improve security measures and counter possible threats in LiD_{sen} .

8.4. Comparison with state-of-the-art schemes

To compare the different efficiency metrics of the proposed scheme with other state-of-the-art schemes, in this section, we have added a comparison in Table 4. In this table, various factors have been discussed and concluded for different parameters. By comparing different values, the proposed scheme works better in success rate and object detection ratio, with the highest true positive rates (TPRs) and lower true negative rates (TNRs).

9. Conclusion and future directions

LiD Technology, vital for various applications, including AVs , uses laser light to generate accurate 3D maps recognizing objects and their properties. Although LiD systems are typically robust, they can be vulnerable to attacks that compromise signal integrity, resulting in incorrect data. In this research, we suggest a novel method to identify and avoid spoofing attacks on LiD signals using an optimal path strategy for safe navigation. It helps to provide a deeper understanding of the

problems and issues involved in developing successful object detection systems, particularly in the context of LiD -based technologies for AVs . The results of the experiments confirmed that the system was highly effective, with a success rate of 94.57% in true and false positives, an average accuracy rate of 0.95, adaptability to various intersection over union (IoU) rates, and attacker success rates. This approach helps improve the security of LiD systems, especially in safety-critical applications such as autonomous driving. Despite the numerous engineering challenges associated with LiD -based technology, effectively addressing real-time spoofing attacks remains a big challenge. First, attacking LiD_{sen} from a distance is a dominant task. The limited number of distant LiD scan points affects synchronization, requiring larger optical devices or additional photodiodes. Furthermore, because faked signals diverge with distance, which affects the strength of the signal, a more advanced optical system is necessary to converge these signals successfully. Given the variation in LiD models between AVs , a universally applicable model that can accommodate multiple LiD_{sen} in various situations is required for effective attacks. Another challenge is that aiming for a rapidly changing world LiD requires greater accuracy. To do this, the attacker must have a laser diode with enhanced power to target a larger area at once. Despite significant advancements in the perception of LiD -based 3DX of AD , LiD -3DX technology remains vulnerable

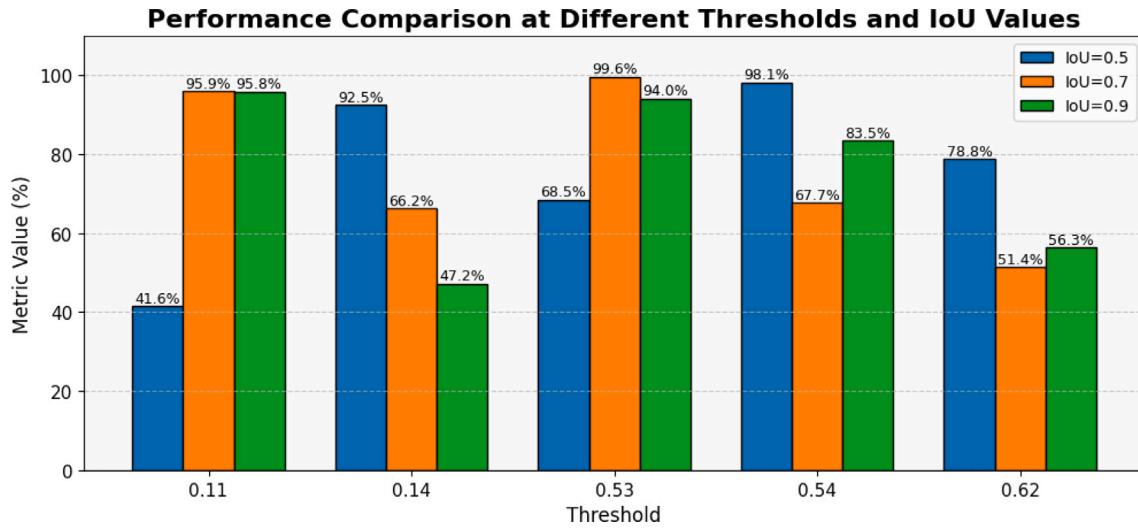


Fig. 16. Attacker success rate in different thresholds and IoU.

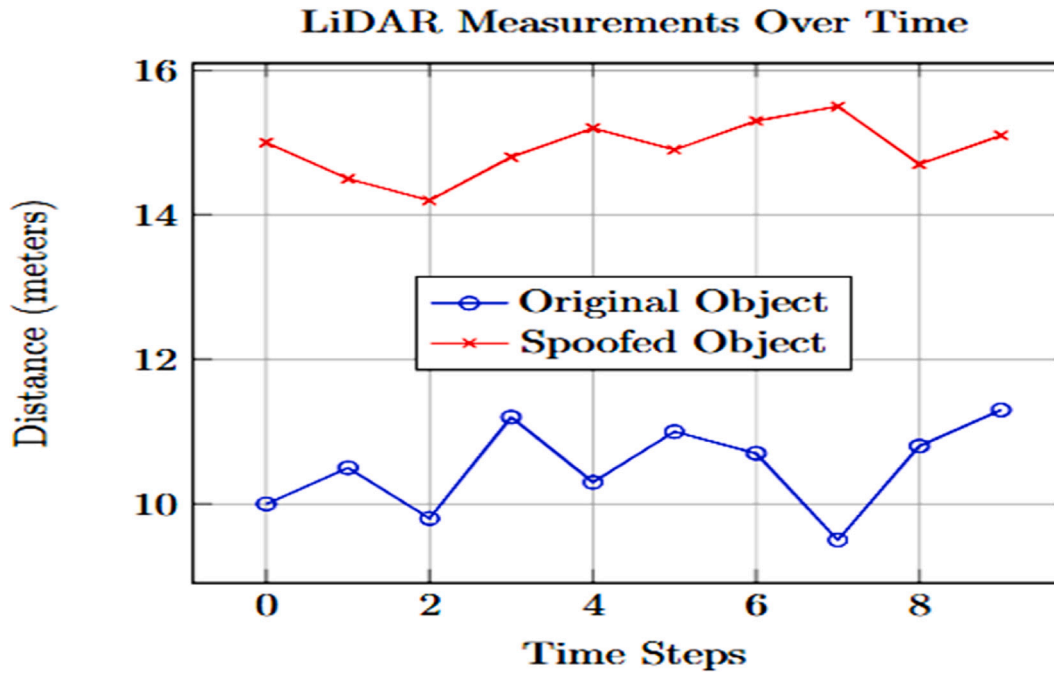


Fig. 17. Attacker success rate in different thresholds.

Table 4

Summary of techniques, Achievements, and Limitations.

Schemes	TPRs and TNRs	Success rate %	Detection ratio %
Cao et al. (2019)	High and moderate	0.852	0.931
Cao et al. (2023)	Low and moderate	0.921	0.899
Sun et al. (2020a)	Lower and Moderate-High	0.797	0.981
You et al. (2021)	High and moderate	0.567	0.838
Alheeti et al. (2022)	Moderate-High and lower	0.723	0.891
Changalvala et al.	Lower and moderate	0.901	0.879
Jakobsen et al. (2023)	Higher and lower	0.922	0.901
Jin et al. (2023)	Lower and Moderate-Higher	0.899	0.652
Hallyburton et al. (2022)	Lower and High-Moderate	0.901	0.867
Mahima et al. (2023)	Higher and lower	0.938	0.909
Tu et al. (2020)	High-moderate and moderate	0.971	0.893
Abdelfattah et al. (2021)	Higher and lower	0.799	0.821
Li et al. (2021c)	High-moderate and moderate-low	0.712	0.901
Liu and Park (2021)	Higher and lower	0.812	0.839
Rieken and Maurer (2020)	Lower and moderate	0.722	0.981
Proposed scheme	Highest and lower	0.997	0.996

to spoofing attacks, which can compromise the reliability and safety of the system. One major limitation is the susceptibility of *LiD* sensors to adversarial manipulations, where attackers can introduce fake or altered *3DX* data to deceive the perception system. Attackers can manipulate *LiD* data by injecting false objects, removing real obstacles, or misclassifying objects. Spoofing attacks can mislead the perception system, increasing the chances of accidents. Computational overhead is another concern, as robust defense strategies can require significant processing power, which could impact the real-time performance of autonomous systems. The absence of standardized security protocols for 3D *LiD* data transmission makes it difficult to implement universal and effective countermeasures. Each system may have unique vulnerabilities. Identifying and countering spoofing attacks in real-time scenarios remains a challenge due to the complexity of attack patterns; this is a critical constraint for autonomous driving.

CRedit authorship contribution statement

Tariq Hussain: Writing – review & editing, Writing – original draft, Conceptualization. **Muhammad Nawaz Khan:** Funding acquisition, Conceptualization. **Bailin Yang:** Supervision, Software, Resources. **Razaz Waheeb Attar:** Investigation, Funding acquisition. **Ahmed Alhomoud:** Conceptualization.

Ethical approval

We confirm that relevant guidelines and regulations are carried out in all methods.

Funding

This work was supported by the “Pioneer” and “Leading Goose” R.D. Program of Zhejiang Province (2023C01150). This research was supported by the Zhejiang Provincial Natural Science Foundation of China under Grant No. LD24F020003. and also supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R 343), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number “NBU-FFR-2025-1092-12”.

Declaration of competing interest

The authors of this manuscript declare no conflicts of interest.

Acknowledgments

This work was supported by the “Pioneer” and “Leading Goose” R.D. Program of Zhejiang Province (2023C01150). This research was supported by the Zhejiang Provincial Natural Science Foundation of China under Grant No. LD24F020003. This research was supported by the Natural Science Foundation of China under the Grant No. 62172366. and also supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R 343), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number “NBU-FFR-2025-1092-12”. Tariq Hussain and Bailin Yang contributed equally to this work and are the first co-authors.

Data availability

Data were not used to support this study.

References

- Abdelfattah, M., Yuan, K., Wang, Z.J., Ward, R., 2021. Adversarial attacks on camera-lidar models for 3d car detection. In: 2021 IEEE/RSJ International Conference on Intelligent Robots and Systems. IROS, IEEE, pp. 2189–2194.
- Airlangga, G., Liu, A., 2023. A study of the data security attack and defense pattern in a centralized UAV-cloud architecture. *Drones* 7 (5), 289.
- Alheeti, K.M.A., Alzahrani, A., Al Dosary, D., 2022. Lidar spoofing attack detection in autonomous vehicles. In: 2022 IEEE International Conference on Consumer Electronics. ICCE, IEEE, pp. 1–2.
- Beck, J., Arvin, R., Lee, S., Khattak, A., Chakraborty, S., 2023. Automated vehicle data pipeline for accident reconstruction: new insights from LiDAR, camera, and radar data. *Accid. Anal. Prev.* 180, 106923.
- Bhupathiraju, S.H.V., Sheldon, J., Bauer, L.A., Bindschaedler, V., Sugawara, T., Rampazzi, S., 2023. EMI-lidar: Uncovering vulnerabilities of LiDAR sensors in autonomous driving setting using electromagnetic interference. In: Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks. pp. 329–340.
- Cao, Y., Bhupathiraju, S.H., Naghavi, P., Sugawara, T., Mao, Z.M., Rampazzi, S., 2023. You can't see me: Physical removal attacks on (lidar-based) autonomous vehicles driving frameworks. In: 32nd USENIX Security Symposium (USENIX Security 23). pp. 2993–3010.
- Cao, Y., Xiao, C., Cyr, B., Zhou, Y., Park, W., Rampazzi, S., Chen, Q.A., Fu, K., Mao, Z.M., 2019. Adversarial sensor attack on lidar-based perception in autonomous driving. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. pp. 2267–2281.
- Cheng, M., Yi, J., Chen, P.-Y., Zhang, H., Hsieh, C.-J., 2020. Seq2sick: Evaluating the robustness of sequence-to-sequence models with adversarial examples. In: Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 34, pp. 3601–3608, no. 04.
- Coops, N.C., Tompalski, P., Goodbody, T.R., Queinnee, M., Luther, J.E., Bolton, D.K., White, J.C., Wulder, M.A., van Lier, O.R., Hermosilla, T., 2021. Modelling lidar-derived estimates of forest attributes over space and time: A review of approaches and future trends. *Remote Sens. Environ.* 260, 112477.
- Cui, H., Nguyen, T., Chou, F.-C., Lin, T.-H., Schneider, J., Bradley, D., Djuric, N., 2020. Deep kinematic models for kinematically feasible vehicle trajectory predictions. In: 2020 IEEE International Conference on Robotics and Automation. ICRA, IEEE, pp. 10563–10569.
- Dasgupta, S., Irfan, M.S., Rahman, M., Chowdhury, M., 2025. Detection and mitigation of spoofing attacks in-based autonomous ground vehicle navigation systems. In: *Data Analytics for Intelligent Transportation Systems*. Elsevier, pp. 403–427.
- Deschaud, J.-E., 2021. KITTI-CARLA: a KITTI-like dataset generated by CARLA simulator. *arXiv preprint arXiv:2109.00892*.
- Dosovitskiy, A., Ros, G., Codevilla, F., Lopez, A., Koltun, V., 2017. CARLA: An open urban driving simulator. In: *Conference on Robot Learning*. PMLR, pp. 1–16.
- Fan, H., Zhu, F., Liu, C., Zhang, L., Zhuang, L., Li, D., Zhu, W., Hu, J., Li, H., Kong, Q., 2018. Baidu apollo em motion planner. *arXiv preprint arXiv:1807.08048*.
- Feng, M., Zhang, H., 2022. Application of baidu apollo open platform in a course of control simulation experiments. *Comput. Appl. Eng. Educ.* 30 (3), 892–906.
- Guesmi, A., Shafique, M., 2024. Navigating threats: A survey of physical adversarial attacks on lidar perception systems in autonomous vehicles. *arXiv preprint arXiv:2409.20426*.
- Hallyburton, R.S., Liu, Y., Cao, Y., Mao, Z.M., Pajic, M., 2022. Security analysis of {camera-lidar} fusion against {black-box} attacks on autonomous vehicles. In: 31st USENIX Security Symposium. USENIX Security 22, pp. 1903–1920.
- Hu, X., Liu, T., Shu, T., Nguyen, D., 2024. Spoofing detection for LiDAR in autonomous vehicles: A physical-layer approach. *IEEE Internet Things J.*
- Huang, J., He, Z., Arakawa, Y., Dawton, B., 2023. Trajectory planning in frenet frame via multi-objective optimization. *IEEE Access* 11, 70764–70777.
- Jakobsen, S.B., Knudsen, K.S., Andersen, B., 2023. Analysis of sensor attacks against autonomous vehicles. In: 8th International Conference on Internet of Things, Big Data and Security. SCITEPRESS Digital Library, pp. 131–139.
- Jeong, D., Choi, S.B., 2024. Efficient trajectory planning for autonomous vehicles using quadratic programming with weak duality. *IEEE Trans. Intell. Veh.* 9 (1), 2878–2892.
- Jin, Z., Ji, X., Cheng, Y., Yang, B., Yan, C., Xu, W., 2023. Pla-lidar: Physical laser attacks against lidar-based 3d object detection in autonomous vehicle. In: 2023 IEEE Symposium on Security and Privacy. SP, IEEE, pp. 1822–1839.
- Jin, Z., Ji, X., Cheng, Y., Yang, B., Yan, C., Xu, W., 2024. Laser-based LiDAR spoofing: Effects validation, capability quantification, and countermeasures. *IEEE Internet Things J.*
- Khan, M.A., Menouar, H., Abdallah, M., Abu-Dayya, A., 2024. Lidar in connected and autonomous vehicles-perception, threat model, and defense. *IEEE Trans. Intell. Veh.*
- Li, B., Hou, J., Li, D., Yang, D., Han, H., Bi, X., Wang, X., Hinkelmann, R., Xia, J., 2021a. Application of LiDAR UAV for high-resolution flood modelling. *Water Resour. Manag.* 35, 1433–1447.
- Li, B., Ouyang, Y., Li, L., Zhang, Y., 2022. Autonomous driving on curvy roads without reliance on frenet frame: A cartesian-based trajectory planning method. *IEEE Trans. Intell. Transp. Syst.* 23 (9), 15729–15741.

- Li, Z., Pan, M., Zhang, T., Li, X., 2021b. Testing dnn-based autonomous driving systems under critical environmental conditions. In: International Conference on Machine Learning. PMLR, pp. 6471–6482.
- Li, Y., Wen, C., Juefei-Xu, F., Feng, C., 2021c. Fooling lidar perception via adversarial trajectory perturbation. In: Proceedings of the IEEE/CVF International Conference on Computer Vision. pp. 7898–7907.
- Li, J., Xu, R., Liu, X., Ma, J., Chi, Z., Ma, J., Yu, H., 2023. Learning for vehicle-to-vehicle cooperative perception under lossy communication. *IEEE Trans. Intell. Veh.* 8 (4), 2650–2660.
- Li, B., Zhang, Y., 2020. Fast trajectory planning in cartesian rather than frenet frame: A precise solution for autonomous driving in complex urban scenarios. *IFAC-Pap.* 53 (2), 17065–17070.
- Liu, J., Park, J.-M., 2021. “Seeing is not always believing”: detecting perception error attacks against autonomous vehicles. *IEEE Trans. Dependable Secur. Comput.* 18 (5), 2209–2223.
- Mahima, K.Y., Perera, A., Anavatti, S., Garratt, M., 2023. Exploring adversarial robustness of LiDAR semantic segmentation in autonomous driving. *Sensors* 23 (23), 9579.
- Petit, J., Stottelaar, B., Feiri, M., Kargl, F., 2015. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. *Black Hat Eur.* 11 (2015), 995.
- Polack, P., Althé, F., d’Andréa Novel, B., de La Fortelle, A., 2017. The kinematic bicycle model: A consistent model for planning feasible trajectories for autonomous vehicles? In: 2017 IEEE Intelligent Vehicles Symposium. IV, IEEE, pp. 812–818.
- Qiao, D., Zulkernine, F., 2023. Adaptive feature fusion for cooperative perception using lidar point clouds. In: Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision. pp. 1186–1195.
- Ravindran, R., Santora, M.J., Jamali, M.M., 2020. Multi-object detection and tracking, based on DNN, for autonomous vehicles: A review. *IEEE Sensors J.* 21 (5), 5668–5677.
- Rieken, J., Maurer, M., 2020. A lidar-based real-time capable 3D perception system for automated driving in urban domains. *arXiv preprint arXiv:2005.03404*.
- Rigó, E., Árvai, P., Póser, V., 2024. Cybersecurity and autonomous driving: Experiments with LiDAR sensor spoofing. In: 2024 5th International Conference on Communications, Information, Electronic and Energy Systems. CIEES, IEEE, pp. 1–5.
- Roriz, R., Cabral, J., Gomes, T., 2021. Automotive LiDAR technology: A survey. *IEEE Trans. Intell. Transp. Syst.* 23 (7), 6282–6297.
- Schepis, D., Purchase, S., Olaru, D., Smith, B., Ellis, N., 2023. How governments influence autonomous vehicle (AV) innovation. *Transp. Res. Part A: Policy Pr.* 178, 103874.
- Schneider, S., Himmelsbach, M., Luettel, T., Wuensche, H.-J., 2010. Fusing vision and lidar-synchronization, correction and occlusion reasoning. In: 2010 IEEE Intelligent Vehicles Symposium. IEEE, pp. 388–393.
- Shafique, A., Mehmood, A., Elhadeif, M., 2021. Detecting signal spoofing attack in uavs using machine learning models. *IEEE Access* 9, 93803–93815.
- Shin, H., Kim, D., Kwon, Y., Kim, Y., 2017. Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications. In: Cryptographic Hardware and Embedded Systems—CHES 2017: 19th International Conference, Taipei, Taiwan, September 25–28, 2017, Proceedings. Springer, pp. 445–467.
- Sun, J., Cao, Y., Chen, Q.A., Mao, Z.M., 2020a. Towards robust (lidar-based) perception in autonomous driving: General black-box adversarial sensor attack and countermeasures. In: 29th USENIX Security Symposium. USENIX Security 20, pp. 877–894.
- Sun, S., Zhang, Z., Pan, Q., Liu, M., Li, Z., 2023. Vehicle-cluster-based opportunistic relays for data collection in intelligent transportation systems. *Comput. Netw.* 220, 109509.
- Tu, J., Ren, M., Manivasagam, S., Liang, M., Yang, B., Du, R., Cheng, F., Urtasun, R., 2020. Physically realizable adversarial examples for lidar object detection. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. pp. 13716–13725.
- Usmani, K., O’Connor, T., Wani, P., Javidi, B., 2022. 3D object detection through fog and occlusion: passive integral imaging vs active (LiDAR) sensing. *Opt. Express* 31 (1), 479–491.
- Vishnu, C., Khandelwal, J., Mohan, C.K., Reddy, C.L., 2023. EVAA—Exchange vanishing adversarial attack on LiDAR point clouds in autonomous vehicles. *IEEE Trans. Geosci. Remote Sens.* 61, 1–10.
- Wang, X., Zhu, H., Ning, Z., Guo, L., Zhang, Y., 2023. Blockchain intelligence for internet of vehicles: Challenges and solutions. *IEEE Commun. Surv. & Tutorials* 25 (4), 2325–2355.
- Xiao, C., Li, B., Zhu, J.-Y., He, W., Liu, M., Song, D., 2018a. Generating adversarial examples with adversarial networks. *arXiv preprint arXiv:1801.02610*.
- Xiao, C., Zhu, J.-Y., Li, B., He, W., Liu, M., Song, D., 2018b. Spatially transformed adversarial examples. *arXiv preprint arXiv:1801.02612*.
- You, C., Hau, Z., Demetriou, S., 2021. Temporal consistency checks to detect LiDAR spoofing attacks on autonomous vehicle perception. In: Proceedings of the 1st Workshop on Security and Privacy for Mobile AI. pp. 13–18.
- Zhang, Y., Sun, H., Zhou, J., Hu, J., Miao, J., 2019. Optimal trajectory generation for autonomous vehicles under centripetal acceleration constraints for in-lane driving scenarios. In: 2019 IEEE Intelligent Transportation Systems Conference. ITSC, IEEE, pp. 3619–3626.
- Zhang, Y., Sun, H., Zhou, J., Pan, J., Hu, J., Miao, J., 2020a. Optimal vehicle path planning using quadratic optimization for baidu apollo open platform. In: 2020 IEEE Intelligent Vehicles Symposium. IV, IEEE, pp. 978–984.
- Zhou, Z., Feng, X., Di, S., Zhou, X., 2023. A LiDAR mapping system for robot navigation in dynamic environments. *IEEE Trans. Intell. Veh.* 1–20.
- Zhu, Y., Miao, C., Hajiaghajani, F., Huai, M., Su, L., Qiao, C., 2021. Adversarial attacks against lidar semantic segmentation in autonomous driving. In: Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems. pp. 329–342.