

# Exploring Lidar Resilience: A Review of Spoofing Threats in Autonomous Driving

Mihir Nemana

*Mechanical and Aerospace Engineering*  
Illinois Institute of Technology  
Chicago, U.S.  
mnemana@hawk.iit.edu

Kana Nagai

*Mechanical and Aerospace Engineering*  
Illinois Institute of Technology  
Chicago, U.S.  
knagai@hawk.iit.edu

Samer Khanafseh

*Mechanical and Aerospace Engineering*  
Illinois Institute of Technology  
Chicago, U.S.  
khansam1@iit.edu

Boris Pervan

*Mechanical and Aerospace Engineering*  
Illinois Institute of Technology  
Chicago, U.S.  
pervan@iit.edu

**Abstract**—Autonomous Driving Systems heavily rely on Lidar for tasks like mapping, localization, and object detection, especially in GNSS-denied environments. However, these systems remain vulnerable to cyberattacks, including spoofing and interference, due to Lidar’s inherent limitations. This paper highlights the need for resilience in safety critical applications where navigation integrity and continuity needs to be maintained even under adversarial conditions. We survey Lidar vulnerabilities, explore spoofing attack mechanisms, and outline future work on mitigation strategies, such as spoofing detection and system augmentation, to enhance the reliability of these systems.

**Index Terms**—Integrity, Continuity, Autonomous Driving Vehicles, Lidar, Spoofing, Resiliency.

## I. INTRODUCTION

Modern automated transportation systems heavily rely on navigation technologies, including navigation satellite systems (GNSS), inertial navigation systems (INS), and light detection and ranging (Lidar) sensors. However, critical threats to these systems, such as spoofing and interference, are becoming increasingly frequent [1]. These threats have disrupted airport operations and caused significant inconvenience for users [2].

This background underscores the importance of resilience, defined as the ability to maintain navigation accuracy, integrity, and continuity in the face of environmental disruptions or malicious attacks. Resilient navigation systems have gained significant attention in recent studies, with a focus on enhancing GNSS resilience through sensor augmentation to detect and mitigate spoofing and interference, thereby improving robustness [3]–[6]. However, augmented sensors may also be vulnerable to similar threats. This paper highlights the need for resilience in Lidar-based localization, a critical component of augmented sensors, particularly in GNSS-denied environments [7].

This article is based on work supported by the Center for Assured and Resilient Navigation in Advanced Transportation Systems (CARNATIONS) under the US Department of Transportation (USDOT)’s University Transportation Center (UTC) program (Grant No. 69A3552348324).

Lidar functions as an active remote sensing technology, emitting laser beams to detect objects within its field of view and measure their distances, azimuths, and intensities. Distance is calculated based on the time it takes for the laser beam to return after reflecting off an object, azimuths are determined by the angles at which the beams are emitted, and intensities are derived from the number of photons returning to the sensor [8], [9].

Autonomous driving applications extensively utilize Lidar for tasks such as lane detection, object detection, tracking, segmentation, mapping, and localization [10]. Simultaneous Localization and Mapping (SLAM) enables the creation of maps in unfamiliar environments while simultaneously estimating the system’s position. Although SLAM is highly effective for generating high-resolution maps in GNSS-denied environments using Lidar, it is prone to drift errors, necessitating post-processing to ensure accuracy [11], [12].

Since our previous work emphasized integrity evaluation requiring accurate and drift-free positioning, we assumed the navigation system had access to a pre-defined *map*. Map-based Lidar localization, under fault-free conditions, can provide accuracy at the centimeter-level [13], [14]. Approaches to map-based Lidar localization include scan-matching and landmark-based localization [7], [15].

This paper investigates the vulnerabilities of Autonomous Driving Systems, with a particular focus on how cybersecurity threats can compromise Lidar-based localization. It provides a comprehensive survey of attacks that undermine feature-based landmark localization, including both laser-based and physical spoofing threats. By examining these integrity-compromising attacks, the paper highlights the urgent need for resilience in localization systems. To support this, it first establishes the preferred localization methodology and identifies the specific threats that such systems may encounter. Overall, this work aims to present a thorough overview of the factors that can compromise integrity in safety-critical applications.

Following this introduction, Section II explores the basic

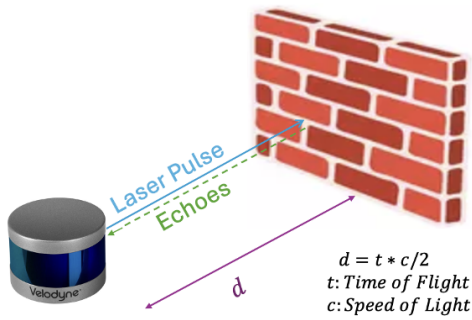


Fig. 1. Lidar basic functionality setup

functionality of Lidar. Section III introduces several types of Lidar-based localization. Section IV discusses landmark-based integrity evaluation, and Section V addresses Lidar spoofing. Section VI presents a discussion of spoofing threats. Finally, Section VII concludes the study and summarizes its key contributions.

## II. LIDAR BASIC FUNCTIONALITY

Lidar sensors function by emitting laser pulses from laser diodes and measuring the time it takes for these pulses to reflect off objects and return to the sensor, a process managed by the internal timing circuit. The photodiodes in the Lidar system play a critical role in detecting these reflected pulses (called “echoes”) and converting the light energy into electrical signals. These signals provide information about the reflection’s intensity, which helps distinguish between materials and surfaces. The timing information from the reflected pulses, combined with the angle of emission, allows the Lidar to calculate the precise distance and location of objects, which are then plotted as points in a 3D space to form a point cloud [16].

A key parameter in Lidar operation is the Minimum Operational Threshold (MOT) [8], [16], which defines the minimum distance from the Lidar sensor at which reflected signals can be reliably detected and processed. Reflected signals below this threshold are often considered unreliable due to design limitations and are typically filtered out by the Lidar’s firmware or middleware. Depending on the environment and application, Lidar can operate in different modes to handle the reflections, or “echoes,” from the laser pulses.

There are three types of echo modes for the Lidar operational modalities: Single Echo mode, Strongest Echo mode, and Multiple Echo mode. In Single Echo mode [16], [17], the sensor records only the first reflection detected, making it efficient for simple, open environments with clear obstacles. However, it may miss multiple or partially obscured surfaces. In Strongest Echo mode [17], the sensor captures the reflection with the highest intensity, which is advantageous for detecting solid or reflective objects but may ignore weaker signals from less reflective surfaces. Lastly, in Multiple Echo mode [16], [18], the sensor records the first, strongest, and last reflections for each pulse. This mode excels in complex, cluttered, or

occluded environments by capturing information from different depths, but it generates a dense point cloud and requires significant computational resources to process efficiently. The most commonly used echo mode in autonomous vehicles is the single echo mode [16], [17].

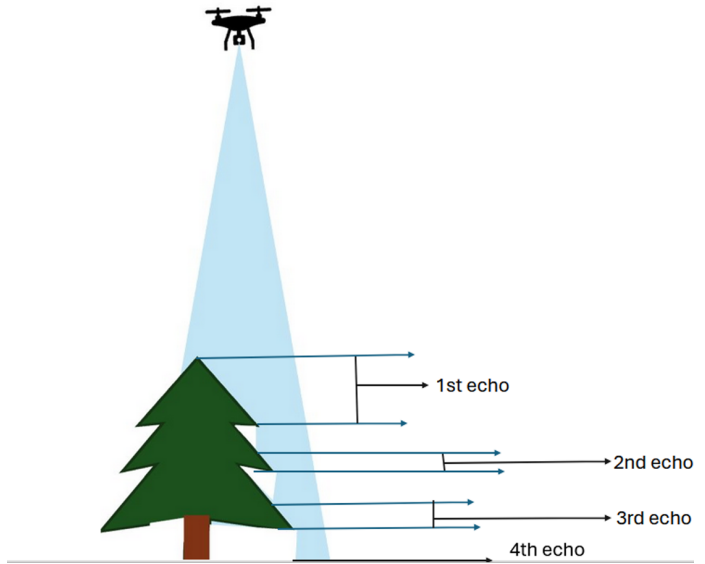


Fig. 2. Lidar multi-echo mode scanning over a tree.

## III. LIDAR LOCALIZATION

This section discusses various Lidar localization methodologies and highlights the importance of a specific Lidar localization method that helps maintain integrity requirements.

Numerous localization methods have been developed for Lidar. One of the most commonly used methods is the Iterative Closest Point (ICP) method [19]. Over time, researchers have transitioned from ICP to more robust methodologies, such as the Normal Distribution Transform (NDT) [20], Iterative Closest Ellipsoid Transform (ICET) [21], and other enhanced versions of ICP. We classify these approaches as map-matching methods, which align each Lidar scan to a pre-existing map to determine the vehicle’s position.

In addition to map-matching, different methodologies leverage features within the point cloud map to estimate a vehicle’s position. One such approach is the landmark-based method, which has been utilized to fulfill integrity requirements for vehicle navigation. Landmark-based architectures [7] rely on existing objects in the environment—such as lampposts, traffic signs, and poles — as reference points to estimate the vehicle’s position. These objects are termed “landmarks” because their known positions are stored in a map database.

We focus on the landmark-based methodology over the other localization approaches mentioned earlier. Although we examined scan-matching methods [22], this work centers on landmark-based localization, where our integrity-focused research is more advanced. Although scan matching has been widely utilized, its integrity aspects have not been explored

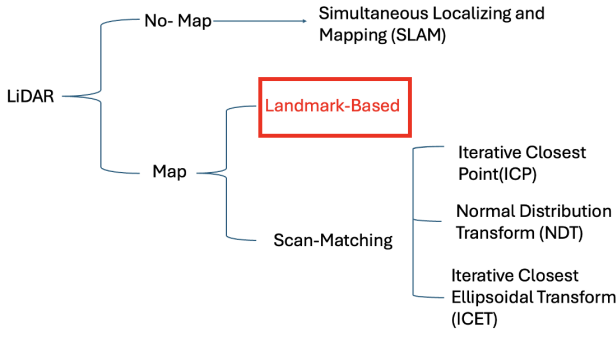


Fig. 3. Lidar Localization methods.

as extensively as those of landmark-based localization. In our evaluation of scan matching, we analyzed its methodology and identified key factors influencing its performance. Given our emphasis on high-integrity localization, we direct our analysis toward the landmark-based methodology, where our research has provided deeper insights. In the following sections, we present a detailed discussion of the integrity considerations specific to landmark-based localization. Additionally, as part of our exploration of scan matching, we conducted an aliasing error analysis to assess the impact of environmental quantization on localization accuracy, which we discuss in detail later in the paper.

#### A. Information loss in scan matching

Most Lidar localization methods based on scan matching rely on quantizing the environment, which leads to information loss. This loss makes it challenging to validate and quantify localization integrity. In this study, we analyze the impact of this loss, referred to as aliasing error. Assuming that surface roughness affects the quantization process, the wall measurement errors are modeled as a first-order Gauss–Markov process. The details and deviations are provided in the Appendix. The aliasing error in this example can be described as:

$$\begin{aligned}
 \sigma_{\delta y}^2(x) &= \sigma_y^2(x) - 2 \sum_{k=-\infty}^{\infty} R_y(x - kD) \operatorname{sinc} \pi \left( \frac{x - kD}{D} \right) \\
 &+ \sum_{k=-\infty}^{\infty} \sum_{j=-\infty}^{\infty} R_y((k - j)D) \\
 &\operatorname{sinc} \pi \left( \frac{x - kD}{D} \right) \operatorname{sinc} \pi \left( \frac{x - jD}{D} \right)
 \end{aligned} \tag{1}$$

where

- $\sigma_y(x)$ : the original Gaussian-distributed error in the wall distance along the y-direction (m)
- $R_y$ : auto-correlation
- $x$ : wall distance in the x-direction (m)
- $k, j$ : number of intervals (integer)
- $D$ : the sample interval distance in the x-direction (m)

Figure 4 shows the aliasing error results calculated using this equation when the Lidar measures at the point  $x = \frac{D}{2}$ . It

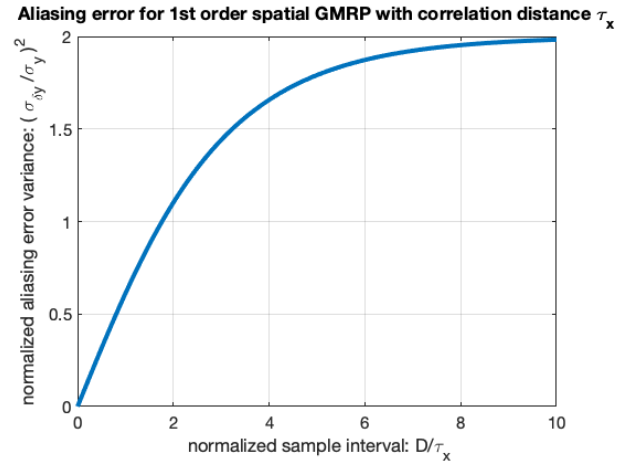


Fig. 4. The normalized aliasing error variance versus the normalized sampling interval.

plots the normalized aliasing error variance against the normalized sampling interval. This figure illustrates that the sampling interval affects the aliasing error. If the normalized sampling interval is 10, the aliasing error becomes twice as large as the original error. Even with this simple assumption—the infinite wall scenario—the information loss from environment simplification introduces the errors. A real Lidar scan-matching application handles more complex environments, considering factors such as building edges and other structural details. The information loss caused by the quantization of these environments can potentially lead to integrity risk.

#### B. Landmark-based Lidar Positioning

The landmark-based localization method begins by detecting landmarks, which are specific features whose positions are recorded in a database known as a map [7]. Subsequently, the sensor measures their distances and angles, and the measured landmarks are matched with the information in the map [13]. The system can estimate a vehicle’s position by combining these measurements with the pre-defined landmark locations. Although all objects in urban environments are candidates for landmarks, we specifically focus on extracting pole-like landmarks (e.g., street lamp posts) because of their distinct shapes, semi-permanent locations, weather resistance, defined centroids, and relative ubiquity, as demonstrated in [23]–[25].

Landmark-based localization relies on two intermediary procedures for positioning from point clouds—feature extraction and data association—both having the potential to introduce faults [26]. The feature extraction process involves identifying pre-defined landmarks from point clouds. Incorrect Extraction (IE) faults occur when the system mistakenly identifies undefined “obstacles” as landmarks. Even if feature extraction works correctly, uncertainty regarding the source of each measurement can lead to an Incorrect Association (IA), resulting in a mismatch between the measurement observations and their corresponding landmark locations in the map.

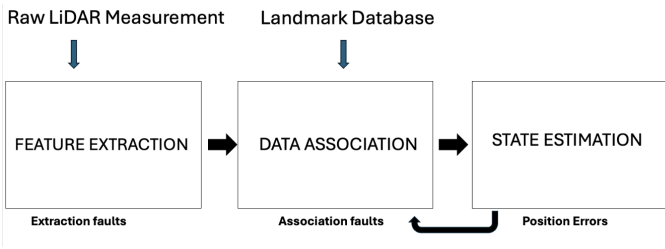


Fig. 5. Landmark-Based Positioning Flow Chart.

#### IV. LANDMARK-BASED INTEGRITY EVALUATION

The core integrity equation shown below provides a probabilistic bound on the risk of Hazardously Misleading Information (HMI) in landmark-based Lidar localization systems. The equation can be described as follows.

$$P(\text{HMI}) \leq 1 - (1 - P(\text{HMI} | \text{CA}, \text{CE})) P(\text{CA} | \text{CE}) P(\text{CE}) \quad (2)$$

It captures how three sequential processes contribute to the overall safety of localization: landmark extraction, data association, and position estimation. Mathematically, the equation ensures that the probability of an undetected HMI remains bounded, even in fault-free conditions. Specifically, it considers: 1. the probability of HMI occurring given that extraction and association were correct,  $P(\text{HMI} | \text{CA}, \text{CE})$ , 2. the probability of correctly associating extracted landmarks to the map,  $P(\text{CA} | \text{CE})$ , and 3. the probability of correctly extracting a real landmark from Lidar data,  $P(\text{CE})$ . The product of these three terms defines an “integrity envelope,” and as long as each component remains reliable, the system is guaranteed to uphold bounded integrity risk, a critical requirement for safety in autonomous navigation.

#### V. LIDAR SPOOFING

Lidar-based localization systems in autonomous vehicles are vulnerable to a wide range of threats that can compromise their performance. These threats can be broadly categorized into unintentional interferences and intentional spoofing attacks. Unintentional interference [27] typically arises when multiple Lidar systems operate in proximity, causing their laser beams to overlap and generate false readings or “ghost points.” More severe, however, are spoofing attacks, which involve deliberate manipulation of the environment to deceive the Lidar sensor. These attacks fall into two main types: physical spoofing, where real landmarks are moved or fake landmarks are added; and laser spoofing, where fake echoes are injected into the sensor’s data stream to simulate or erase objects. At the core, our definition of Lidar spoofing refers to any intentional act where an adversary manipulates the sensor’s perception, either by injecting false points, removing legitimate ones, or modifying physical features in the environment.

The primary goal of such attacks is to undermine both integrity, by causing the system to estimate an incorrect position, and continuity, by causing a complete failure in

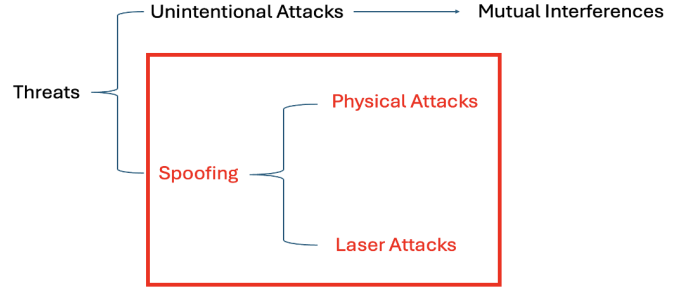


Fig. 6. Spoofing Threats.

position estimation. This is particularly critical in landmark-based localization, where the Lidar system relies on a pre-mapped set of environmental features. Here, even minor tampering—such as shifting a pole by a few inches—can lead to IE of features or IA between observed and mapped landmarks, severely degrading the reliability of the localization process.

##### A. Laser Attacks - Object Injection

One class of integrity-compromising attacks on Lidar-based localization is laser-based object injection spoofing [28]–[30], in which adversaries emit carefully timed and shaped laser pulses to create false environmental structures in the Lidar’s point cloud. This process begins with point cloud fabrication, where spoofer emit laser signals synchronized with the victim Lidar’s scanning cycle, generating fake echoes that are recorded as legitimate returns. These spoofed points are then shaped and clustered to mimic real pole-like landmarks. To increase their believability and likelihood of being selected by the feature extraction algorithm, these fake landmarks are placed near genuine mapped landmarks.

The spoofed points are positioned above the MOT of the Lidar, ensuring they are not rejected by the sensor’s internal filters. A common spoofing setup involves the use of a photodiode to detect outgoing Lidar pulses and a laser emitter to send return signals with minimal delay, effectively mimicking real reflections.

The Lidar perceives both real and fake landmarks within the same vicinity, causing confusion during feature extraction and data association. These manipulations can lead to IE and IA faults, both of which degrade the integrity of the localization system. From an integrity risk perspective, such attacks reduce the probabilities of correct extraction  $P(\text{CE})$  and correct association  $P(\text{CA})$ , thereby increasing the overall probability of Hazardously Misleading Information  $P(\text{HMI})$ , as described in the integrity risk equation, described as Equation (2).

Figure 7 illustrates how a spoofer carries out an object injection attack by imitating the Lidar’s sensing process. The spoofer, shown on the right, uses a photodiode to detect outgoing Lidar pulses and immediately responds by emitting a spoofed echo using a laser. These spoofed signals are carefully placed in the attack region—close to a real object—so that

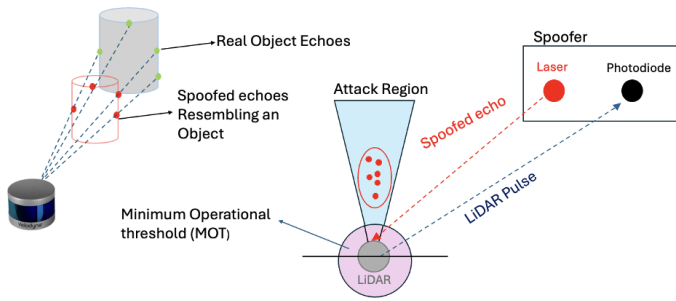


Fig. 7. Object Injection Setup.

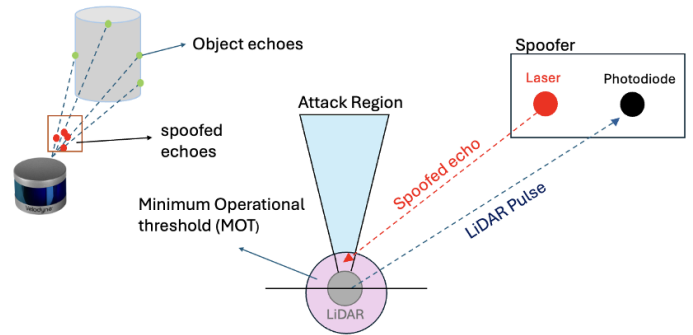


Fig. 9. Object Removal Setup.

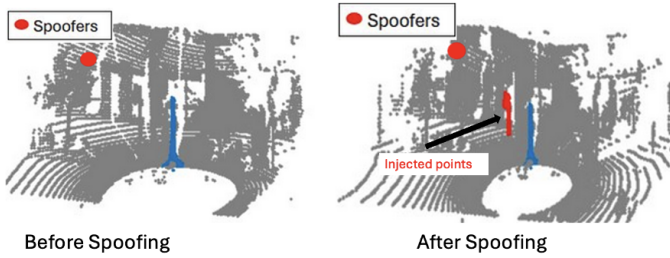


Fig. 8. Illustration. Before Object injection vs After Object Injection.

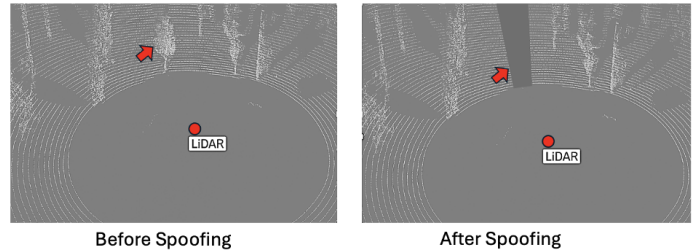


Fig. 10. Illustration. Before Object Removal vs After Object Removal.

they resemble actual echoes. As shown by the red dots, the injected points form a false structure that appears realistic in the Lidar’s point cloud. By ensuring that these points lie above the MOT, they bypass the Lidar’s internal filtering and are treated as valid returns. This tricks the system into recording a fake object, which can then be mistakenly extracted and associated as a legitimate landmark.

Figure 8 shows the effect of a laser-based object injection spoofing attack on a Lidar system. The left side of the figure, which shows the scene before spoofing, depicts a normal environment where the blue points correspond to a real, pole-like landmark accurately detected by the Lidar and matched to the map. On the right, after spoofing, red points have been injected by an attacker. These are fake echoes generated using carefully timed laser pulses designed to mimic real object returns. The spoofed points are strategically placed close to the real landmark, making them appear legitimate to the sensor. As a result, the system perceives both the true and false landmarks simultaneously, increasing the chance of confusion during feature extraction and data association.

### B. Laser Attacks - Object Removal

Laser-Based Object Removal Spoofing is a sophisticated Lidar attack that erases real obstacles from the point cloud using fabricated signals [17], [29]. The process begins with Point Cloud Fabrication, where the spoofer emits laser pulses designed to mimic legitimate returns. These spoofed echoes are then strategically injected into the scan at ranges closer than the MOT of the Lidar—this is the Spoofed Echo Injection stage. Since Lidar systems discard echoes detected below the MOT to filter out noise, any real echoes from farther, legitimate obstacles arriving afterward are ignored by the

internal processing logic. This final phase, called Obstacle Removal, results in the real object effectively vanishing from the point cloud, even though it physically remains in the environment. This is achieved by a photodiode in the spoofer intercepting the original Lidar pulse and instantly responding with a high-intensity fake echo, preemptively occupying the MOT range. As a result, the Lidar system fails to register the real obstacle, presenting a seemingly clear scene to the navigation stack. This manipulation introduces serious risks to the continuity and integrity of autonomous vehicle perception and positioning.

Figure 10 illustrates a laser-based spoofing technique designed to remove real objects from Lidar perception. In the left scan of the figure, taken before the spoofing attack, a clearly visible object—highlighted by a red arrow—appears in the Lidar’s point cloud. However, in the right scan, captured after the spoofing, the object is no longer present. This is not due to any physical change in the environment but rather the result of a spoofing device that has injected fake echoes at a distance closer than the real object, specifically below the sensor’s MOT. Since Lidar systems are designed to ignore any returns that fall below this threshold to reduce false positives, they discard legitimate echoes that arrive slightly later from actual objects. Consequently, the real object is effectively filtered out of the point cloud, despite still existing in the real world. This results in a misleadingly clean scan, omitting critical environmental features. The spoofing setup works by intercepting the Lidar’s outgoing pulse using a photodiode, then rapidly emitting a spoofed echo using a laser. This spoofed signal is returned with high intensity and at a closer

range—within the MOT—causing the Lidar’s internal filtering logic to suppress subsequent echoes, including those from real obstacles. As a result, the Lidar records the spoofed return and dismisses the genuine one, leading to the erasure of real objects from its environmental representation. This method of spoofing presents a serious threat to autonomous driving systems by creating the illusion of a clear environment, while in reality, essential features like pedestrians, poles, or barriers may be entirely invisible to the system.

### C. Physical Spoofing

Physical Spoofing refers to the intentional, manual manipulation of environmental landmarks that are used by autonomous vehicles for localization. Unlike laser-based spoofing, which requires technical sophistication and precise optical equipment, physical spoofing is comparatively low-tech and accessible, yet equally dangerous. This type of attack involves slightly shifting real landmarks or placing fake, similar-looking landmarks near known, pre-mapped ones. These subtle physical alterations disrupt the alignment between the perceived environment and the vehicle’s internal map.

Since landmark-based localization relies on the correct extraction and association of known landmarks, even minor displacement can result in IE or IA errors. Consequently, the navigation system may either latch onto a fake landmark or misinterpret a real one, leading to degraded integrity and continuity in positioning. In effect, physical spoofing achieves the same harmful outcome as laser-based spoofing: corrupting the localization solution. Its simplicity and effectiveness make it an especially concerning threat, and detection techniques developed for physical spoofing can also inform defense mechanisms against more complex spoofing attacks.

## VI. DISCUSSION OF SPOOFING THREATS

Both physical and laser-based spoofing attacks threaten the integrity and continuity of Lidar-based localization in similar ways. While laser spoofing relies on advanced optical injection techniques and timing manipulation, physical spoofing can be executed by simply altering or relocating landmarks in the environment. Despite their different mechanisms, both result in corrupted localization outputs and increased risk of HMI. To defend against these threats, we propose a unified detection framework that is effective for both spoofing types. This is especially critical in GNSS-denied environments such as urban canyons or tunnels, where Lidar often functions as the primary localization sensor.

A key strategy to enhance resilience is sensor augmentation—fusing Lidar with INS and GNSS, enabling cross-verification among sensors. If one system is spoofed, inconsistencies detected by others can flag anomalies. Beyond sensor fusion, developing comprehensive threat models is essential. These models anticipate how spoofing attacks manifest, helping engineers design robust defense strategies in advance. On the detection side, techniques such as integrity monitoring can play a crucial role. By tracking indicators like residuals or innovation vectors, the system can identify deviations from

expected sensor behavior, which may signal the onset of a spoofing attack.

## VII. CONCLUSIONS

This work highlights the full spectrum of spoofing threats to Lidar-based localization, categorizing them into two main types: laser-based attacks and physical attacks. Within the laser-based category, we examined both object injection, where fake landmarks are added to mislead the system, and object removal, where real environmental features are erased from the point cloud using strategically placed spoofed echoes. While differing in execution, both laser-based and physical spoofing methods pose critical risks to localization accuracy, especially in GNSS-denied or cluttered urban environments. These attacks degrade integrity by introducing incorrect position estimates and threaten continuity by disrupting the vehicle’s ability to localize altogether. The overarching aim of this work is to raise awareness of these emerging vulnerabilities and emphasize the urgent need for resilient localization systems capable of operating under adversarial conditions. Future research will focus on the development of multi-sensor fusion strategies, such as combining Lidar with INS and GNSS, and the refinement of real-time detection mechanisms, including integrity monitoring and threat modeling, to ensure robust and secure autonomous navigation.

## ACKNOWLEDGMENT

This article is based on work supported by the Center for Assured and Resilient Navigation in Advanced Transportation Systems (CARNATIONS) under the US Department of Transportation (USDOT)’s University Transportation Center (UTC) program (Grant No. 69A3552348324). Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the sponsors.

## APPENDIX

The discrete time measurements in the y-direction, denoted by  $y^*(x)$ , can be modeled as a stationary spatial random process  $y(x)$  with auto-correlation expressed by the Dirac delta function (see Fig. 11).

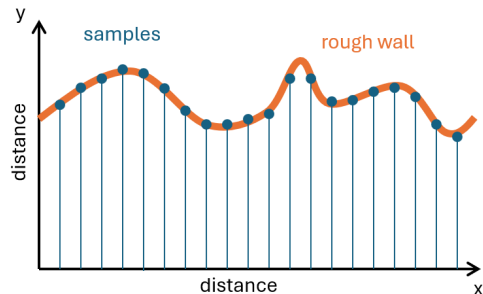


Fig. 11. Illustration of the wall example used in aliasing error analysis

$$y^*(x) = \sum_{k=-\infty}^{\infty} y(x)\delta(x - kD) \quad (3)$$

where

- $y(x)$ : wall distance in the y-direction, expressed a stationary spatial random process (m)
- $x$ : wall distance in the x-direction (m)
- $k$ : number of intervals (integer)
- $D$ : the sample interval distance in the x-direction (m)

Once the measurements are obtained, an attempt is made to reconstruct the original environment using these samples [31].

$$y_r(x) = \sum_{k=-\infty}^{\infty} y(kD) \text{sinc} \pi \left( \frac{x - kD}{D} \right) \quad (4)$$

Since Lidar points represent an environment, applying a low-pass filter in the same way as in signal processing is not feasible, and aliasing errors are expected. The source of aliasing error lies in the distortions that occur during the reconstruction of the original signal when a continuous signal is sampled at an insufficient rate. The aliasing error caused by Lidar measurements,  $\delta y(x)$ , is described as:

$$\delta y(x) = y(x) - \sum_{k=-\infty}^{\infty} y(kD) \text{sinc} \pi \left( \frac{x - kD}{D} \right). \quad (5)$$

Squaring both sides of Equation (5) and taking the expectation value yields the noise equation.

$$\begin{aligned} \sigma_{\delta y}^2(x) &= \sigma_y^2(x) - 2 \sum_{k=-\infty}^{\infty} R_y(x - kD) \text{sinc} \pi \left( \frac{x - kD}{D} \right) \\ &\quad + \sum_{k=-\infty}^{\infty} \sum_{j=-\infty}^{\infty} R_y((k - j)D) \\ &\quad \text{sinc} \pi \left( \frac{x - kD}{D} \right) \text{sinc} \pi \left( \frac{x - jD}{D} \right) \end{aligned} \quad (6)$$

*A. Analysis 1: The Lidar Measures at the Point  $x = 0$*

$$\begin{aligned} \sigma_{\delta y}^2(0) &= \sigma_y^2(0) - 2 \sum_{k=-\infty}^{\infty} R_y(-kD) \text{sinc} \pi(-k) \\ &\quad + \sum_{k=-\infty}^{\infty} \sum_{j=-\infty}^{\infty} R_y((k - j)D) \text{sinc} \pi(-k) \text{sinc} \pi(-j). \end{aligned} \quad (7)$$

Since both  $k$  and  $j$  are integers, the sinc function equals 1 only when  $k = j = 0$ ; otherwise, it equals 0. As a result, all errors cancel out, and no aliasing error occurs.

$$\sigma_{\delta y}^2(0) = \sigma_y^2(0) - 2\sigma_y^2(0) + \sigma_y^2(0) = 0 \quad (8)$$

*B. Analysis 2: The Lidar Measures at the Point  $x = D/2$*

The second analysis shows that information loss occurs at a point in the middle of the Lidar sampling rate. Substituting  $x = D/2$  into Equation (6) yields the following result:

$$\begin{aligned} \sigma_{\delta y}^2 \left( \frac{D}{2} \right) &= \sigma_y^2 \left( \frac{D}{2} \right) - 2 \sum_{k=-\infty}^{\infty} R_y \left( \left( \frac{1}{2} - k \right) D \right) \\ &\quad \text{sinc} \pi \left( \frac{1}{2} - k \right) + \sum_{k=-\infty}^{\infty} \sum_{j=-\infty}^{\infty} R_y((k - j)D) \\ &\quad \text{sinc} \pi \left( \frac{1}{2} - k \right) \text{sinc} \pi \left( \frac{1}{2} - j \right). \end{aligned} \quad (9)$$

Given our assumption that the Lidar measures points on an infinite wall, the autocorrelation components are modeled as a first-order Gauss-Markov process:

$$R_y \left( \left( \frac{1}{2} - k \right) D \right) = \sigma_y^2 \left( \frac{D}{2} \right) \exp \left( - \left| \frac{1}{2} - k \right| \frac{D}{\tau_x} \right) \quad (10)$$

$$R_y((k - j)D) = \sigma_y^2 \left( \frac{D}{2} \right) \exp \left( - |k - j| \frac{D}{\tau_x} \right). \quad (11)$$

Combining Equations (9), (10), and (11), the fraction of aliasing error to the original error can be expressed as:

$$\begin{aligned} \left( \frac{\sigma_{\delta y} \left( \frac{D}{2} \right)}{\sigma_y \left( \frac{D}{2} \right)} \right)^2 &= 1 - 2 \sum_{k=-\infty}^{\infty} \exp \left( - \left| \frac{1}{2} - k \right| \frac{D}{\tau_x} \right) \\ &\quad \text{sinc} \pi \left( \frac{1}{2} - k \right) + \sum_{k=-\infty}^{\infty} \sum_{j=-\infty}^{\infty} \exp \left( - |k - j| \frac{D}{\tau_x} \right) \\ &\quad \text{sinc} \pi \left( \frac{1}{2} - k \right) \text{sinc} \pi \left( \frac{1}{2} - j \right). \end{aligned} \quad (12)$$

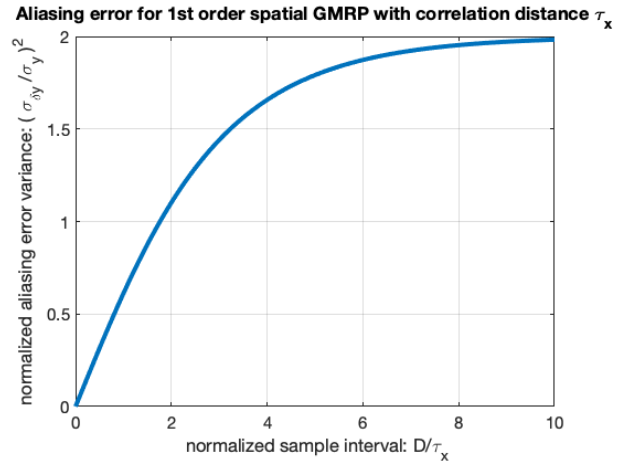


Fig. 12. The normalized aliasing error variance versus the normalized sampling interval.

## REFERENCES

- [1] Z. Liu, S. Lo, and T. Walter, "Characterization of ADS-B performance under GNSS interference," in *Proceedings of the 33rd International Technical Meeting of The Institute of Navigation (ION GNSS+ 2020)*, 2020, pp. 3581–3591.
- [2] M. Joerger, C. Fan, and S. Jada. (2023) The unsolved mystery of the 2022 texas interference. [Online]. Available: <https://insidegnss.com/the-unsolved-mystery-of-the-2022-texas-interference/>
- [3] Ç. Tanil, S. Khanafseh, M. Joerger, and B. Pervan, "An ins monitor to detect gnss spoofers capable of tracking vehicle position," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 1, pp. 131–143, 2017.
- [4] B. Kujur, S. Khanafseh, and B. Pervan, "Optimal ins monitor for gnss spoofer tracking error detection," *NAVIGATION: Journal of the Institute of Navigation*, vol. 71, no. 1, 2024.
- [5] W. Zhao, S. Khanafseh, and B. Pervan, "Adaptive multiple-model kalman filter for gnss carrier phase and frequency estimation through wideband interference," *NAVIGATION: Journal of the Institute of Navigation*, vol. 71, no. 2, 2024.
- [6] S. Ahmed, S. Khanafseh, and B. Pervan, "Gnss spoofing detection based on decomposition of the complex cross ambiguity function," in *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, 2021, pp. 3569–3580.
- [7] K. Nagai, M. Spenko, R. Henderson, and B. Pervan, "Fault-free integrity of urban driverless vehicle navigation with multi-sensor integration: A case study in downtown chicago," *NAVIGATION: Journal of the Institute of Navigation*, vol. 71, no. 1, 2024.
- [8] A. G. Kashani, M. J. Olsen, C. E. Parrish, and N. Wilson, "A review of lidar radiometric processing: From ad hoc intensity correction to rigorous radiometric calibration," *Sensors*, vol. 15, no. 11, pp. 28 099–28 128, 2015.
- [9] Ouster. (2024) Os1 hardware user manual. [Online]. Available: <https://data.ouster.io/downloads/hardware-user-manual/hardware-user-manual-rev7-os1.pdf>
- [10] C. Benedek, A. Majdik, B. Nagy, Z. Rozsa, and T. Sziranyi, "Positioning and perception in LIDAR point clouds," *Digital Signal Processing*, vol. 119, p. 103193, 2021.
- [11] K. Jo, C. Kim, and M. Sunwoo, "Simultaneous localization and map change update for the high definition map-based autonomous driving car," *Sensors*, vol. 18, no. 9, 2018.
- [12] A. Keitaanniemi, P. Rönholm, A. Kukko, and M. T. Vaaja, "Drift analysis and sectional post-processing of indoor simultaneous localization and mapping (SLAM)-based laser scanning data," *Automation in Construction*, vol. 147, p. 104700, 2023.
- [13] J. Levinson, M. Montemerlo, and S. Thrun, "Map-based precision vehicle localization in urban environments," in *Robotics: science and systems*, vol. 4, 2007, p. 1.
- [14] G. Wan, X. Yang, R. Cai, H. Li, Y. Zhou, H. Wang, and S. Song, "Robust and precise vehicle localization based on multi-sensor fusion in diverse city scenes," in *2018 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 2018, pp. 4670–4677.
- [15] J. Levinson and S. Thrun, "Robust vehicle localization in urban environments using probabilistic maps," in *2010 IEEE International Conference on Robotics and Automation*, 2010, pp. 4372–4378.
- [16] Y. Cao, S. H. Bhupathiraju, P. Naghavi, T. Sugawara, M. Z. Morley, and S. Rampazzi. (2023) You can't see me: Physical removal attacks on lidar-based autonomous vehicles driving frameworks. [Online]. Available: <https://www.youtube.com/watch?v=3y66bQdfvF0>
- [17] Y. Cao, S. H. Bhupathiraju, P. Naghavi, T. Sugawara, Z. M. Mao, and S. 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, pp. 2993–3010.
- [18] Y. Man, X. Weng, P. K. Sivakumar, M. O'Toole, and K. M. Kitani, "Multi-echo lidar for 3d object detection," in *Proceedings of the IEEE/CVF International Conference on Computer Vision*, 2021, pp. 3763–3772.
- [19] P. J. Besl and N. D. McKay, "Method for registration of 3-d shapes," in *Sensor fusion IV: control paradigms and data structures*, vol. 1611. Spie, 1992, pp. 586–606.
- [20] P. Biber and W. Straßer, "The normal distributions transform: A new approach to laser scan matching," in *Proceedings 2003 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2003)(Cat. No. 03CH37453)*, vol. 3. IEEE, 2003, pp. 2743–2748.
- [21] M. McDermott and J. Rife, "Icet online accuracy characterization for geometry-based laser scan matching," *NAVIGATION: Journal of the Institute of Navigation*, vol. 71, no. 2, 2024.
- [22] J. H. Rife, S. Khanafseh, B. Pervan, and H. Wassaf, "Fundamental architectures for high-integrity georeferenced lidar positioning," in *Proceedings of the 37th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2024)*, 2024, pp. 245–267.
- [23] J. Gim, C. Ahn, and H. Peng, "Landmark attribute analysis for a high-precision landmark-based local positioning system," *IEEE Access*, vol. 9, pp. 18 061–18 071, 2021.
- [24] M. Sefati, M. Daum, B. Sondermann, K. D. Kreisköther, and A. Kampker, "Improving vehicle localization using semantic and pole-like landmarks," in *2017 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2017, pp. 13–19.
- [25] T. Tee-Ann and C. Chi-Min, "Pole-like road object detection from mobile lidar system using a coarse-to-fine approach," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 8, no. 10, pp. 4805–4818, 2015.
- [26] Y. Bar-Shalom and T. Fortmann, *Tracking and Data Association*, ser. Mathematics in science and engineering. Academic Press, 1988.
- [27] G. Kim, J. Eom, and Y. Park, "An experiment of mutual interference between automotive lidar scanners," in *2015 12th International Conference on Information Technology-New Generations*. IEEE, 2015, pp. 680–685.
- [28] J. Sun, Y. Cao, Q. A. Chen, and Z. M. Mao, "Towards robust {LiDAR-based} perception in autonomous driving: General black-box adversarial sensor attack and countermeasures," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 877–894.
- [29] T. Sato, Y. Hayakawa, R. Suzuki, Y. Shiiki, K. Yoshioka, and Q. A. Chen, "Lidar spoofing meets the new-gen: Capability improvements, broken assumptions, and new attack strategies," *arXiv preprint arXiv:2303.10555*, 2023.
- [30] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "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, 2017, pp. 445–467.
- [31] G. Franklin, J. Powell, and M. Workman, *Digital Control of Dynamic Systems*, ser. Addison-Wesley series in electrical and computer engineering: Control engineering. Addison-Wesley Publishing Company, 1990. [Online]. Available: <https://books.google.com/books?id=Iw8oAQAAMAAJ>