PhantomLiDAR: Cross-modality Signal Injection Attacks against LiDAR

Zizhi Jin, Qinhong Jiang, Xuancun Lu, Chen Yan, Xiaoyu Ji✉* , Wenyuan Xu
Zhejiang University
{zizhi, qhjiang, xuancun_lu, yanchen, xji, wyxu}@zju.edu.cn

***Abstract*—LiDAR (Light Detection and Ranging) is a pivotal sensor for autonomous driving, offering precise 3D spatial information. Previous signal attacks against LiDAR systems mainly exploit laser signals. In this paper, we investigate the possibility of cross-modality signal injection attacks, i.e., injecting intentional electromagnetic interference (IEMI) to manipulate LiDAR output. Our insight is that the internal modules of a LiDAR, i.e., the laser receiving circuit, the monitoring sensors, and the beam-steering modules, even with strict electromagnetic compatibility (EMC) testing, can still couple with the IEMI attack signals and result in the malfunction of LiDAR systems. Based on the above attack surfaces, we propose the PhantomLiDAR attack, which manipulates LiDAR output in terms of *Points Interference*, *Points Injection*, *Points Removal*, and even *LiDAR Power-Off*. We evaluate and demonstrate the effectiveness of PhantomLiDAR with both simulated and real-world experiments on five COTS LiDAR systems. We also conduct feasibility experiments in real-world moving scenarios. We provide potential defense measures that can be implemented at both the sensor level and the vehicle system level to mitigate the risks associated with IEMI attacks. Video demonstrations can be viewed at https://sites.google.com/view/phantomlidar.**

I. Introduction

Autonomous systems empowered by artificial intelligence are having a transformative impact on our society. LiDAR (Light Detection and Ranging), which directly measures the coordinates and shapes of objects with precision, has been increasingly integrated into various applications such as autonomous vehicles (AVs), drones, and robots. According to Yole [38], more than 119 car models are to be released with LiDAR by OEMs all over the world in 2023 or shortly thereafter.

LiDAR plays a critical role in autonomous vehicles to perceive surrounding environments and make intelligent decisions. The safety and reliability of autonomous vehicles highly depend on the trustworthiness of the LiDAR perception. A critical question is how safe LiDAR systems are facing surrounding physical signals. Numerous studies [55], [70], [19], [43], [31], [18] indicate that LiDAR can be compromised by lasers. However, with lasers operating on the same physical channel, attacks typically target the photoelectric sensor in the ToF circuit, and the attack principle focuses on the transduction process. To explore a more expansive set of attack vectors besides the laser signals, we propose and investigate the possibility of the **cross-modality signal attacks**. A recent work [17] demonstrates that EMI can compromise LiDAR's ToF circuits and induce attack effects of "sensor data perturbations". Overall, all previous works compromise LiDAR by attacking the circuits or photoelectric sensor in ToF module. Whether there are new vulnerabilities and new attack surfaces against lidar systems remains an open question.

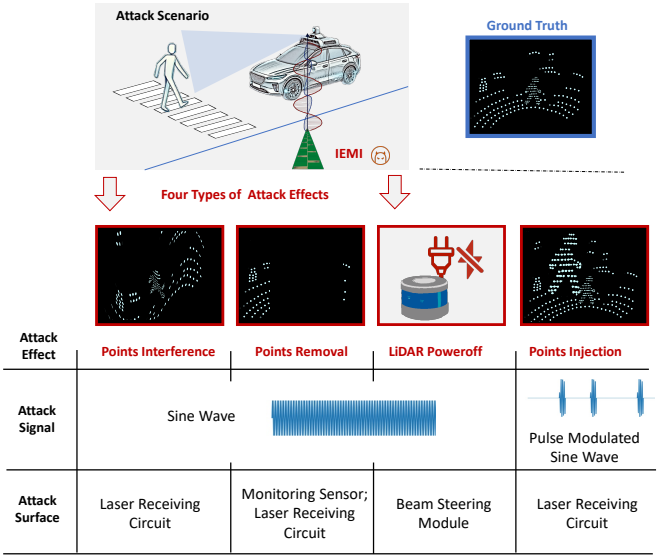


Fig. 1: **Illustration of the PhantomLiDAR attack.** By injecting different signals into diverse attack surfaces, i.e., the laser receiving circuit, the monitoring sensor, and the beam steering module, PhantomLiDAR can succeed in achieving the *Points Interference, Points Removal, Points injection*, and even *LiDAR Power-Off* attacks.

In this paper, our goal is to explore novel attack vulnerabilities and new attack vectors for compromising LiDAR using IEMI. The challenge of achieving this goal is considerable for two reasons: (1) Exploiting novel attack vulnerabilities proves difficult owing to the robust encapsulation and tamper-proof features of commercial off-the-shelf (COTS) LiDAR systems, which conceal their internal mechanics and complicate the analysis of underlying principles. (2) LiDAR systems typically exhibit resistance to IEMI due to rigorous Electromagnetic Compatibility (EMC) testing and the incorporation of anti-interference designs, such as shielding and layout optimization, which mitigate IEMI effects.

To tackle these challenges, we systematically analyze the

* Xiaoyu Ji is the corresponding author

Network and Distributed System Security (NDSS) Symposium 2025
24-28 February 2025, San Diego, CA, USA
ISBN 979-8-9894372-8-3
https://dx.doi.org/10.14722/ndss.2025.230997
www.ndss-symposium.org

LiDAR's internal architectures by referring to reverse engineering reports [37], [74] and infer that the monitoring sensors (e.g., temperature sensors [77],hall effect sensors [80]) and the beam-steering module can be good candidates to couple with EMI signals. Then, we establish a set of high-performance EM attack devices with a broad frequency range to experimentally search for vulnerabilities. Subsequently, we identify attack surfaces by utilizing the fault detection and diagnostic (FDD) mechanism and conducting validation experiments on LiDAR's internal circuits. Through these steps, we discovered two new attack surfaces: monitoring sensors (temperature sensors and hall effect sensors) and the optical encoder in beam steering module. Based on this, we can achieve novel attack effects such as points removal and LiDAR power-off.

Furthermore, to explore the feasibility of skillfully manipulating LiDAR systems using EM signals for precise control, we experiment with injecting controllable points into the LiDAR system. Previous efforts [55], [70], [19], [43], [31], [18] in this domain typically involved using lasers which forge LiDAR echoes to inject controllable points. However, directly employing the same method with EM signals to forge LiDAR echoes faces the challenge of signal coupling into the circuit. To overcome this challenge, we utilize amplitude modulation (AM). We identified an appropriate carrier frequency and modulated the fine-grained baseband signal onto the sinusoidal carrier signal, thereby achieving effective signal injection. Through this method, we successfully managed to inject controllable points using EM signals. In this paper, only the points injection attack requires signal amplitude modulation.

In general, as illustrated in Fig. 1, we successfully implemented four types of attacks: 1) **Points Interference.** By injecting EMI into laser receiving ciruit, we can introduce errors (up to 10cm in this paper) in LiDAR ranging, thereby distorting the point cloud. 2) **Points Removal:** By injecting EMI into monitoring sensors or laser receiving ciruit, this attack causes the point cloud to deviate significantly from its true position or to disappear completely. The effect can be applied to part or all of the point cloud. 3) **LiDAR Power-off:** By injecting EMI into beam steeing module, this attack causes the LiDAR system to shut down and stop working. Even after the attack stops, the LiDAR system must be manually rebooted before it can resume operation. 4) **Points Injection:** By injecting amplitude-modulated EMI into laser receiving ciruit, this attack allows for the injection of controllable points.

Among these, *Points Removal*, *LiDAR Power-off* and *Points Injection* are three new attacks. Additionally, the *Points Interference* attack enhances the attack capability established in previous work [17]. We hope that the increased types of attack effects and enhanced attack capabilities can help the security community and LiDAR manufacturers accurately recognize the threats posed by EMI to LiDAR systems. This recognition should further promote the establishment of more advanced EMC standards and the design of more secure LiDAR systems.

To evaluate the PhantomLiDAR attacks, we explore the IEMI vulnerability on five COTS LiDAR systems including three rotating LiDARs and two MEMS LiDARs. To better understand the advantages and limitations of the four types of attacks, we designed unique evaluation methods for each. We evaluate the attack in both emulated and real-world setups on five 3D object detection models, considering the impacts of attackers' location and aiming. Notably, we validate that PhantomLiDAR can hide a targeted object even when the attack distance is 5 meters away. In addition, PhantomLiDAR can inject over 16,000 fake points in the VLP-16 LiDAR, a quantity that is five times greater than that achieved by SOTA laser-based attacks [43], which could inject less than 3,000 fake points in the VLP-16 under the same rotation speed. What's more, we conduct feasibility experiments in moving scenarios.

We summarize our main contributions as follows:

- **Attack Surfaces:** As far as we know, we are the first to propose the attack surfaces of monitoring sensors and optical encoder in beam-steering module on LiDAR.
- **Attack Effects:** We propose three new attack effects including *Points Removal*, *LiDAR Power-off*, and *Points Injection*.
- **Attack Capabilities:** The *Points Interference* show 2x stronger interference capability compared to SOTA works. The *Points Removal* can hide a target remotely without precise aiming. The *LiDAR Power-off* can success on popular mehchanical LiDAR VLP-16 and MEMS LiDAR RS-M1. *Points Injection* can inject controllable points number 5x more than SOTA laser-based attacks.
- **Experiments:** We conducted experiments on five COTS LiDAR systems. For the four types of attacks, we designed specific simulated and real-world experiments to better evaluate their effectiveness and limitations.

II. Background

A. LiDAR System

LiDAR provides precise 3D spatial information through point cloud data. Fig. 2 illustrates the main components of a typical lidar, which include an emitter-receiver pair (or pairs). During a ranging process, the main board controls the emitter to emit the laser signal, and its direction and firing time τ_0 are registered. The laser pulse travels through air, and when it hits an object, a portion of that energy is reflected and received by the paired receiver. The light signal is then converted into an analog electrical signal through a photoelectric sensor. After passing through an amplifier, filter, and ADC, the analog signal is transformed into a digital signal that is input into the FPGA. The algorithms within the FPGA can determine the receiving time τ_1 and intensity of the echo signal. The range R is measured based on the round-trip delay of light to the target:

$$R = \frac{1}{2} c \cdot (\tau_1 - \tau_0) \tag{1}$$

where c is the speed of light in the medium (e.g., air) between the LiDAR and the target. This process is called Time-of-Flight (ToF) ranging. Based on this equation, the lidar-based range measurement is equivalent to measuring the round-trip delay of light waves to the target. This is achieved by modulating the intensity, phase, and/or frequency of the waveform of the transmitted light and measuring the time required for that modulation pattern to appear back at the receiver.

To create the point cloud, the light should be directed to all the points in a desired field of view (FOV). This can be done by employing a beam-steering unit to scan the FOV. Over the years, many different beam-steering techniques have been developed. Foremost among these are mechanical motion of

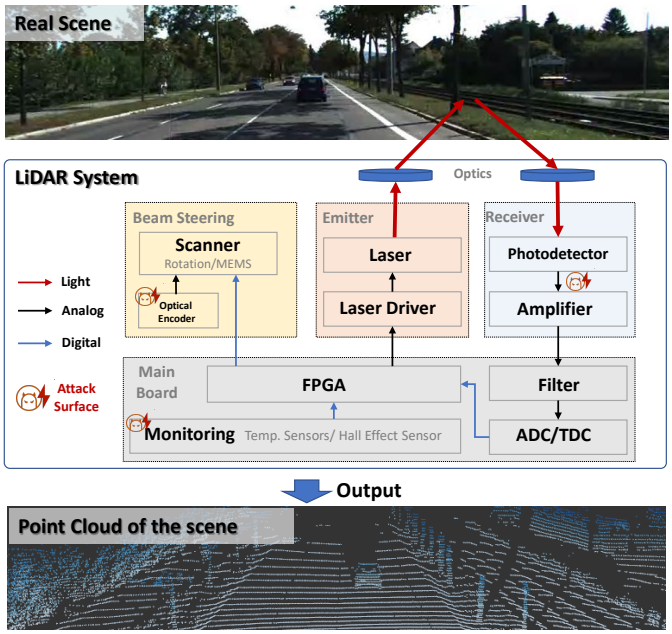


Fig. 2: **LiDAR System.** A typitcal LiDAR system includes one (multiple) emitter-receiver pair (pairs) for ranging, a beam-steering module for laser scanning and a main board for controlling.

the light source [78], [60], [32]; deflection of the light using a macro [36] or micro-mechanical mirror [62]; optical-phased arrays [84]. To date most commercially available LiDAR system have been direct detection time-of-flight (ToF) sensors operating at 905 nm using mechanical motion or mirrors for beam steering [38], [68]. In our study, we primarily focus on these commercially available LiDAR systems, as they are broadly utilized in today's autonomous vehicles. There is usually an optical encoder in the beam steering module to monitor the running state of the motor.

In addition to the aforementioned components related to point cloud generation, LiDAR manufacturers typically incorporate state monitoring sensors to oversee the operational status of these modules, such as the state of supply voltage (hall effects sensor), temperature. In this paper, we experimentally validate that the receiving circuits, the monitoring sensors and the optical encoder can be the attack surfaces for IEMI.

B. LiDAR Fault Detection and Diagnostic

To ensure that the LiDAR operates as intended, the LiDAR manufacturers typically utilizes fault detection and diagnostic (FDD) [15], [30] mechanisms to ensure these modules function as intended. If a LiDAR system fails to operate as expected, it could potentially cause damage. For instance, excessive laser emission power or a motor malfunction leading to continuous laser exposure on a single spot could pose risks to the eyes. Therefore, for the protection of both people and the LiDAR system itself, FDD and response mechanisms are often integrated into the design of the LiDAR.

According to the patents released by LiDAR and car manufactures [33], [59], [49], manufacturers categorize common LiDAR faults and classify them based on severity and consequences into two levels: Level 1 (L1) faults are those with lower impact. The LiDAR can continue to operate under

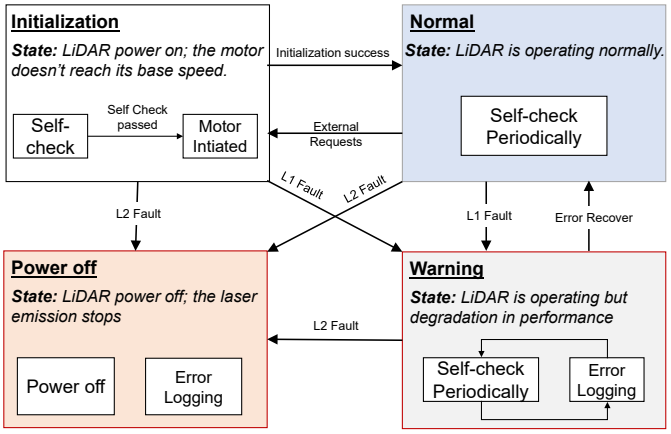


Fig. 3: **LiDAR fault detection and diagnostic.** There are four typical states during LiDAR operation: Initialization, Normal, Warning, and Power-off. A LiDAR system may alternate among the four operational states when different-level faults are detected.

L1 faults but with reduced performance or parameters; Level 2 (L2) faults are more severe, which either render the LiDAR inoperable or lead to performance degradation beyond acceptable limits. The LiDAR may shut down when the L2 faults are diagnosed. As shown in Fig. 3, there are four typical states during LiDAR operation: *Initialization, Normal, Warning, and Power-off*. A LiDAR system may alternate among the four operational states when faults are detected. When a LiDAR powers on, it first enters *Initialization* and performs self-check. Then the LiDAR activates the motor, and once the motor speed has reached the preset value and the self-check is passed, it enters the *Normal* operating state. In the *Normal* state, the LiDAR periodically performs self-check. If an L1 fault is detected during the *Initialization* or *Normal* states, the LiDAR enters the *Warning* state. If an L2 fault is detected at any state, the LiDAR will enter the *Power-off* state, where it typically shuts down power or communication.

A typical FDD list from an anonymous LiDAR manufacturer is shown in Table. IV in the Appendix. It should be noted that different LiDAR manufacturers may have their own definitions for diagnosing and managing faults in LiDAR systems.

C. Backgroud of IEMI Attacks

The IEMI term is officially defined by the International Electrotechnical Committee (IEC) as "intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing, or damaging these systems for terrorist or criminal purposes" [56]. The adversary should first consider possible ways to couple the IEMI signals into the target to implement a successful IEMI attack. We refer to this process as constructing the coupling channel, and there are three essential components for a coupling channel:

Attack Surfaces is a "wire" that exists in the victim circuit that acts as an unintentional receiving antenna to be interfered with by the malicious IEMI signals. This kind of "wire" can be analog electrical traces on the printed circuit boards (PCB) [45], [23], [75], [41], [46], [82], [27] or the

digital sensory communication channel between the sensor and controller [40], [39].

Coupling Path decides how the IEMI generated by attackers reaches the victim device. The selection of coupling paths largely depends on the target coupling interface to achieve the best coupling efficiency. There are two categories of coupling paths: radiated and conducted. Radiated coupling propagates electromagnetic energy through the air or vacuum without making any physical contact with the target, such as magnetic coupling (changing magnetic fields (H-fields)), electrical coupling (changing electric fields (E-fields)), and electromagnetic coupling (changing both magnetic and electric fields (EM-fields)). Conducted coupling propagates electromagnetic energy from an electromagnetic source to a coupling interface via wire conduction [85].

IEMI Sources. To deliver the IEMI signals into target systems efficiently, attackers need to generate IEMI signals at frequencies that are compatible with the electrical characteristics of the target systems and at suitable amplitudes that can change system data in the desired manner.

III. Threat Model

A. Attack Goal

The attacker's goal is to diminish the reliability and performance of LiDAR systems by stealthily interfering with the point cloud or LiDAR operating status using EM signals. Specifically, we consider 4 types of attacks:

- **Points Interference:** The goal of this attack is to introduce errors in the distance measurement of the LiDAR.
- **Points Removal:** The goal here is to significantly displace the point cloud of an object from its actual position or to completely erase it, consequently preventing the LiDAR-based perception models from detecting the object.
- **LiDAR Power-off:** The effect of this attack is to shut down the LiDAR, rendering it inoperative. Even after the attack stops, the LiDAR requires a reboot to resume functioning.
- **Points Injection:** This attack focuses on injecting false points with controllable positions and patterns.

B. Attacker's Capability

We consider the attacker with the following assumptions.

EM Attack Capability to the LiDAR. The attacker can transmit EM signals to the LiDAR in the victim autonomous cars or robots remotely without attaching any hardware or software on the target LiDAR systems. To achive it, we assume the attacker is equipped with commercial devices that can generate EM signals including an RF antenna, a signal generator and an RF power amplifier. The attack devices can be set up in the attacker's car, allowing the attacker to follow the victim vehicle and conduct EM injection attacks within a certain distance. They can also park on the roadside to attack passing vehicles or those stopped at red lights.

Budget-related Considerations. Attackers may require high-end devices to perform wide-frequency range sweeps in order to identify the vulnerabilities of LiDAR systems. Once these vulnerabilities are identified, lower-cost attack devices can be used to carry out the attack.

LiDAR Parameter Awareness. We assume the attacker knows the model of the target LiDAR, and she may obtain a similar substitute LiDAR for assessment beforehand. For example, she may implement frequncy sweep experiments on the substitude LiDAR to find a vulnerability frequency offline before officially implement attack.

Black Box. The adversary does not have access to the machine learning model or the perception system. Attackers can exploit only the characteristics and vulnerabilities of the sensors to achieve their attack target.

IV. Preliminary Study: Feasibility and Vulnerability Analysis

In this section, we first investigate the feasibility of efficient electromagnetic injection and its potential attack effects on LiDAR systems. Subsequently, we analyze the principle of various attack effects.

A. Attack Intuition

There are two attacks intuitions can be formulated that can potentially compromise LiDAR: direct attack and indirect attack.

Direct Attack: From Sec. II-A, we learned that a LiDAR point is generated by a ToF ranging process, in which a laser signal is converted into an analog electrical signal by a photodetector in the receiving circuit. Therefore, a direct way to compromise the point cloud is to interfer with the analog signal in the receiving module, directly affecting the LiDAR's ranging mechanism and subsequently disrupting the point cloud.

Indirect Attack: From Sec. II-B and Table. IV, we learned that when the FDD mechanism of a LiDAR detects a fault, the LiDAR enters an abnormal self-protection status, in which it may treat the point cloud as invalid or even shut down. Therefore, it may be feasible to compromise other modules in LiDAR, e.g., temperature sensors [77], power supplies[80], and optical encoder in the beam-steering unit [71]. This may induce the LiDAR to detect errors, triggering the FDD's inherent operations, forcing the LiDAR into fault recovery, and thereby leading to denial of service or even shut down.

B. Feasibility of IEMI attack on LiDAR

When we attempt to inject EM signals to compromise a LiDAR, we consider the LiDAR's analog electrical traces on the PCB and the electric wire as receiving antennas. The frequency of the EM signal determines the efficiency of its reception by a specific antenna. Theoretically, we can estimate the resonant frequency where the maximum coupling efficiency occurs based on the length and shape of the targeted/selected antenna [58]. However, accurately calculating the signal frequency is challenging due to the unknown nature of the target antenna in LiDAR. To address this challenge, one of the most commonly used methods is frequency sweep.

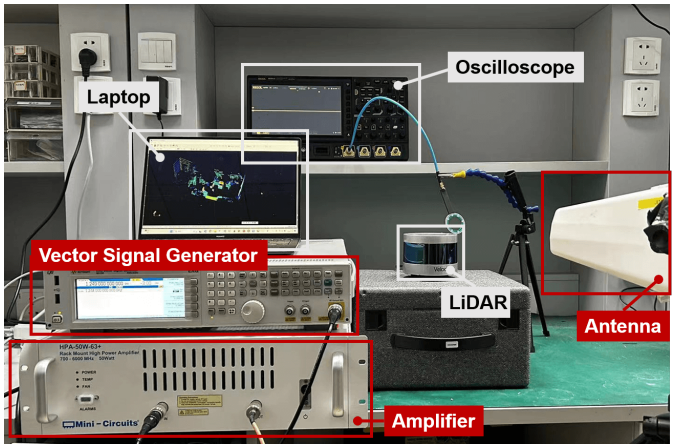


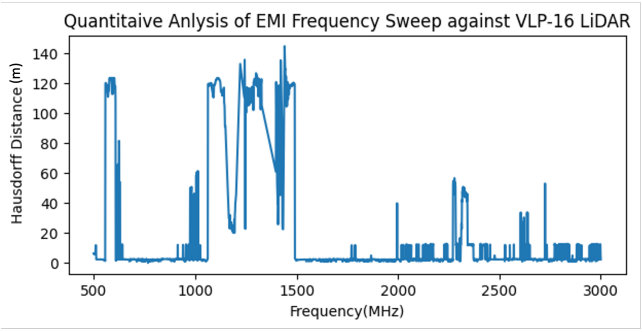
Fig. 4: **The testbed for IEMI attack against LiDAR**

1) Setup: The experimental setup for the feasibility study is shown in Fig. 4. The attack devices include a Keysight N5712b vector signal generator for EMI signal generation, a Mini-Circuits HPA-50W-63+ power amplifier for amplifying the EMI signal, and a log-periodic antenna for signal transmission. The LiDARs under test is the VLP-16 [78], which is the most popular LiDAR in related work [70], [19], [43], [17].

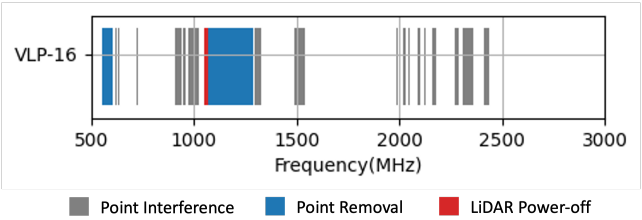
We conduct frequency sweep ranging from 500 MHz to 3500 MHz with an interval of 1 MHz. The signal generator output is set at 0 dbm with an amplifier gain of 50 W. The video demo of the frequency sweep can be found on the website [16]. We record the point cloud and observe the running status of LiDAR under EMI at various frequencies. Both quantitative calculation and attack effects analysis are employed to present the results of the frequency sweep.

2) Quantitative Analysis: In the quantitative analysis, we utilize the parameter *Hausdoff distance* [35] between the benign point cloud and the interfered point cloud to quantify the level of distortion for point clouds under IEMI. In mathematics, the Hausdoff distance measures how far two subsets of a metric space are from each other. Consider the benign point cloud $\mathbb{PC}$ and the interfered point cloud $\mathbb{PC}'$, the Hausdorff distance between them is denoted as $D_H(\mathbb{PC}, \mathbb{PC}')$. A larger value of $D_H(\mathbb{PC}, \mathbb{PC}')$ indicates a stronger degree of interference by IEMI on the LiDAR system. During the sweep process, apart from the varying frequency of the EM signal, we strive to maintain a consistent laboratory environment. After recording the point clouds during frequency sweep, we calculate the Hausdorff distance between point clouds at each frequency ranging from 500 MHz to 3500 MHz and the benign point cloud. The results, as shown in Fig. 5(a), reveal that many different frequencies can cause significant interference effects. For instance, at frequencies around 1200 MHz, the Hausdorff distance reaches as high as 120 meters. Observing the point cloud under 1200 MHz EMI, we find that all points have been erased. In summary, the quantitative analysis of frequency sweep validates the feasibility of EMI attacks on LiDAR. However, to systematically investigate the principles of these attacks, we also need to focus on the effects of the attacks.

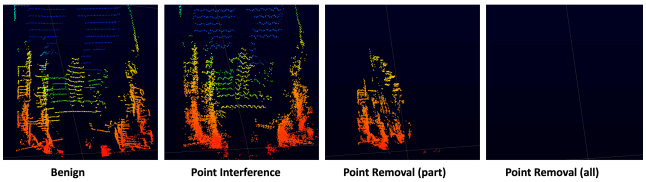
3) Attack Effects Analysis: From quantitative analysis, it can be observed that signals of different frequencies can cause varying degrees of interference with LiDAR point clouds. To



(a) **Quantitative analysis.** We utilize Hausdoff distance to quantify the distortion of point clouds under EMI at various frequencies.



(b) **Attack Effects.** By employing EM signals of varying frequency, we can induce effects such as *Point Interference*, *Point Removal* and *LiDAR Power-off* against VLP-16 LiDAR.



(c) **Illustration of the Attack Effects.** The *Points Interference* and *Points Removal* on VLP-16. Best viewed on a screen and zoomed in.

Fig. 5: **Feasibility Experiments.**

systematically analyze the principles of attacks, we categorize them based on the extent of interference in the point clouds under EMI and the changes in the operational state of the LiDAR. The attack effects are intuitively categorized as *Points Interference*, *Points Removal*, and *LiDAR Poweroff*. The results of attack effect analysis on VLP-16 are presented in Fig. 5(b).

The criteria for categorising attack effects are presented below. In a static environment, we measure the Euclidean distance between points on the same ray before and after an attack. If the average Euclidean distance is less than 2 cm, we consider the LiDAR unaffected by Electromagnetic Interference (EMI), given that the inherent range accuracy of LiDAR is 2 cm. If the average Euclidean distance is greater than 2 cm but less than 1 m, we define this type of attack effect as *Points Interference*. Should the average Euclidean distance exceed 1 m, it implies that the points have been displaced from their original positions, leading us to categorize this effect as *Points Reomval*. *Points Removal* can affect either part or all of the point cloud. Furthermore, we find that when the electromagnetic frequency is swept to $1040 \sim 1070$ MHz, the VLP-16 LiDAR system shuts down completely and fails to recover even after cessation of the EM attack. The system must be rebooted to resume operation. This type of attack effect is categorized as *LiDAR Power-off*.

C. Principle Analysis and Validation

We analyze and validate the principle of the aforementioned three types of attack effects in this section.

1) Why Points Interference Can be Induced:

Principle Analysis for Point Interference: We propose that the *direct attack* is the primary principle of point interference. As detailed in Sec. II-A, a benign LiDAR signal is typically a laser pulse. When the LiDAR emits a laser pulse, its time-of-shooting and direction are registered. The laser pulse travels through the air until it hits an obstacle which reflects some of the energy, which is returned laser pulse. The distance of the object is calculated by measuring the time interval, so-called time of flight, between the emitted and the returned laser pulse. The time of acquisition is acquired according to the peak of the laser pulse. The point interference principle is illustrated in Fig. 6(a), the EMI can introduce noise into the benign signal by coupling the interfering signal into the wires between the transducer and amplifier. The interfering signal, when superimposed on the benign signal, alters the peak of the echo signal, thereby affecting the LiDAR's ranging. Besides, as shown in Fig. 6(b), we have also observed that when we slightly change the frequency, the interfering patterns will change significantly. This phenomenon is because the injected EM signal approaches or exceeds 1 GHz, and the sample rate of VLP-16's ADC is only 500 MHz, undersampling can lead to aliasing. This results in minor frequency changes altering the interference pattern, a phenomenon that has also been discovered in a concurrent prior work [17]. In our study, owing to the use of different frequencies and powerful devices, we can induce a distance error of up to 10 cm as illustrated in Fig. 6(b), compared to the 4 cm error reported in the prior work [17].

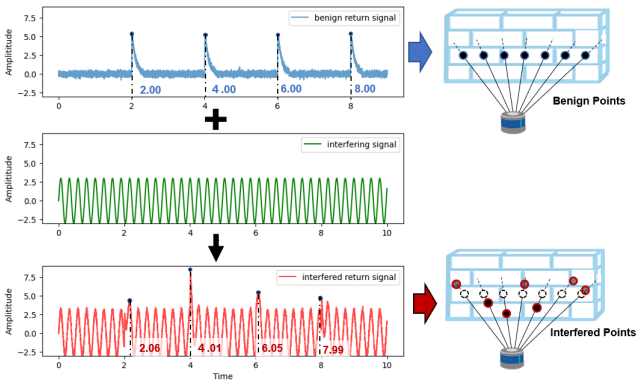
Principle Validation for Point Interference: To validate that the signal could couple into the LiDAR's receiver, we disassembled the LiDAR and extracted its receiving module. We then emitted a 990MHz EM signal towards the receiving module, a frequency capable of causing point interference. We observed that electromagnetic interference was indeed coupled into the transmission line of the receiving board as shown in Fig. 6(c).

2) Why Points Removal can be Induced:

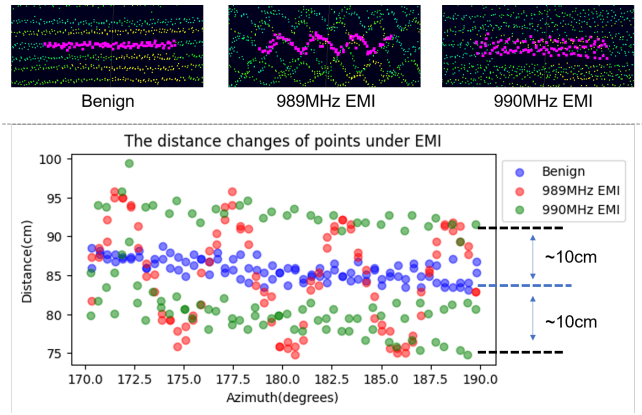
Principle Analysis for *Points Removal*: We propose *direct attack* and *indirect attack* are both potential principles to induce *Points Removal*.

- Attack principle 1 (*direct attack*): if we can inject high-amplitude EM signal into receiving circuit, it may saturate the receiving circuit and make the real laser pulse undetectable.
- Attack principle 2 (*indirect attack*): if we can compromise temperature sensor or hall effect sensor, it may induce LiDAR to detect L1 fault, leading LiDAR to consider some or all of the points as invalid.

Principle Validation for *Points Removal*: We validate the two principles through the Hypothetico-deductive method. If Principle 1 (direct attack) is correct, then when observing *Points Removal* at a certain signal strength and gradually reducing the signal strength, we should observe a gradual recovery of the removed point cloud due to the decreasing amplitude of interference signals coupled to the receiving circuit. If Principle 2 is correct, then when gradually reducing the signal strength to a certain value, a sudden recovery of the point cloud will be observed because at this point, the FDD mechanism no longer detects errors. Experimental evidence demonstrates that at certain frequencies, such as 1.1 GHz, we can indeed observe the gradual recovery of the removed point cloud, confirming that Principle 1 is correct at this frequency. However, at certain frequencies, such as 1.2 GHz, as the EM amplitude decreases, we observe a sudden recovery of the point cloud, indicating that at this frequency, Principle 2 is correct.



(a) **Principle of *Point Interference*.** The sinusoidal interfering signal can be injected into the receiving circuit by EMI, causing minor variations in the peak time of the return signal. This subsequently causes a slight shift in the position of the points, either forwards or backwards. This distance shift is defined as distance error, which can quantify the intensity of *Points Interference*.

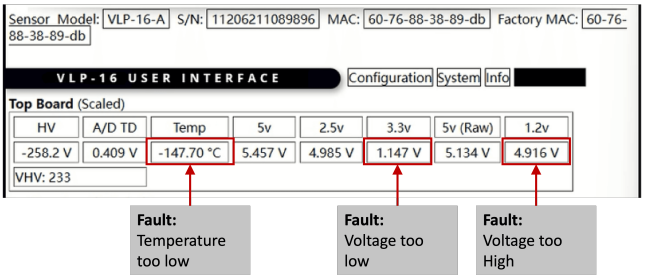


(b) **The patterns of Points Interference.** Due to the aliasing effect caused by ADC undersampling, different frequencies can cause different interference patterns.

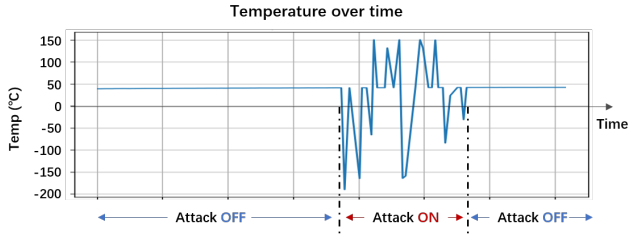
Validation Setup — The Signals on the Receive Borad

(c) **Principle validation.** EMI can couple into the transmission line in the receive board of LiDAR.

Fig. 6: **Points Interference.**



(a) **The diagnostic interface of VLP-16 LiDAR.** Under 1.25 GHz EMI, the value of temperature and voltage will will significantly deviate from their normal values.



(b) **The output of temperature sensor**.When EMI is off, the temperature is around 40 °C. When EMI is on, the temperature is fluctuate between -200°C and 150°C.

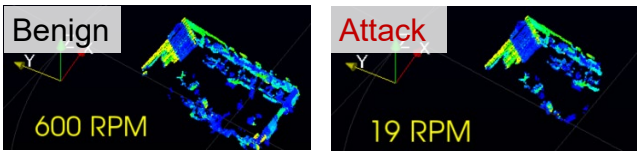
Fig. 7: **Points Removal**

In addition to the Hypothetico-deductive method, we further validate the Principle 2 by directly observing the readings of the monitoring sensor through the fault diagnostic interface. As shown in Fig. 7(a), the diagnostic information can be viewed through the fault diagnostic interface of VLP-16. We find that when EMI causes the points removed, some readings in the diagnostic interface exhibit anomalies. First, as shown in Fig. 7(b), the temperature sensor readings, which should be around 40 Celsius degree, fluctuate between -200 and 150 degrees. Second, some voltage rail readings deviate from normal values. We highly recommend readers to watch the demo video of fault diagnostic when *Points Removal* occurs on the website [16].

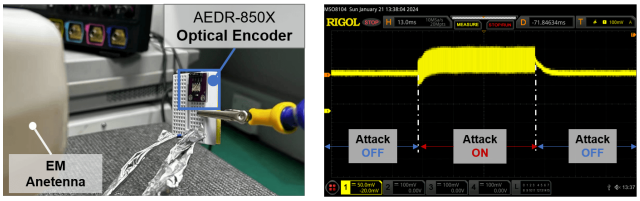
3) Why LiDAR Power-off can be Induced:

Principle Analysis for *LiDAR Power-off*: When EMI causes the LiDAR to power off, and we subsequently stop the attack and reboot the LiDAR, it still operates normally. Therefore, it is clear that we are not causing the LiDAR to power off by damaging the hardware. From Sec. II-B and Fig. 3, we learned that the LiDAR may be forced to shut down when it encounters recoverable severe errors. Therefore, we propose that the *indirect attack* is the principle of *LiDAR Power-off*. Specifically, the *LiDAR Power-off* is triggered by interfering the LiDAR's beam steering module.

Principle Validation for *LiDAR Power-off*: We utilize Wireshark to record communication data of VLP-16 from the onset of the EM attack until the LiDAR shuts down. We find that in addition to some faults that also occurred during *Points Removal*, the LiDAR's rotation speed exhibited severe anomalies. As shown in Fig. 8(a), despite being preset to 600 revolutions per minute (RPM), the speed will drop to 19 RPM, a reduction of 96.7%. Based on our analysis above, such a drastic reduction in speed constitutes a severe fault, highly likely to cause the LiDAR to report an L2 fault and enter the power-off state. We further investigate which part of the beam steering module was disrupted by the EM signal. As shown in Fig. 20, upon disassembling the LiDAR, we discovered that the VLP-16's beam steering module is a rotating motor monitored by an optical encoder AEDR-850X. As shown in Fig. 8(b), we attacks an AEDR-850X with sinusoidal EM signals of 1050 MHz, which is the EM frequency inducing LiDAR Power-off. The test result reveals that EM signals can interfere with the data perceived by the optical encoder, which probably leads the LiDAR to erroneously detect an abnormally low motor speed, thereby causing a power-off.



(a) **The Rotational Speed of LiDAR before Powering Off.** When conduct LiDAR Power-off attack, the rotational speed of VLP-16 LiDAR significantly decreases, then leading to a denial of service, and ultimately resulting in powering off.



(b) **Principle Validation.** The output of optical encoder AEDR-850X can be manipulated by EM signal.

Fig. 8: **LiDAR Power-off.**

V. Controllable Point Injection Design

In this section, we focus on how to inject and precisely manipulate fake (legitimate but erroneous) points with EMI against LiDAR systems. To execute a controllable point injection attack, it is crucial to address the following questions:

- Q1. How to effectively inject EM signal?
- Q2. How to inject fake points?
- Q3. How to control fake points?

For Q1, based on the preliminary study in Sec. IV, the most direct method for precise point cloud manipulation is to inject EM signals into the Time-of-Flight (ToF) circuit, rather than through fault management mechanisms to affect the point cloud. Therefore, the principle of *Points Interference* attacks can be utilized, which is manipulating echo signal of LiDAR to control points. In addition, we investigate the factors that influencing the effectiveness and efficiency of EM injection, including the frequency and amplitude of carrier signals and the types of antenna in different attack distances. Our goal is to identify the optimal conditions for these factors which, when combined, can achieve the maximum intensity of EM injection.

For Q2, the fake points can be injected by forging laser signal echoes. However, unlike the direct forgery of signals

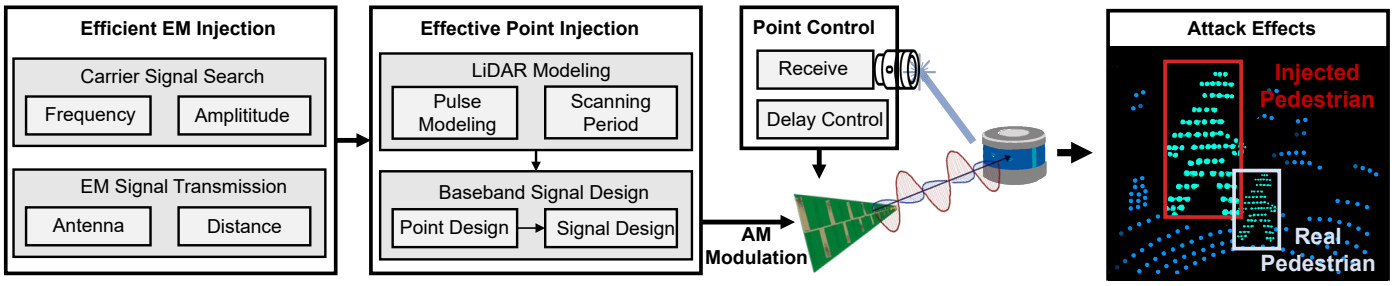


Fig. 9: **The Work Flow of Controllable Point Injection.** First, the adversary identifies the optimal conditions for carrier signal and transmission which, when combined, can achieve the maximum intensity of EM injection. Subsequently, the adversary models the LiDAR parameters and designs a baseband signal capable of injecting points. After synchronization based on the receiver and delay control is completed, the baseband signal is modulated onto the carrier signal through amplitude modulation to generate the attack signal. This attack signal is capable of injecting controllable points.

in laser attacks [43], [19], [70], the transmission and coupling of pulse-shaped electromagnetic waves encounter significant attenuation and distortion. Therefore, we employ signal amplitude modulation (AM), using the designed laser pulse signal as the baseband signal, modulated onto a sinusoidal carrier signal of a resonant frequency.

For Q3, we reference methods from laser-based attack [43], using photoelectric sensors to detect the operational status of LiDAR systems, then set a precise delay to control the timing of EM signal emission, ultimately achieving control over the point cloud.

The workflow of controllable points injection is shown in Fig. 9. The **Efficient EM Injection** module identify the optimal conditions for carrier signal and transmission which, when combined, can achieve the maximum intensity of EM injection. The **Effective Point Injection** Module models the LiDAR parameters and design baseband signal that can inject points. The **Point Control** module introduces a closed-loop feedback mechanism integrating receive and delay control.

A. *Efficient EM Injection*

We utilize a sinusoidal EM signal as the carrier wave. The stronger the intensity of the EM injection, the more likely the forged echo signal is to be perceived as a valid echo, thereby increasing the success rate of fake points injection. Consequently, we are motivated to study the main factors that affect the effectiveness and efficiency of EM injection.

1) Carrier Signal Search: The coupling efficiency between a victim circuit and an EM signal is determined by the frequency and amplitude of the EM signal.

Frequency. When conducting IEMI attacks, we consider the wires in the victim LiDAR system as receiving antennas. The effective EM signal frequency can be estimated based on the electrical length of the targeted/selected antenna [58], [79]. Empirically, if the length of the targeted antenna is l, the optimal coupling frequency of the EM signal lies between $\frac{c}{50l}$and $\frac{c}{2l}$, where c is the light speed. The specific optimal coupling frequency also depends on the shape, material, and other characteristics of the targeted antenna. In realistic attack scenarios, attackers can utilize the aforementioned theory to establish an approximate frequency range and subsequently identify the resonant frequency with higher coupling efficiency through frequency sweep.

Amplitude. The amplitude is a critical factor in EMI, it is generally considered that higher signal amplitude results in stronger interference. In practical experiments, there may be instances where increasing the device's displayed amplitude does not enhance interference. For example, in our experiments, the signal generator's maximum amplitude is 19 dBm (80 mW), and the amplifier is 50 W. However, we observed that changing the signal generator's amplitude (e.g., from 10 dBm to 19 dBm) sometimes does not affect the final output. This is due to the saturation characteristics of the amplifier, which limits the maximum output strength of the signal.

2) EM Signal Transmission: Firstly, the frequency range of the antenna must cover the range of the sweep. Secondly, it is advantageous for the antenna to have as high a gain as possible to reduce signal attenuation. In our experiments, to accommodate various attack distances, we selected two types of transmission antennas. For attack distances less than 10 cm, we choose a near-field probe to generate the EM signal due to its greater portability. For attack distances greater than 10 cm, we opt for a log-periodic antenna due to its superior directionality.

B. *Effective Point Injection*

We inject fake points by forging LiDAR signal echoes. Firstly, we model the LiDAR system, then design the pulsed signal based on the points we intend to inject. Finally, we modulate the pulsed signal onto a sinusoidal carrier signal.

1) LiDAR Modeling: For the target victim LiDAR, we need to acquire the necessary information to guide signal design. First, we must obtain its signal waveform, typically consisting of one or multiple pulses. For instance, the signal of VLP-16 is a pulse with a width of about 10 ns. Then, we need to determine the LiDAR's scanning cycle, which is usually available in the data manual. For example, the VLP-16 operates on a cycle of 55.296 μs, during which 16 laser lines are emitted and received at intervals of 2.304 μs in a specific sequence, followed by a recharge period of 18.432 μs.

2) Baseband Signal Design: The design process of the attack signal involves converting the intended point cloud into a series of pulses, where each pulse corresponds to a spoofing point, and the timing of each pulse's peak defines the spatial coordinates of the spoofing point. The method for designing the baseband signal is akin to that used in previous laser-based attacks [43]. However, using the baseband signal directly is

ineffective for injecting the signal into LiDAR systems through EMI. Therefore, we use the attack signal as the baseband signal and modulate it onto a carrier signal using amplitude modulation (AM) to enable effective injection.

C. Point Control

With the AM-modulated EM pulses, we can inject spoofing points into the LiDAR. However, However, these spoofing points are disorganized and cannot be stabilized in a fixed pattern and position, as shown in Fig. 21 in Appendix. To achieve controllable injection, it is necessary to synchronize the signal with the LiDAR's scanning sequence. Inspired by previous laser-based attack [43], We introduce an integrated receive-delay-fire closed-loop feedback mechanism for point cloud control. we utilize a photoelectric sensor to detect the operational cycle of the LiDAR and adopt the delay control function in signal generator to achieve synchronization.

VI. Evaluation

In this section, We evaluate the effectiveness of the PhantomLiDAR in terms of four types of attacks: *Points Interference, Points Removal, LiDAR Power-off* and *Points Injection*.

A. Evaluation Overview

1) Methodology: As each attack possesses distinct characteristics, we designed unique evaluation methods for each attack to better understand their strength and limitations.

Firstly, in Sec. VI-B, we focus on the *Points Interference, Points Removal,* and *LiDAR Power-off* attacks, as these three attacks posing greater potential threats in real-world scenarios due to their simple implementation. We evaluated the effectiveness of these attacks on five LiDARs and discovered that different LiDARs have varying vulnerable frequencies and show different robustness to IEMI. This experiment may provide insights for future LiDAR design or contribute to the establishment of new electromagnetic compatibility (EMC) testing standards.

In Sec. VI-C, we evaluate the *Points Interference* attack on five LiDAR-based 3D object detection models. We synthesize the *Points Interference* datasets based on the KITTI [2] dataset, which is a large-scale dataset collected from the real world. By conducting experiments on two LiDAR-based models and three fusion-based models, we observed that point cloud interference attacks lead to a degradation in the performance of 3D object detection models.

In Sec. VI-D, we evaluate the *Points Removal* attack in the real world. As Point Removal can completely erase point clouds, it enables the *Hiding* attacks on object detection models, making specified target objects undetectable. With the attack goal of *Hiding* attack, we focus on evaluating the attack impacts of the attacker's distance and angle. Additionally, we evaluated the aiming requirements for EMI attacks. This evaluation highlights an advantage of EM attacks over laser attacks with the reduced need for precise aiming.

In Sec. VI-E, for the *LiDAR Power-off* attack, we evaluate the impact of attack distance and discuss its potential threats in realistic scenarios.

TABLE I: **Attacks on Five LiDARs**

LiDAR	Beam Steering	Laser Pulse	Timing Random	Attack		
				Points Interference	Points Removal	LiDAR Power-off
VLP-16	Rotary	Single	N/A	✓	✓	✓
RS-16	Rotary	Single	Yes	✓	✓	–
RS-Bpearl	Rotary	Encode	Yes	–	✓	–
RS-M1	MEMS	Encode	Yes	✓	✓	✓
RS-M1P	MEMS	Encode	Yes	✓	✓	–

✓ Attack Succeed – Not Observed

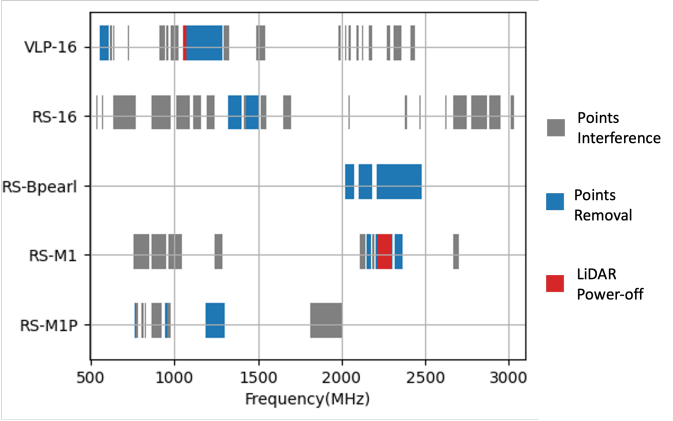


Fig. 10: **Attack effects on five LiDARs and the frequency corresponding to each attack**

In Sec. VI-F, we evaluate *Point Injection* from the maximum number of injected points and the precise control over the points, thereby verifying the effectiveness of the attack.

In Sec. VI-G, we explore the feasibility of hiding a targeted object when the victim LiDAR is in motion.

2) Attack Devices: All experiments in this section utilized shared attack attack devices, including a Keysight N5712b vector signal generator (32K USD) [8] for EMI signal generation, a Mini-Circuits HPA-50W-63+ power amplifier(20K USD) [7] for EMI signal amplification, and a log-periodic antenna for remote signal transmission. The log-periodic antenna, valued at approximately 15 USD [6], has a frequency range of 600MHz to 6000MHz and a gain of 15 dBi. Additional devices specific to *Points Injection* attacks are detailed in Sec. VI-F.

B. Attack on Different LiDARs

1) Victim LiDAR:: We evaluate EMI attacks on five off-the-shelf LiDARs as shown in Fig. 22, which include three mechanical LiDARs (VLP-16 [78], RS-16 [60], RS-Bpearl [61]) and two MEMS LiDARs(RS-M1 [62],RS-M1P [63]). The RS-M1 and RS-M1P, serve as primary LiDARs for perception, and are widely deployed in both currently released [14], [13], [12] and upcoming [3] vehicles.

2) Attack Setup: We put the antenna 30 cm away from LiDARs, and conduct a frequency sweep test on these LiDARs from 500 MHz to 3500 MHz with a step of 5MHz. The output amplitude of the signal generator is 0 dBm and the amplifier is 50 W.

3) Attack Results: The attack results are shown in Table I. The relationship between attack effects and EMI frequency

is shown in Fig. 10. It is observed that LiDARs with different structures exhibit varying vulnerabilities and susceptible frequencies. We did not observe the phenomenon of *Point Interference* attacks on the RS-Bpearl, indicating that its EM protection for received signals is superior compared to the other LiDAR models. *Points Removal* was observed in all LiDAR, but it is important to note that on the VLP-16 and RS-16, EMI could erase all point clouds. However, on the other three LiDAR models, we only observed partial removal of point clouds, which we speculate is due to the directionality of EM waves affecting only certain circuits. As for the *LiDAR Power-off* attack, it was observed only on the older models, VLP-16 and RS-M1, suggesting that newer generations of LiDAR have optimized diagnostic and management of serious faults.

C. Points Interference

1) Impact of Signal Amplitude: To systematically explore the influence of amplitude on point interference, we conducted further experiments on the VLP-16 LiDAR. First, we selected two typical frequencies: 989MHz and 990 MHz. As shown in Fig. 6(b), 989 MHz can produce a sinusoidal pattern, whereas 990 MHz can generate a random pattern. We then increased the signal generator's amplitude from -40 dBm to 0 dBm and connected it to an amplifier with a gain of 56 dB and a maximum output of 50 W (47 dBm). By recording the distance error at different amplitudes, we obtained the results shown in Fig. 11. It can be seen that as the amplitude increases, the distance error gradually increases and the trend is consistent across different frequencies. When the signal generator's amplitude reaches approximately -10 dBm, the distance error reaches around 14 cm at most. However despite further increases in the signal generator's output, the distance error did not increase significantly. This is primarily because the amplifier output reached saturation, preventing accurate control of the final signal amplitude by the signal generator. Furthermore, the saturation distortion caused by the amplifier resulted in signal distortion after -10 dBm, which explains the decrease in distance error around -10 dBm.

2) Evaluation on Large-scale Dataset: To systematically evaluate the impact of Point Interference on 3D object detection models, we simulated the attack based on the large-scale dataset and then input the corrupted dataset into the detection models.

Dataset: We synthesize the attack on KITTI dataset, which comprises diverse real-world driving scenarios. Based on Sec. IV-C1, the Point Interference can be formulated as the following equation:

$$\begin{cases} r_i' = r_i + Random[-\varepsilon, \varepsilon] \\ (r_i, \theta_i, \varphi_i) \in \mathbb{PC}, i \in [1, n] \\ (r_i', \theta_i, \varphi_i) \in \mathbb{PC}', i \in [1, n], \end{cases} \tag{2}$$

where $\mathbb{PC}$ stands for benign point cloud and $\mathbb{PC}'$ stands for compromised point cloud. We represent a point with spherical coordinates (r, θ, φ), where r denotes the radial distance, θ the polar angle, and φ the azimuthal angle. EM interference affects only r, introducing random noise within the range of $[-\varepsilon, \varepsilon]$. As shown in Fig. 11, up to 10 cm distance error can be stably induced based on our attack device. Therefore, to ensure the physical realizability of the corrupted dataset, we synthesize the datasets when ε is set at 5 cm and 10 cm, respectively.

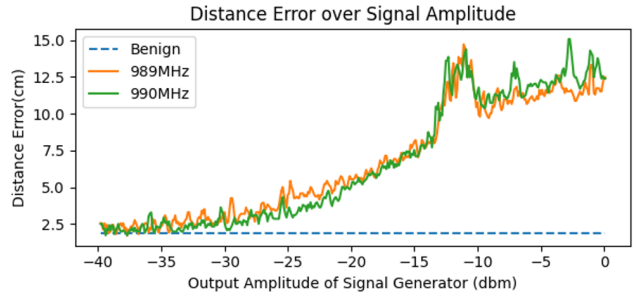


Fig. 11: **Impacts of signal amplitude to distance error of *Points Interference*.** As the amplitude increases, the distance error gradually increases, and the trend is consistent across different frequencies.

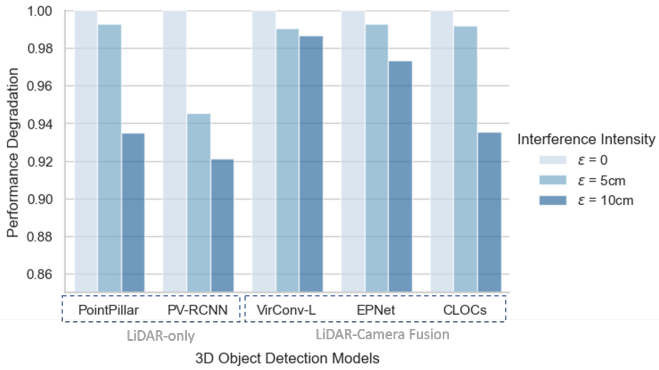


Fig. 12: **Robustness (Rb) of five 3D objection detection models against Point Interference.** The robustness of fusion-based models is generally stronger than that of LiDAR-based models

Detection Models: We evaluate the impact of *Points Interference* on five 3D object detection models. Two are LiDAR-based models: PointPillar [47] and PV-RCNN [69]. Additionally, there are three LiDAR-Camera fusion models: the early-fusion model VirConv-L [81], the feature-fusion model EPNet [34] and the results-fusion model CLOCs [54].

Metrics: Same as the KITTI benchmark [29], we consider a car detection as successful when the IoU between a ground-truth 3D bounding box and a predicted 3D bounding box exceeds 0.7. Based on the IoU threshold, we use Average Precision(AP) to measure the overall detection performance of a model. AP is the official metric for the KITTI benchmark for a comprehensive assessment of a model's performance. We calculate the AP in the moderate difficulty, aligning with the KITTI benchmark [2], where models are ranked based on the moderately difficult results. To evaluate the model's robustness against interference, we introduce a new metric Robustness Coefficient Rb:

$$Rb = \frac{AP'}{AP_{benign}} \tag{3}$$

where AP' and AP_{begnin} denote the model's average precision on the interfered dataset and the benign dataset, respectively.

Results: The APs of the five 3D Object detection models under different-intensity points interference are presented in Table. III. It is observed that with increasing interference intensity, the performance of the detection models decreases,

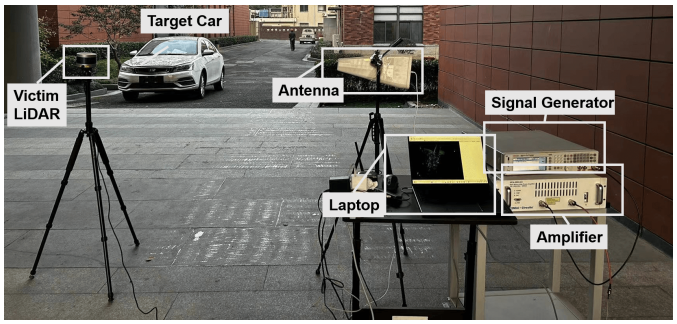
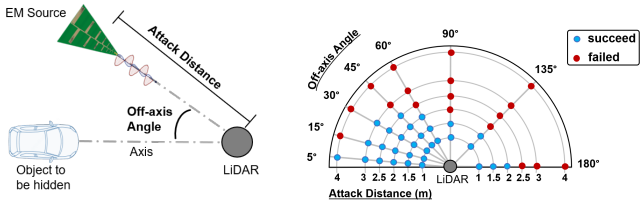


Fig. 13: **The Attack Setup Outdoors.** The attack goal is to attack the victim LiDAR by IEMI, and make the target car undetectable on 3D object detection model.



(a) Illustration of setup (b) Results

Fig. 14: **Impacts of attacker's location.** Within a distance of 1.5 meters, the attacker can hide the target object from any angle. When the off-axis angle is 5°, the attack can succeed beyond 4 meters away (5.5 meters at most in this paper).

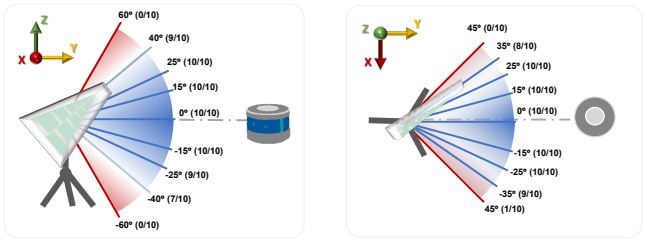
demonstrating the attack devices with higher power can, demonstrating that devices with higher power have stronger attack effects.

The Rbs of models are shown in Fig. 12. The robustness of Fusion-based models is generally stronger than that of LiDAR-based models, indicating that sensor fusion has potential as a countermeasure against Points Interference attacks. Within the fusion-based models, CLOCs exhibits the least robustness. This is attributed to CLOCs being a result fusion approach that combines camera and LiDAR detection candidates before applying Non-Maximum Suppression (NMS). Such a loosely coupled fusion method is ineffective in defending against Points Interference attacks. Further, we note that even interference at 10cm does not significantly compromise the 3D object detection models(Rbs ¿ 0.92), indicating that existing models have a certain level of robustness to interference. This experiment helps us objectively understand that the harmfulness of *Points Interference*

D. Points Removal

The attack goal of *Points Removal* is to hide a target object against 3D object detection model. The efficiency of Point Removal in achieving this goal is unquestionable, as it can completely erase the points representing the target object. Therefore, to gain a more comprehensive understanding of the attack's capabilities, we investigate the impacts of the attacker's location and aiming.

1) Experimental Setup: The experimental setup is shown in Fig. 13. We conducted physical experiments on campus roads. The attack target is a car, which is the most prevalent target in real autonomous driving scenarios. The victim LiDAR is VLP-16, and the detection model is PointPillars [47].



(a) Vertical Angle (b) Horizontal Angle

Fig. 15: **Impacts of Aiming.** The EM antenna could deviate up to 40° vertically or 35° horizontally while still achieving a hiding attack effect. The results show very low aiming requirement for our attacks.

2) Impacts of Attacker's Location: As illustrated in Fig. 14(a), the attacker's location includes their off-axis angle and distance to the LiDAR and the target object. A larger range of locations from which an attack can be successfully executed implies greater robustness and stealth of the attack in real-world scenarios. We investigated the attack's effectiveness by conducting attacks on the LiDAR from distances of $[1, 1.5, 2, 2.5, 3, 4]$ meters at off-axis angles of $[5, 15, 30, 45, 60, 90, 145, 180]$ degrees.

The results are shown in Fig. 14(b). It demonstrates that within a distance of 1.5 meters, the attacker can hide the target object from any angle, as all LiDAR point clouds are erased at this distance. Furthermore, we found that the smaller the off-axis angle, the greater the distance at which an attack can be successful. To find the longest attack distance, we move the EM source as far as possible. With our test setup, the attack could be successfully executed when the EM source was up to 5.5 meters away from the LiDAR. We anticipate that the maximum effective attack distance could be more than 5.5 meters, particularly with the use of a high-power EM source.

3) Impacts of Aiming: Aiming is a common challenge faced in remote attacks in the real world, a problem that has been especially pronounced in previous laser attacks [43]. In this experiment, we investigate the aiming requirements for EM attacks. The lower the aiming precision required for an attack, the more feasible it is in real-world scenarios. We kept the location of the EM antenna constant (1 meter from the LiDAR) and then varied the direction in which the EM antenna was pointed. The point clouds were then input into the detection model to observe whether the attack is successful. The results are shown in Fig. 15, the EM antenna could deviate up to 40° vertically or 35° horizontally while still achieving a hiding attack effect. This result suggests that EM attacks do not require precise aiming, an advantage over laser attacks.

E. LiDAR Poweroff

As analyzed in Sec. IV-C2, the power-off is a protective mechanism employed by LiDAR systems when encountering serious faults. In real-world scenarios, remotely inducing a LiDAR power-off via IEMI could significantly impair the functionality of autonomous vehicles. To explore the realistic threats of *LiDAR Power-off*, we evaluate the impacts of attack distance on VLP-16 and RS-M1. With the attack devices illustrated in Fig. 13, we were able to induce *LiDAR Power-off* against VLP-16 and RS-M1 at distances of 30 cm and 50 cm, respectively. This distance is sufficient to pose a threat in real

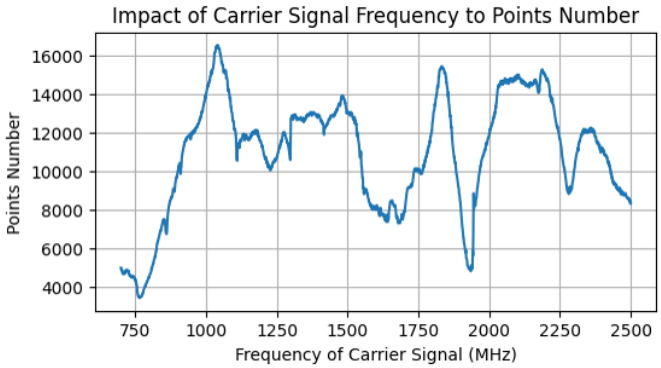
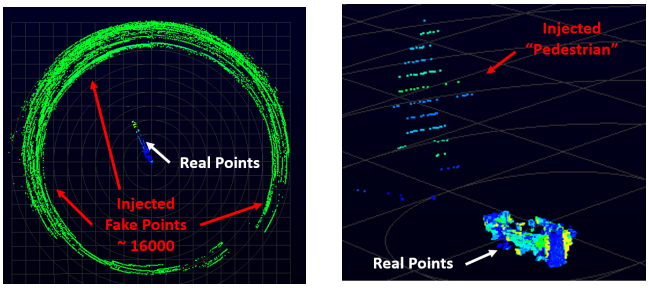


Fig. 16: **Impact of Carrier Frequency to Points Number.**



(a) Maximum Injected Points. (b) Specified Pattern Injection

Fig. 17: **Points Injection with Different baseband signals.** (a) When the baseband signal is a periodic pulse signal, over 16000 controllable fake points can be injected. (b) With a fine-grained baseband signal, the pedestrian-pattern spoofing points can be injected.

life, as it allows for attacks to be conducted from outside a vehicle. We recommend readers to watch the demo video of *LiDAR Power-off* available on the website [16].

A conceivable attack scenario is that an attacker places the amplifier and signal generator inside their vehicle and extends the EM antenna outside through a long wire. When an autonomous vehicle stops, such as at a red light, the attacker could bring the EM antenna close to the LiDAR of the autonomous vehicle, causing it to power off. Then, even if the vehicle moves away, the power-off effect would persist.

F. Points Injection

We evaluate *Points Injection* from two perspectives: firstly, the maximum number of injected points, which has been an important metric in previous LiDAR attacks, and secondly, the control over the points, specifically whether we can inject a point cloud with a specified pattern.

1) Setup: The setup of *Point Injection* is shown in Fig. 23 in Appendix. In addition to a vector signal generator, an amplifier, an EM antenna, Point Injection also requires an arbitrary waveform generator to create the baseband signal and set the delay, and a photodetector to receive signals from the LiDAR. The LiDARs under test are VLP-16 and RS-16, which are the two LiDARs tested in SOTA laser-based attacks [43].

2) Number of Injected Points: The comparison of the number of injected points is only meaningful when the victim LiDAR models are the same and have same rotation speed. Therefore, we selected VLP-16 as the victim LiDAR, a LiDAR commonly used in previous point injection research [43], [19], [70].

To inject as many points as possible, we designed the baseband signal to forge the echo signal in every receiving period of LiDAR. With the same baseband signal, we test the impact of different carrier signal frequencies to the number of injected points. We set the signal output power to 50 W and varied the carrier frequency between 700 MHz and 2500 MHz, recording the number of injected fake points. The results are shown in Fig. 16. We find that different carrier frequencies indeed impact the number of injected points. We attribute this to the receiving circuit's varying response to different signal frequencies. Notably, a carrier frequency of approximately 1040 MHz enabled the injection of the highest number of points (over 16,500), forming a circular wall-like structure around the LiDAR, as shown in Fig. 17(a).At the same rotation speed, previous works could inject 3,000 fake points at most [43], [65]. This significant increase is primarily because EM attacks affect a wider range (almost 360° horizontal angle), while laser attacks can only influence the area (less than 35° horizontal angle) illuminated by the laser spot.

3) Specified Pattern Injection: Fig. 17 shows that different-pattern spoofing point cloud can be injected using various baseband signals. With the fine-grained baseband signal and attack devices detailed in Sec. V, we successfully inject a "pedestrian" pattern into VLP-16 (Fig. 17(b)) and RS-16 (Fig. 21(c)in Appendix) LiDARs. This showcases that EM attacks possess capabilities akin to those of laser-based attacks [43] for precisely manipulating the point cloud of a LiDAR system.

G. Feasibility Experiments on Moving Vehicle

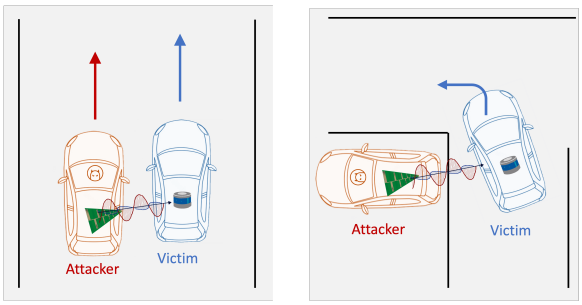
In this section, we explore the feasibility of our attacks when the victim LiDAR is in motion. Videos of attacks can be found at our website [16].

1) Attack Setup: The attack setting of moving vehicles is shown in Fig18. The vehicle equipped with a VLP-16 LiDAR moves at a speed below 10 km/h (for safety considerations). During the experiment, we do not require the victim car to travel at a constant speed, which is in line with the real-world conditions where the attacker has no access to the victim car. The attack devices, including a signal generator, an amplifier, and an antenna, are integrated into the attack car. The attacker holds antenna in the car and aims it at the moving victim LiDAR. The attacker's goal is to compromise the victim LiDAR and make the LiDAR-based 3D object detection model unable to detect the attack car. Therefore, we set the parameters of attack signal to a frequency of 1.2GHz and an output amplitude of 50W, with which the *Points Removal* can be easily achieved.

2) Attack Scenarios: We define two real-world attack scenarios. *Scenario A* is the "tailgating attack", where both the attacker car and the victim car are moving on a straight road, and the driver of the attacker car will drive close to the victim car at a similar speed. *Scenario B* is the "roadside attack", where the attacker is stationary at the roadside while the victim car is making a turn. Compared to the stationary attack in

(a) Attack Setup (b) Attack Devices

Fig. 18: **Experimental Setup for the Attack on Moving Target.**



(a) Tailgating Attack (b) Roadside Attack

Fig. 19: **Two Attack Scenarios.** (a) Tailgating attack: the attacker car drive close to the victim car at a similar speed. (b) Roadside attack: the attacker is stationary at the roadside while the victim car is making a turn.

Sec. VI-D, *Scenario A* primarily faces challenges due to the constantly changing attack distance and vehicle vibrations, while *Scenario B* primarily faces aiming challenges due to the constantly changing attack angle.

3) Results: We demonstrated the feasibility of hiding a specified target in both moving scenarios. Specifically, for the tailgating attack, we conducted five trials, each covering a distance of 40 meters. Each trial collected 100 frames uniformly, resulting in an attack success rate of 87.2% (436/500). For the roadside attack, we also conducted five trials and collected 40 frames from each trial. We found that despite the continuously changing angle of the victim car, an attack success rate of 83.5% (167/200) was still achievable within an attack distance of 4 meters. In summary, due to the relatively low aiming requirement for EM attacks, as long as the attacker can approach the victim LiDAR (within 4 meters in this paper), the hiding attack can be carried out with above 80% attack success rate.

VII. Discussion

A. Comparison with laser-based attack

In this section, we compare EM-based attacks with recent laser-based attacks. It should be noted that the purpose of this comparison is not to determine whether EM-based or laser-based attacks are superior, as such a determination would require a more rigorous benchmark, including identical power levels or equivalent attack costs. Our aim is to provide the security community with a dialectical understanding of the characteristics of both types of attacks and to raise awareness, thereby inspiring more robust hardware design and customized defense strategies.

TABLE II: **Comparison with Laser-based Attacks**

Attack Type	Attack Surface	Attack Effect				Aiming Require.	Attack Distance
		Points Interference	Poionts Removal	LiDAR Poweroff	Points Injection		
Laser-based	photodetector in receiving circuit	-	✓ [43], [18], [64], [73]	-	✓ [55], [70], [20] [72], [43], [64]	High	>30meters
EM-based (Ours)	receiving circuit, monitoring sensor, beam steering module	✓	✓	✓	✓	Low	4 meters

We compare attacks in terms of attack surfaces, attack effects, aiming requirements, and attack range, as shown in the Table II. Overall, `PhantomLiDAR` exploits more attack surfaces than laser-based attacks to achieve a wider variety of attack effects and has the advantage of not requiring precise aiming. However, it is inferior to laser-based attacks in terms of attack distance.

B. Feasibility Evaluation with Cheaper Hardware

In the aforementioned experiments, we utilized high-end equipment to conduct wide-range frequency and amplitude sweeps, enabling us to identify new LiDAR vulnerabilities to IEMI signals. However, in practical scenarios, attackers could employ lower-cost equipment with a specific frequency signal generator and amplifier, which can also achieve the desired attack outcomes. To further discuss the practicality of the attack in terms of cost, we conducted experiments using lower-cost equipment. Our first lower-cost setup, as shown in Fig. 24(a) included a 35MHz-4400MHz signal generator board($25 [5]) and a 1080MHz-1360MHz, 50W amplifier ($128 [4]). This $168 atatck setup enabled us to achieve *Points Interference*, *Points Removal* and *LiDAR Power-off* on the VLP-16 LiDAR.However, due to the inability of this setup to support amplitude modulation, *Points Injection* was not feasible. Our second lower-cost setup, as shown in Fig. 24(b), included a USRP B210($2160 [11]), a 50W amplifier($128) and an antenna ($15). Using this $2300 setup where the USRP B210 supports signal amplitude modulation, we successfully conducted all four types of attack effects, including *Points Injection* attack.

C. Countermeasures

When utilizing LiDAR in safety-critical scenarios, countermeasures against *PhantomLiDAR* attacks can be implemented through the following approaches:

EMC Reinforcement: The attack interfaces of *PhantomLiDAR* are the analog portion of the LiDAR. There are three common defenses [46] to reinforce the EMC of analog circuits: shielding, differential comparators, and filters. Shielding involves the application of a conducting material to shield a component from EMI. Where shielding is either not possible or not sufficient, a reference signal can be used to remove the common mode voltage using a differential circuit [57]. Additionally, a filter that attenuates signals outside a sensor's baseband frequency can reduce the vulnerable frequency range of that sensor. However, these methods can increase the complexity and cost of LiDAR circuits. While COTS LiDAR systems undergo rigorous EMC testing before shipment, the experiments in this paper demonstrate that adversaries can easily compromise LiDAR with commercial devices. Therefore, it may be prudent to consider updating the EMC standards for LiDAR systems.

Multi-Sensor Fusion: This paper demonstrates through experimentation in Sec. VI-C that fusion models show promise in mitigating the effects of the attack. In terms of autonomous vehicles, perception can be enhanced by the fusion of camera and LiDAR, and by equipping multiple LiDARs to increase safety redundancy. Therefore, how multiple sensors can better cooperate and complement each other presents an intriguing research question worth exploring[42].

D. Future Work

Although this paper extensively evaluates the *Phantom LiDAR* attack in a physical world setting, it has not been tested on commercial autonomous vehicles equipped with LiDAR. Such an effort may require authorization and collaboration with automotive manufacturers. Due to the integration of multiple sensors and the presence of multiple safety assurance measures[1] in commercial vehicles, we believe that end-to-end testing of PhantomLiDAR on autonomous vehicles could yield novel and interesting effects, which we will investigate in future research.

E. Responsible Disclosure

We have disclosed the EM vulnerability discovered in this work to the relevant product security teams [9], [10], and provided the experimental steps to reproduce the attacks. In addition, we suggested some potential methods to mitigate our attacks.

VIII. Related Work

A. LiDAR Security

The output of LiDAR (i.e. point cloud) can be manipulated by laser and 3D object. Based on the inherent vulnerability of photoelectric sensors, saturation attack against LiDAR can be easily induced by high-power continuous laser [70]. After the iterative efforts of several papers [55], [70], [19], [72], the latest literature [43] proves that a large number of controllable points can be injected into the mechanical (spinning) LiDAR through carefully designed laser pulses, and physically validates the feasibility of hiding attack and creating attack. However, since lasers share the same physical channel as LiDAR, the ability of lasers to compromise LiDAR systems is an unavoidable phenomenon. This makes it challenging to propose improvements to the safety design of LiDAR systems that would fundamentally prevent laser attacks. Additionally, since laser attacks generally face aiming concerns, the real-world threats of laser attacks has not been widely recognized. The way of using 3D objects to manipulate point clouds is also very popular. There are mainly two methods: 3D printing objects and placing arbitrary objects. 3D printing object can realize the adversarial point cloud of specific shape in the physical world, and make the attack difficult to be aware by human beings while spoofing the victim detection model [20], [76], [83]. Some studies have found that for the adversarial attack that aims to hide a target, the position of the adversarial points is more critical than the shape, thus the adversarial effect can be realized by placing the arbitrary object at the specified position [87], [86]. A recent work [17] demonstrates that EMI can compromise LiDAR's ToF circuits and induce attack effecrs of "sensor data perturbations". Compared to this work, `PhantomLiDAR` demonstrates 3 new attack effects with new attack surfaces and signal design methods.

B. IEMI Attacks on Cyber-physical Systems

Intentional electromagnetic interference (IEMI) attacks can induce parasitic current or voltage into the target cyber-physical systems to manipulate their output data or gain unauthorized access [77], [48], [46], [44], [21], [48], [25], [26], [50], [79], [67], [28], [41], [51], [40], [17], [39], [53], [52], [66], [24], [22] and have been of vital interest in recent years. For example, existing works use IEMI attacks to change the output of microphones [46], [44], [21], [48], [25], [26], touchscreen [50], [79], [67], [28], keyboard [41] and smart lock [51] to allow attackers to inject false speech audios and user inputs, often to pretend that a real user is interacting with the smartphones or computer systems. Besides, IEMI attacks are also frequently used to change how autonomous systems perceive their surrounding environment, e.g., by changing the output of camera [40] and inertial measurement units [39], [53], [52], [24] on autonomous vehicles.

IX. Conclusion

In this paper, we uncovered and experimentally validated new vulnerabilities in LiDAR systems, including novel attack surfaces and attack causalities. We validated that the receiving circuit, monitoring sensors(temperature sensor), and optical encoder in beam-steering module in LiDAR can serve as EMI attack surfaces. We identified two primary causalities: direct interference with ranging due to EM coupling into the receiving circuit, and indirect compromise of LiDAR by exploiting its fault management mechanisms. Based on the new attack surfaces and attack principles, we introduce four types of EM-based attacks against LiDAR. To the best of our knowledge, we are the first to design and propose *Points Removal*, *LiDAR Power-off*, and *Points Injection* attacks with EMI. Additionally, compared to prior SOTA works, our attack capabilities show significant improvements in terms of the ranging errors (2x more) and the number of fake points (5x more). Comprehensive experiments conducted on five LiDARs and five models demonstrate the efficacy of our attacks. The attack's practical threat is evidenced by its considerable attack distances, its low aiming requirements, and its feasibility in moving scenarios. In addition, we discussed the countermeasures proposed against our attacks. We hope our research can enhance future LiDAR systems by considering a wider range of attack vectors. Future directions include exploring the feasibility of PhantomLiDAR on autonomous vehicles.

X. Acknowledgments

This work is supported by NSFC (Natural Science Foundation of China) Grant 61925109, 62222114, 62071428 and 62201503. We would like to thank Weiying Kong, Yubo Qu and Yu Wang for providing valuable feedbacks on our work. The views and conclusions contained in this paper are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the NSF.

REFERENCES

[1] "Iso26262:2018," https://www.iso.org/standard/68383.html, 2018.

[2] "Kitti benchmark," https://www.cvlibs.net/datasets/kitti/index.php, 2023.

[3] "Rs-m1: Nominated orders for more than 60 models," https://www.robosense.cn/en/rslidar/RS-LiDAR-M1, 2023-12-18.

[4] "1.2ghz 50w amplifier," https://www.aliexpress.us/item/3256807300998703.html, 2024.

[5] "35mhz-4400mhz rf signal generator adf4351," https://www.aliexpress.us/item/3256806804711048.html, 2024.

[6] "698-2700mhz 16dbi lte outdoor antenna," https://www.aliexpress.us/item/3256803272069914.html, 2024.

[7] "Hpa-50w-63+," https://www.minicircuits.com/pdfs/HPA-50W-63+.pdf, 2024.

[8] "N5172b exg x-series rf vector signal generator," https://www.keysight.com/us/en/product/N5172B/exg-x-series-rf-vector-signal-generator-9-khz-6-ghz.html, 2024.

[9] *Ouster, Inc.*, https://ouster.com/products/hardware/vlp-16, 2024.

[10] *RoboSense Technology Co., Ltd*, https://www.robosense.ai/en, 2024.

[11] "Usrp b210," https://www.ettus.com/all-products/ub210-kit/, 2024.

[12] "Xiaopeng g9," https://www.xpeng.com/g9, 2024.

[13] "Yangwang u8," https://www.yangwangauto.com/car-type.html, 2024.

[14] "Zeeker 007," https://www.zeekrlife.com/zeekr007, 2024.

[15] A. Abid, M. T. Khan, and J. Iqbal, "A review on fault detection and diagnosis techniques: basics and beyond," *Artificial Intelligence Review*, vol. 54, no. 5, pp. 3639–3664, 2021.

[16] Anonymous, *The website of PhantomLiDAR*, https://sites.google.com/view/phantomlidar, 2024.

[17] S. H. V. Bhupathiraju, J. Sheldon, L. A. Bauer, V. Bindschaedler, T. Sugawara, and S. Rampazzi, "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*, 2023, pp. 329–340.

[18] 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.

[19] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial sensor attack on lidar-based perception in autonomous driving," in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 2267–2281.

[20] Y. Cao, C. Xiao, D. Yang, J. Fang, R. Yang, M. Liu, and B. Li, "Adversarial objects against lidar-based autonomous driving systems," *arXiv preprint arXiv:1907.05418*, 2019.

[21] D. Dai, Z. An, and L. Yang, "Inducing wireless chargers to voice out for inaudible command attacks," in *Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP)*.

[22] G. Y. Dayanıklı, "Electromagnetic interference attacks on cyber-physical systems: Theory, demonstration, and defense," Ph.D. dissertation, Virginia Tech, 2021.

[23] G. Y. Dayanikli, R. R. Hatch, R. M. Gerdes, H. Wang, and R. Zane, "Electromagnetic sensor and actuator attacks on power converters for electric vehicles," in *Proceedings of the 2020 IEEE Security and Privacy Workshops (SPW)*.

[24] G. Y. Dayanıklı, S. Sinha, D. Muniraj, R. M. Gerdes, M. Farhood, and M. Mina, "Physical-layer attacks against pulse width modulation-controlled actuators," in *Proceedings of the 31st USENIX Security Symposium (USENIX Security 22)*, 2022.

[25] J. L. Esteves and C. Kasmi, "Remote and silent voice command injection on a smartphone through conducted iemi," *Wireless Security Lab, French Network and Information Security Agency (ANSSI), Tech. Rep*, 2018.

[26] T. Fokkens, "Prediction and root-cause analysis for smart speaker intentional electromagnetic interference attacks," Ph.D. dissertation, Missouri University of Science and Technology, 2023.

[27] T. Fokkens, Z. Xu, O. H. Izadi, and C. Hwang, "Machine learning voice synthesis for intention electromagnetic interference injection in smart speaker devices," in *2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium*. IEEE, 2021, pp. 673–677.

[28] M. Gao, F. Xiao, W. Liu, W. Guo, Y. Huang, Y. Liu, and J. Han, "Expelliarmus: Command cancellation attacks on smartphones using electromagnetic interference," in *Proceedings of the IEEE INFOCOM 2023-IEEE Conference on Computer Communications*.

[29] A. Geiger, P. Lenz, C. Stiller, and R. Urtasun, "Vision meets robotics: The kitti dataset," *The International Journal of Robotics Research*, vol. 32, no. 11, pp. 1231–1237, 2013.

[30] T. Goelles, B. Schlager, and S. Muckenhuber, "Fault detection, isolation, identification and recovery (fdiir) methods for automotive perception sensors including a detailed literature survey for lidar," *Sensors*, vol. 20, no. 13, p. 3662, 2020.

[31] R. S. Hallyburton, Y. Liu, Y. Cao, Z. M. Mao, and M. Pajic, "Security analysis of {Camera-LiDAR} fusion against {Black-Box} attacks on autonomous vehicles," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 1903–1920.

[32] R. Halterman and M. Bruch, "Velodyne hdl-64e lidar for unmanned surface vehicle obstacle detection," in *Unmanned Systems Technology XII*, vol. 7692. SPIE, 2010, pp. 123–130.

[33] L. Hesai Technology Co., "State detection device for lidar, lidar, and state detection method," Patent US20 220 268 904A1, 2022.

[34] T. Huang, Z. Liu, X. Chen, and X. Bai, "Epnet: Enhancing point features with image semantics for 3d object detection," in *Computer Vision–ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, Proceedings, Part XV 16*. Springer, 2020, pp. 35–52.

[35] D. P. Huttenlocher, G. A. Klanderman, and W. J. Rucklidge, "Comparing images using the hausdorff distance," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 15, no. 9, pp. 850–863, 1993.

[36] I. Innovusion, *innovusion-Falcon*, https://www.innovusion.com/products/, 2023.

[37] T. Insights, "Deep dive teardown of the velodyne lidar puck vlp-16 lidar sensor," https://www.techinsights.com/products/ddt-1902-808, 2019.

[38] Y. Intelligence, *LiDAR for Automotive 2023*, 2023.

[39] J.-H. Jang, M. Cho, J. Kim, D. Kim, and Y. Kim, "Paralyzing drones via emi signal injection on sensory communication channels," in *Proceedings of the 2023 Network and Distributed System Security Symposium*.

[40] Q. Jiang, X. Ji, C. Yan, Z. Xie, H. Lou, and W. Xu, "Glitchhiker: Uncovering vulnerabilities of image signal transmission with iemi," in *Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23)*, 2023.

[41] Q. Jiang, Y. Ren, Y. Long, C. Yan, Y. Sun, X. Ji, K. Fu, and W. Xu, "Ghosttype: The limits of using contactless electromagnetic interference to inject phantom keys into analog circuits of keyboards," in *Network and Distributed Systems Security (NDSS) Symposium*, 2024.

[42] Z. Jin, X. Lu, B. Yang, Y. Cheng, C. Yan, X. Ji, and W. Xu, "Unity is strength? benchmarking the robustness of fusion-based 3d object detection against physical sensor attack," in *Proceedings of the ACM on Web Conference 2024*, 2024, pp. 3031–3042.

[43] Z. Jin, J. Xiaoyu, Y. Cheng, B. Yang, C. Yan, and W. Xu, "Pla-lidar: Physical laser attacks against lidar-based 3d object detection in autonomous vehicle," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2022, pp. 710–727.

[44] C. Kasmi and J. L. Esteves, "Iemi threats for information security: Remote command injection on modern smartphones," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 6, pp. 1752–1755, 2015.

[45] S. Köhler, R. Baker, and I. Martinovic, "Signal injection attacks against ccd image sensors," in *Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security*.

[46] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in *Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP)*.

[47] A. H. Lang, S. Vora, H. Caesar, L. Zhou, J. Yang, and O. Beijbom, "Pointpillars: Fast encoders for object detection from point clouds," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2019, pp. 12 697–12 705.

[48] T. Liu, F. Lin, Z. Wang, C. Wang, Z. Ba, L. Lu, W. Xu, and K. Ren, "Magbackdoor: Beware of your loudspeaker as a backdoor for magnetic injection attacks," in *Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP)*.

[49] G. G. T. O. LLC, "Lidar laser health diagnostic," Patent US20 220 236 410A1, 2021.

[50] S. Maruyama, S. Wakabayashi, and T. Mori, "Tap 'n ghost: A compilation of novel attack techniques against smartphone touchscreens," in *Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP)*.

[51] A. Z. Mohammed, A. Singh, G. Y. Dayanıklı, R. Gerdes, M. Mina, and M. Li, "Towards wireless spiking of smart locks," in *Proceedings of the 2022 IEEE Security and Privacy Workshops (SPW)*.

[52] A. Pahl and S. Dickmann, "Analysis of sensor disturbances caused by iemi," *https://doi. org/10.15488/12553*, pp. 159–165, 2022.

[53] A. Pahl, K.-U. Rathjen, and S. Dickmann, "Intended electromagnetic interference with motion detectors," in *2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium*, 2021.

[54] S. Pang, D. Morris, and H. Radha, "Clocs: Camera-lidar object candidates fusion for 3d object detection," in *2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 2020, pp. 10 386–10 393.

[55] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," *Black Hat Europe*, vol. 11, no. 2015, p. 995, 2015.

[56] W. Radasky and E. Savage, "Intentional electromagnetic interference (iemi) and its impact on the us power grid," *Meta*, vol. 1, pp. 1–3, 2010.

[57] B. Razavi, *Design of analog CMOS integrated circuits*, 2005.

[58] J.-M. Redouté and M. Steyaert, *EMC of analog integrated circuits*. Springer Science & Business Media, 2009.

[59] I. Robosense LiDAR, "Fault diagnostic methods, devices, storage media and lidar," Patent CN 115 825 931 A, 2023.

[60] ——, *RS-16*, https://www.robosense.ai/en/rslidar/RS-LiDAR-16, 2023.

[61] ——, *RS-Bpearl*, https://www.robosense.ai/en/rslidar/RS-Bpearl, 2023.

[62] ——, *RS-M1*, https://www.robosense.ai/en/RS-LiDAR-M1, 2023.

[63] ——, *RS-M1P*, https://www.robosense.ai/en/RS-LiDAR-M1, 2023.

[64] 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.

[65] ——, "Revisiting lidar spoofing attack capabilities against object detection: Improvements, measurement, and new attack," *arXiv preprint arXiv:2303.10555*, 2023.

[66] J. Selvaraj, G. Y. Dayanıklı, N. P. Gaunkar, D. Ware, R. M. Gerdes, and M. Mina, "Electromagnetic induction attacks against embedded systems," in *Proceedings of the 2018 ACM Asia Conference on Computer and Communications Security*.

[67] H. Shan, B. Zhang, Z. Zhan, D. Sullivan, S. Wang, and Y. Jin, "Invisible finger: Practical electromagnetic interference attack on touchscreen-based electronic devices," in *Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP)*.

[68] J.-W. Shi, J.-I. Guo, M. Kagami, P. Suni, and O. Ziemann, "Photonic technologies for autonomous cars: feature introduction," *Optics Express*, vol. 27, no. 5, pp. 7627–7628, 2019.

[69] S. Shi, C. Guo, L. Jiang, Z. Wang, J. Shi, X. Wang, and H. Li, "Pv-rcnn: Point-voxel feature set abstraction for 3d object detection," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2020, pp. 10 529–10 538.

[70] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications," in *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2017, pp. 445–467.

[71] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *Cryptographic Hardware and Embedded Systems-CHES 2013: 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings 15*. Springer, 2013, pp. 55–72.

[72] 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.

[73] R. Suzuki, T. Sato, Y. Hayakawa, K. Ikeda, O. Sako, R. Nagata, Q. A. Chen, and K. Yoshioka, "Wip: Towards practical lidar spoofing attack against vehicles driving at cruising speeds."

[74] Y. SystemPlus, "Reverse of robosense rs-lidar-m1," https://www.yolegroup.com/product/teardown-track/robosense-rs-lidar-m1-lidar-sample-version/, 2022.

[75] M. Szakály, S. Köhler, M. Strohmeier, and I. Martinovic, "Assault and battery: Evaluating the security of power conversion systems against electromagnetic injection attacks," *arXiv preprint arXiv:2305.06901*, 2023.

[76] J. Tu, M. Ren, S. Manivasagam, M. Liang, B. Yang, R. Du, F. Cheng, and R. Urtasun, "Physically realizable adversarial examples for lidar object detection," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2020, pp. 13 716–13 725.

[77] Y. Tu, S. Rampazzi, B. Hao, A. Rodriguez, K. Fu, and X. Hei, "Trick or heat?: Manipulating critical temperature-based control systems using rectification attacks," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*.

[78] I. Velodyne LiDAR, *VLP-16 User Manual*, https://velodynelidar.com/downloads/#datasheets, 2023.

[79] K. Wang, R. Mitev, C. Yan, X. Ji, A.-R. Sadeghi, and W. Xu, "{GhostTouch}: Targeted attacks on touchscreens without physical touch," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 1543–1559.

[80] K. Wang, S. Xiao, X. Ji, C. Yan, C. Li, and W. Xu, "Volttack: Control iot devices by manipulating power supply voltage," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2023, pp. 1771–1788.

[81] H. Wu, C. Wen, S. Shi, X. Li, and C. Wang, "Virtual sparse convolution for multimodal 3d object detection," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2023, pp. 21 653–21 662.

[82] Z. Xu, R. Hua, J. Juang, S. Xia, J. Fan, and C. Hwang, "Inaudible attack on smart speakers with intentional electromagnetic interference," *IEEE Transactions on Microwave Theory and Techniques*, vol. 69, no. 5, pp. 2642–2650, 2021.

[83] K. Yang, T. Tsai, H. Yu, M. Panoff, T.-Y. Ho, and Y. Jin, "Robust roadside physical adversarial attack against deep learning in lidar perception modules," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 2021, pp. 349–362.

[84] X. Zhang, K. Kwon, J. Henriksson, J. Luo, and M. C. Wu, "A large-scale microelectromechanical-systems-based silicon photonics lidar," *Nature*, vol. 603, no. 7900, pp. 253–258, 2022.

[85] H. Zhu, Z. Yu, W. Cao, N. Zhang, and X. Zhang, "Powertouch: A security objective-guided automation framework for generating wired ghost touch attacks on touchscreens," in *Proceedings of the 41st IEEE/ACM International Conference on Computer-Aided Design*, 2022.

[86] Y. Zhu, C. Miao, F. Hajiaghajani, M. Huai, L. Su, and C. Qiao, "Adversarial attacks against lidar semantic segmentation in autonomous driving," in *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, 2021, pp. 329–342.

[87] Y. Zhu, C. Miao, T. Zheng, F. Hajiaghajani, L. Su, and C. Qiao, "Can we use arbitrary objects to attack lidar perception in autonomous driving?" in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 1945–1960.

APPENDIX

A. The Fault Diagnostic and Management

In the realm of electronic device engineering, The Fault Diagnostic and Management (FDM) mechanisms play a pivotal role in ensuring the reliability and efficiency of electronic devices. FDM methodologies are designed to detect, diagnose, and manage faults within electronic circuits and components, minimizing downtime and preventing catastrophic failures.

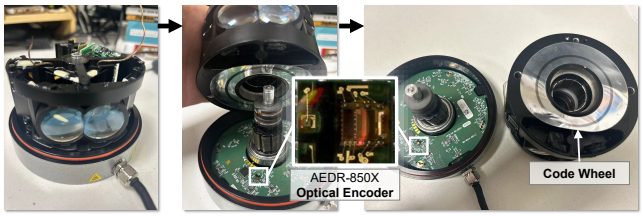
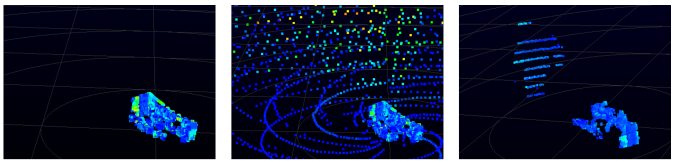


Fig. 20: **The Teardown of VLP-16 LiDAR.** By disassembling the LiDAR, we find that the VLP-16's bottom board is equipped with an optical encoder, AEDR-850X, utilized for measuring the rotational speed of the LiDAR.



(a) Benign Point Cloud of Lab room (b) Pulse Modulation Without Synchronization (c) Controllable Point Injection With Synchronization

Fig. 21: **Illustration of the necessity of synchronization for point control.** (a)Benign point cloud of the lab room. (b) Random fake points injected by pulse-modulated EM signals without synchronization. (c) Fake "pedestrian" points injected by modulated EM signals with synchronization.

These systems leverage a combination of advanced algorithms, including machine learning and artificial intelligence, to analyze data from sensors and other sources. This data-driven approach enables the early detection of anomalies, facilitating prompt intervention. Furthermore, FDM mechanisms are integral in predicting potential failures through proactive health monitoring, thereby extending the lifespan of electronic components. The integration of FDM mechanisms in electronic devices not only enhances performance but also contributes significantly to safety, particularly in critical applications such as medical devices, automotive electronics, and aerospace systems. As technology advances, the complexity and sophistication of FDM mechanisms continue to evolve, offering more robust and intelligent solutions for fault management in the ever-expanding landscape of electronic devices.

B. The Necessity of Synchronization for Point Control

The necessity of synchronization is illustrated in Fig. 21. Without a synchronization mechanism based on receiving and delaying, as shown in Fig. 21(b), the injected point cloud would be random. In contrast, as shown in Fig.21(c), when synchronization is induced, the desired fake points can be injected. It is worth noting that, for a more intuitive demonstration of the effect without synchronization, the signal used in Fig.21(b) is designed with a pulse at every receiving time of the LiDAR. If the signal from Fig.21(c) is used without synchronization, the scarcity of pulses may often result in the inability to inject a point cloud.

TABLE III: **Average Precision (AP) of Five 3D Object Detection Models under Different-Intensity Points Interference**

Interference Intensity	LiDAR-only		LiDAR-Camera Fusion		
	PointPillar	PV-RCNN	VirConv-L	EPNet	CLOCs
0	77.616	83.660	86.818	78.831	76.885
5cm	77.068	79.101	86.006	78.273	76.267
10cm	72.585	77.069	85.651	76.746	71.918

Fig. 22: **The LiDARs under test.**

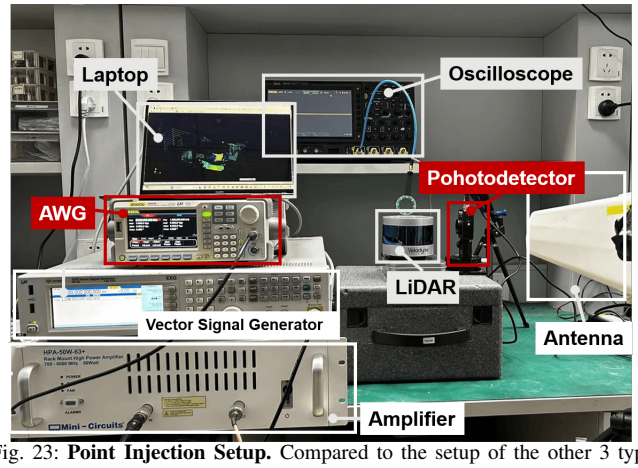
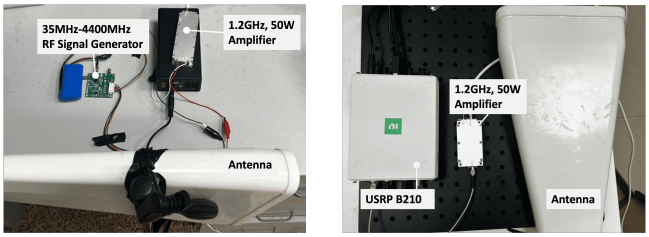


Fig. 23: **Point Injection Setup.** Compared to the setup of the other 3 types of attacks, an arbitray signal generator and a photodetector are added.



(a) The Attack Setup Costs $160 (b) The Attack Setup Costs $2300

Fig. 24: **Attack Setup with Cheaper Hardwares.** With approximately $168 worth of equipment, we were able to achieve *Points Interference*, *Points Removal* and *LiDAR Power-off*. With approximately $2300 worth of equipment, we were able to achieve *Points Injection*.

TABLE IV: **Fault Detection and Diagnostic List from an Anonymous LiDAR Manufacturer**

Fault Name	Fault Description	Faults Causes	Dtection Period	Fault Debounce	Conditions for Fault Recovery	Fault Management
TimeSync_Error	Abnormal of synchronization	Failure on time synchronization. The time of rising edge of the detection frame exceed 5ms when the second signal changed.	100ms	No debounce, a single fault triggers immediately	Fault recovery when no faults occur within a single detection cycle.	L0 error, Lidar shall send out awarning message to external ACU, point cloud is valid
Window_Blockage	Abnormal of window blockage	There are something (dirt, frost, ice, etc) on the surface of window. The blockage area detected exceed 30%	100ms	fault for three consecutive times.	Fault recovery when no faults occur within five detection cycles.	
Battery_High	Input voltage of Lidar is too high	Supply voltage is beyond 16.8V. Report recoverable error, voltage is beyond 19.5V, communication signal stop.	100ms	fault for three consecutive times.	Fault recovery when no faults occur within five detection cycles.	
Battery_Low	Input voltage of Lidar is too low	Supply voltage is lower than 8.2V.Report recoverable error,voltage is lower than 6.5V, communication signal stop.	100ms	fault for three consecutive times.	Fault recovery when no faults occur within five detection cycles.	
The supply voltage at the ECU is too low	Mismatch between the measured ECU voltage and the battery voltage value received via the CAN signal VehBattUSysU.	The measured ECU voltage ia less than the battery voltage value received via the CAN signal VehBattUSysU by 3V	100ms	fault for three consecutive times.	Fault recovery when no faults occur within five detection cycles.	
Missing_ADCU_Signal	Missing ADCU Signa.	The ADCU signal is missing for 10 cycles.	dpends on ADCU	fault for ten consecutive times.	Fault recovery when no faults occur within five detection cycles.	
Temperature_Low	Internal temperature is too low	Internal temperature is lower than -43.5℃.	1s	fault for five consecutive times.	FL2, no automatic recovery	L1 error, Lidar shall send out a warning message to external ACU, stop the point cloud. ADCU shall treat the point cloud data as invalid
Temperature_High	Internal temperature is too high	Internal temperature is beyond 120℃.	1s	fault for five consecutive times.	FL2, no automatic recovery	
Lidar_Internal_voltage_Error	Abnormal of the internal voltage of Lidar	The tolerance of internal voltage monitored exceed 5.5V±5%.	<100ms	fault for once	FL2, no automatic recovery	
MEMS_Working_Error	MEMS failure during operation	The failure of fast axis or slow axis of MEMS occurred. 1. The frequency of fast axis or slow axis exceed ±15Hz. 2. The amplitude of fast axis or slow axis exceed ±20%	<100ms	fault for once	FL2, no automatic recovery	
TX_Error	Failure of TX module	Internal TX module failure occurred. 1. The time interval between two adjacent lidar transmitting control signals is below 3us. 2. The pulse width of lidar transmitting control signal exceed 748ns.	<100ms	fault for once	FL2, no automatic recovery	
RX_Error	Failure of RX module	Internal RX module failure occurred. 1. No distance information of reference signal 2. No noise signal near the baseline at the threshold value	<100ms	fault for once	FL2, no automatic recovery	
Clock_Error	Abnormal of clock	The accuracy of crystal oscillator decreased or failure on crystal oscillator.1. The tolerance of independent clock exceed the range 1±5% for two consecutive 10us.	<100ms	fault for once	FL2, no automatic recovery	
LiDAR_Calibration_Error	Lidar intrinsic parameter abnormal	The CRC of intrinsic parameter is incorrectly.	Self-Diagnostic Test Upon LiDAR Power-On	Self-check upon each power-on; if self-check fails, initiate a restart. After two consecutive restarts, confirm the fault.	FL2, no automatic recovery	
FL2_Error	Level 2 error need ADCU detection and reaction	Failures occur during the start-up or running mode, such as watchdog monitoring(detection cycle 10ms), lidar Asic crashing, power and signal line broken	NA	<150ms	Unrecoverble	L2 error. Lidar shall stop the laser emmision and power off. ADCU could not receive any message/data from Lidar. ADCU shall monitor the message from Lidar.