PhantomLiDAR: Cross-modality Signal Injection Attacks against LiDAR

Zizhi Jin, Qinhong Jiang, Xuancun Lu, Chen Yan, Xiaoyu Ji *, Wenyuan Xu

Ubiquitous System Security Lab (USSLAB), Zhejiang University

LiDAR (Light Detection And Ranging)

- LiDAR sensor is **widely used** for **3D perception** in safety-critical systems.

Self-driving Car

CVIS

Robots

Drones

[1] Pic Source: www.velodynelidar.com

LiDAR (Light Detection And Ranging)

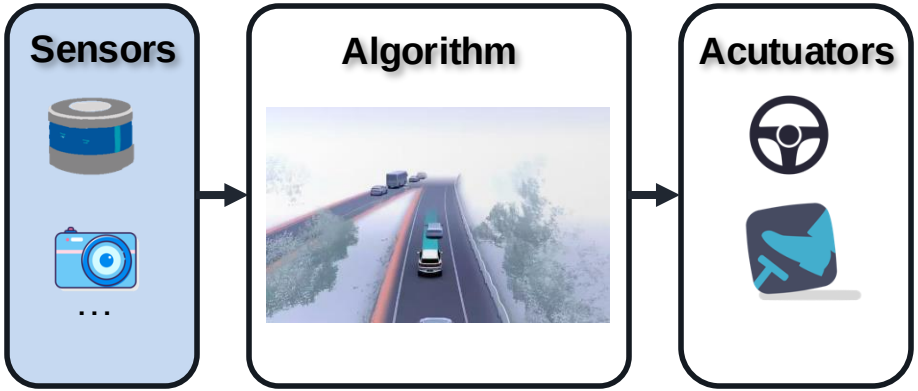
- LiDAR sensor is **widely used** for **3D perception** in safety-critical systems.
- **Correct Sensing** of LiDAR is the **foundation** for **system safety**.

Self-driving Car

CVIS

Robots

Drones



A typical workflow of self-driving system

[1] Pic Source: www.velodynelidar.com

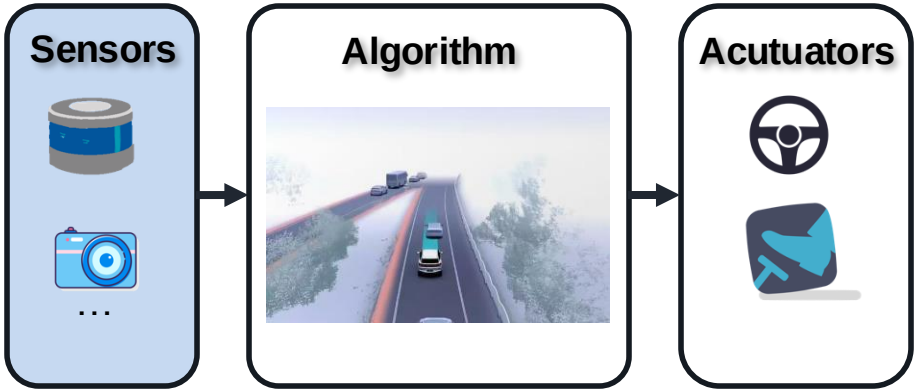
LiDAR (Light Detection And Ranging)

- LiDAR sensor is **widely used** for **3D perception** in safety-critical systems.

Self-driving Car

CVIS

- **Correct Sensing** of LiDAR is the **foundation** for **system safety**.



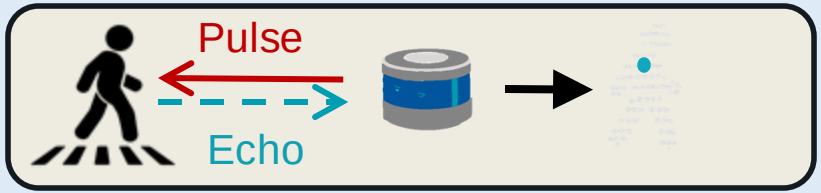
LiDAR security is important !

Research Goal: Make the LiDAR more Reliable.

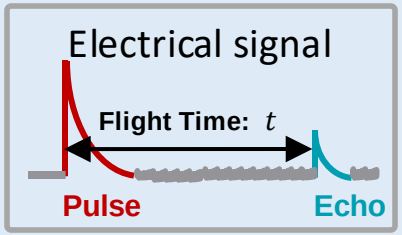
How Does LiDAR Work?

- LiDAR perceives the environment by generating **point cloud** through **Laser Ranging** and **Laser Scanning**.

Laser Ranging:
Generate One LiDAR Point



Time of Flight (ToF) principle



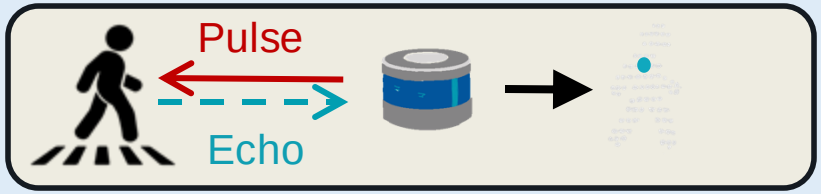
- **Direction** (θ, φ)
- **Distance**

$$d = 0.5 * t * c$$

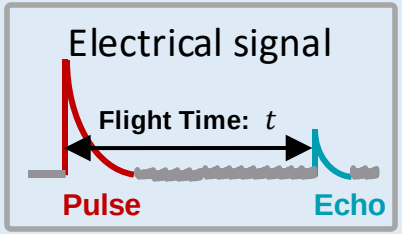
How Does LiDAR Work?

- LiDAR perceives the environment by generating **point cloud** through **Laser Ranging** and **Laser Scanning**.

Laser Ranging:
Generate One LiDAR Point



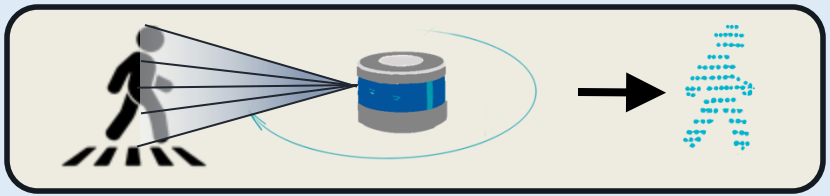
Time of Flight (ToF) principle

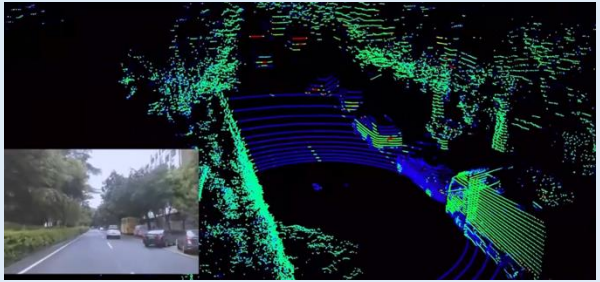


- **Direction** (θ, φ)
- **Distance**

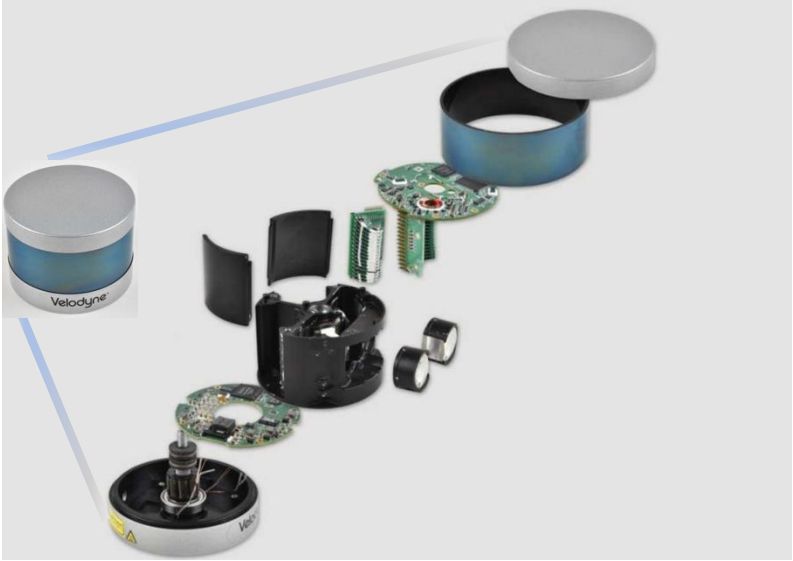
$$d = 0.5 * t * c$$

Laser Ranging + Laser Scanning:
Generate Point Cloud





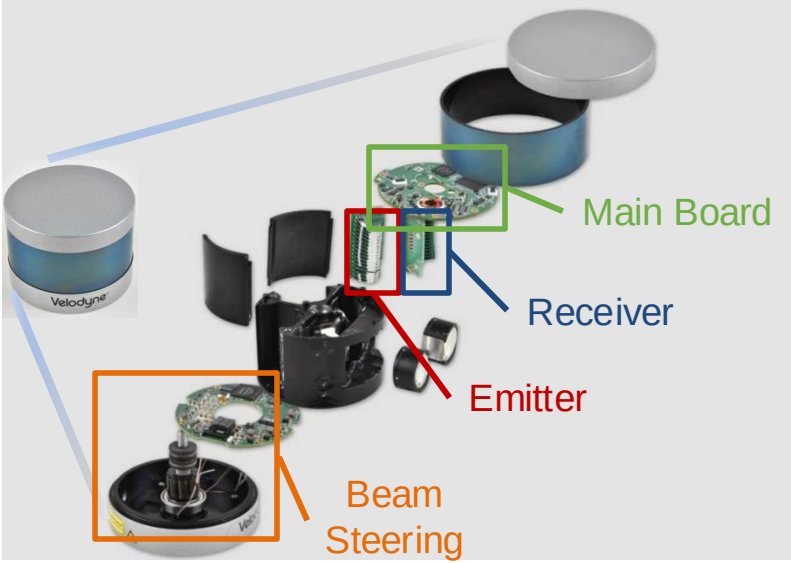
Functional Modules of LiDAR



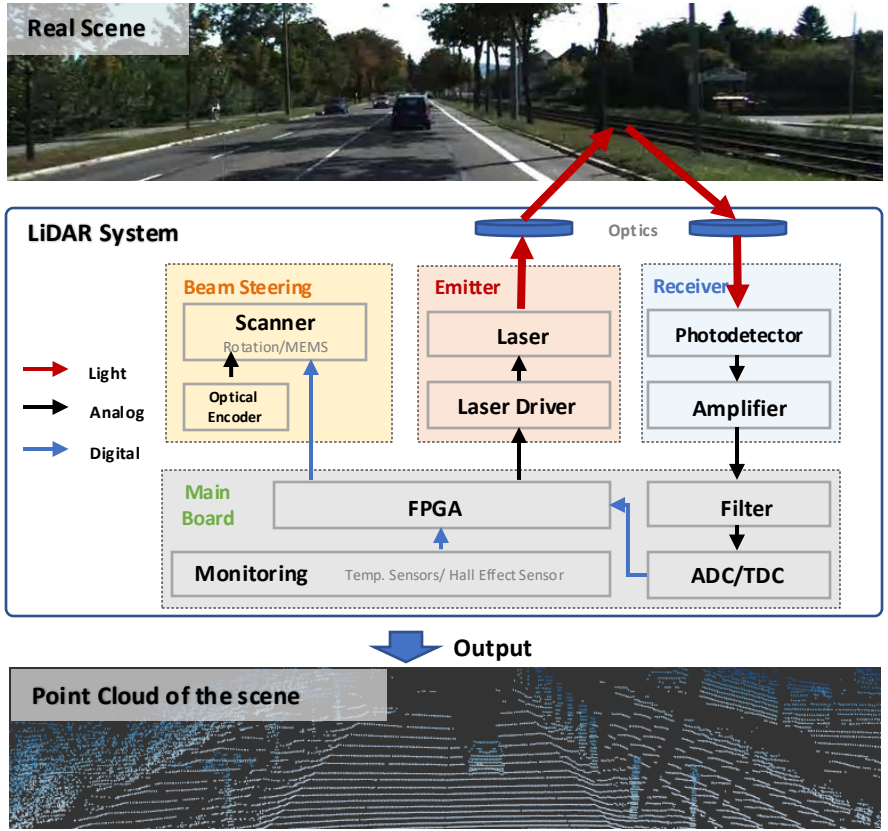
Teardown of a LiDAR[1]

[1] Source: techinsights.com

Functional Modules of LiDAR



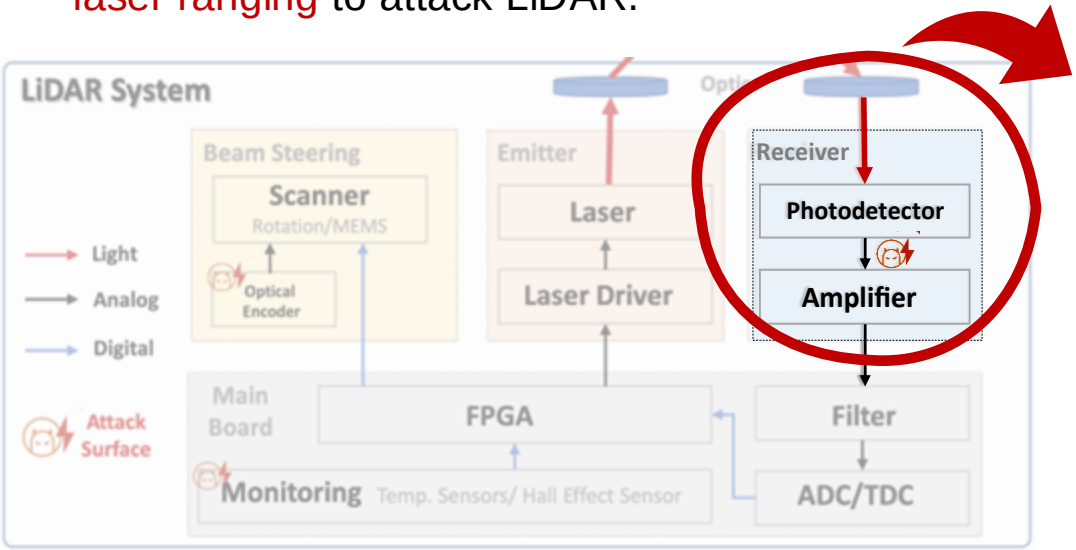
Teardown of a LiDAR[1]

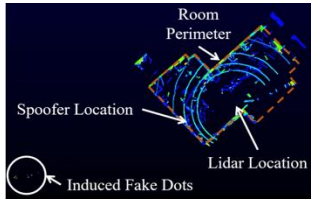


[1] Source: techinsights.com

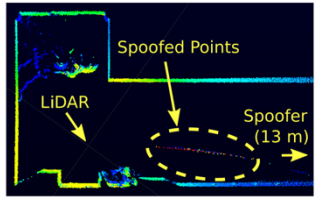
Related Work - LiDAR Attack

- Previous works all considered the "Receiver" as the attack Surface, focusing on manipulating laser ranging to attack LiDAR.

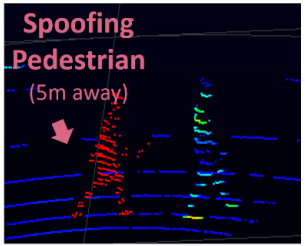




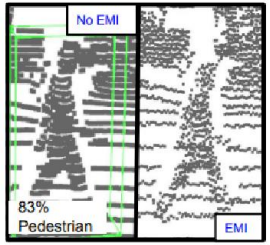
Illusion and Dazzle
Shin et al. CHES'17



AdvLiDAR,
Cao et al. CCS'19



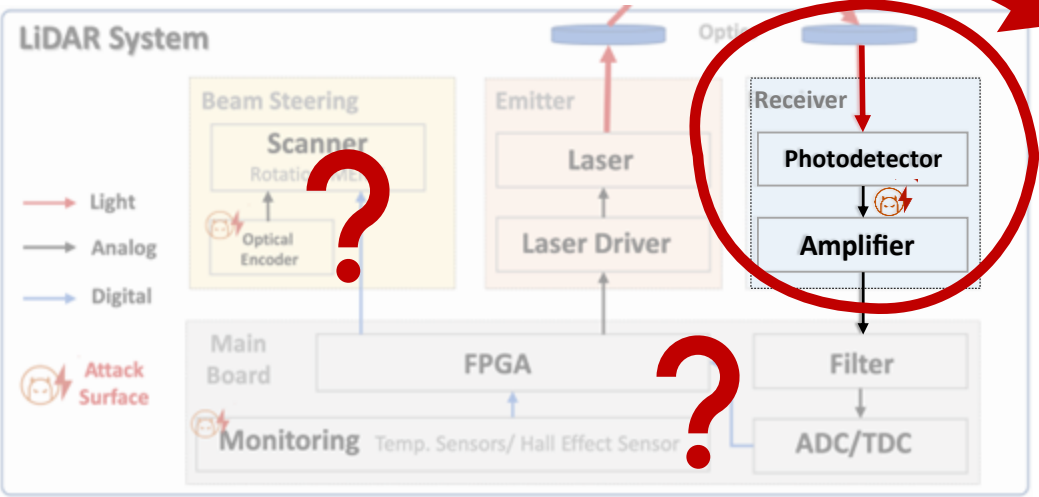
PLA-LiDAR,
Jin et al. S&P'23

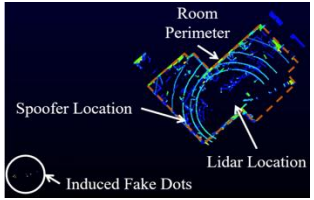


EMI-LiDAR,
S.H.V et al. WISec'23

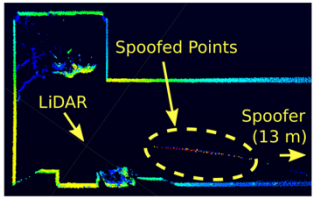
Related Work - LiDAR Attack

- Previous works all considered the "Receiver" as the attack Surface, focusing on manipulating laser ranging to attack LiDAR.

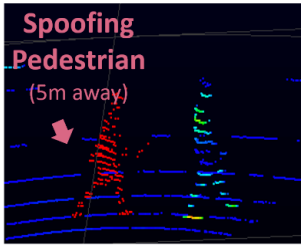


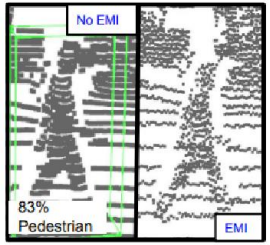


Illusion and Dazzle
Shin et al. CHES'17



AdvLiDAR,
Cao et al. CCS'19

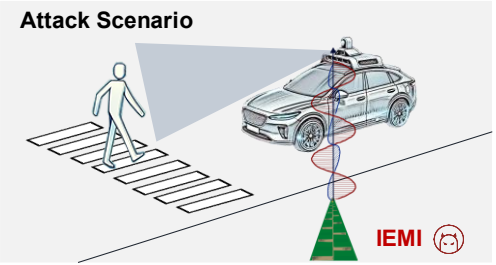




Research Gap: The vulnerabilities of **other modules** within the LiDAR system remain underexplored

We Propose *PhantomLiDAR*

- **EM-based** attack with 4 Effects, 3 Attack Surfaces and 2 Principle.



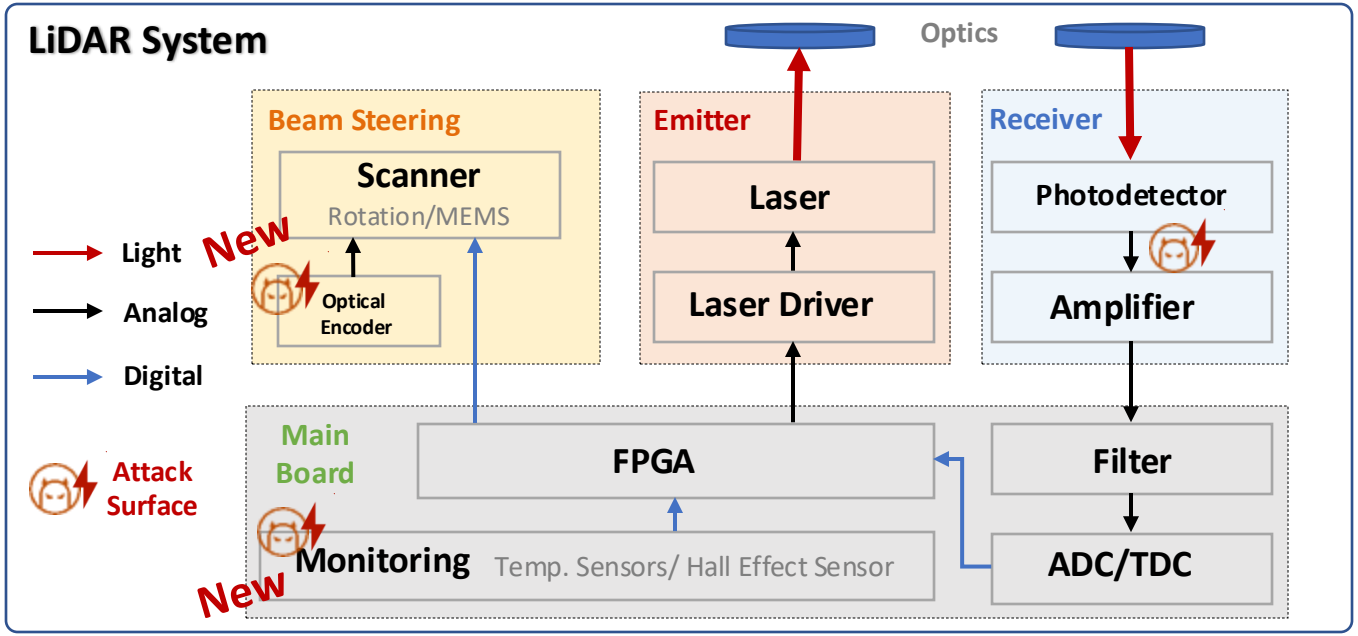
Ground Truth

Four Types of Attack Effects

Attack Effect	 Points Interference	 Points Removal	 LiDAR Poweroff	 Points Injection
Attack Signal	Sine Wave 			 Pulse Modulated Sine Wave
Attack Surface	Laser Receiving Circuit	Monitoring Sensor; Laser Receiving Circuit	Beam Steering Module	Laser Receiving Circuit

Attack Surfaces of *PhantomLiDAR*

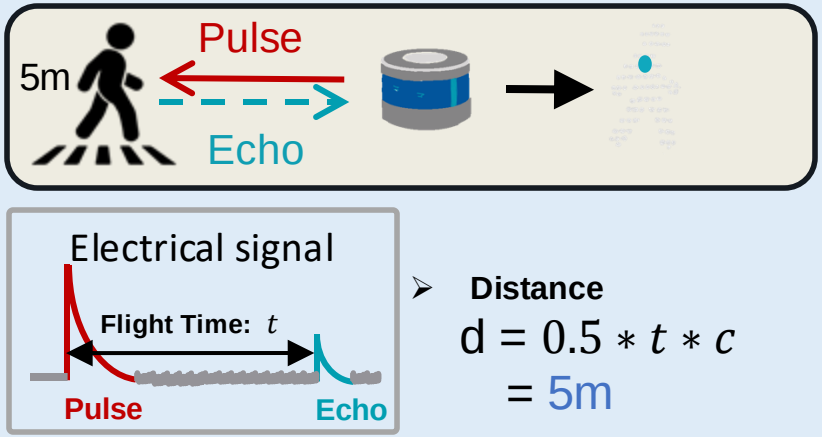
- Attack surfaces include the (1) laser receiving analog circuit in receiver , (2) monitoring sensors on mainboard and (3) optical encoder in beam steering module



Two Attack Principles of *PhantomLiDAR*

1. **Direct Attack:** interfere with the analog signal in the **receiving module**, **directly affecting the LiDAR's echo signal** and subsequently disrupting the point cloud.

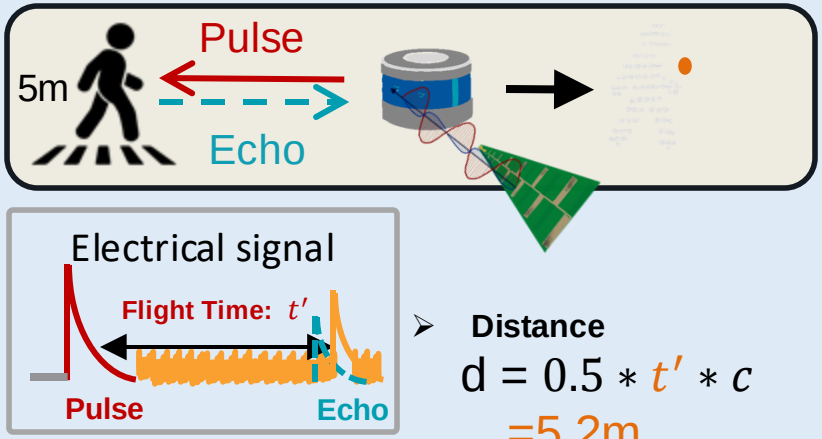
Laser Ranging (Benign)



- **Distance**

$$d = 0.5 * t * c$$
$$= 5m$$

Laser Ranging (Under Direct Attack)

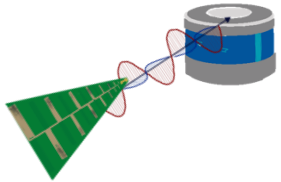


- **Distance**

$$d = 0.5 * t' * c$$
$$=5.2m$$

Two Attack Principles of *PhantomLiDAR*

2. **Indirect Attack:** First, the attacker induces errors in the auxiliary circuit. Then, by exploiting LiDAR's Fault Detection and Diagnostic (FDD) mechanism, these errors can indirectly trigger severe issues such as point removal or LiDAR power-off.



Errors in Auxiliary Circuit

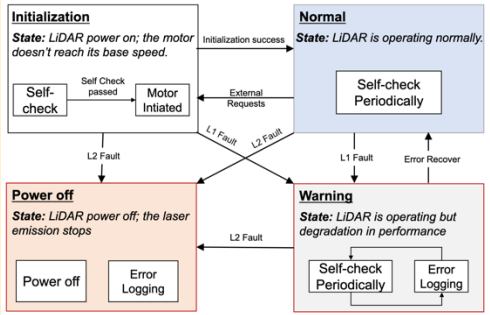
L1: Temp. Error

37℃ → 150℃

L2: Rotation Speed Error

600RPM → 12RPM

LiDAR's Fault Detection and Diagnostic (FDD) mechanism



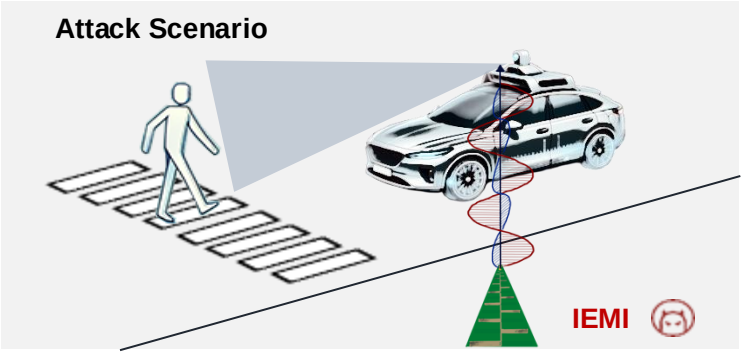
Errors in Point Cloud or LiDAR

Points Removal

Points Invalid

LiDAR Power-off

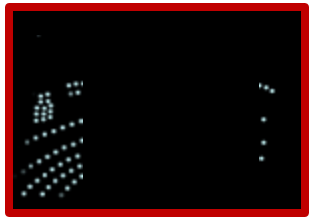
Let’s Dive into the Four Attack Effcts



Ground Truth

Four Types of Attack Effects

1. Points Interference



2. Points Removal

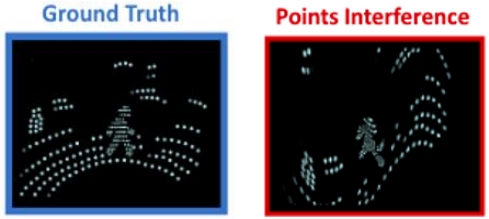
3.LiDAR Poweroff

4. Points Injection

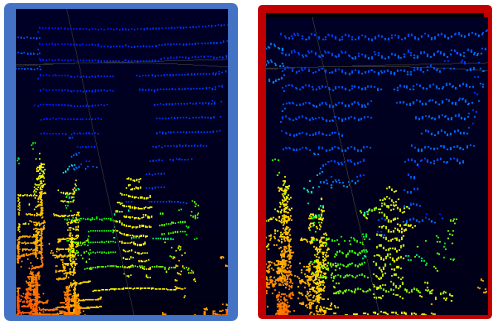
Detail of Points Interference

☐ Attack Effect

Introduce errors in LiDAR ranging, thereby distorting the point cloud.



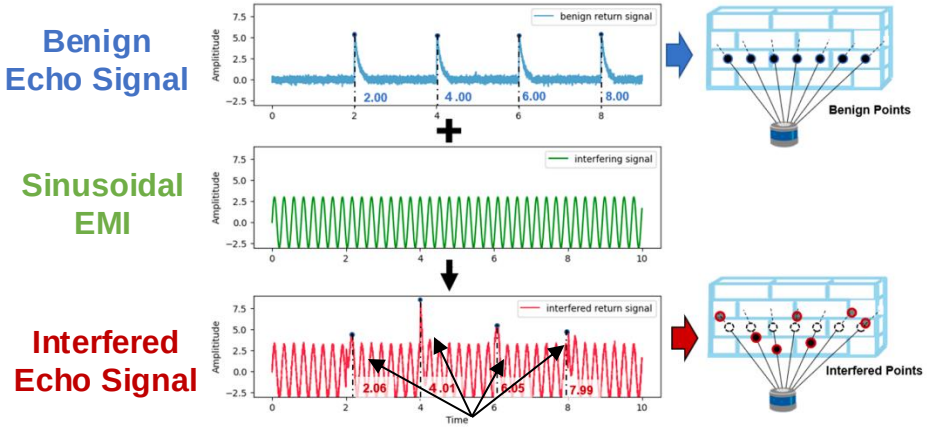
Illustration



Real Attack

☐ Attack Principle - Direct Attack

- **Attack Surface:** Analog circuit in the receiver
- **Attack Signal:** Sinusoidal EMI at a specific frequency
- **Attack Principle:** The sinusoidal interference from EMI can cause minor variations in the peak time of the return signal. This subsequently causes a shift in the position of the points.



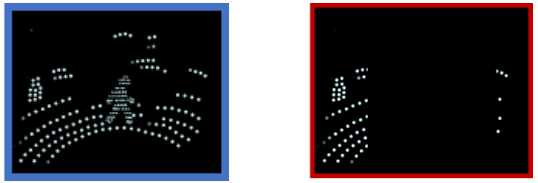
minor variations

Detail of Points Removal

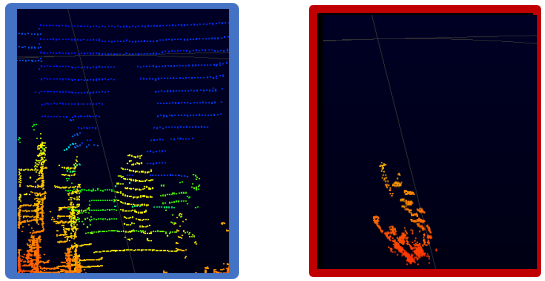
☐ Attack Effect

Causes the points to deviate significantly from its true position or to disappear.

Ground Truth **Points Removal**



Illustration

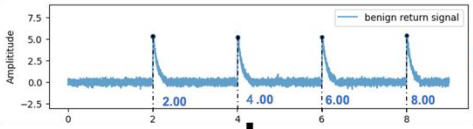


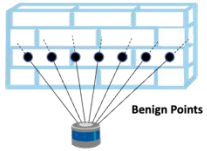
Real Attack

☐ Attack Principle1 - Direct Attack

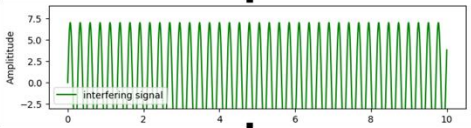
- **Attack Surface:** Analog circuit in the Receiver
- **Attack Signal:** High Amplitude Sinusoidal EMI
- **Attack Principle:** Inject high amplitude EM signal into receiving circuit, it may saturate the receiving circuit and make the real echo laser pulse undetectable.

Benign Echo Signal

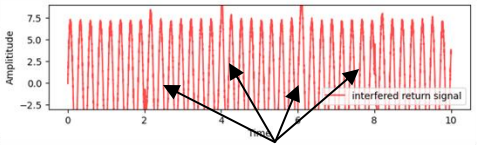


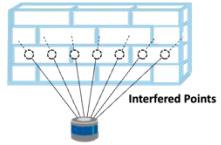


High Amp. EMI



Interfered Echo Signal





Peak Undetectable

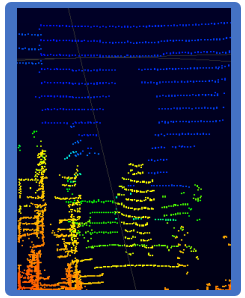
Detail of Points Removal

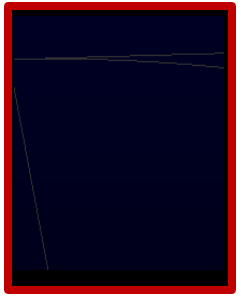
☐ Attack Effect

Causes the points to deviate significantly from its true position or to disappear.

Ground Truth **Points Removal**

Illustration





Real Attack

☐ Attack Principle2 - Indirect Attack

- **Attack Surface:** Monitoring Sensors
- **Attack Principle:** Compromise temperature sensor, it may induce LiDAR to detect L1 fault, leading LiDAR to consider some or all of the points as invalid.

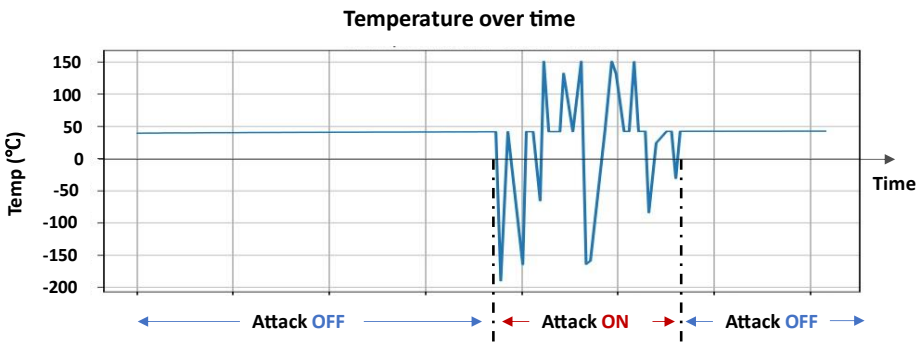
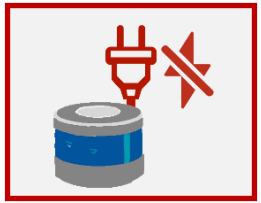


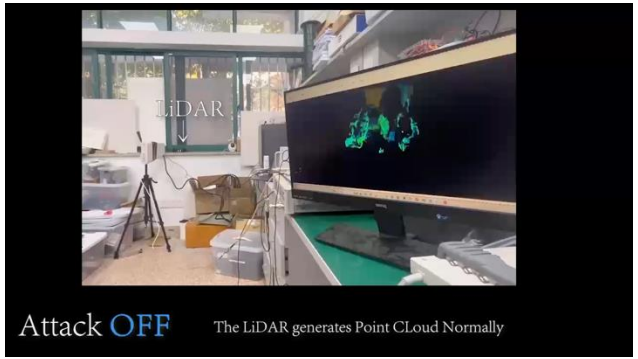
Fig. The output of temperature sensor. When EMI is off, the temperature is around 40 ◦C. When EMI is on, the temperature is fluctuate **between -200◦C and 150◦C**.

Detail of LiDAR Power-off

☐ Attack Effect

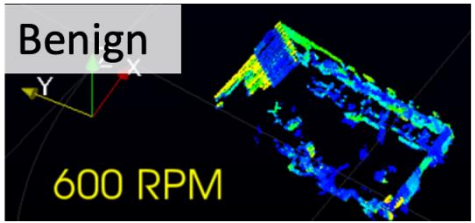
Causes the LiDAR system to shut down and stop working





☐ Attack Principle - Indirect Attack

- **Attack Surface:** Optical Encoder in Beam Steering Module
- **Attack Signal:** Sinusoidal EMI at a specific frequency
- **Attack Principle:** Compromise Optical Encoder in beam steering module, it may induce LiDAR to detect L2 fault, leading LiDAR power off to protect itself.



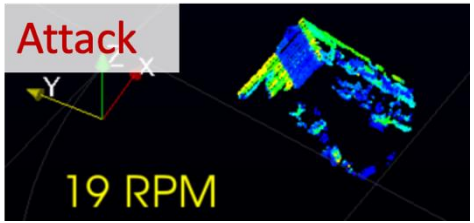


Fig. The Rotational Speed of LiDAR. When conducting LiDAR Power-off attack, the rotational speed of the LiDAR significantly decreases, then leading to a denial of service, and ultimately resulting in powering off.

Detail of Points Injection

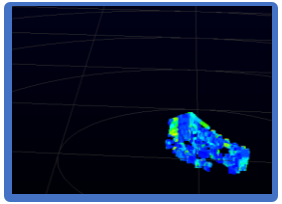
☐ Attack Effect

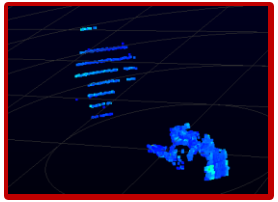
Inject controllable points

Ground Truth

Points Injection

Illustration



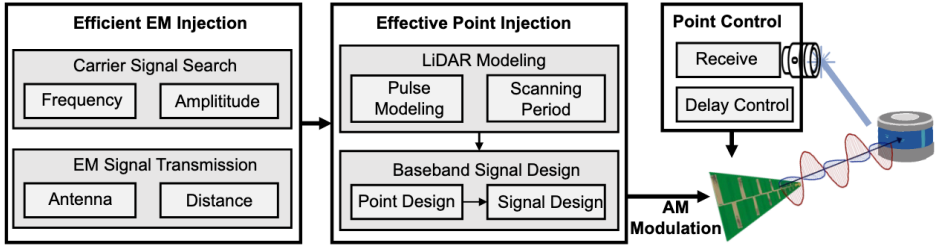


Real Attack

☐ Attack Principle - Direct Attack

- **Attack Surface:** Analog circuit in the receiver
- **Attack Signal:** Amplitude Modulated Sine Wave
  - Carrier Signal: Sinusoidal Wave
  - Baseband Signal: Fine-grained Pulses

- **Attack Principle:** Forging echo signal of LiDAR to control points.



Evaluation

☐ Overview

1) Attack on 5 COTS LiDARs
2) Points Interference
3) Points Removal
4) LiDAR Poweroff
5) Points Injection
6) Feasibility Experiments on Moving Vehicle

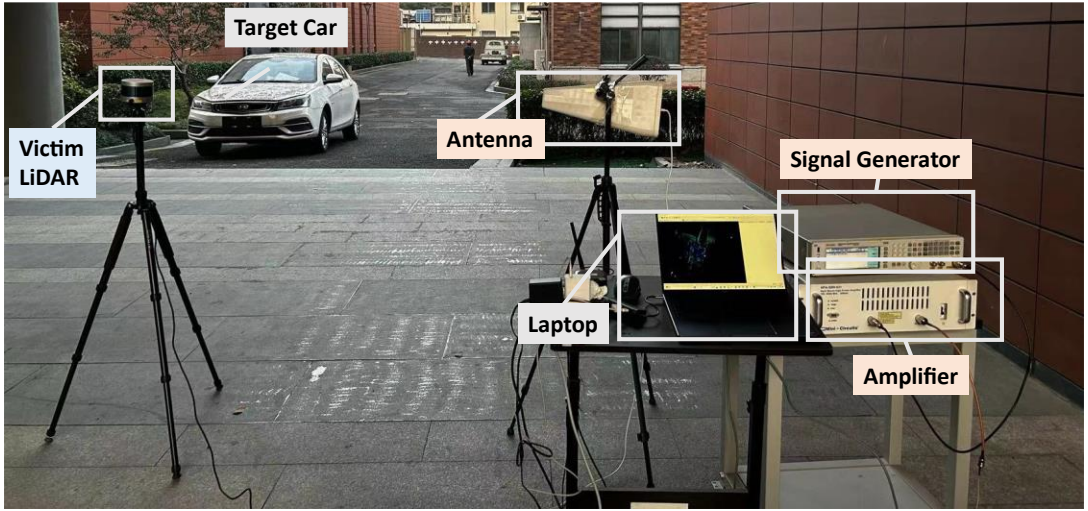


Fig. Attack Setup. The attack devices include a Keysight N5712b vector signal generator for EMI signal generation, a MiniCircuits HPA-50W-63+ power amplifier for amplifying the EMI signal, and a log-periodic antenna for signal transmission.

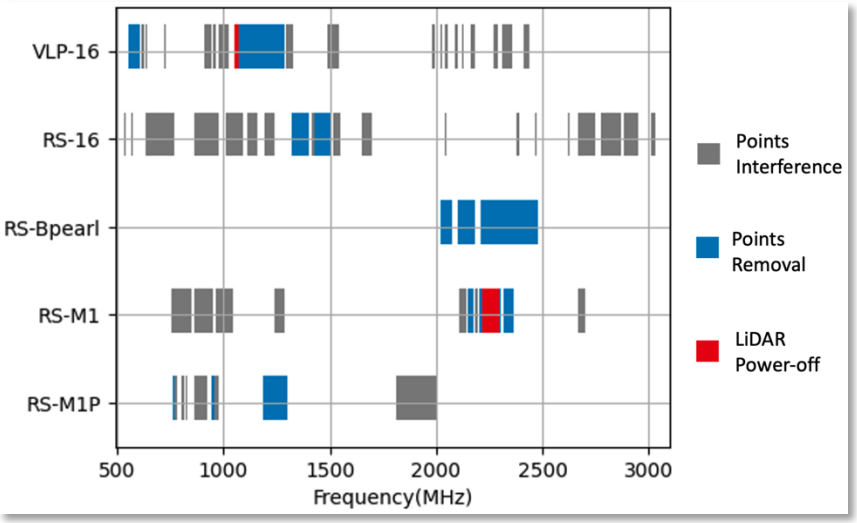
Evaluation – Fuzzing Different LiDARs

Mechanical Rotary. MEMS

Fig. The Five LiDARs under test.

☐ Fuzzing Parameters

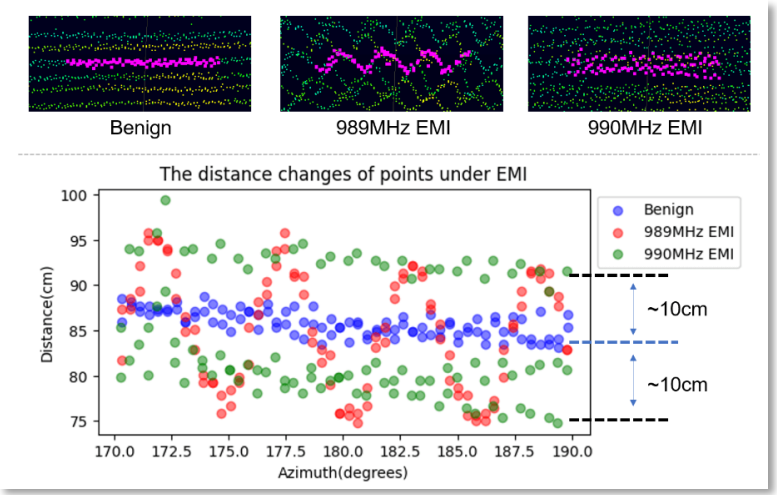
- Frequency Range: 500MHz – 3500MHz
- Amplitude: 37dBm
- Distance: 30cm



Observation: Different LiDARs exhibit different vulnerabilities and vulnerable frequencies.

- **Points Interference** can be achieved on all LiDARs except RS-Bpearl, demonstrating that the electromagnetic protection of RS-Bpearl's receiving circuit is more robust.
- **Points Removal** can be implemented on all LiDARs.
- **LiDAR Power-off** can be achieved on VLP-16 and RS-M1.

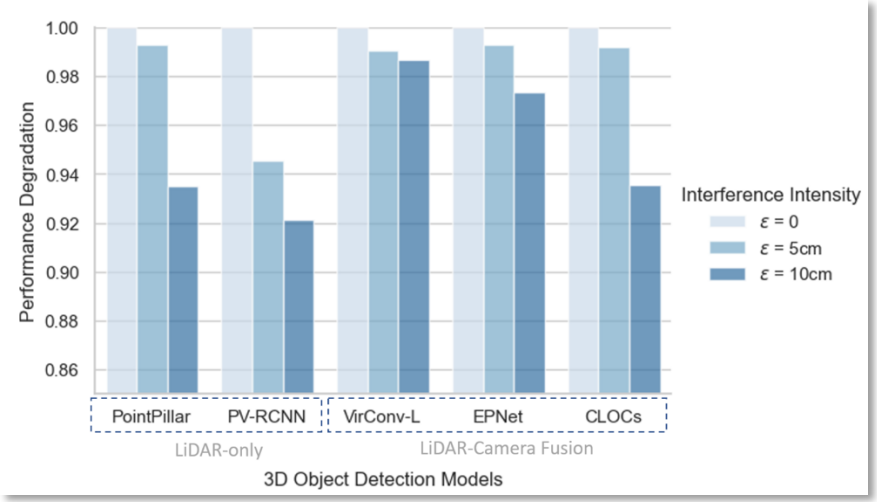
Evaluation – Points Interference



Points Interference Intensity.

Our attack devices can induce above 10cm distance errors.

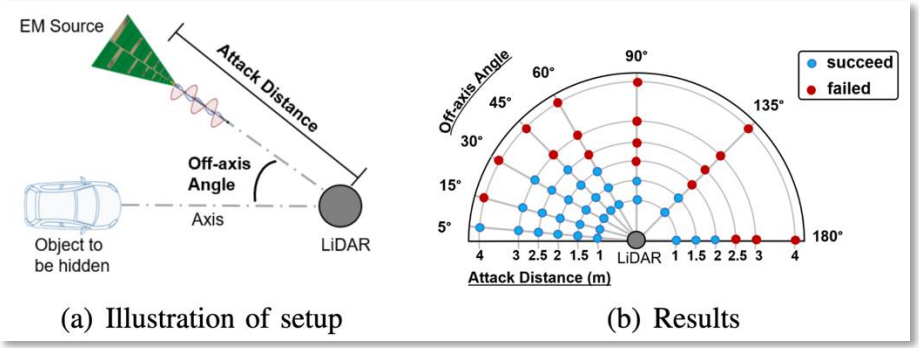
This will reduce the performance of the object detection model by 10%↓.



The impact of Point Interference on 3D object detection models.

Observation：**Sensor fusion mitigates points interference effectively.**

Evaluation – Points Removal

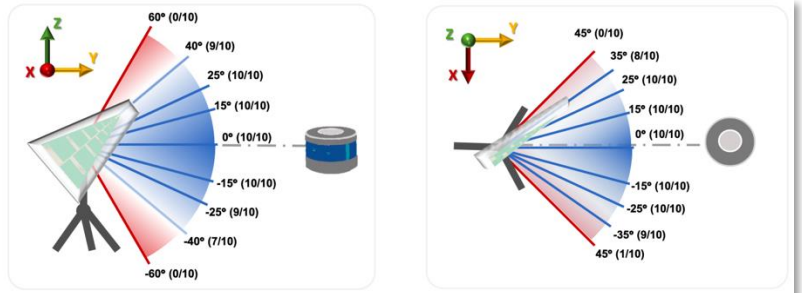


(a) Illustration of setup (b) Results

Fig1. Impacts of attacker's location. The attacker can hide the target object from any location within a distance of 1.5 meters. The attacker can succeed beyond 4 meters away (5.5 meters at most).

1) Long Attack Distance ✅

2) Low Location Requirements ✅

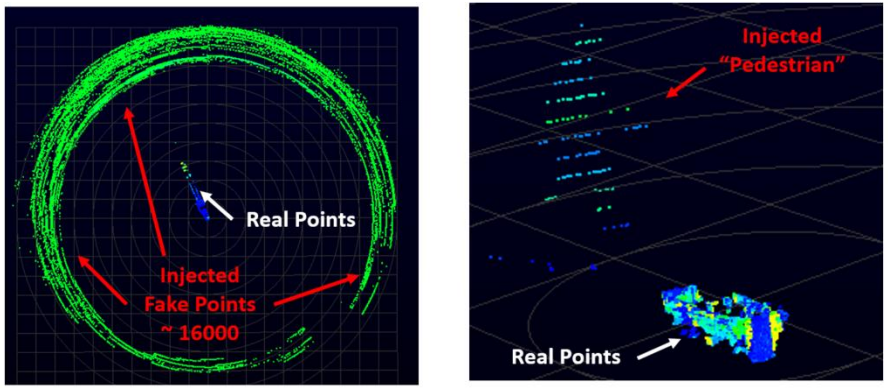


(a) Vertical Angle (b) Horizontal Angle

Fig2. Impacts of Aiming. The EM antenna could deviate up to 40◦ vertically or 35◦ horizontally while still achieving a hiding attack effect..

1) Low Aiming Requirements ✅

Evaluation – Points Injection



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

Fig. Points Injection with Different baseband signals. (a) When the baseband signal is a periodic pulse signal, the wall-pattern spoofing points can be injected. (b) With a fine-grained baseband signal, the pedestrian-pattern spoofing points can be injected.

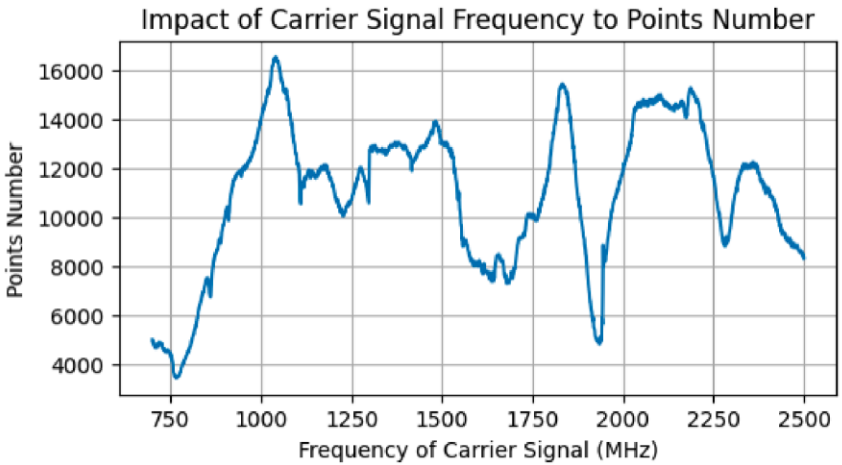
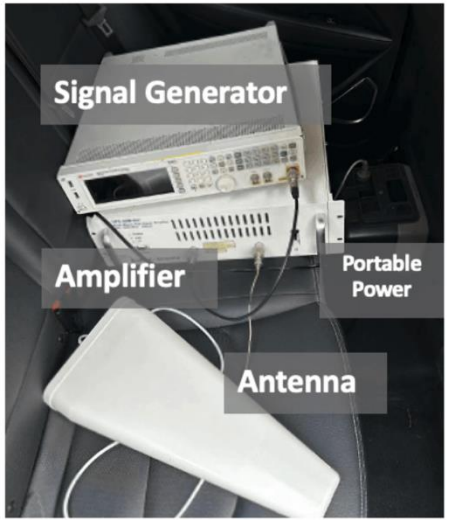


Fig. Impact of Carrier Frequency to Points Number. Different carrier frequencies indeed impact the number of injected points. Notably, a carrier frequency of approximately 1040 MHz enabled the injection of the highest number of points (over 16,500).

Feasibility Experiments on Moving Vehicle

- **Attack Goal:** Compromise the victim LiDAR and make the LiDAR-based 3D object detection model **unable to detect the target car**.

(a) Attack Setup

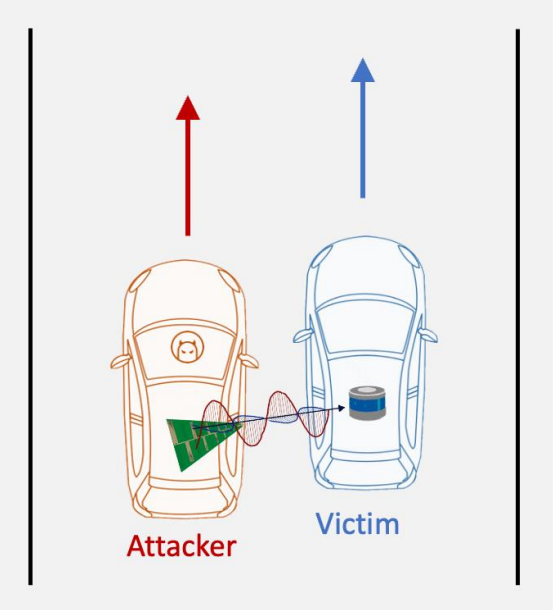


(b) Attack Devices

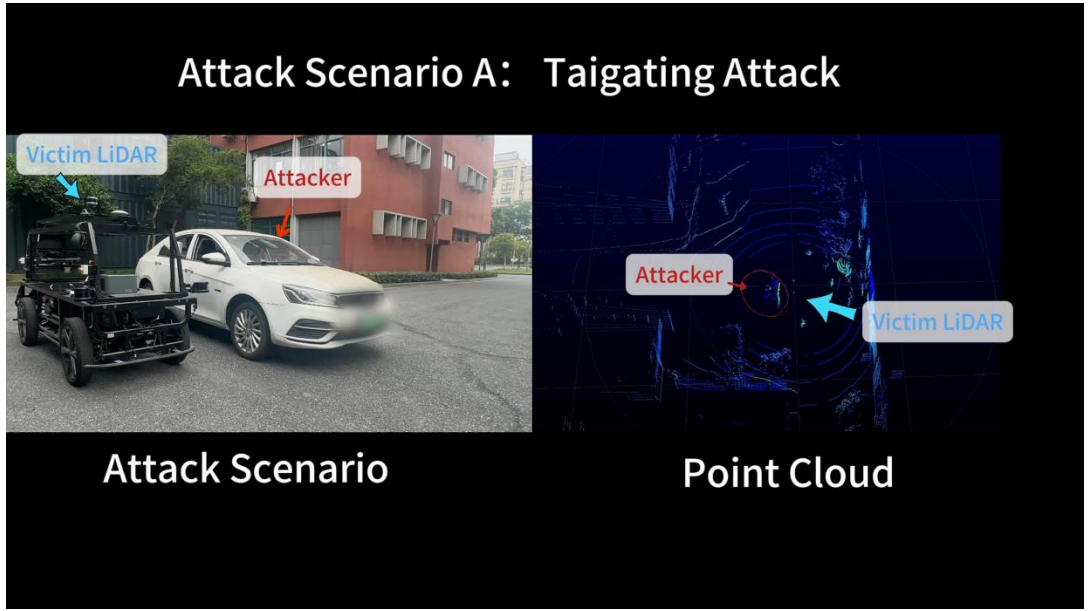
Please visit our website for more videos……

Feasibility Experiments on Moving Vehicle

☐ Moving Attack Scenario: Tailgating attack.



The attacker car drives close to the victim car at a similar speed.



Please visit our website for more videos……

Conclusion

- **New 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.

- **New EM-based Attack Effects.** We propose three new EM-based attack effects including Points Removal, LiDAR Power-off, and Points Injection.

- **Strong Attack Capabilities:**
  - **Points Interference** shows 2x stronger interference capability compared to SOTA works.
  - **Points Removal** can hide a target remotely without precise aiming.
  - **LiDAR Power-off** can success on popular mechanical LiDAR VLP-16 and MEMS LiDAR RS-M1.
  - **Points Injection** can inject controllable points number 5x more than SOTA laser-based attacks.

PhantomLiDAR:
Cross-modality Signal Injection Attacks against LiDAR






Zizhi Jin: zizhi@zju.edu.cn
Xiaoyu Ji: xji@zju.edu.cn
Wenyuan Xu: wyxu@zju.edu.cn

Project Website:
https://sites.google.com/view/phantomlidar

USSLAB Website: www.usslab.org