Outline:

1.What is LiDAR?

LiDAR (Light Detection And Ranging) is an indispensable sensor for precise long- and wide-range 3D sensing, which directly benefited the recent rapid deployment of autonomous driving (AD)

2.What is its security issue?

one can manipulate the LiDAR point cloud and fool object detectors by firing malicious lasers against LiDAR. (LiDAR spoofing attack) 🡺false positives (injecting a non-existing fake object) and false negatives (removing an existing object).

3.What does this paper feature?

we conduct the first large-scale measurement study on LiDAR spoofing attack capabilities on object detectors with 9 popular LiDARs, covering both first- and new-generation LiDARs, and 3 major types of object detectors trained on 5 different datasets.

4.What are the problems of previous work?

(a) Considering only one specific LiDAR: VLP-16

(b) Assuming unvalidated attack capabilities: Chosen Pattern Injection (CPI) attack capability 🡺 spoofing a specifically chosen point cloud pattern that was

carefully optimized/identified offline beforehand. # However, they didn’t really think how to achieve it to be a real threat. (all <6000 points)

(c)The limited models. #not considering the errors and diversity in real life.

5.What are the motivations of this paper?

RQ1: Are the common design-level assumptions made in prior LiDAR spoofing attacks actually realizable? If so, can they also hold for the more recent new-gen LiDARs? #The realizability of the prior spoofing attacks.

RQ2: Do different types of LiDARs, especially the new-gen ones with security-related features, have different vulnerability characteristics to LiDAR spoofing attacks? #Different types of LiDARs to test for the different vulnerability.

RQ3: Does the vulnerability status of popular object detectors to spoofing attacks significantly change due to the new-gen LiDAR features and different model setups? # Different types of LiDARs to test for the different extent of vulnerability. 🡺 asynchronized spoofing attack

6.What is the brief findings of this work?

(a) an attacker actually does not really need to exploit object detector-level vulnerabilities to achieve a near-front road object injection.

(b) VLP-16 is actually the only LiDAR model for which the CPI attack capability assumption is feasible.

(c) new-gen LiDAR features may not be effective as expected. 🡺 We find that the latest synchronized object removal attack can no longer be applied to the new-gen LiDARs, but there exist asynchronized object removal attacks that can

overcome such a limitation and can lead to a similar level of practical attack capabilities.

7. LiDAR tech: laser with reflection 🡺 Flash LiDARs: a broad laser that covers the entire field of view (FOV)/ simultaneous laser firings/ laser timing randomization/ fingerprinting.

8. traditional DNN cannot be used in point clouds🡺 3 major types of 3D object detection methods are widely adopted: voxel-based, point-based, and point voxel-based method.

9. Spoofing:

(a)synchronous 🡪 to synchronize the malicious laser firing timing with the victim LiDAR scanning (injection: reflecting the same frequency/ removal: strong continuous laser.)

(b) asynchronized 🡪 High-Frequency Removal (HFR)/

10. Errors for the real-life attack:

inadequate optical design can significantly affect the number and angle coverage of spoofable points due to undesired diffusion and convergence

of the attack laser beam.

1. injection (CPI): inner-frame error (spoofing a point at a chosen 3D position within an individual frame) / inter-frame error (maintaining the spoofed position of the same point in the chosen pattern across consecutive frames)

11. Results:

(a) RQ1 🡪 no longer held.

(b) Weakness:

Simultaneous Laser Firing: on VLP-32c we can always inject spoofed points pair by pair, and the injected pair will always have the same distance to LiDAR.

Timing Randomization: if the randomization is not strong enough, it will become ineffective.

Pulse Fingerprinting: not complex enough to perfectly prevent spoofing attacks. (injection, but could show the defense ability if designed well.)

1. new mathematic model.
2. Strongness:

Timing randomization 🡪 can have significant defense capabilities against object injection attacks. / high defense capabilities against object removal attacks in general.

Pulse Fingering 🡪 high defense capabilities against object removal attacks in general. / quite effective in defending against the removal attack effect at the system level.

12. Discussion: typically tuned to avoid false negatives rather than false positives, especially for AD scenarios.

Ideas:

I don’t understand why we should care about the LiDAR spoofing. Although it will cause serious problems to make drivers misjudge, it seems to be very difficult and unworthy of implementing in real life.

Another idea is that if the time randomization and pulse fingering are suitable to protect from the different attacks, why not we just combine them together?

<https://opg.optica.org/oe/fulltext.cfm?uri=oe-31-2-2013&id=524833>

(Random-modulated pulse lidar using a gain-switched semiconductor laser with a delayed self-homodyne interferometer, 2023 OPTICA)

Next Step:

1. The methods to spoof the LiDAR:

<https://ieeexplore.ieee.org/abstract/document/10179458>

(From the perspective of attackers to design the attack and take VLP-16 LiDAR as an example to implement the Synchronized attacks, 2023)

<https://ieeexplore.ieee.org/abstract/document/10173629>

(In theory, class-specific adversarial attack to vanish any targeted LiDAR point cloud, 2023)

Attack for other parts of LiDAR:

<https://www.ndss-symposium.org/wp-content/uploads/vehiclesec2024-14-paper.pdf>

(the real implementation of the attack for the LiDAR-based location systems, 2024Network and Distributed System Security (NDSS) Symposium)

1. The methods to protect from the spoofing in LiDAR.

(Google Scholar: lidar spoofing defense since 2023, no related result.)

1. The methods to detect a spoofing laser:

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10453355>

(using the Doppler frequency to differentiate the spoofing laser and the original laser, 2024)

1. The overall of the cybersecurity issues in AV: <https://ieeexplore.ieee.org/document/10097455>

(Relating to AI-based attacks to different parts of AV. 2023)