On the Realism of LiDAR Spoofing Attacks against Autonomous Driving Vehicle at High Speed and Long Distance

Takami Sato*, Ryo Suzuki*, Yuki Hayakawa*, Kazuma Ikeda,
Ozora Sako, Rokuto Nagata, Ryo Yoshida,
Qi Alfred Chen, and Kentaro Yoshioka

NDSS SYMPOSIUM/2025

Keio University 1858 CALAMVS GLADIO FORTIOR

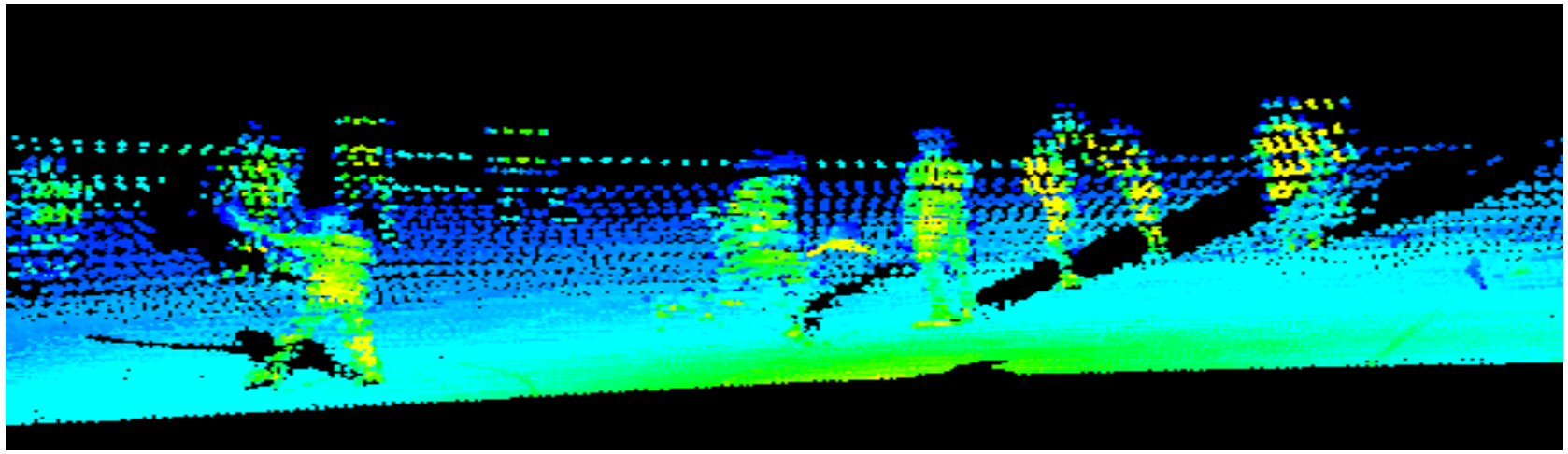
Yoshioka Lab

UC Irvine

AS²Guard
Autonomous & Smart Systems Guard Research Group

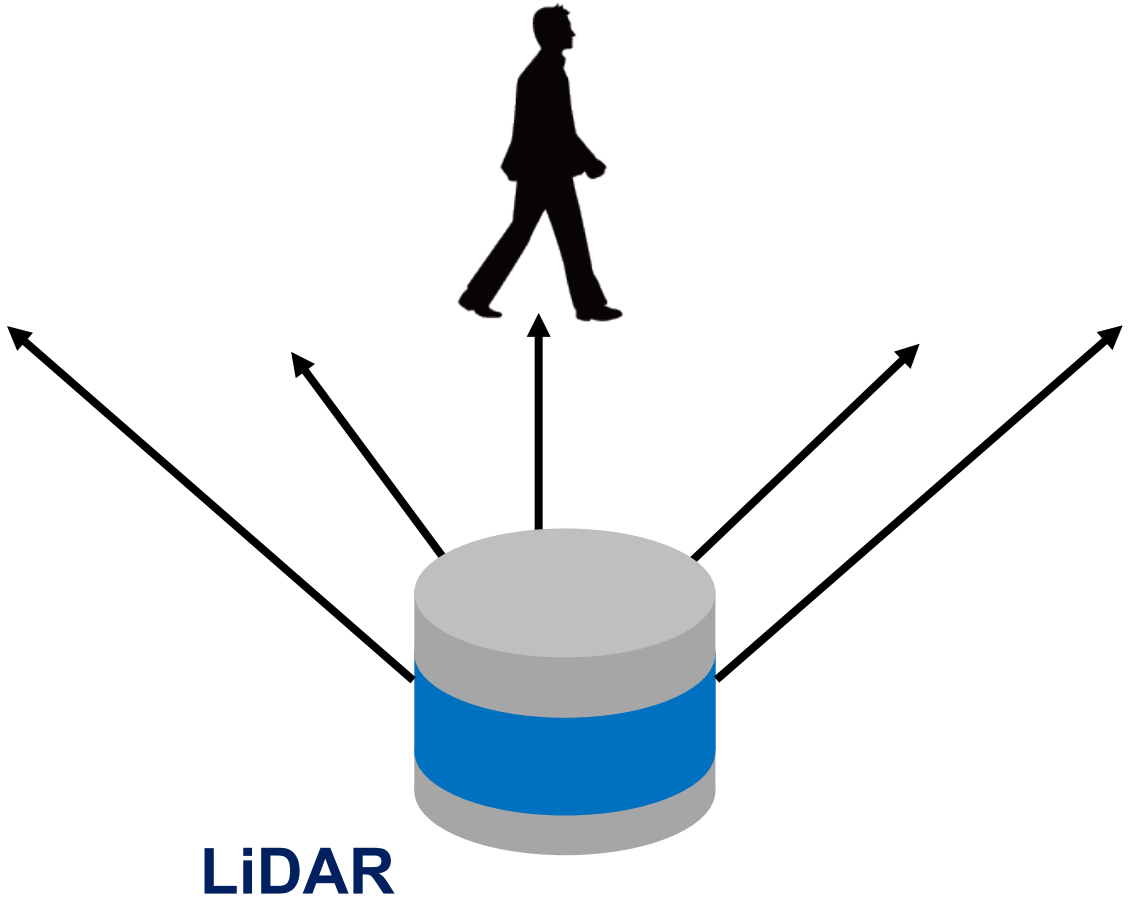
About LiDAR & Spoofing Attack

- **LiDAR is widely used as a primary sensor for Autonomous Vehicles (AVs)**



About LiDAR & Spoofing Attack

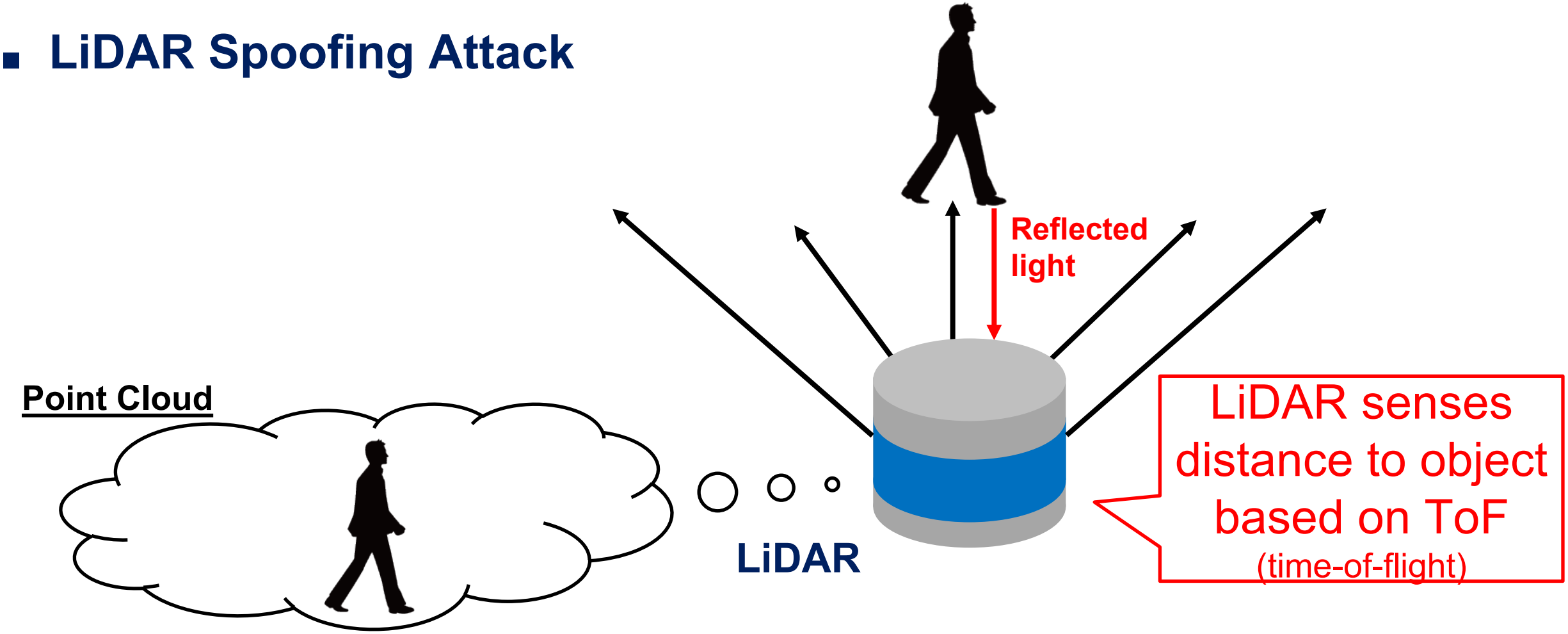
- LiDAR Spoofing Attack



LiDAR scans its surroundings by emitting lasers

About LiDAR & Spoofing Attack

- LiDAR Spoofing Attack

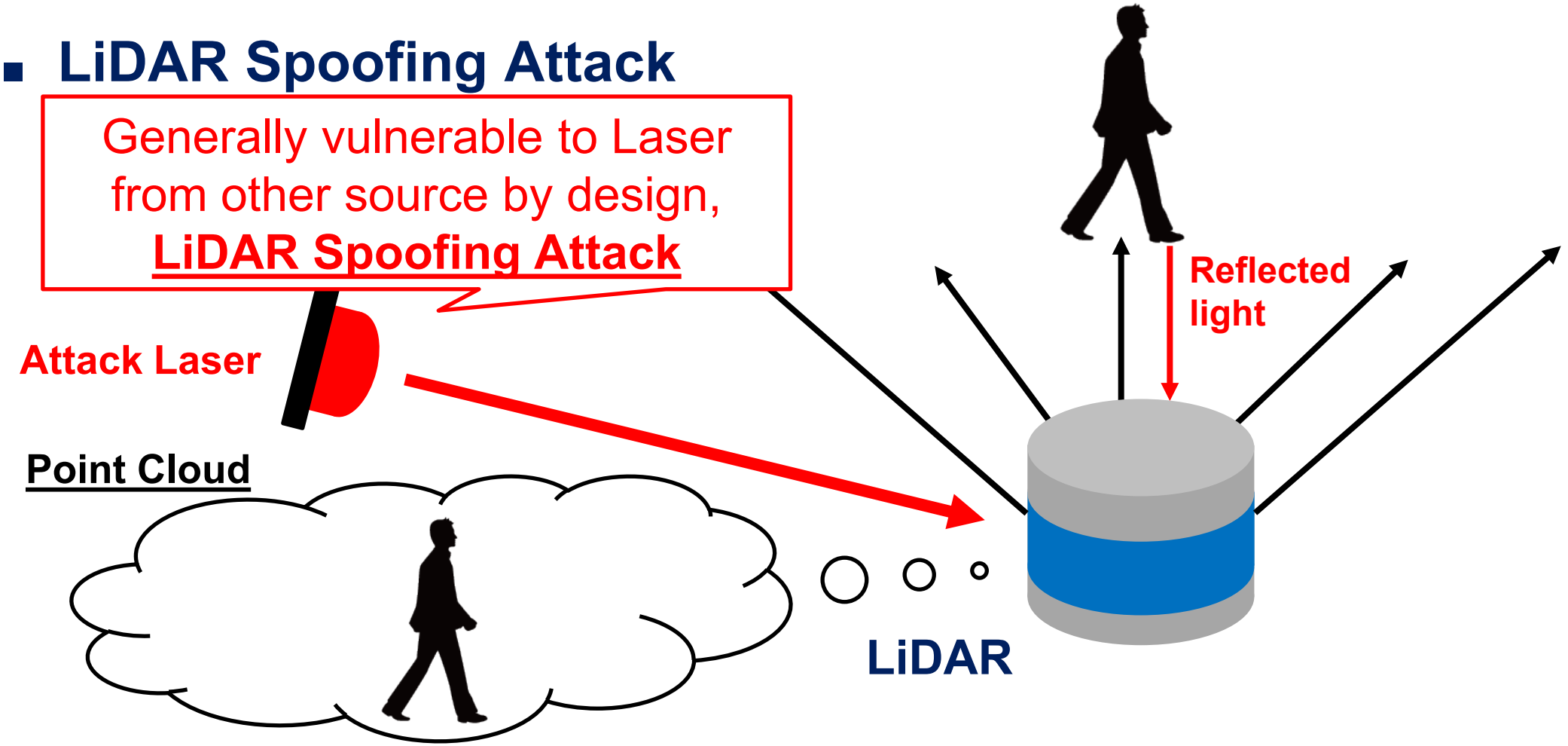


$$ToF\ distance = Light\ Speed \times Flight\ Time \div 2$$

About LiDAR & Spoofing Attack

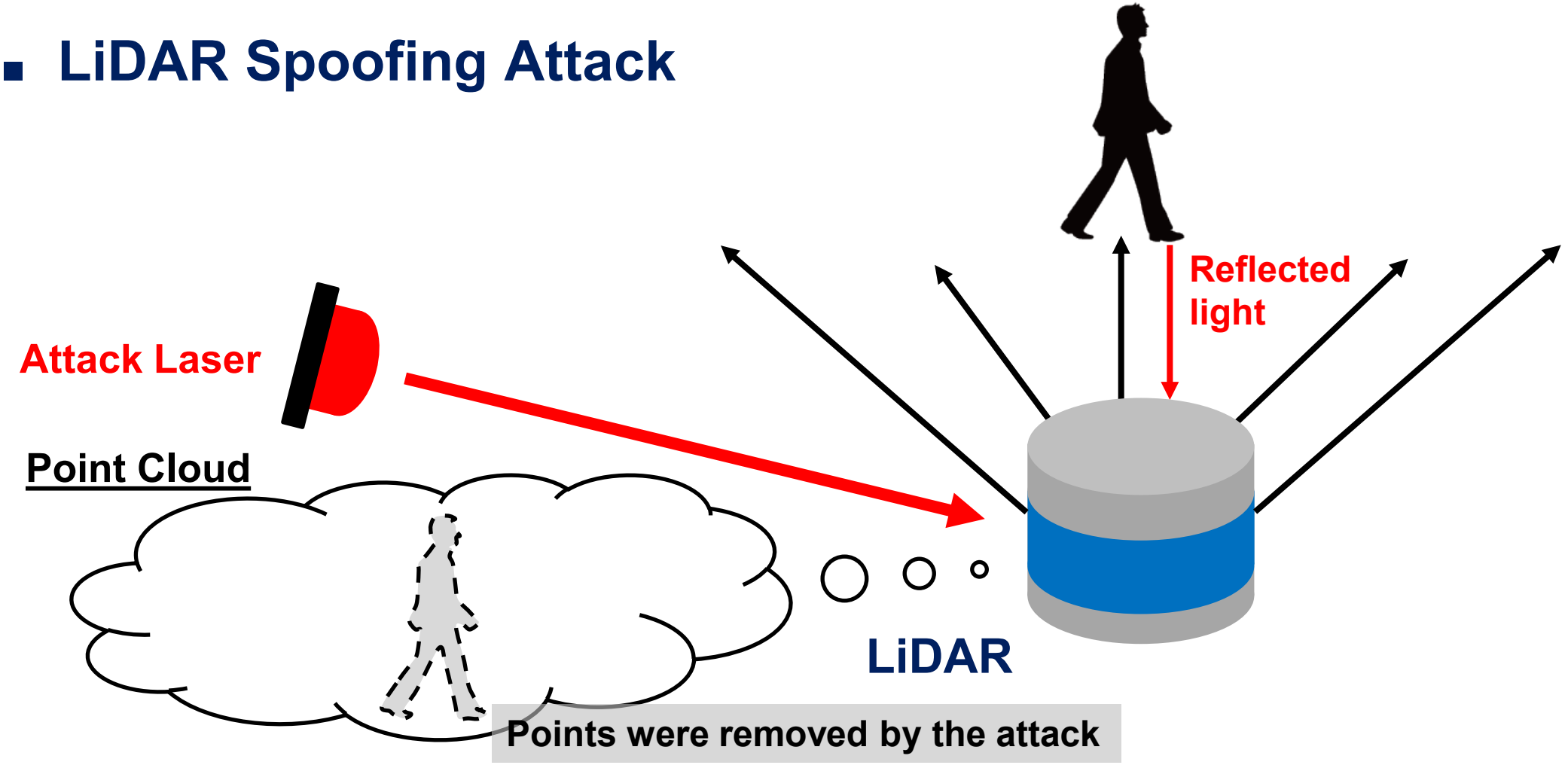
- **LiDAR Spoofing Attack**

Generally vulnerable to Laser from other source by design, **LiDAR Spoofing Attack**



About LiDAR & Spoofing Attack

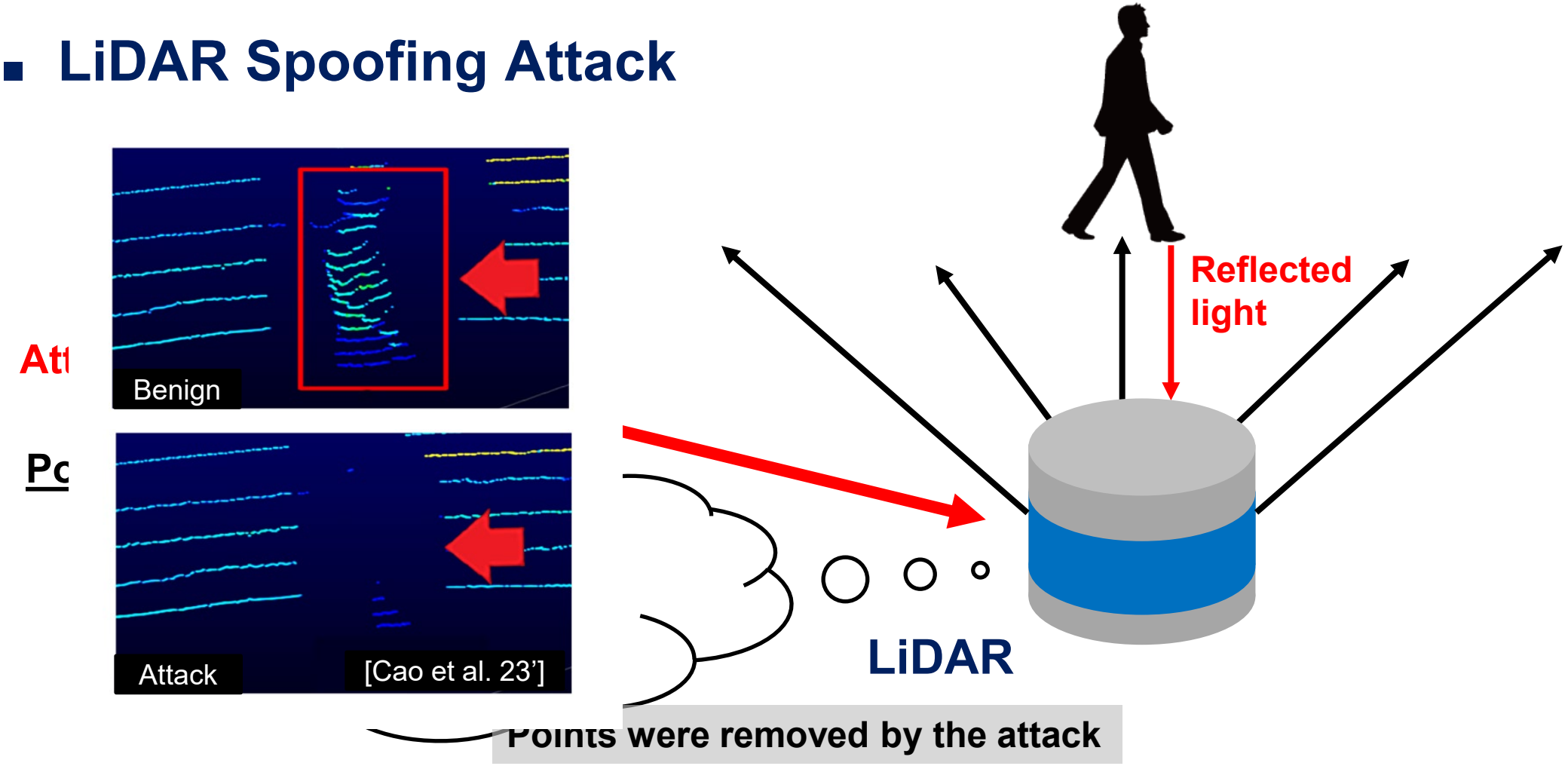
- LiDAR Spoofing Attack



Autonomous driving system fails to detect a car in front and crashes into it.

Spoofing Attack in Physical World

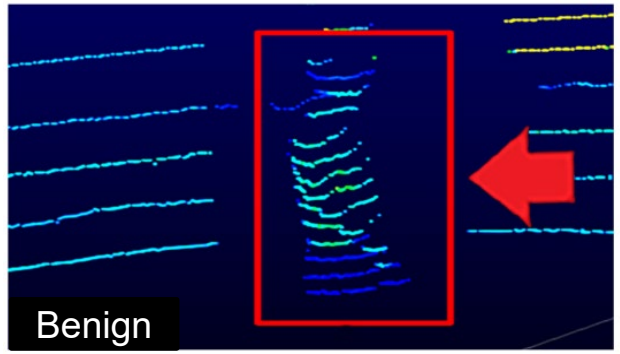
- LiDAR Spoofing Attack

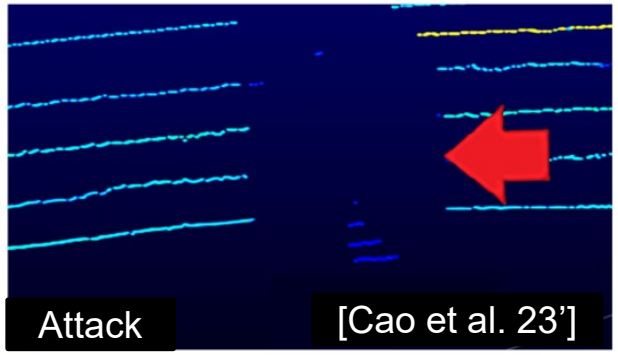


Autonomous driving system fails to detect a car in front and crashes into it.

Spoofing Attack in Physical World

- **LiDAR Spoofing Attack**





Points were remov

Predominantly validated against stationary LiDARs☹

Autonomous driving system fails to detect a car in front and crashes into it.

Limitations when attacking driving AVs

L1. Lack of practical detection and tracking system capable of high speeds and long distances

L2. Lack of practical spoofing devices capable on public roads

L3. Lack of practical spoofing attacks against recent LiDARs

Previous Research (L1)

L1. Lack of practical detection and tracking system capable of high speeds and long distances

- **Prior Attempt to Attack Moving Vehicles**

	Maximum Speed	Maximum Attack Range	Attack on AD Vehicle
Ours	**60 km/h**	**110 m**	✓
Cao et al. [12]	5 km/h	10 m	-
Cao et al. [14]	0.4 km/h	4 m	-
Jin et al. [10]	0 km/h (running parallel)	15 m	-

Low Speed **Close Range**

- **This is because of the lack of practical detection and tracking system**

Previous Research (L2)

L2. Lack of practical spoofing devices capable on public roads

- **Prior Attempt to Attack Moving Vehicles**

	Maximum Speed	Maximum Attack Range	Attack on AD Vehicle
Ours	**60 km/h**	**110 m**	✓
Cao et al. [12]	5 km/h	10 m	-
Cao et al. [14]	0.4 km/h	4 m	-
Jin et al. [10]	0 km/h (running parallel)	15 m	-

Not Covered

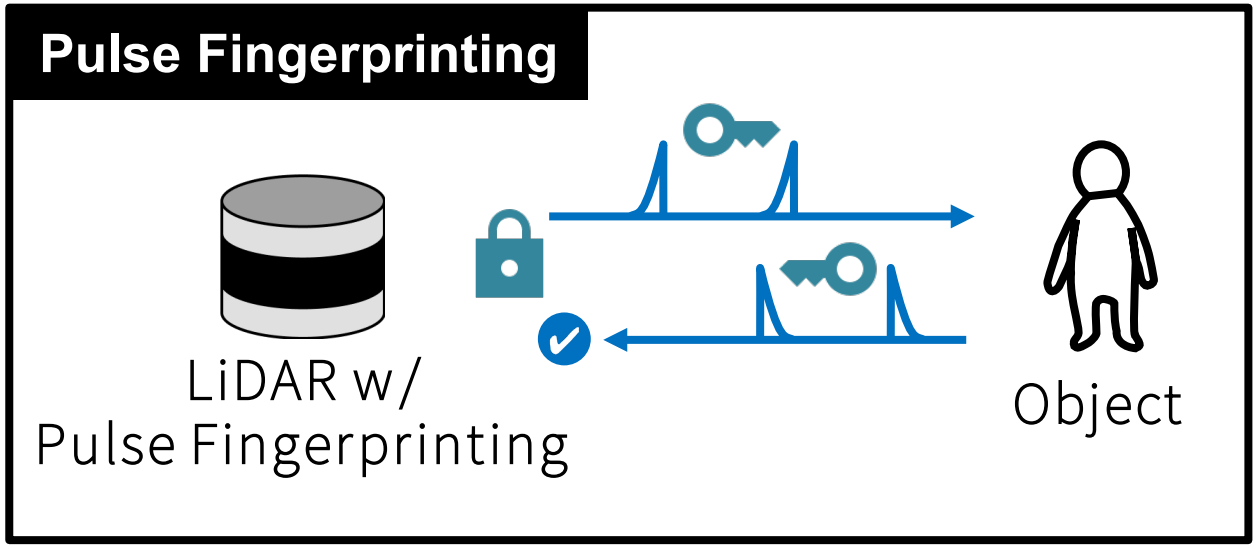
- **No existing study performed closed-loop evaluation against AVs in the physical world**

Previous Research (L3)

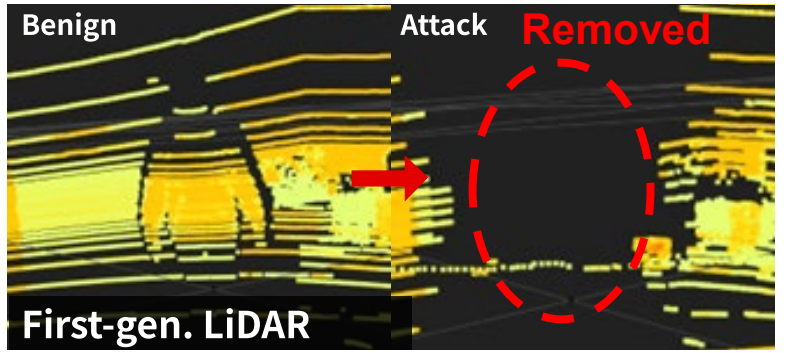
L3. Lack of practical spoofing attacks against recent LiDARs

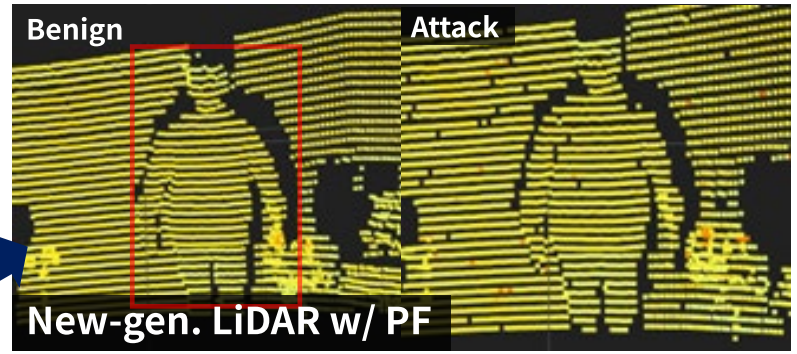
- **New-Generation LiDAR with Pulse Fingerprinting (PF)**
  - **Prevents existing spoofing attacks**

- **However, there is still a lack of security studies on recent LiDARs (L3)**
  - **Potential vulnerabilities remain unclear**



PF prevents existing attacks





Limitations in prior works

L1. Lack of practical detection and tracking system capable of high speeds and long distances

L2. Lack of practical spoofing devices capable on public roads

L3. Lack of practical spoofing attacks against recent LiDARs

Limitations in prior works

L1. Lack of practical detection and tracking system capable of

RQ: Can LiDAR spoofing attacks actually have end-to-end safety impacts in practical AD scenarios?

L3. Lack of practical spoofing attacks against recent LiDARs

Contributions

- **Design a novel LiDAR spoofing system for practical AD scenarios**
  - **Developed the MVS system, a powerful spoofer composed of three subsystems**
  - **Can aim at a target vehicle at 60 km/h from 110 meters away**

- **Design new removal attack on New-Gen LiDARs w/ Pulse Fingerprinting**
  - **A-HFR attack can remove ≥96% of points in attack angles**

- **First to perform closed-loop attack evaluation in real-world AD scenarios**
  - **Achieves ≥96% success rate on vehicles at 60 km/h up to braking distance**
  - **Demonstrated closed-loop attack on a vehicle with a popular AD stack in real-world**

Contributions

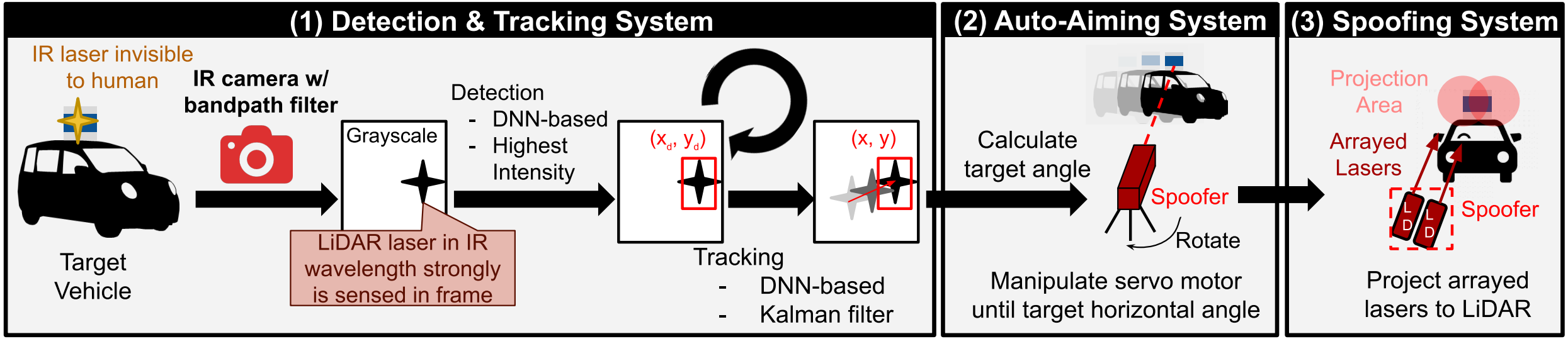
- **Design a novel LiDAR spoofing system for practical AD scenarios**
  - **Developed the MVS system, a powerful spoofer composed of three subsystems**
  - **Can aim at a target vehicle at 60 km/h from 110 meters away**

- **Design new removal attack on New-Gen LiDARs w/ Pulse Fingerprinting**
  - **A-HFR attack can remove ≥96% of points in attack angles**

- **First to perform closed-loop attack evaluation in real-world AD scenarios**
  - **Achieves ≥96% success rate on vehicles at 60 km/h up to braking distance**
  - **Demonstrated closed-loop attack on a vehicle with a popular AD stack in real-world**

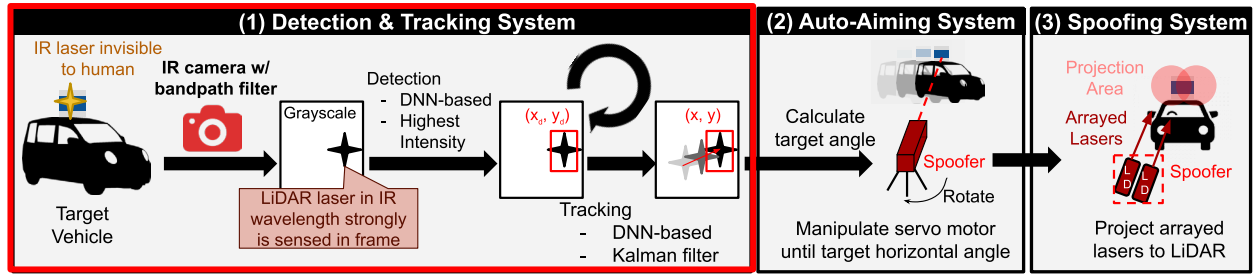
MVS System: Overview

- **Consisted of 3 subsystems**
  1. **Detection & Tracking System**
  2. **Auto-Aiming System**
  3. **LiDAR Spoofing System**

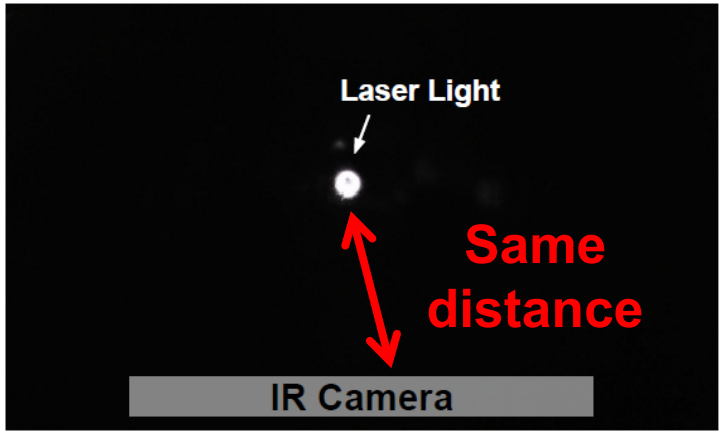


MVS System: Detection & Tracking System

- **Consisted of 3 subsystems**
  1. **Detection & Tracking System**

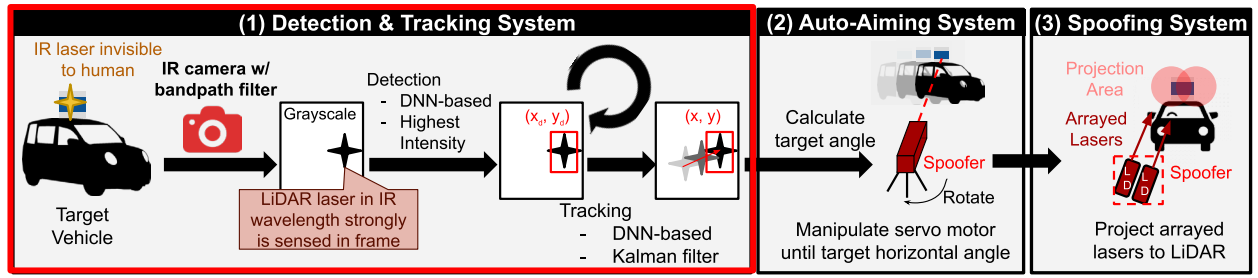


Detection



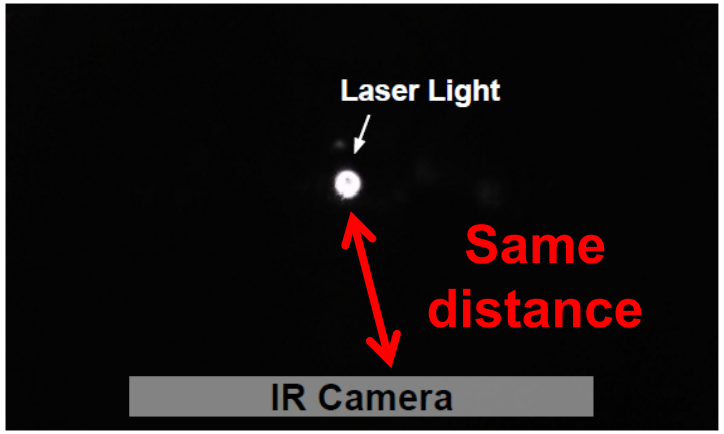
MVS System: Detection & Tracking System

- **Consisted of 3 subsystems**
  1. **D**



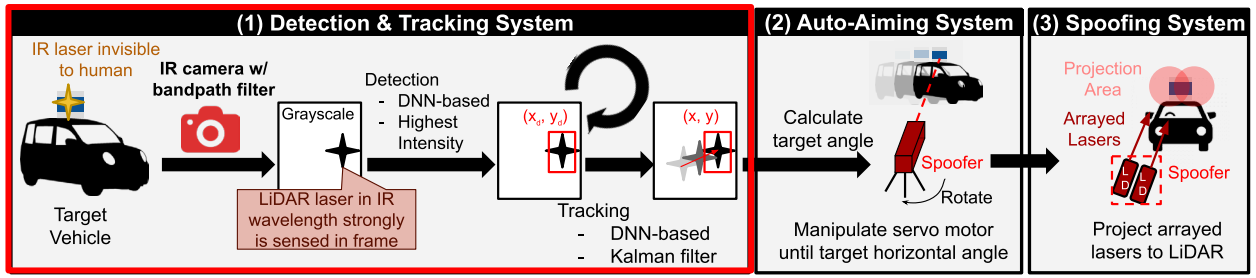
Normal cameras struggle with long-range detection

Detection



MVS System: Detection & Tracking System

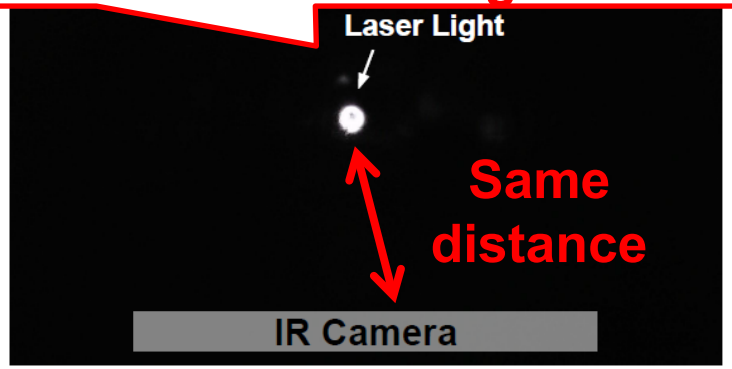
- **Consisted of 3 subsystems**
  1. **D**



Normal cameras struggle with long-range detection

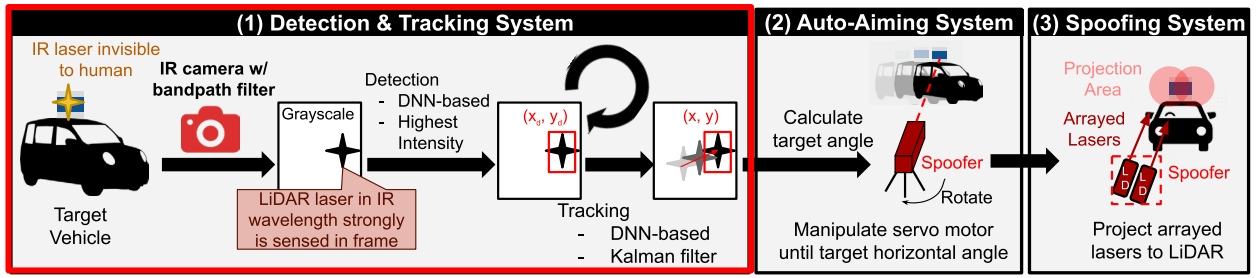
Detection

IR camera stably detects LiDAR position even at long distances.



MVS System: Detection & Tracking System

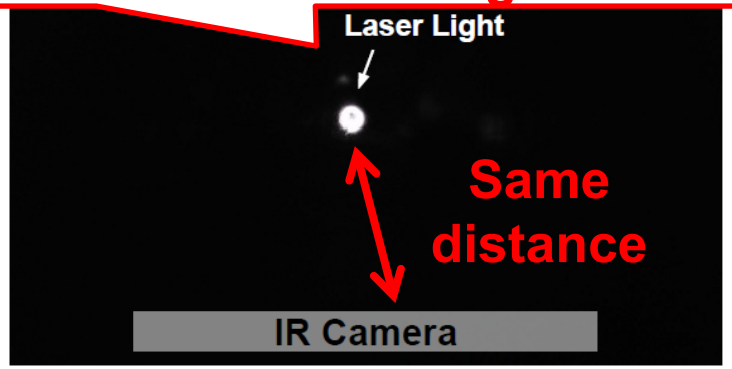
- **Consisted of 3 subsystems**
  1. [illegible]



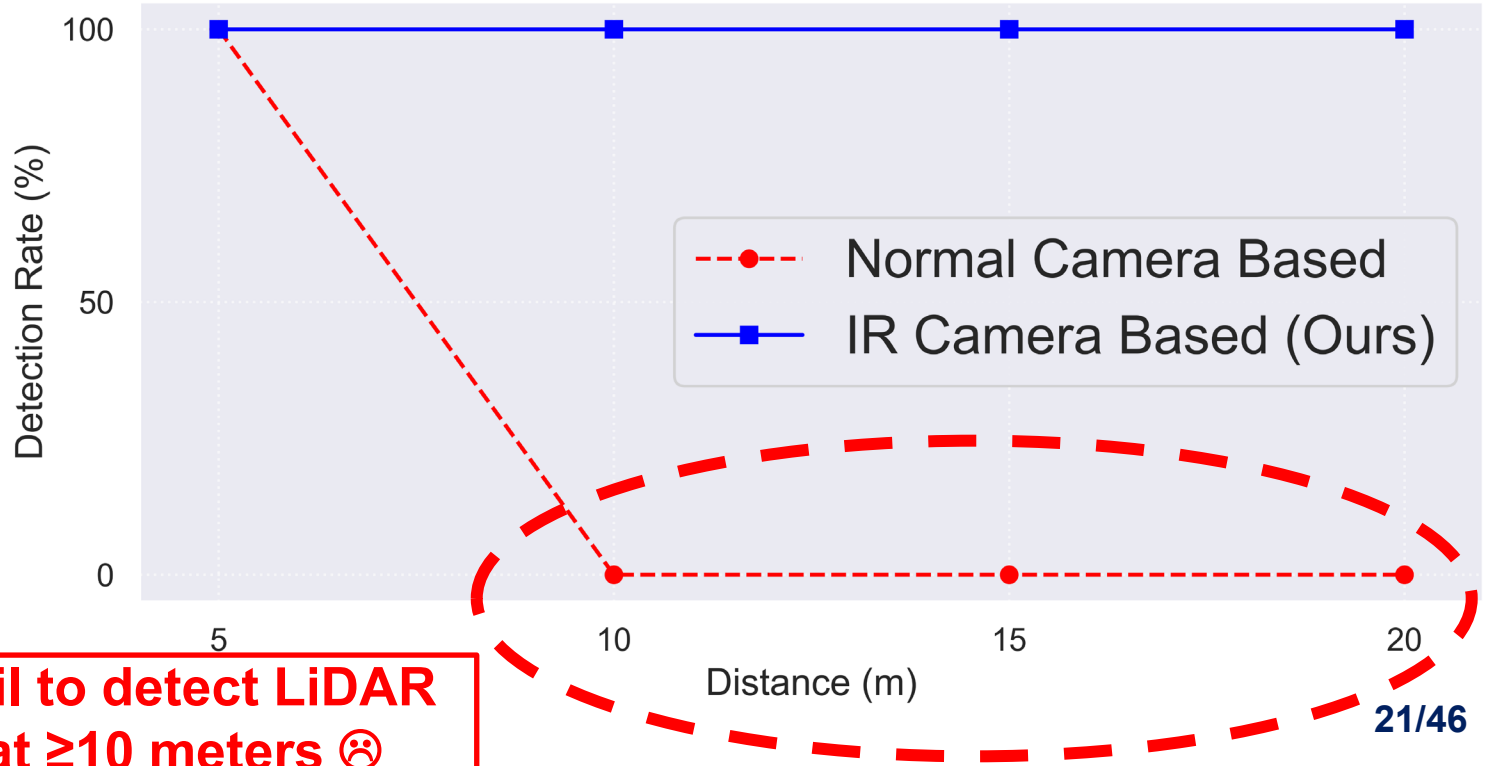
Normal cameras struggle with long-range detection

Detection

IR camera stably detects LiDAR position even at long distances.



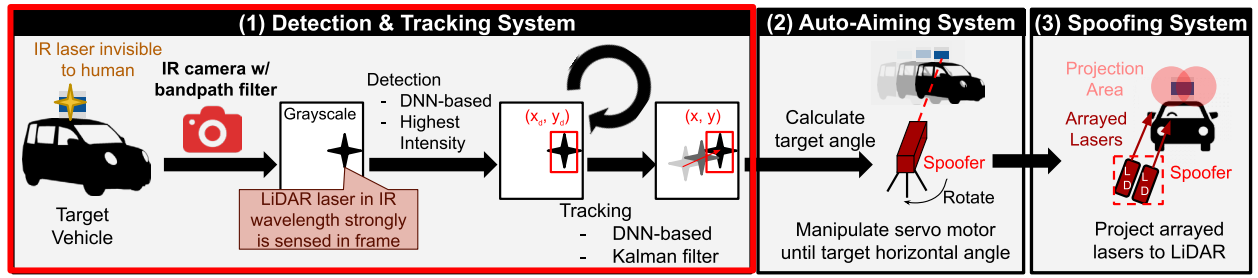
Test Result (LiDAR: VLP-32c, Detection: YOLOv5)



Fail to detect LiDAR at ≥10 meters ☹

MVS System: Detection & Tracking System

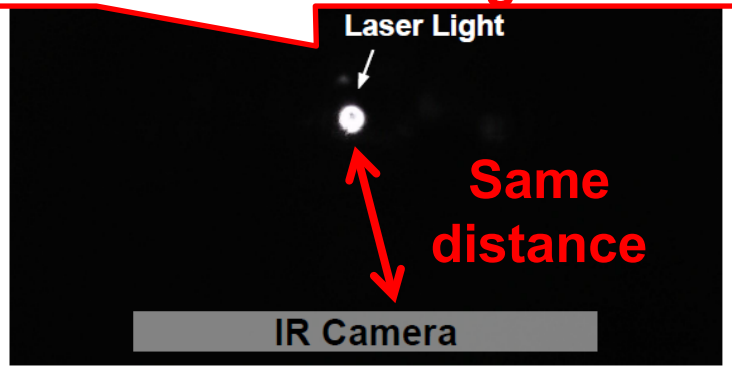
- **Consisted of 3 subsystems**
  1. [illegible]



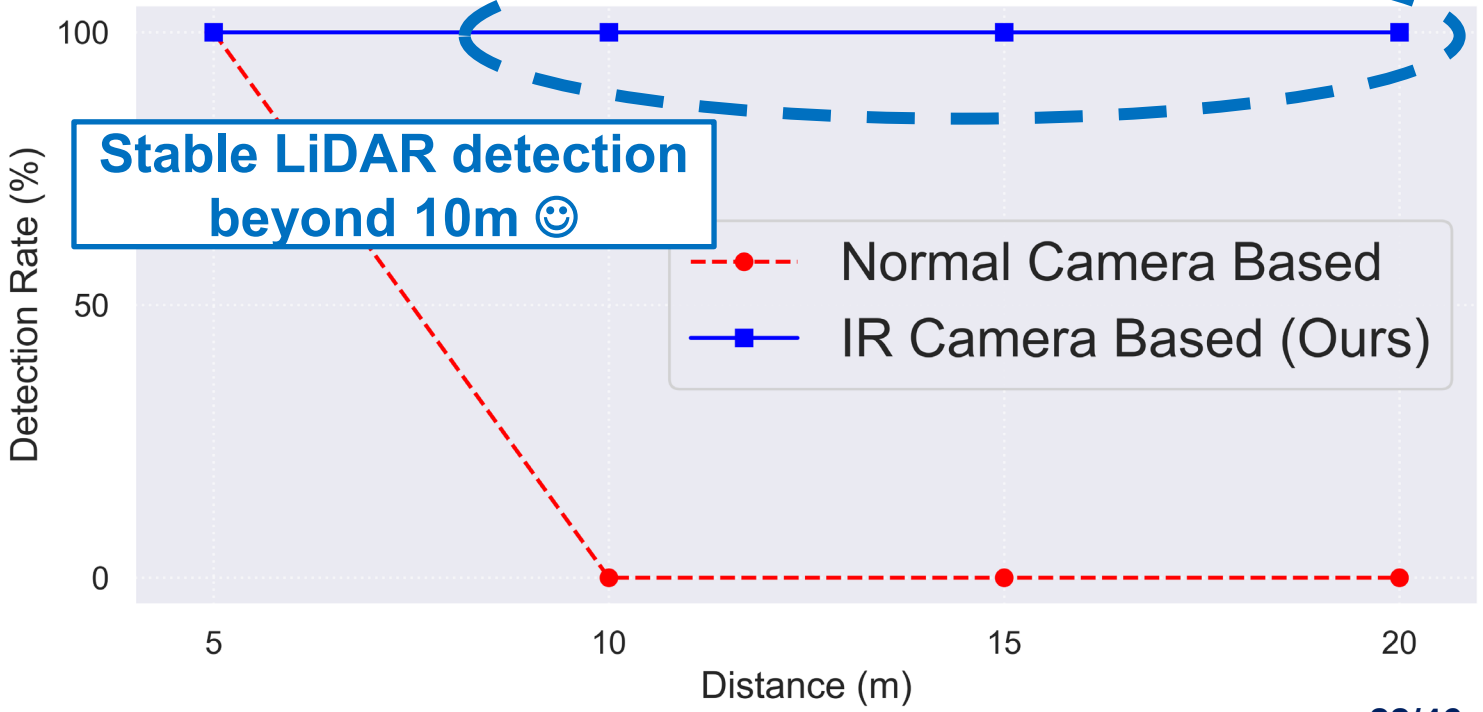
Normal cameras struggle with long-range detection

Detection

IR camera stably detects LiDAR position even at long distances.

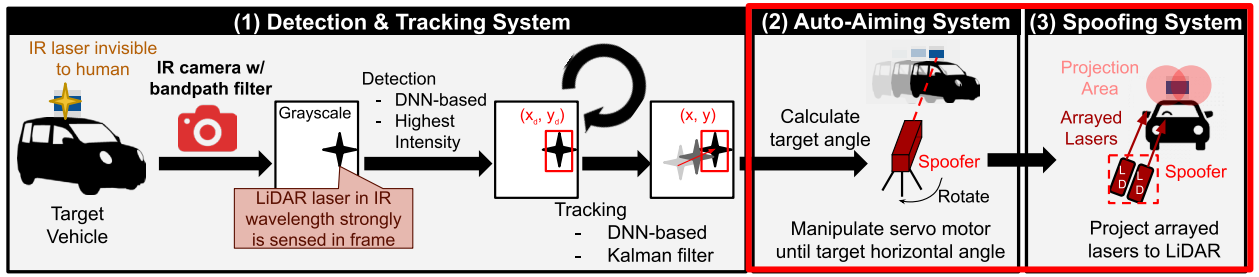


Test Result (LiDAR: VLP-32c, Detection: YOLOv5)

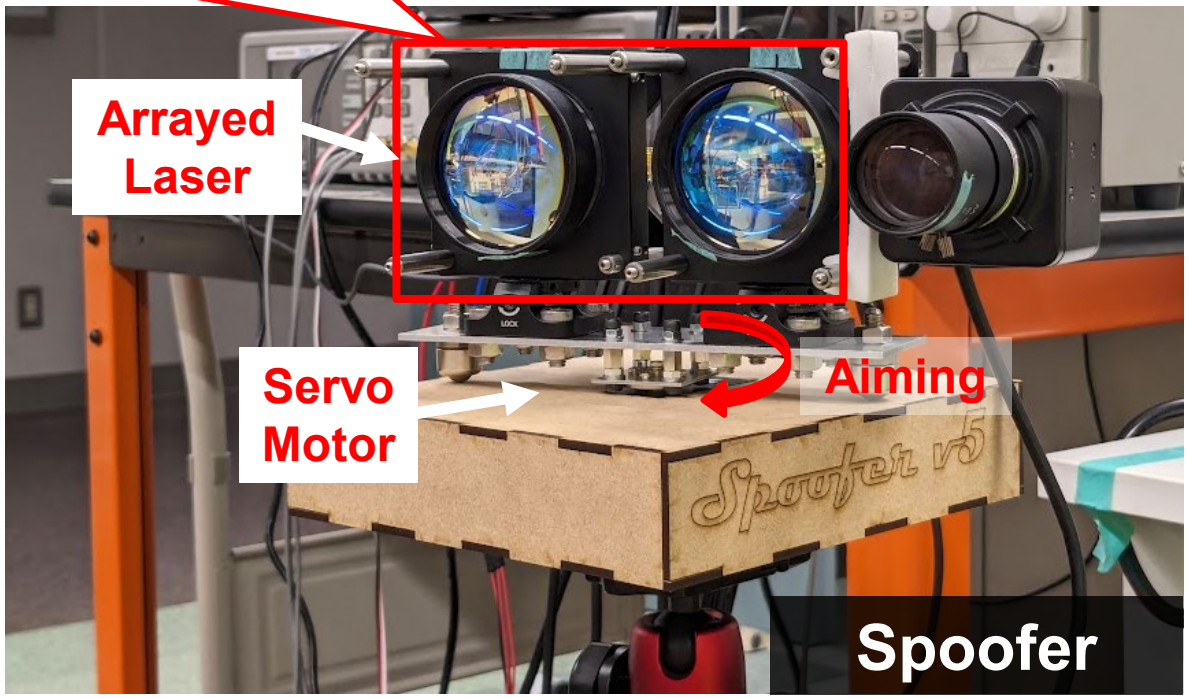


MVS System: Auto-Aiming & Spoofing Systems

- **Consisted of 3 subsystems**
  2. **Auto-Aiming System**
  3. **Spoofing System**

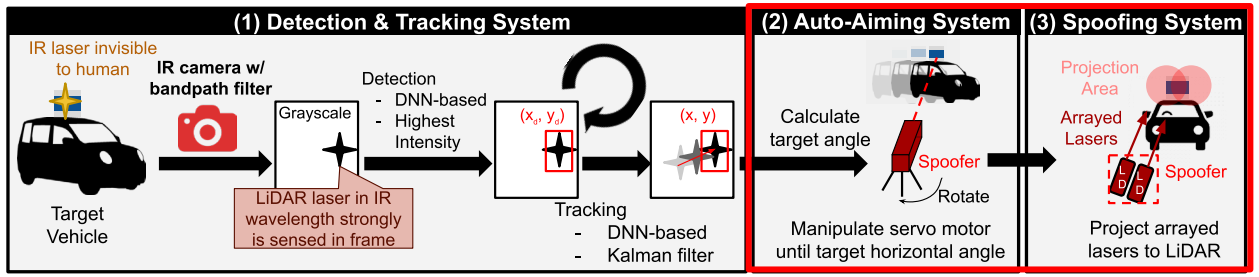


Parallelized lasers expand irradiation area for continuous attacks despite errors.

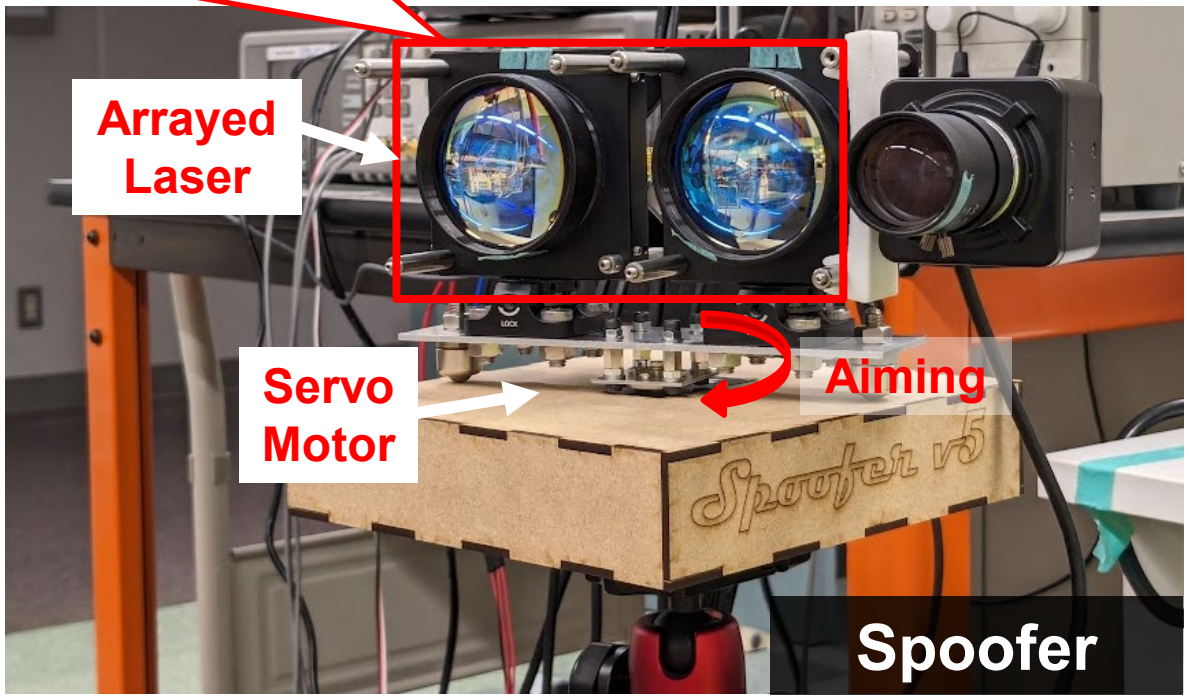


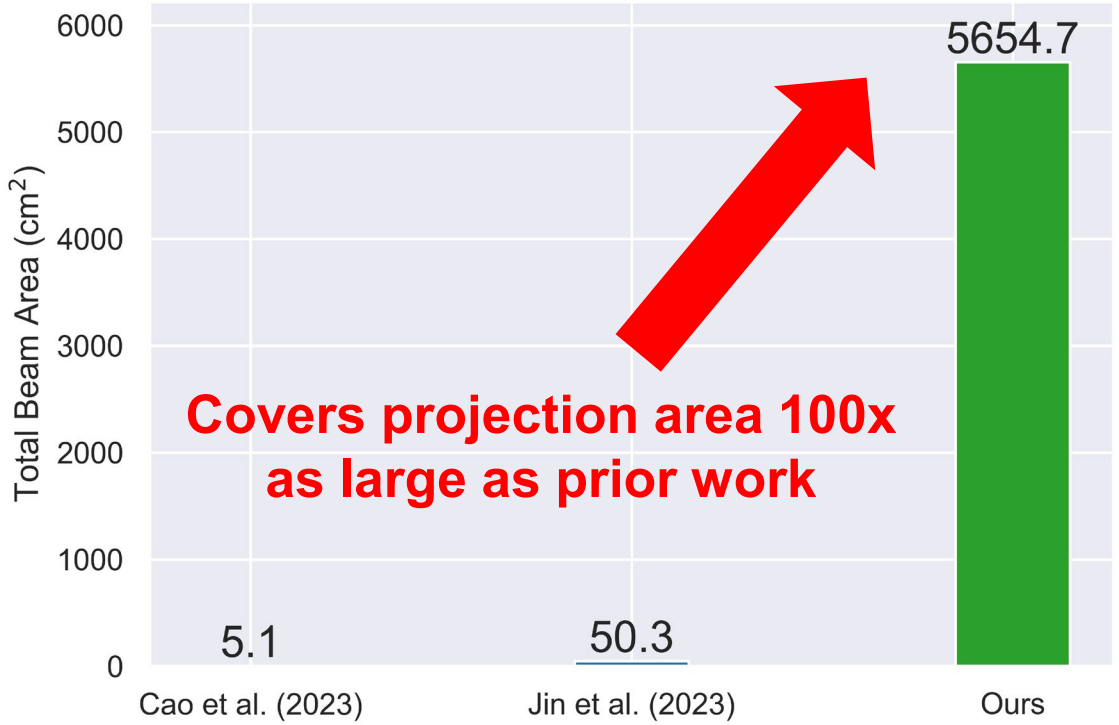
MVS System: Auto-Aiming & Spoofing Systems

- **Consisted of 3 subsystems**
  2. **Auto-Aiming System**
  3. **Spoofing System**



Parallelized lasers expand irradiation area for continuous attacks despite errors.





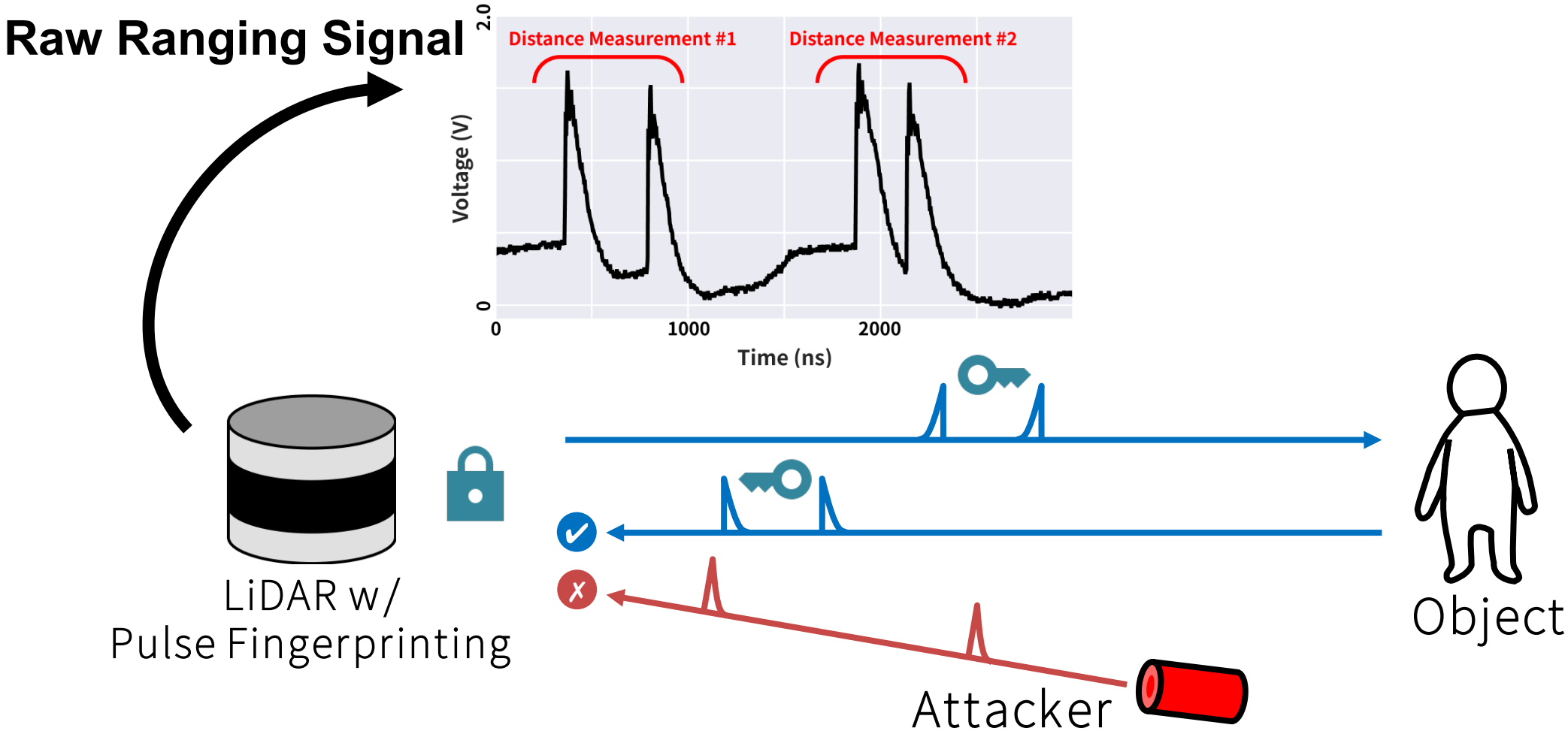
Contributions

- Design a novel LiDAR spoofing system for practical AD scenarios
  - Developed the MVS system, a powerful spoofer composed of three subsystems
  - Can aim at a target vehicle at 60 km/h from 110 meters away

- **Design new removal attack on New-Gen LiDARs w/ Pulse Fingerprinting**
  - **A-HFR attack can remove ≥96% of points in attack angles**

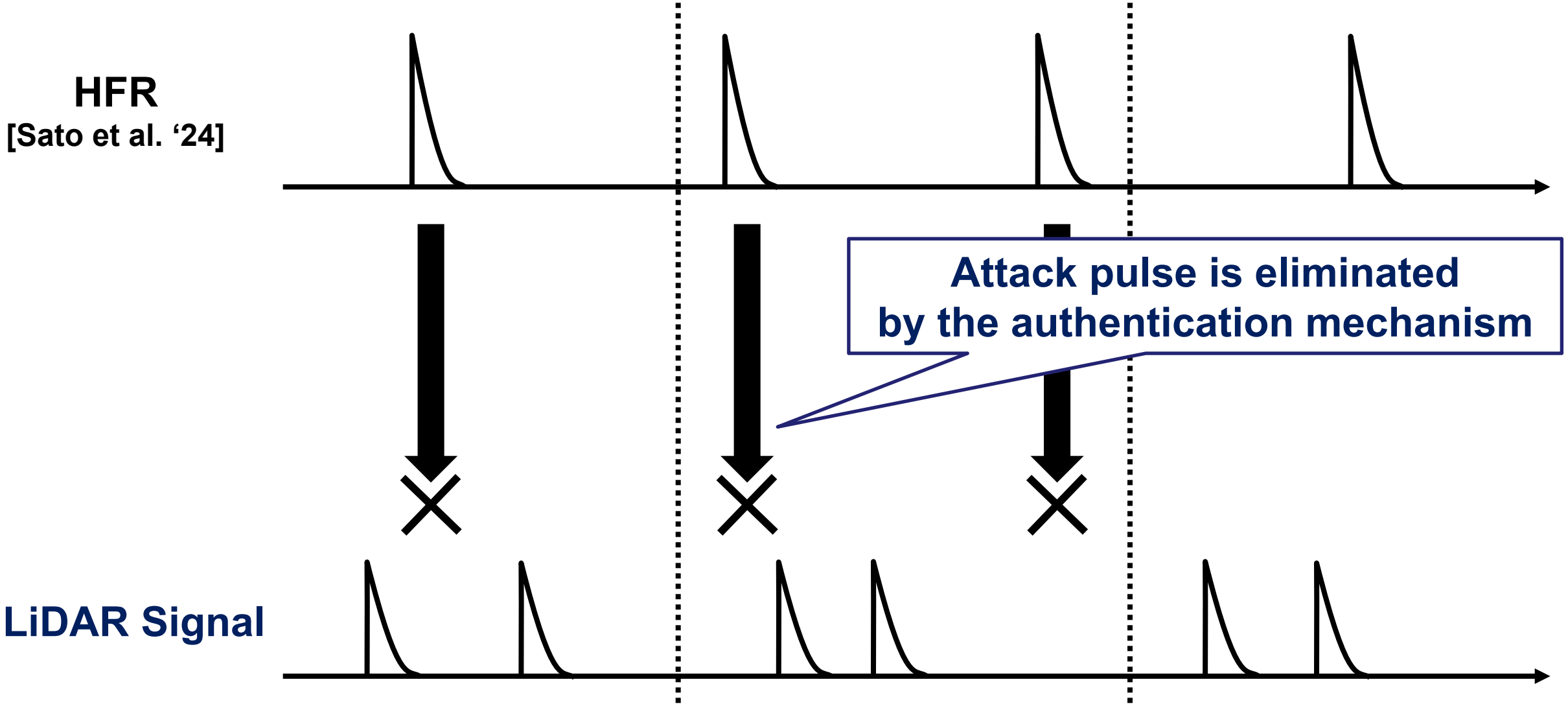
- First to perform closed-loop attack evaluation in real-world AD scenarios
  - Achieves ≥96% success rate on vehicles at 60 km/h up to braking distance
  - Demonstrated closed-loop attack on a vehicle with a popular AD stack in real-world

A New-Gen LiDAR's Feature: Pulse Fingerprinting

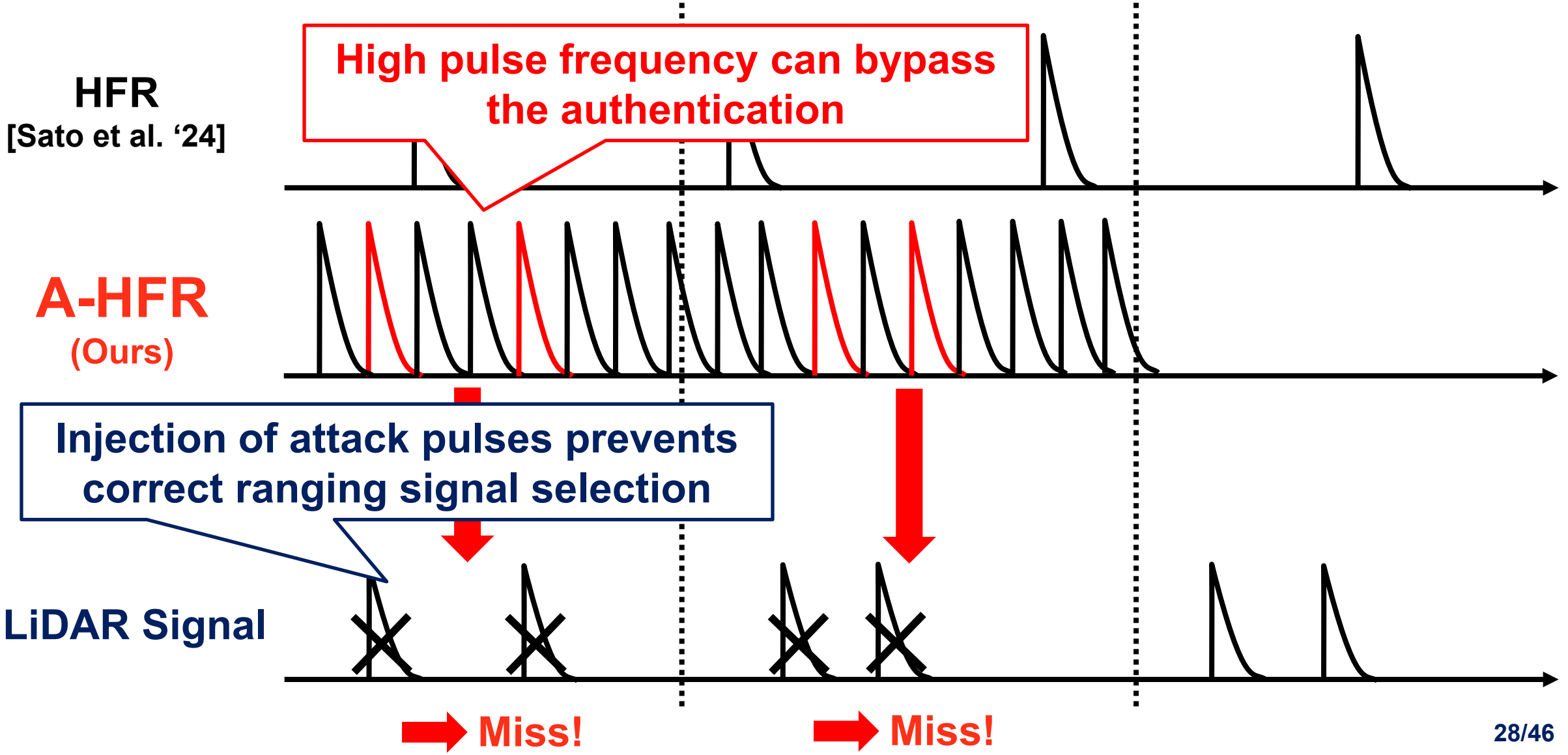


Signal fingerprint consisting of two pulses allows for attack elimination

New Attack against New-Gen LiDARs: Adaptive HFR



New Attack against New-Gen LiDARs: Adaptive HFR



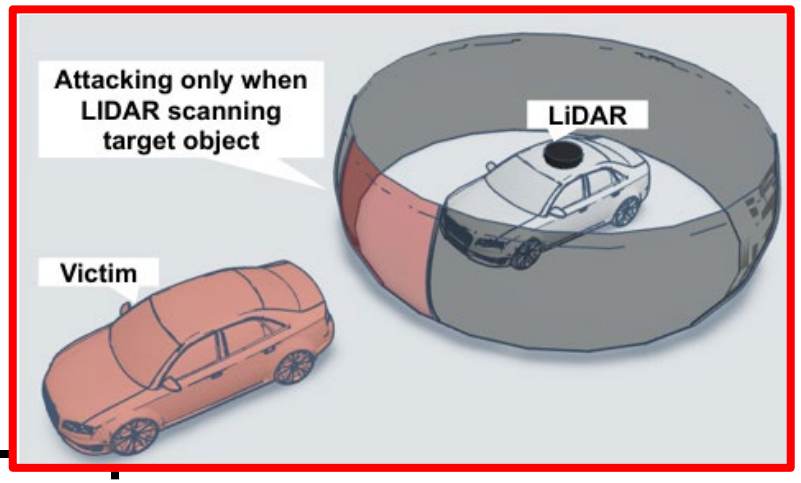
New Attack against New-Gen LiDARs: Adaptive HFR

HFR
[Sato et al. '24]

A-HFR
(Ours)

LiDAR Signal

Adaptively select attack area to burst high-freq. lasers while avoiding device overheating

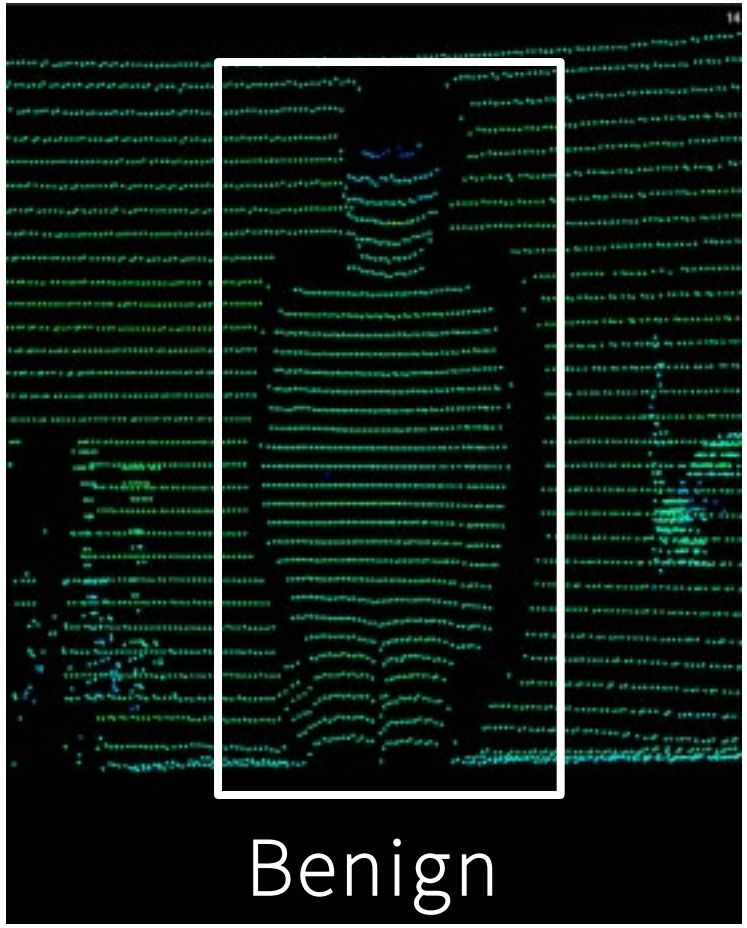


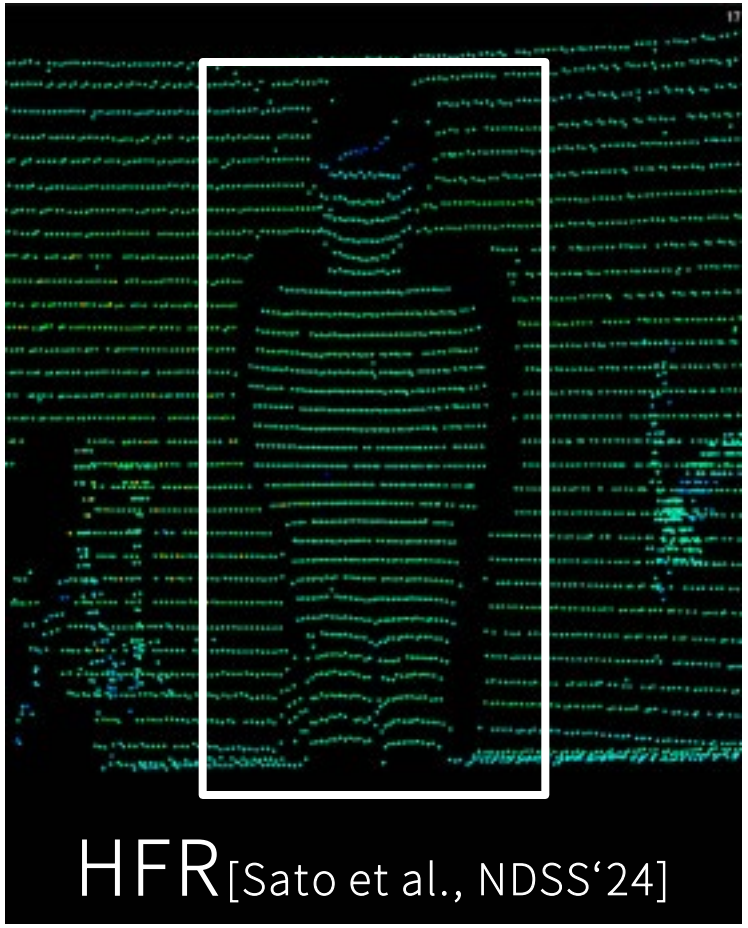
Miss!

Miss!

Indoor Demo

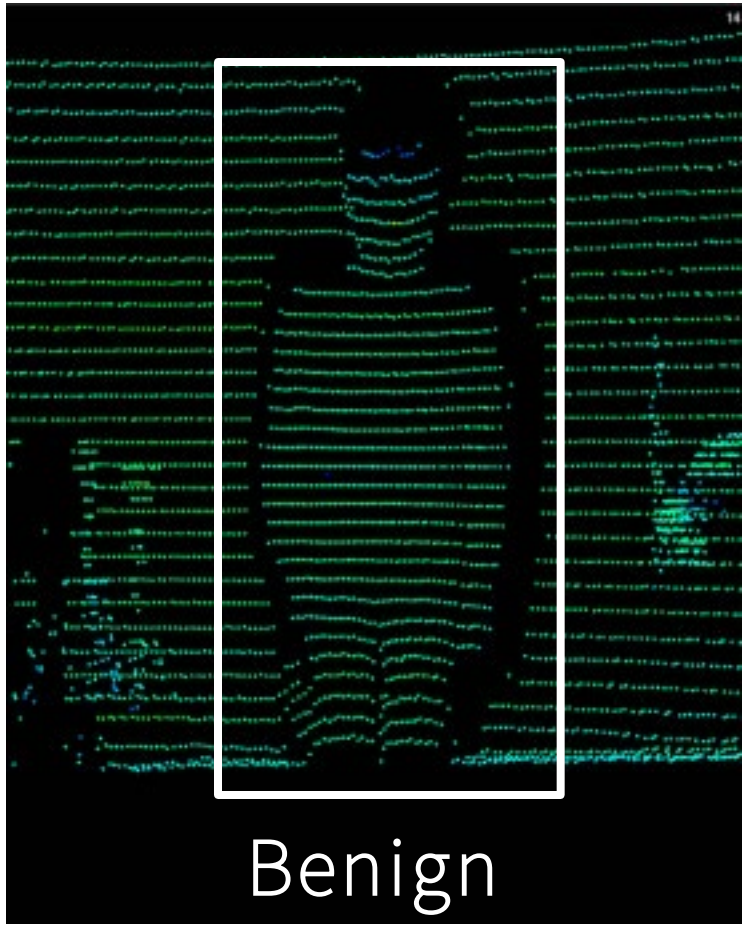
- **With A-HFR attack, person's point cloud at 3 m away is almost removed**

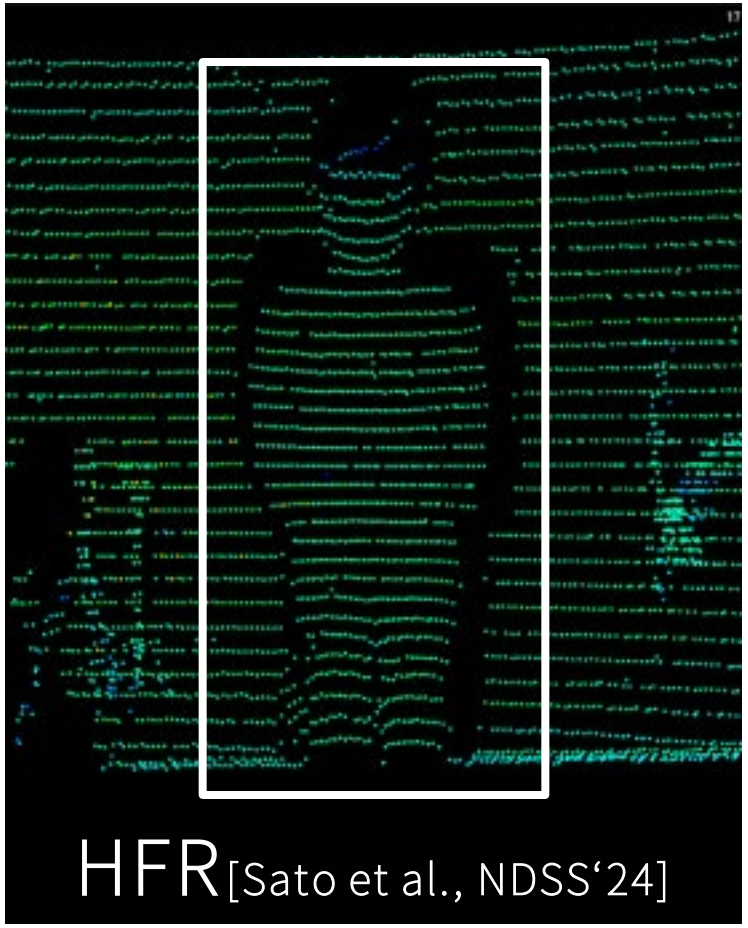


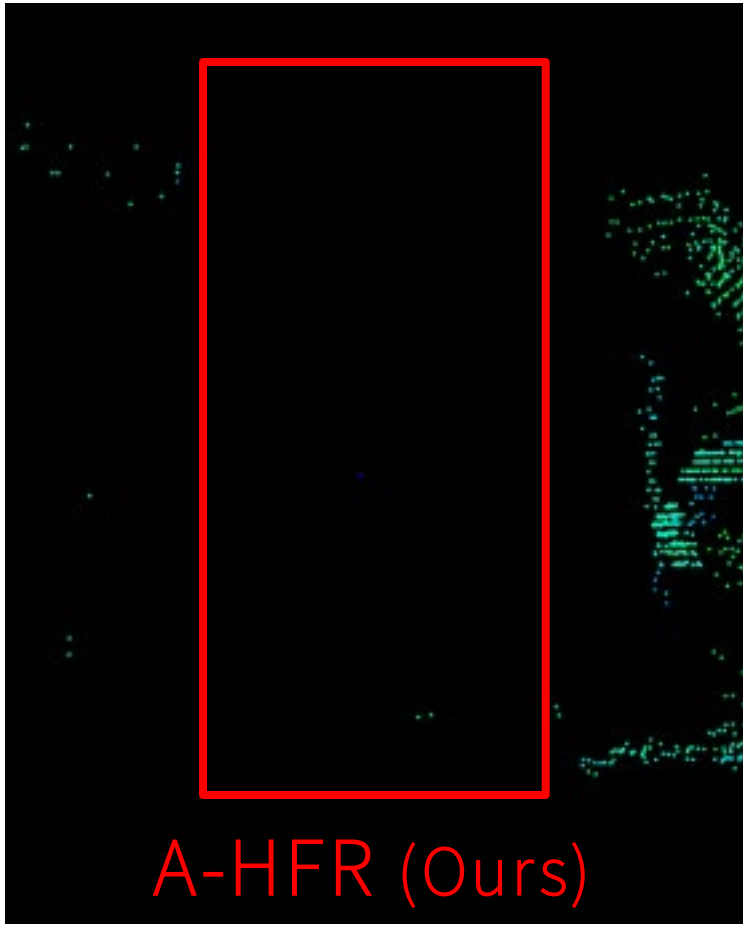


Indoor Demo

- **With A-HFR attack, person's point cloud at 3 m away is almost removed**

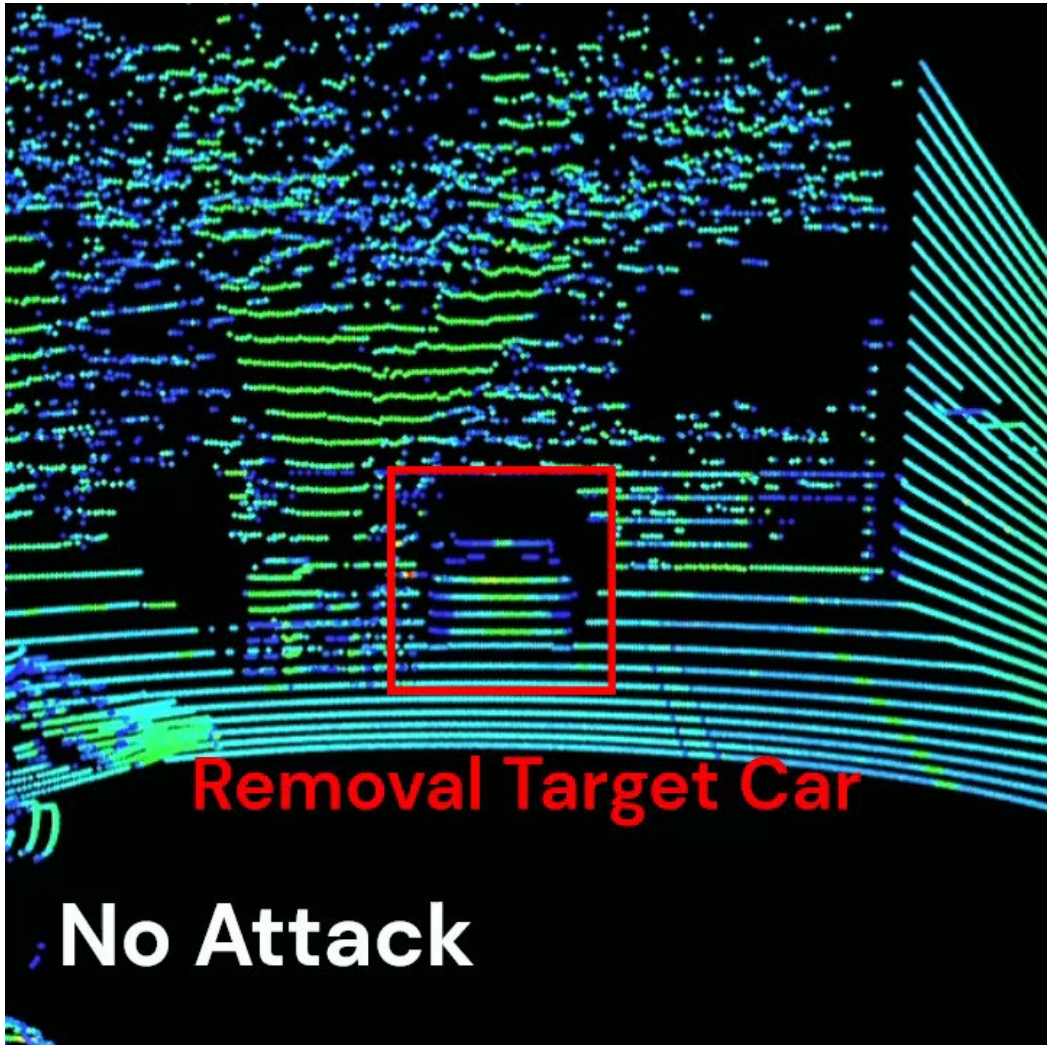


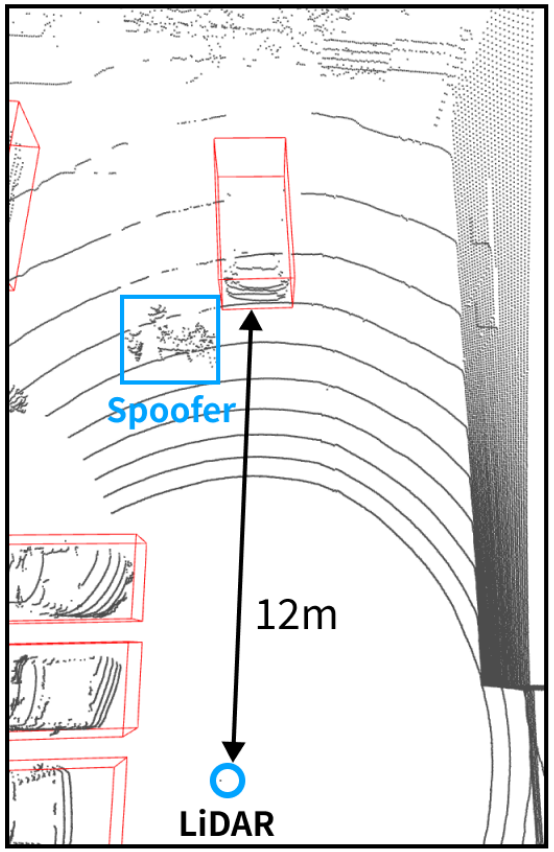




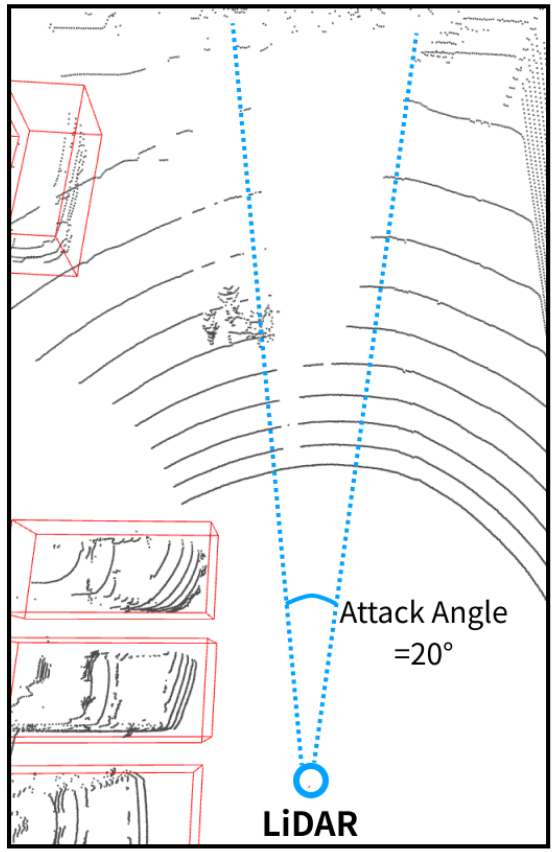
Outdoor Demo

- The car went undetected in Apollo 6.0 detector when under attack





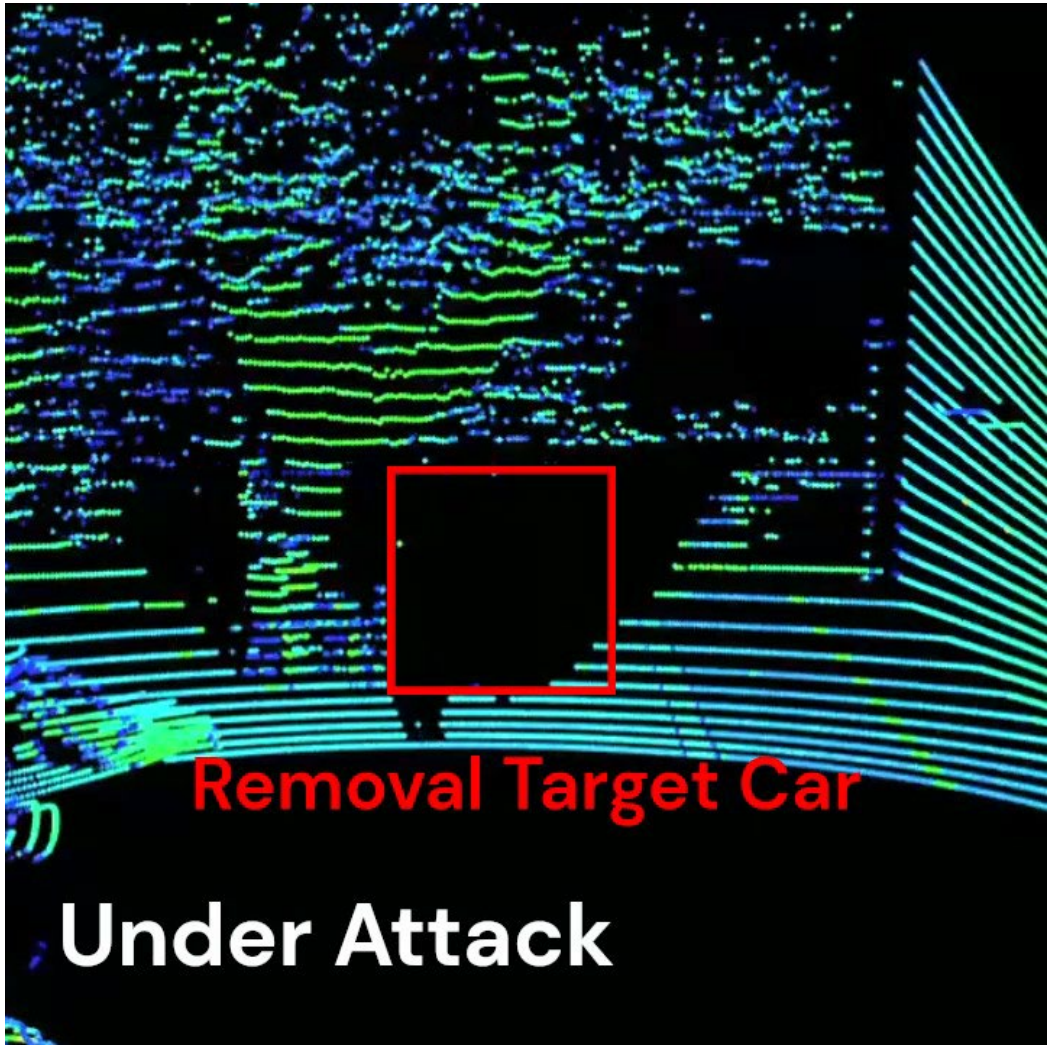
Benign

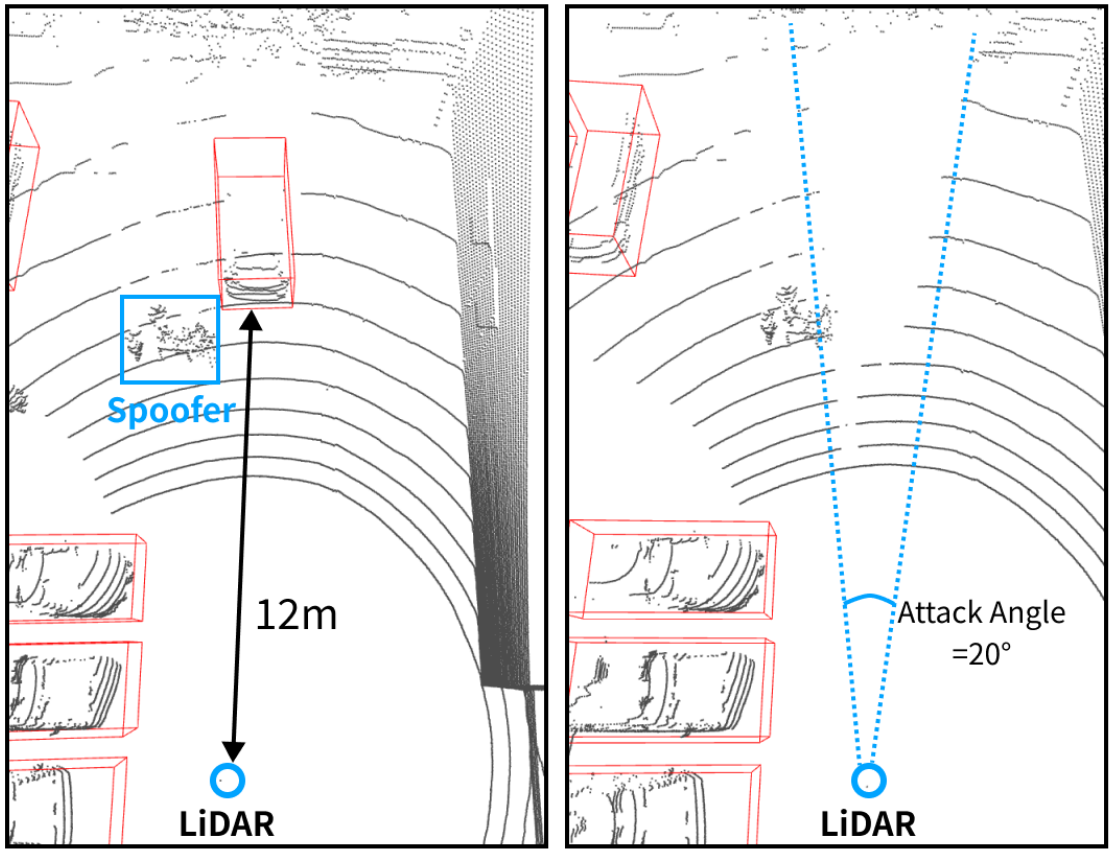


Under Attack
(24 MHz, h=20°, v=16°)

Outdoor Demo

- The car went undetected in Apollo 6.0 detector when under attack





Benign

Under Attack
(24 MHz, h=20°, v=16°)

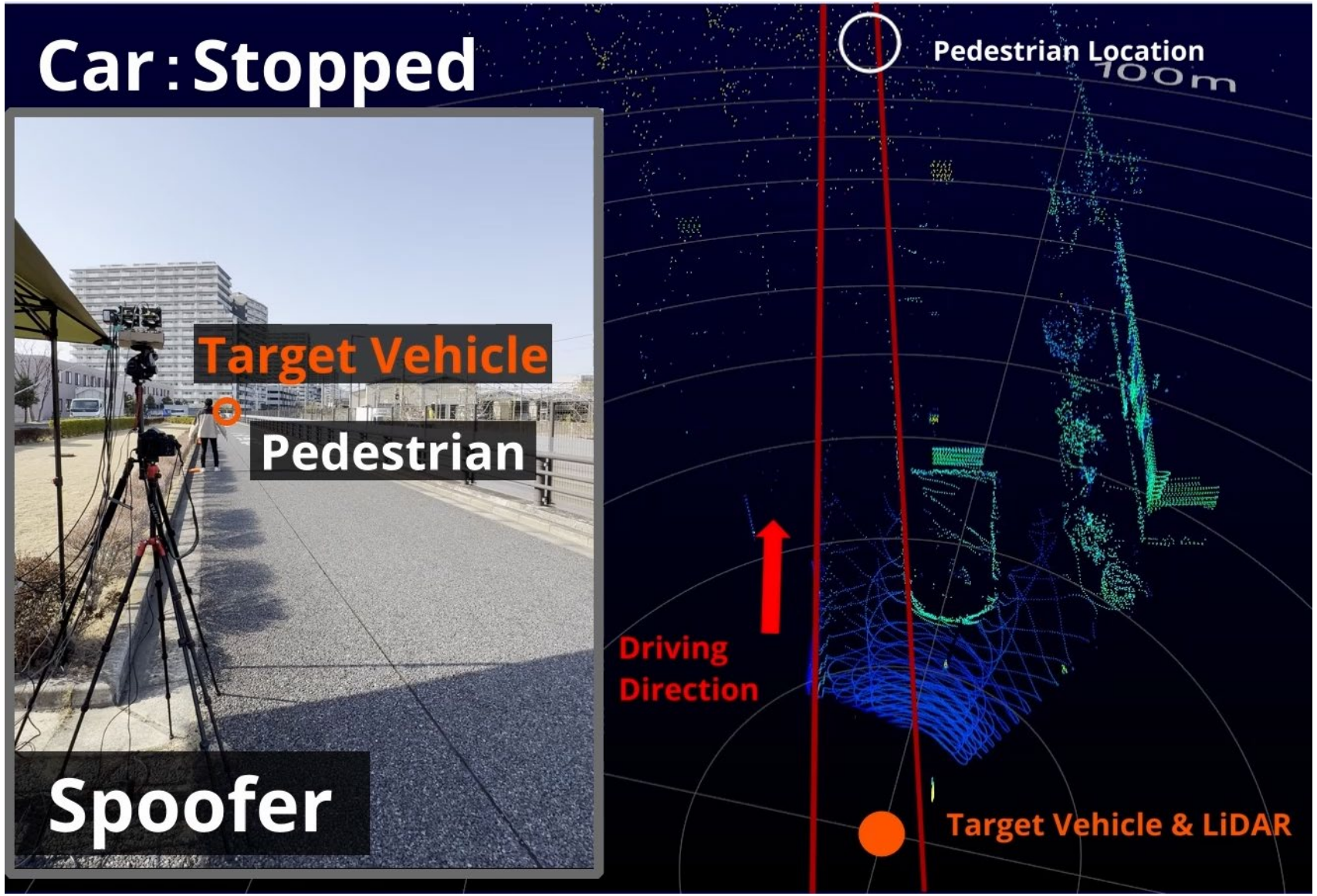
Contributions

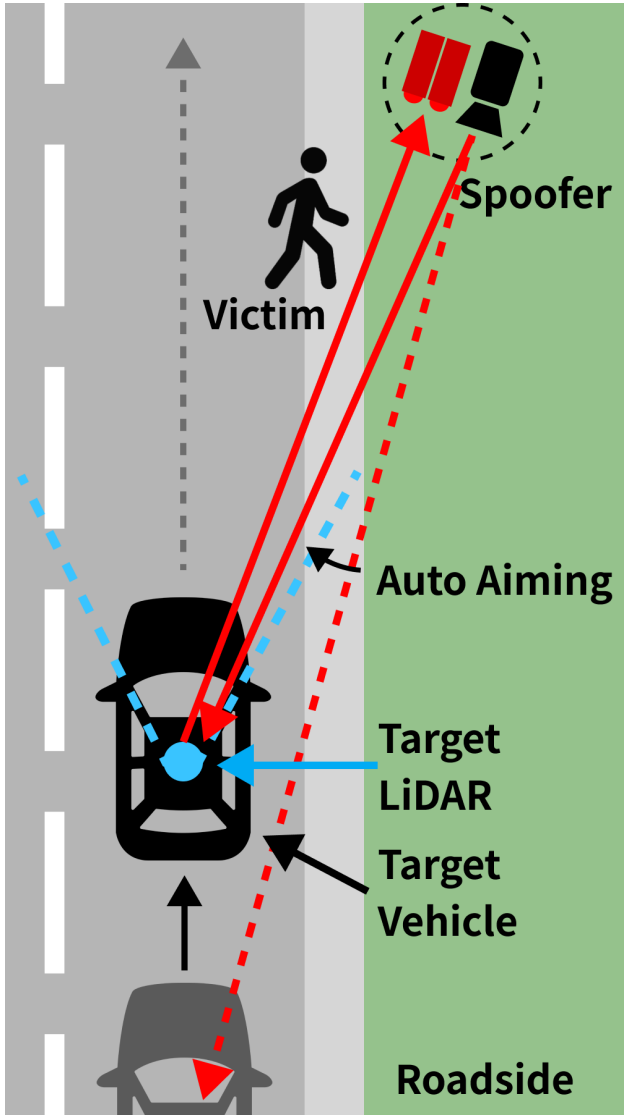
- Design a novel LiDAR spoofing system for practical AD scenarios
  - Developed the MVS system, a powerful spoofer composed of three subsystems
  - Can aim at a target vehicle at 60 km/h from 110 meters away

- Design new removal attack on New-Gen LiDARs w/ Pulse Fingerprinting
  - A-HFR attack can remove ≥96% of points in attack angles

- **First to perform closed-loop attack evaluation in real-world AD scenarios**
  - **Achieves ≥96% success rate on vehicles at 60 km/h up to braking distance**
  - **Demonstrated closed-loop attack on a vehicle with a popular AD stack in real-world**

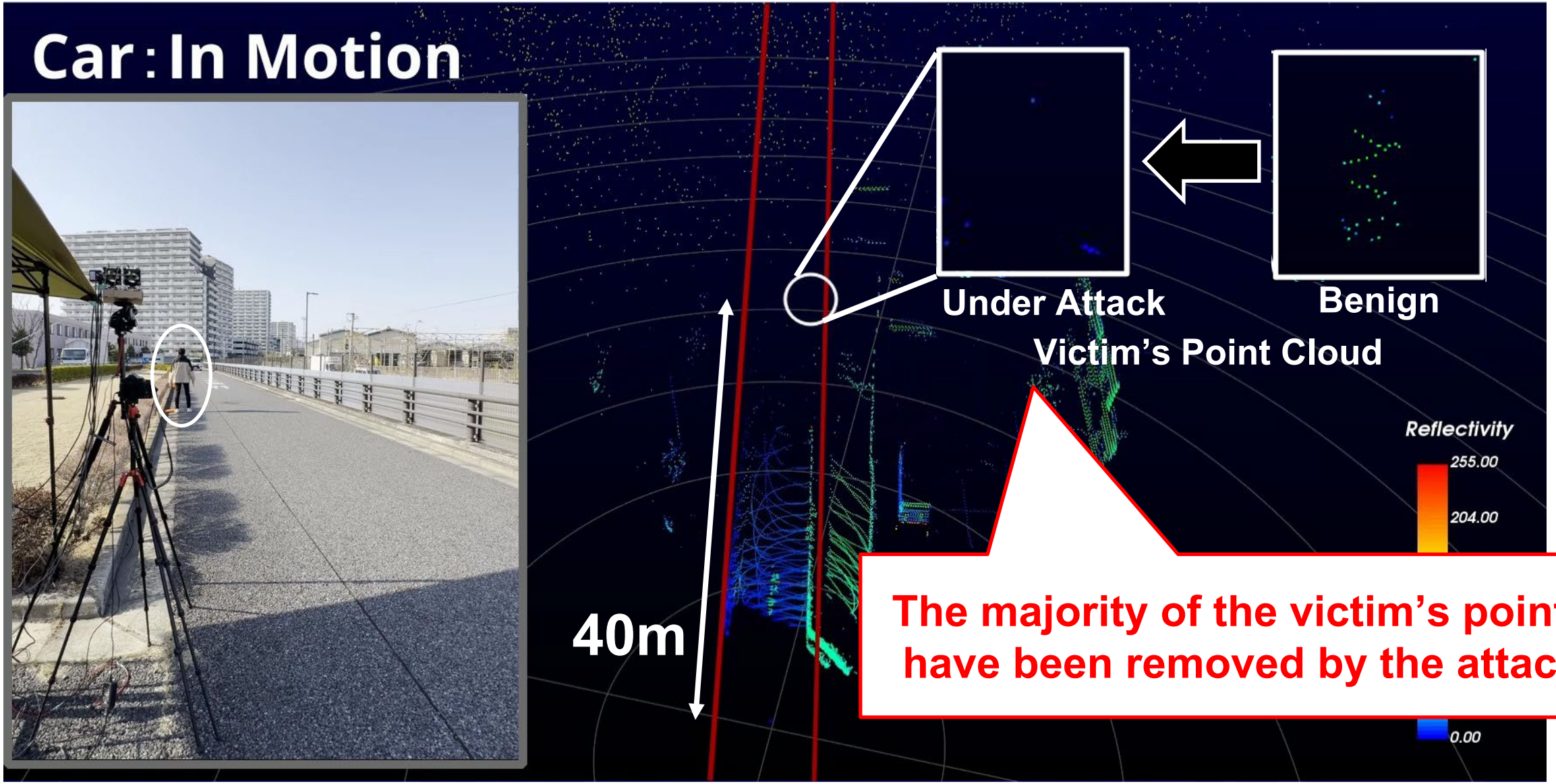
Evaluation in the High-Speed Scenario



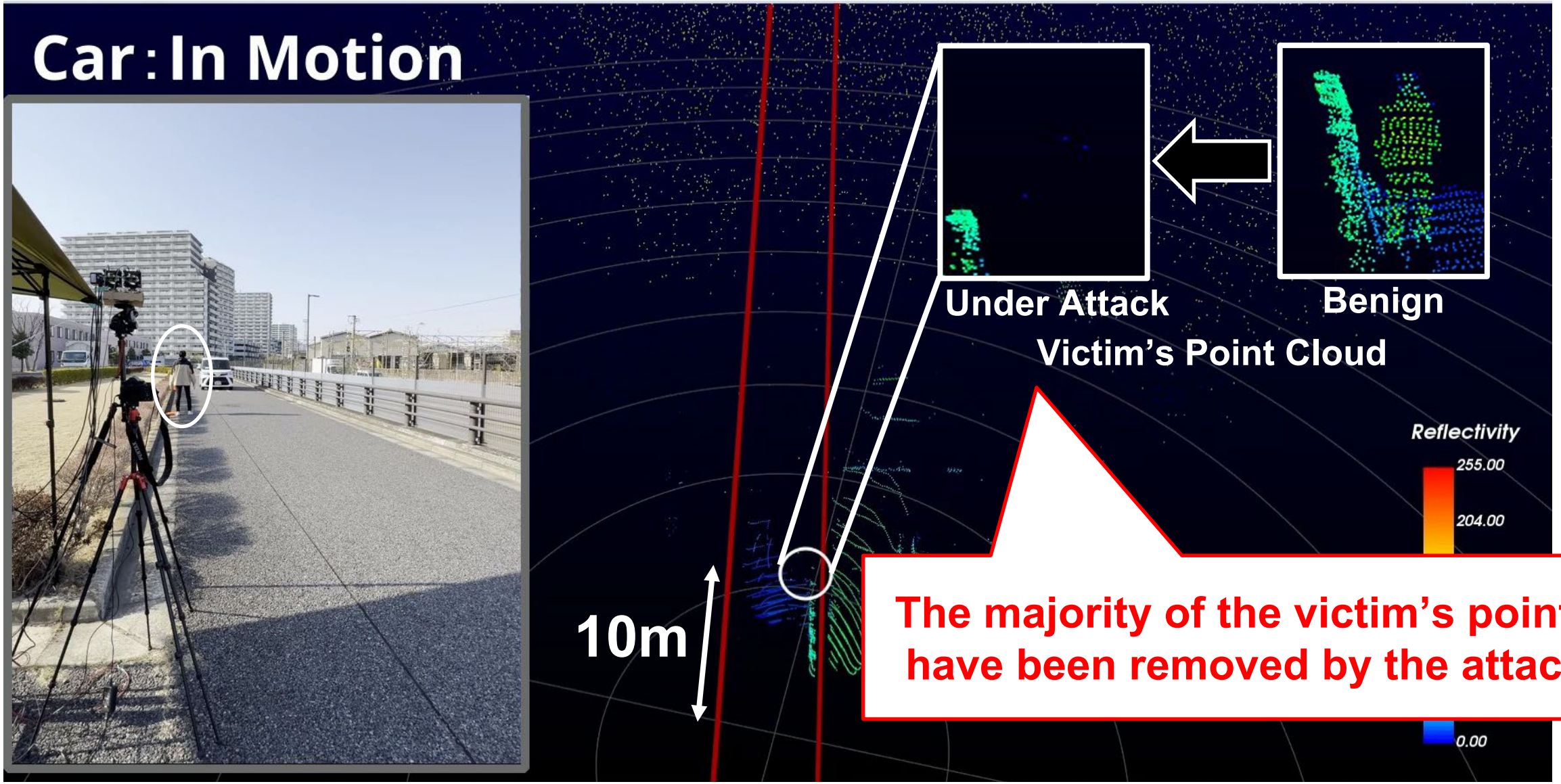


Attack Scenario

Evaluation in the High-Speed Scenario

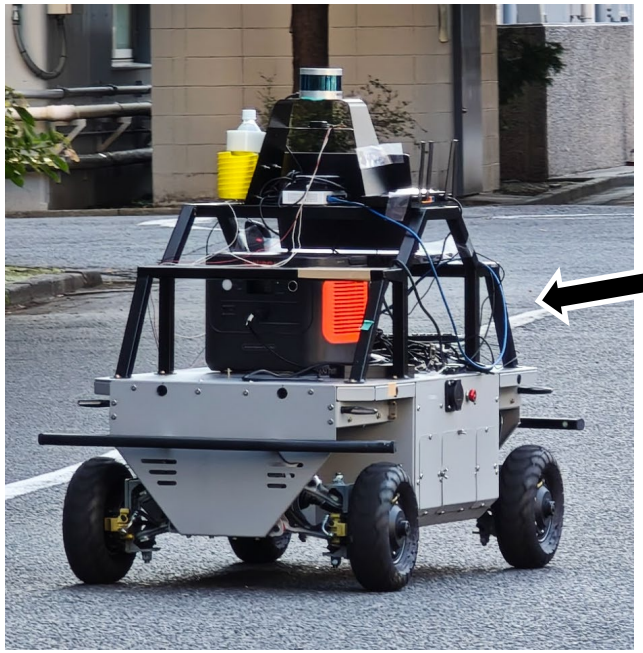


Evaluation in the High-Speed Scenario

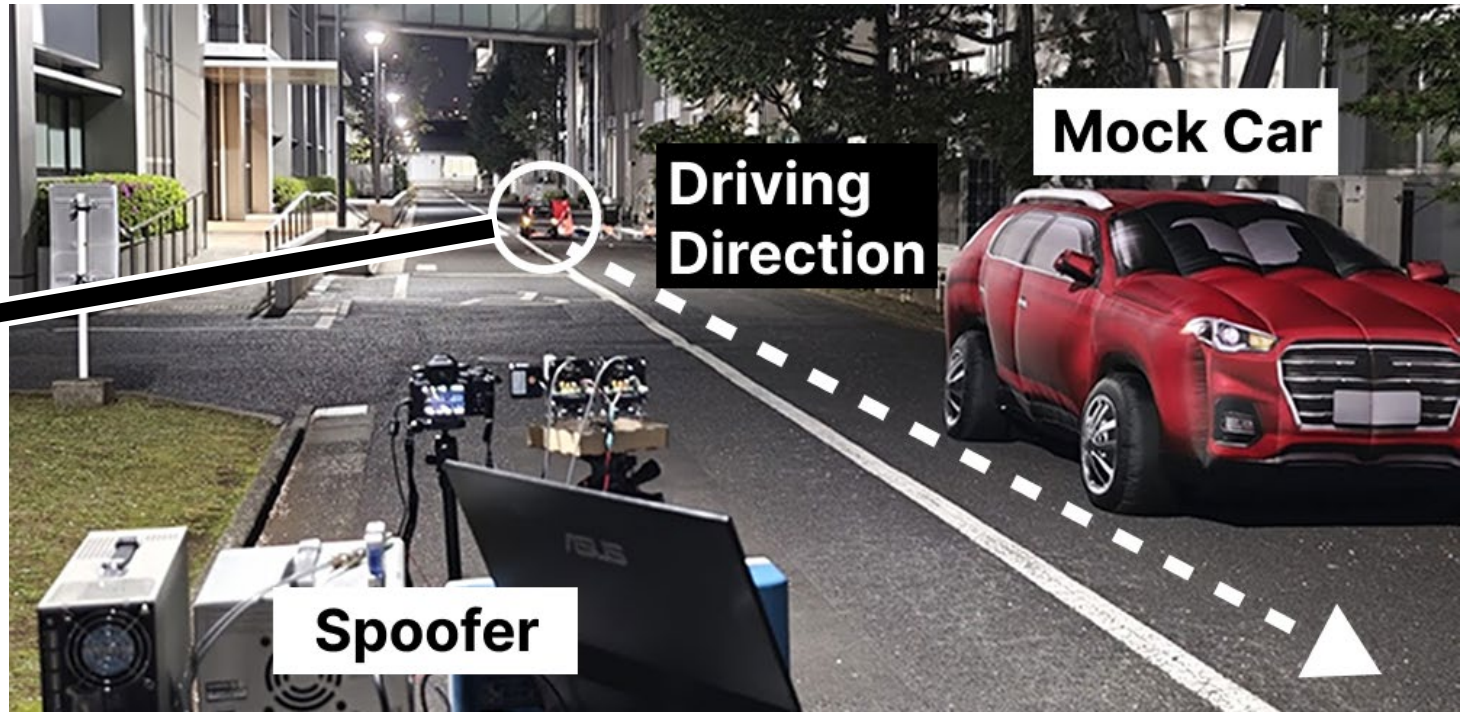


End-to-End Attack Evaluation

- **End-to-end evaluation with a popular AD stack, Autoware.ai**



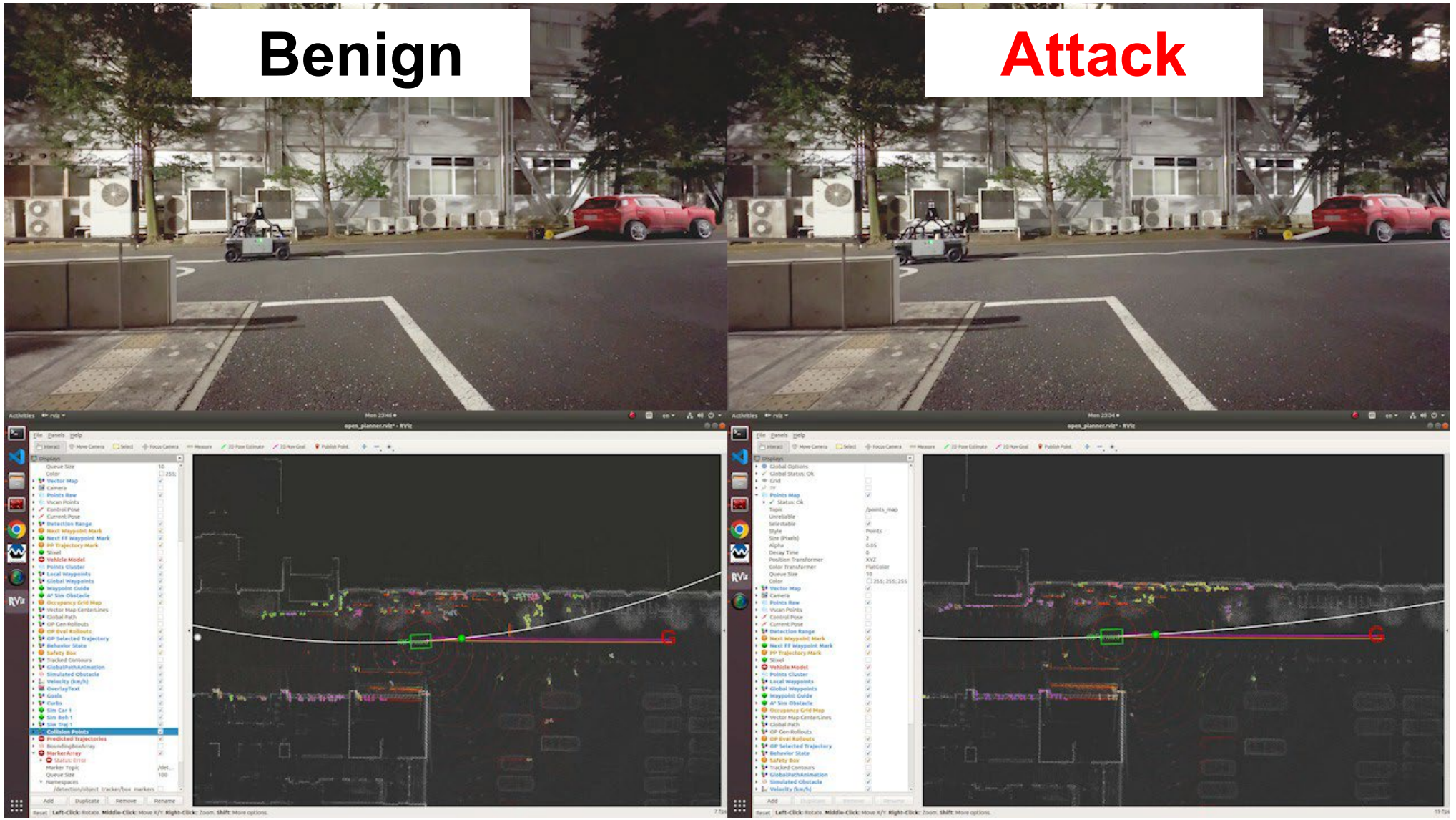
Autoware.ai on PIXKIT



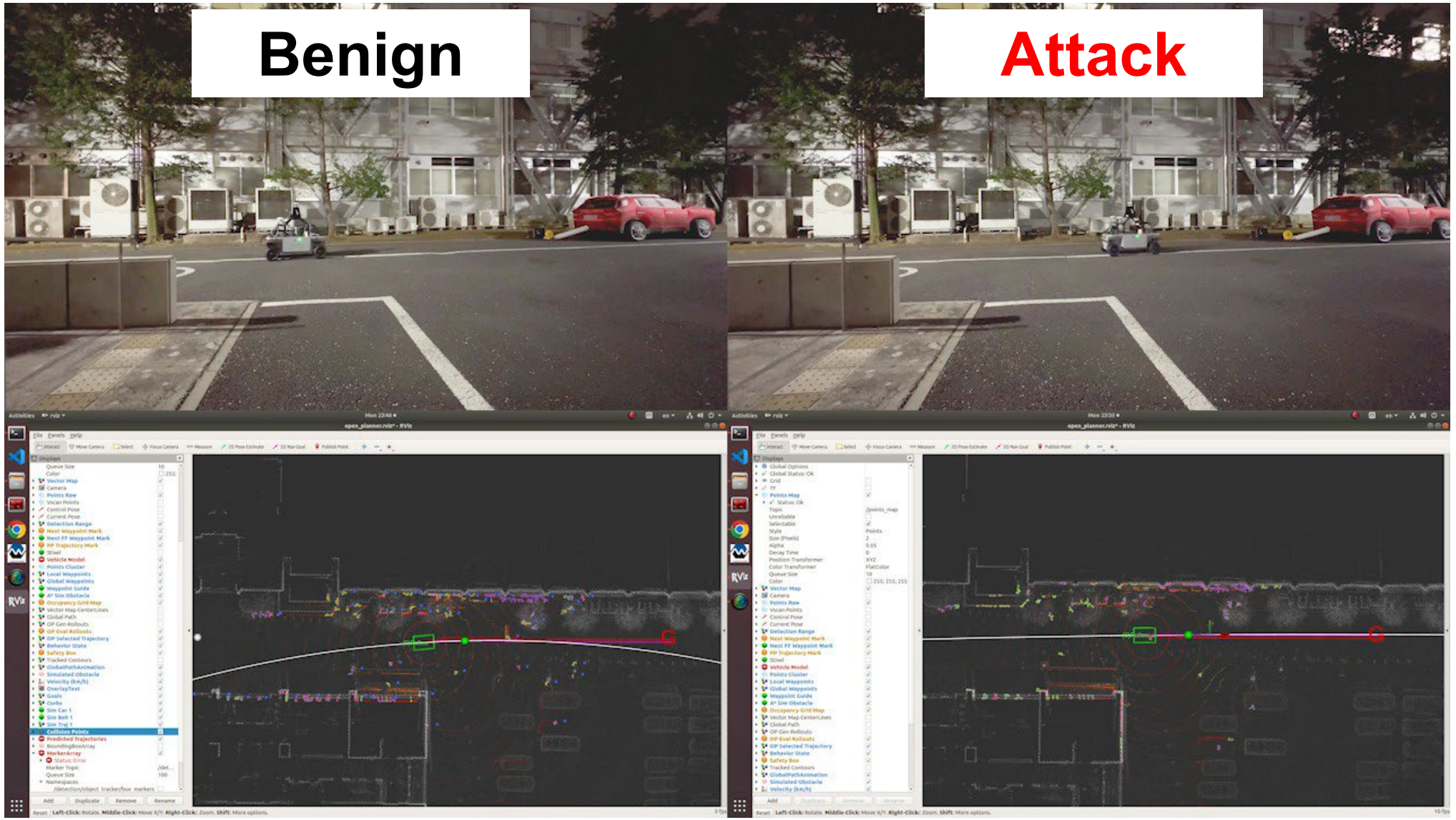
Experimental Setup

End-to-End Attack Results

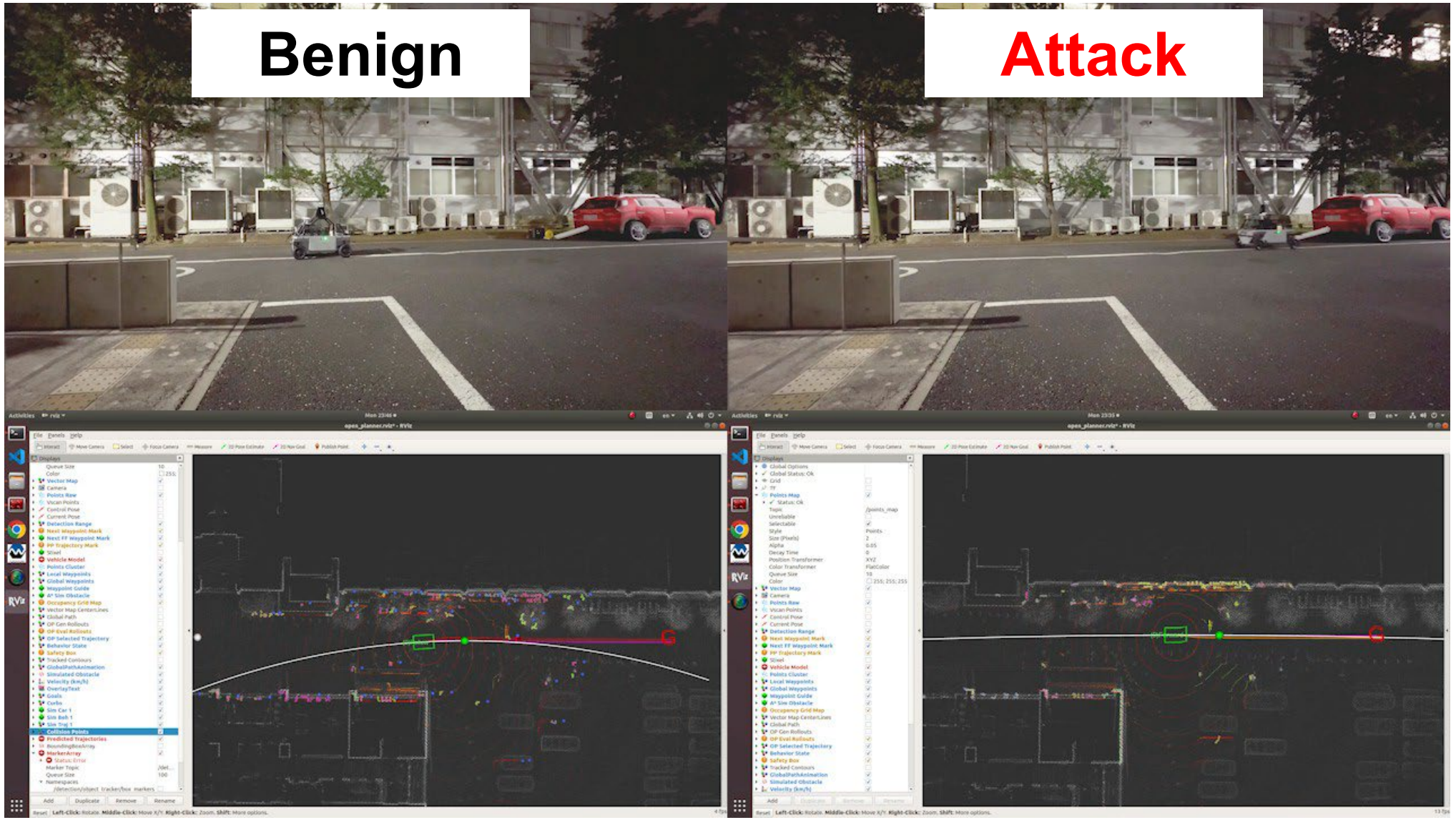
End-to-End Attack Results



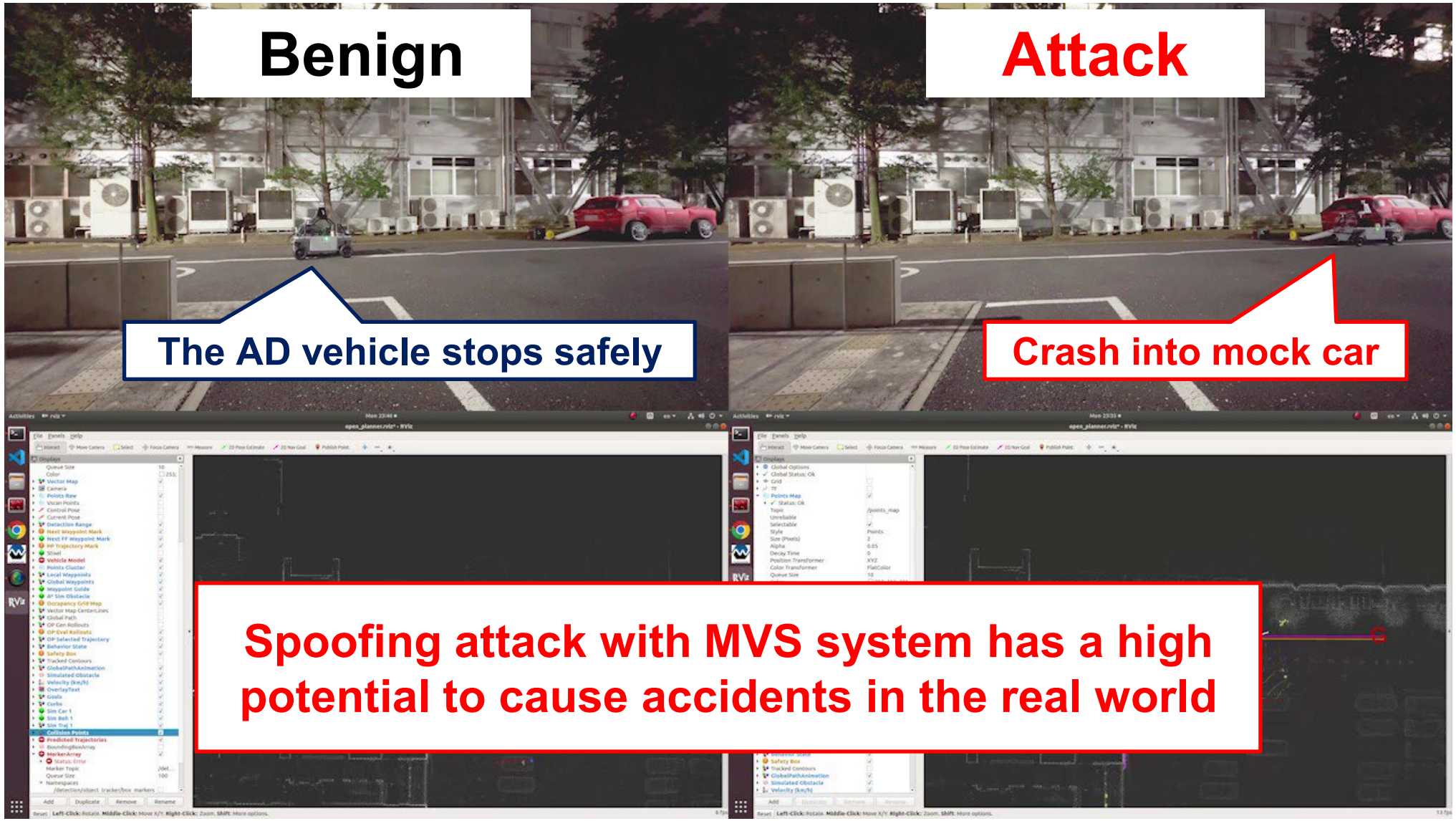
End-to-End Attack Results



End-to-End Attack Results



End-to-End Attack Results



Limitations & Countermeasures

- **Large Deployment Effort and Cost**
  - No major technical challenge to deploy our MVS system on public road
  - However, it costs $2.3k (device) + $10k (FG, Power Supply, etc.)
  - Need high engineering cost to build the system

- **Attack on uneven roads**
  - However, road should be even in high-speed scenarios
  - Adding vertical tracking is not technically hard

- **Possible countermeasures**
  - Availability-check
  - Multi-Sensor fusion

Conclusion

- **Investigate the safety and security impact of LiDAR spoofing attacks in the practical scenarios**
  - Identify 3 research limitations
- **Design a novel MVS system capable of practical speeds and distances**
  - Can detect, track, and aim at the target LiDAR moving at high speeds
  - Reveal that spoofing attack can be deployed against high-speed (60km/h) vehicles
  - Demonstrate closed-loop attack on a vehicle with a popular AD stack
- **Design a new practical removal attack: A-HFR**
  - A-HFR shows the effectiveness against New-Gen LiDARs with pulse fingerprinting
- **Performed Responsible Vulnerability Disclosure**
  - Informed 5 LiDAR suppliers and 8 AD Companies
  - One car manufacturer asked to extend the embargo term to investigate the impact

Thank you!

For demos, data & other details,
Please visit our project websites:

https://sites.google.com/keio.jp/keio-csg/projects/AttackonDrivingVehicle
https://sites.google.com/view/av-ioat-sec/real-av-lidar-attack

Contact : Yuki Hayakawa <hykwyuk@keio.jp>
Ryo Suzuki <suzuki.ryo@keio.jp>
Takami Sato <takamis@uci.edu>

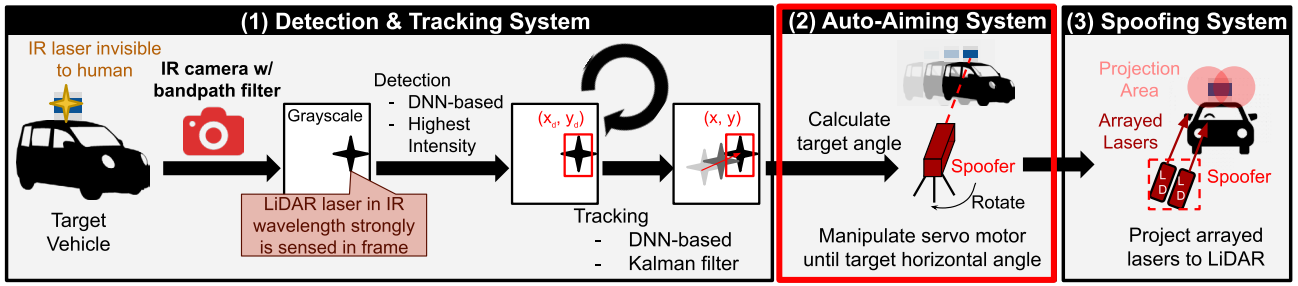
Keio University
1858
CALAMVS GLADIO FORTIOR

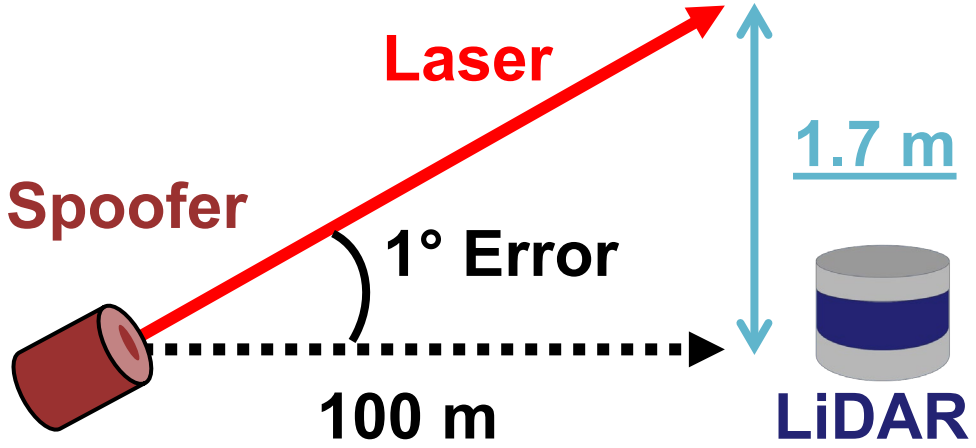
Yoshioka Lab

UC Irvine
AS²Guard
Autonomous & Smart Systems Guard Research Group

Appendix: Auto-Aiming System

- **Consisted of 3 subsystems**
  2. **Auto-Aiming System**





At long distances,
even small angular errors cause significant targeting deviations
→ **Servo motor precision is crucial**

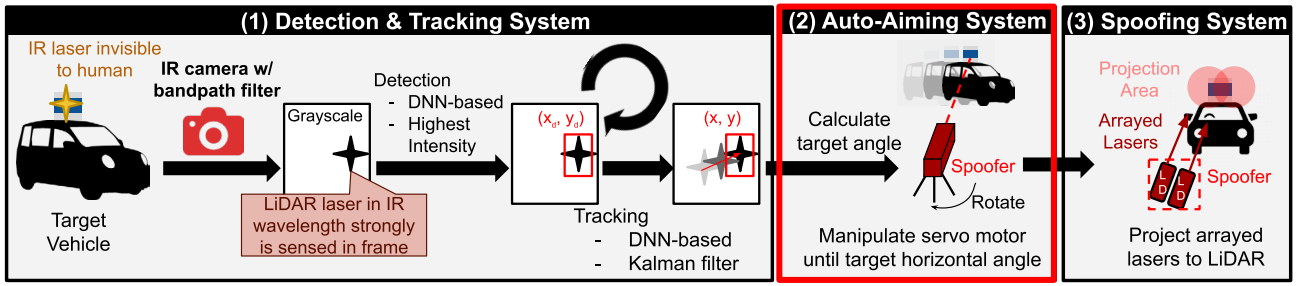
Appendix: Auto-Aiming System

- **Consisted of 3 subsystems**
  2. **Auto-Aiming System**

- **Built the system using a high-precision servo motor**

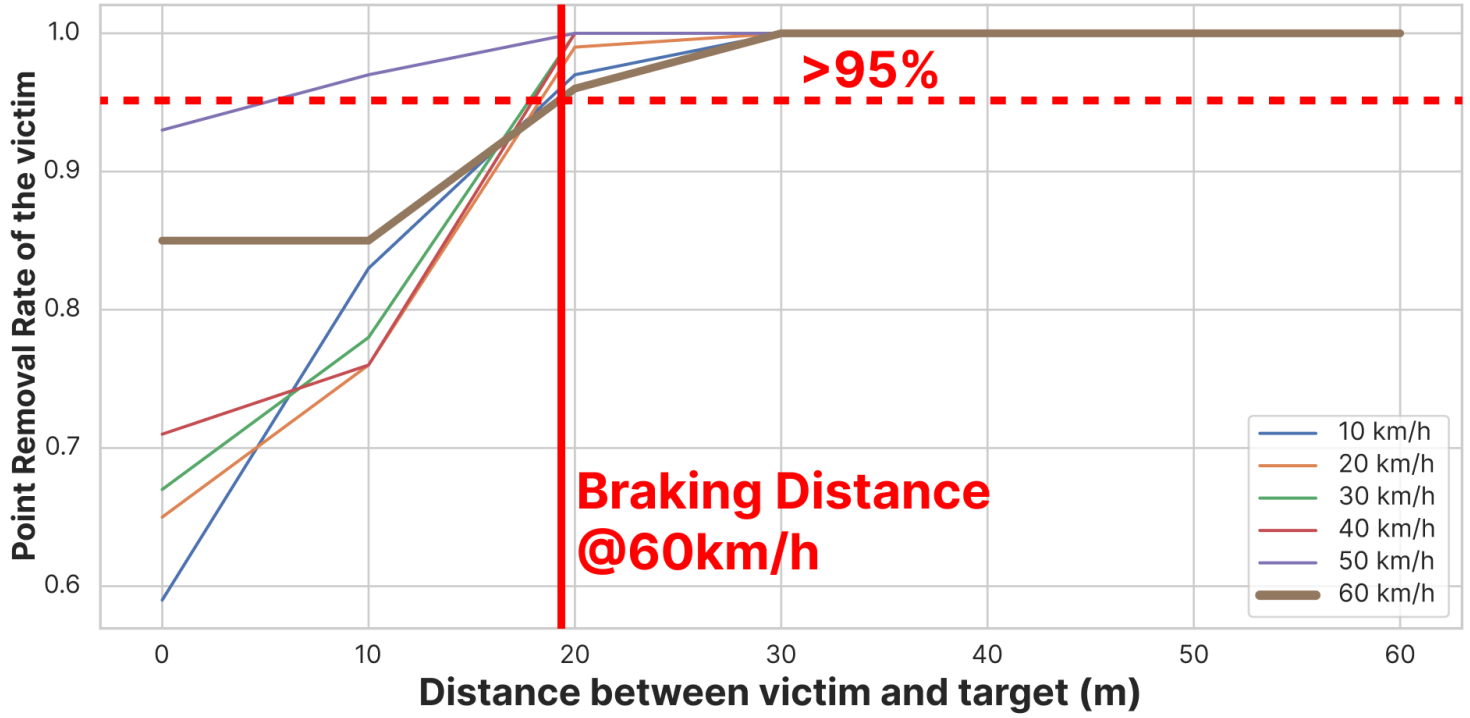
Servo Motor: DYNAMIXEL MX-28R

Resolution: 0.088°



Appendix: High-speed evaluation results

- **MVS system can hide the victim with almost 100% until 20m away**
  - **Braking distance at 60km/h is over 20m without the reaction distance**



MVS system has a significant impact on the safety implications that occur collision accidents