WIP: Practical Removal Attacks on LiDAR-based Object Detection in Autonomous Driving

Takami Sato*, Yuki Hayakawa*, Ryo Suzuki*, Yohsuke Shiiki*, Kentaro Yoshioka, and Qi Alfred Chen

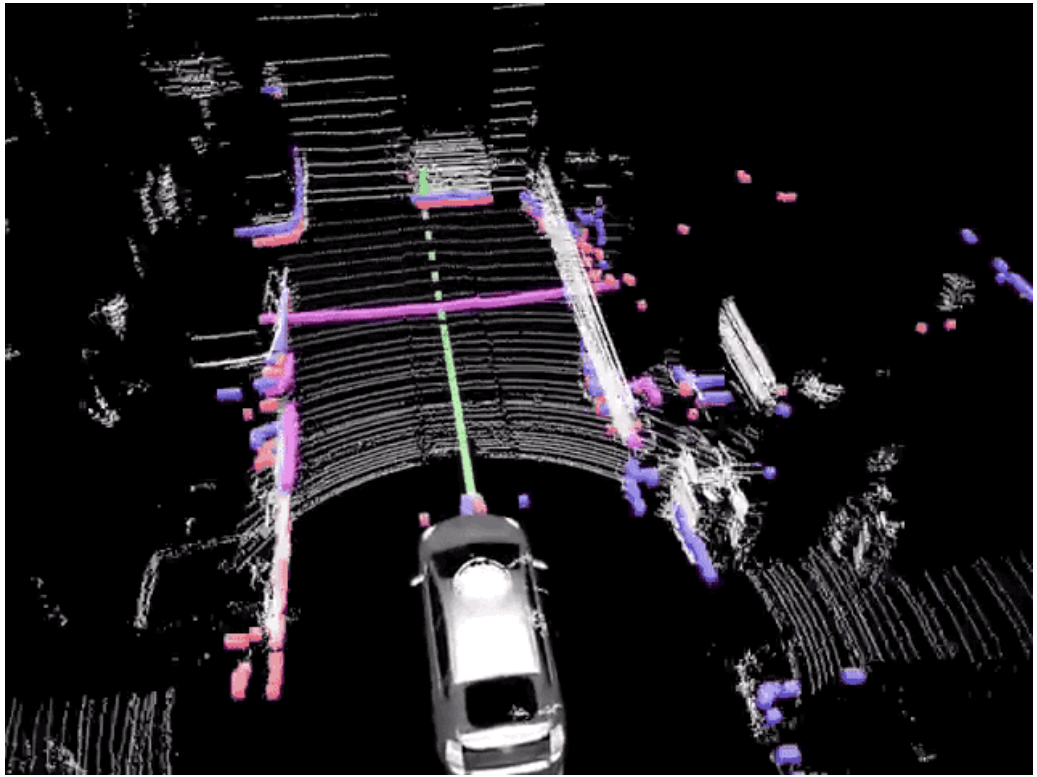
AS²Guard Autonomous & Smart Systems Guard Research Group

UCI

Keio University 1858 CALAMVS GLADIO FORTIOR

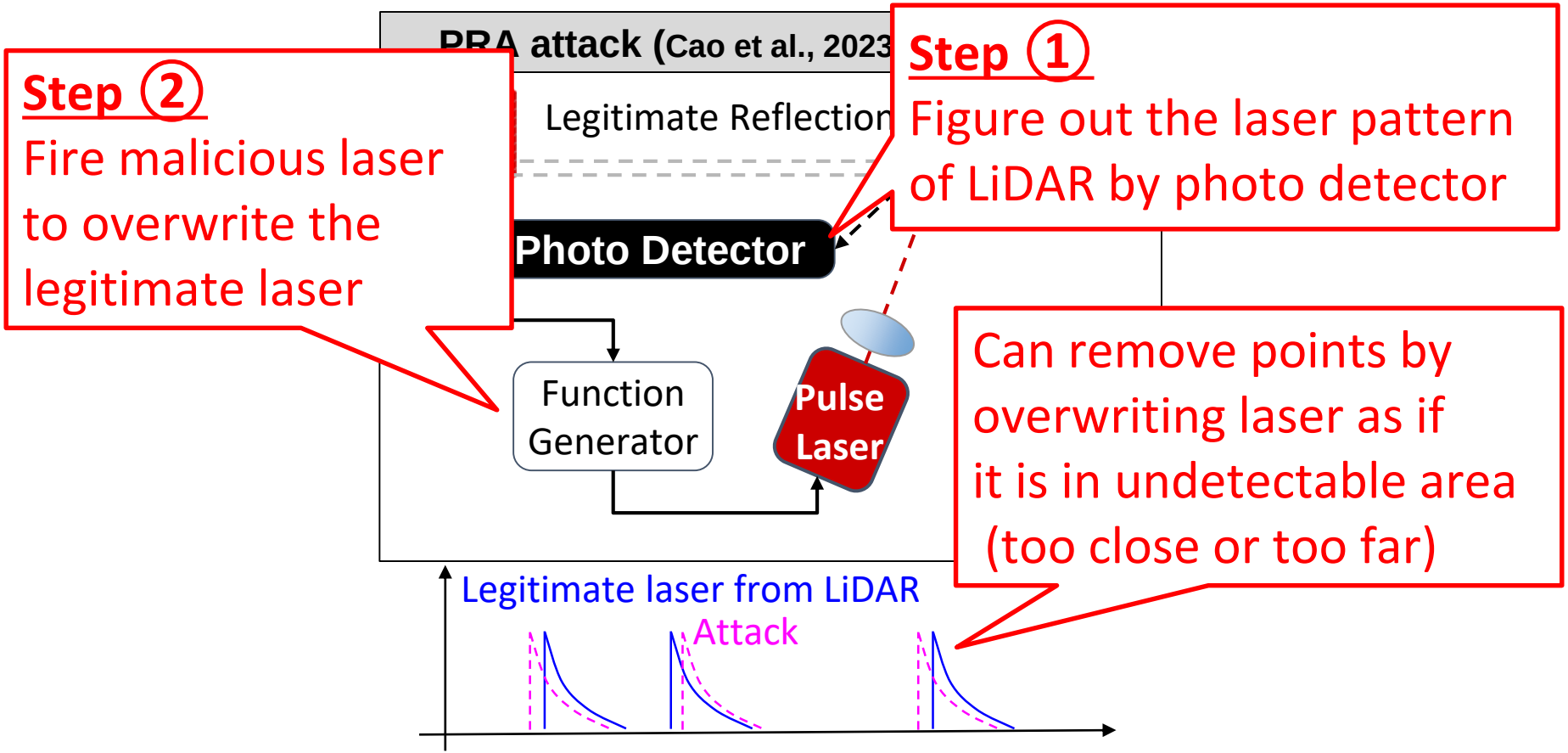
*co-first authors

LiDAR plays an essential role in Autonomous Driving (AD)



Current Level-4 AD heavily relies on LiDAR sensing for object detection

Existing Removal Attack: PRA attack



Step ①
Figure out the laser pattern of LiDAR by photo detector

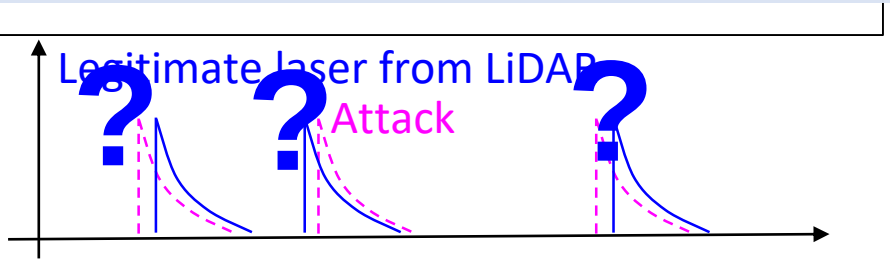
Step ②
Fire malicious laser to overwrite the legitimate laser

Can remove points by overwriting laser as if it is in undetectable area (too close or too far)

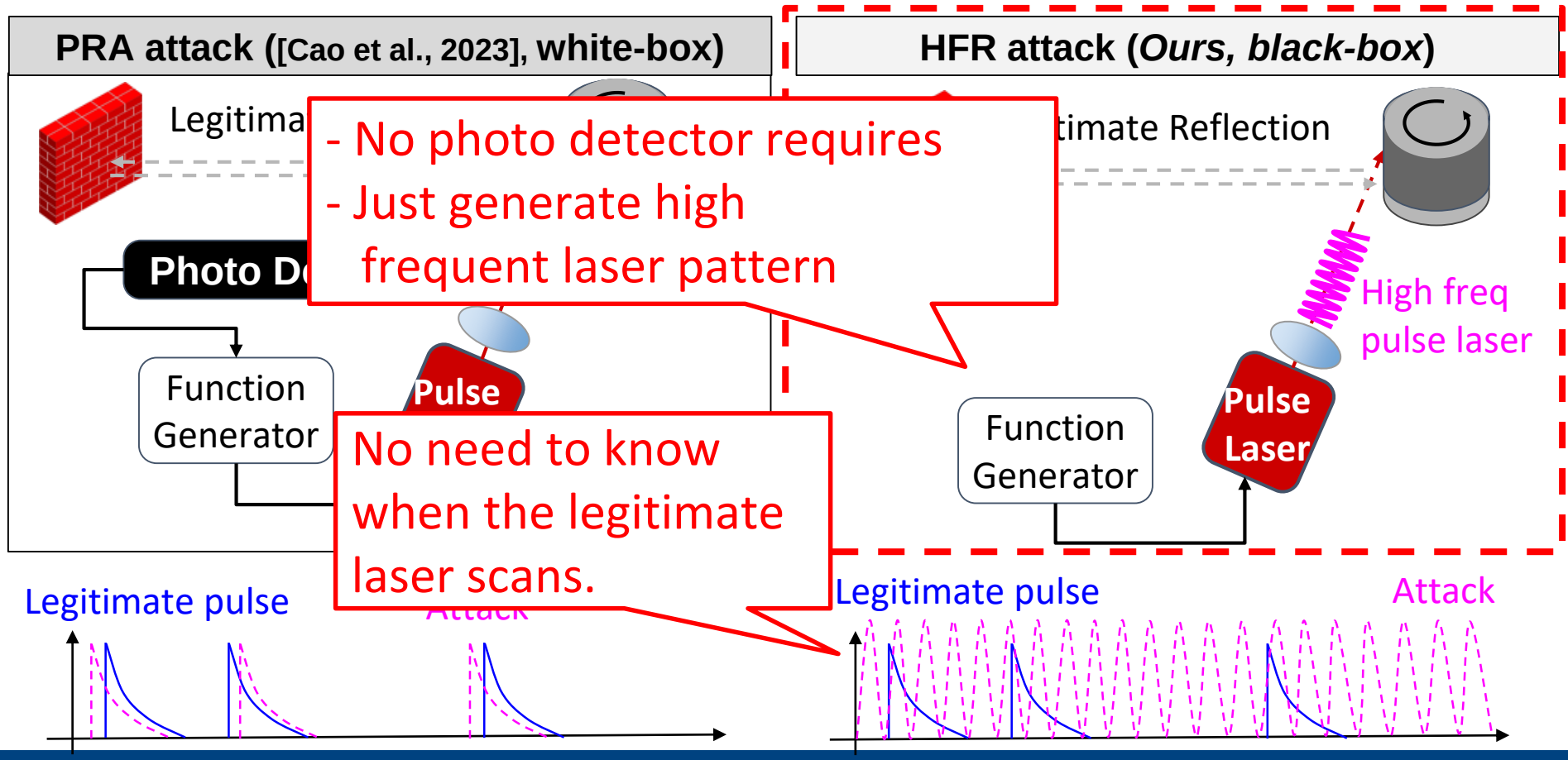
Existing Removal Attack: PRA attack

Limitation of PRA Attack

- Need white-box knowledge on **LiDAR scan Pattern**
- Defensible **by randomizing the scan pattern**
  - **5 out of 6 new generation of LiDARs** we were able to access have the **laser timing randomization**
  - State-of-the-art prior attacks can **only work for 1st-generation LiDARs**, not the new generation ones

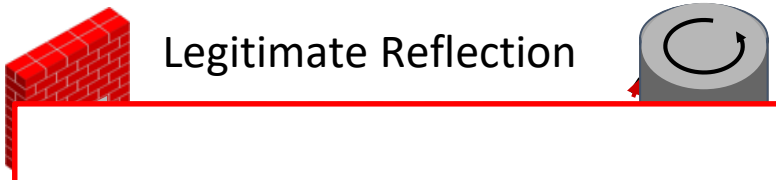


Our Attack: High-Frequency Removal (HFR) Attack

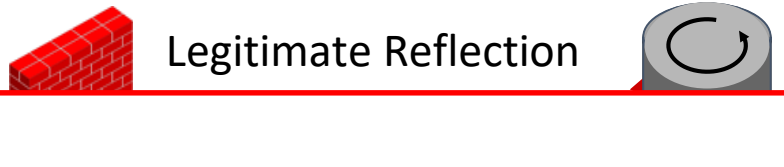


Our Attack: High-Frequency Removal (HFR) Attack

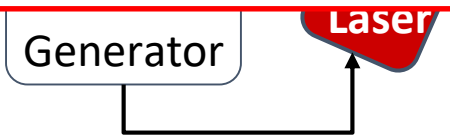
PRA attack ([Cao et al., 2023], white-box)

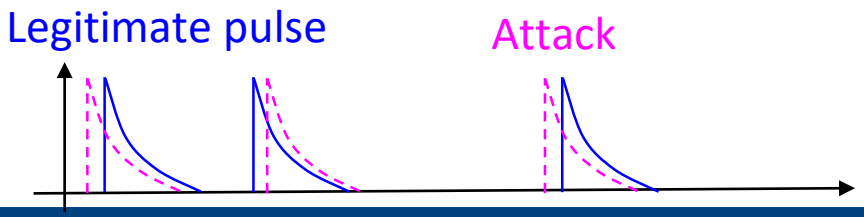


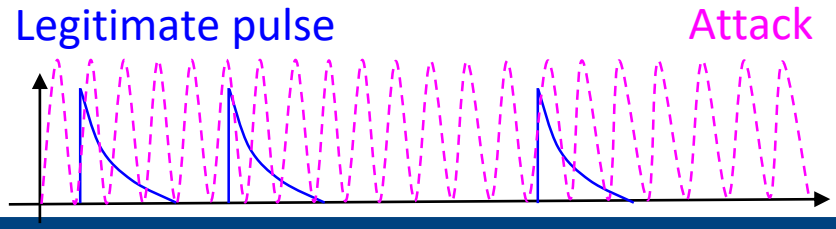
HFR attack (*Ours, black-box*)



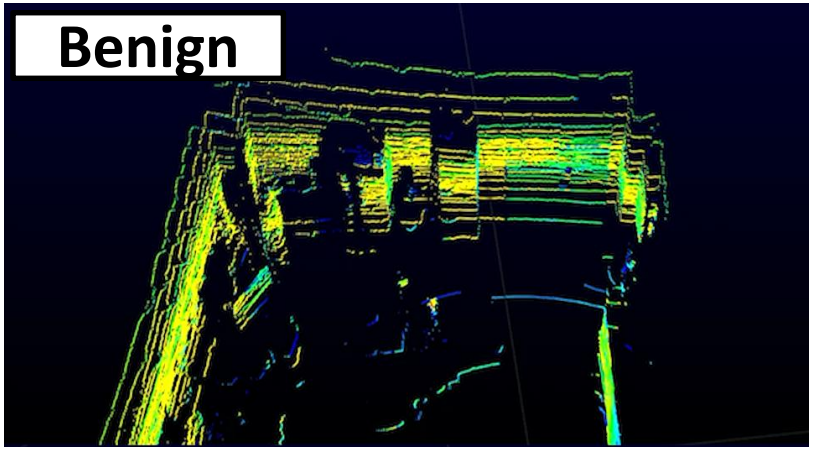
Our HFR attack is the first removal attack that can work for both old and new generations of LiDARs today

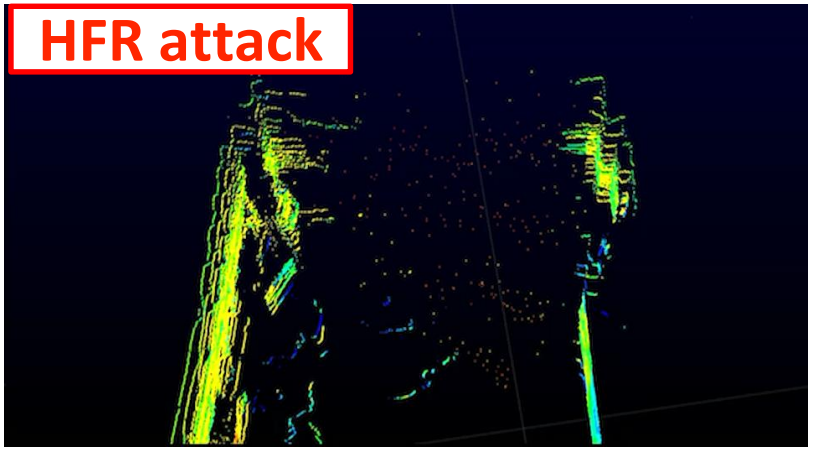




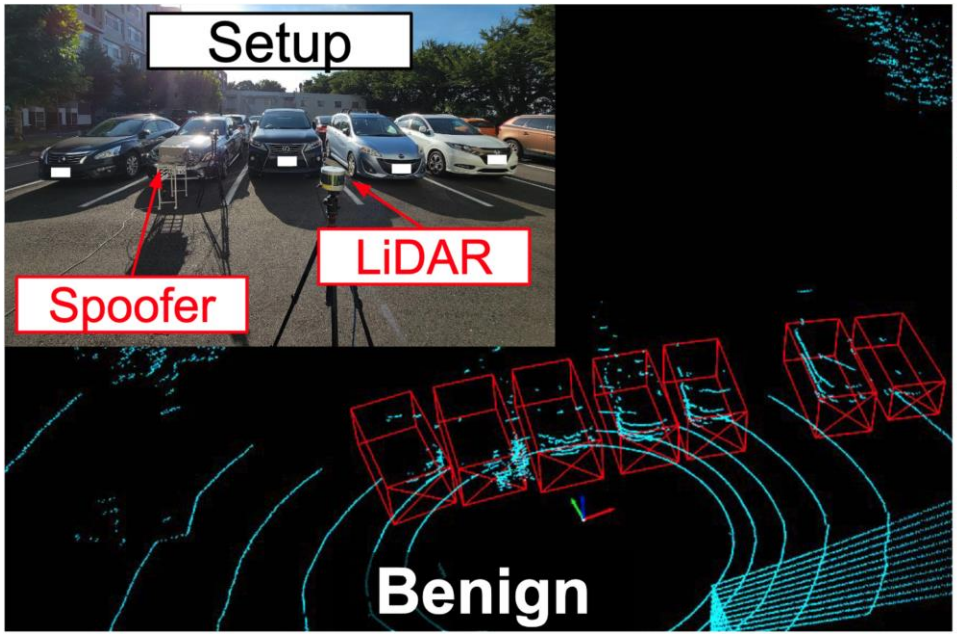


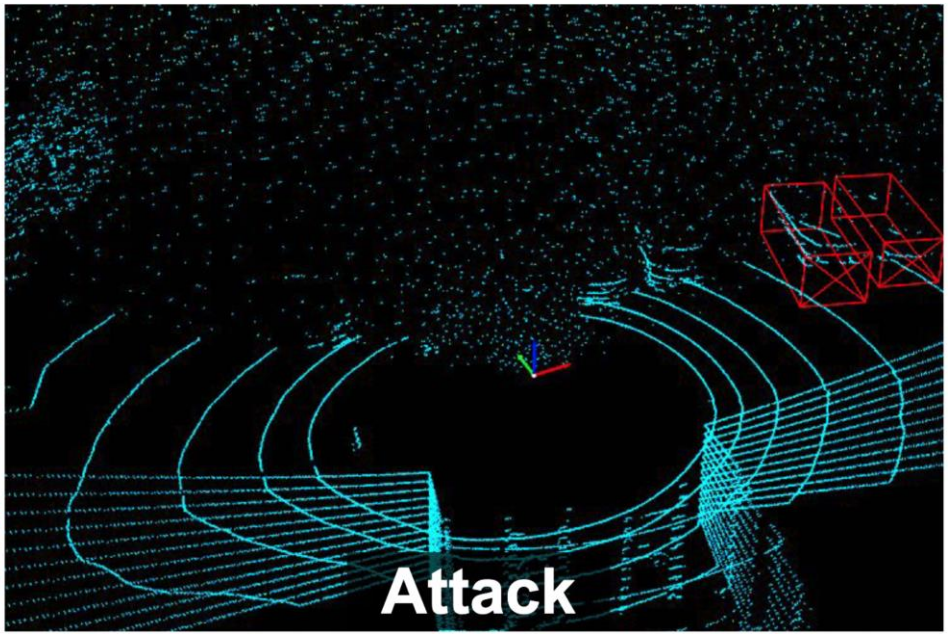
HFR Attack Indoor Demo





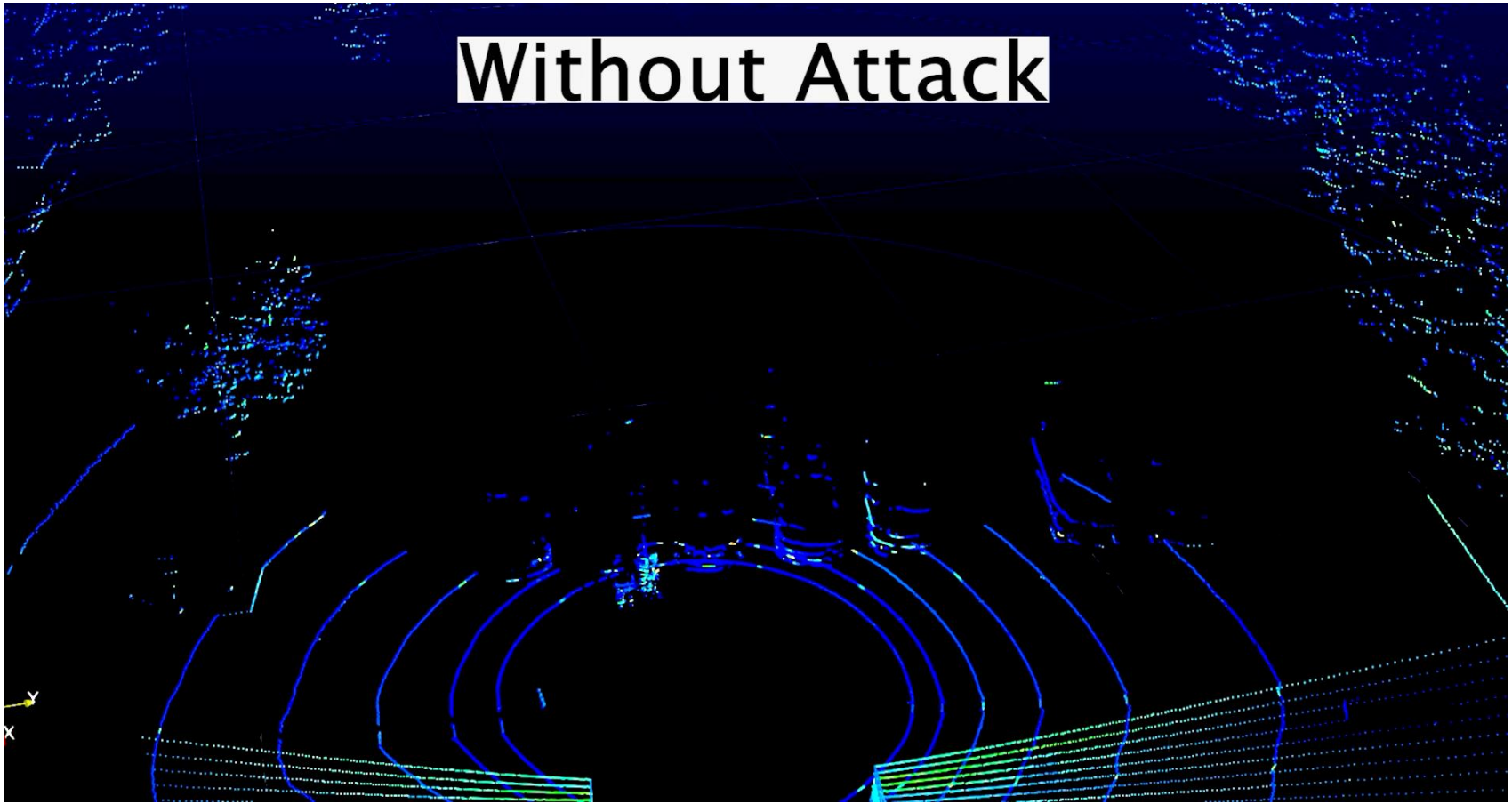
HFR Attack Outdoor Demo





5 cars are not detected by Apollo 6.0's PointPillars object detector

HFR Attack Indoor Demo



Take Away & Future Plan

- Design HFR attack, which is the first black-box removal attack that can be effective against next-gen LiDARs with timing randomization
- HFR can remove **~75% of points** in the attack area on a next-gen LiDAR

Future Plan

- **Large-scale Measurement Study on Multiple Next-Gen. LiDARs**
  - How are next-gen. LiDARs robust against LiDAR spoofing attacks?
- **Evaluation against Moving Vehicle**
  - Can be effective against end-to-end autonomous driving scenarios?
- **Defense Evaluation**
  - Can design effective defense for HFR attack?

Thank you!

For more details, please check out our paper

AS²Guard

Autonomous & Smart Systems Guard Research Group

UCI

Keio University

1858

CALAMVS GLADIO FORTIOR