NDSS SYMPOSIUM

LiDAR Spoofing Meets the New-Gen: Capability Improvements, Broken Assumptions, and New Attack Strategies

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

AS²Guard Autonomous & Smart Systems Guard Research Group

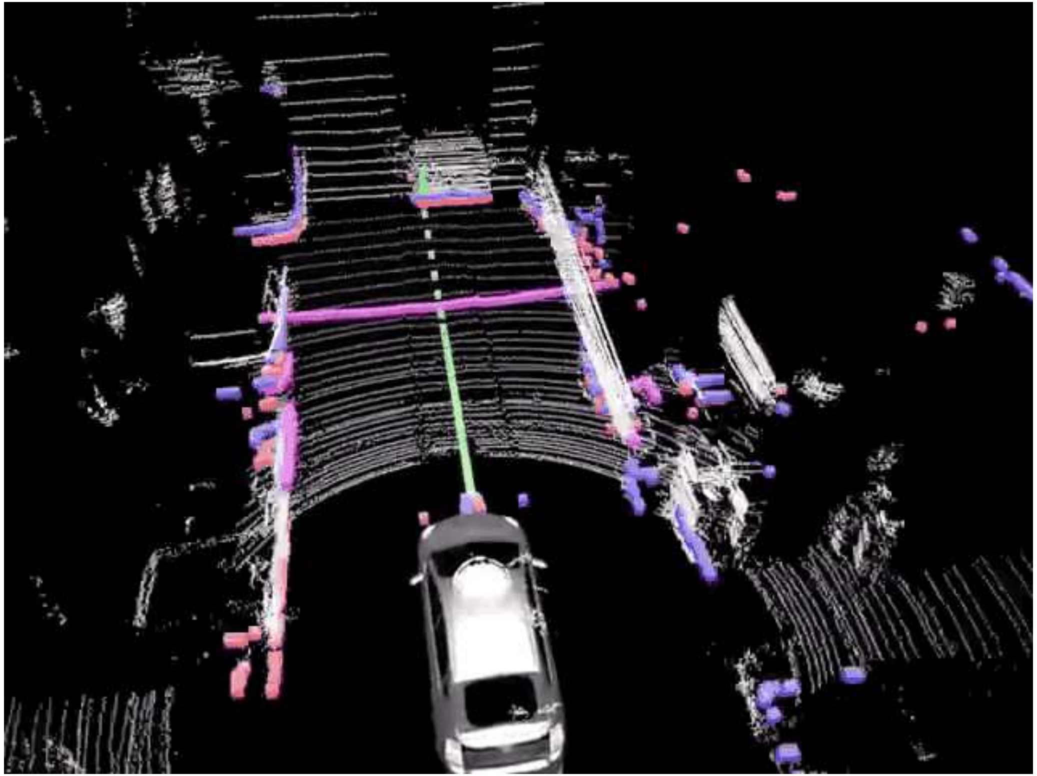
UCI

Yoshioka Lab

Keio University

*co-first authors

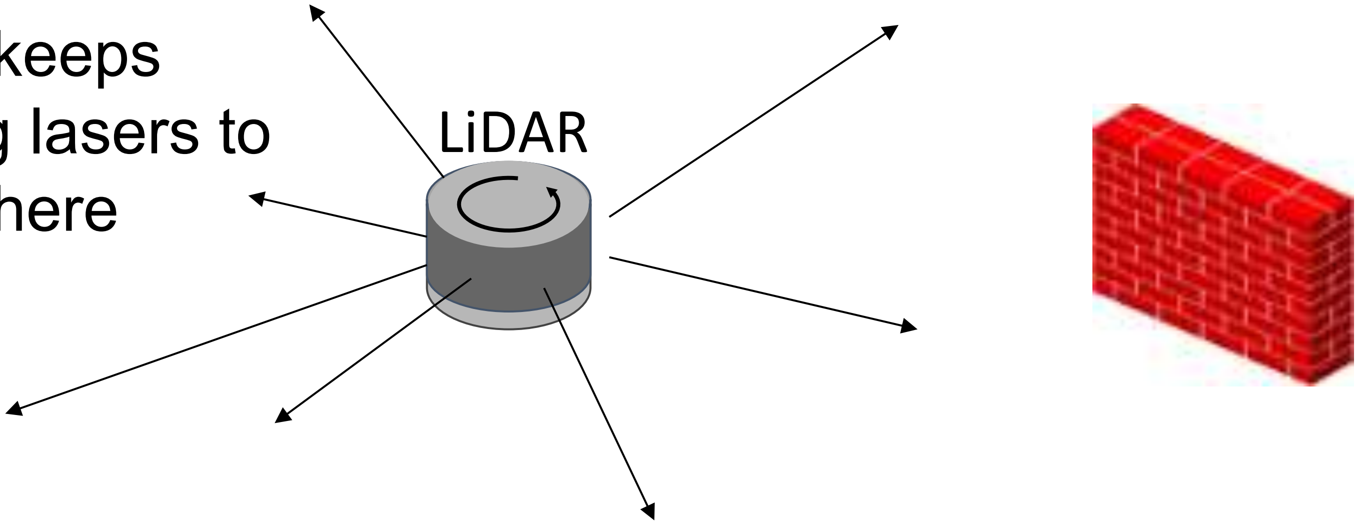
LiDAR plays an essential role in Autonomous Driving (AD)



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

LiDAR spoofing attack

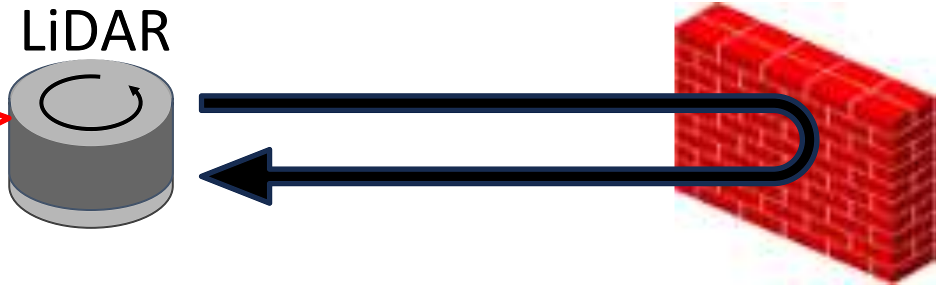
LiDAR keeps emitting lasers to everywhere



LiDAR spoofing attack

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

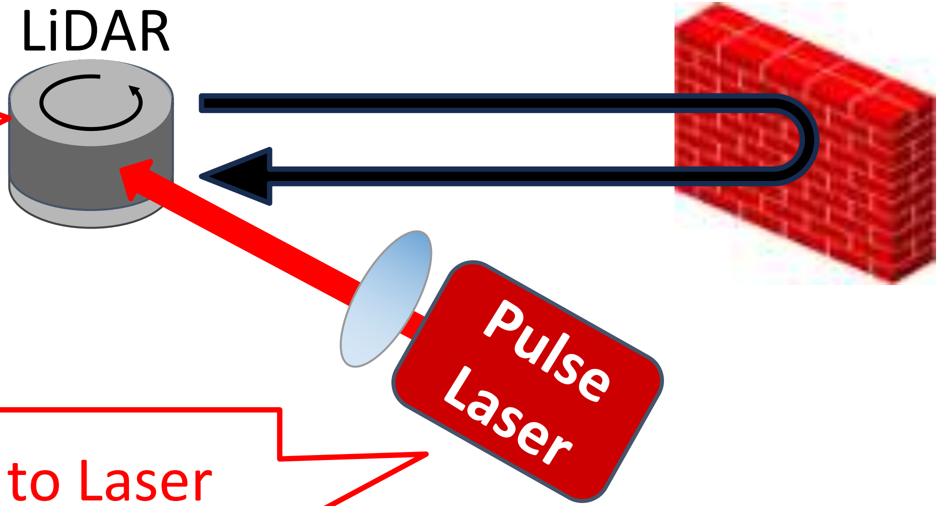
LiDAR senses distance to object based on ToF (time-of-flight)



LiDAR spoofing attack

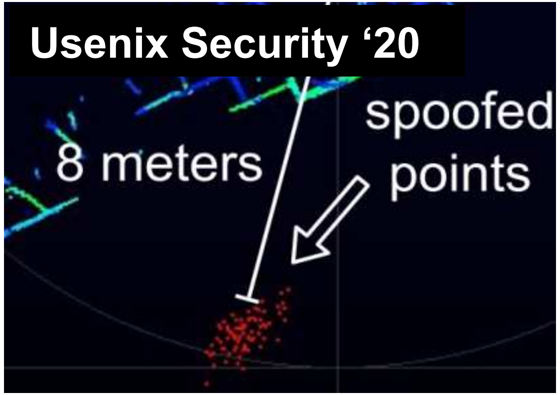
$$distance = Light\ Speed \times Flight\ Time \div 2$$

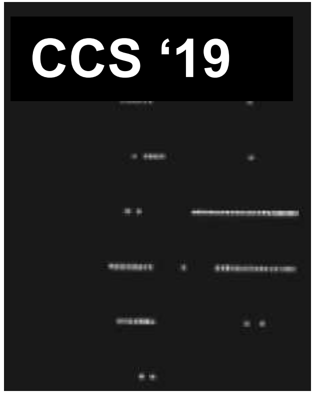
LiDAR senses distance to object based on ToF (time-of-flight)

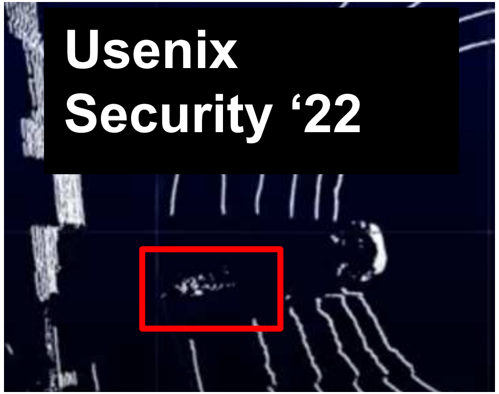


Generally vulnerable to Laser from other source by design, **LiDAR Spoofing Attack**

Limitations in prior works



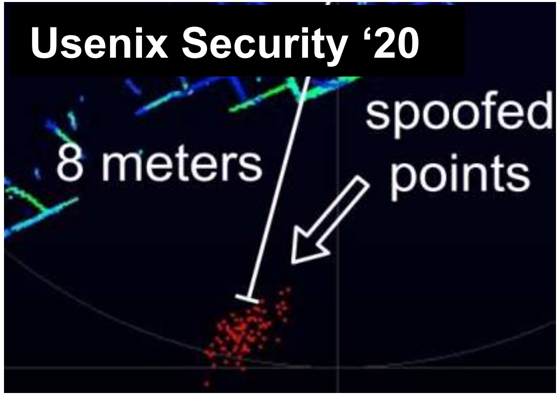


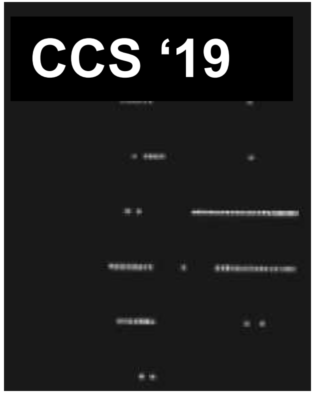


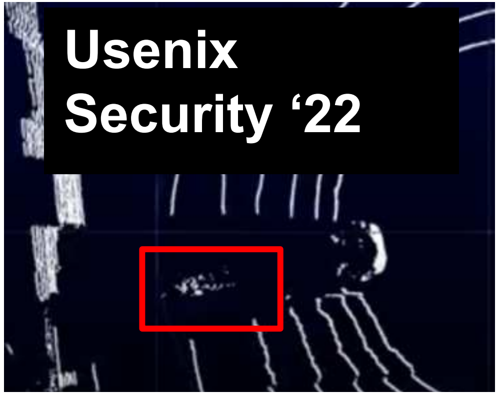
No prior attack shows precise injection pattern control: Chosen Pattern Injection (CPI)

- Despite CPI is **essential assumption for their adversarial attack** against ML models
- Only evaluated on a specific LiDAR (VLP-16) **w/o recent security-related features**
    - e.g., timing randomization and pulse fingerprinting

Limitations in prior works







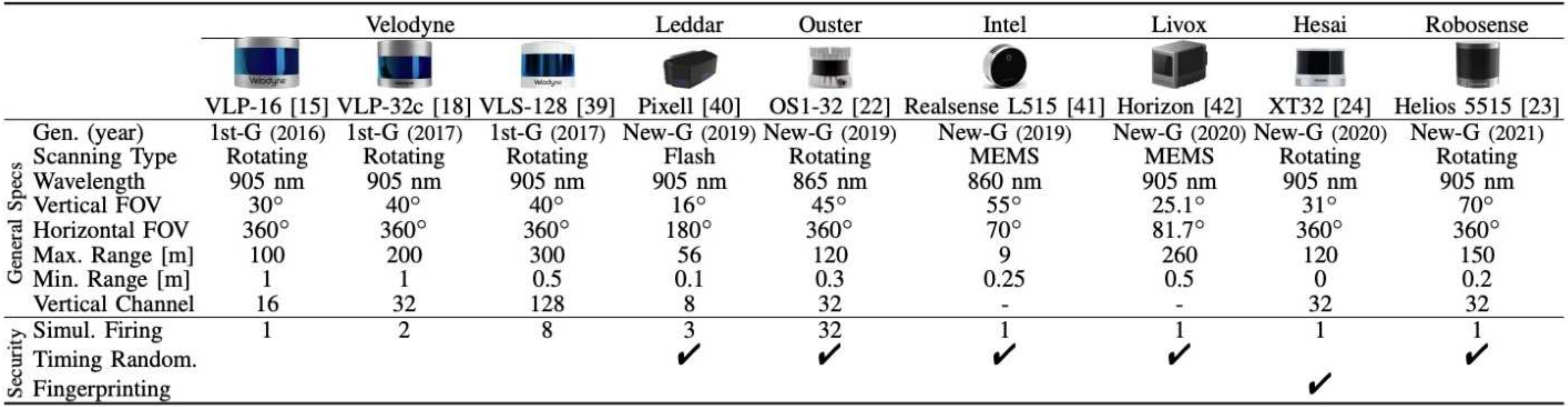
No prior attack shows precise injection pattern control: Chosen Pattern Injection (CPI)

- Despite CPI is **essential assumption for their adversarial attack** against ML models

- Only evaluated on a specific LiDAR (VLP-16) **w/o recent security-related features**
  - e.g., timing randomization and pulse fingerprinting

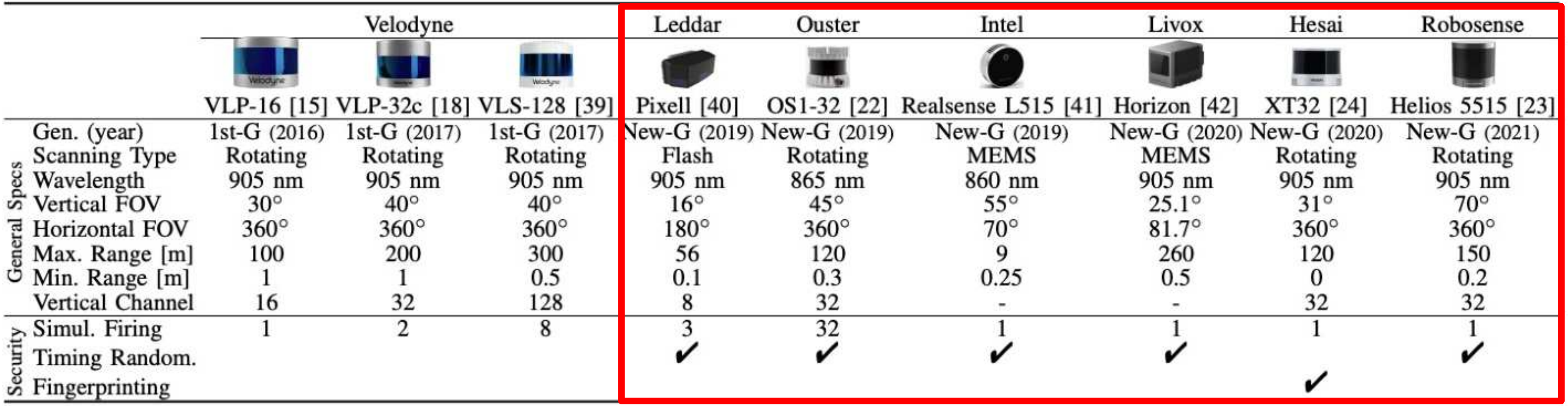
- Concurrent work [Jin et al., IEEE S&P'23] has demonstrated CPI attack capability, but, only on 2 LiDARs (VLP-16 and RS-16) w/o systematic study on security-related features
  - Meanwhile, our attack is >1.5x stronger with >7k (vs ~4.2k) point injection

Our work: First large-scale study on New-Gen LiDARs



		Velodyne			Leddar	Ouster	Intel	Livox	Hesai	Robosense
		VLP-16 [15]	VLP-32c [18]	VLS-128 [39]	Pixell [40]	OS1-32 [22]	Realsense L515 [41]	Horizon [42]	XT32 [24]	Helios 5515 [23]
General Specs	Gen. (year)	1st-G (2016)	1st-G (2017)	1st-G (2017)	New-G (2019)	New-G (2019)	New-G (2019)	New-G (2020)	New-G (2020)	New-G (2021)
	Scanning Type	Rotating	Rotating	Rotating	Flash	Rotating	MEMS	MEMS	Rotating	Rotating
	Wavelength	905 nm	905 nm	905 nm	905 nm	865 nm	860 nm	905 nm	905 nm	905 nm
	Vertical FOV	30°	40°	40°	16°	45°	55°	25.1°	31°	70°
	Horizontal FOV	360°	360°	360°	180°	360°	70°	81.7°	360°	360°
	Max. Range [m]	100	200	300	56	120	9	260	120	150
	Min. Range [m]	1	1	0.5	0.1	0.3	0.25	0.5	0	0.2
	Vertical Channel	16	32	128	8	32	-	-	32	32
Security	Simul. Firing	1	2	8	3	32	1	1	1	1
	Timing Random.				✓	✓	✓	✓		✓
	Fingerprinting								✓	

Our work: First large-scale study on New-Gen LiDARs

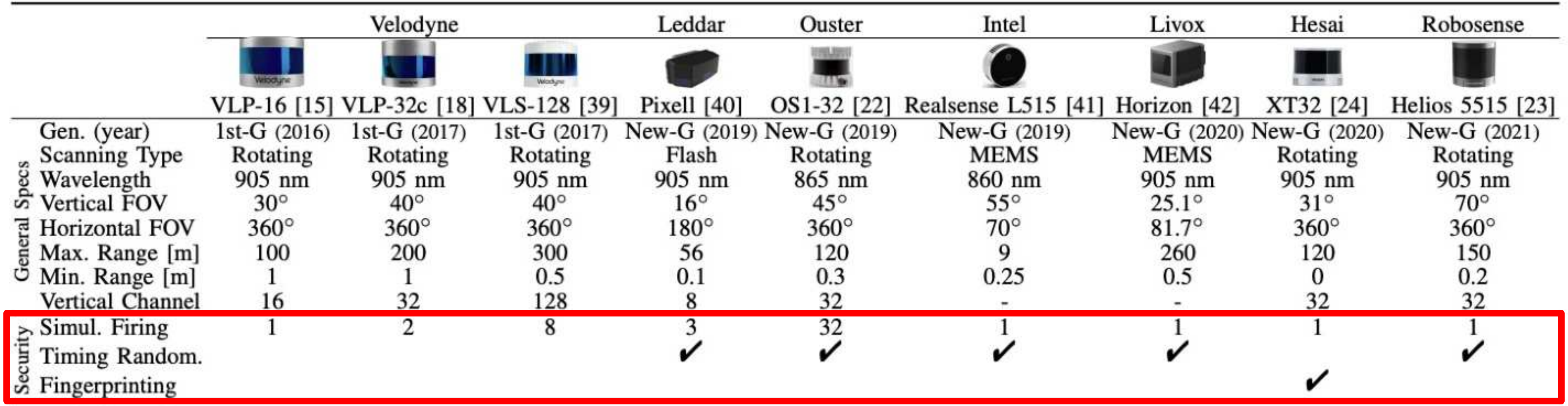


		Velodyne			Leddar	Ouster	Intel	Livox	Hesai	Robosense
		VLP-16 [15]	VLP-32c [18]	VLS-128 [39]	Pixell [40]	OS1-32 [22]	Realsense L515 [41]	Horizon [42]	XT32 [24]	Helios 5515 [23]
General Specs	Gen. (year)	1st-G (2016)	1st-G (2017)	1st-G (2017)	New-G (2019)	New-G (2019)	New-G (2019)	New-G (2020)	New-G (2020)	New-G (2021)
	Scanning Type	Rotating	Rotating	Rotating	Flash	Rotating	MEMS	MEMS	Rotating	Rotating
	Wavelength	905 nm	905 nm	905 nm	905 nm	865 nm	860 nm	905 nm	905 nm	905 nm
	Vertical FOV	30°	40°	40°	16°	45°	55°	25.1°	31°	70°
	Horizontal FOV	360°	360°	360°	180°	360°	70°	81.7°	360°	360°
	Max. Range [m]	100	200	300	56	120	9	260	120	150
	Min. Range [m]	1	1	0.5	0.1	0.3	0.25	0.5	0	0.2
	Vertical Channel	16	32	128	8	32	-	-	32	32
Security	Simul. Firing	1	2	8	3	32	1	1	1	1
	Timing Random.				✓	✓	✓	✓		✓
	Fingerprinting								✓	

- Cover 9 LiDARs including both 1st and **New-Gen LiDARs**

System-on-Chip (SoC) approach allows New-Gen LiDARs more complex signal processing.
e.g., timing randomization & pulse fingerprinting

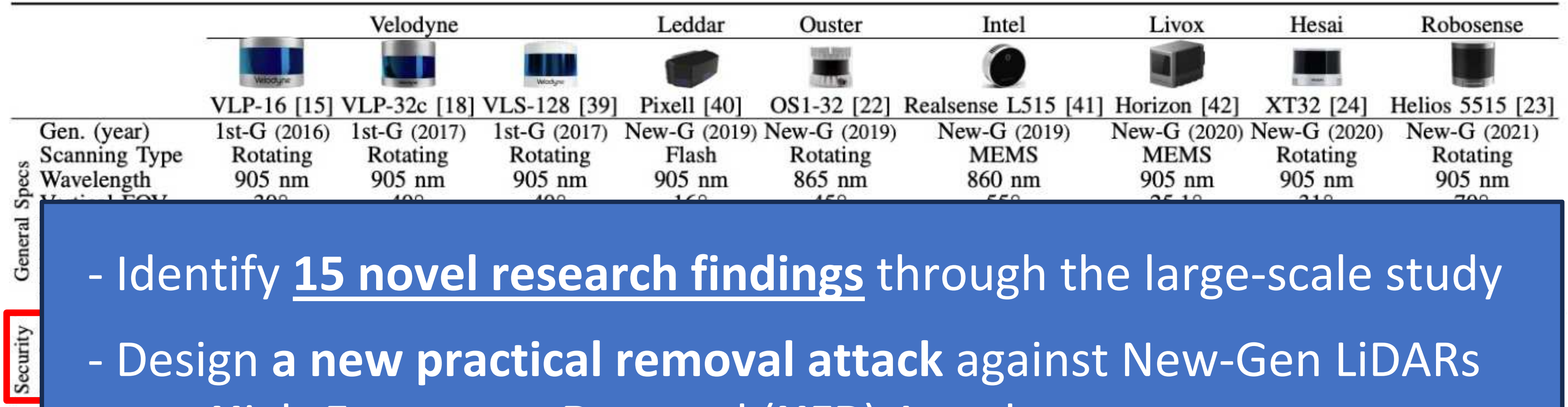
Our work: First large-scale study on New-Gen LiDARs



		Velodyne			Leddar	Ouster	Intel	Livox	Hesai	Robosense
		VLP-16 [15]	VLP-32c [18]	VLS-128 [39]	Pixell [40]	OS1-32 [22]	Realsense L515 [41]	Horizon [42]	XT32 [24]	Helios 5515 [23]
General Specs	Gen. (year)	1st-G (2016)	1st-G (2017)	1st-G (2017)	New-G (2019)	New-G (2019)	New-G (2019)	New-G (2020)	New-G (2020)	New-G (2021)
	Scanning Type	Rotating	Rotating	Rotating	Flash	Rotating	MEMS	MEMS	Rotating	Rotating
	Wavelength	905 nm	905 nm	905 nm	905 nm	865 nm	860 nm	905 nm	905 nm	905 nm
	Vertical FOV	30°	40°	40°	16°	45°	55°	25.1°	31°	70°
	Horizontal FOV	360°	360°	360°	180°	360°	70°	81.7°	360°	360°
	Max. Range [m]	100	200	300	56	120	9	260	120	150
	Min. Range [m]	1	1	0.5	0.1	0.3	0.25	0.5	0	0.2
	Vertical Channel	16	32	128	8	32	-	-	32	32
Security	Simul. Firing	1	2	8	3	32	1	1	1	1
	Timing Random.				✓	✓	✓	✓		✓
	Fingerprinting								✓	

- Cover 9 LiDARs including both 1st and **New-Gen LiDARs**
- Evaluate **3 security-related features** in mainly New-Gen LiDARs
  - **Simultaneous Laser Firing**
  - **Laser Timing Randomization**
  - **Pulse Fingerprinting**

Our work: First large-scale study on New-Gen LiDARs



		Velodyne			Leddar	Ouster	Intel	Livox	Hesai	Robosense
		VLP-16 [15]	VLP-32c [18]	VLS-128 [39]	Pixell [40]	OS1-32 [22]	Realsense L515 [41]	Horizon [42]	XT32 [24]	Helios 5515 [23]
General Specs	Gen. (year)	1st-G (2016)	1st-G (2017)	1st-G (2017)	New-G (2019)	New-G (2019)	New-G (2019)	New-G (2020)	New-G (2020)	New-G (2021)
	Scanning Type	Rotating	Rotating	Rotating	Flash	Rotating	MEMS	MEMS	Rotating	Rotating
	Wavelength	905 nm	905 nm	905 nm	905 nm	865 nm	860 nm	905 nm	905 nm	905 nm
Security										

- Identify **15 novel research findings** through the large-scale study

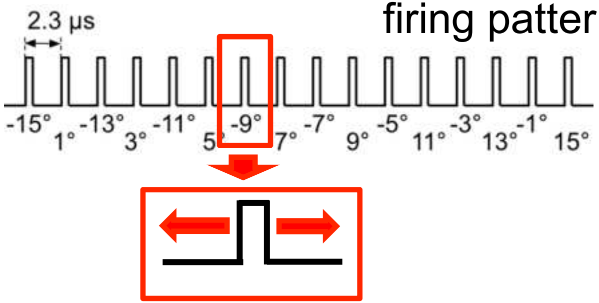
- Design **a new practical removal attack** against New-Gen LiDARs
  - High-Frequency Removal (**HFR**) Attack

- Evaluate **3 security-related features** in mainly New-Gen LiDARs
  - **Simultaneous Laser Firing**
  - **Laser Timing Randomization**
  - **Pulse Fingerprinting**

Main security-related features in New-Gen LiDARs

Laser Timing Randomization

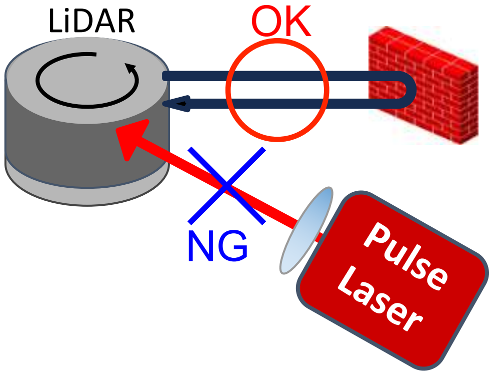
Randomly perturb laser firing timing



VLP-16's periodic firing pattern

Pulse Fingerprinting

Authenticate their own laser

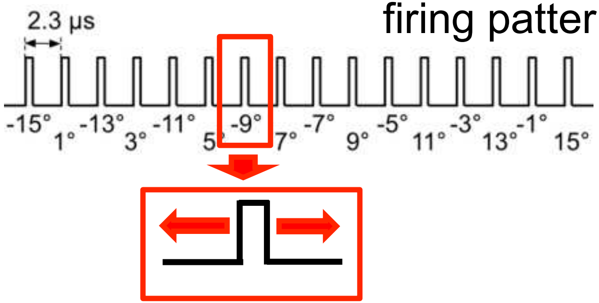


Main security-related features in New-Gen LiDARs

Laser Timing Randomization

Randomly perturb laser firing timing

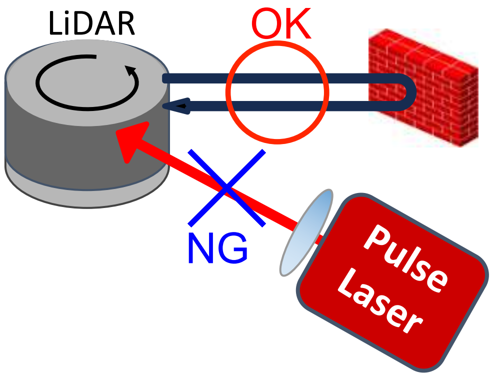
VLP-16's periodic firing pattern



Makes attack impossible to inject points at designed location

Pulse Fingerprinting

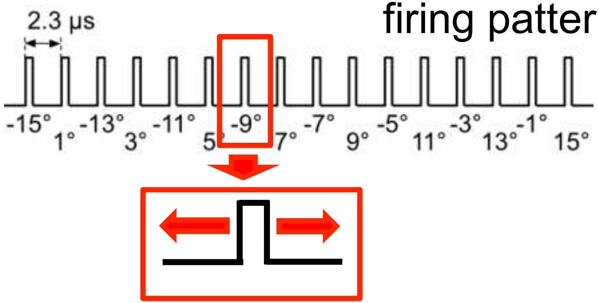
Authenticate their own laser



Main security-related features in New-Gen LiDARs

Laser Timing Randomization

Randomly perturb laser firing timing

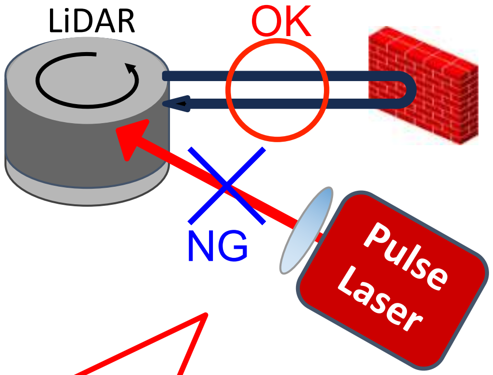


VLP-16's periodic firing pattern

Makes attack impossible to inject points at designed location

Pulse Fingerprinting

Authenticate their own laser

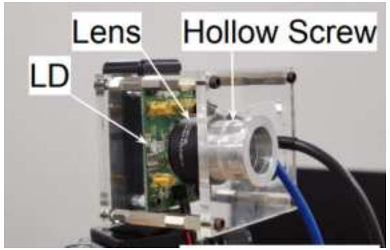


Sounds ultimate defense
But, we found that current one is not strong enough

Overview of our research findings

Attack Device Improvements

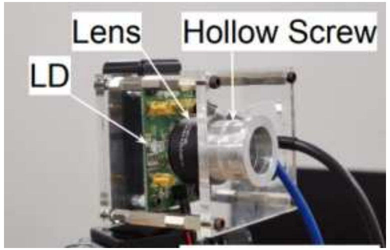
- Our new attack device can achieve inject **>6k** points in **>80°**
- **CPI attack is feasible** on VLP-16 with our device
- Model-level vulnerability may not be necessary to attack object detector



Overview of our research findings

Attack Device Improvements

- Our new attack device can achieve inject **>6k** points in **>80°**
- **CPI attack is feasible** on VLP-16 with our device
- Model-level vulnerability may not be necessary to attack object detector



New-Gen LiDAR Measurements & Attack Modeling

Overview of our research findings

Attack Device Improvements

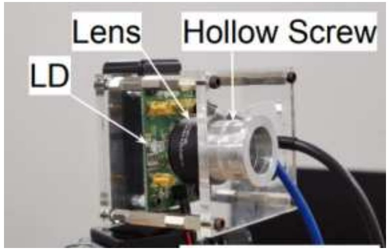
New-Gen LiDAR Measurements & Attack Modeling

New Attack Modeling

Security Analysis w/ 9 object detectors & AD Simulator

(Autonomous Driving)

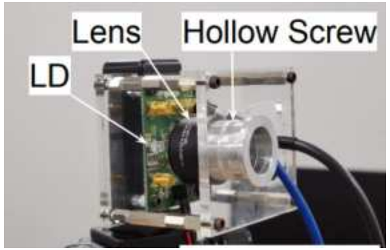
- Our new attack device can achieve inject **>6k** points in **>80°**
- **CPI attack is feasible** on VLP-16 with our device
- Model-level vulnerability may not be necessary to attack object detector



Overview of our research findings

Attack Device Improvements

- Our new attack device can achieve inject **>6k** points in **>80°**
- **CPI attack is feasible** on VLP-16 with our device
- Model-level vulnerability may not be necessary to attack object detector



New-Gen LiDAR Measurements & Attack Modeling

New Attack Modeling

Security Analysis w/ 9 object detectors & AD Simulator
(Autonomous Driving)

Injection Attack

- CPI attack is **feasible only on VLP-16**
- **Pulse fingerprinting is not strong enough** to perfectly prevent injection
- **Error modeling** has major impact

- **Pulse fingerprinting is effective mitigation** against injection attacks
- **Timing randomization is effective mitigation** against injection

Removal Attack

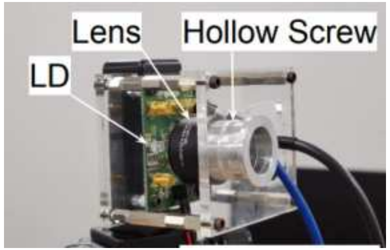
- **Latest removal attack is not feasible** on New-Gen LiDARs
- **Our HFR attack can be effective** even against New-Gen LiDARs

- **Pulse fingerprinting is effective mitigation** against removal attacks
- Vulnerability of object detector heavily **depends on their training data**
- **HFR attack can be effective against autonomous driving scenarios**

Overview of our research findings

Attack Device Improvements

- Our new attack device can achieve inject **>6k** points in **>80°**
- **CPI attack is feasible** on VLP-16 with our device
- Model-level vulnerability may not be necessary to attack object detector



New-Gen LiDAR Measurements & Attack Modeling

New Attack Modeling

Security Analysis w/ 9 object detectors & AD Simulator

(Autonomous Driving)

Injection Attack

- CPI attack is **feasible only on VLP-16**
- **Pulse fingerprinting is not strong enough** to perfectly prevent injection
- **Error modeling** has major impact

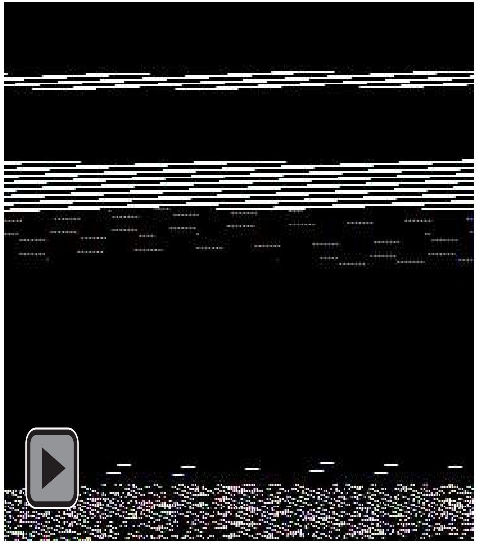
- **Pulse fingerprinting is effective mitigation** against injection attacks
- **Timing randomization is effective mitigation** against injection

Removal Attack

- **Latest removal attack is not feasible** on New-Gen LiDARs
- **Our HFR attack can be effective** even against New-Gen LiDARs

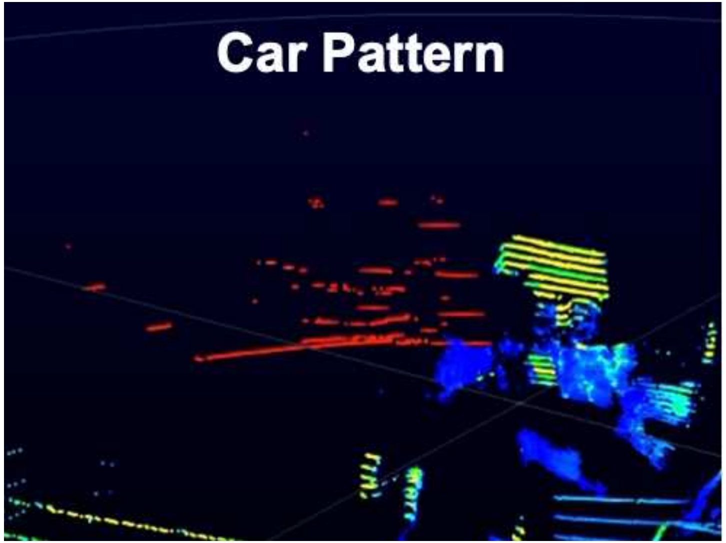
- **Pulse fingerprinting is effective mitigation** against removal attacks
- Vulnerability of object detector heavily **depends on their training data**
- **HFR attack can be effective against autonomous driving scenarios**

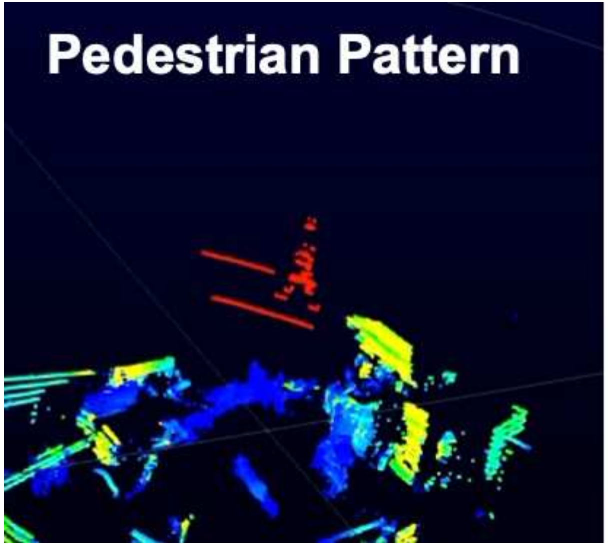
CPI attack is feasible, but only on VLP-16



- Successfully inject **6.5k points** in **83° wide range** (**99% success rate**)
    - Significantly improve the **optics** and **electronics** of spoofer devise

CPI attack is feasible, but only on VLP-16

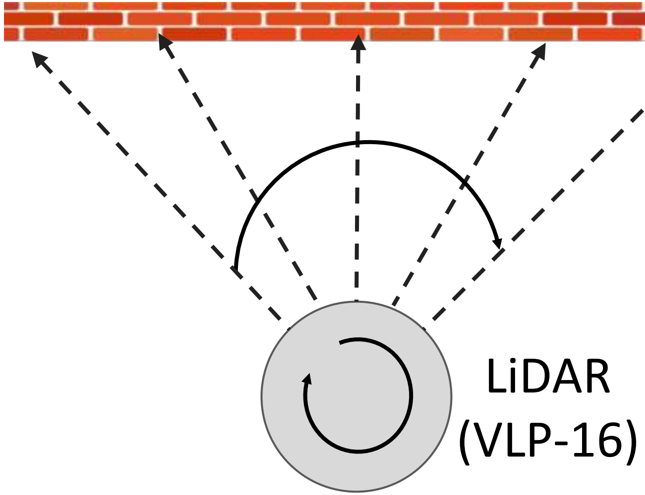

Car Pattern


Pedestrian Pattern

Text

- Successfully inject **6.5k points** in **83° wide range** (**99% success rate**)
  - Significantly improve the **optics** and **electronics** of spoofer devise
- Furthermore, **CPI attack only works on VLP-16**
  - Other LiDARs have at least one new security-related features
    - Particularly, due to **timing randomization** and **fingerprinting**

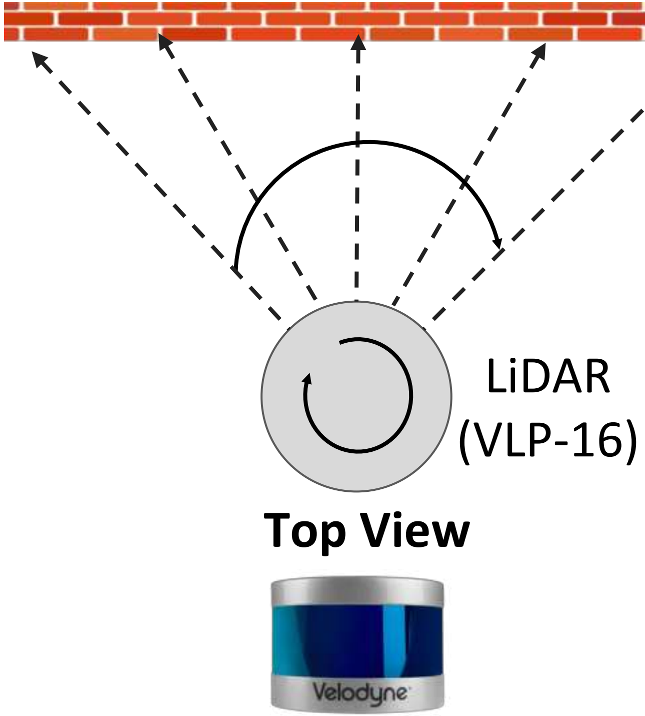
All existing attacks effective against AD are *white-box*



LiDAR
(VLP-16)

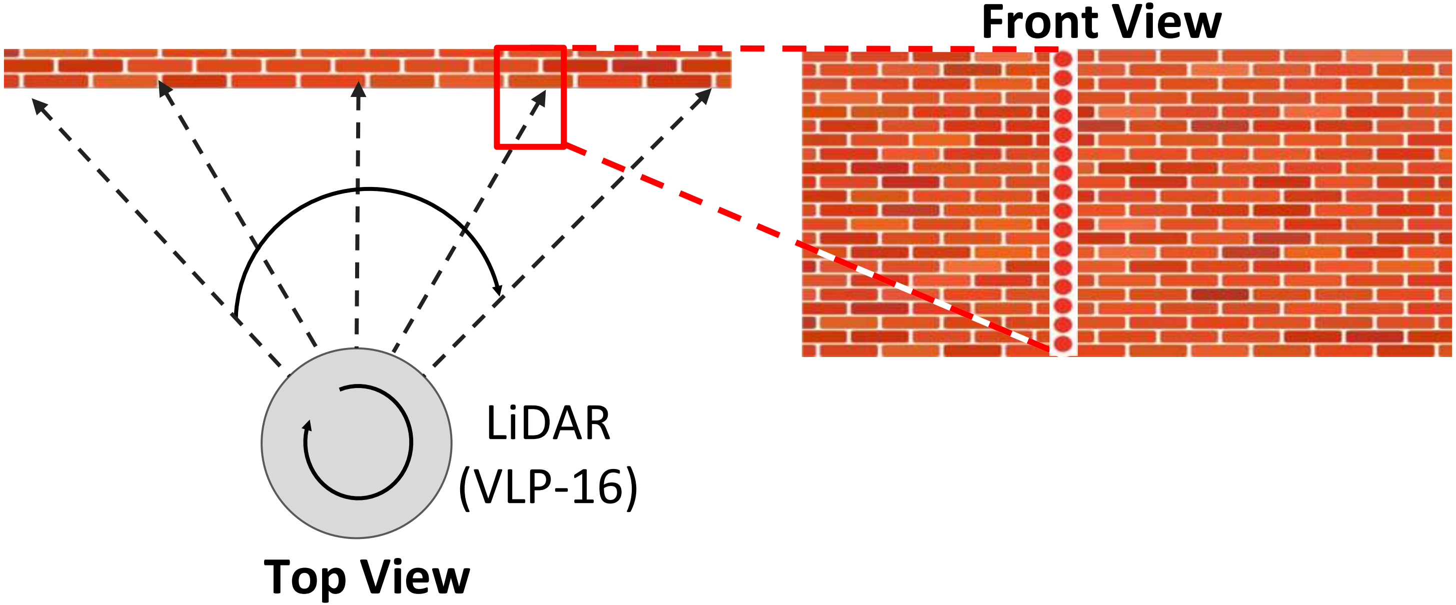
Top View

All existing attacks effective against AD are *white-box*

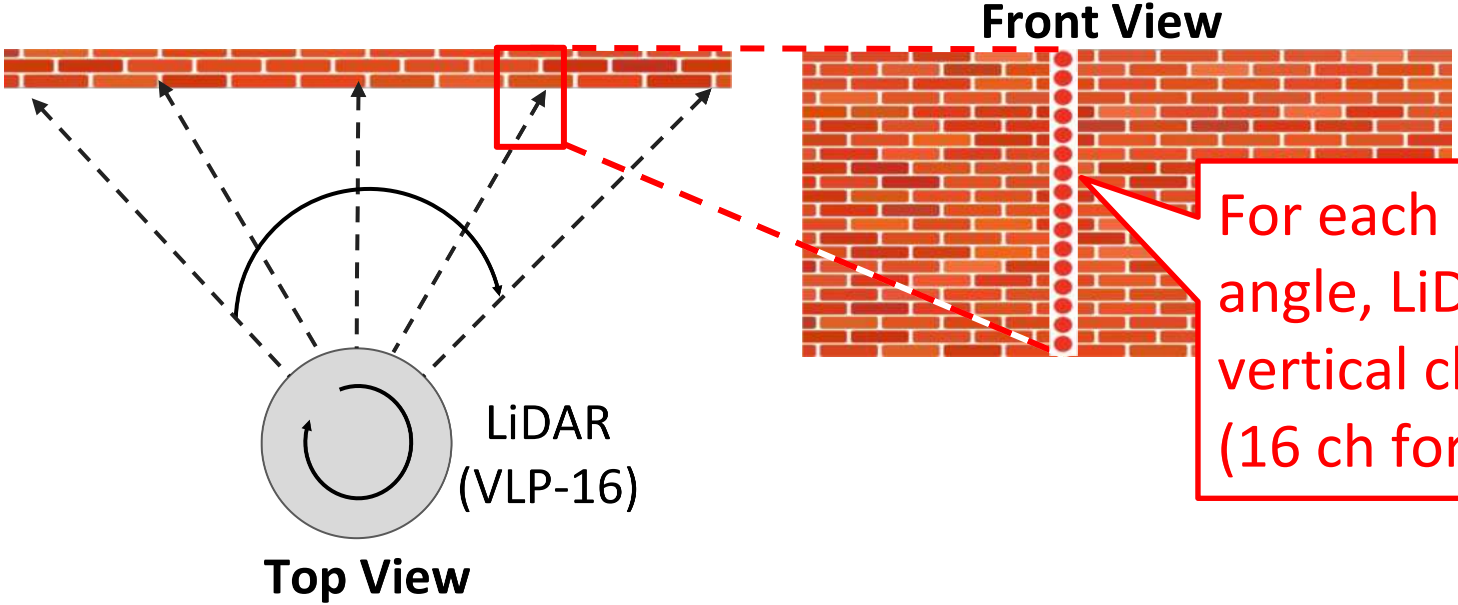


LiDAR scan horizontal angle one-by-one (e.g. every 0.1°)

All existing attacks effective against AD are *white-box*

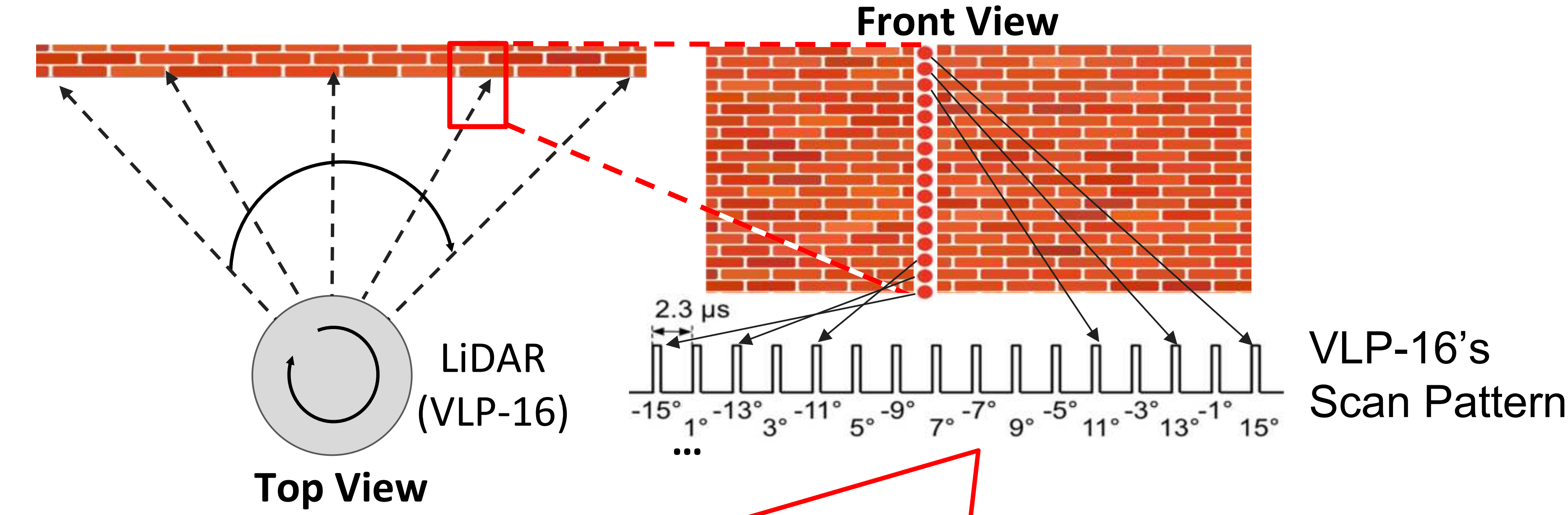


All existing attacks effective against AD are *white-box*



For each horizontal angle, LiDAR scans vertical channels (16 ch for VLP-16)

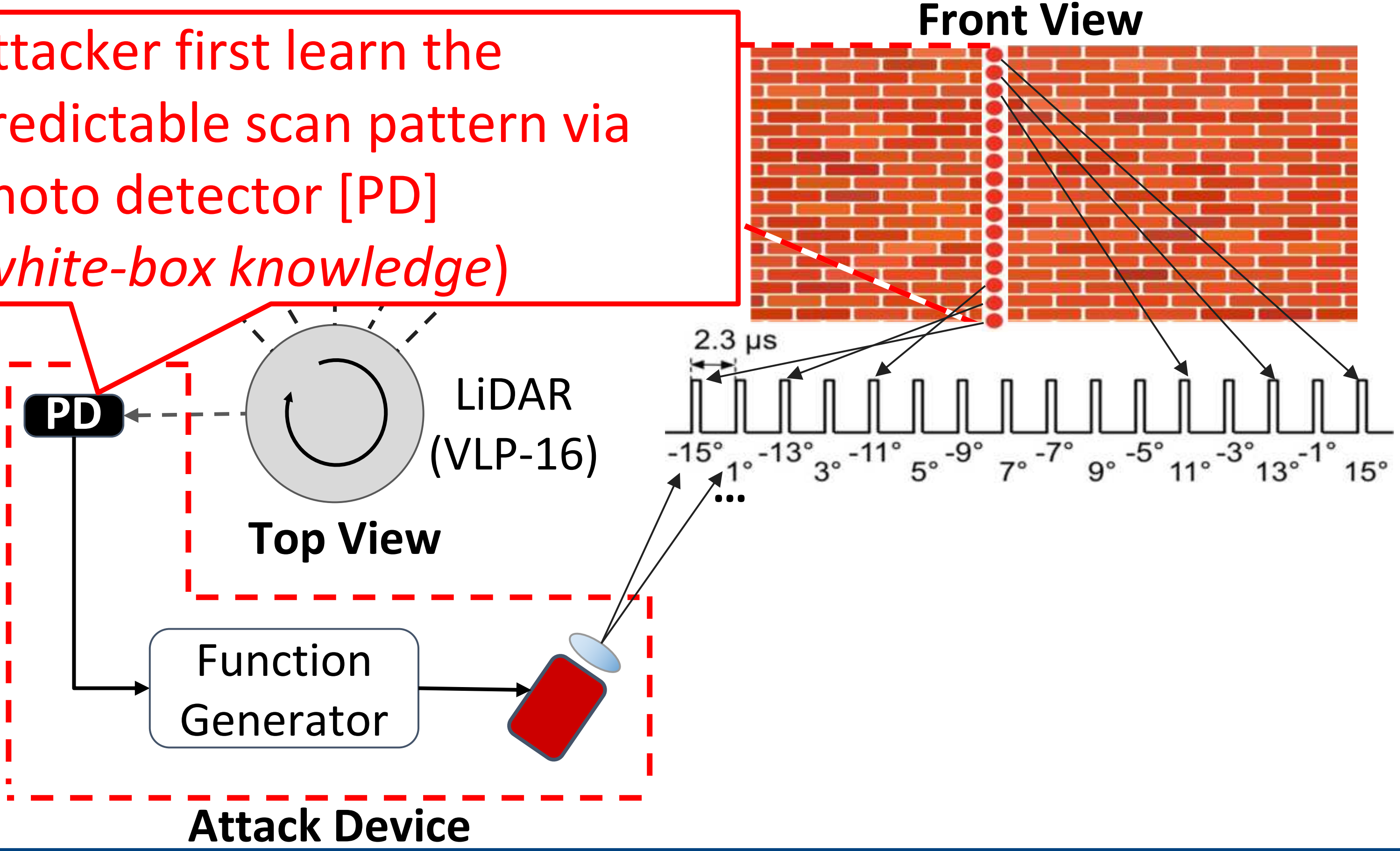
All existing attacks effective against AD are *white-box*



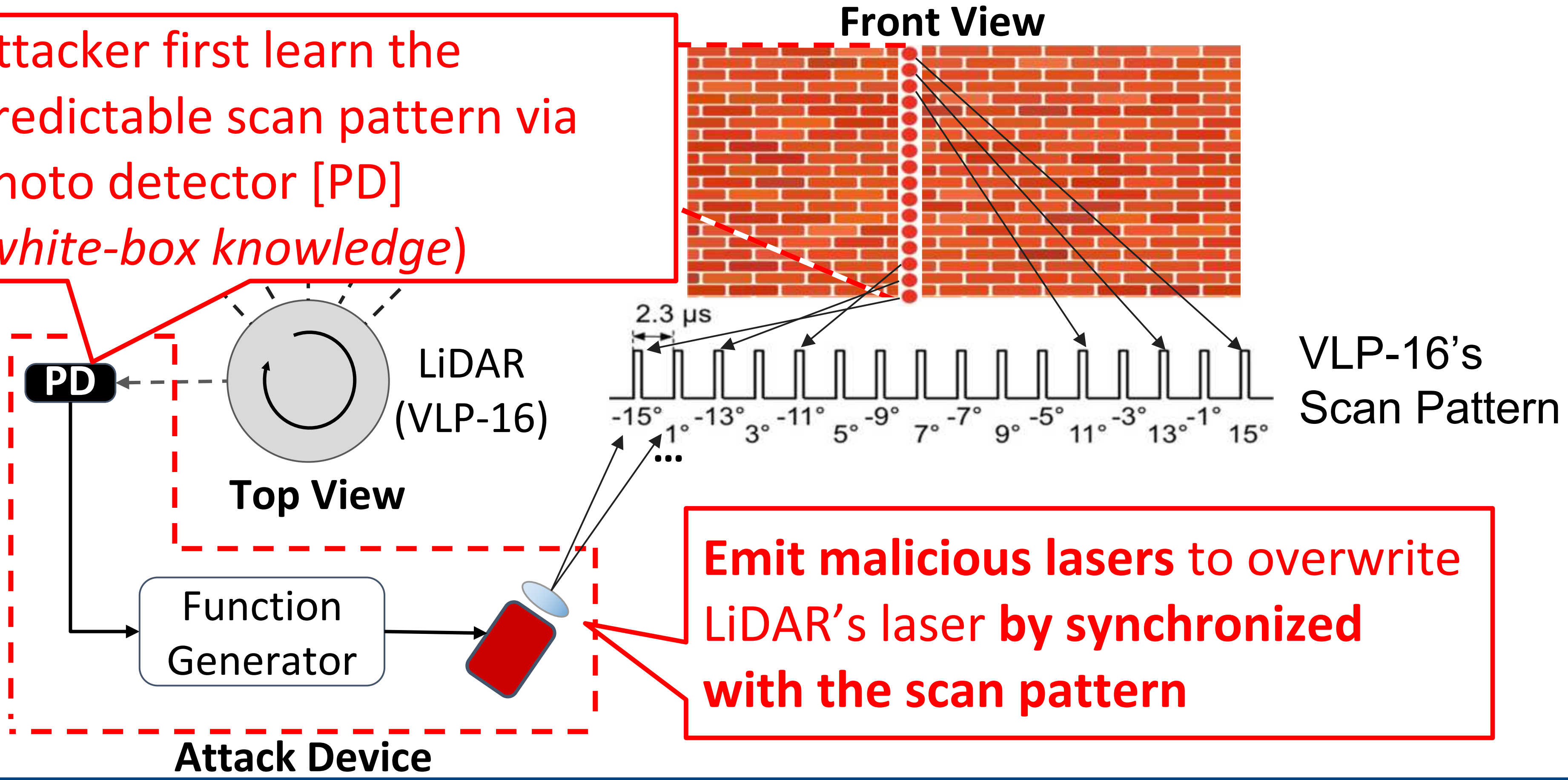
Scan pattern of VLP-16 (1st Gen LiDARs) is **deterministic** and thus **predictable**

All existing attacks effective against AD are *white-box*

Attacker first learn the predictable scan pattern via photo detector [PD] (*white-box knowledge*)



All existing attacks effective against AD are *white-box*



Attacker first learn the predictable scan pattern via photo detector [PD] (*white-box knowledge*)

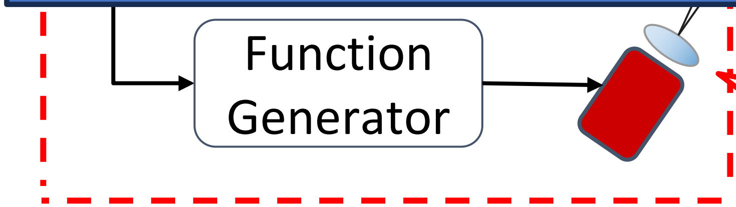
Emit malicious lasers to overwrite LiDAR's laser **by synchronized with the scan pattern**

All existing attacks effective against AD are *white-box*

Attacker first learn the predictable scan pattern via

Front View

- **Timing randomization** can directly disrupt this attack
  - **5 out of 6 New-Gen LiDARs** in our study have timing randomization
- Existing *black-box* attack is not strong enough for AD
  - Saturating attack [Sin et al, 2017] can dismiss only small area (42 cm x 42 cm) in a short time (~4 sec)

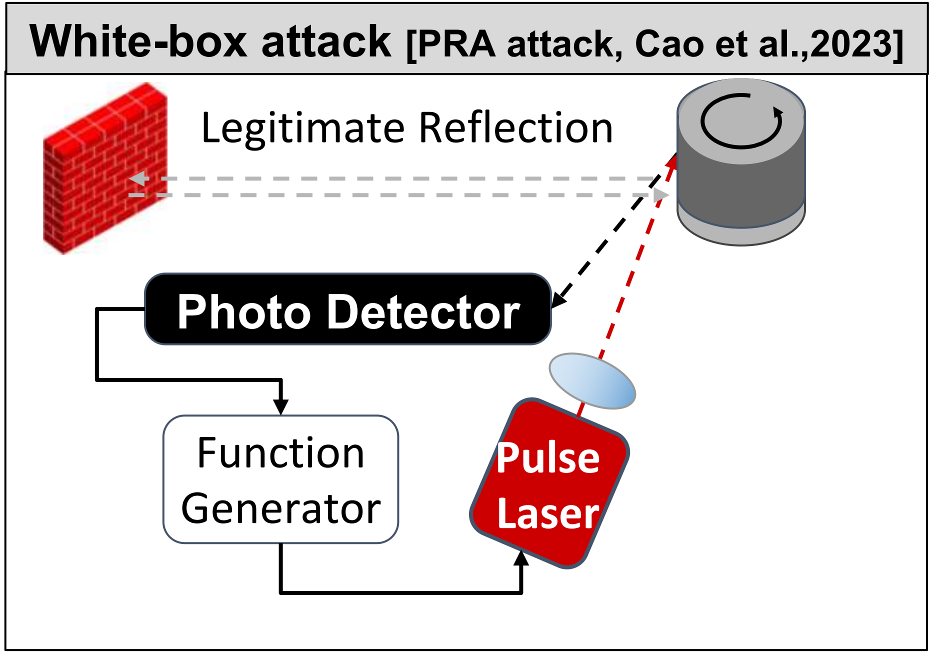


Attack Device

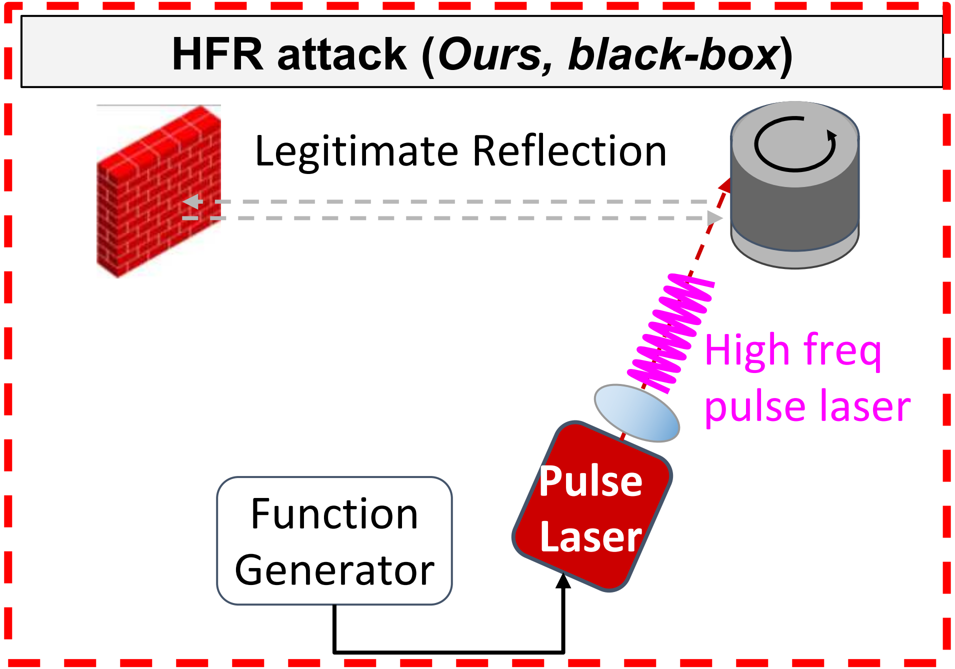
Limit malicious lasers to overwrite LiDAR's laser **by synchronized with the scan pattern**

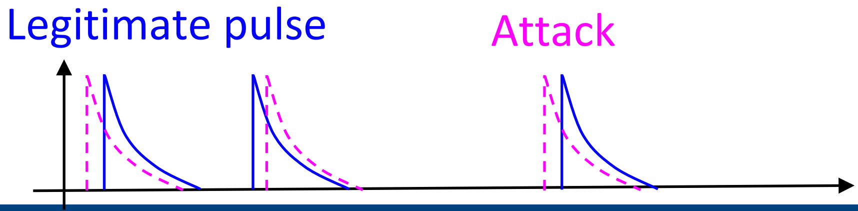
Our attack: High-Frequency Removal (HFR) attack

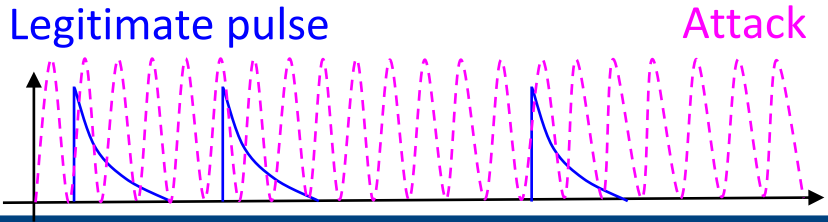
White-box attack **[PRA attack, Cao et al.,2023]**



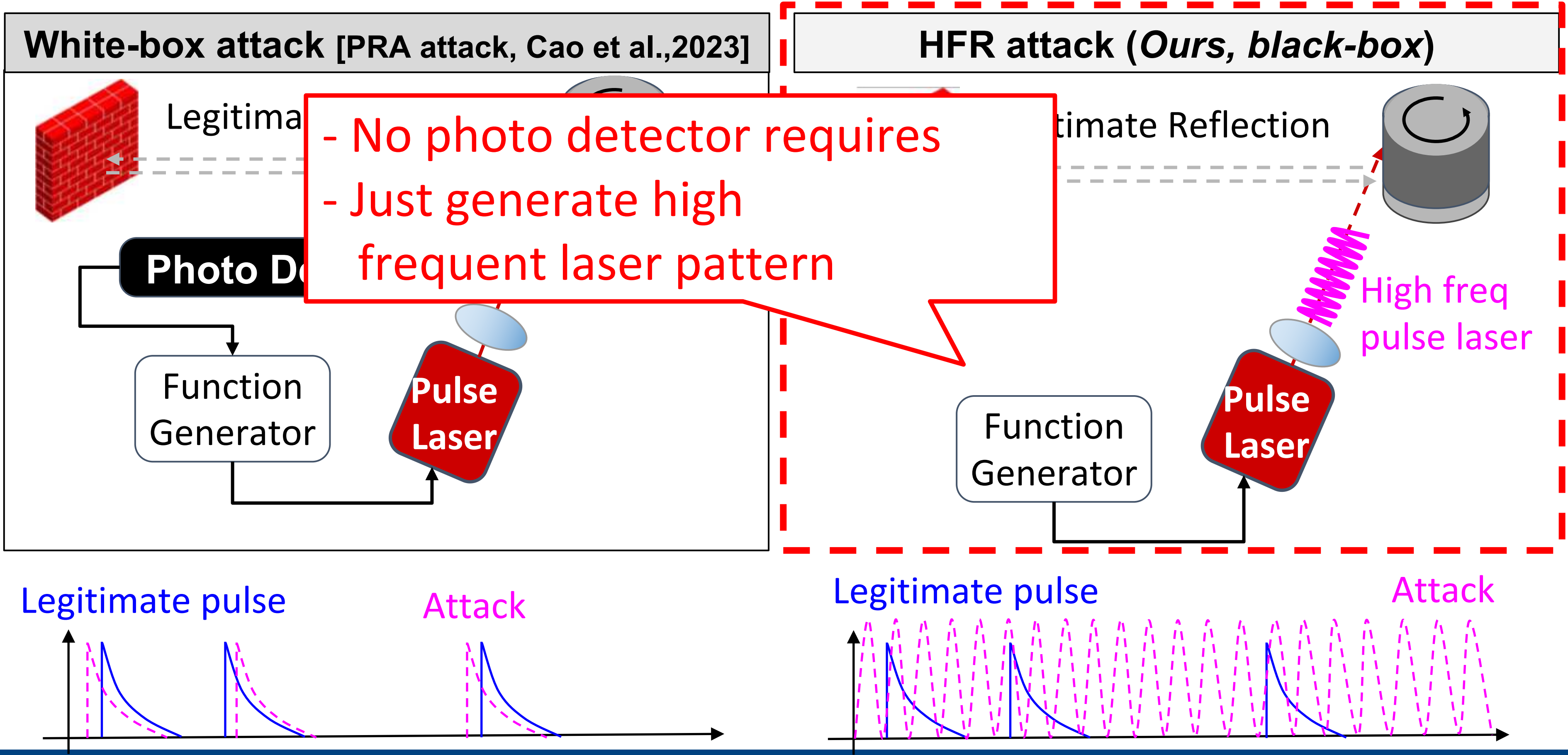
HFR attack (*Ours, black-box*)







Our attack: High-Frequency Removal (HFR) attack

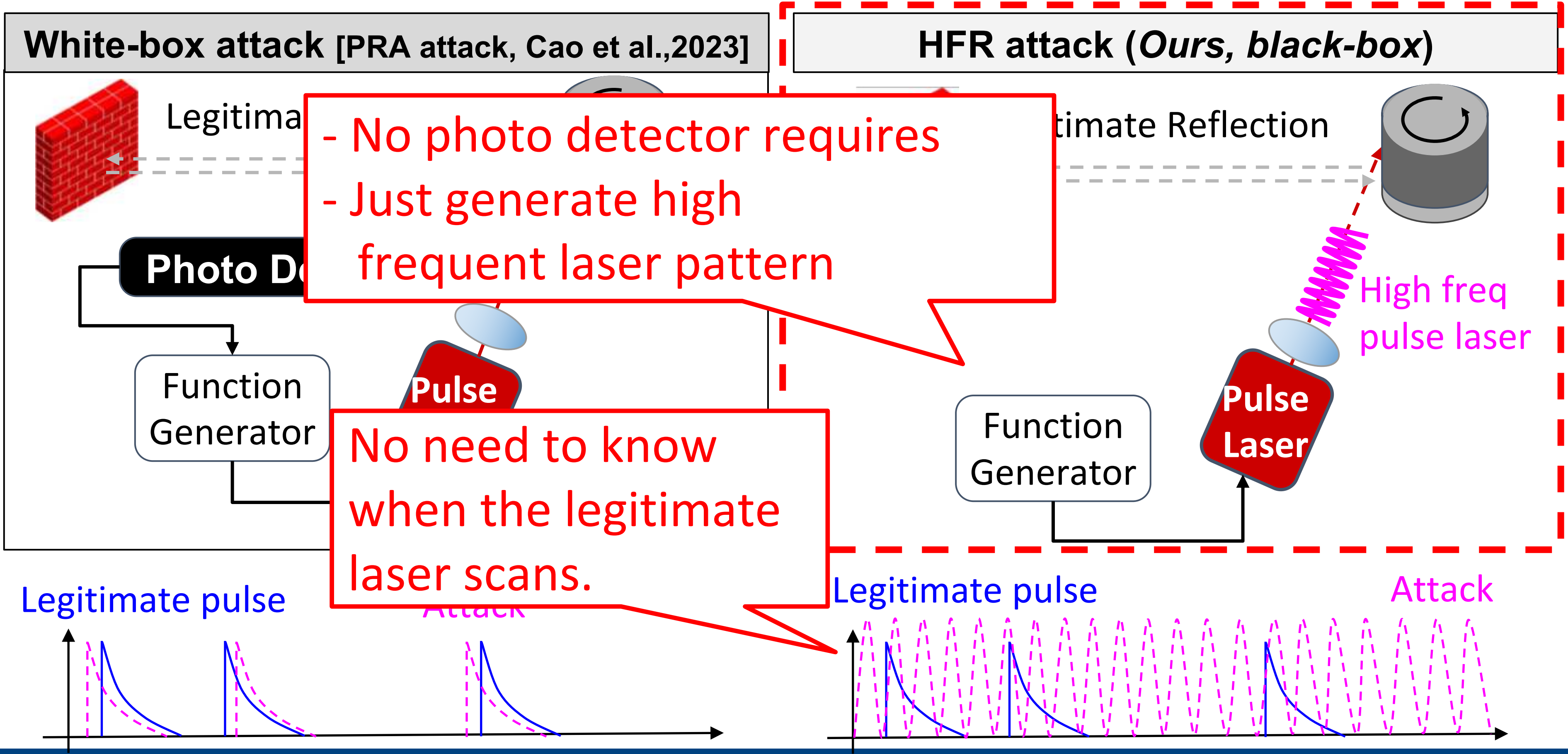


White-box attack **[PRA attack, Cao et al.,2023]**

HFR attack (*Ours, black-box*)

- No photo detector requires
- Just generate high frequent laser pattern

Our attack: High-Frequency Removal (HFR) attack



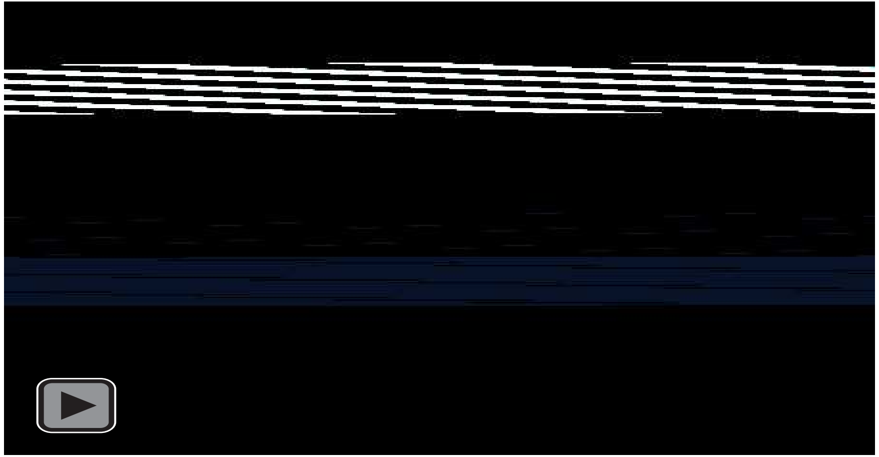
- No photo detector requires
- Just generate high frequent laser pattern

No need to know when the legitimate laser scans.

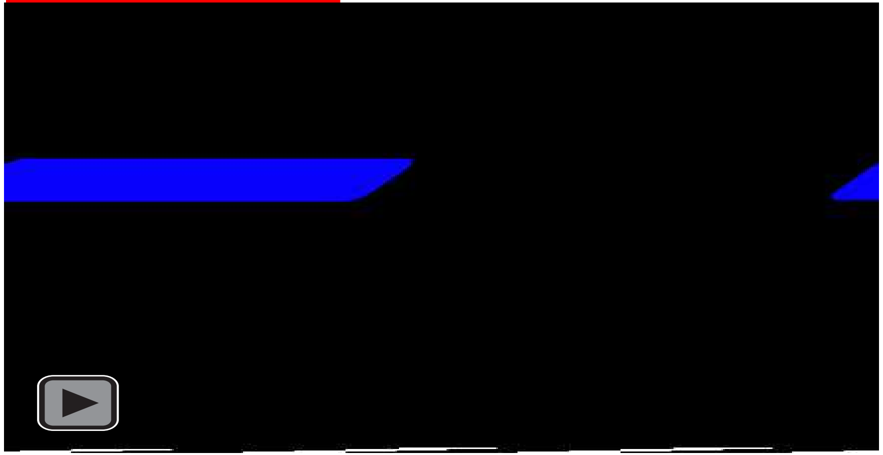
HFR attack indoor demo

Camera

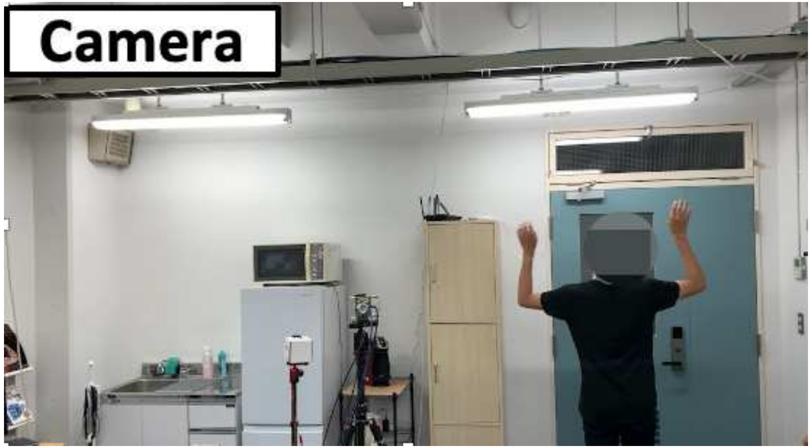
Benign

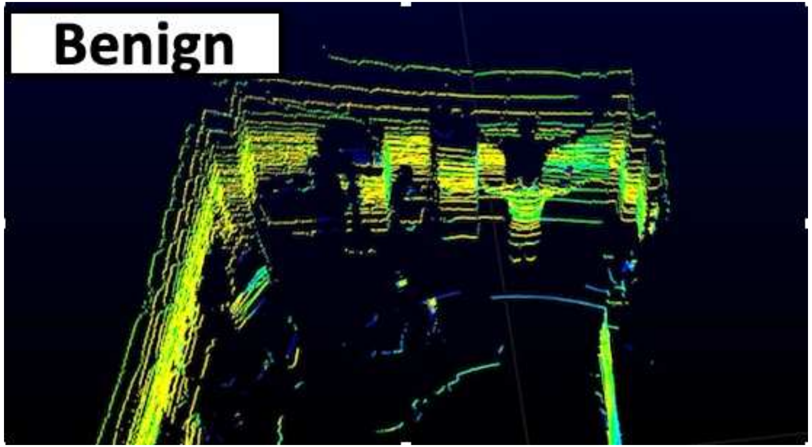


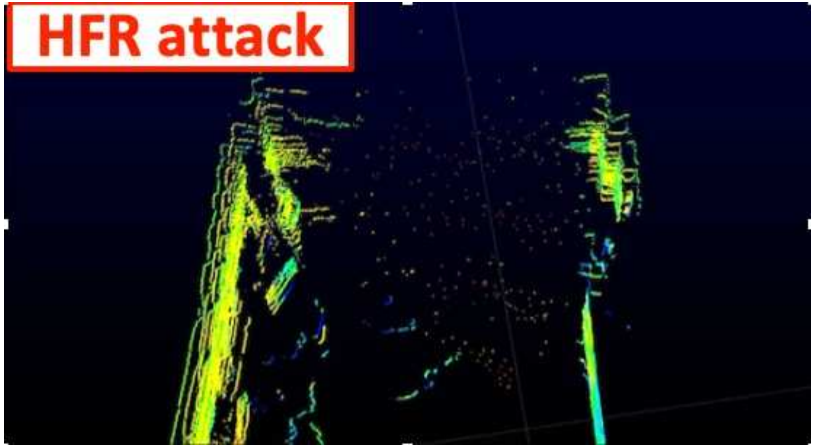
HFR attack



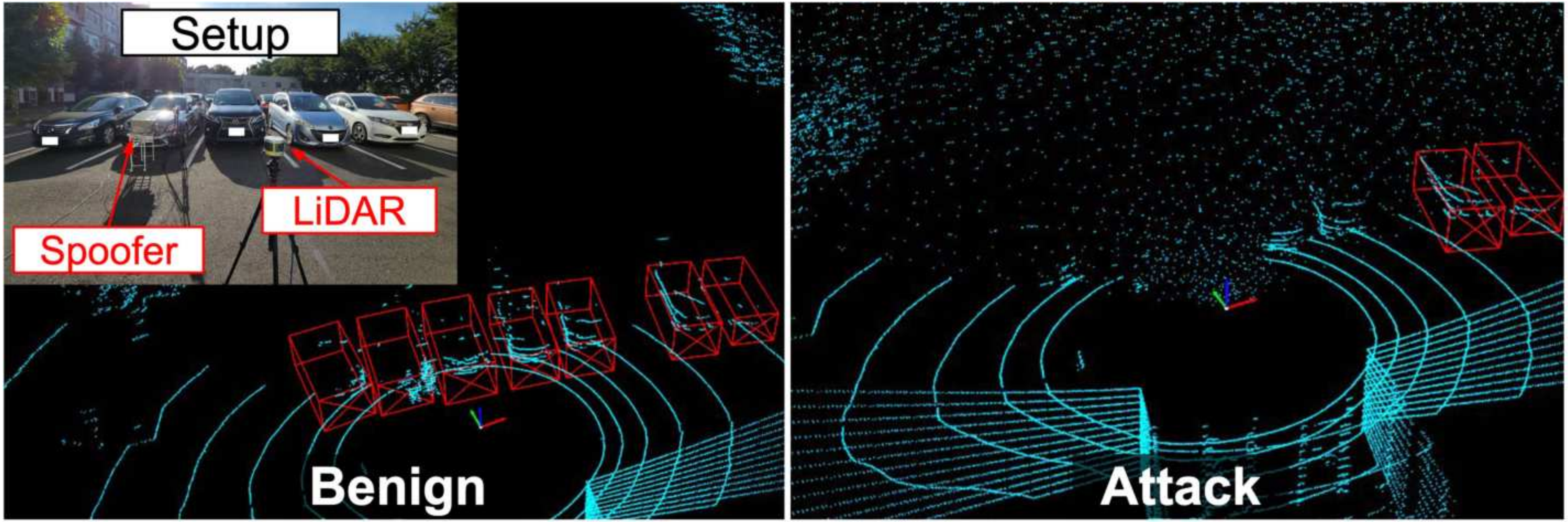
HFR attack indoor demo





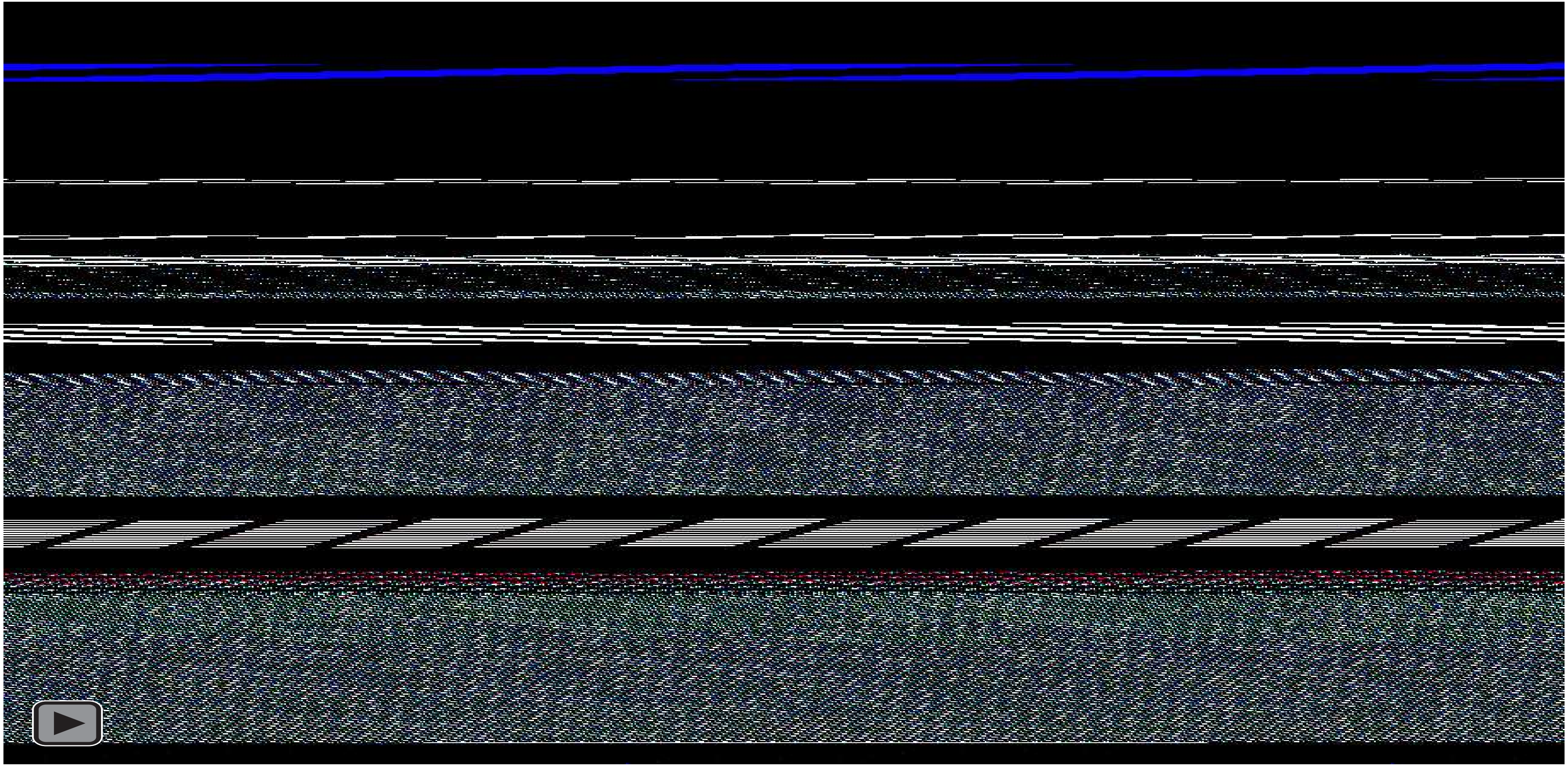


HFR attack outdoor demo

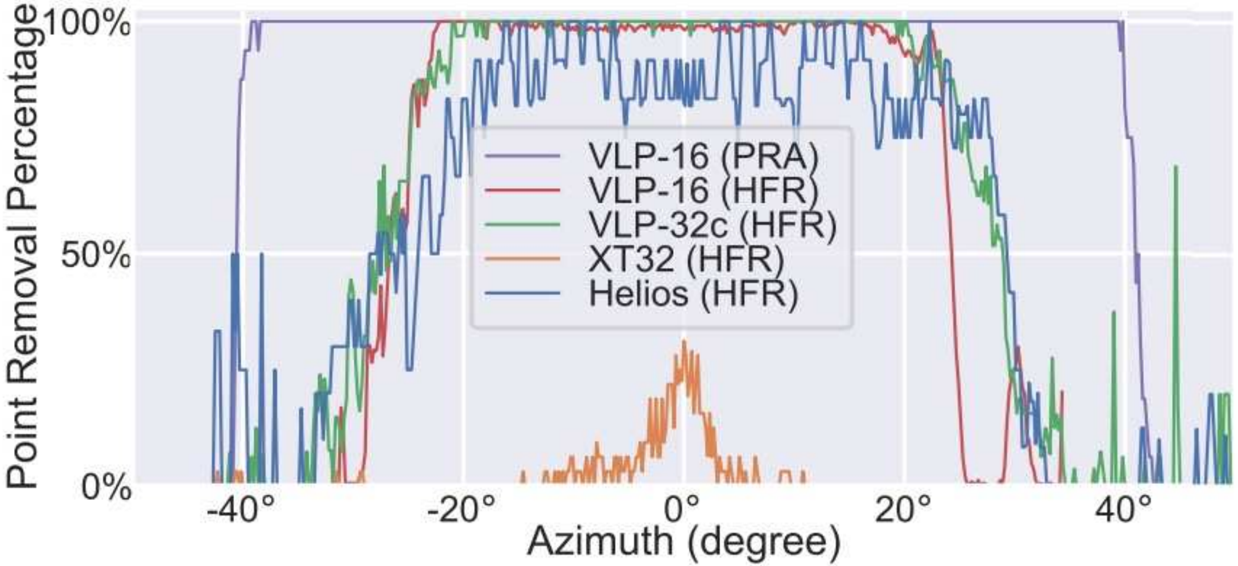


5 cars are not detected by Apollo 6.0’s PointPillars object detector

HFR attack outdoor demo

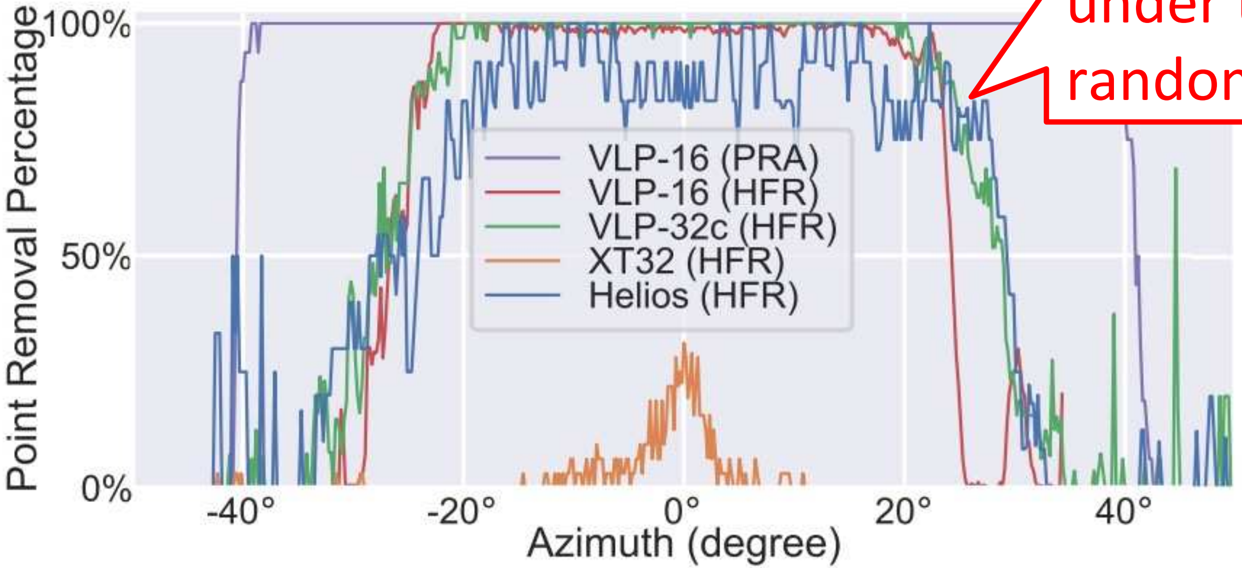


Modeling HFR attack capability



- Measure removal success rates for each azimuth angle for each LiDAR
  - PRA attack (prior work) can only work on 1st Gen (VLP-16)

Modeling HFR attack capability

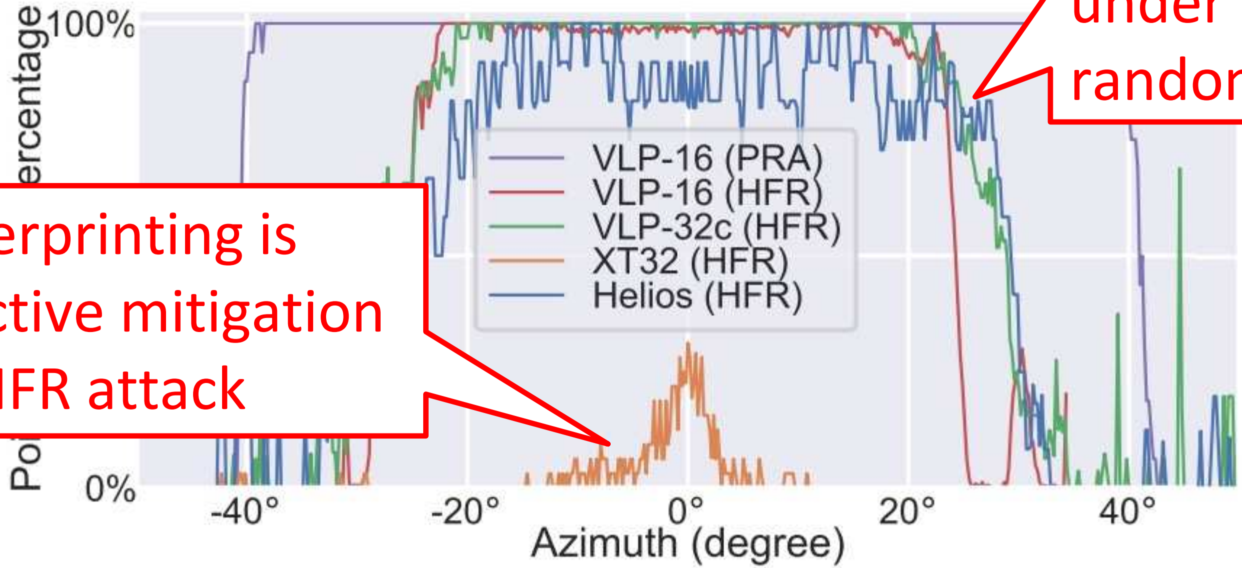


HFR attack is effective even under timing randomization

- Measure removal success rates for each azimuth angle for each LiDAR
  - PRA attack (prior work) can only work on 1st Gen (VLP-16)

Modeling HFR attack capability

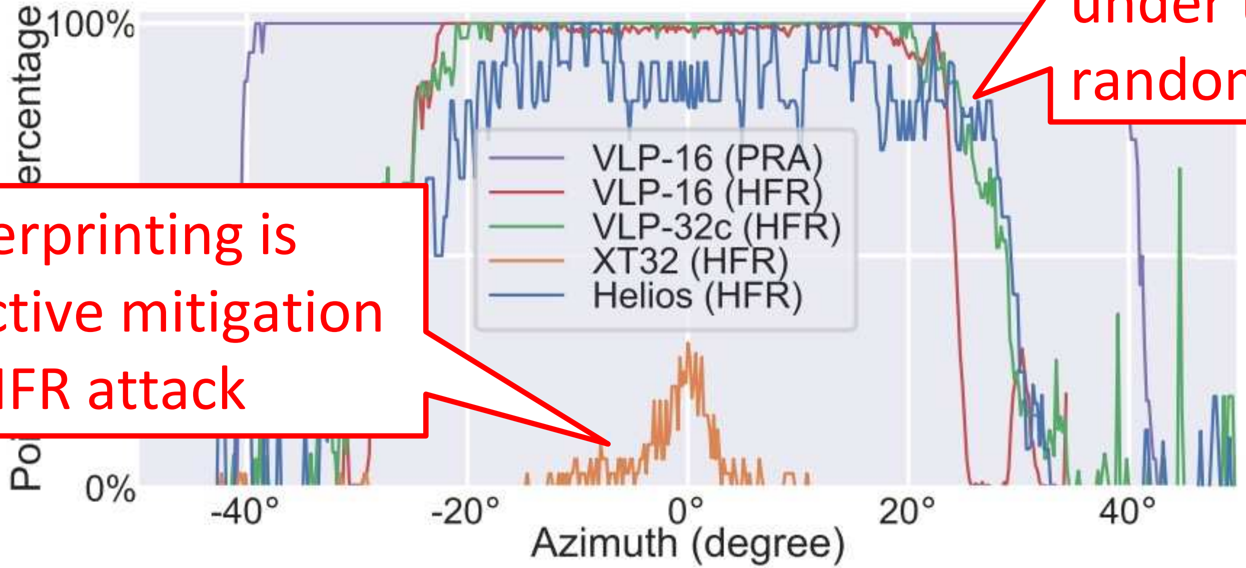
HFR attack is effective even under timing randomization



Fingerprinting is effective mitigation for HFR attack

- Measure removal success rates for each azimuth angle for each LiDAR
  - PRA attack (prior work) can only work on 1st Gen (VLP-16)

Modeling HFR attack capability

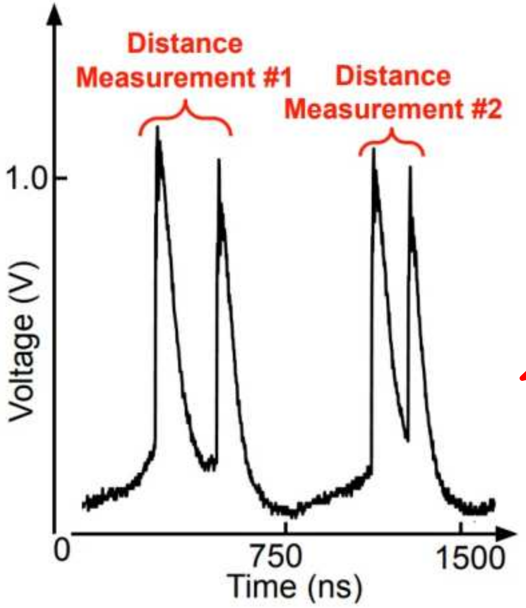


HFR attack is effective even under timing randomization

Fingerprinting is effective mitigation for HFR attack

- Measure removal success rates for each azimuth angle for each LiDAR
  - PRA attack (prior work) can only work on 1st Gen (VLP-16)

Our observations on XT32's Fingerprinting

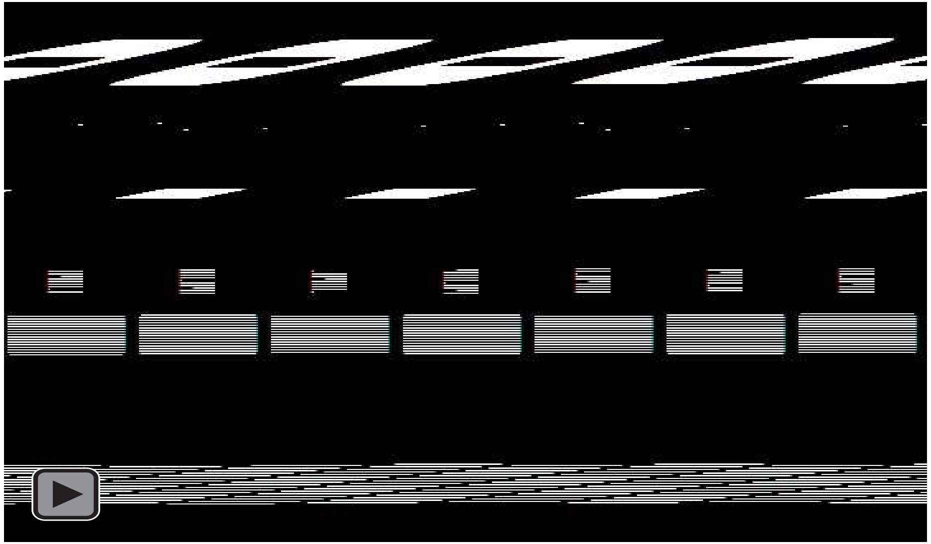


Pulse shapes of XT32's lasers

- XT32 emits couple of lasers for each point measurement
- We suspect that the fingerprinting is embedded in the interval
    - High freq. lasers may sometimes hit the interval
    - No official documentation is available on this

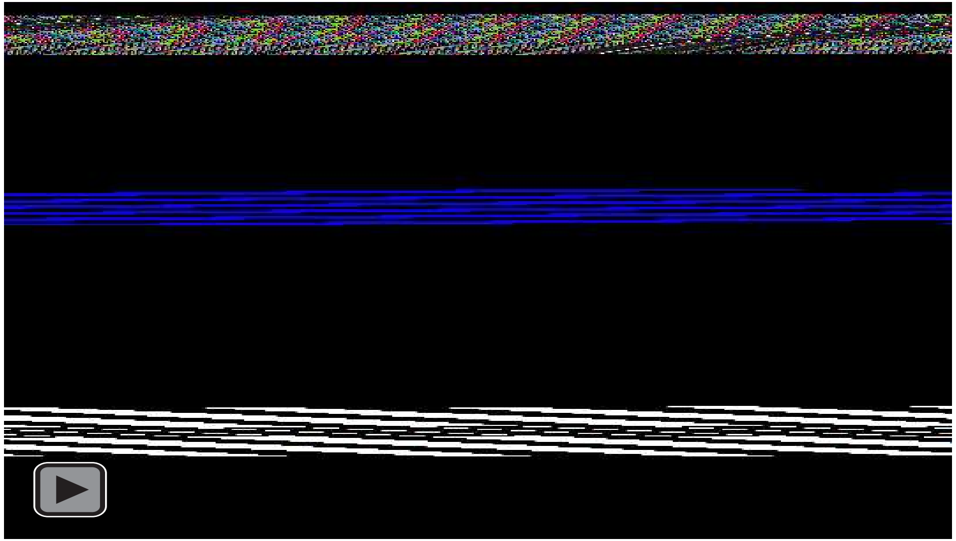
HFR attack evaluation in AD Scenarios

Benign



(x2 faster)

HFR attack on LiDAR w/ timing rand.

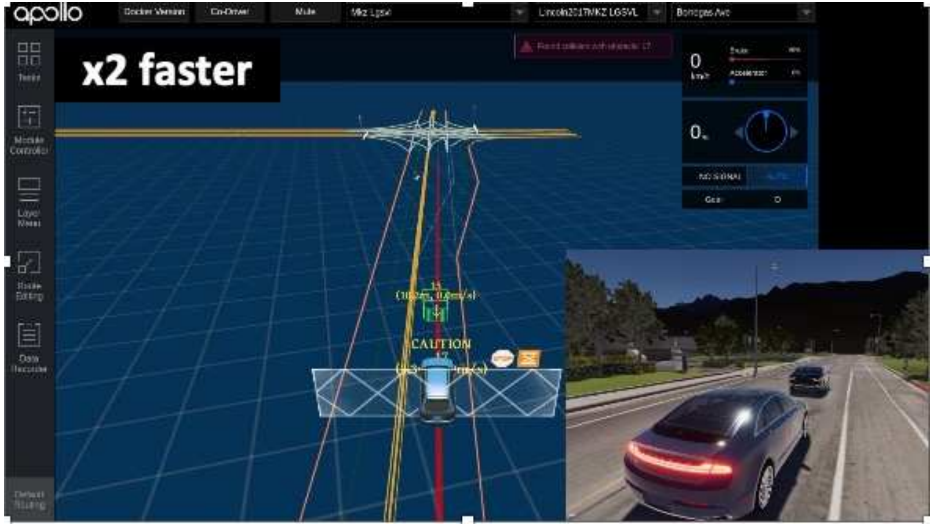


(x2 faster)

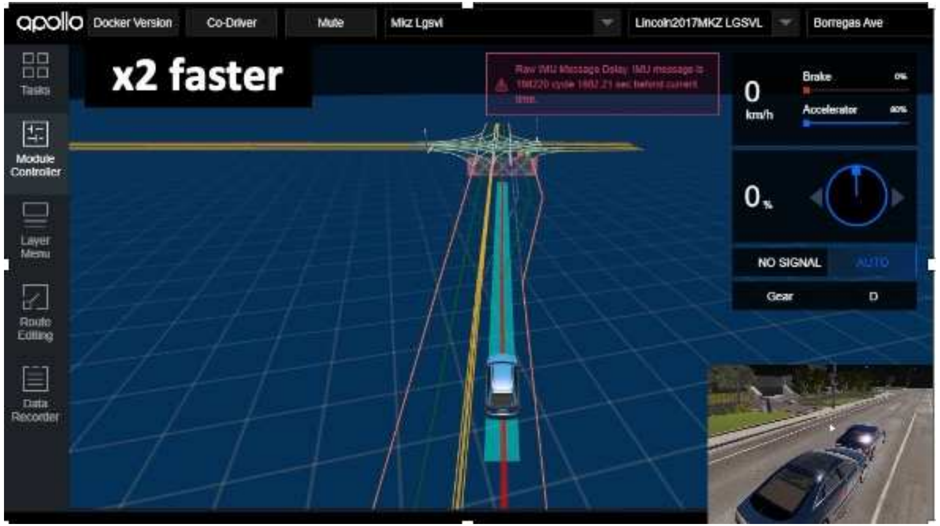
- AD Stack: Apollo 7.0
- Simulator: LGSVL
- Speed: 40 km/h
- Attack Model: Helios (HFR)
- Attack starts at 20 m away from the obstacle (sedan car)

HFR attack evaluation in AD Scenarios

Benign



HFR attack on LiDAR w/ timing rand.



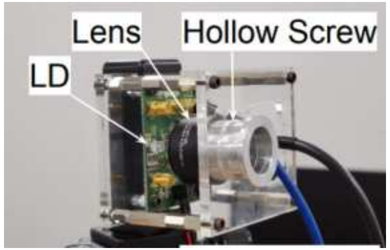
Raw IMU Message Delay. IMU message is [illegible] sec behind current time.

- AD Stack: Apollo 7.0
- Simulator: LGSVL
- Speed: 40 km/h
- Attack Model: Helios (HFR)
- Attack starts at 20 m away from the obstacle (sedan car)

Other findings

Attack Device Improvements

- Our new attack device can achieve inject **>6k** points in **>80°**
- **CPI attack is feasible** on VLP-16 with our device
- Model-level vulnerability may not be necessary to attack object detector



New-Gen LiDAR Measurements & Attack Modeling

New Attack Modeling

Injection Attack

- CPI attack is **feasible only on VLP-16**
- **Pulse fingerprinting is not strong enough** to perfectly prevent injection
- **Error modeling** has major impact

Removal Attack

- **Latest removal attack is not feasible** on New-Gen LiDARs
- **Our HFR attack can be effective** even against New-Gen LiDARs

Security Analysis w/ 9 object detectors & AD Simulator

(Autonomous Driving)

- **Pulse fingerprinting is effective mitigation** against injection attacks
- **Timing randomization is effective mitigation** against injection

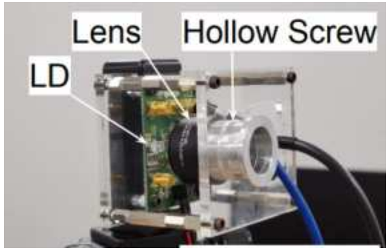
- **Pulse fingerprinting is effective mitigation** against removal attacks
- Vulnerability of object detector heavily **depends on their training data**
- **HFR attack can be effective against autonomous driving scenarios**

Other findings

Error modeling is important. Prior work's model is not accurate [Hallyburton et al., 2022]

Attack Device Improvements

- Our new attack device can achieve inject **>6k** points in **>80°**
- **CPI attack is feasible** or VLP-16 with our device
- Model-level vulnerability may not be necessary to attack object detector



New-Gen LiDAR Measurements

ack
ng

enough to perfectly pre injection

- **Error modeling** has major impact

Removal Attack

- **Latest removal attack is not feasible** on New-Gen LiDARs
- **Our HFR attack can be effective** even against New-Gen LiDARs

Security Analysis w/ 9 object detectors & AD Simulator

(Autonomous Driving)

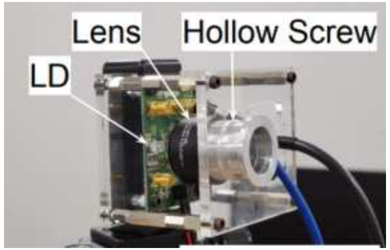
- **Pulse fingerprinting is effective mitigation** against injection attacks
- **Timing randomization is effective mitigation** against injection

- **Pulse fingerprinting is effective mitigation** against removal attacks
- Vulnerability of object detector heavily **depends on their training data**
- **HFR attack can be effective against autonomous driving scenarios**

Other findings

Attack Device Improvements

- Our new attack device can achieve inject **>6k** points in **>80°**
- **CPI attack is feasible** on VLP-16 with our device
- Model-level vulnerability may not be necessary to attack object detector



New-Gen Li
& Att

Timing randomization is effective mitigation strategy both for injection and removal attack

ysis w/ 9 object
AD Simulator
nomous Driving)

Injection At

- CPI attack is
- **Pulse fingerprinting is not strong enough** to perfectly prevent injection
- **Error modeling** has major impact

nting is effective
tion against injection attacks

- **Timing randomization is effective mitigation** against injection

Removal Attack

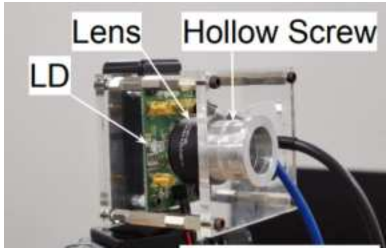
- **Latest removal attack is not feasible** on New-Gen LiDARs
- **Our HFR attack can be effective** even against New-Gen LiDARs

- **Pulse fingerprinting is effective mitigation** against removal attacks
- Vulnerability of object detector heavily **depends on their training data**
- **HFR attack can be effective against autonomous driving scenarios**

Other findings

Attack Device Improvements

- Our new attack device can achieve inject **>6k** points in **>80°**
- **CPI attack is feasible** on VLP-16 with our device
- Model-level vulnerability may not be necessary to attack object detector



New-Gen LiDAR Measurements & Attack Modeling

New Attack Modeling

Injection Attack

- CPI attac
- **Pulse fin** **enough** t
- **Error mo**

Removal

- **Latest re** **feasible** on New-Gen LiDARs
- **Our HFR attack can be effective** even against New-Gen LiDARs

Security Analysis w/ 9 object detectors & AD Simulator

(Autonomous Driving)

ngerprinting is effective **on** against injection attacks

randomization is effective **on** against injection

ngerprinting is effective **nitigation** against removal attacks

- Vulnerability of object detector heavily **depends on their training data**
- **HFR attack can be effective against autonomous driving scenarios**

Selection of training data is important. Some model is very sensitive to small number of points.

Conclusion

- **First large-scale measurement study on New-Gen LiDARs**
  - Uncover **15 novel research findings**
  - Significantly **improve spoofing capability with enhanced optics and electronics**
  - Show that **common assumptions in 1st Gen LiDARs do not hold on New-Gen**
- **Design more accurate attack modeling of LiDAR spoofing attacks**
  - Model attack capabilities **both for injection and removal attacks**
  - Evaluate **3 major object detectors** trained on **5 datasets** with the attack models
  - Identify that **timing randomization** and **pulse fingerprinting** have **high mitigation capability** against LiDAR spoofing attacks
- **Design first practical black-box removal attack on New-Gen LiDARs**
  - **HFR** shows **high effectiveness on New-Gen LiDARs with timing randomization**
- **Performed Responsible Vulnerability Disclosure**
  - Informed 7 LiDAR suppliers and 3 AD companies. 5 are investigating our report

Thank you!

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

https://sites.google.com/view/cav-sec/new-gen-lidar-sec

or

Contact me, Takami Sato <takamis@uci.edu>

AS^{2}Guard Autonomous & Smart Systems Guard Research Group

UCI

Yoshioka Lab

Keio University
CALAMVS GLADIO FORTIOR
1858