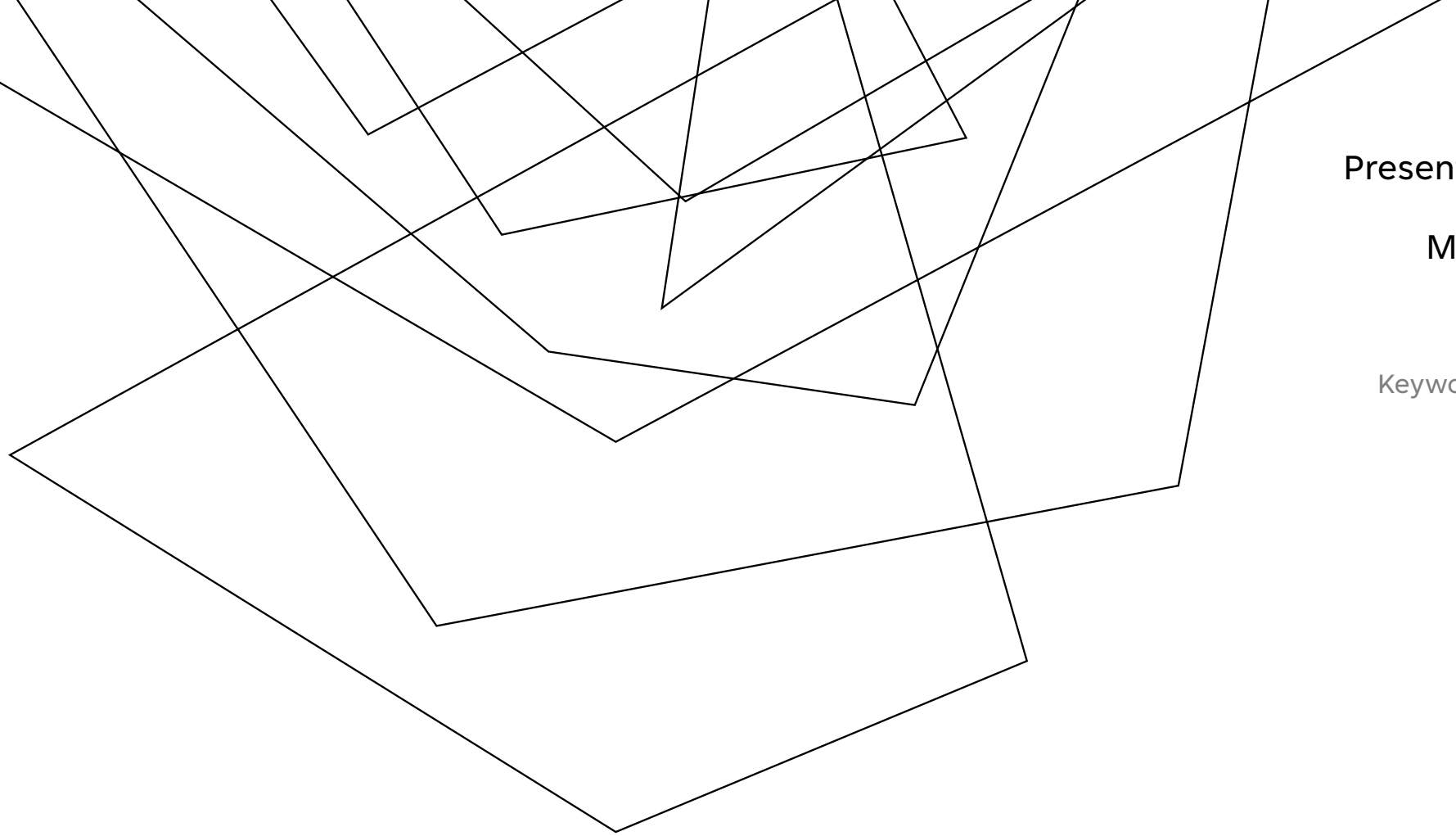


Presented by Mateo PENA CAMPOS

Most slides are borrowed from author's slide

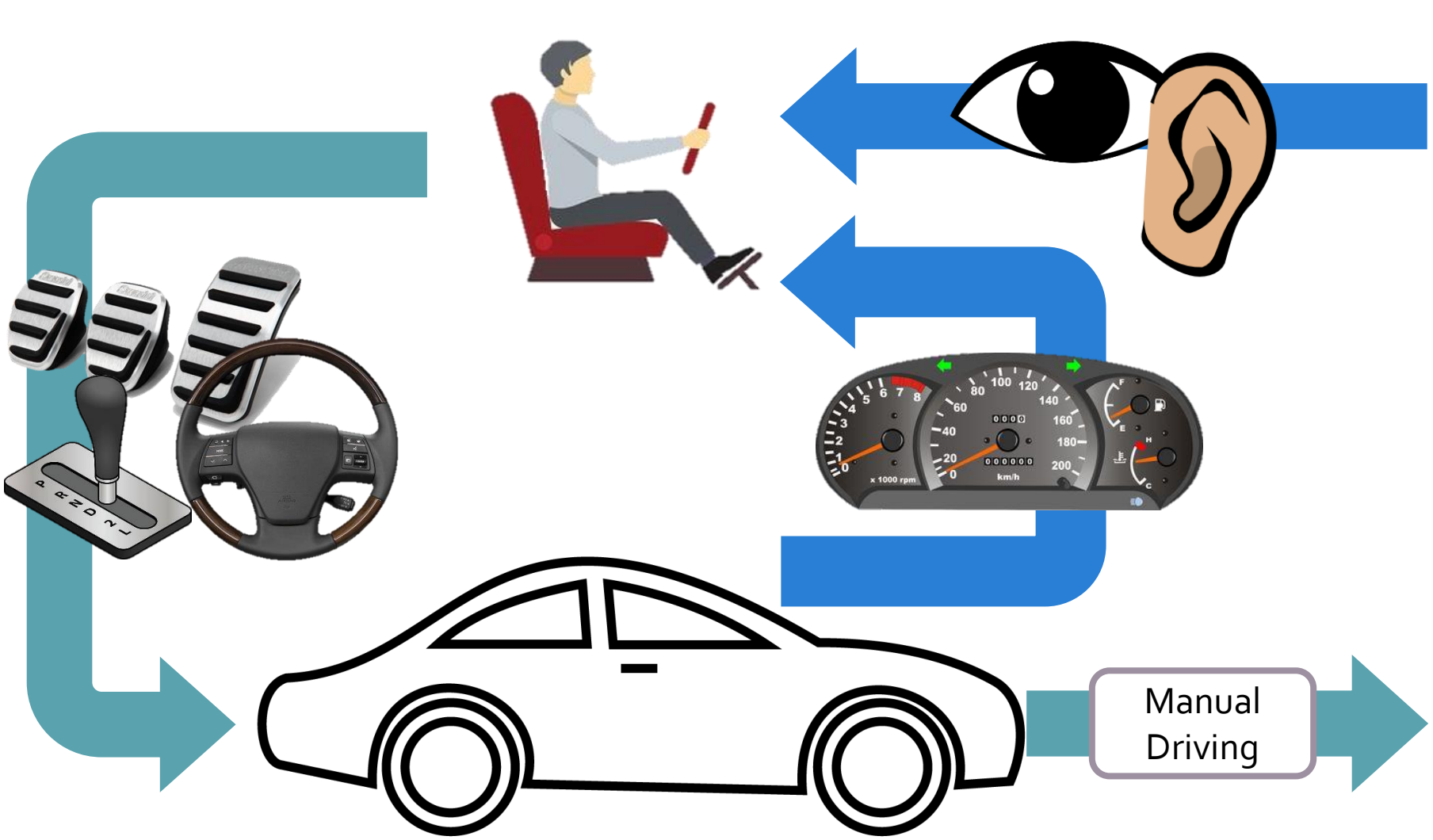
Keywords: attack, autonomous car, sensor, lidar, saturating, spoofing

Illusion and Dazzle: Adversarial Optical Channel Exploits against Lidars for Automotive Applications

Hocheol Shin, Dohyun Kim, Yujin Kwon, and Yongdae Kim

CHES'17

Human Driving



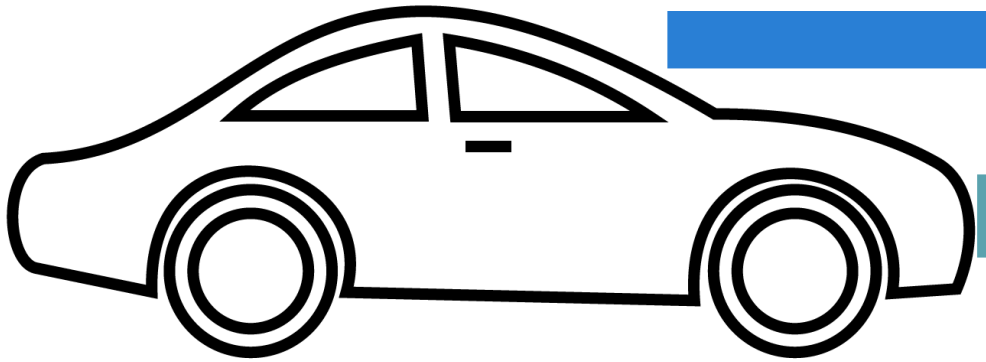
Autonomous Driving: a Sensing & Actuation System

Inter-vehicle Network

GNSS

Intra-vehicle Network

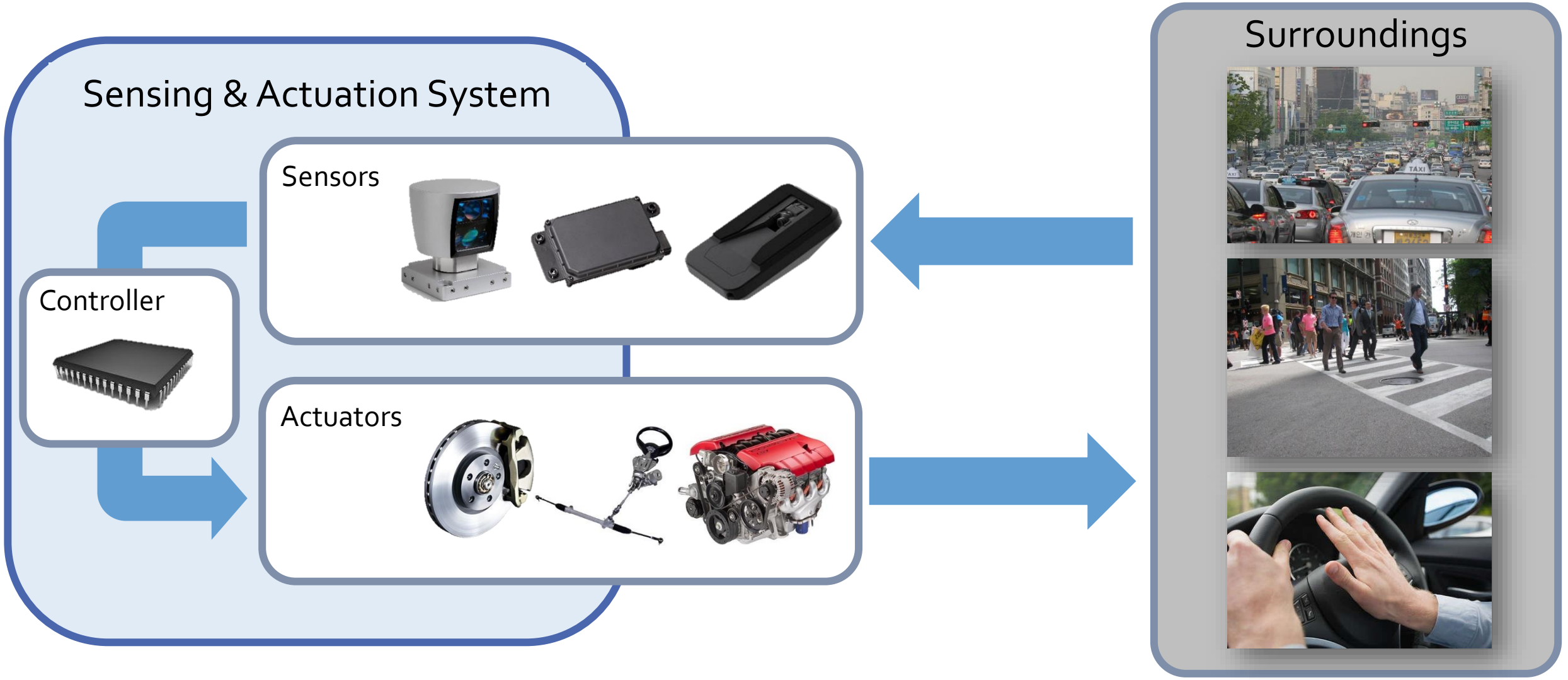
Intra-vehicle Network



Autonomous Driving

Surroundings

Sensor Attacks against Sensing & Actuation Systems



Sensor Attacks against Sensing & Actuation Systems

W/O Security Features

ation System

Sensors



Cont er

Actuators



Surroundings

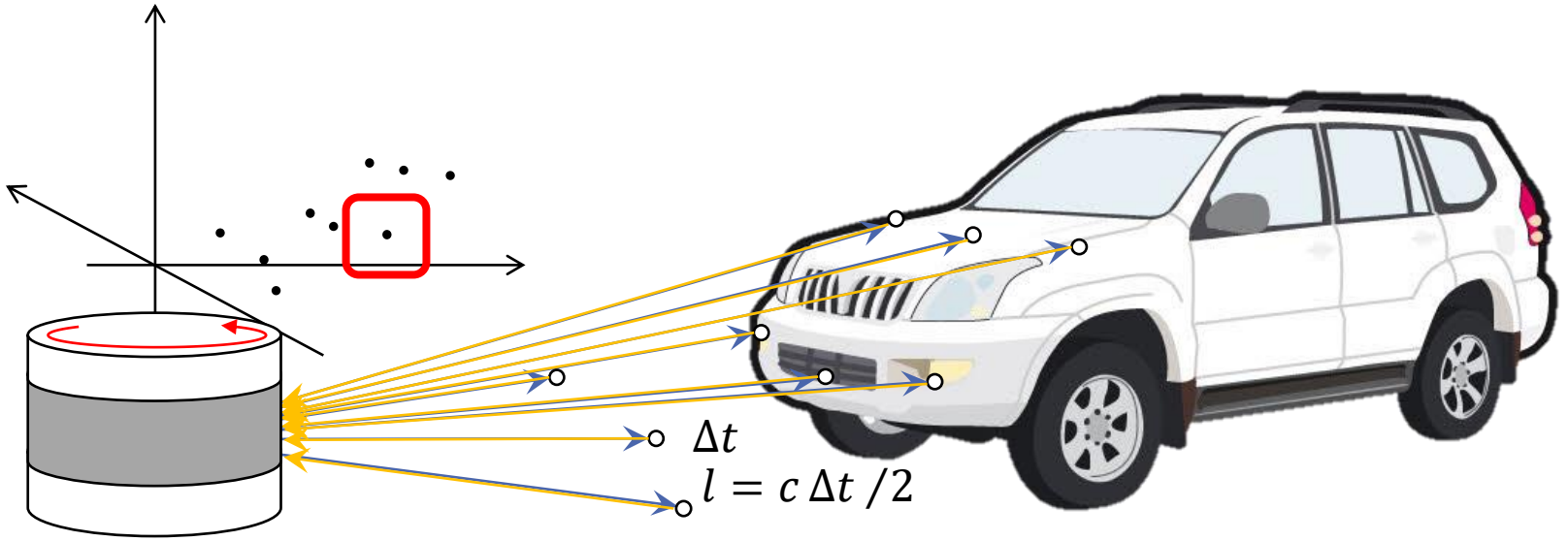


Introduction

- What is lidar ? How does it work ?
- 2 attacks against lidar
  - Saturation attack
  - Spoofing attack
- Countermeasures and its limitations

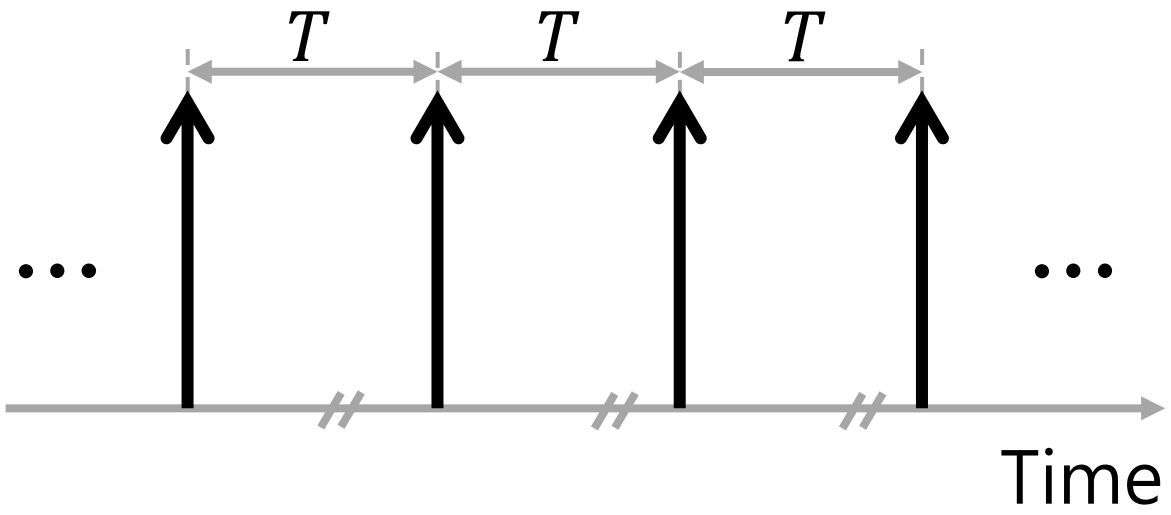
Lidar = **Li**ght **D**etection **a**nd **R**anging

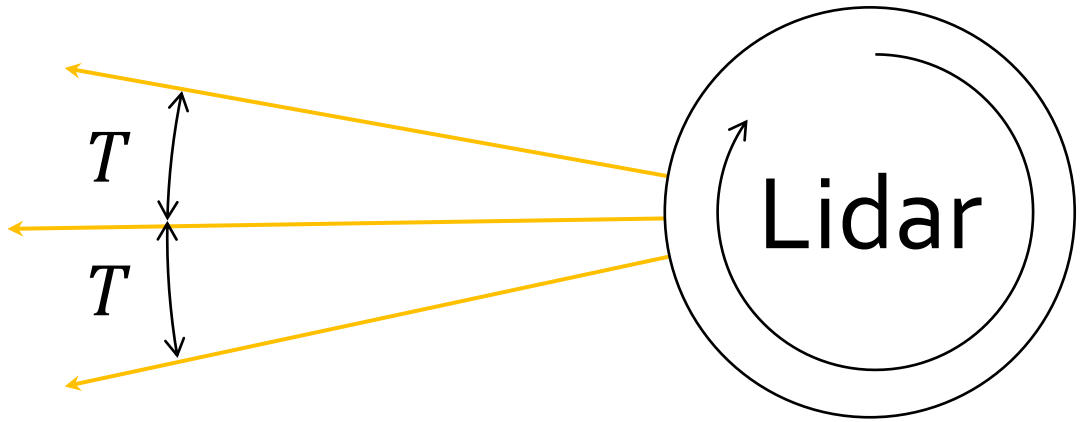
- Working principle
  - Similar to radars / sonars / ultrasonic sensors except media
  - Multi-layer scanning lidar ≙ rotating 3D-mapping lidar



Lidar

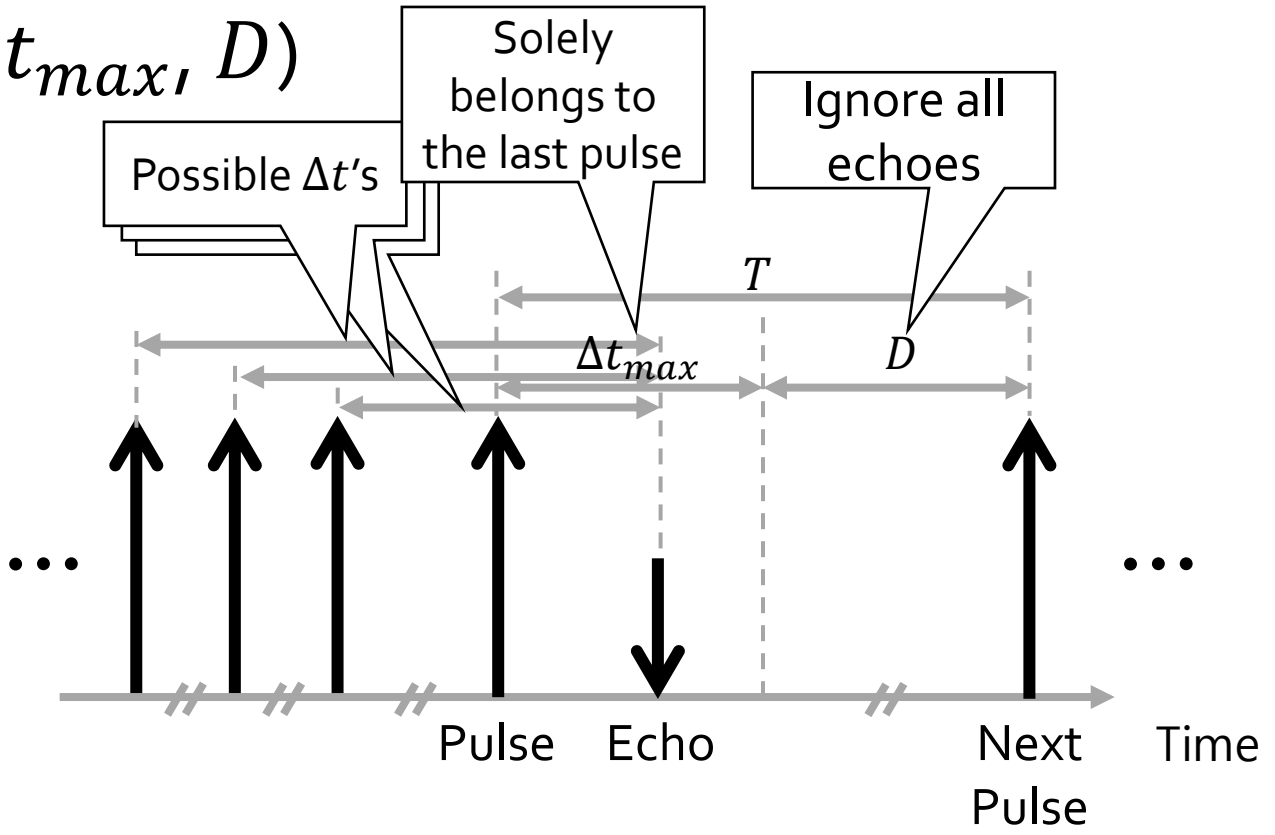
- Important parameters
  - Pulse repetition time (PRT, T)





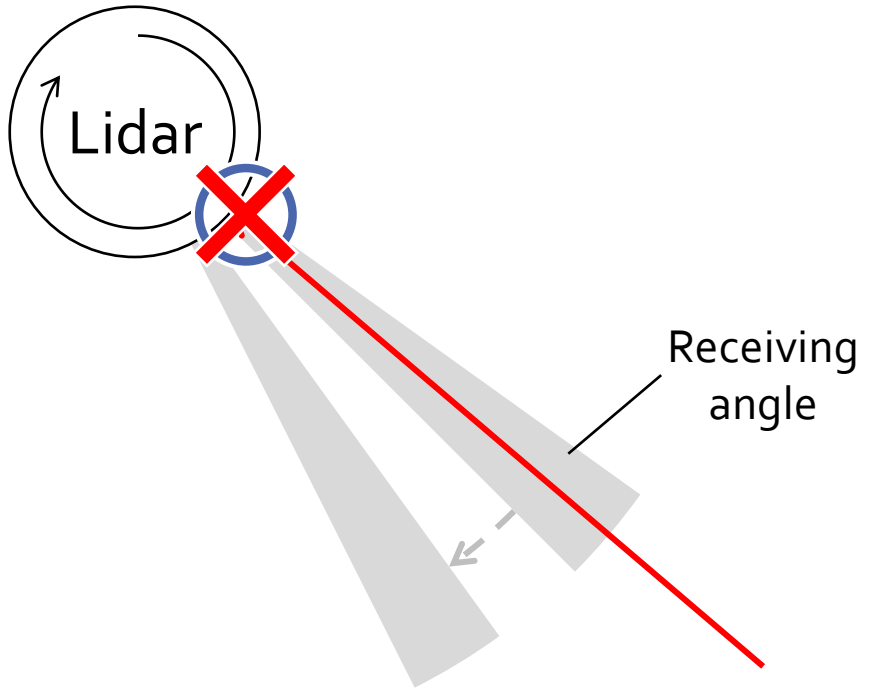
Lidar

- Important parameters
  - Pulse repetition time (PRT, T)
  - Receiving time / dead time (Δt_{max}, D)
    - To limit the ambiguity
    - Lidar range l_{max} → $c\Delta t_{max}/2$



Lidar

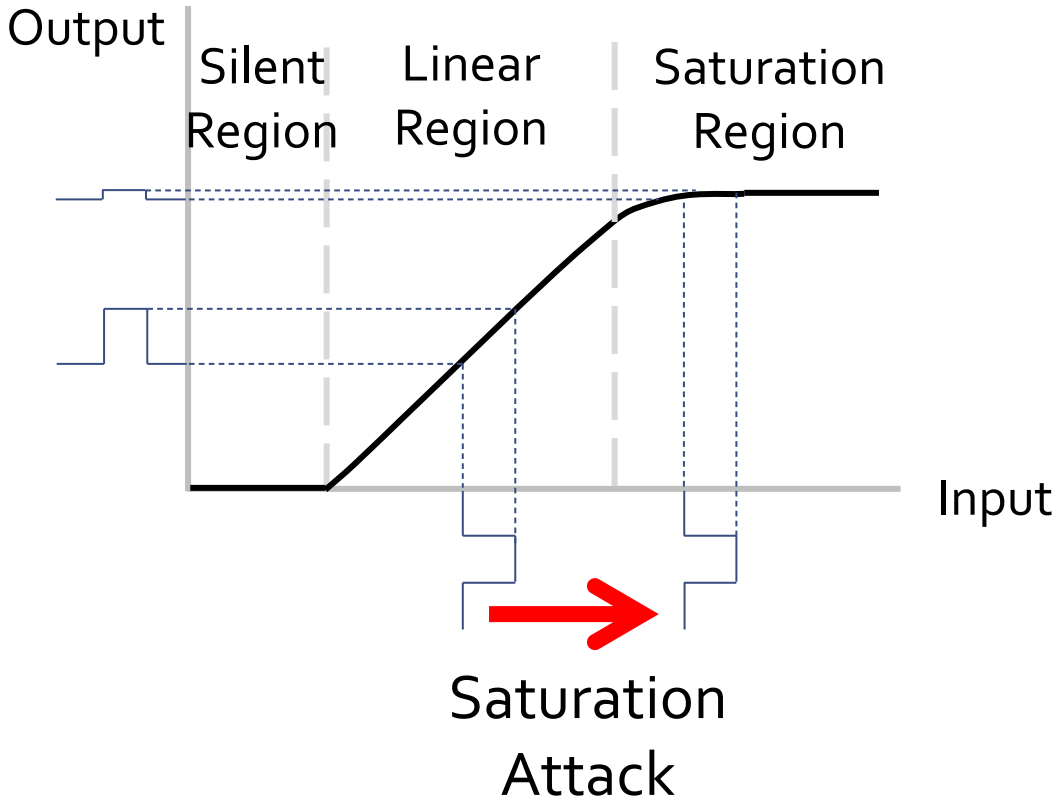
- Important parameters
  - Pulse repetition time (PRT, T)
  - Receiving time / dead time (Δt_{max}, D)
    - To limit the ambiguity
    - Lidar range $l_{max} \rightarrow c\Delta t_{max}/2$
  - Receiving angle
    - Angle of receiver aperture
    - If precisely calibrated,
      covering up to the farthest point is enough



Sensor Attacks

Sensor Saturating

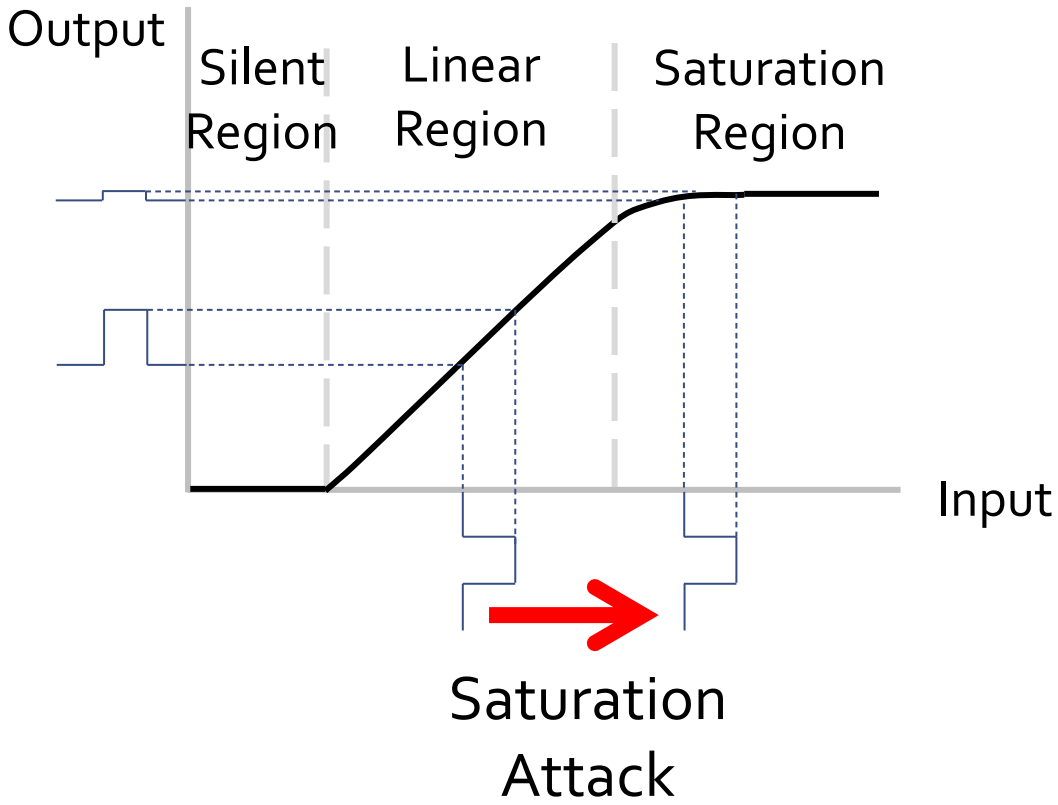
- Exploiting the transition curve



Sensor Attacks

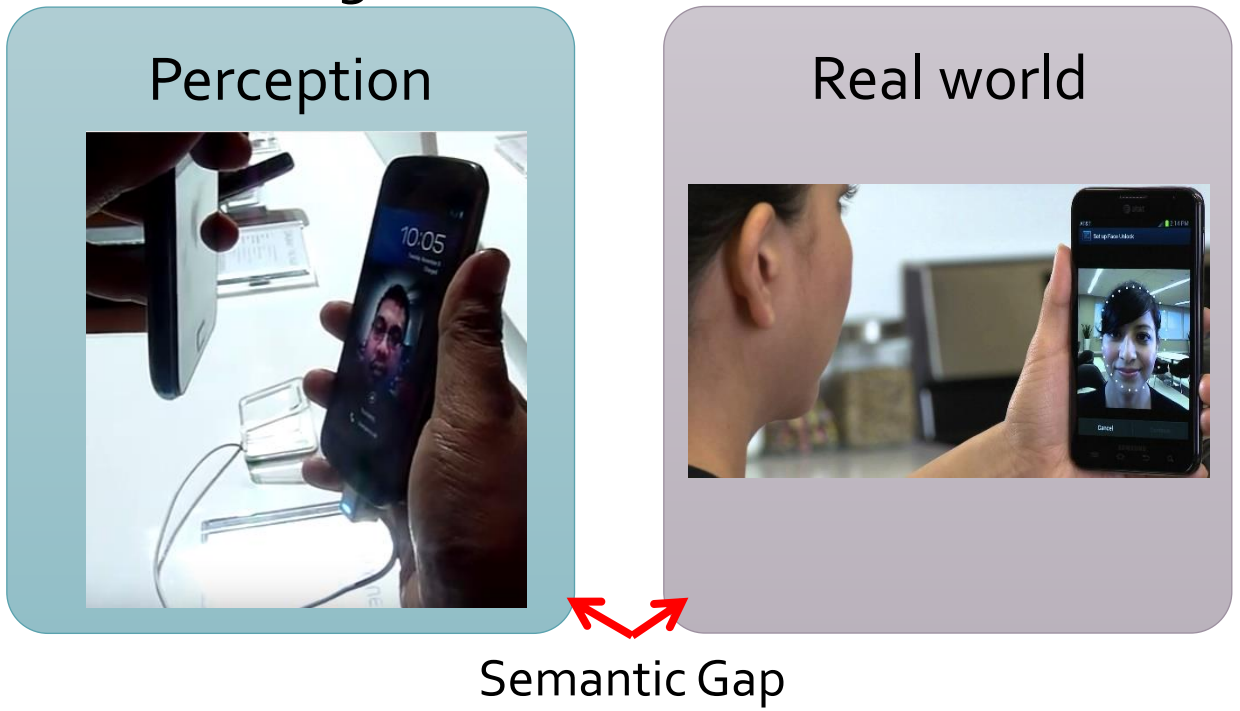
Sensor Saturating

- Exploiting the transition curve



Sensor Spoofing

- Deceiving sensors

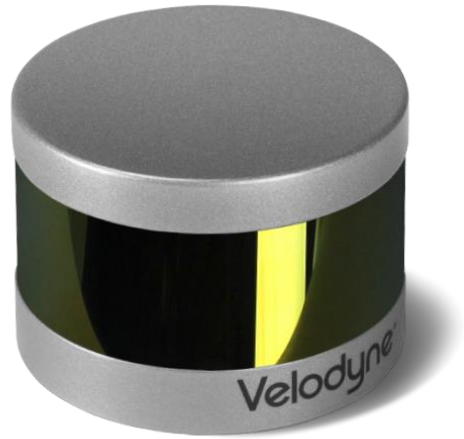


- Lidar spoofing: make a lidar see an object that does not exist in fact

Target System

- Velodyne's VLP-16
  - Outputs via Ethernet in UDP packets ➔ Used VeloView to visualize sensing outputs

Price	US$7,999
Laser wavelength	903nm
# of vertical layers	16
Update rate	5/10/20Hz (configurable)
Range	100m
Field Of View	360° (hor.), -15°~15° (ver.)
Angular Resolution	0.1/0.2/0.4°(hor., depends on update rate), 2° (ver.)

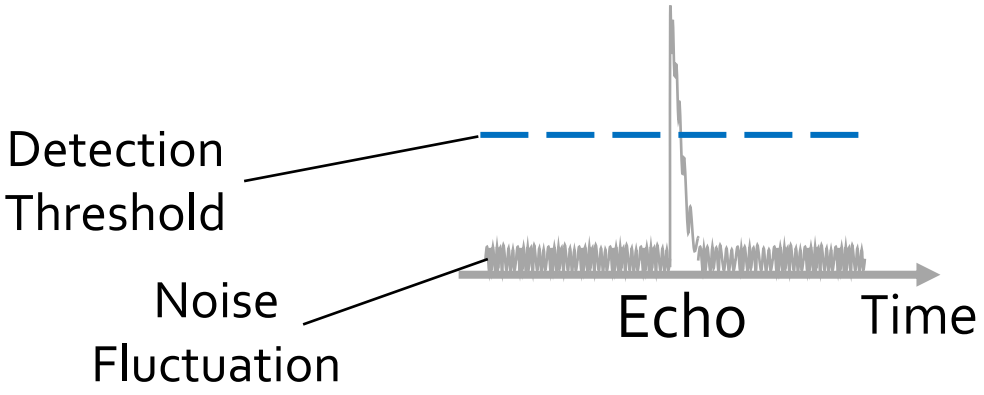


Saturation Attack

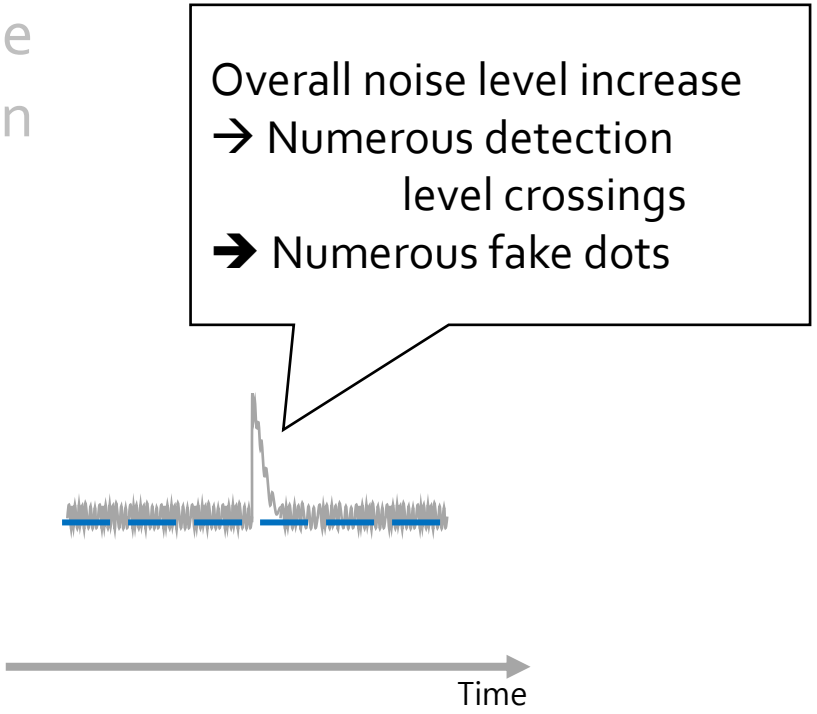
- Illuminating the target lidar with intense light source
  - Saturation → unable to sense incoming echoes → blinding
  - Strong attack because saturation itself is inavoidable
  - Detection is easy, but no COTS lidar has this function

Saturation Attack

- Illuminating the target lidar with intense light source
  - Saturation → unable to sense incoming echoes → blinding
  - Strong attack because saturation itself is inavoidable
  - Detection is easy, but no COTS lidar has this function
- Effect and cause speculation
  - Weak light injection → numerous fake dots



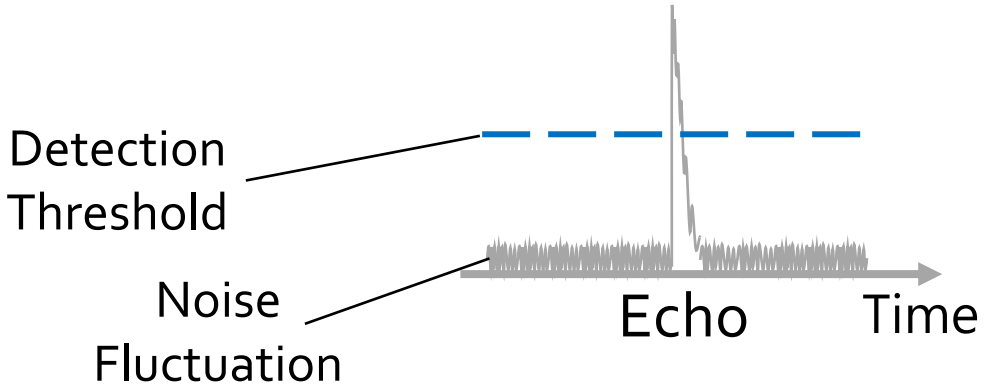
Exposure to weak light source



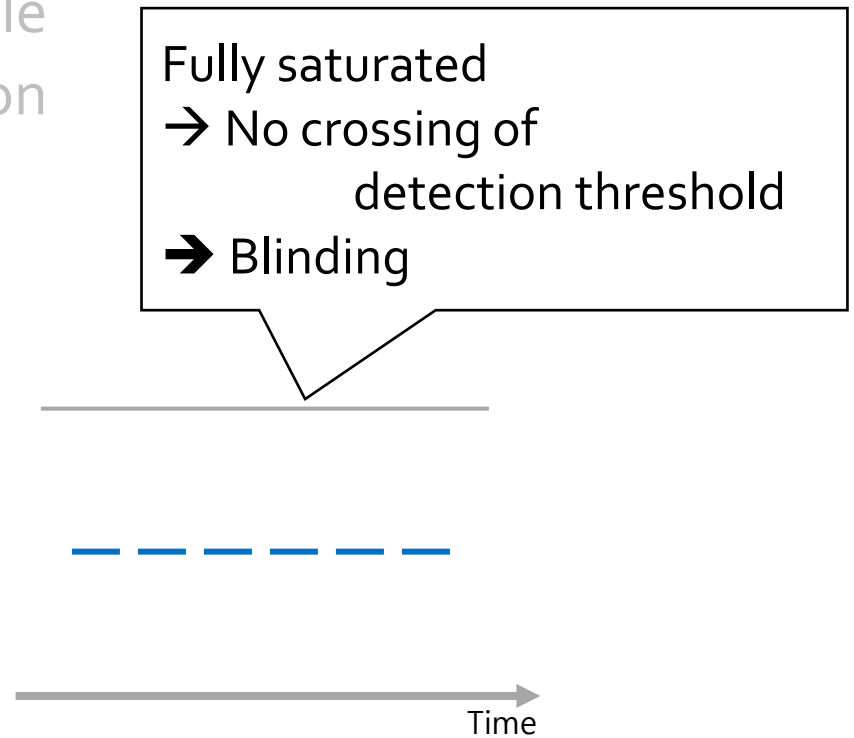

Lidar Exposure to
Weak Light Source

Saturation Attack

- Illuminating the target lidar with intense light source
  - Saturation → unable to sense incoming echoes → blinding
  - Strong attack because saturation itself is inavoidable
  - Detection is easy, but no COTS lidar has this function
- **Effect and cause speculation**
  - Weak light injection → numerous fake dots
  - Strong light injection → blinding of a section



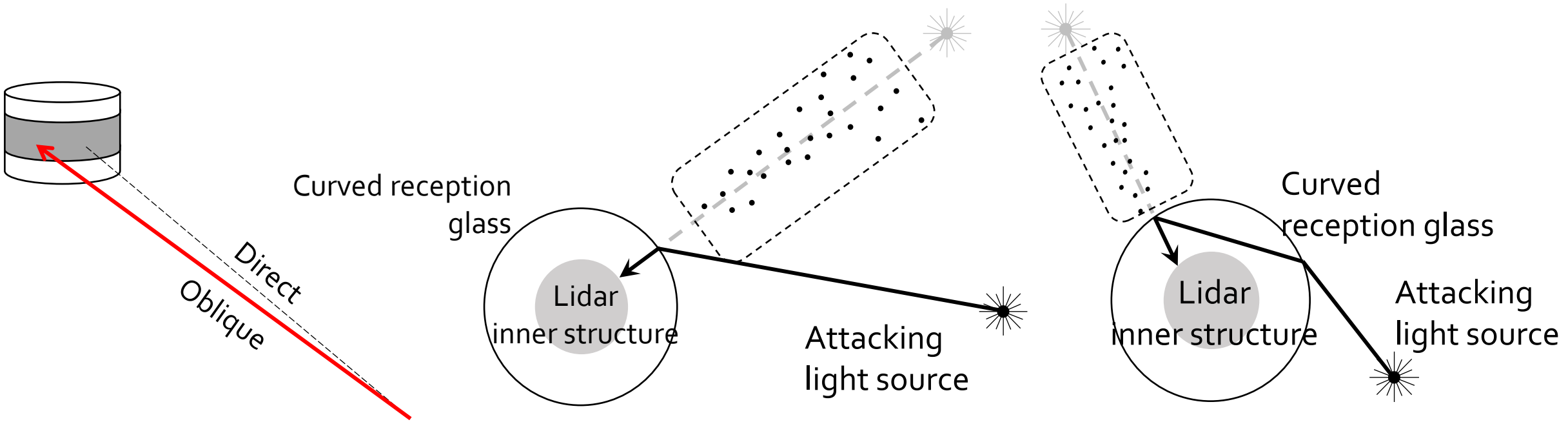
Exposure to Strong light source




Lidar Exposure to
Strong Light Source

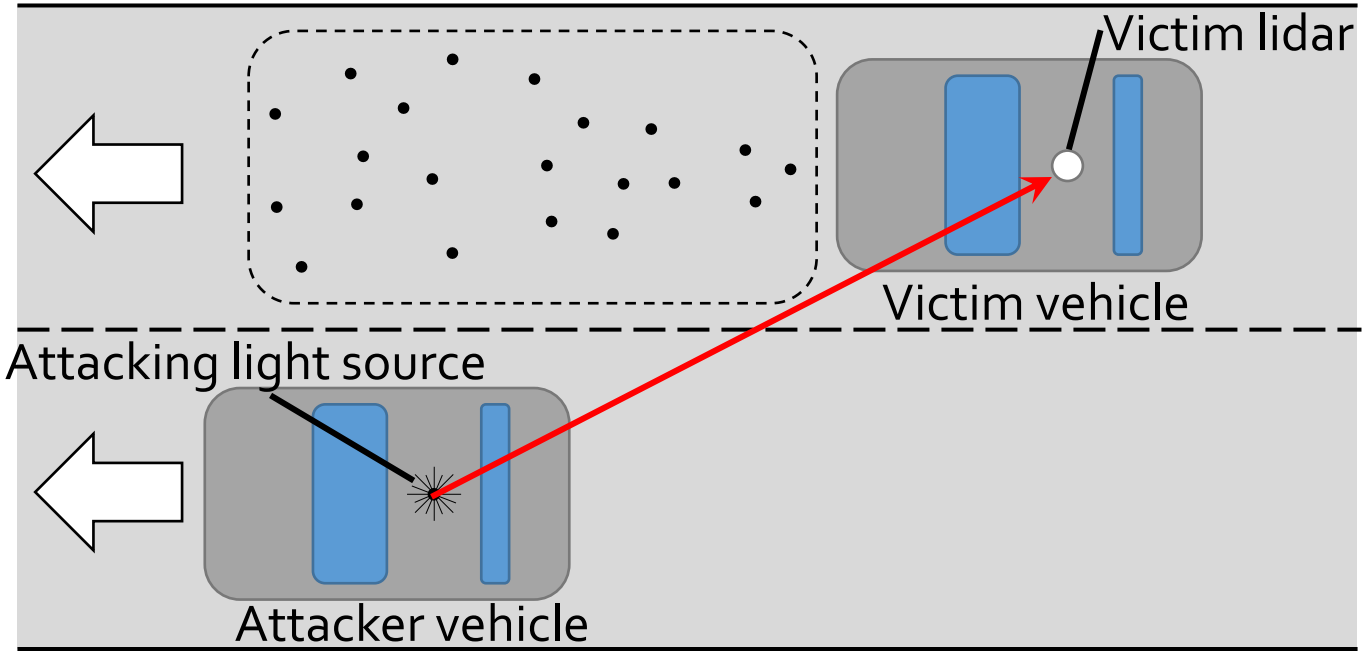
Saturation Attack

- Adverse effect of curved reception glass
  - Obliquely illuminating VLP-16
    ➔ fake dots not in the direction of the attacking light



Saturation Attack

- Adverse effect of curved reception glass
  - Obliquely illuminating VLP-16
    ➔ fake dots not in the direction of the attacking light
  - Other lidars also have curved glass (e.g. HDL-32E, LUX mini, M8)



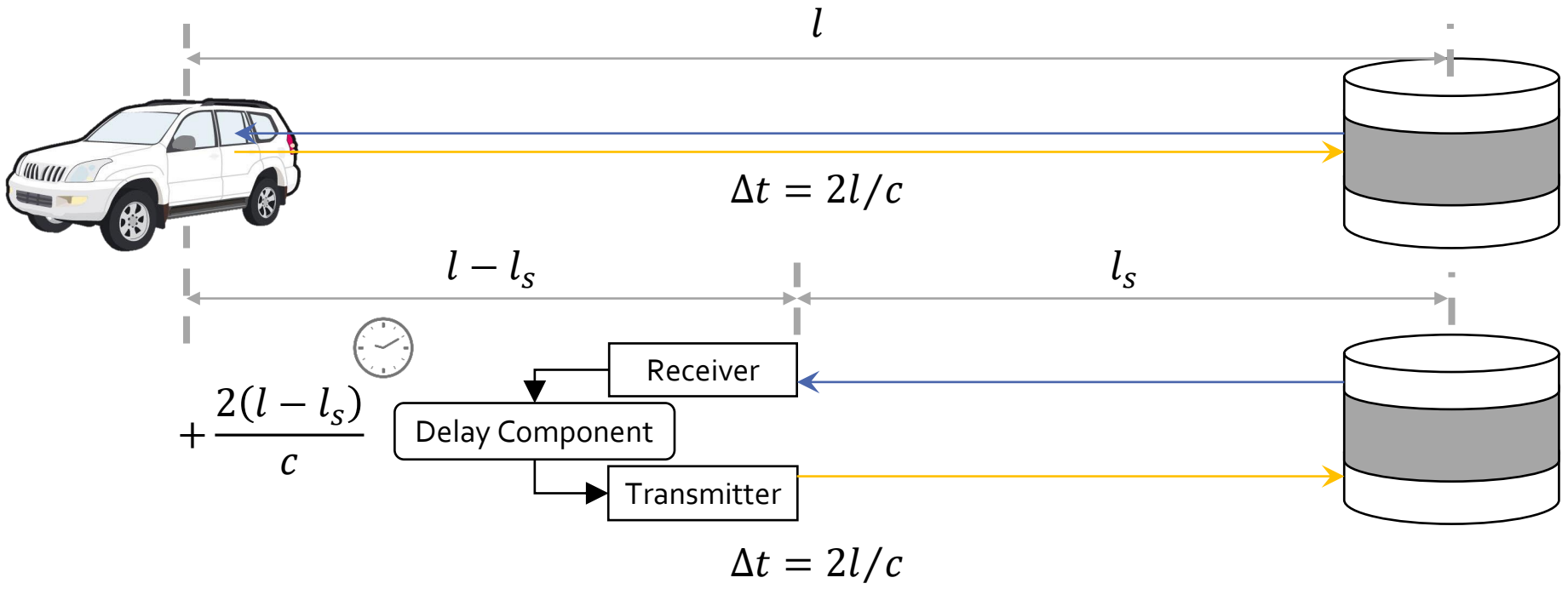
Lidar Obliquely Exposed to Strong Light Source

Saturation Attack

- Stealthy against human since IR laser is invisible,
- For relatively weak light source,
  - They can induce numerous fake dots
- For relatively strong light source,
  - They can make LiDAR completely blind
- By the design of lidar (curved reception glass),
  - They can induce fake dots in direction other than source

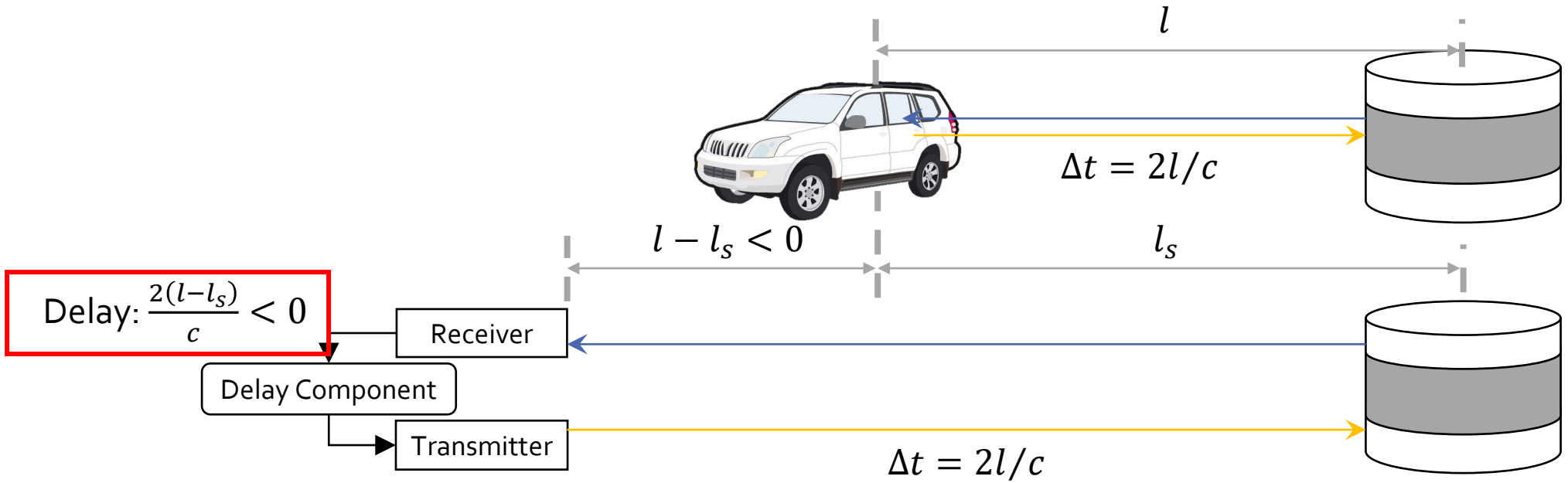
Spoofing by Relaying Attack – Ideal Attack Process

- Inducing a farther fake dot
  - Spoofed fake dots are less important than the spoofer itself



Spoofing by Relaying Attack – Ideal Attack Process

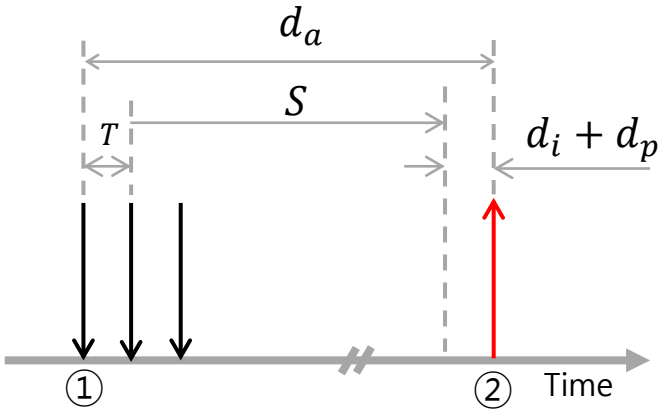
- Why we cannot induce closer fake dots with this model
  - Negative delay required → impossible

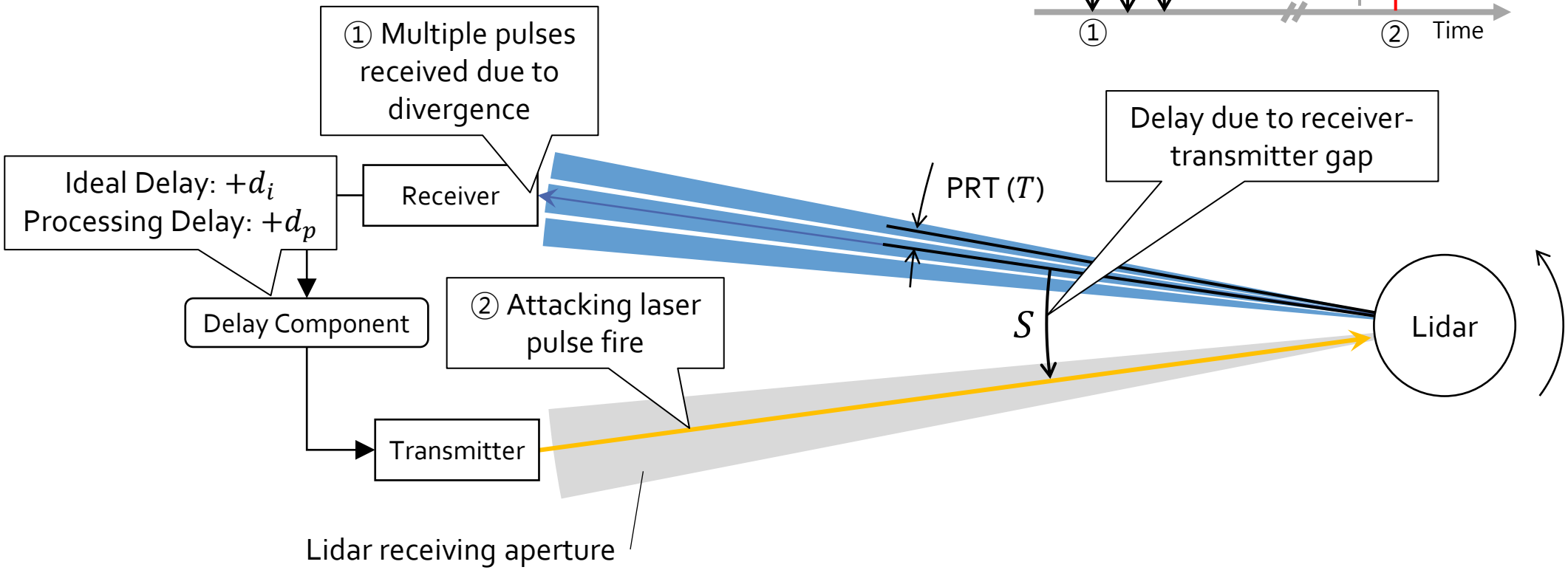


Spoofing by Relaying Attack – Actual Attack Process

◆Difference from the ideal case

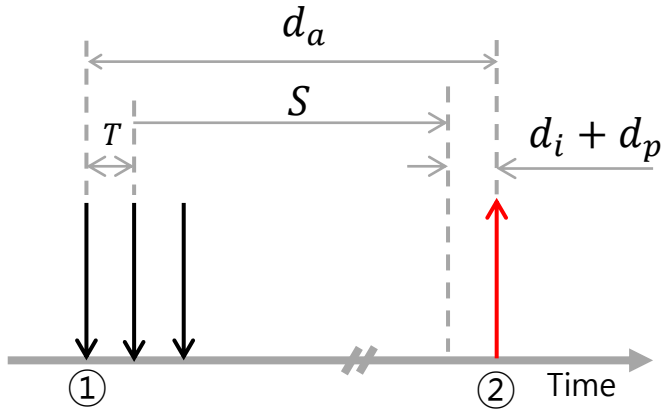
- Laser beam diverges
- Receiver-transmitter gap





Spoofing by Relaying Attack – Actual Attack Process

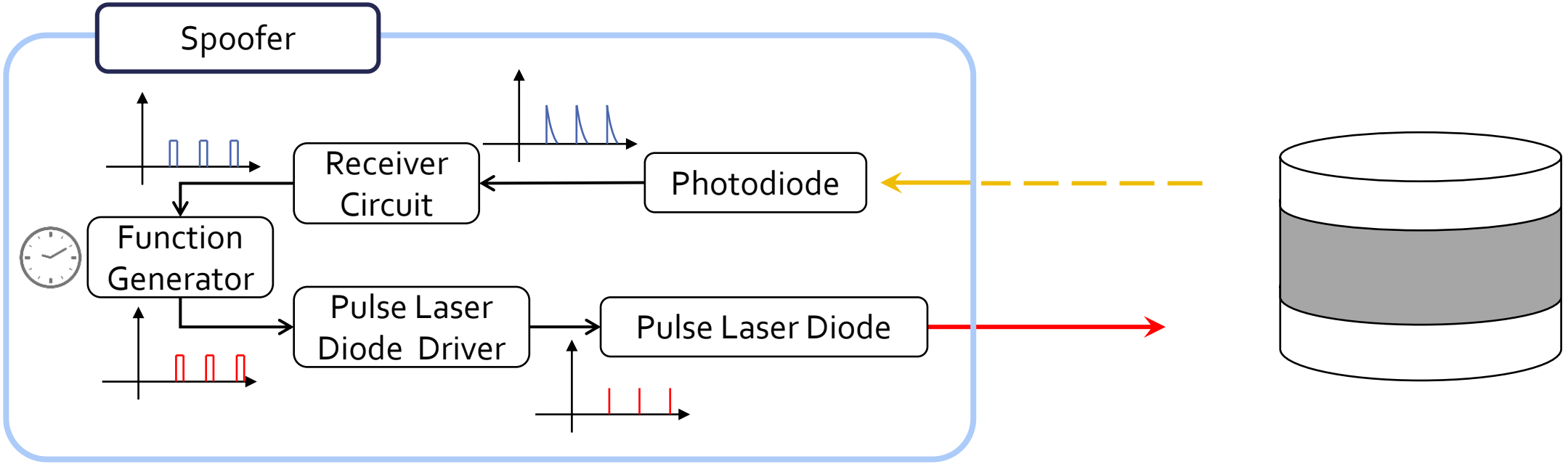
- Difference from the ideal case
  - Laser beam diverges
  - Receiver-transmitter gap



- Why this makes closer fake dots possible
  - $d_a(total\ delay) = d_i + nT + S + d_p$
  - Even if $d_i(ideal\ delay) < 0$ for closer fake dots, $d_a > 0$ ($\because T, S \gg |d_i|$)

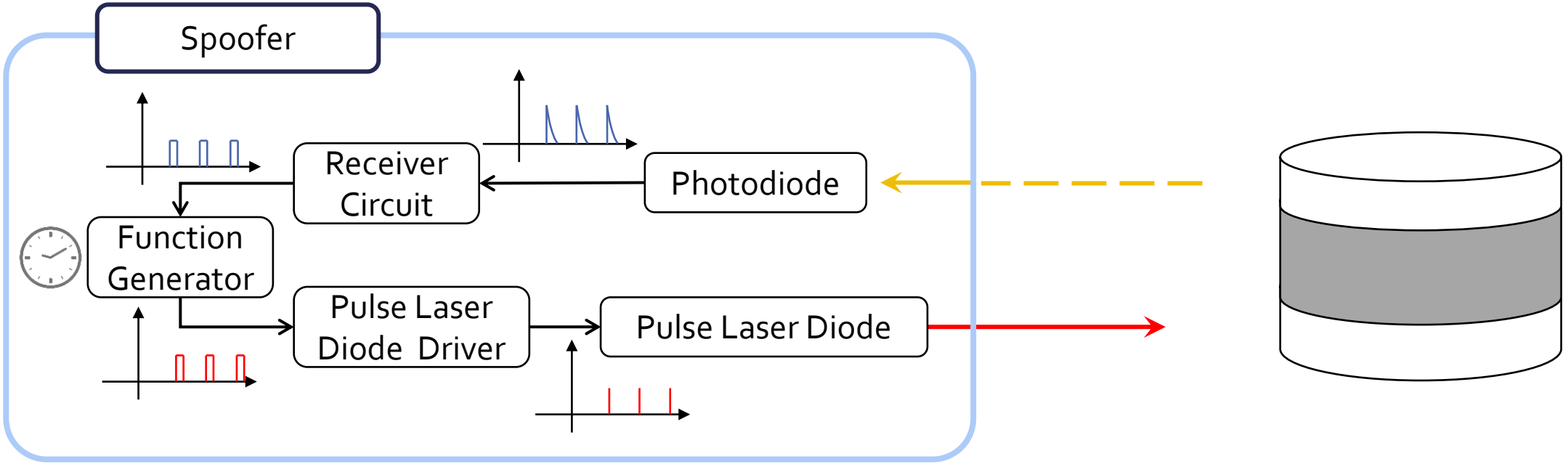
Spoofing by Relaying Attack – Experimental Setup

◆Lidar → PD → Receiver Circuit → Function Generator → PLD driver → PLD



Spoofing by Relaying Attack – Experimental Setup

◆Lidar → PD → Receiver Circuit → Function Generator → PLD driver → PLD



◆Inducing closer fake dots

1. Induce farther dots
2. Reduce the delay in function generator
3. Observe closer dots

Lidar Spoofing of Fake Dots Closer Than Spoofer

Spoofing by Relaying Attack

- Stealthy against human since IR laser is invisible

- Inducing a farther fake dot
  - Mimic the process
  - Fire laser pulse after positive delay

- Inducing a closer fake dot
  - By the characteristic of lidar, making negative delay is possible

Possible Countermeasures and limitations

- Saturation
  - Minimizing receiving angle → reduce the size of affected region
  - Detection is easy
    - Multiple sensors + program to abandon compromised sensor output
    - Alarm, then going into fail-safe mode
  - However, cannot be prevented → none of above is an ultimate solution

Possible Countermeasures and limitations

- Saturation
  - Minimizing receiving angle → reduce the size of affected region
  - Detection is easy
    - Multiple sensors + program to abandon compromised sensor output
    - Alarm, then going into fail-safe mode
  - However, cannot be prevented → none of above is an ultimate solution

- Spoofing
  - Minimizing receiving angle
  - Adding slight random perturbation to PRTs
    ∵ Random probing is hard to be adopted for current rotating lidars
  - However, induction of single, farther fake dot per spoofer is still possible

Conclusion

- Two types of attack against LiDAR; Saturation, Spoofing

- Saturation
  - Make numerous fake dots using weak light source
  - Make LiDAR completely blind using strong light source
  - Make fake dots in direction other than that of the source

- Spoofing
  - Induce closer fake dots

- Defensive measures exists, but not enough to fully trust LiDAR

Related works

Petit, Jonathan, et al. "**Remote attacks on automated v ehicles sensors: Experiments on camera and lidar**." Bla ck Hat Europe 11.2015 (2015): 995.

- Attack camera-based system and LiDAR
- They successfully blinded camera by emitting light into the camera
- Also, they showed relaying, and spoofing attack against LiDAR

Related works

Yan, Chen, Wenyuan Xu, and Jianhao Liu. "**Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle**." Def Con 24.8 (2016): 109.

- Attack the ‘eye’ of autonomous vehicles; MMR radar, ultrasonic sensor, cameras
- They showed jamming, spoofing attack on those sensors in Tesla model S

Follow-up works

Sun, Jiachen, et al. "**Towards robust lidar-based perception in autonomous driving: General black-box adversarial sensor attack and countermeasures**." USENIX Security'20.

- Explore vulnerabilities of LiDAR-based perception layer
- With those vulnerability, they constructed black-box spoofing attack
- Suggested defense model CARLO, which detects spoofed data
- Connected sensor spoofing attack to AI model (perception layer)

Questions

Q: The attacks described in the paper seem unrealistic, it could be much easier for an attacker to use other methods to damage a car or create an accident. Do you think nowadays we could see “lidar attacks” ?

A: The strength of these attacks lies in the fact that they are stealthy. Other methods will have the same result but will be more easily traceable. Moreover, taking into consideration that one can induce fake dots in a different direction than the laser, it can become very difficult to define the source for example in a situation of heavy traffic (traffic jams, ...)

Questions

Q: Putting the cost aside, wouldn't it be much safer if autonomous vehicles use both lidar and vision? If not, what could be an attack for this?

A: I think it would be safer in terms of protection against attacks, since obviously to blind the autonomous car, the attacker would have to perform 2 simultaneous attacks. But this is still possible, as vision systems have also flaws as explained in this paper:

« Robust Physical-World Attacks on Deep Learning Visual Classification » Kevin Eykholt , Ivan Evtimov, Earlence Fernandes , Bo Li , Amir Rahmati , Chaowei Xiao , Atul Prakash , Tadayoshi Kohno , and Dawn Song, 2018

Questions

Q: Is there also a time limit for attack?

A: As long as the laser can inject light pulses into the Lidar field of view, there is no time limit.