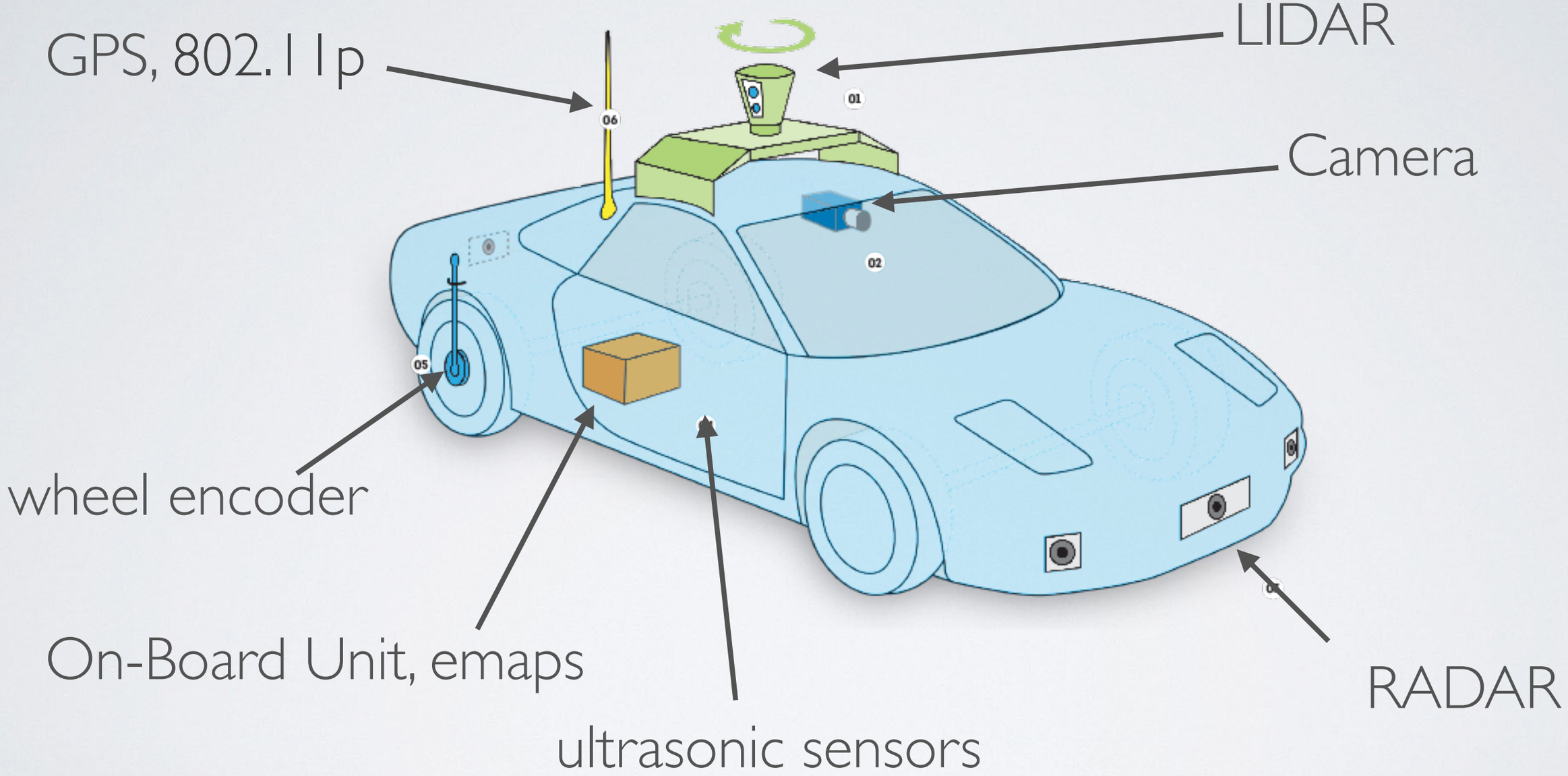
SELF-DRIVING AND CONNECTED CARS: FOOLING SENSORS AND TRACKING DRIVERS

Jonathan Petit

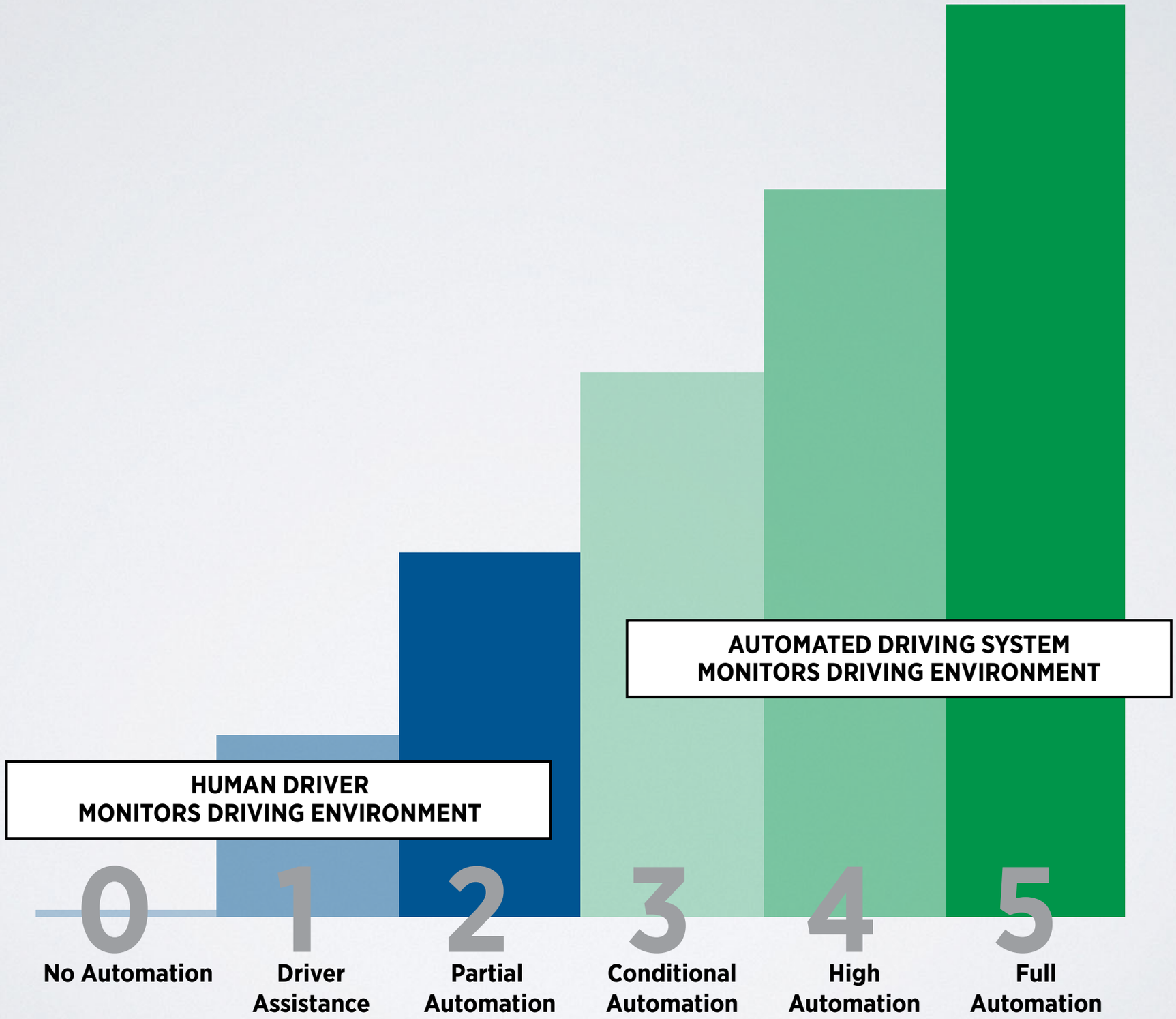
Security Innovation®
THE APPLICATION SECURITY COMPANY

UNIVERSITY OF TWENTE.

AUTOMATED/CONNECTED VEHICLE



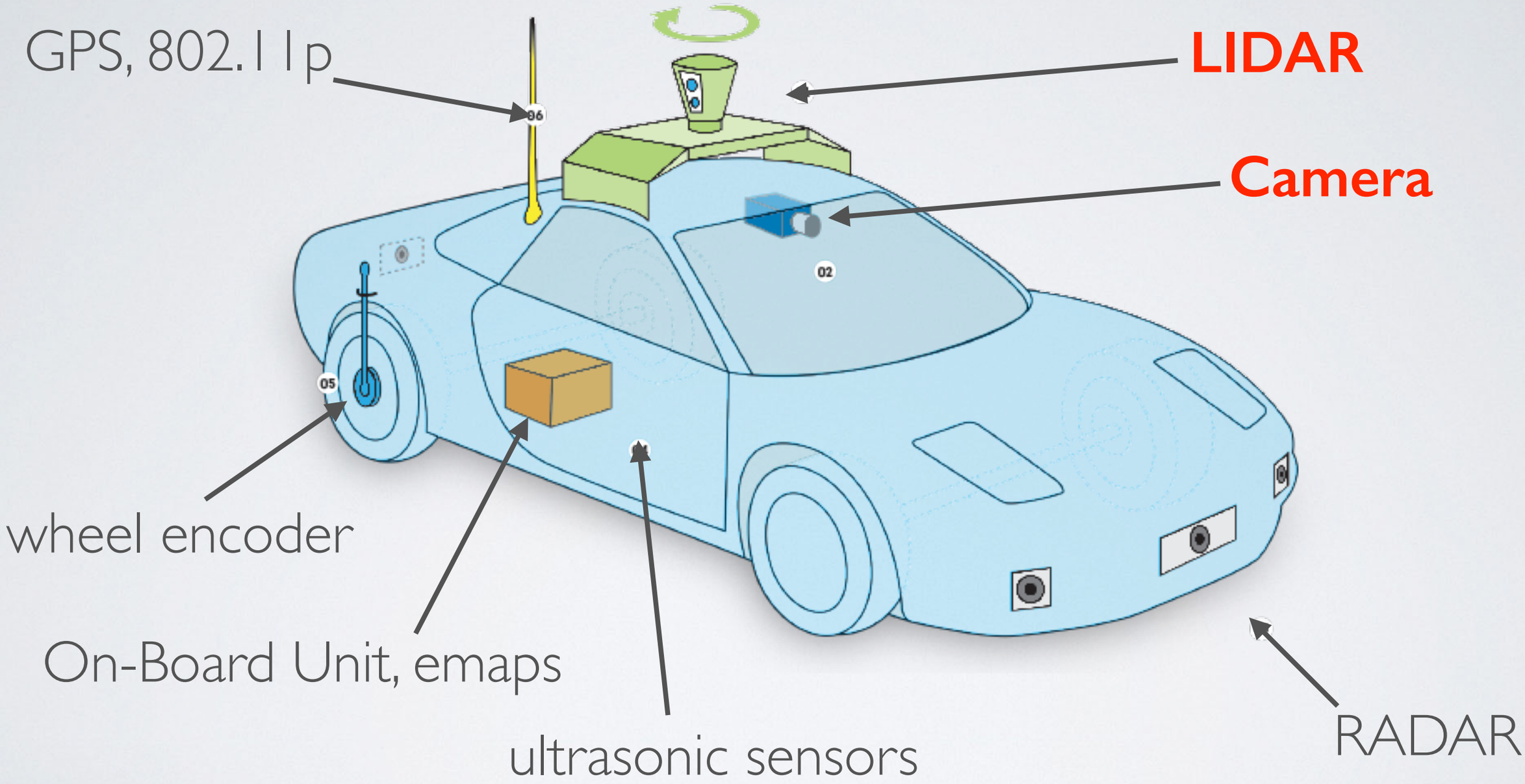
LEVELS OF DRIVING AUTOMATION (SAE J3016)



REMOTE ATTACKS ON AUTOMATED VEHICLES SENSORS: EXPERIMENTS ON CAMERA AND LIDAR

Jonathan Petit, Bas Stottelaar, Michael Feiri, Frank Kargl

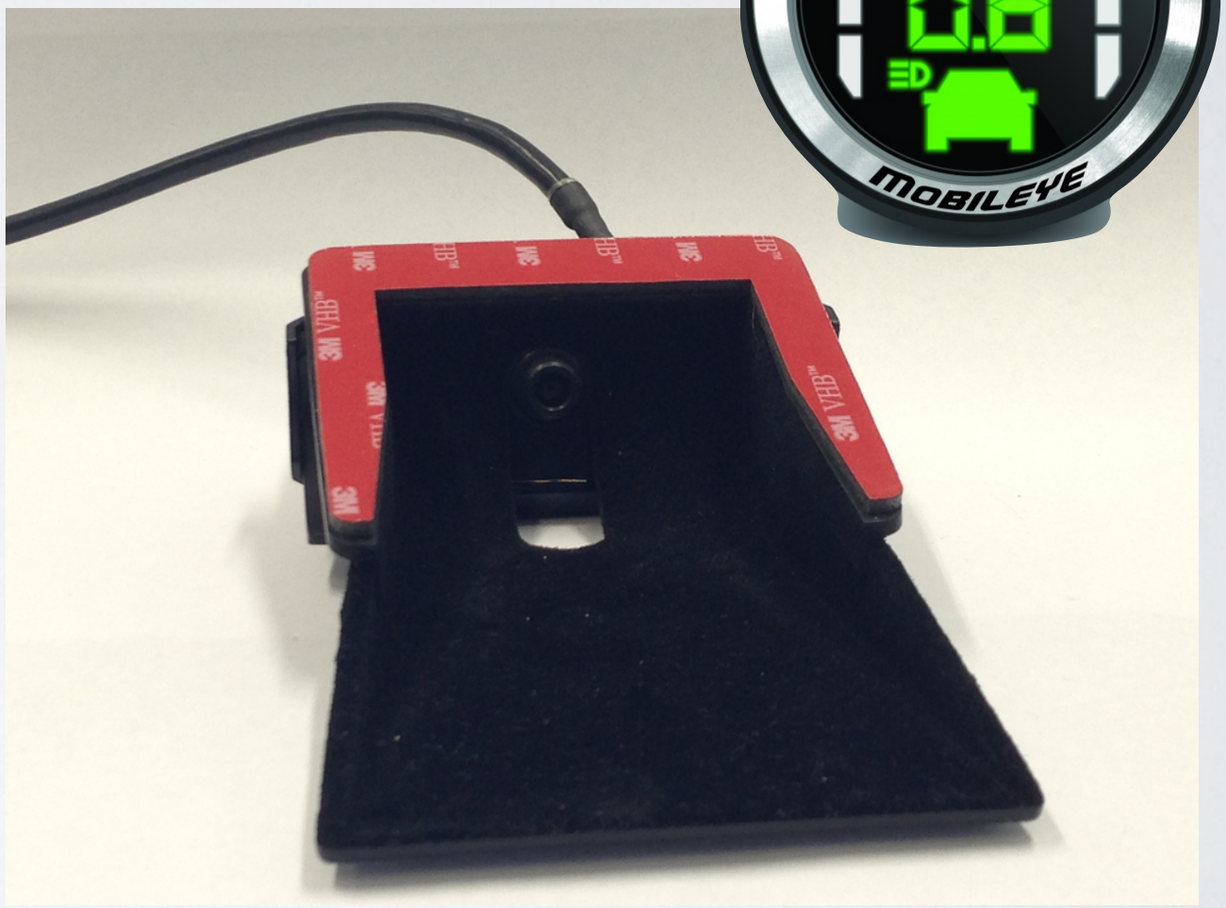
ATTACKING AUTONOMOUS VEHICLE SENSORS



CAMERA

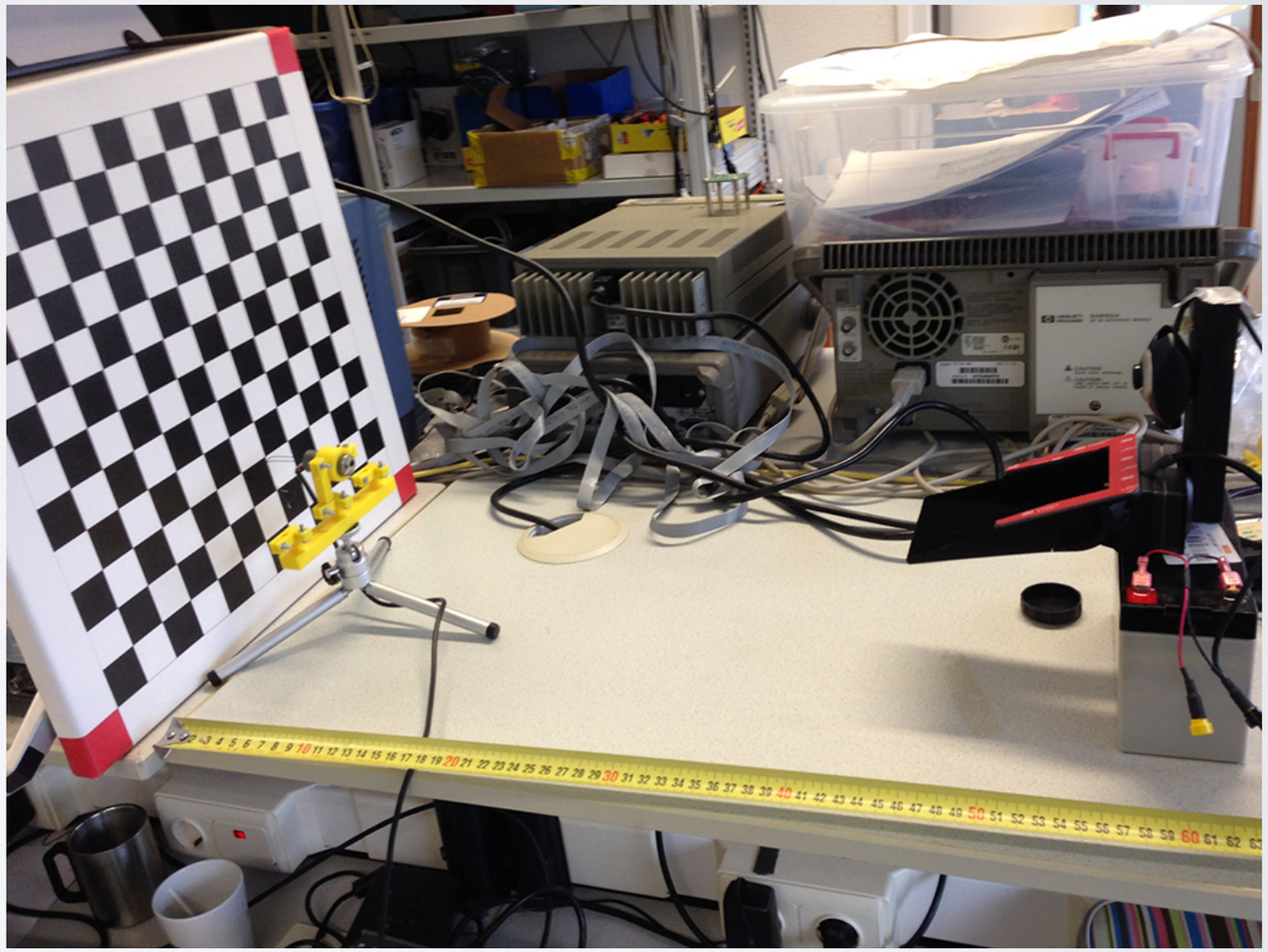
- MobilEye C2-270 (Thanks to V-TRON)

- Features:
  - Lane departure
  - Rear collision alert
  - Pedestrian alert



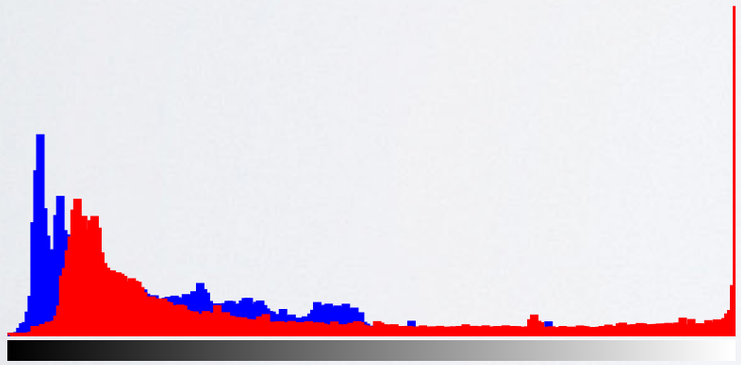
ATTACKING CAMERA

- Attacks:
  - Jamming
  - Blinding
  - Scenery attack
- Equipments:
  - Light sources (LED)
  - Laser
  - Screen

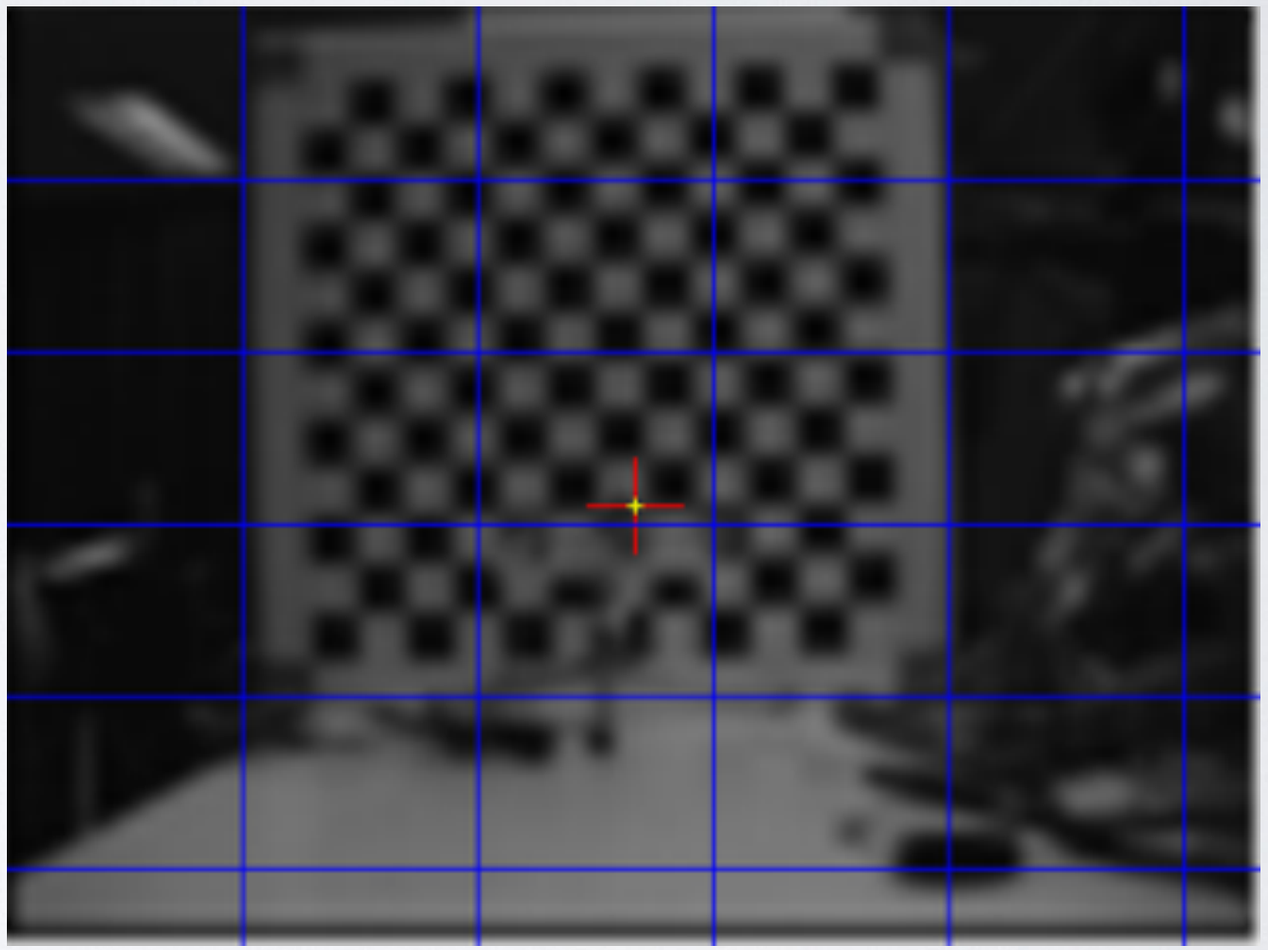


ATTACKING CAMERA - SENSITIVITY

- Ledsee **650 nm** diode point laser with focusable lens.
- Max. output: 5 mW.
- Distance: 1m

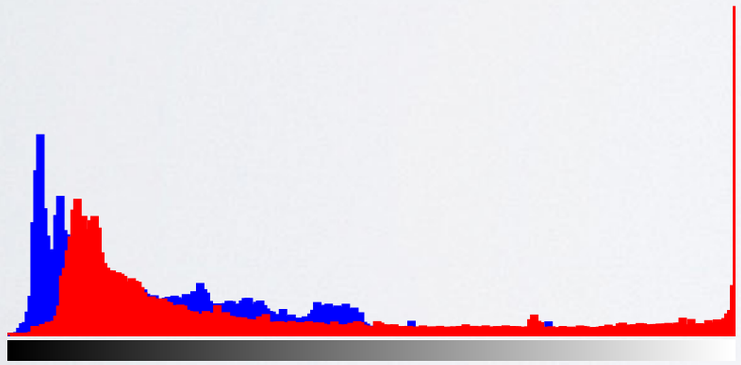


Tonal distribution

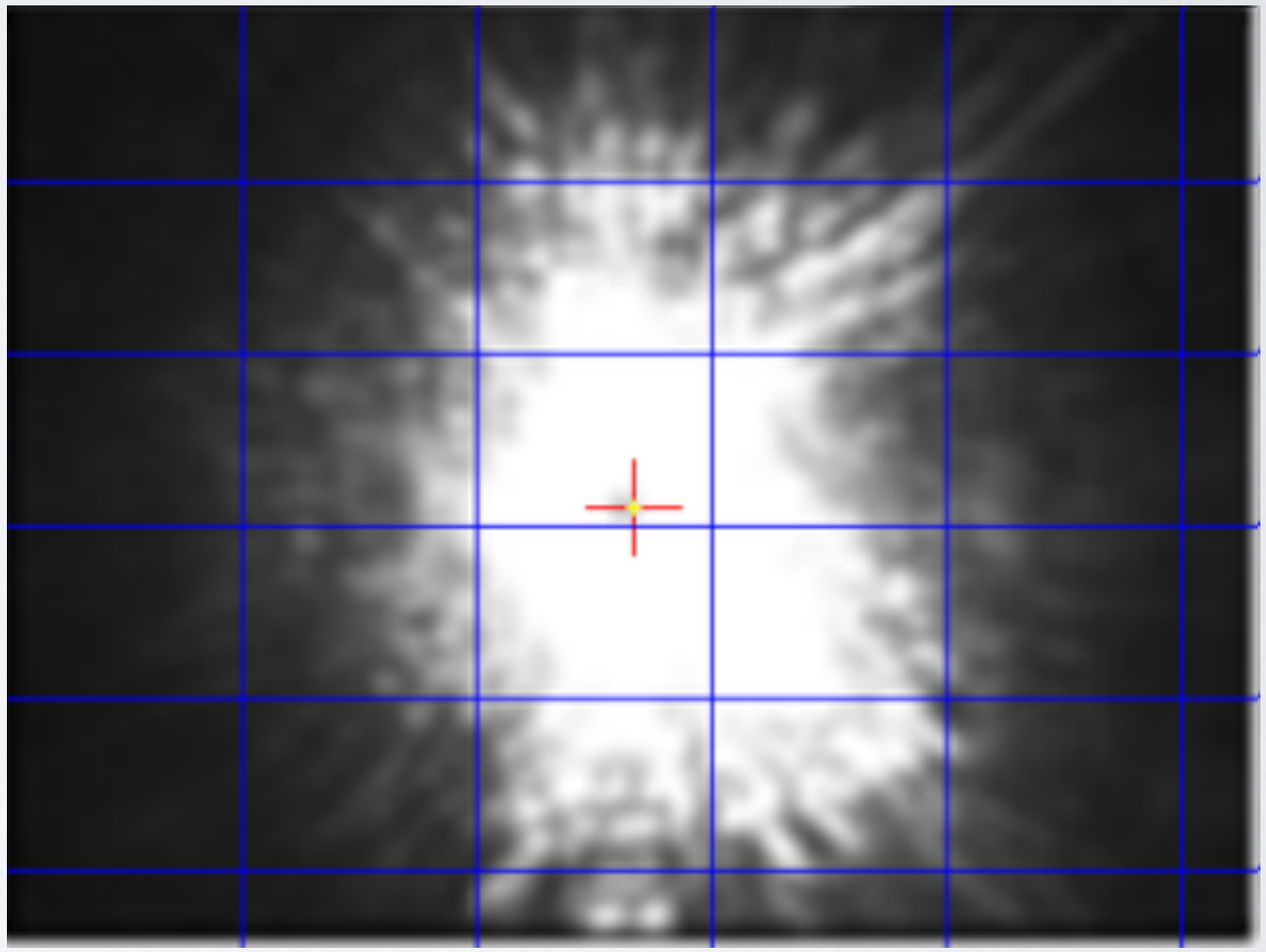


ATTACKING CAMERA - SENSITIVITY

- Ledsee **650 nm** diode point laser with focusable lens.
- Max. output: 5 mW.
- Distance: 1m

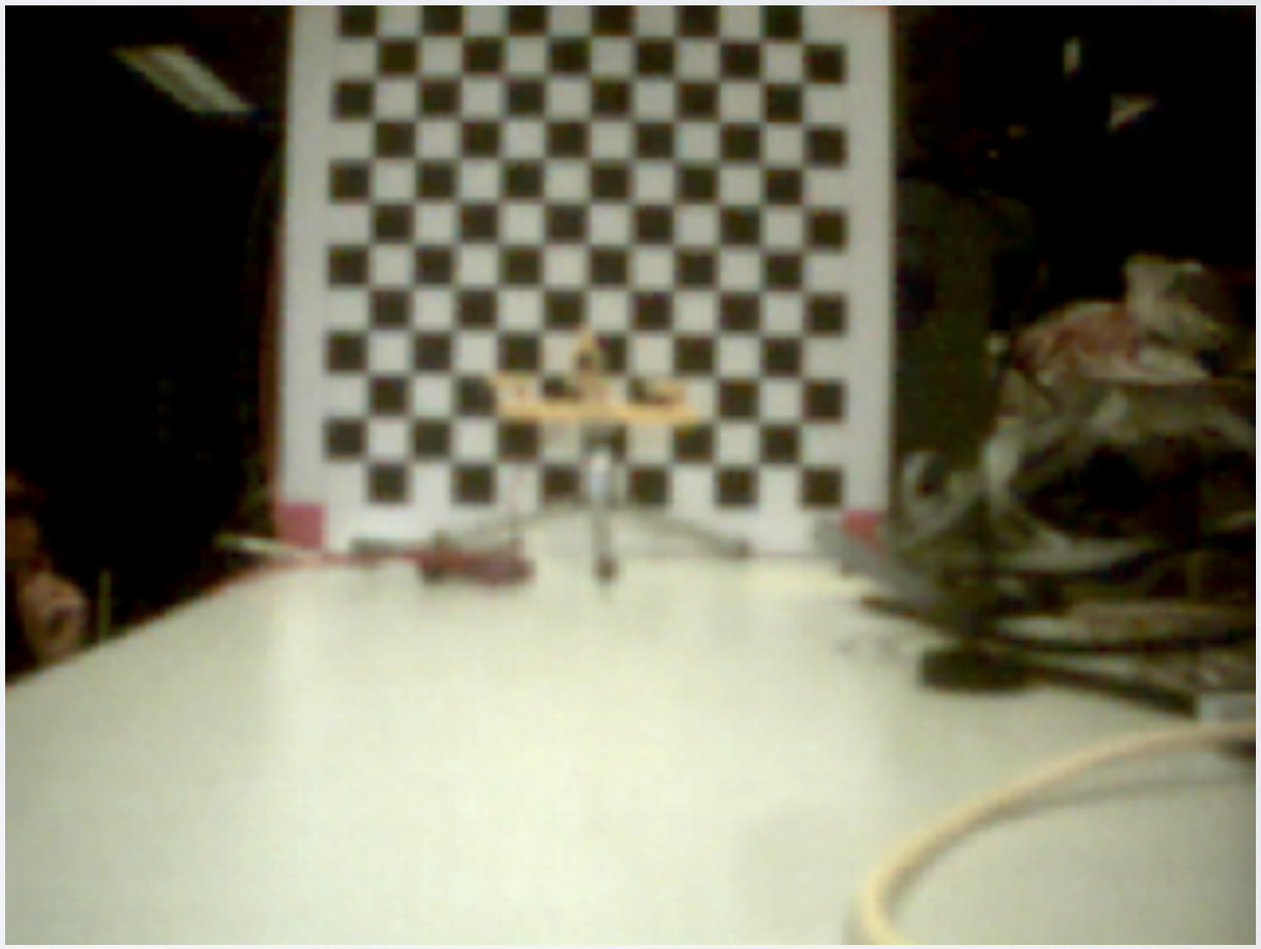


Tonal distribution



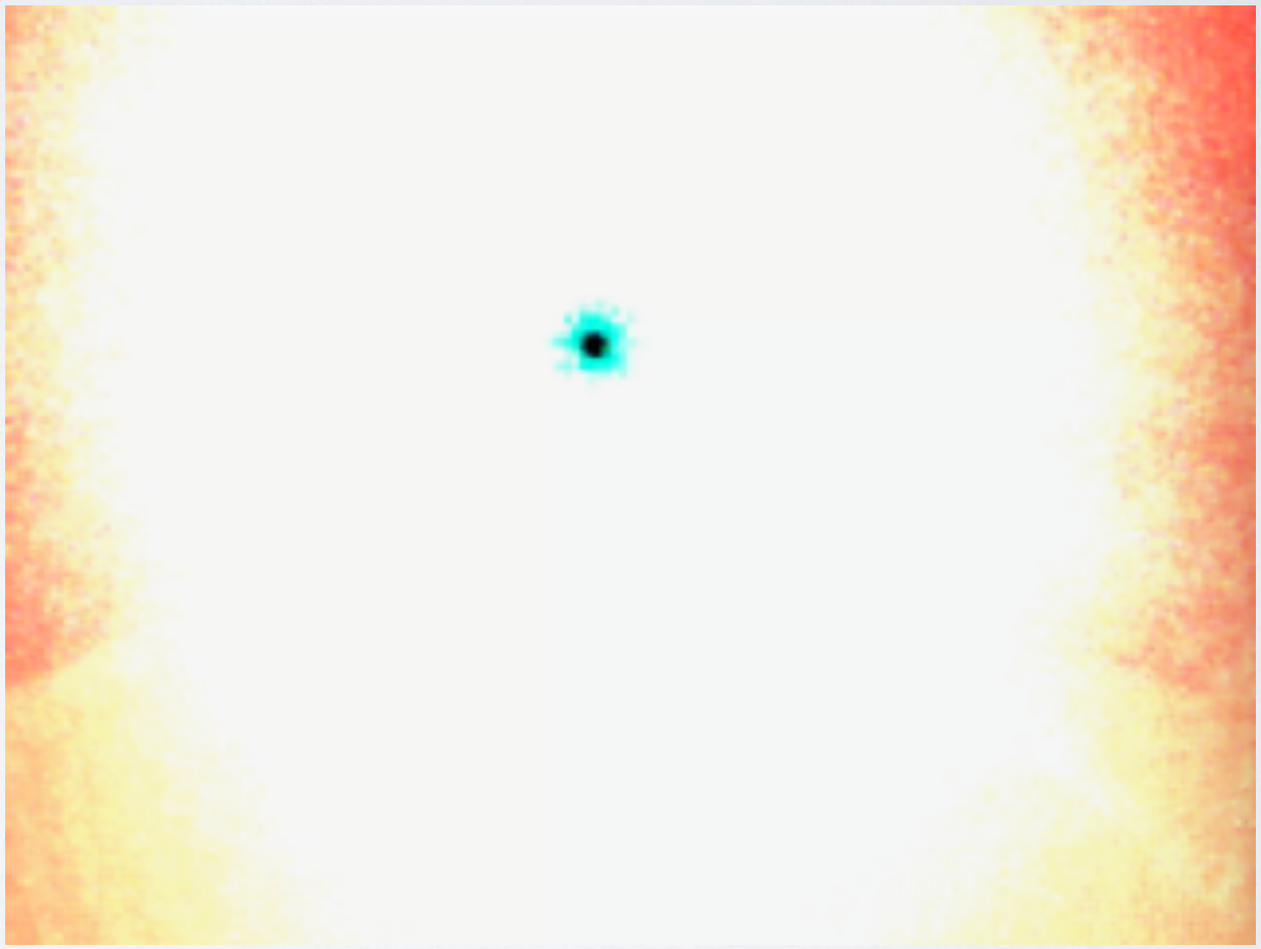
ATTACKING WEBCAM - SENSITIVITY

- Laser 650nm, 1m



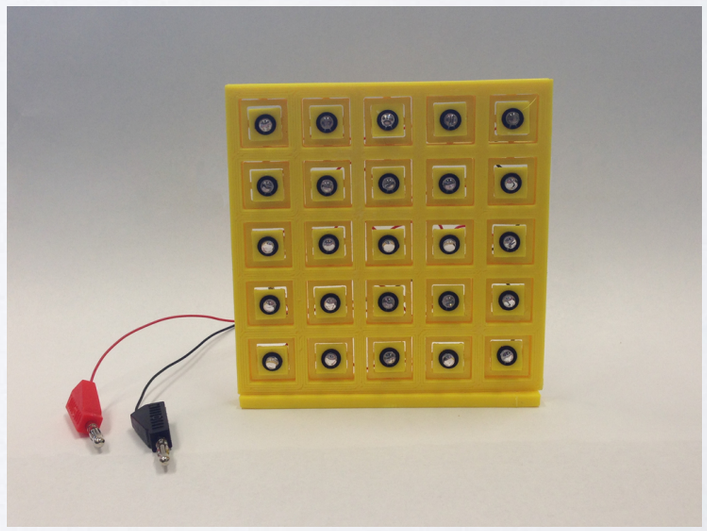
ATTACKING WEBCAM - SENSITIVITY

- Laser 650nm, 1m



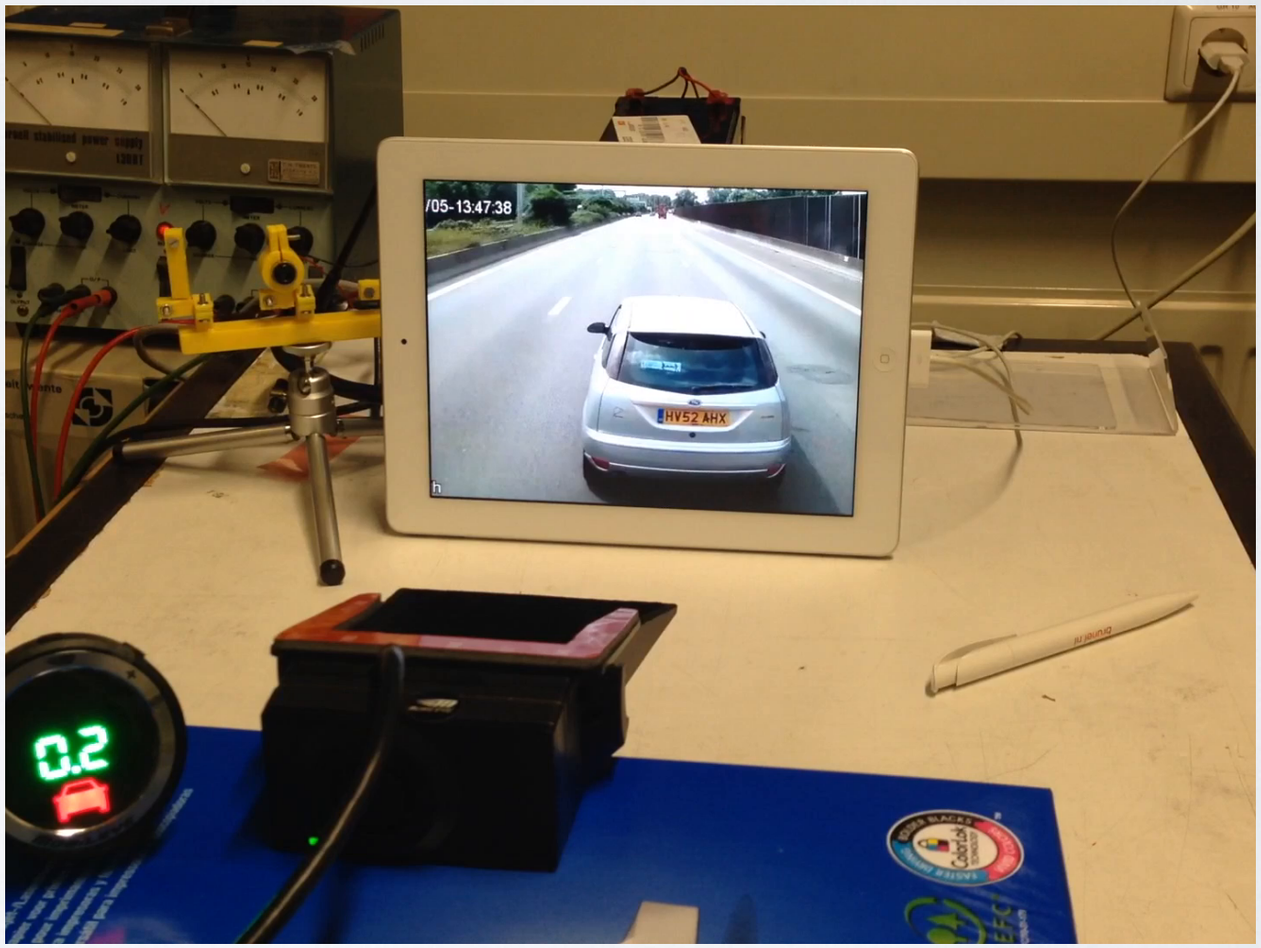
ATTACKING CAMERA - SENSITIVITY

- LED 850nm
- LED 860nm
- LED 875nm
- LED 880nm
- Laser 905nm
- LED 940nm
- **Matrix LED 940nm**



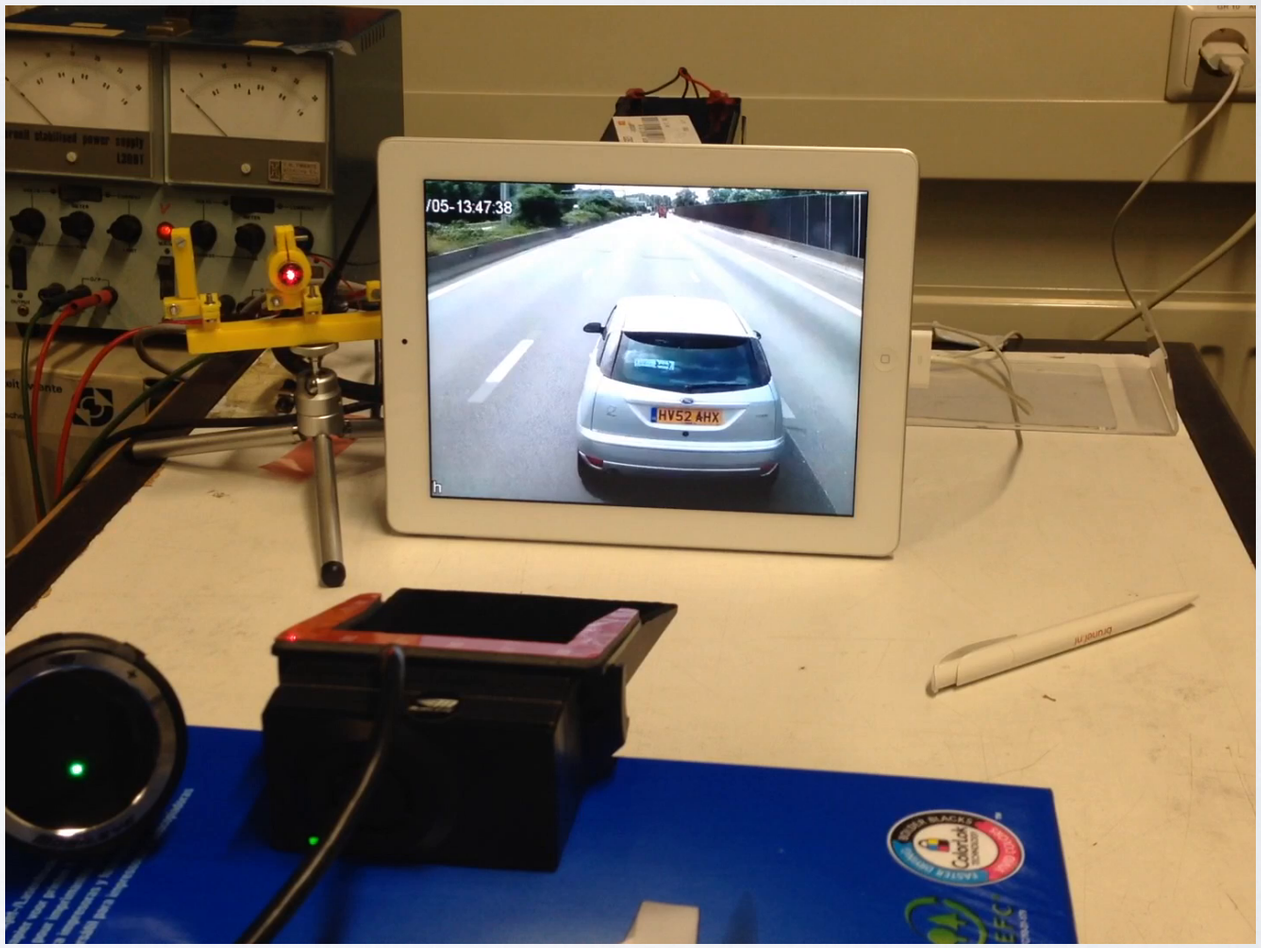
JAMMING CAMERA

- Laser 650nm



JAMMING CAMERA

- Laser 650nm



DAZZLER

DAZZLER

BeamQ

Home > Laser Dazzlers > Laser Weapon 300mW Green laser Dazzler

larger image

Laser Weapon 300mW Green laser Dazzler

$850.00

Add to Cart: 1

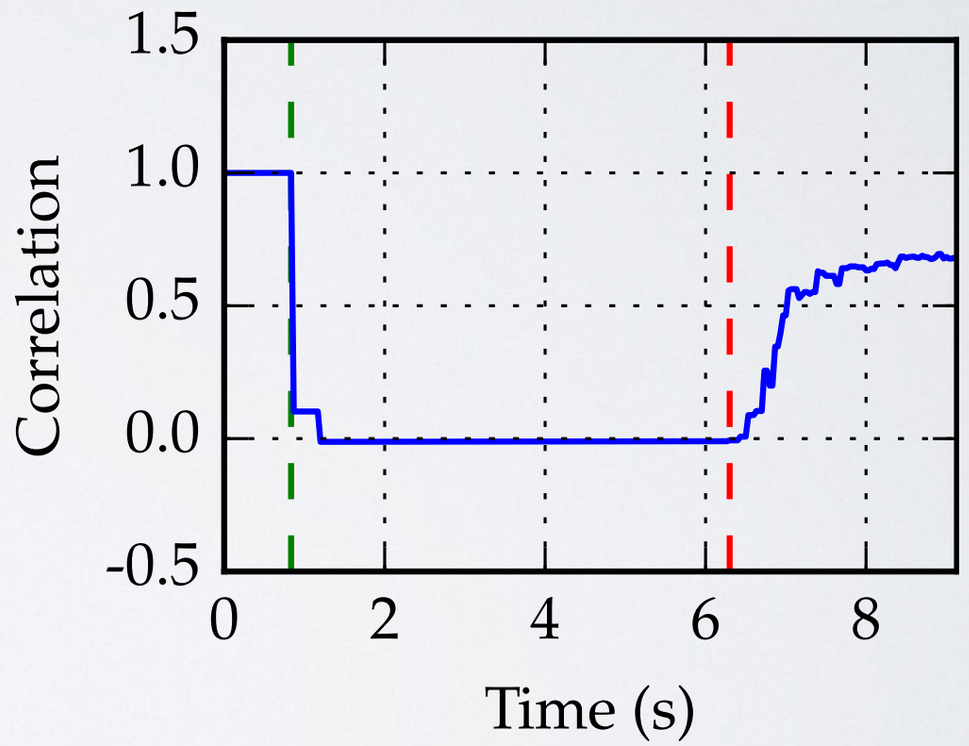
add this to my cart

100% IR FILTERED!
Intelligent Focusable Mechanism
Weapon mountable for versatility
Non-lethal crowd control and tactical area denial
CE/FDA/ROHS CERTIFIED

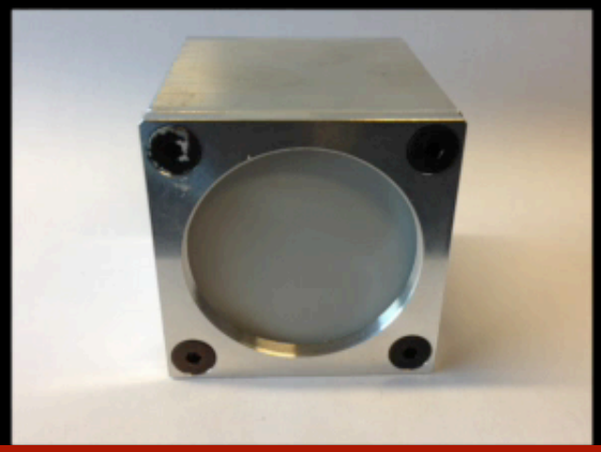
One Year's Guarantee!

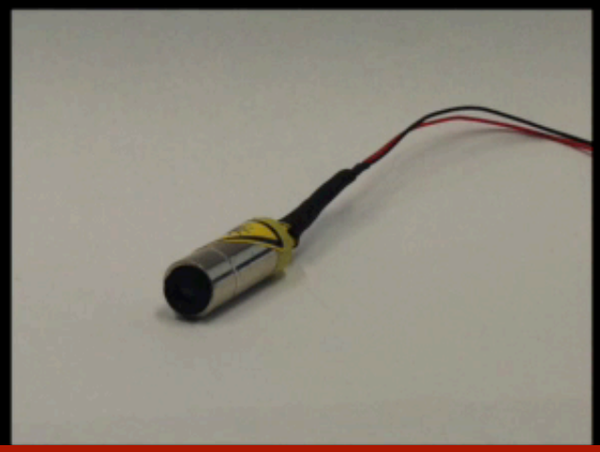
BLINDING CAMERA

- Use auto exposure
- “Time to recover”

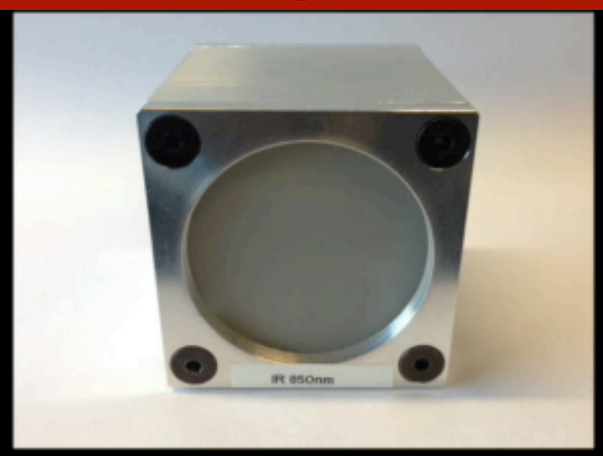


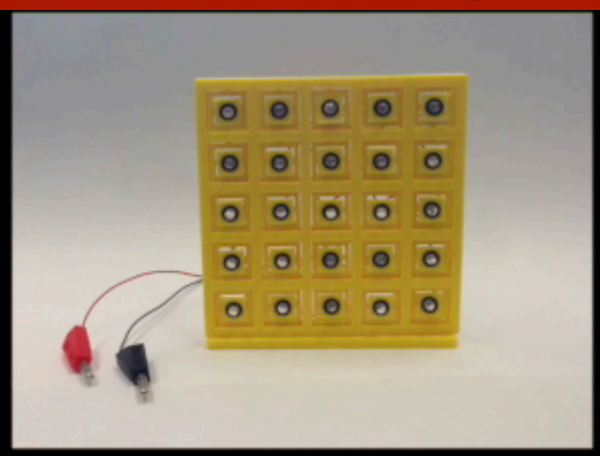
BLINDING CAMERA





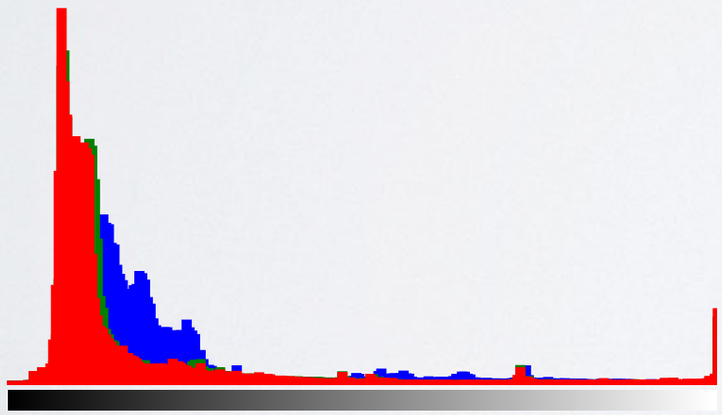
Video of different light sources and their impact on camera



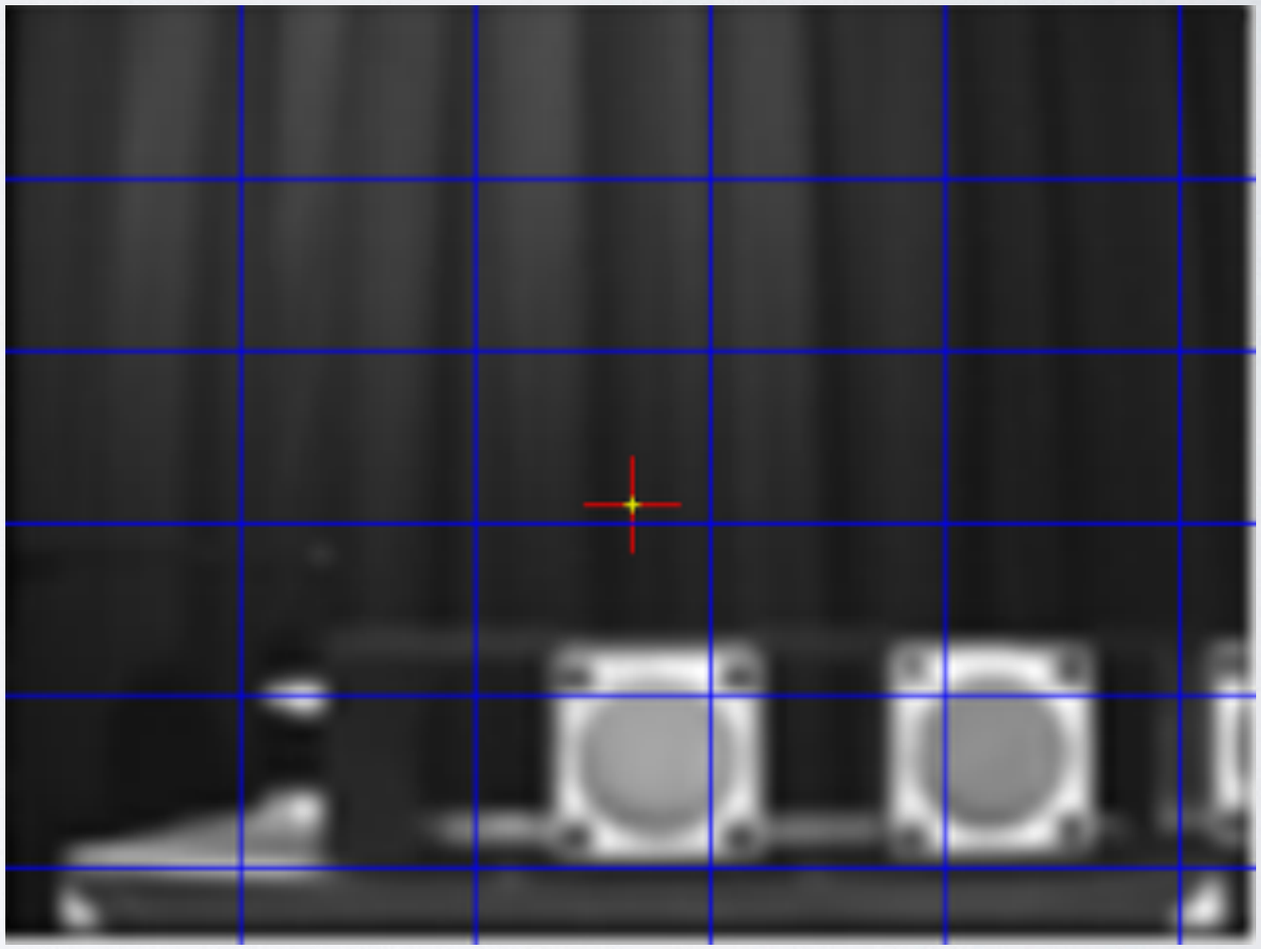


BLINDING CAMERA

- White spot, light, 50cm
- Affect background

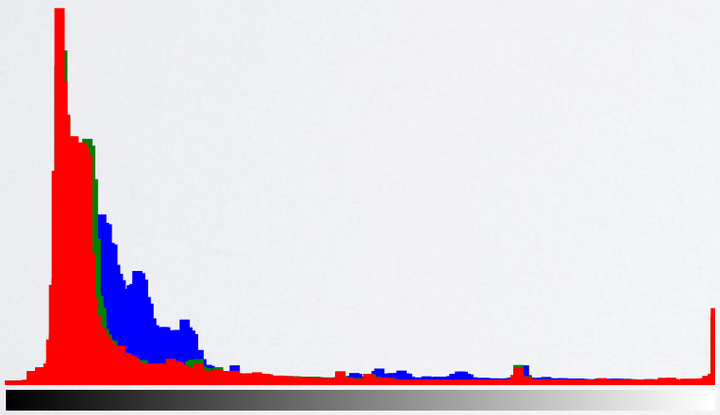


Tonal distribution

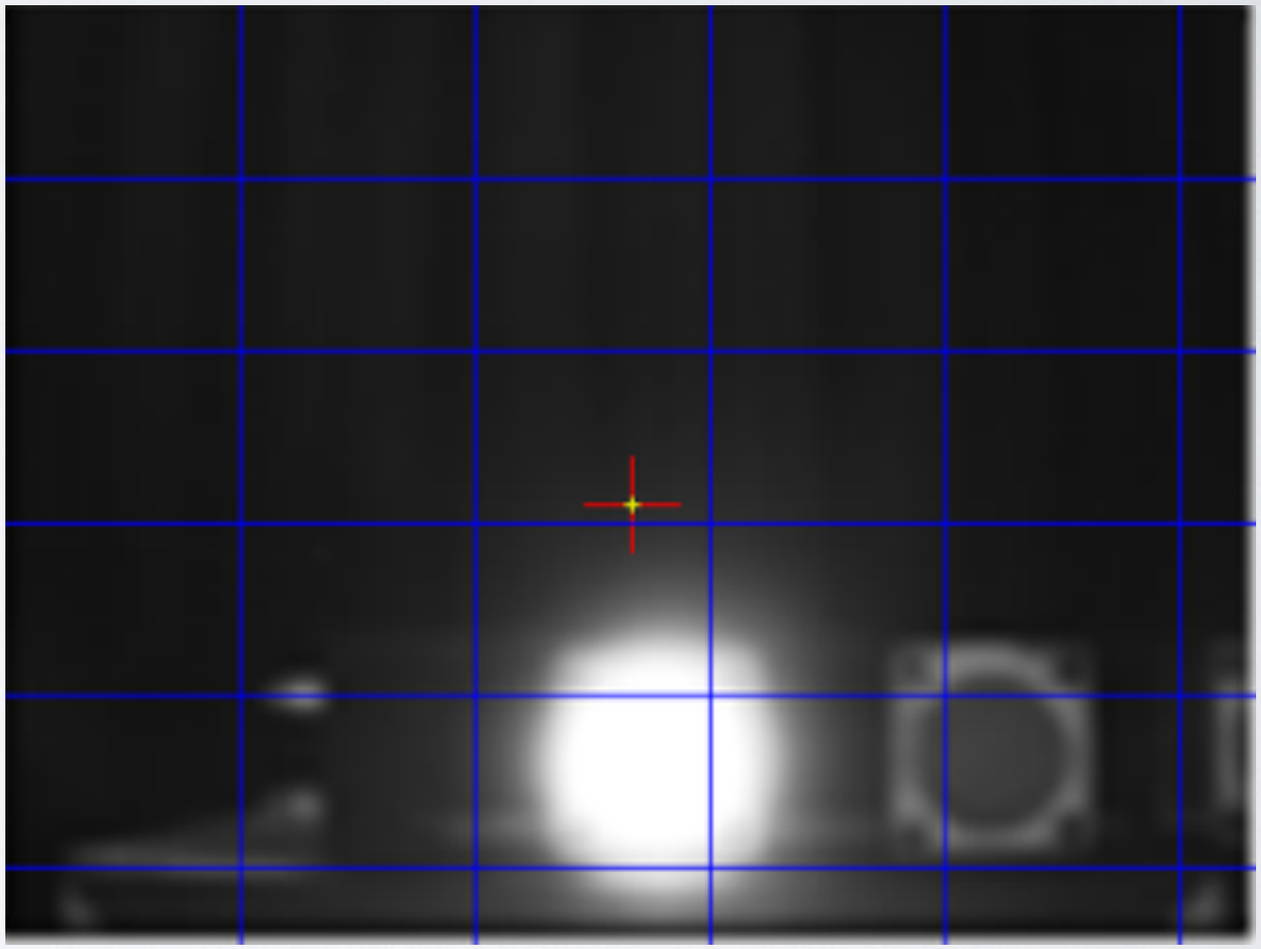


BLINDING CAMERA

- White spot, light, 50cm
- Affect background



Tonal distribution



BLINDING CAMERA

Video of MobilEye C2-270 blinded by laser 650 nm

SCENERY ATTACK

SCENERY ATTACK

- What is real?
- How to react to unclassifiable objects?

Face from cvdazzle.com
"Face not found" on pictriev.com

SCENERY ATTACK

- What is real?
- How to react to unclassifiable objects?

Face from cvdazzle.com
"Face not found" on pictriev.com

COUNTERMEASURES CAMERA

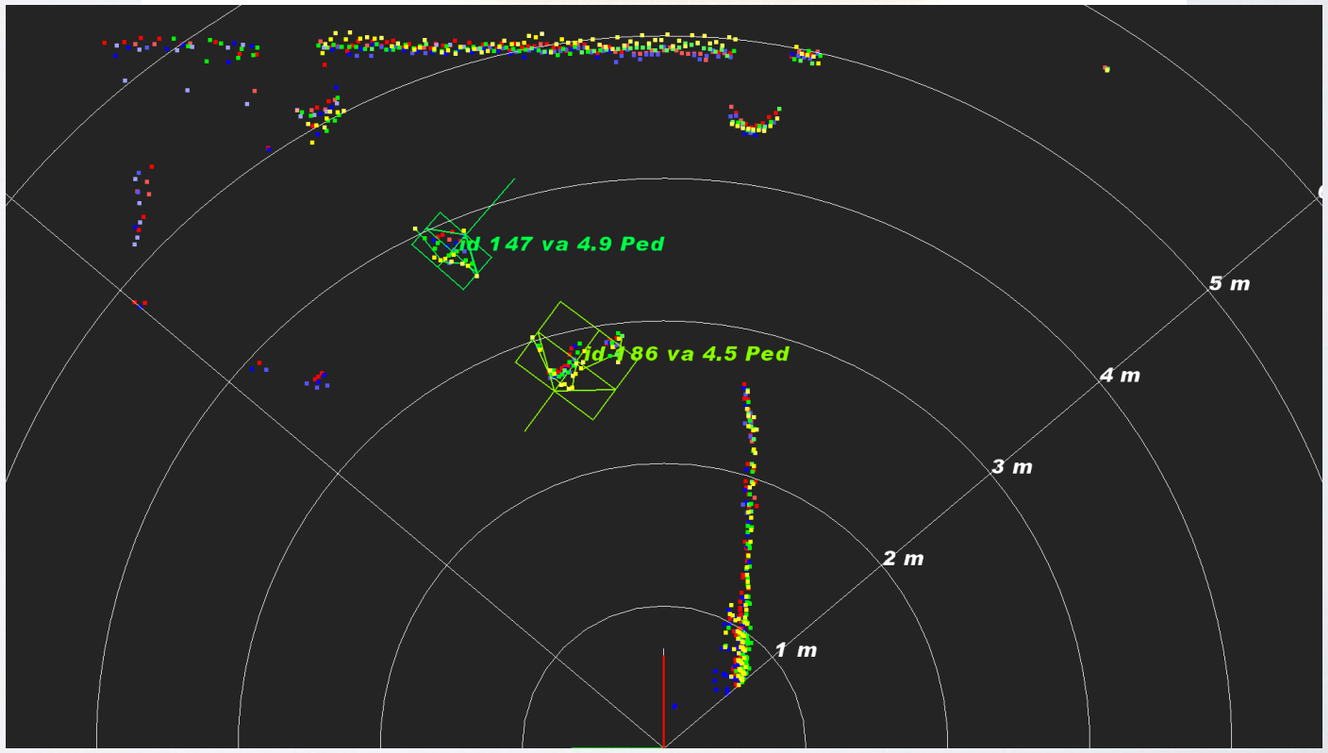
- Increase redundancy by adding cameras to **overlap** fully or partially.

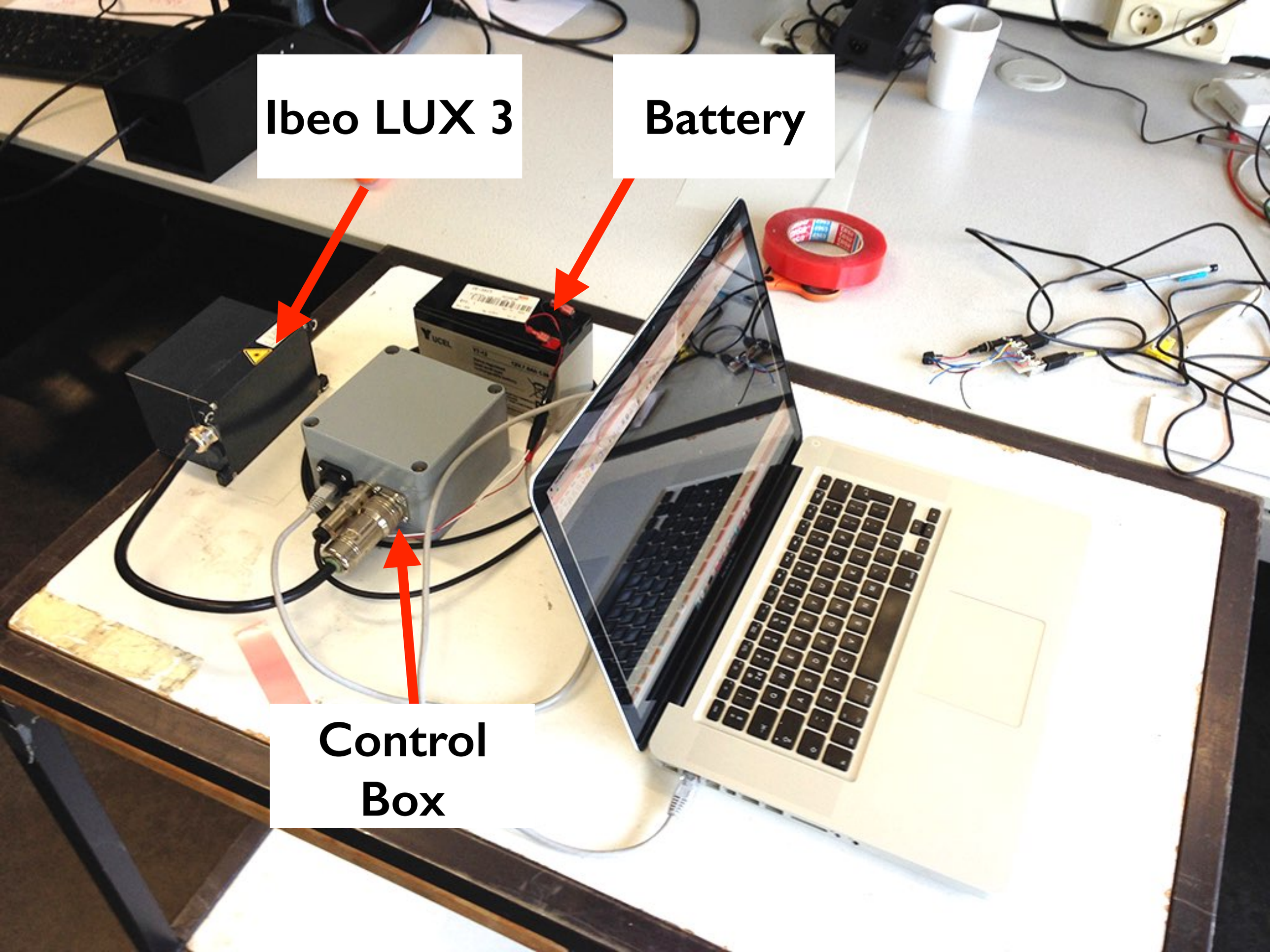
- Limit the effects of high-intensity light sources on image sensors via certain **optics** and materials.

- Detect jamming attacks on cameras via spectral analysis.

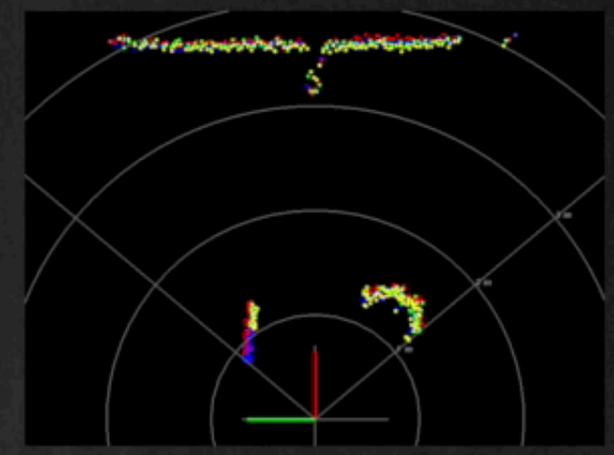
LIDAR

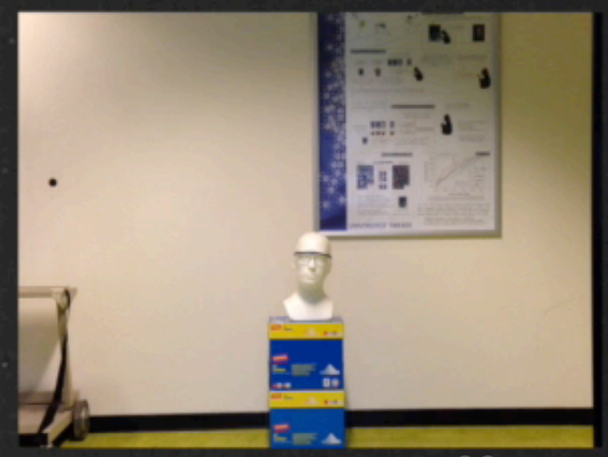
- IBEO LUX 3
- Detect object
- Object tracking
- 200 meters range




Ibeo LUX 3
Battery
Control Box

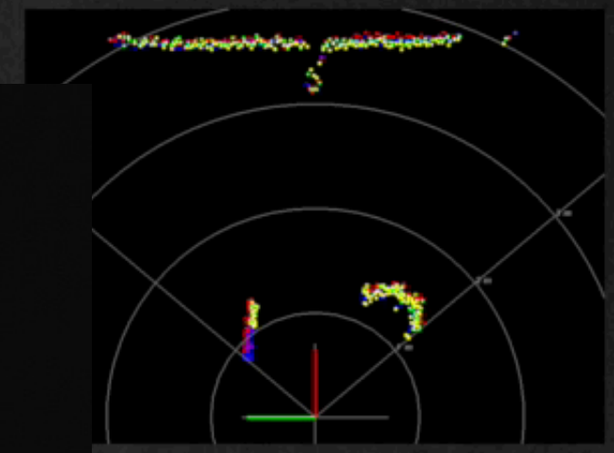
HOW DOES LIDAR WORK?



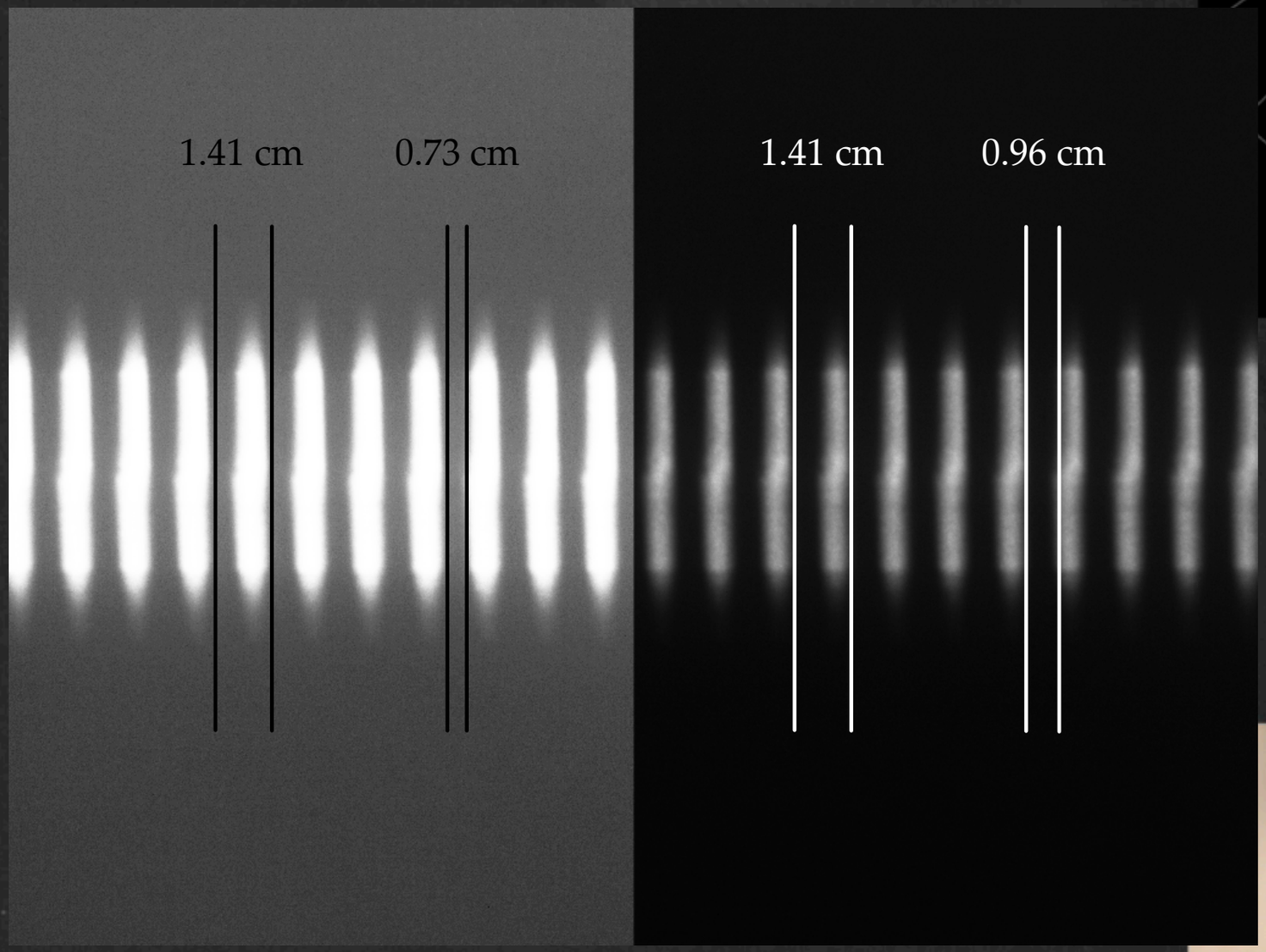


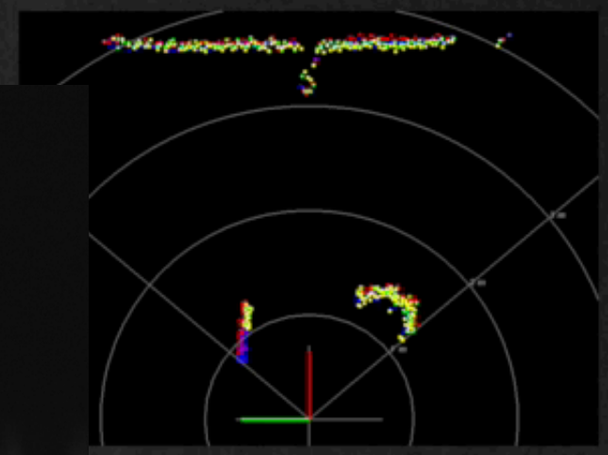
HOW DOES LIDAR WORK?

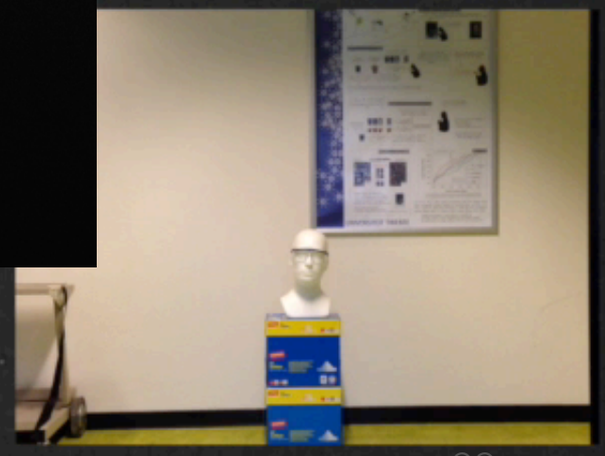
50Hz pulse



HOW DOES LIDAR WORK?

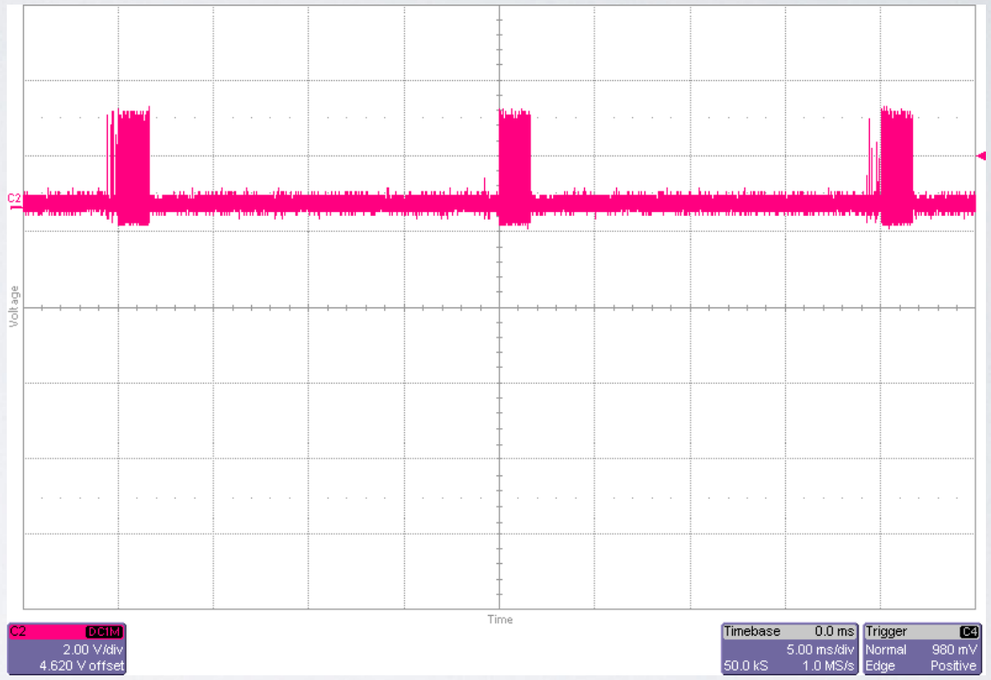


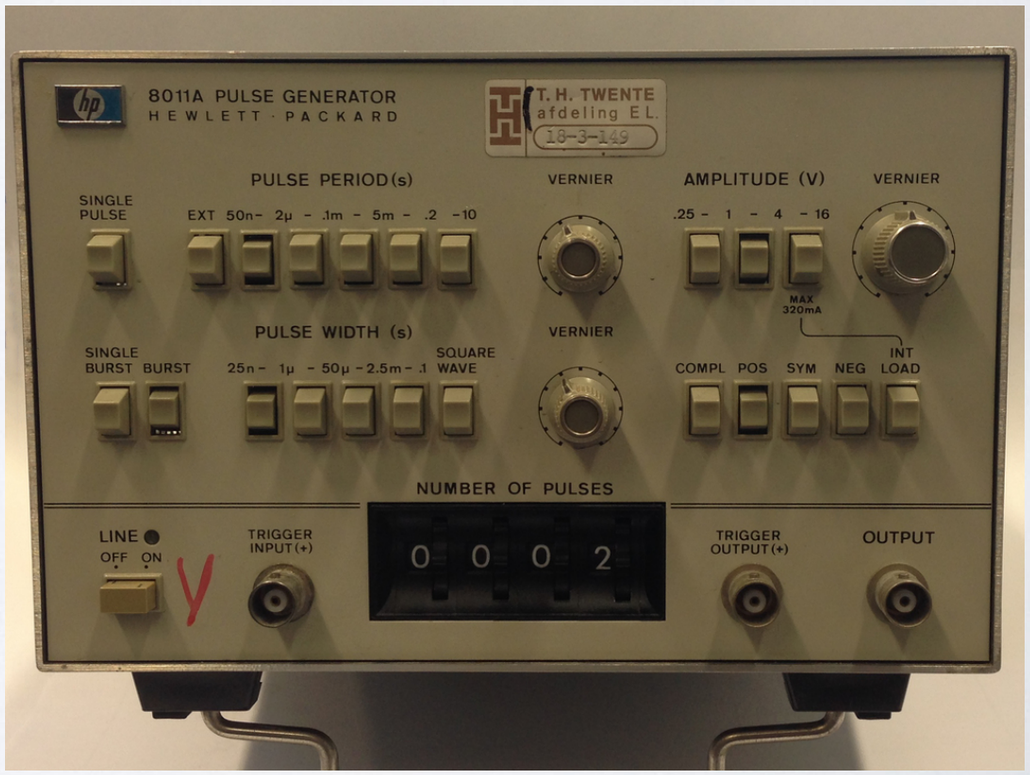




ATTACKING LIDAR

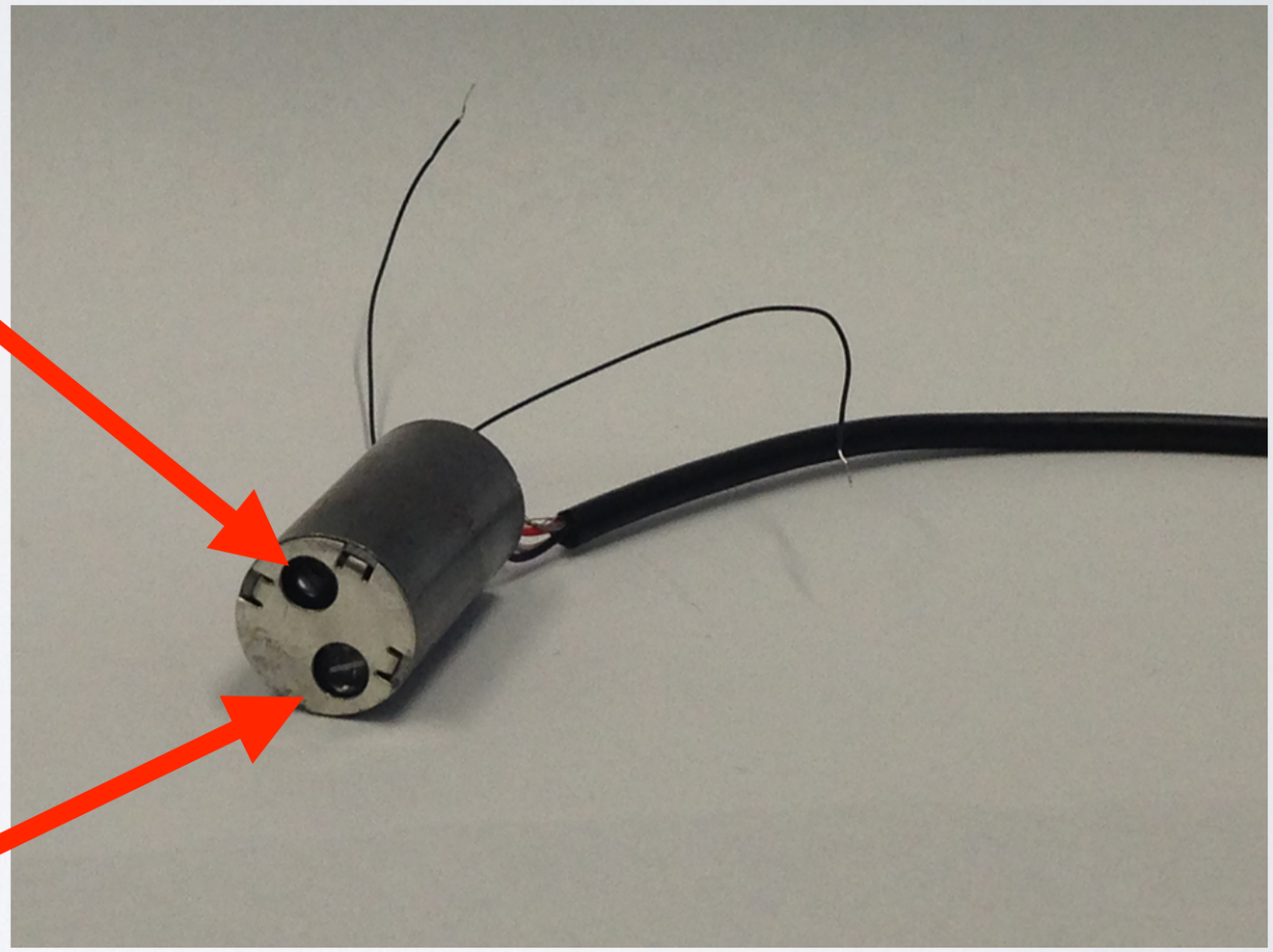
- Attacks:
  - Replay
  - Relay
  - Jamming
  - Spoofing
  - Tracking
- Equipments:
  - Laser
  - Receiver/Transmitter
  - Pulse generator





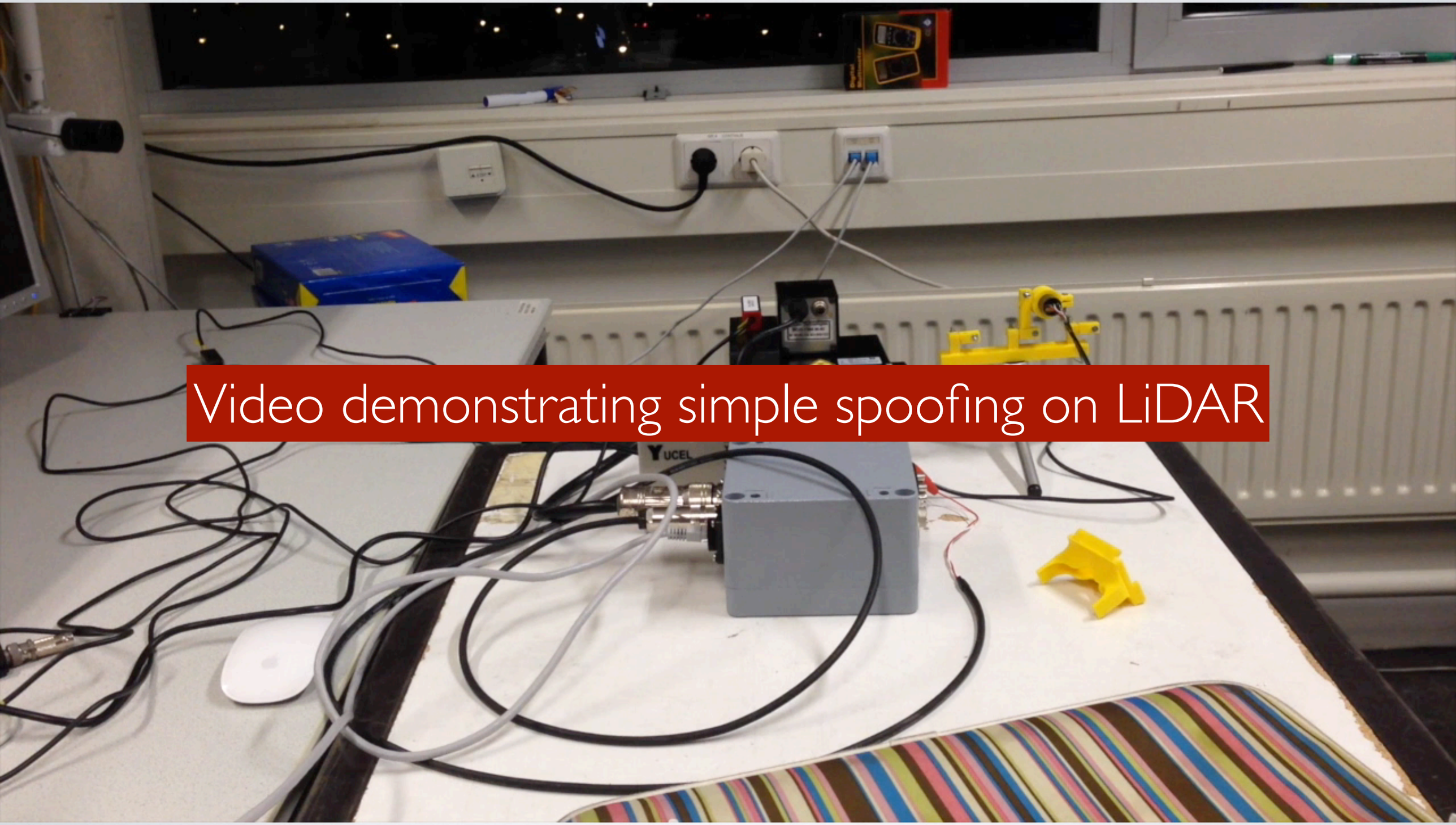
EQUIPMENT

Emitting laser:
Osram SPL-PL90
($43.25)
Max. output: 25W for 100 ns
Viewing angle: 9°

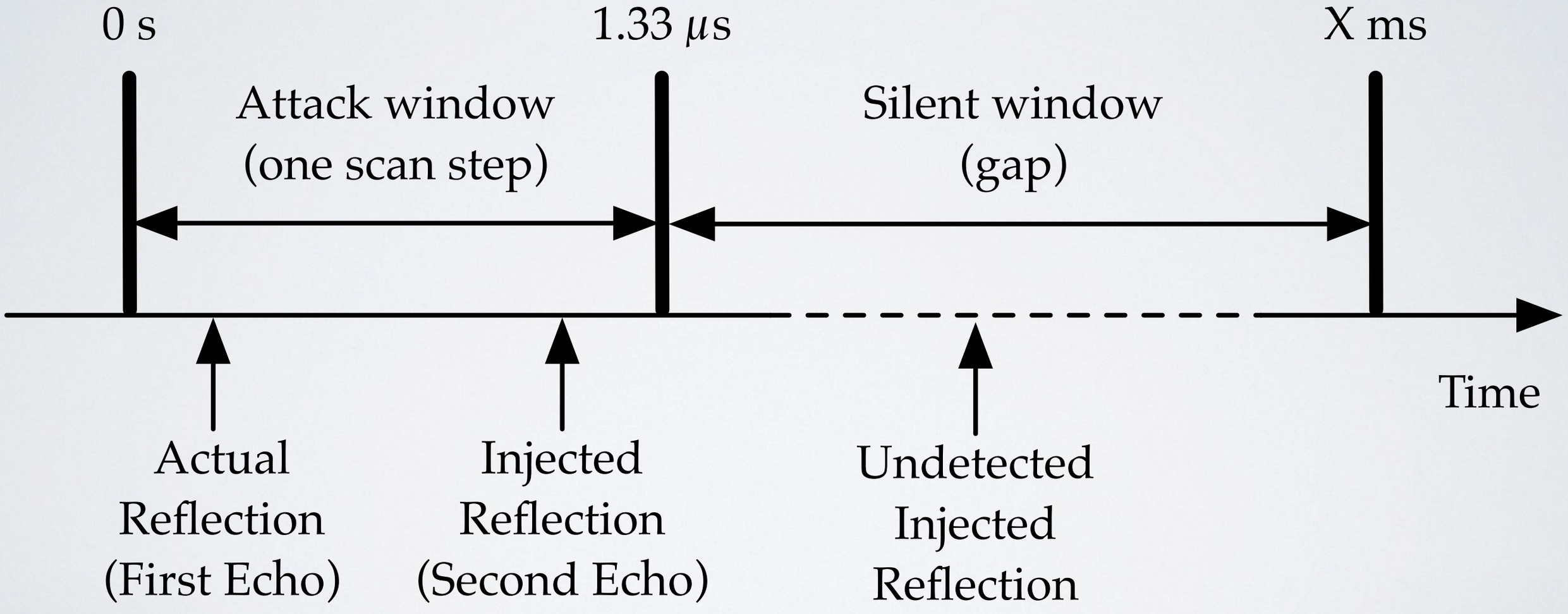


Receiving photodetector:
Osram SFH-213
($0.65)

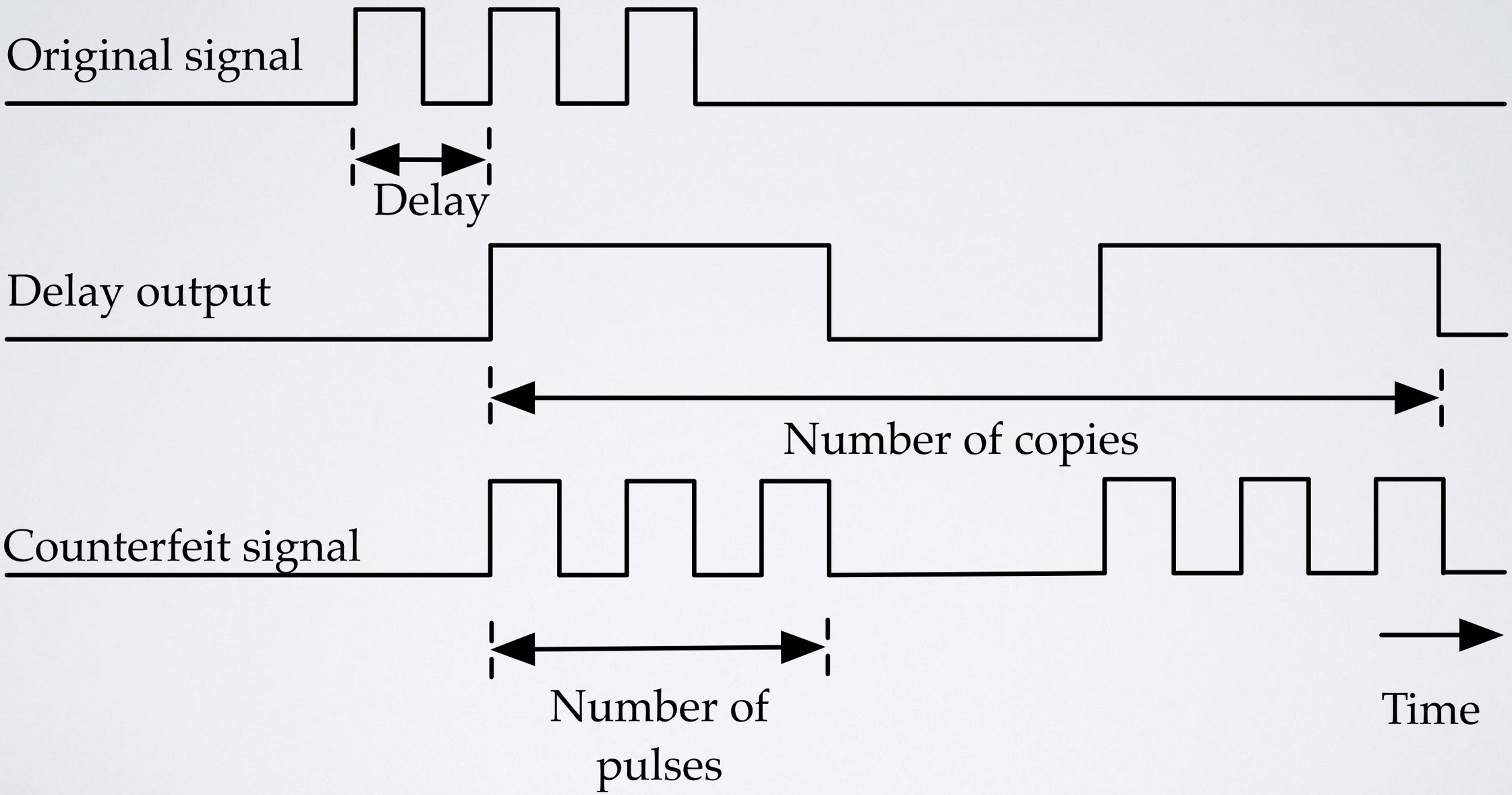
SPOOFING LIDAR (1/4)



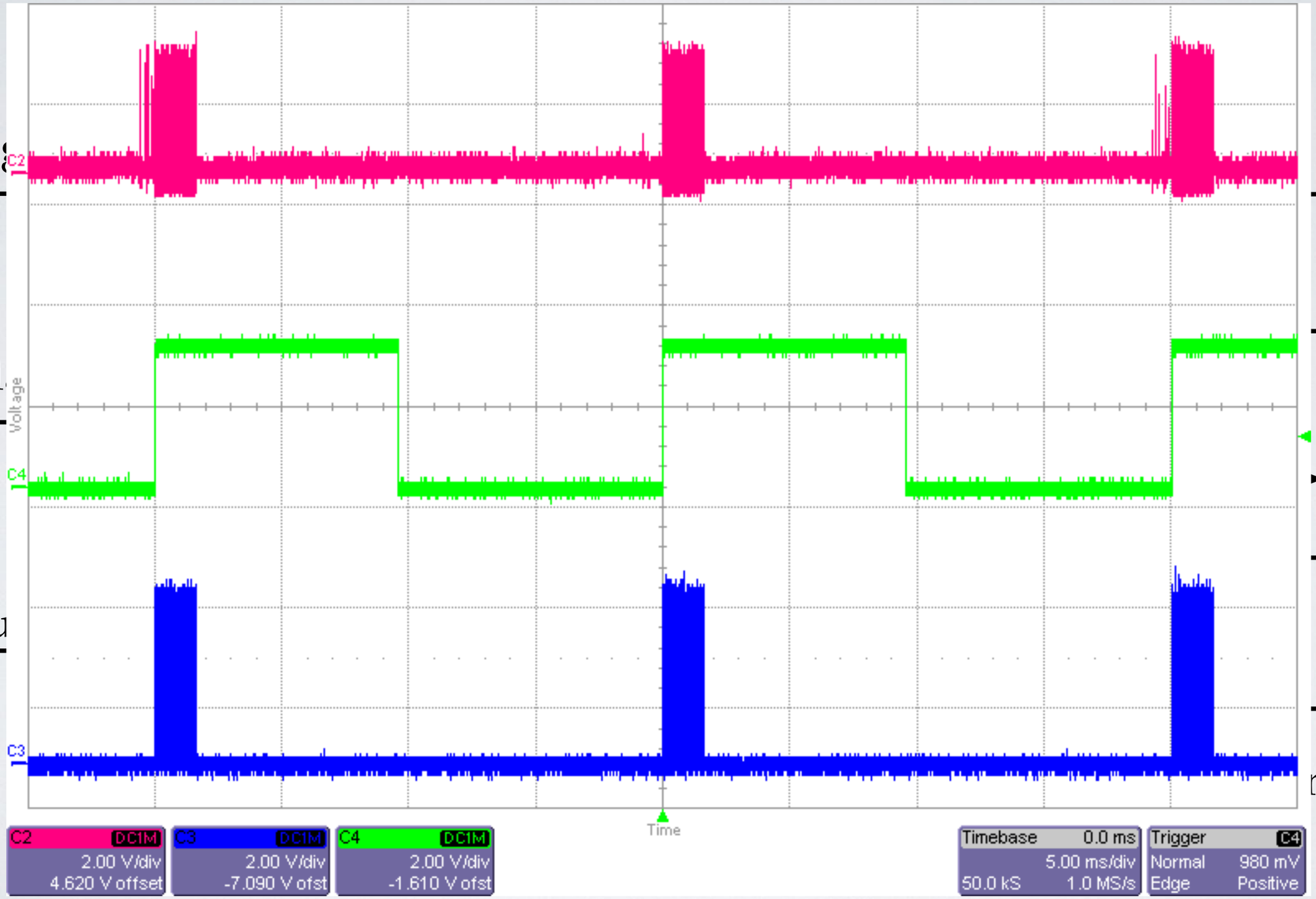
SPOOFING LIDAR (2/4)



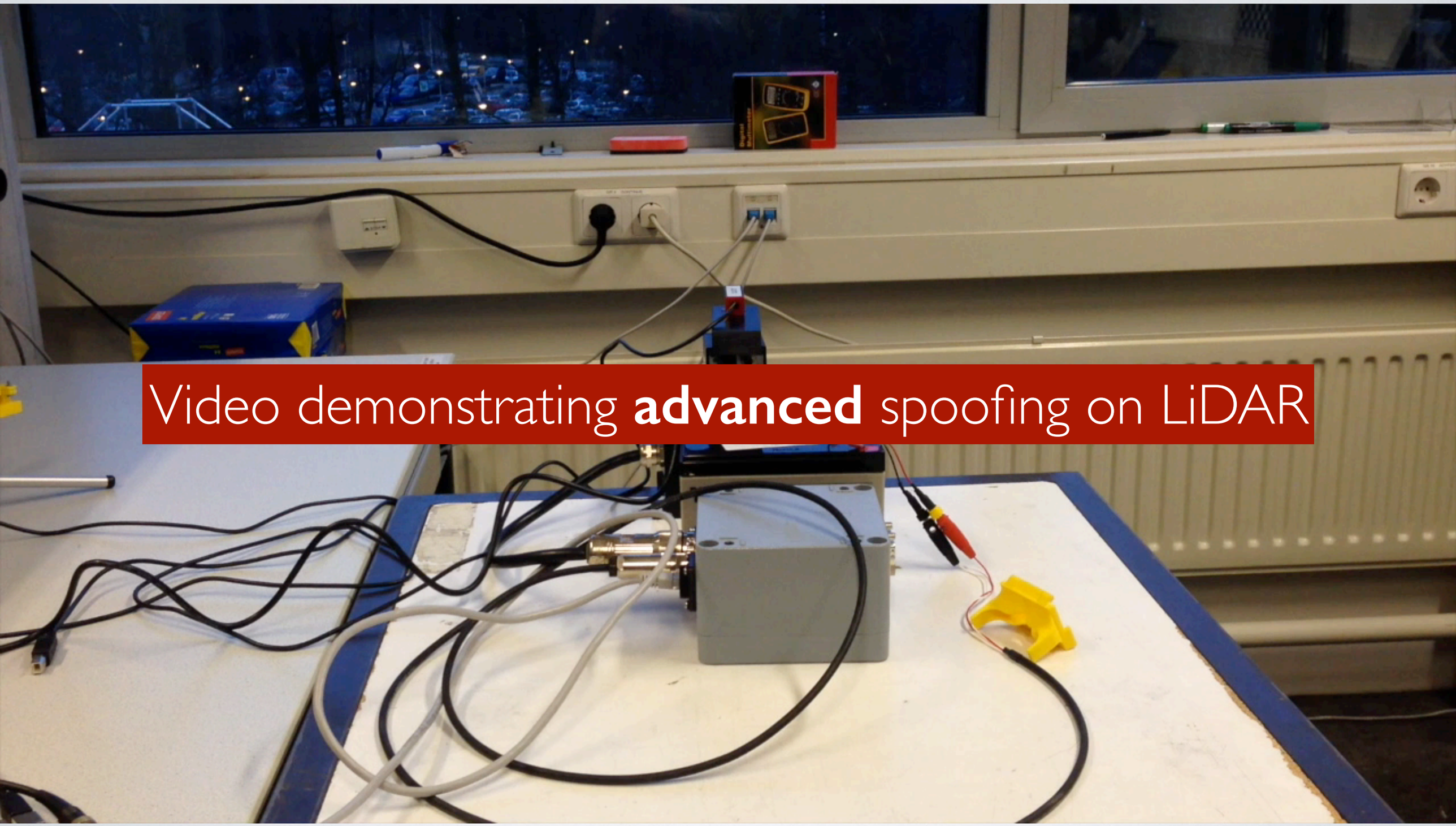
SPOOFING LIDAR (3/4)



SPOOFING LIDAR (3/4)



SPOOFING LIDAR (4/4)



Video demonstrating effect of attacker location

Video demonstrating “flashlight”

TRACKING LIDAR

COUNTERMEASURES LIDAR

- **Use multiple lasers with non-overlapping wavelengths for redundancy:**

  Ibeo: Possible, but currently not preferred by Ibeo

- **Split image into separate channels to detect single-wavelength attacks**

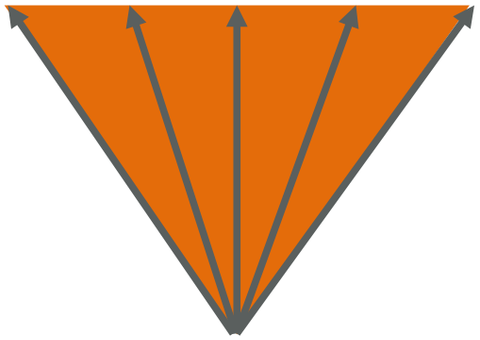
- **Shorten the pulse period by limiting the maximum range:**

  Ibeo: Today Ibeo adapts the maximum range according to the environmental situation

Countermeasures LIDAR

- Introduce random probing - In preparation by Ibeo:
  - Prevents spoofing - spoofing only generates uncorrelated noise but no validated tracks
  - Enables the detection of spoofing attacks
- Probe multiple times to raise the confidence in a measurement:
  - Already implemented by object tracking with dedicated track validation on sensor object output for vehicle control systems
- Increase the number of objects than can be tracked (65 here):
  - Just a question of processing power, today Ibeos systems are able to manage up to 1,023 objects simultaneously

Countermeasures LIDAR - System Setup Analyzed



Meas core
(Standard probing**)**

Raw data
preprocessing

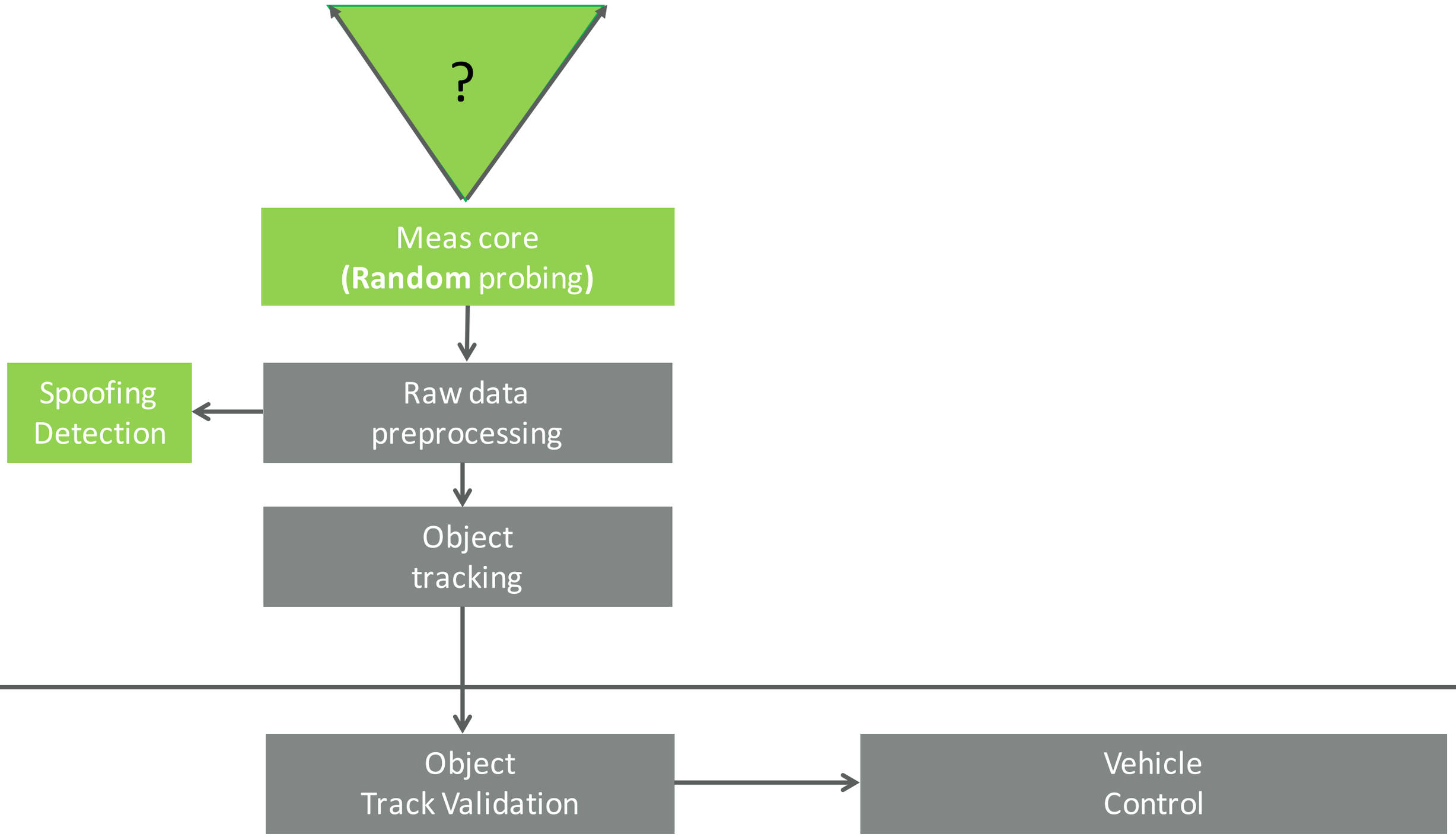
Object
tracking

Developer Interface

Object
Track Validation

Vehicle
Control

Countermeasures LIDAR - System Setup in Preparation



BLACK HAT SOUND BYTES.

1. Fooling LiDAR on raw data level in laboratory environment is possible **but**

   establishing stable objects on sensor output in real driving scenarios level for vehicle control could not be demonstrated

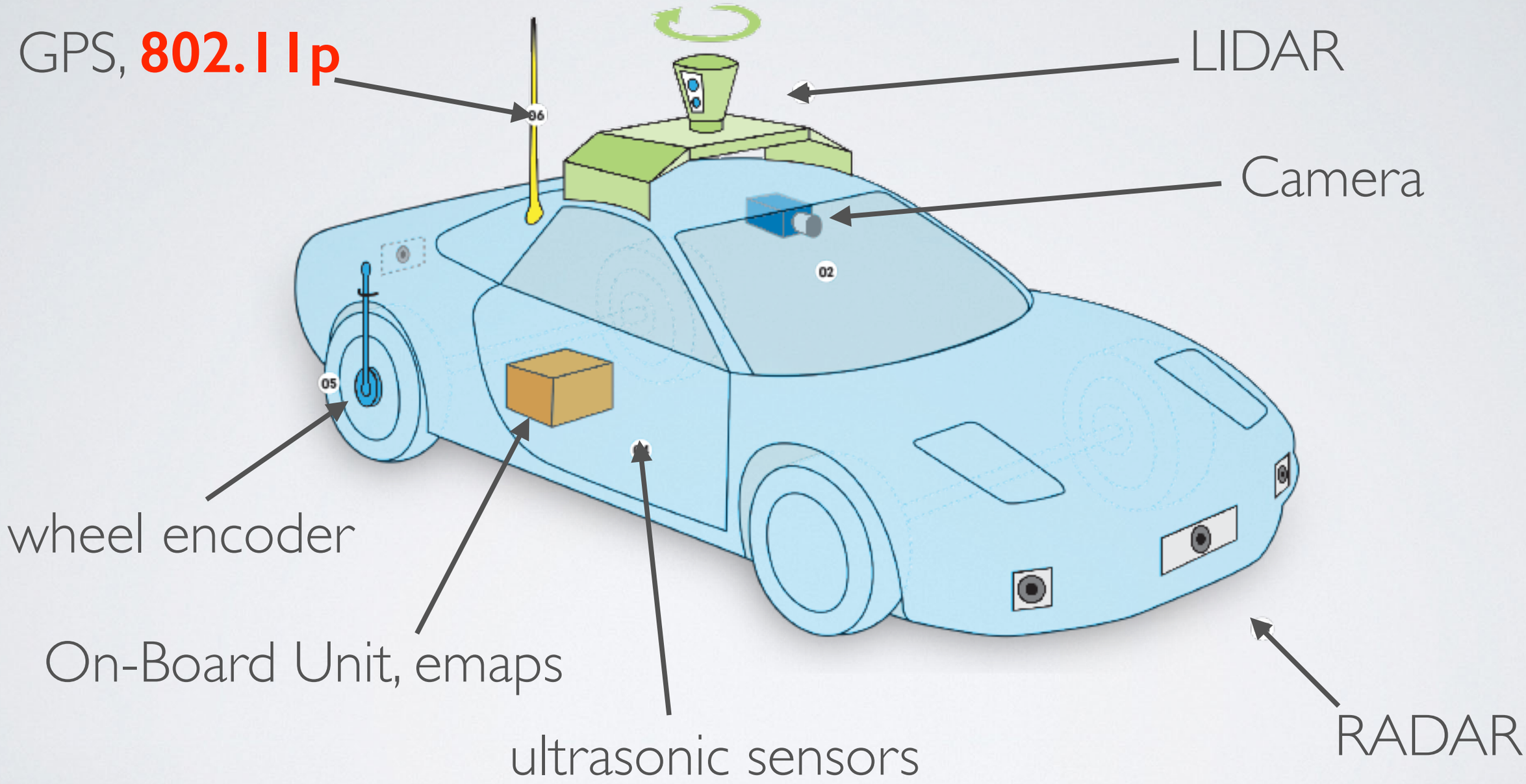
2. Fooling camera-based systems is **easy** and **cheap.**

3. Don't trust automated vehicle sensors unless you implement countermeasures to mitigate such threads.

CONNECTED VEHICLES: I CAN TRACK YOU!

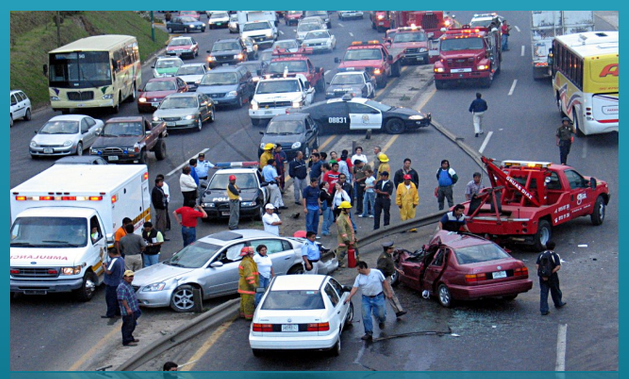
Jonathan Petit, Djurre Broekhuis, Michael Feiri, Frank Kargl

AUTOMATED/CONNECTED VEHICLE



APPLICATION AREAS FOR V2X COMMUNICATION

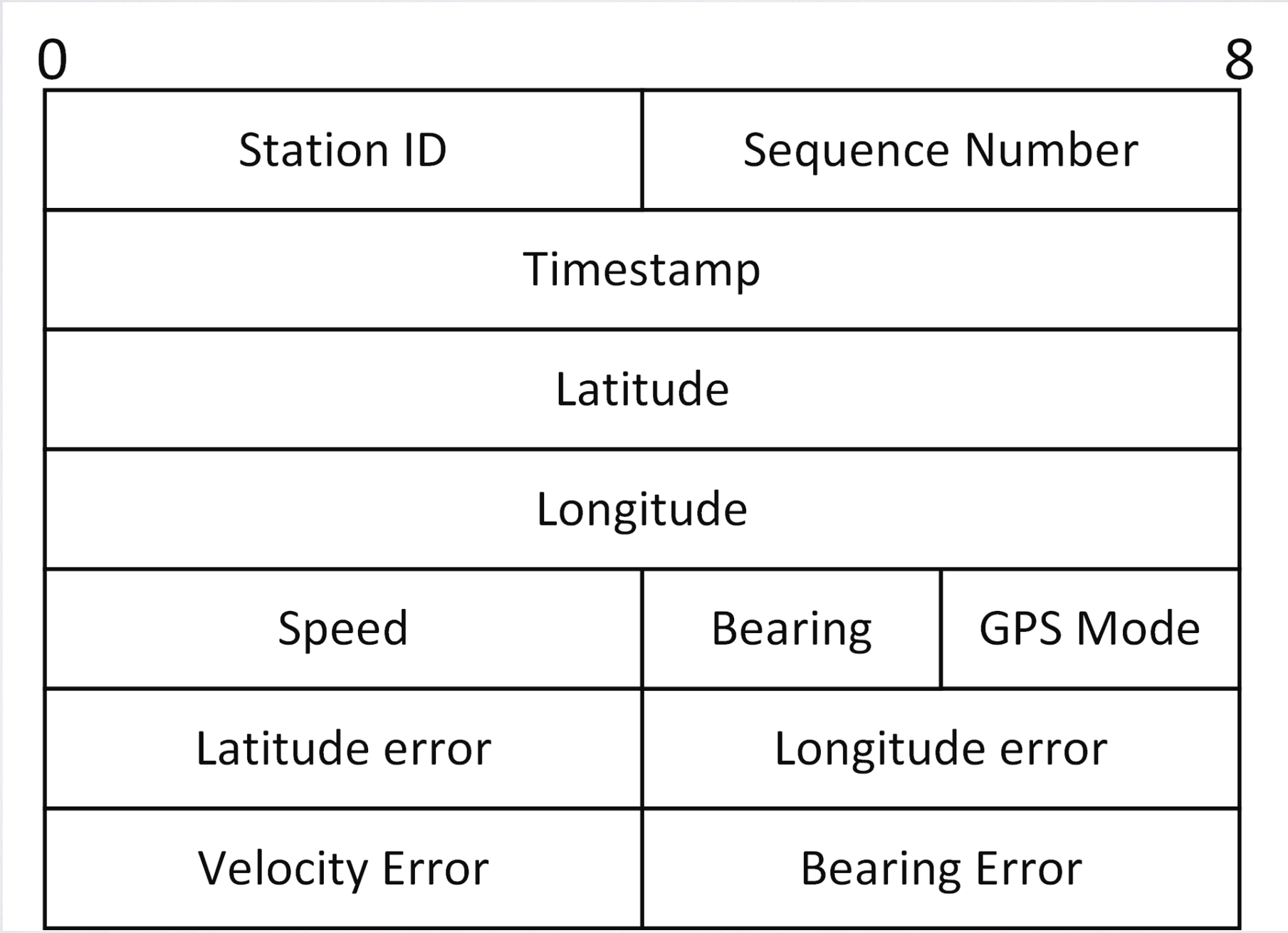
Safety



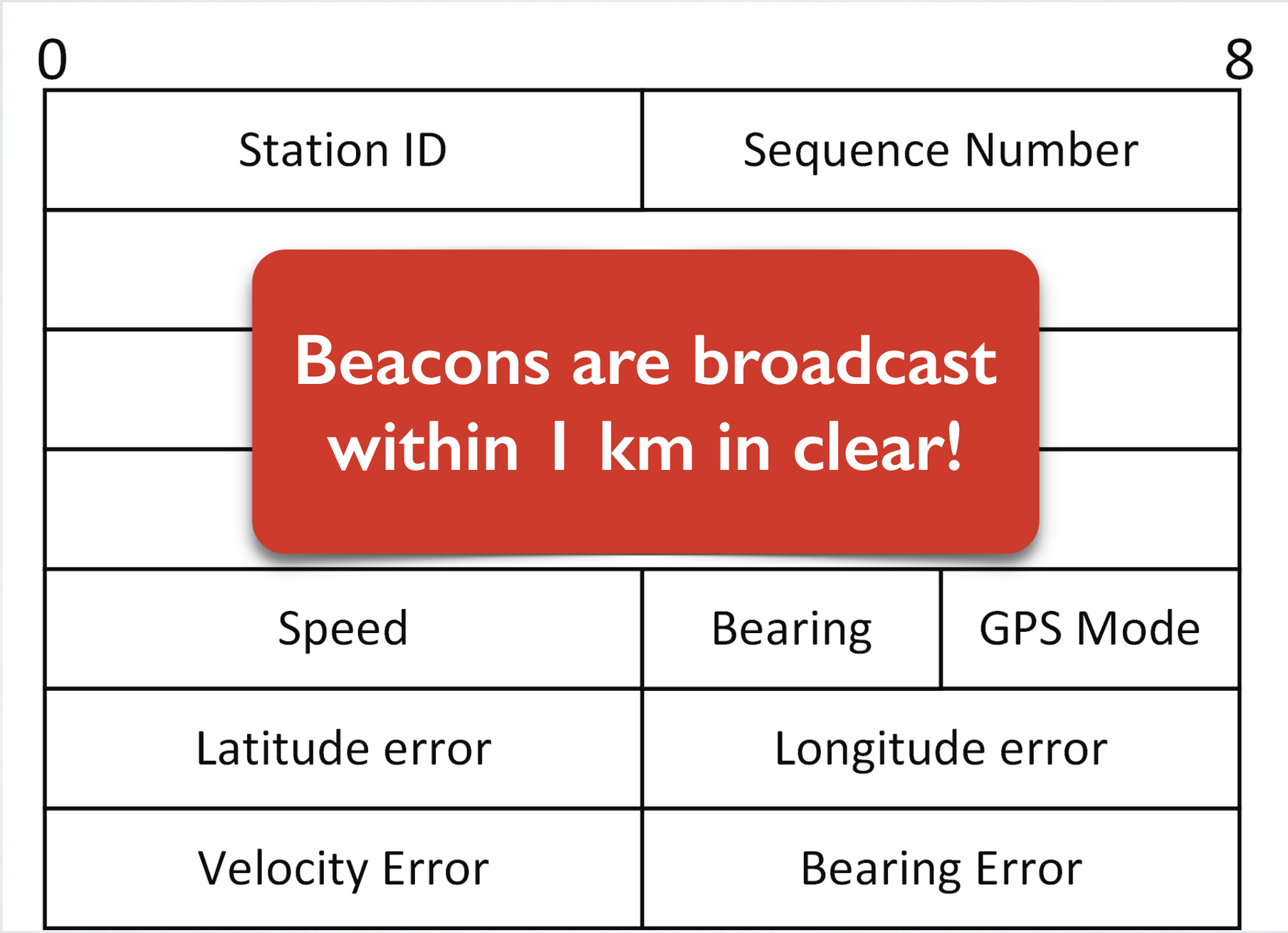
Efficiency

Comfort

CONTENT OF BEACON



CONTENT OF BEACON



Beacons are broadcast within 1 km in clear!

CONTENT OF BEACON

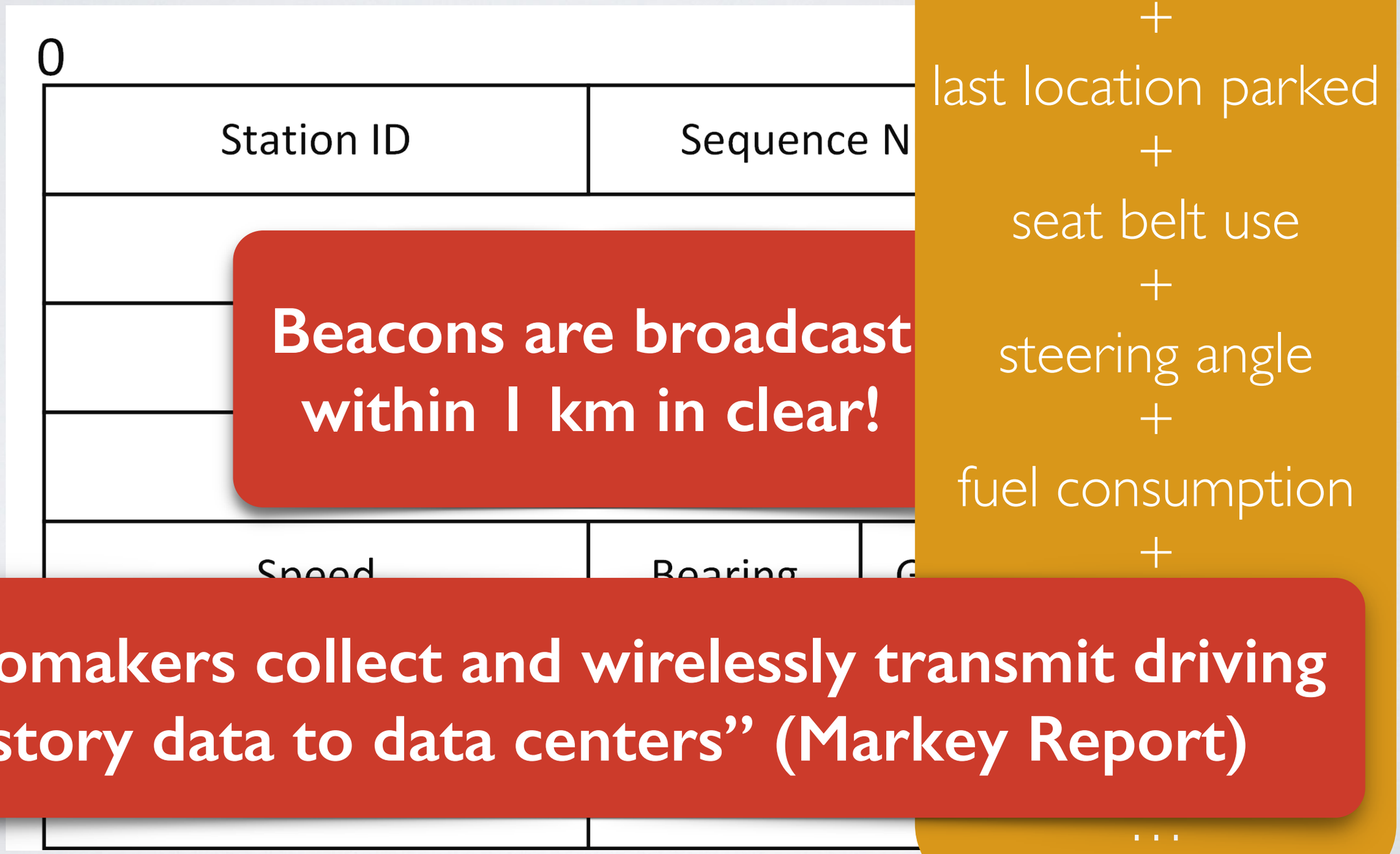
0

Station ID	Sequence N
Speed	Bearing | G
Latitude error	Longitude
Velocity Error	Bearing E

Beacons are broadcast within 1 km in clear!

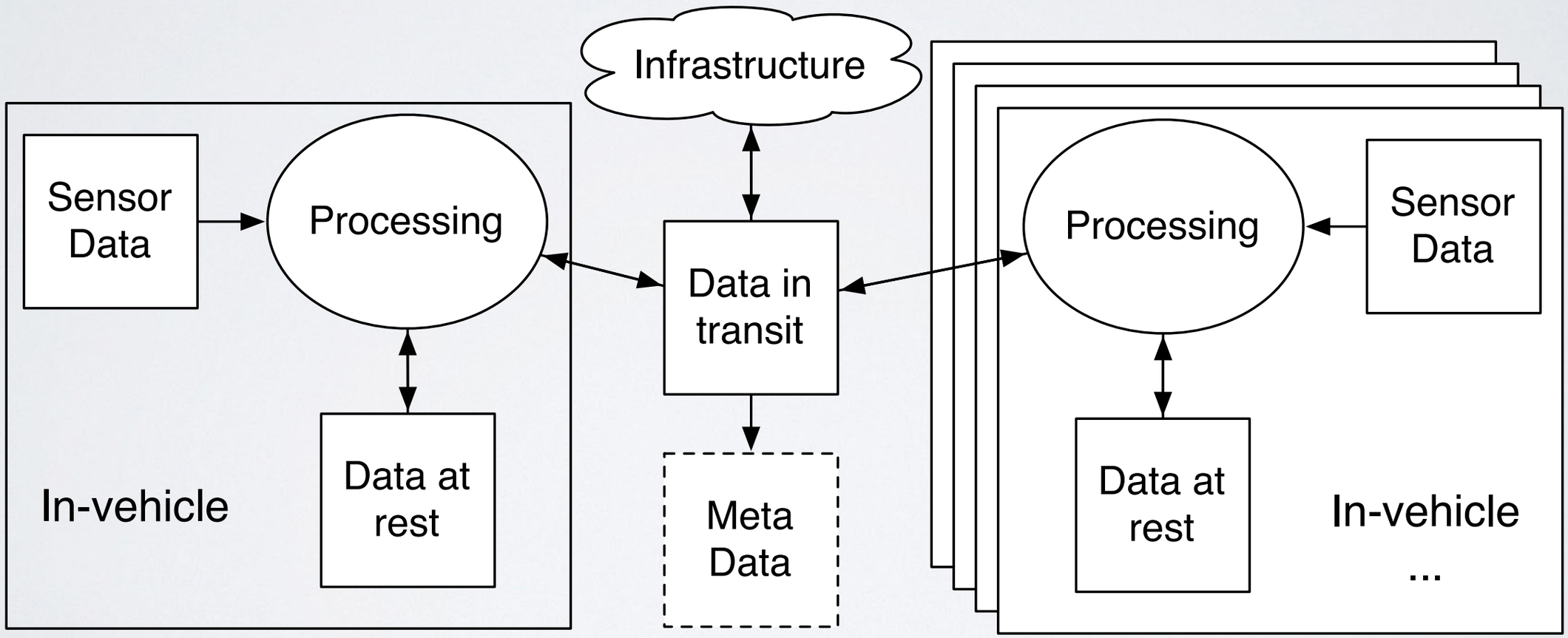
+
pathHistory
+
last location parked
+
seat belt use
+
steering angle
+
fuel consumption
+
exterior temperature
+
…

CONTENT OF BEACON



“Automakers collect and wirelessly transmit driving history data to data centers” (Markey Report)

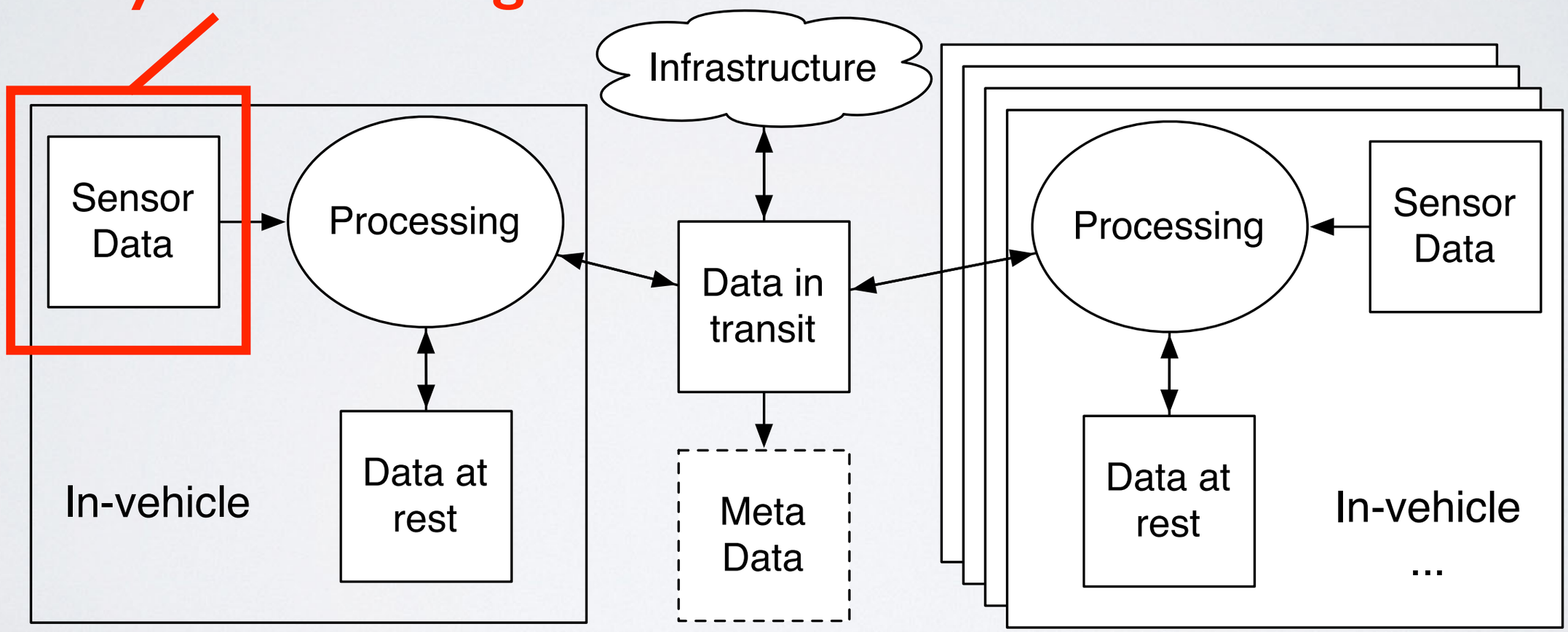
PRIVACY VIOLATIONS



J. Petit et al., "Revisiting Attacker Models for Smart Vehicles", WiVec'14.

PRIVACY VIOLATIONS

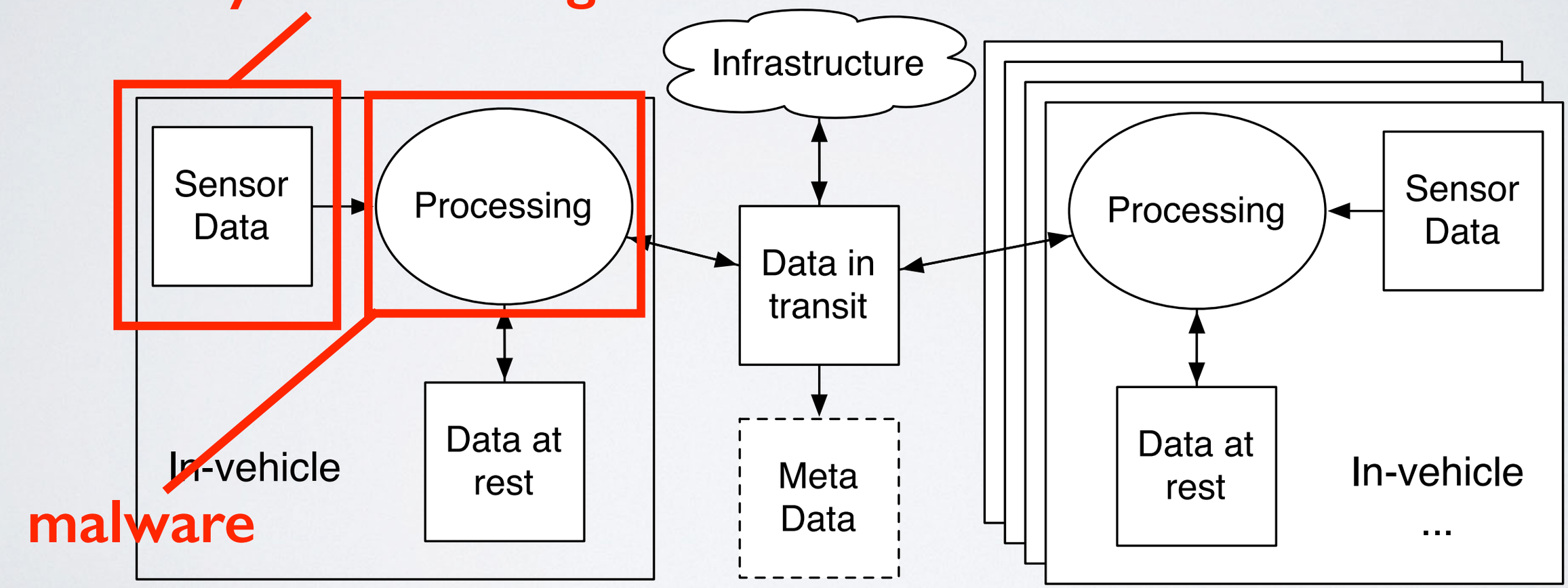
collect information about me, my car, and my surroundings



J. Petit et al., "Revisiting Attacker Models for Smart Vehicles", WiVec'14.

PRIVACY VIOLATIONS

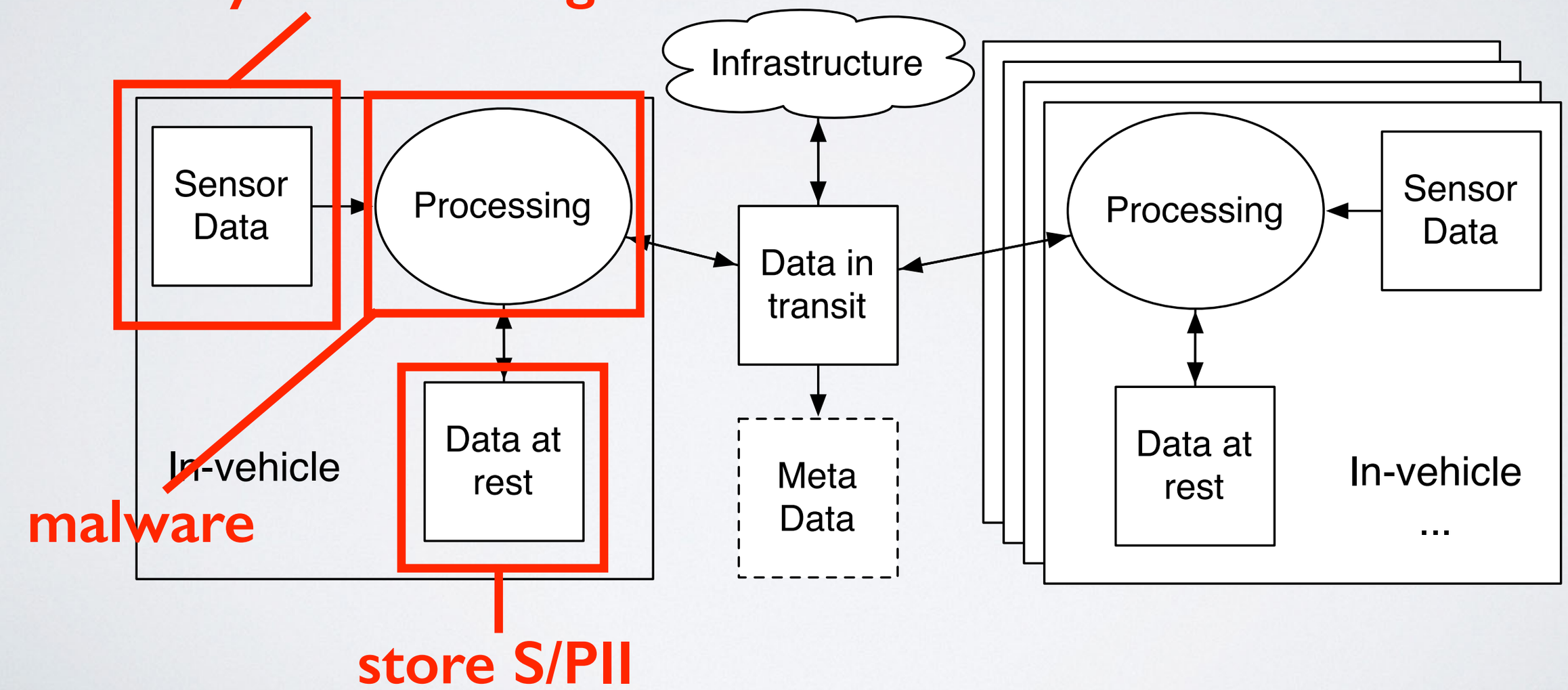
collect information about me, my car, and my surroundings



J. Petit et al., "Revisiting Attacker Models for Smart Vehicles", WiVec'14.

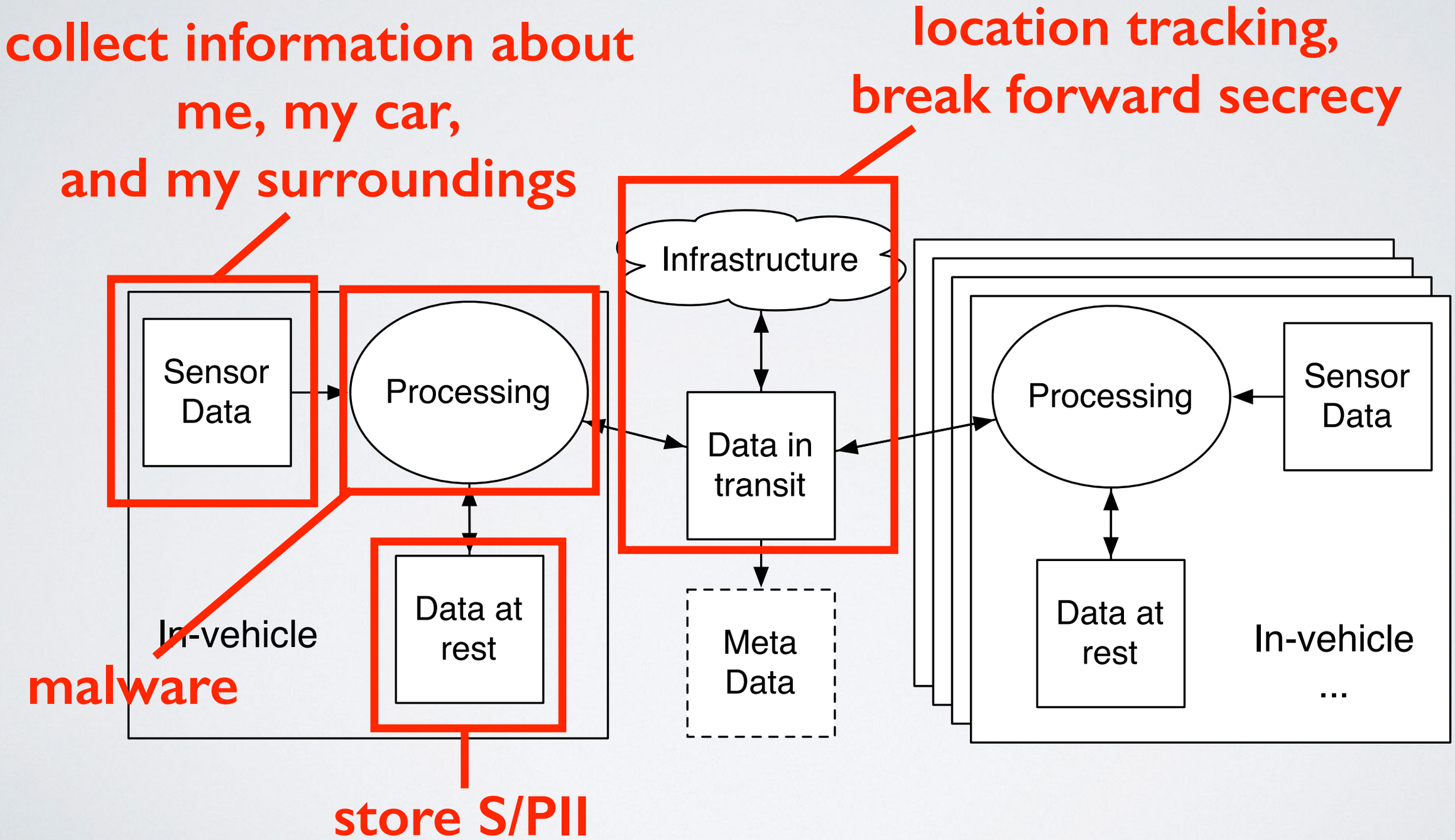
PRIVACY VIOLATIONS

collect information about me, my car, and my surroundings



J. Petit et al., "Revisiting Attacker Models for Smart Vehicles", WiVec'14.

PRIVACY VIOLATIONS

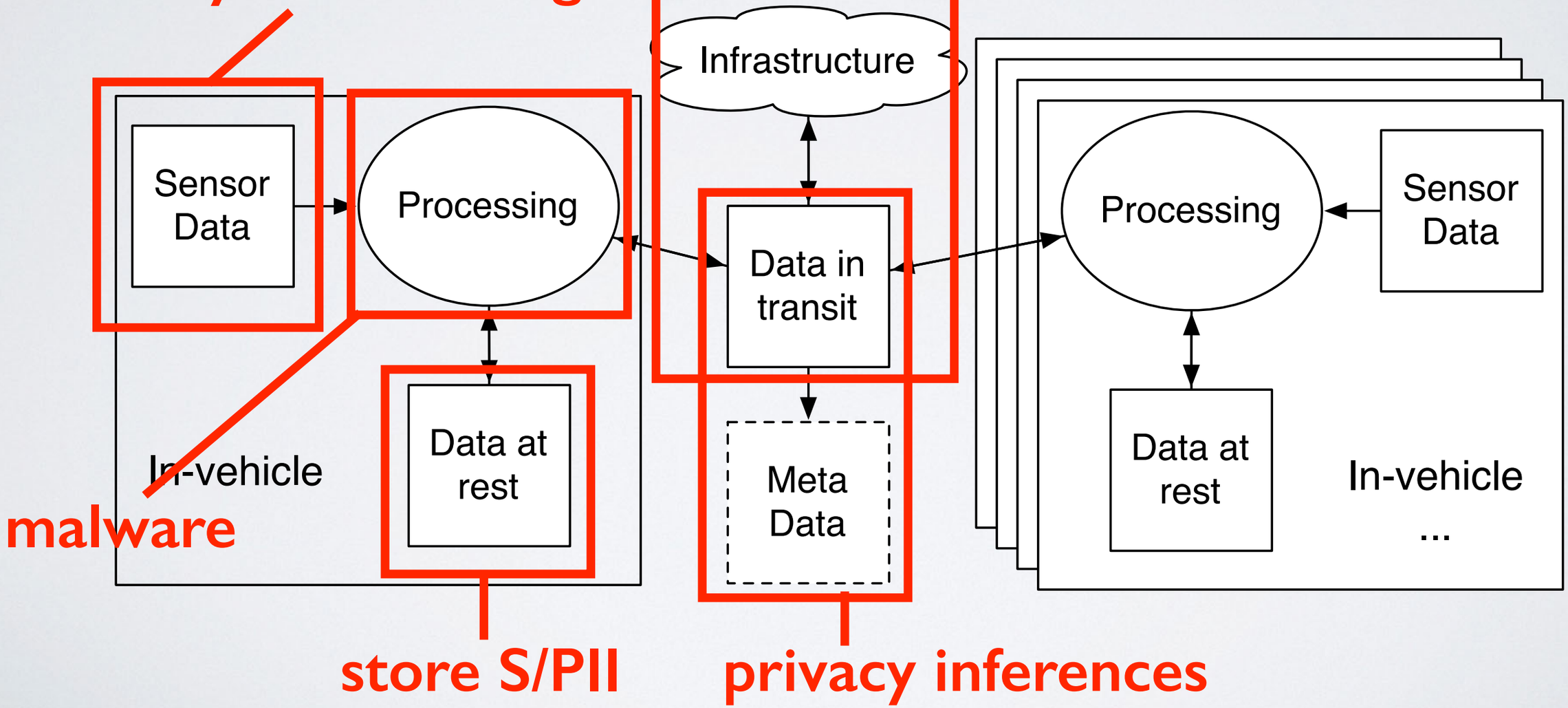


J. Petit et al., "Revisiting Attacker Models for Smart Vehicles", WiVec'14.

PRIVACY VIOLATIONS

collect information about me, my car, and my surroundings

location tracking, break forward secrecy

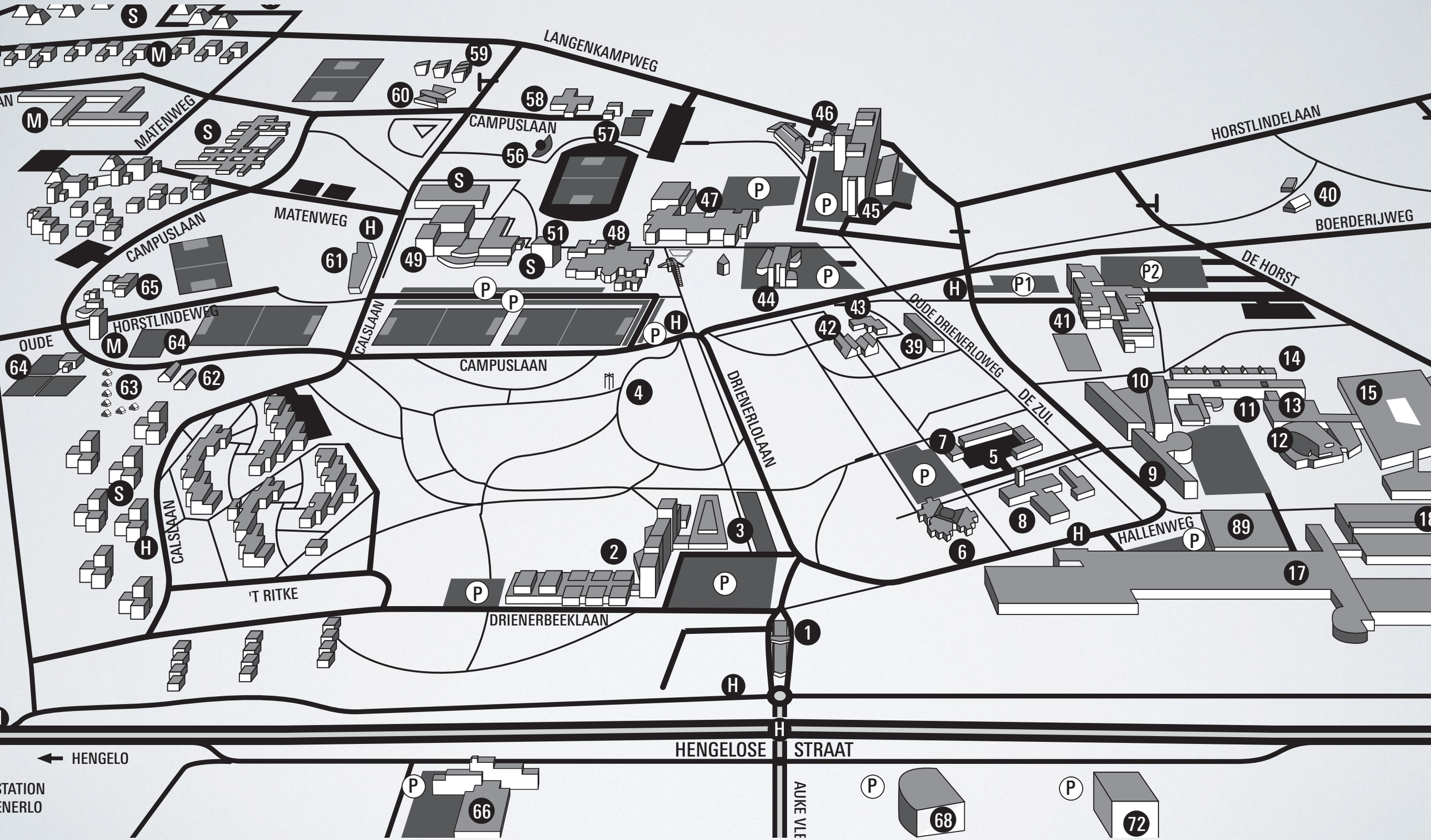


malware

store S/PII

privacy inferences

J. Petit et al., "Revisiting Attacker Models for Smart Vehicles", WiVec'14.


LANGENKAMPWEG
MATENWEG
CAMPUSLAAN
HORSTLINDELAAN
BOERDERIJWEG
DE HORST
OUDE DRIENERLOWEG
DE ZUL
HORSTLINDEWEG
OUDE
CALSLAAN
DRIENERLOLAAN
HALLENWEG
'T RITKE
DRIENERBEEKLAAN
HENGELOSE STRAAT
AUKE VLE
HENGELO
STATION
ENERLO
P1
P2

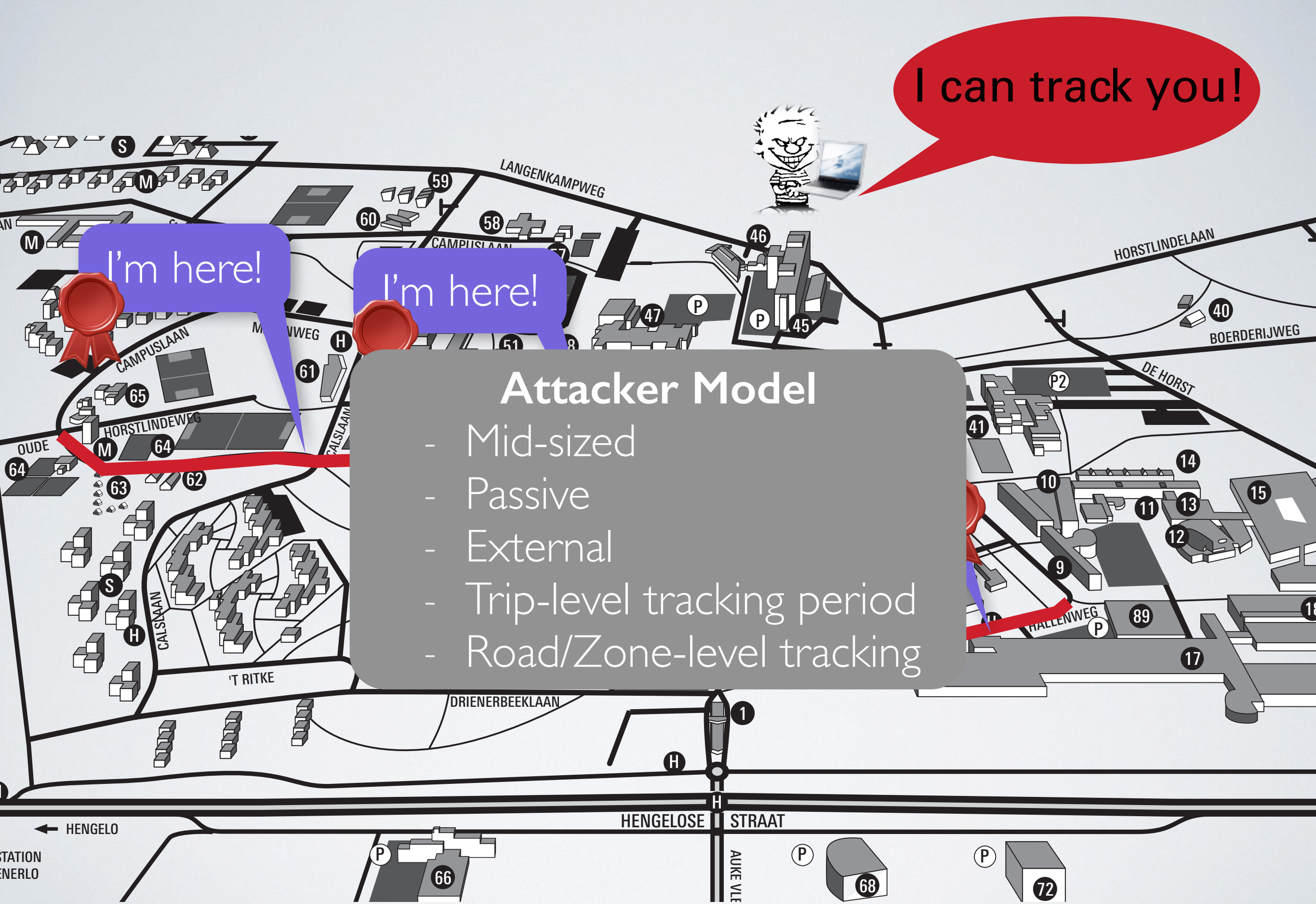
I can track you!

I'm here!

I'm here!

I'm here!

LANGENKAMPWEG
CAMPUSLAAN
HORSTLINDELAAN
BOERDERIJWEG
DE HORST
HORSTLINDEWEG
OUDE
CALSLAAN
DRIENERLOLAAN
'T RITKE
DRIENERBEEKLAAN
HALLENWEG
HENGELOSE STRAAT
AUKE VLE
HENGELO
STATION
ENERLO


I can track you!
I'm here!
I'm here!
Attacker Model
- Mid-sized
- Passive
- External
- Trip-level tracking period
- Road/Zone-level tracking
LANGENKAMPWEG
CAMPUSLAAN
HORSTLINDEWEG
OUDE
HORSTLINDELAAN
BOERDERIJWEG
DE HORST
HALLENWEG
'T RITKE
CALSLAAN
DRIENERBEEKLAAN
HENGELOSE STRAAT
AUKE VLE
HENGELO
STATION
ENERLO

I can track you!

I'm here!

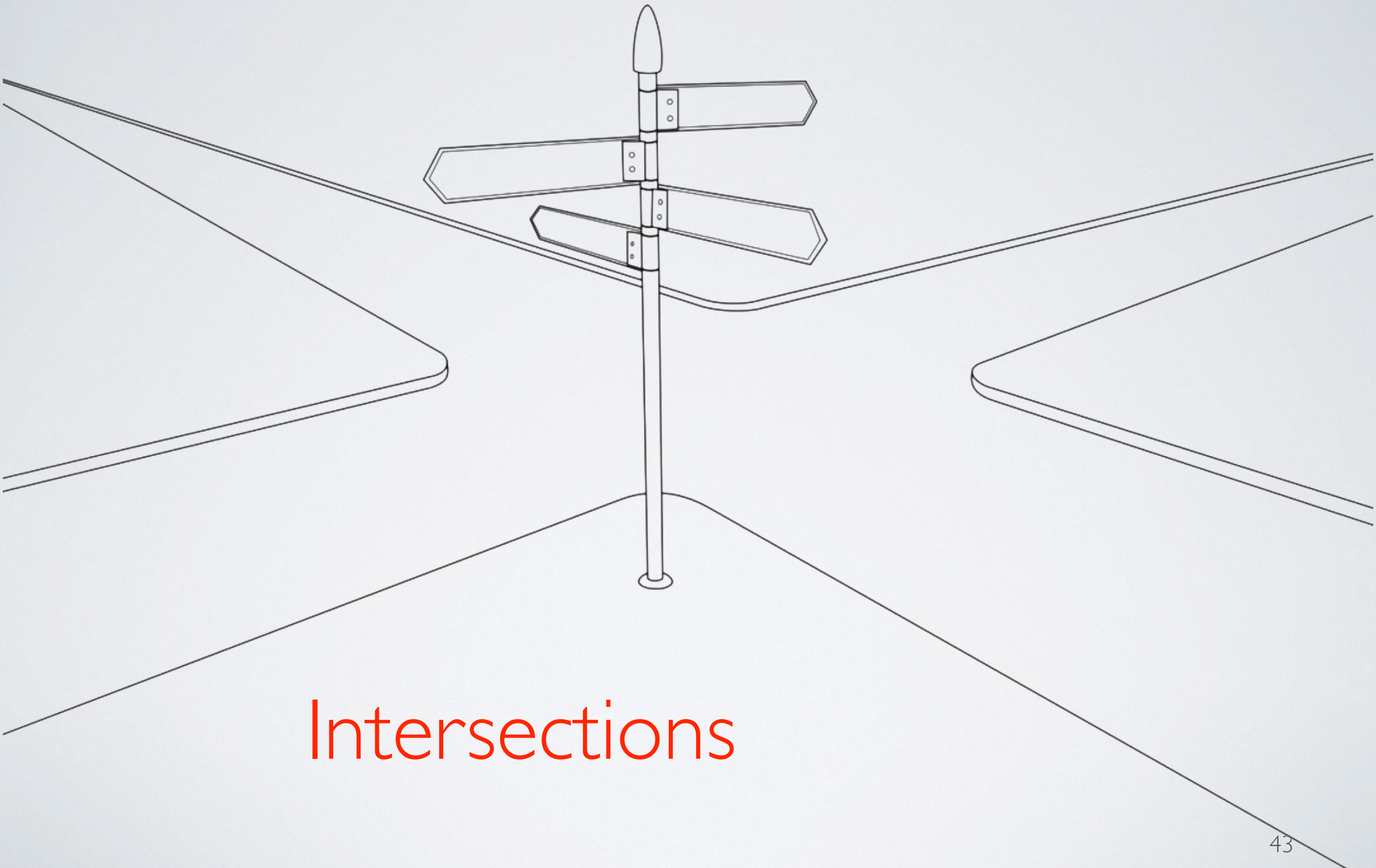
I'm here!

Attacker Model

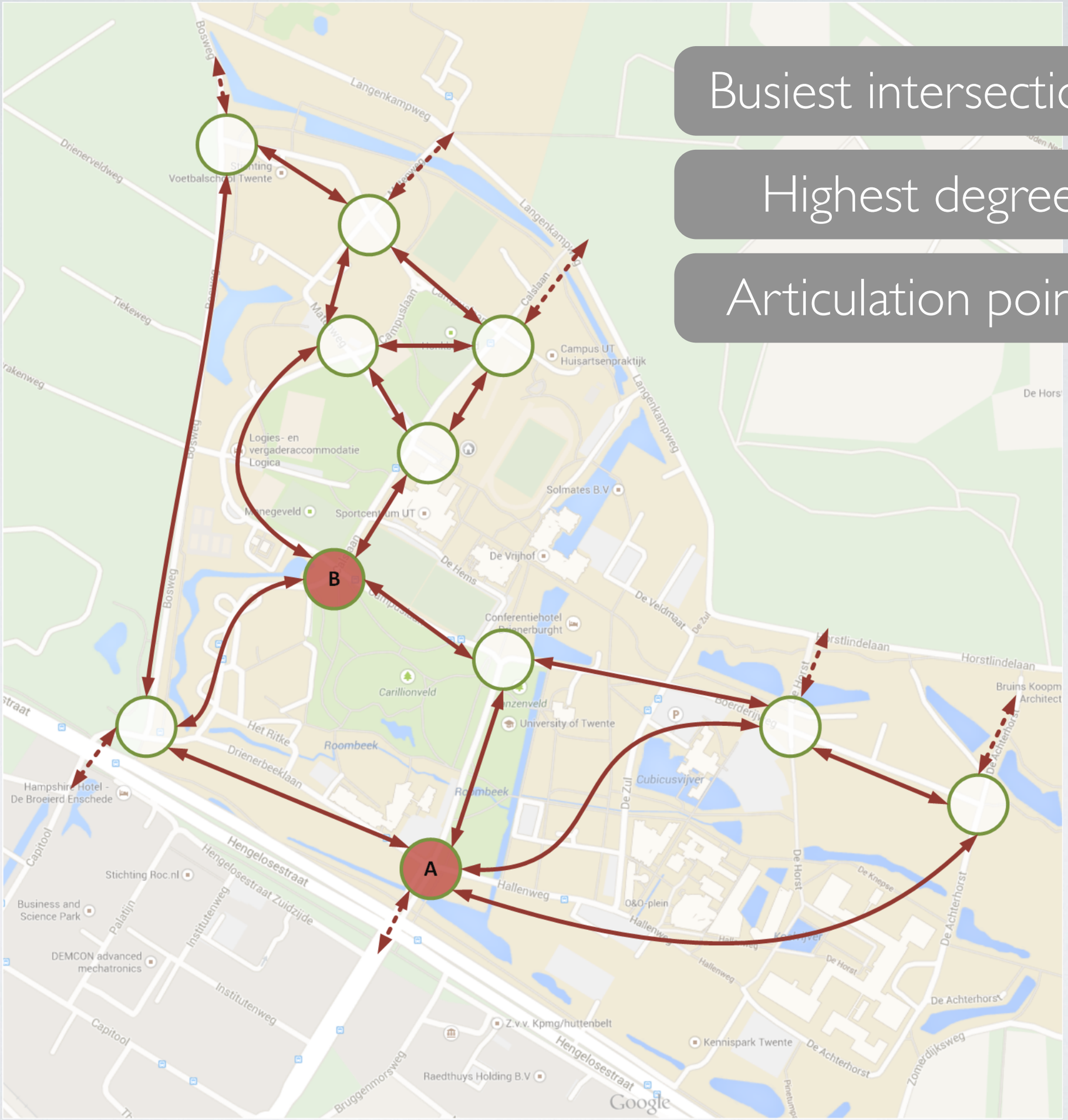
- Mid-sized
- Passive
- External
- Trip-level tracking period
- Road/Zone-level tracking

Let's track the security guard vehicle!

Where should an attacker deploy sniffing stations?



Intersections

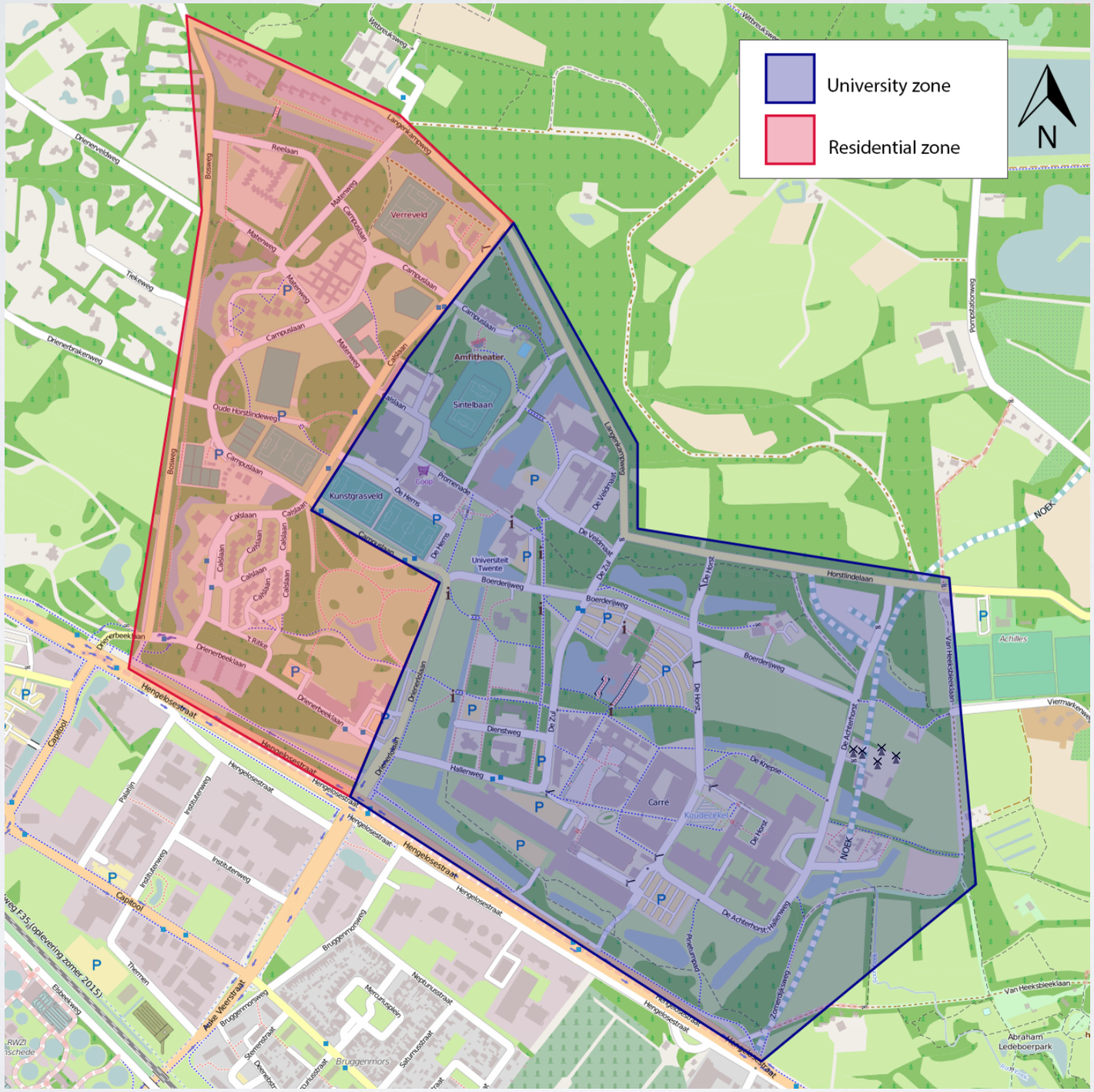


Busiest intersections

Highest degree

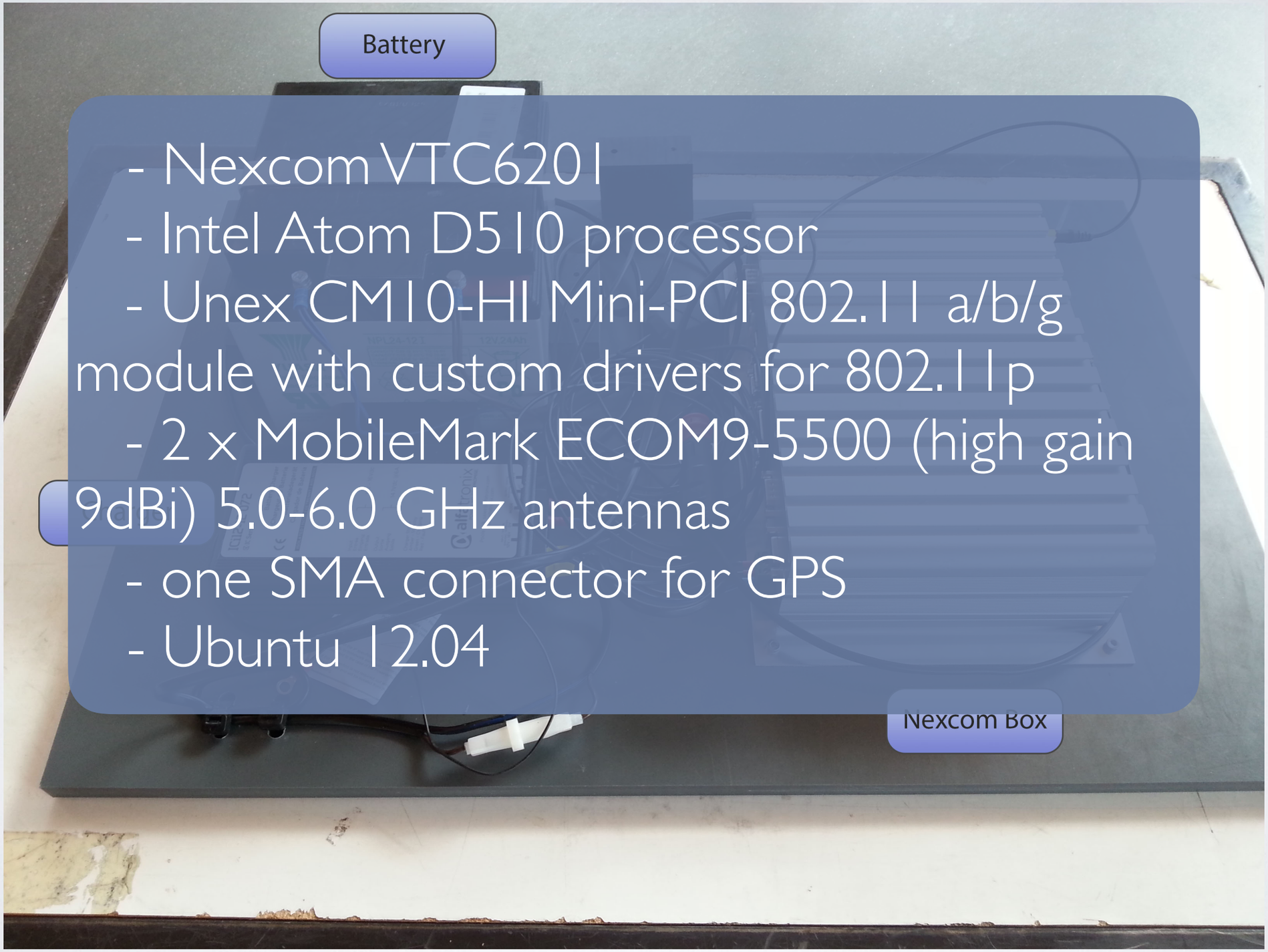
Articulation points

ZONE-LEVEL TRACKING



EXPERIMENTAL SETUP (1/4)

EXPERIMENTAL SETUP (1/4)



EXPERIMENTAL SETUP (2/4)

EXPERIMENTAL SETUP (3/4)

EXPERIMENTAL SETUP (4/4)

<u>Intersection A</u>

Ground floor

75 m from intersection

2 x Smarteq V09/54 antennas (9 dBi gain)

<u>Intersection B</u>

1st floor

110 m from intersection

2 x Smarteq V09/54 antennas (9 dBi gain)

The equipment was deployed for

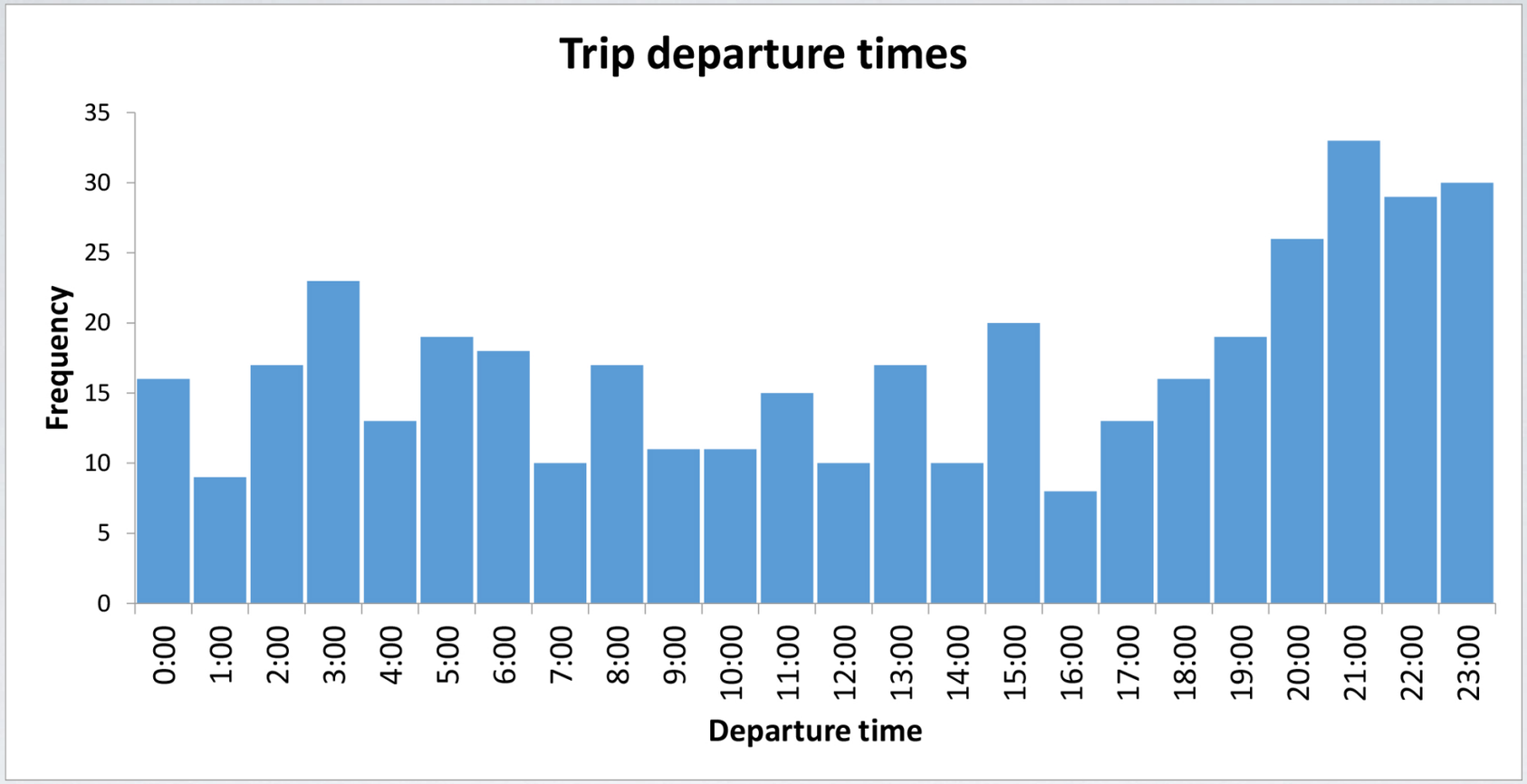
16 days

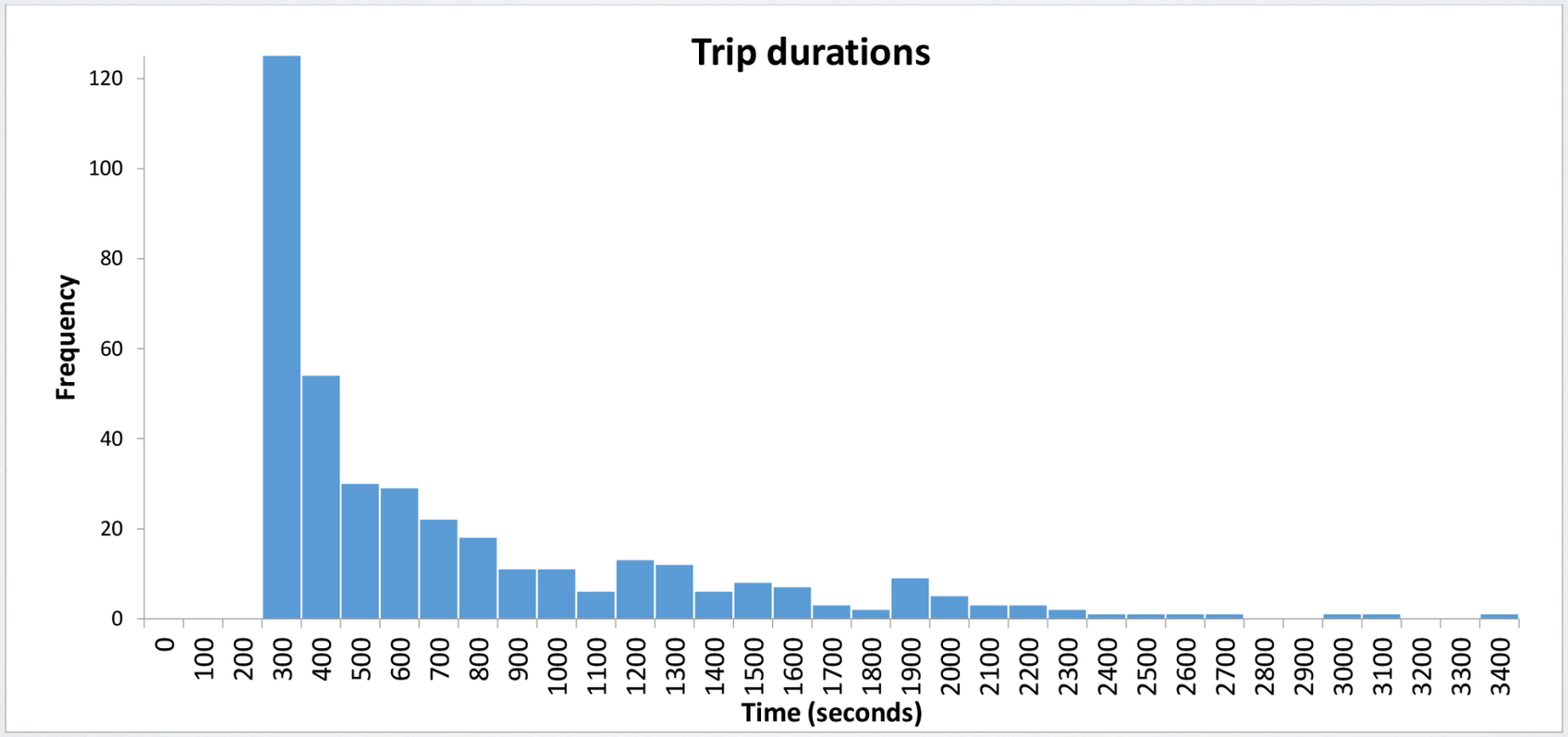
during which the vehicle transmitted

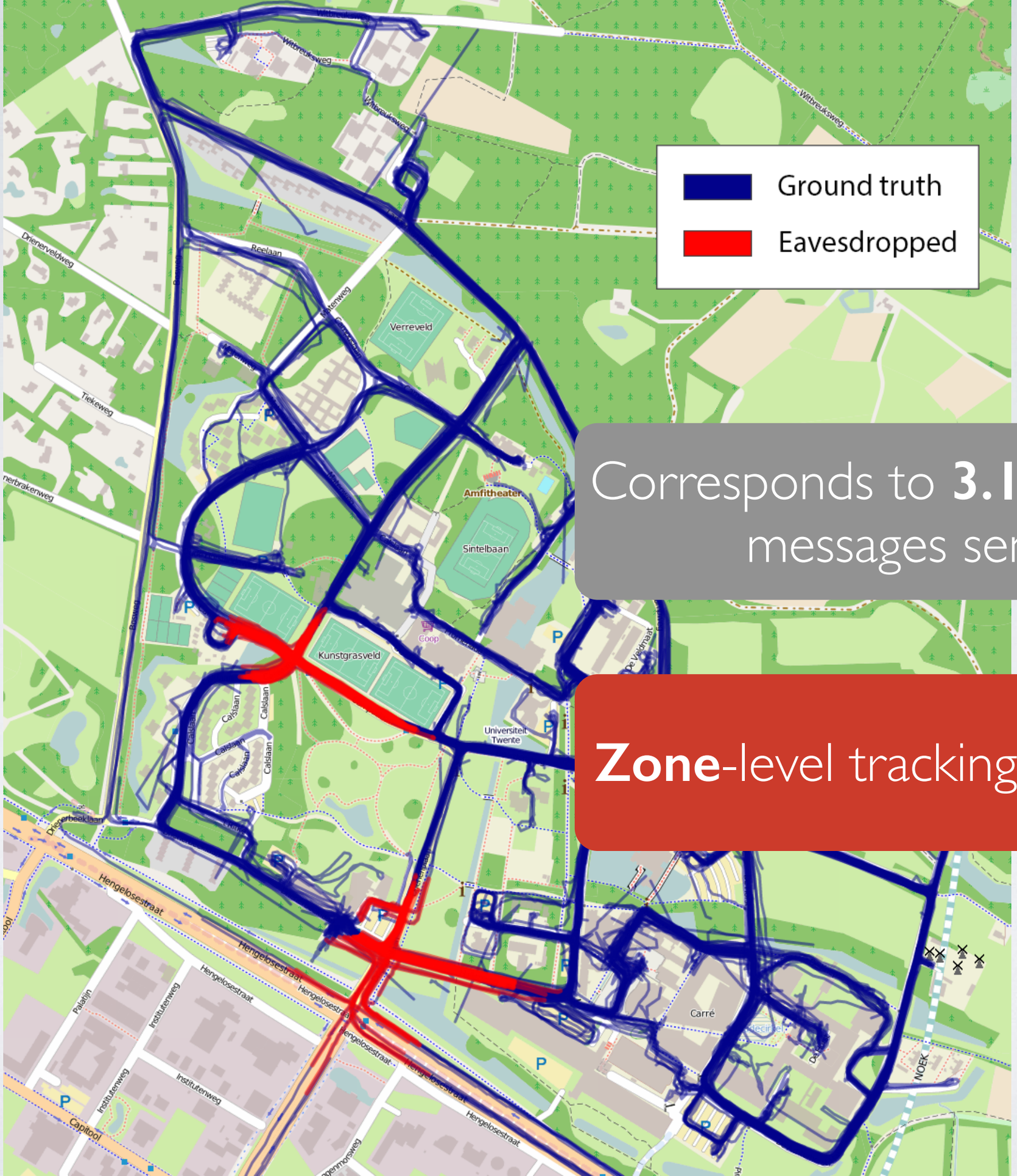
2,734,691 messages

and we eavesdropped on

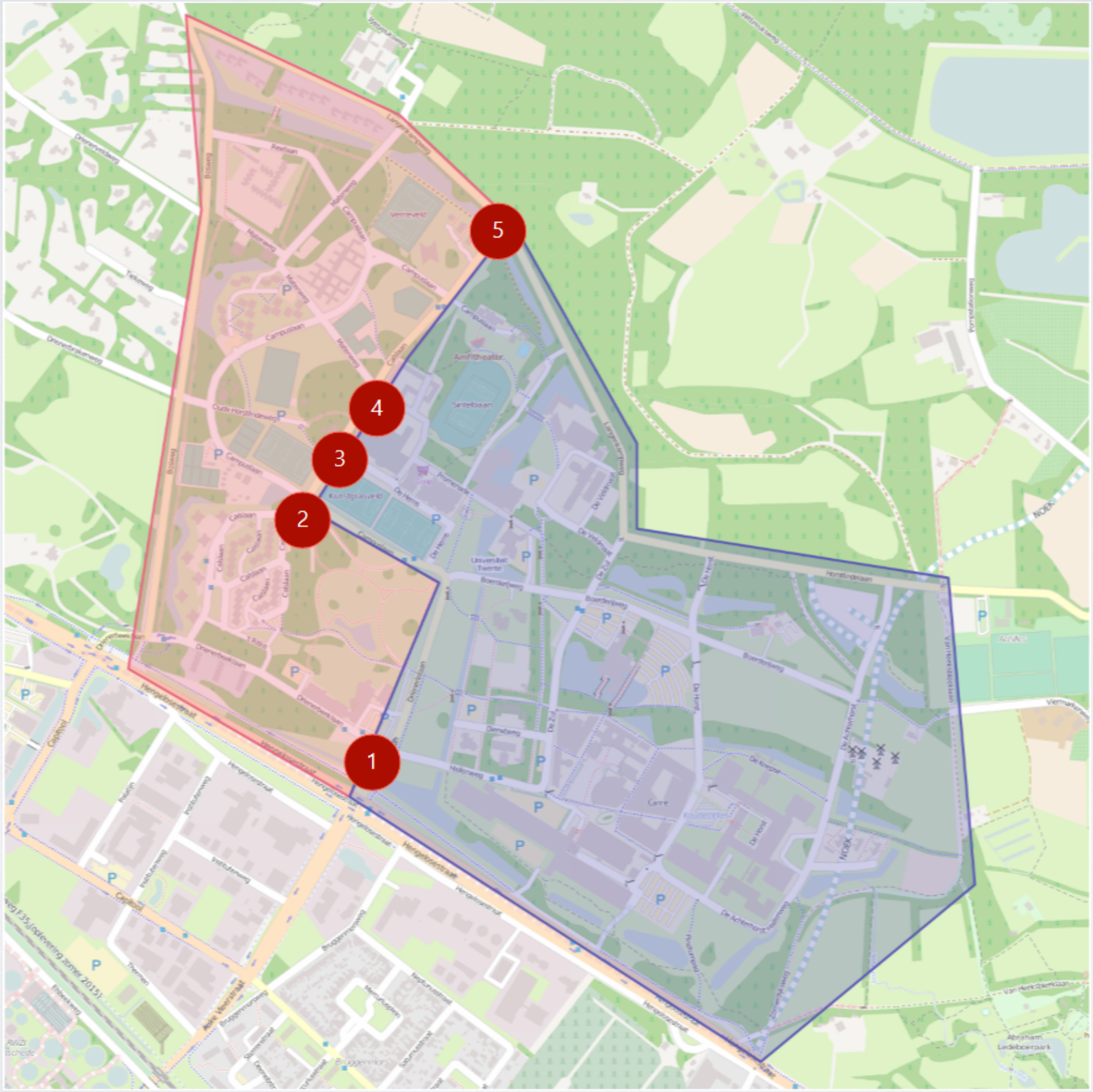
68,542 messages


Trip departure times
Frequency
35
30
25
20
15
10
5
0
0:00
1:00
2:00
3:00
4:00
5:00
6:00
7:00
8:00
9:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
Departure time


Trip durations
Frequency
120
100
80
60
40
20
0
0
100
200
300
400
500
600
700
800
900
1000
1100
1200
1300
1400
1500
1600
1700
1800
1900
2000
2100
2200
2300
2400
2500
2600
2700
2800
2900
3000
3100
3200
3300
3400
Time (seconds)

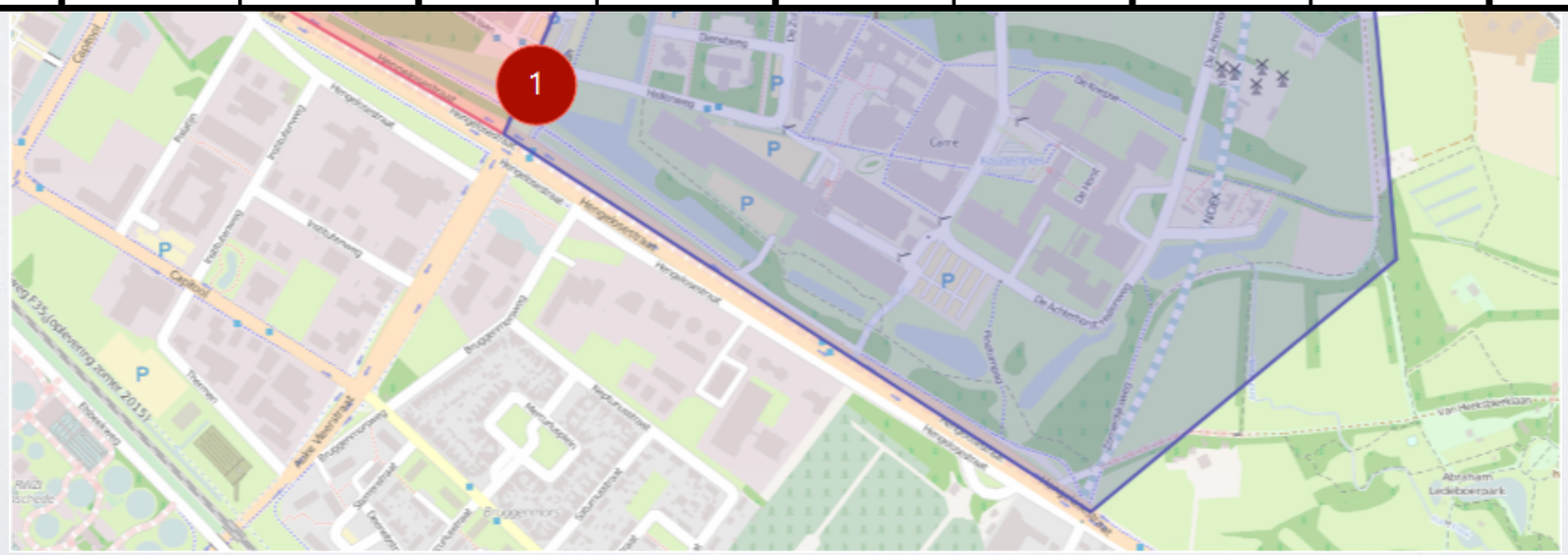

Ground truth
Eavesdropped
Corresponds to **3.17%** of all messages sent
Zone-level tracking: **72.82%**
Witbreuksweg
Drienerveldweg
Reelaan
Verreveld
Trekeweg
Amfitheater
Sintelbaan
Kunstgrasveld
Universiteit Twente
Calslaan
Hengelosestraat
Instituutenweg
Carré
Capitool

TRACKING ACCURACY (MLZ)

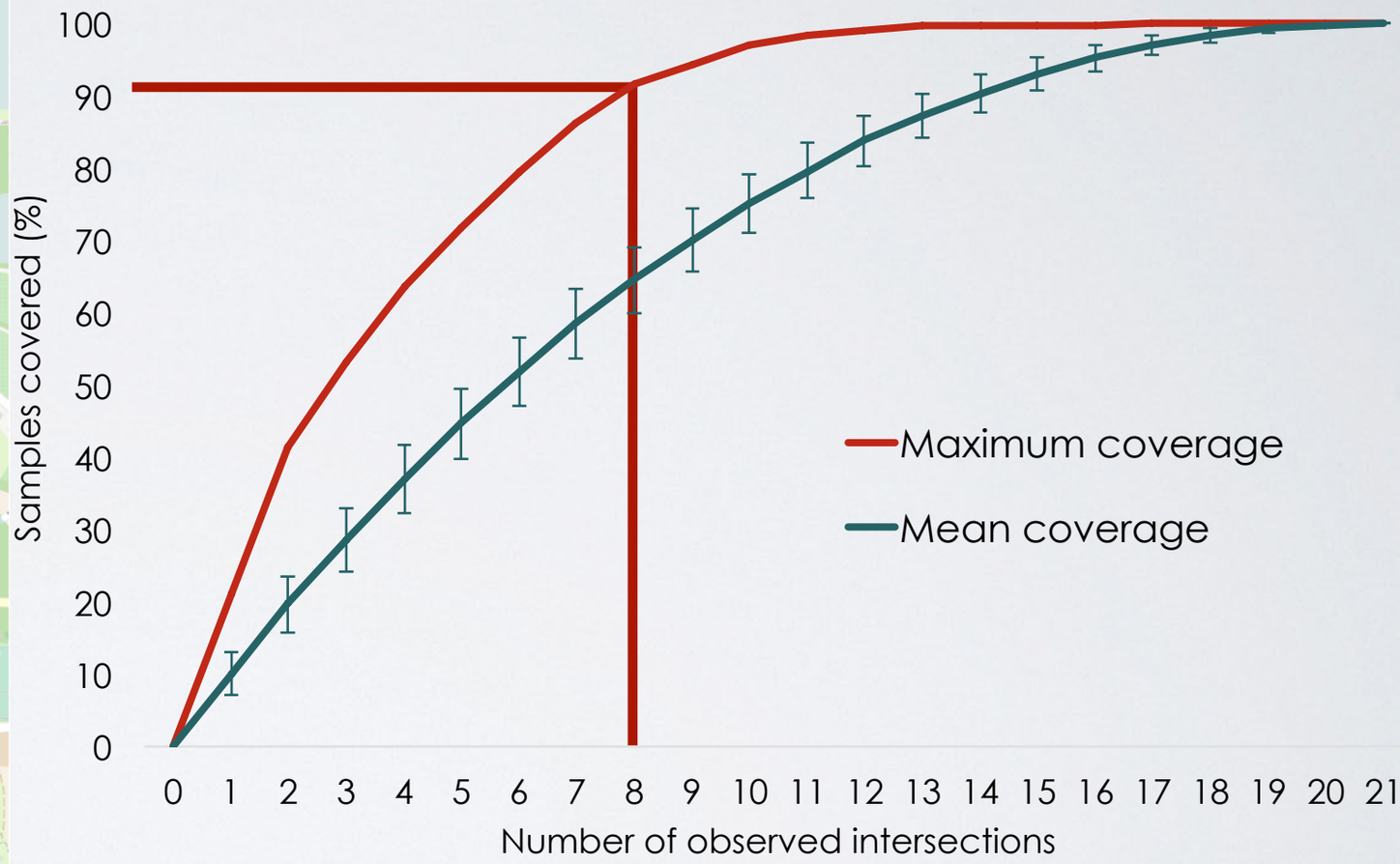


TRACKING ACCURACY (MLZ)

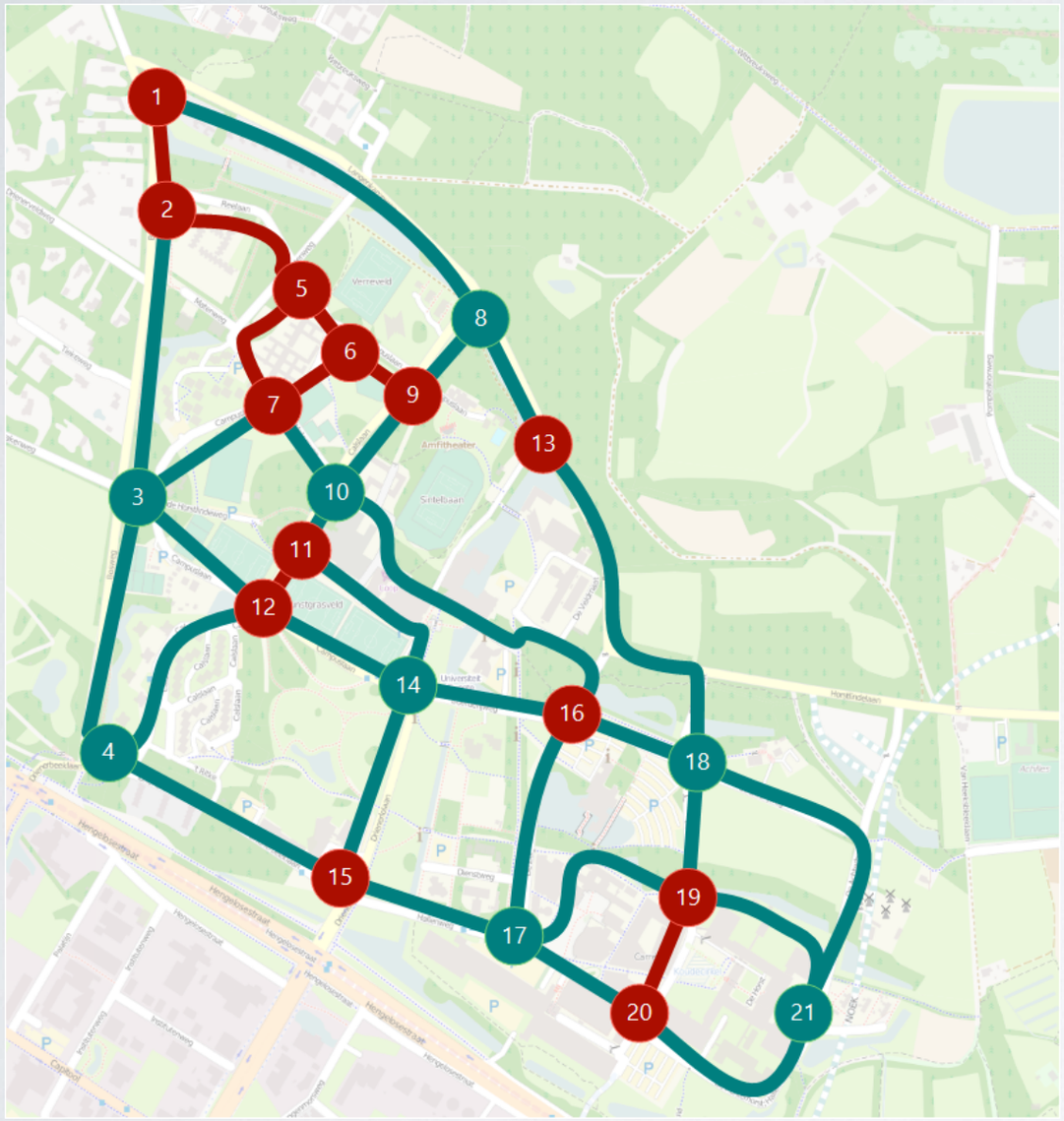
# of intersections	1		2		3		4		5	
	1	61.12%	1-2	72.82%	1-2-3	81.40%	1-2-3-4	84.26%	1-2-3-4-5	95.28%
	2	67.49%	1-3	73.42%	1-2-4	78.96%	1-2-3-5	89.51%		
	3	58.10%	1-4	67.41%	1-2-5	81.53%	1-2-4-5	86.41%		
	4	52.53%	1-5	69.98%	1-3-4	73.15%	1-3-4-5	86.58%		
	5	54.85%	2-3	73.32%	1-3-5	77.44%	2-3-4-5	87.29%		
			2-4	71.76%	1-4-5	74.33%				
			2-5	78.62%	2-3-4	77.38%				
			3-4	61.44%	2-3-5	83.74%				
			3-5	67.66%	2-4-5	82.09%				
			4-5	59.10%	3-4-5	72.50%				
average		58.82%		69.55%		78.25%		86.81%		95.28%

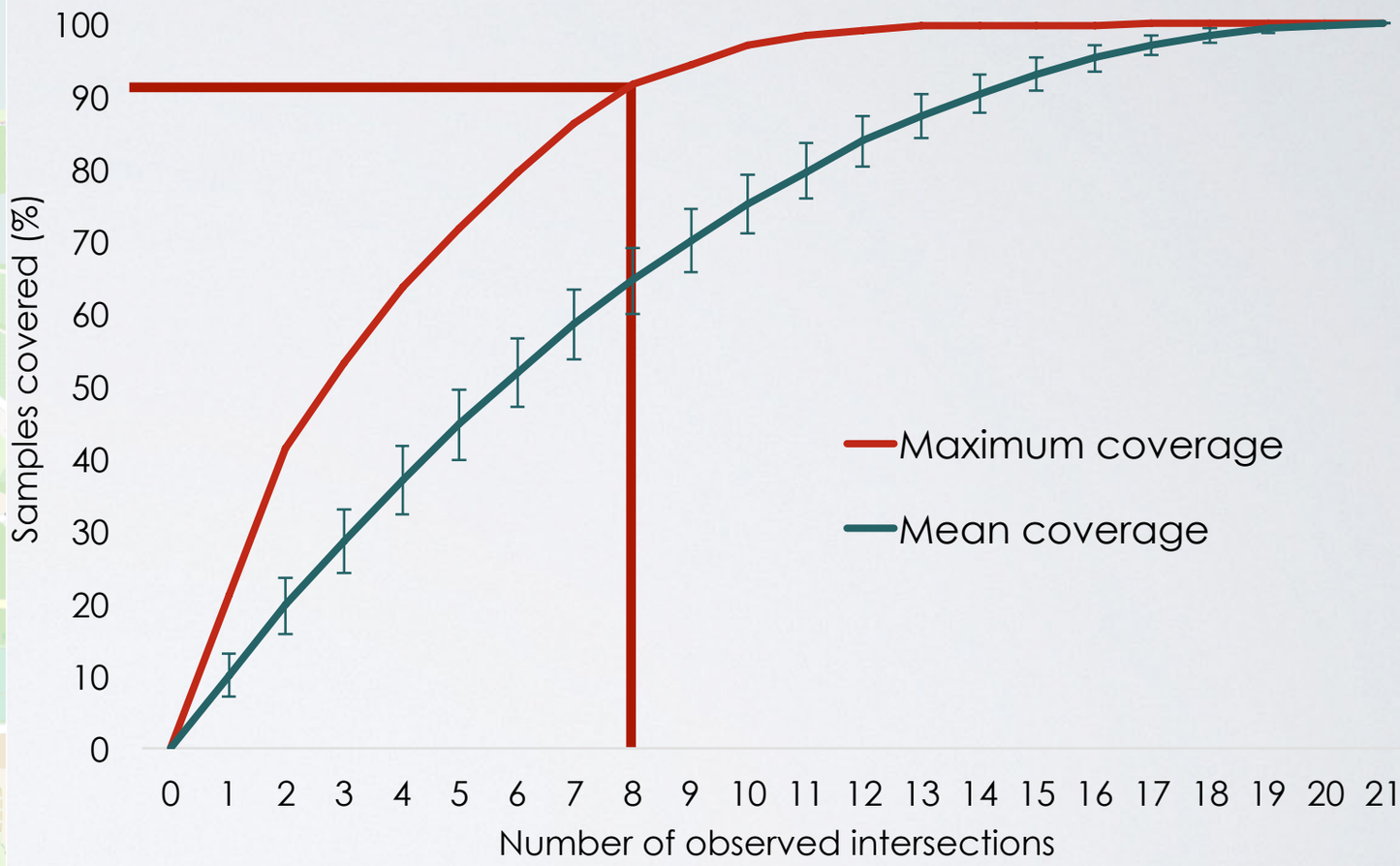


TRACKING ACCURACY (MLR)



TRACKING ACCURACY (MLR)





Can we

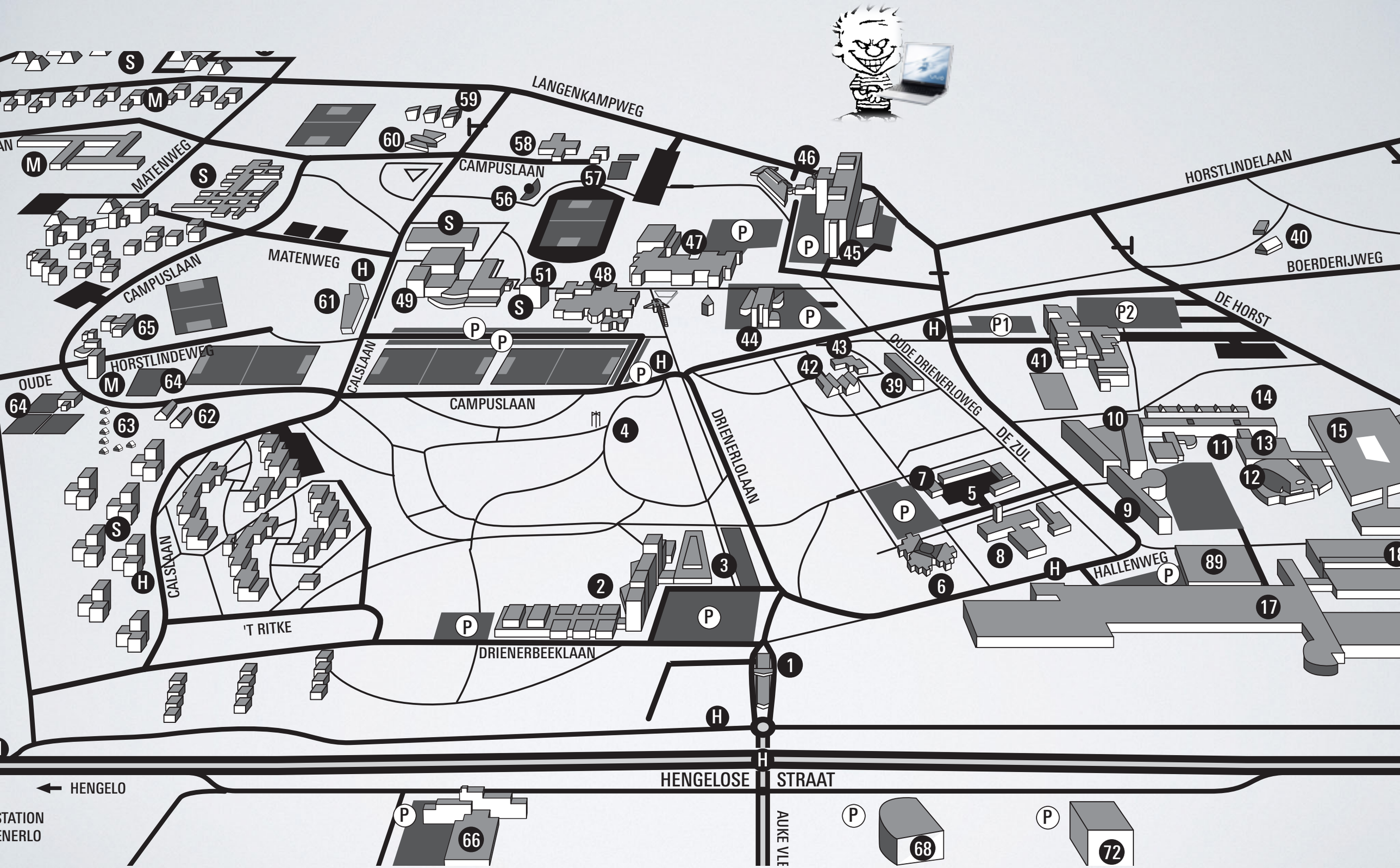
tracking?

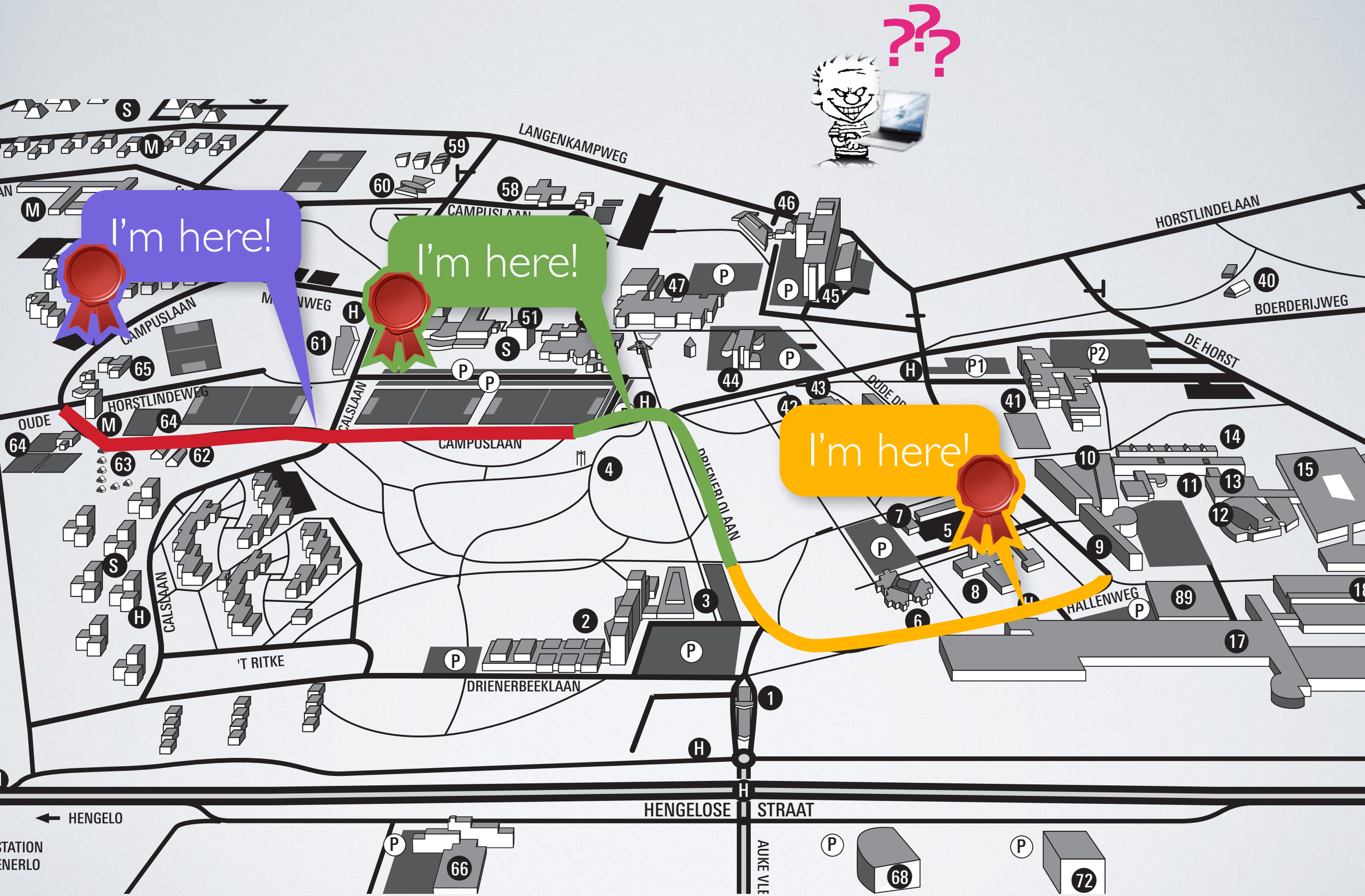
CANDIDATE SOLUTIONS

- Cloaking/Fuzzing location
- Anonymous credentials
- Encryption
- Opt-out
- **Pseudonyms**

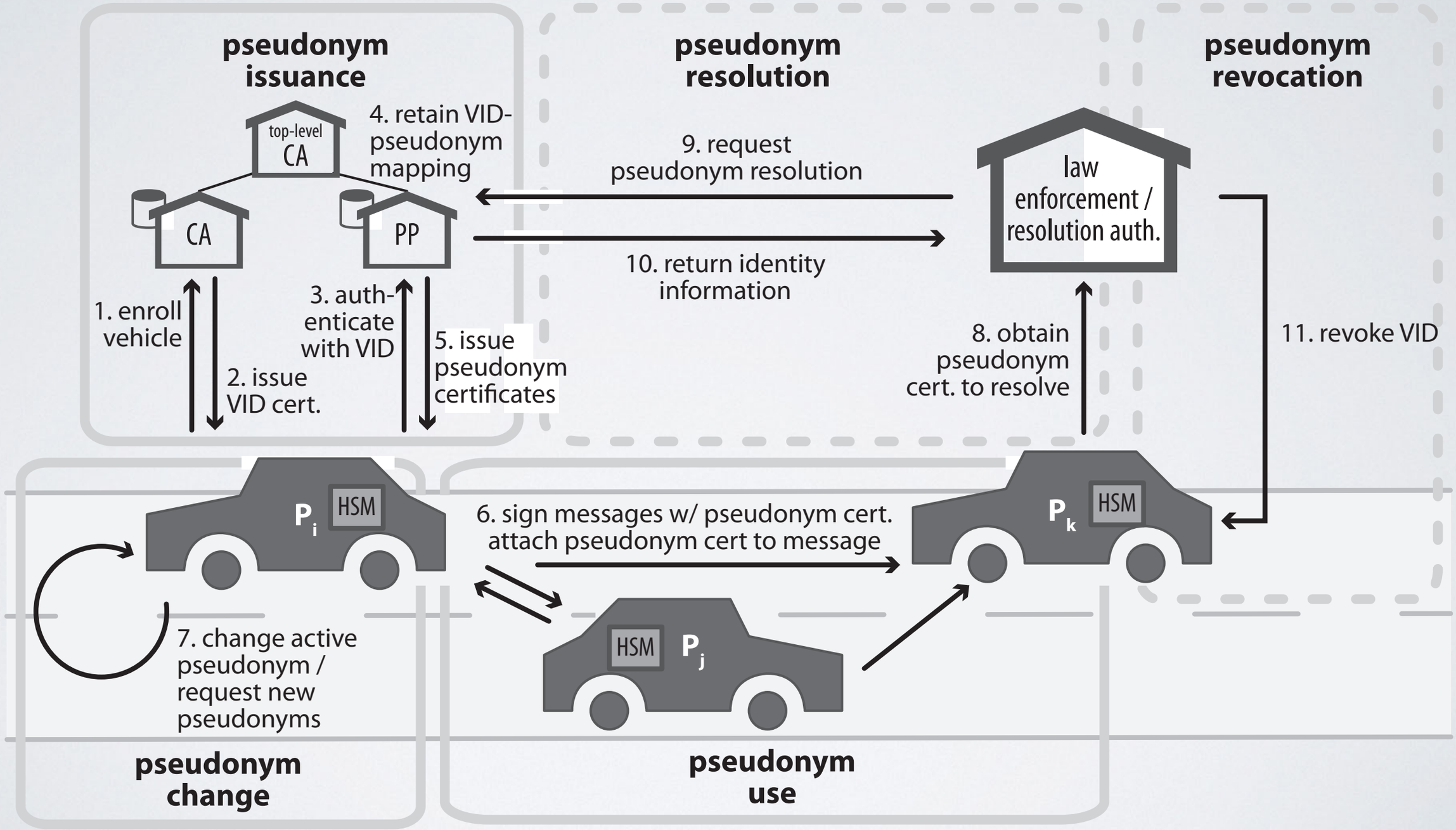
IEEE and ETSI mention the need to

"use a **pseudonym** that cannot be linked to […] the user's true identity" and suggest to change it frequently "[…] to avoid simple correlation between the pseudonym and the vehicle"


LANGENKAMPWEG
MATENWEG
CAMPUSLAAN
HORSTLINDELAAN
BOERDERIJWEG
DE HORST
HORSTLINDEWEG
OUDE
CALSLAAN
OUDE DRIENERLOWEG
DE ZUL
DRIENERLOLAAN
HALLENWEG
'T RITKE
DRIENERBEEKLAAN
HENGELOSE STRAAT
AUKE VLE
HENGELO
STATION
ENERLO
S
M
H
P
P1
P2
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
17
18
39
40
41
42
43
44
45
46
47
48
49
51
56
57
58
59
60
61
62
63
64
65
66
68
72
89

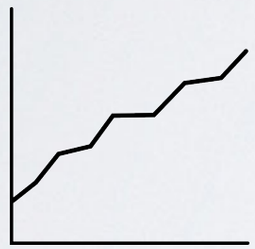

I'm here!
I'm here!
I'm here!
LANGENKAMPWEG
CAMPUSLAAN
HORSTLINDEWEG
OUDE
HORSTLINDELAAN
BOERDERIJWEG
DE HORST
HALLENWEG
'T RITKE
DRIENERBEEKLAAN
HENGELOSE STRAAT
HENGELO
STATION
ENERLO
AUKE VLE

PSEUDONYM LIFECYCLE



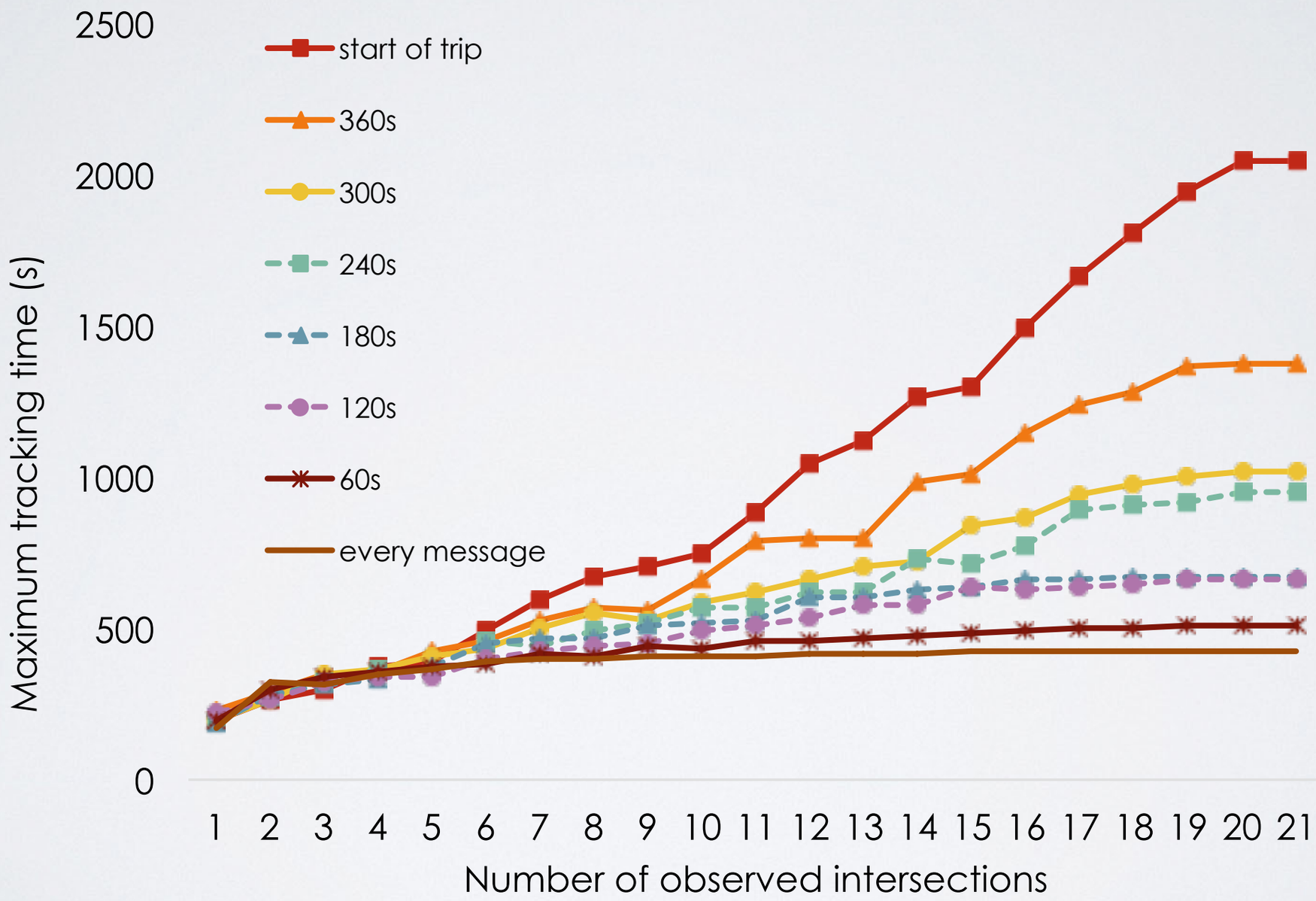
J. Petit et al., "Pseudonym Schemes in Vehicular Networks: A Survey", IEEE Communications Surveys & Tutorials, 2015.

Maximum Tracking Time

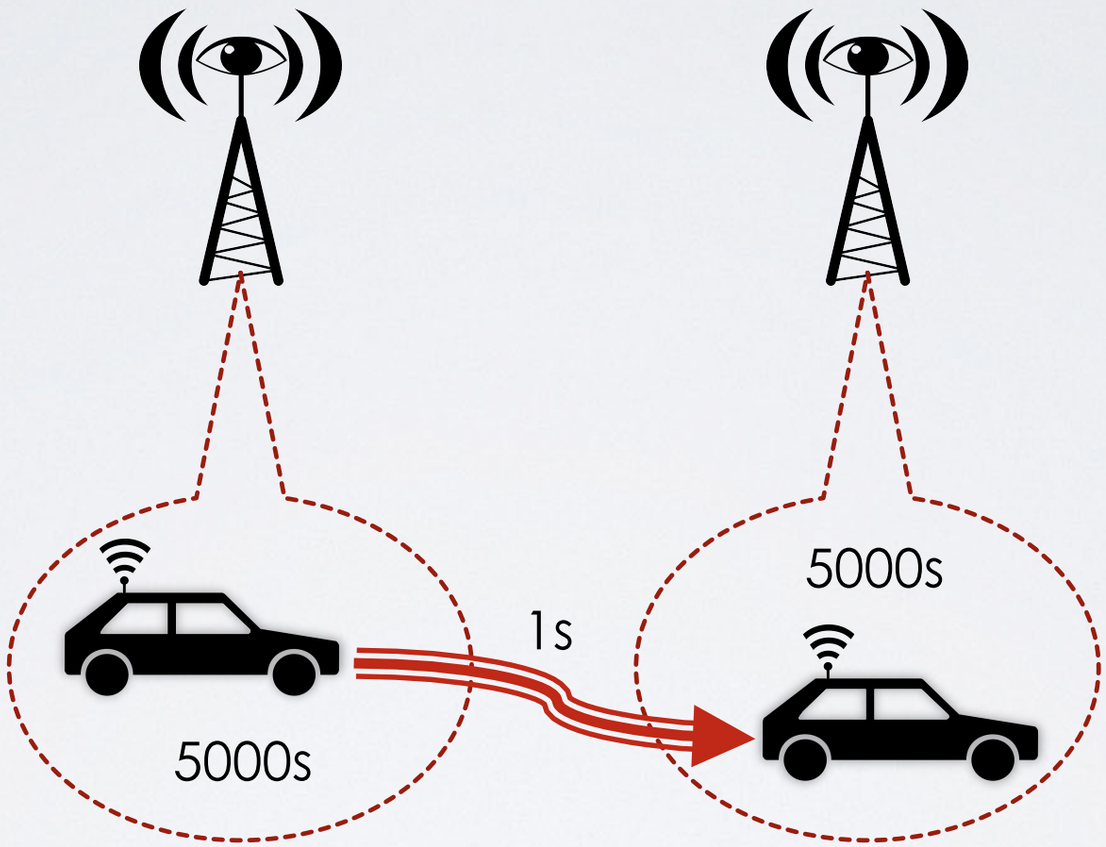


Privacy Loss Function

MAXIMUM TRACKING TIME



But we need to be careful



The MTT might not give a true indication of privacy

PRIVACY LOSS FUNCTION

$$P_{pnm}(t) = \begin{cases} max(P_{pnm}(t-1) - \sum_{i=1}^{N_{veh}} p_i \cdot logp_i, P_{pmax}) & \text{if } t \in T_{upc} \\ 0 & \text{if } t \in T_{obs} \end{cases}$$

Pseudonym changes

$$P_{int}(t) = \begin{cases} max(P_{int}(t-1) - \sum_{j=1}^{N_{road}} p_j \cdot logp_j, P_{rmax}) & \text{if } t \in T_{ui} \\ 0 & \text{if } t \in T_{obs} \end{cases}$$

Unobserved intersections

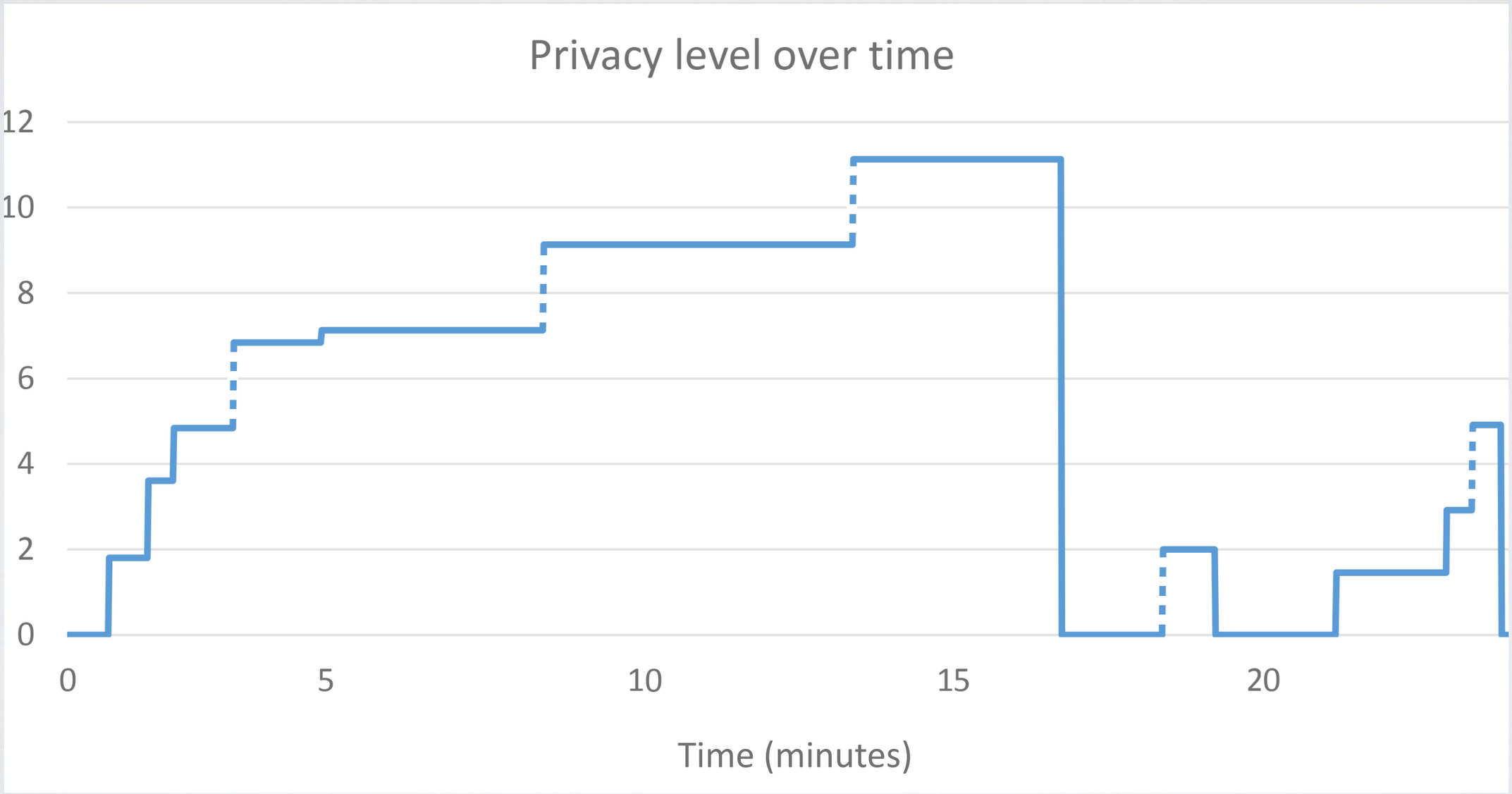
$$P_{road}(t) = \begin{cases} max(P_{road}(t-1) + \lambda(t_{last} - t), P_{dmax}) & \text{if } t \in T_{urs} \\ 0 & \text{if } t \in T_{obs} \end{cases}$$

Time since observation

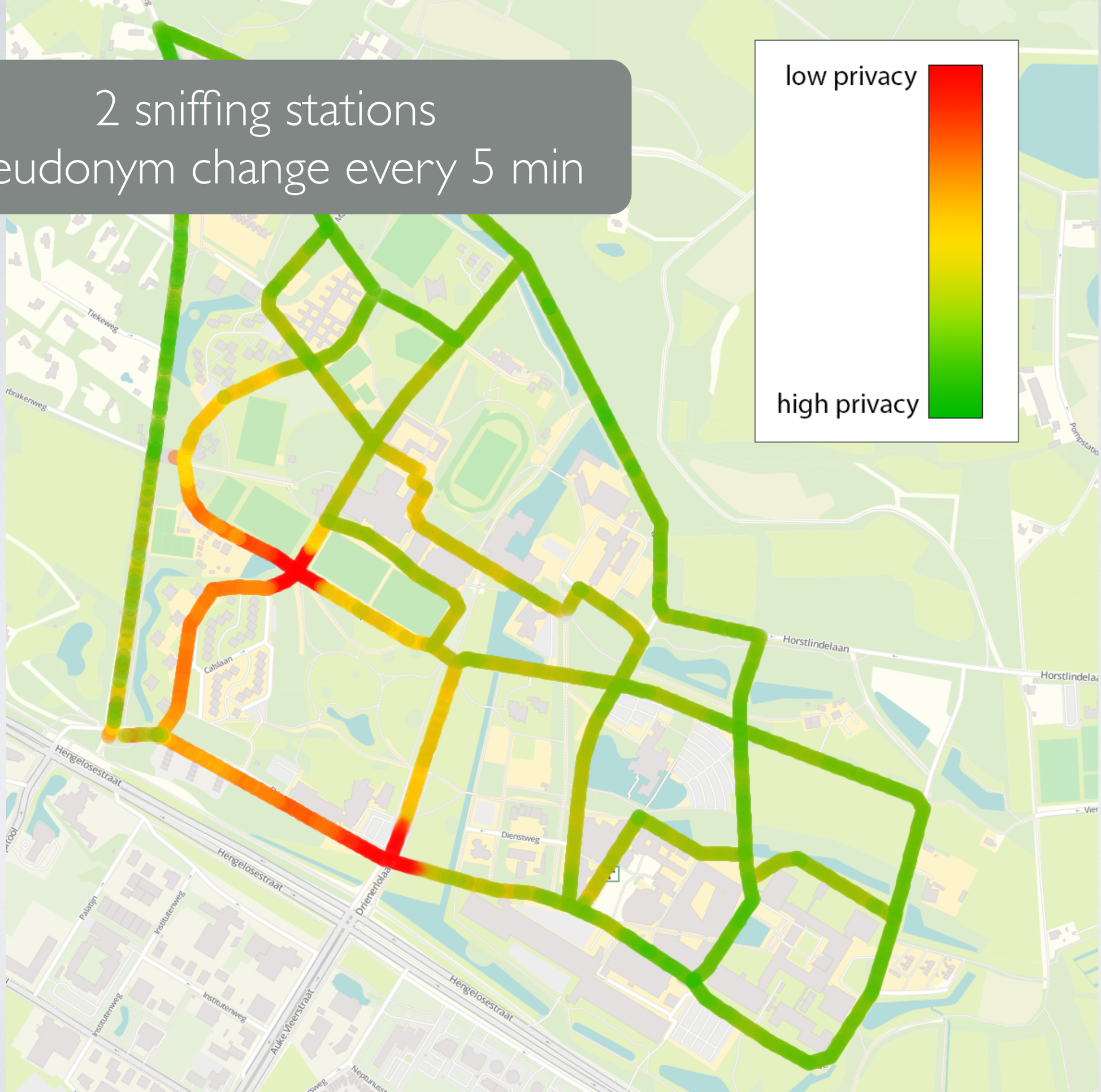
$$P(t) = P_{pnm}(t) + P_{int}(t) + P_{road}(t)$$

Total

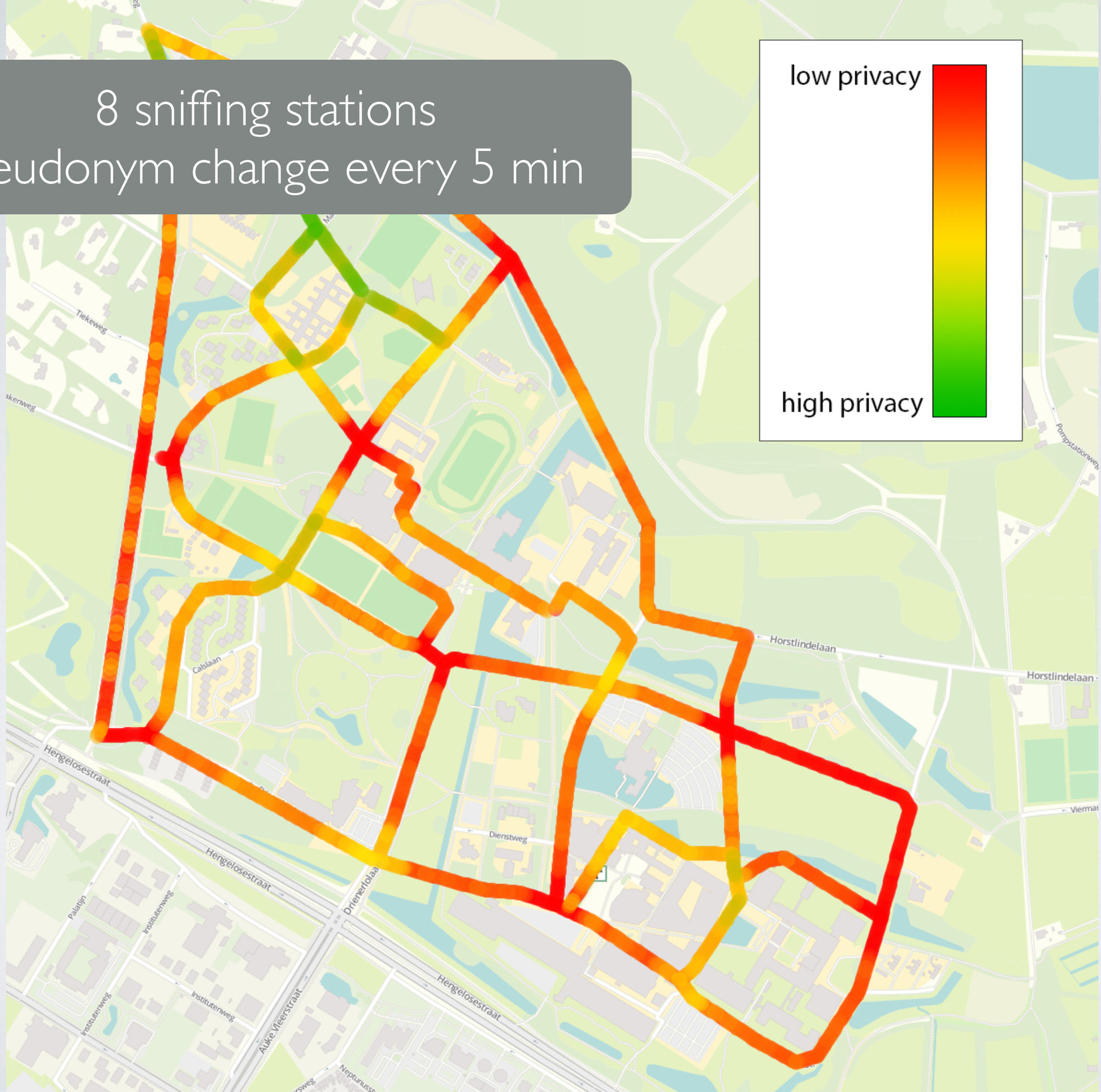
EVOLUTION OF PRIVACY LEVEL



2 sniffing stations
Pseudonym change every 5 min

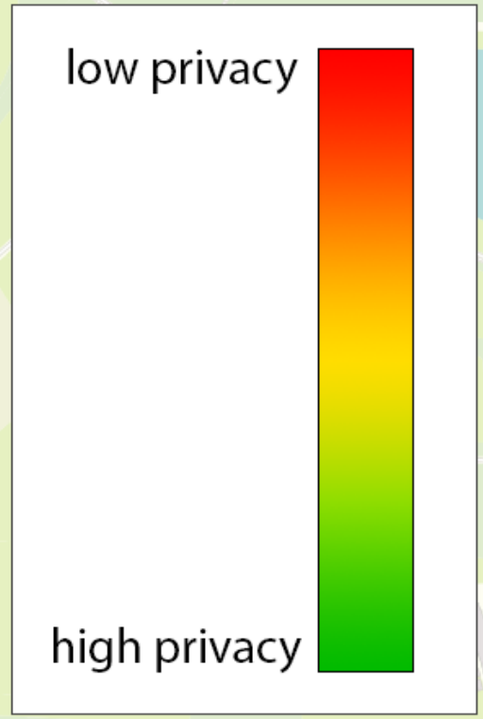


8 sniffing stations
Pseudonym change every 5 min

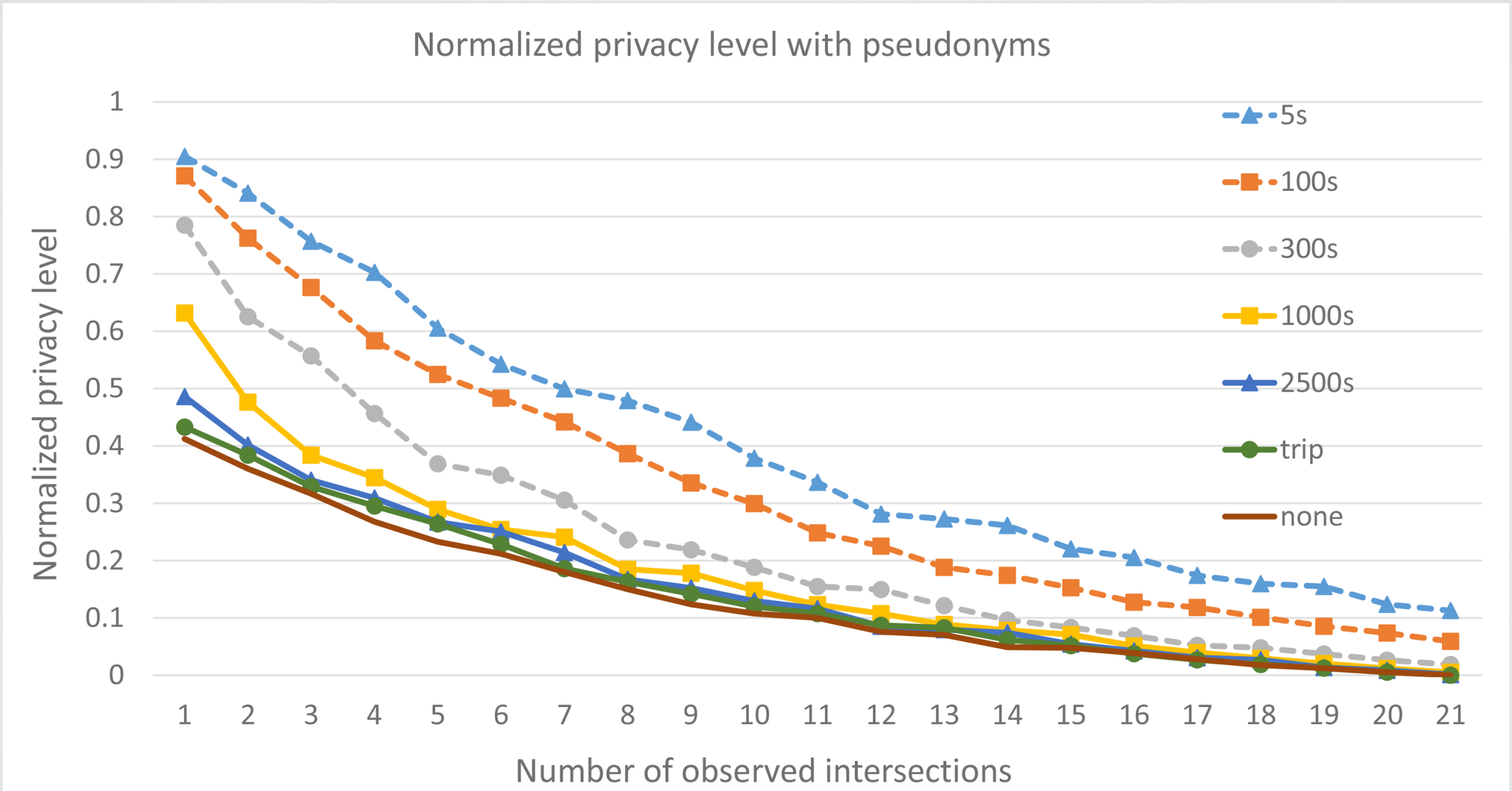


8 sniffing stations
Pseudonym change every 5 min

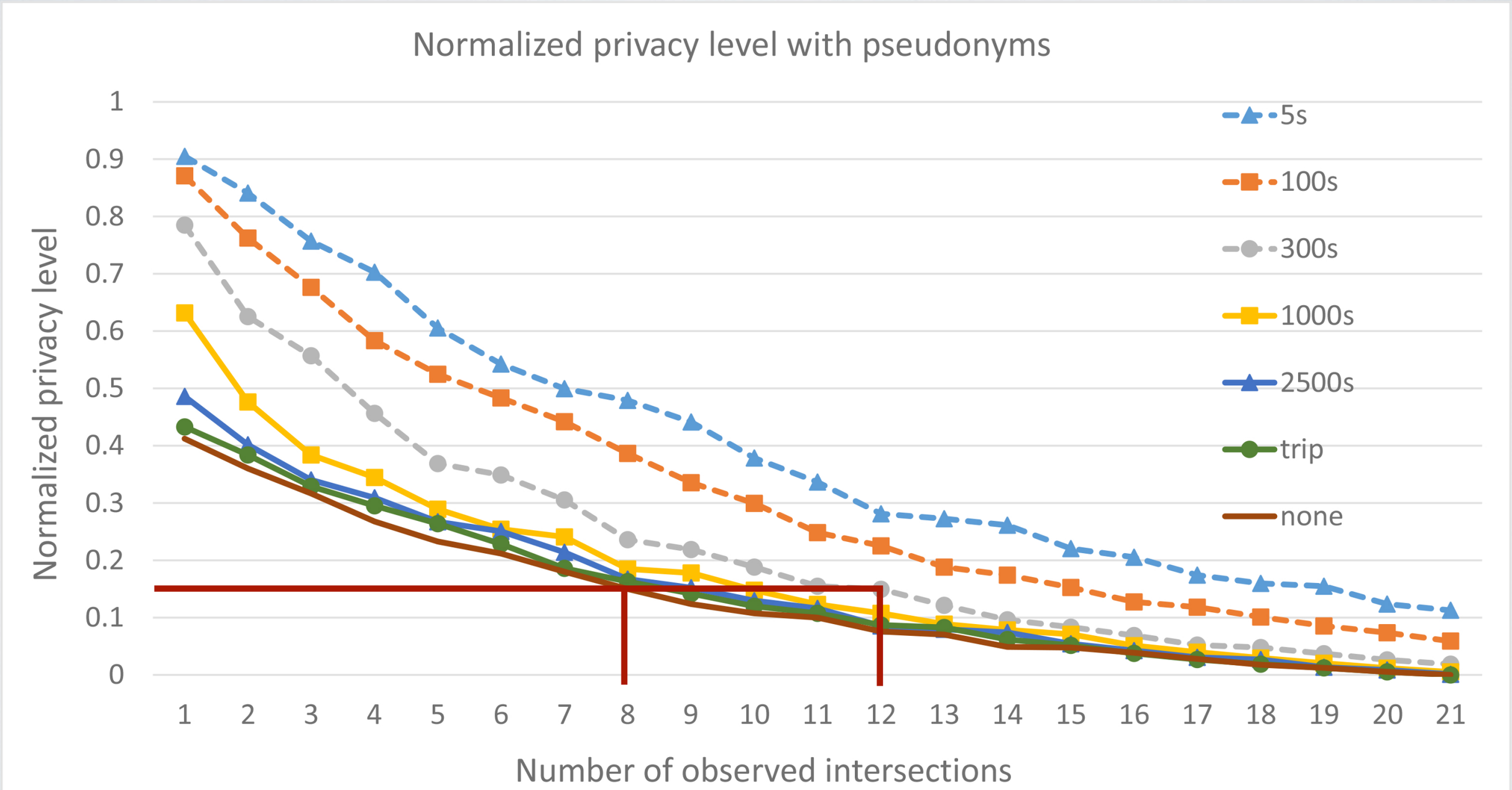
Road-level tracking: **90%**



PSEUDONYM CHANGE STRATEGIES



PSEUDONYM CHANGE STRATEGIES



COST MODEL

#observed intersection	Cost (€)
1	500
2	1000
8	4000
Full campus	10500

6000€/km^2

COST MODEL

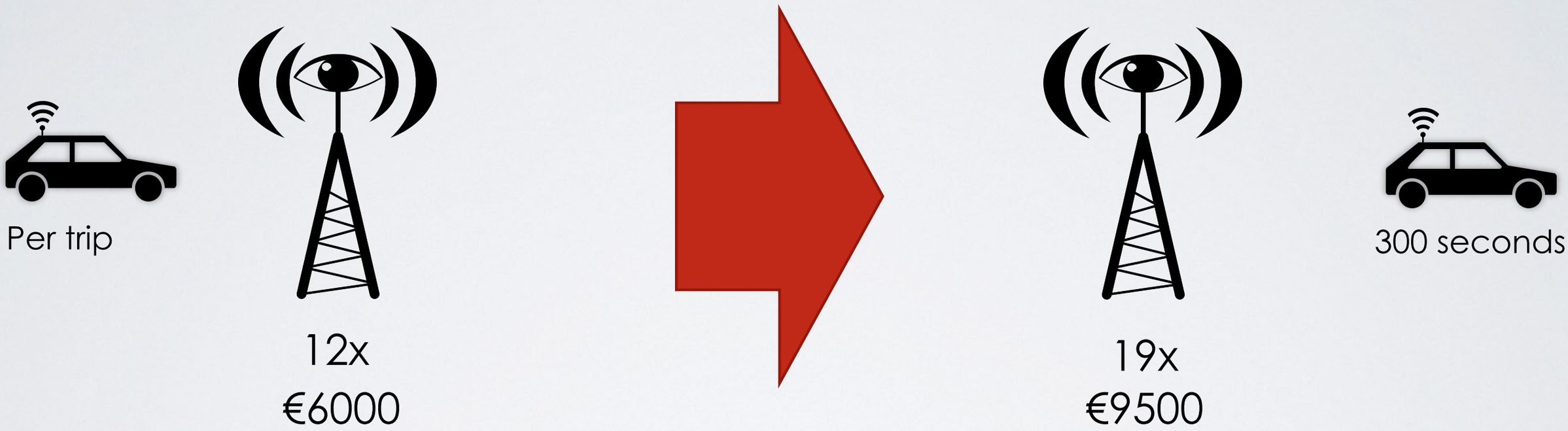
#observed intersection	Cost (€)
1	500
2	1000
8	4000
Full campus	10500

6000€/km^2

Expect price drop!
(Raspberry Pi or SDR:
http://wime-project.net/)

For example

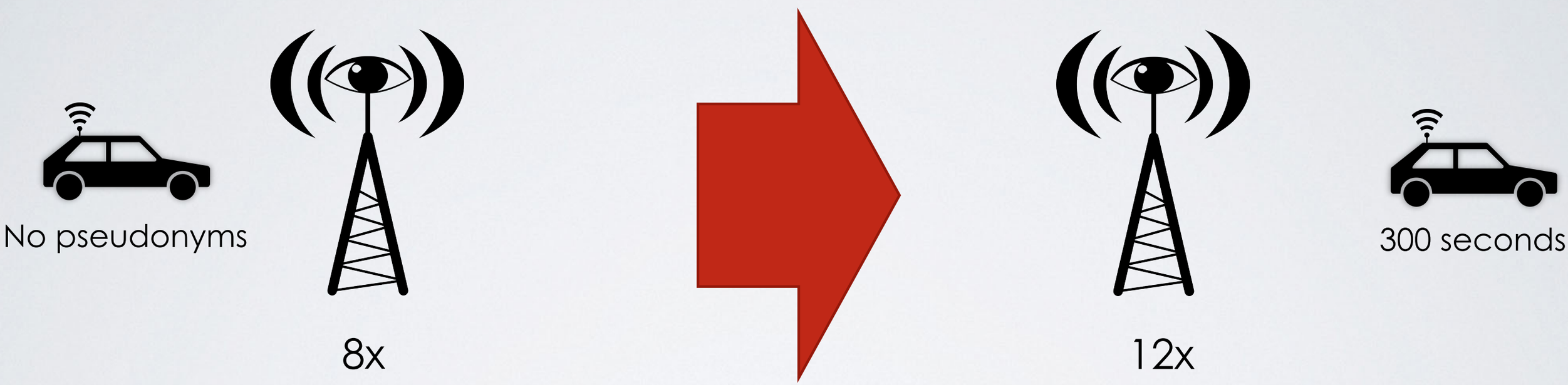
To get a maximum tracking time of 1000 seconds



An attacker need 58% more resources

For example

To get the same privacy level from our flux function



An attacker need 50% more resources

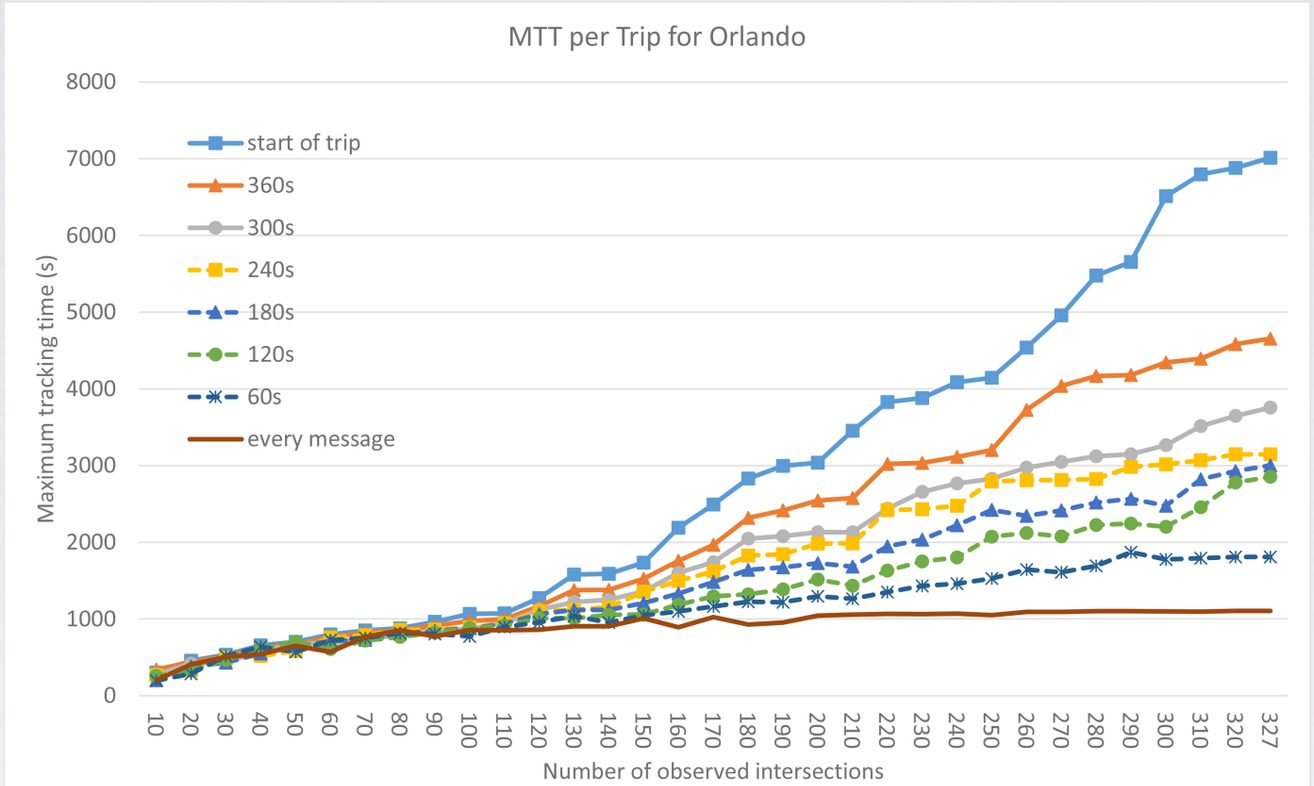
CONCLUSION OF THE EXPERIMENT

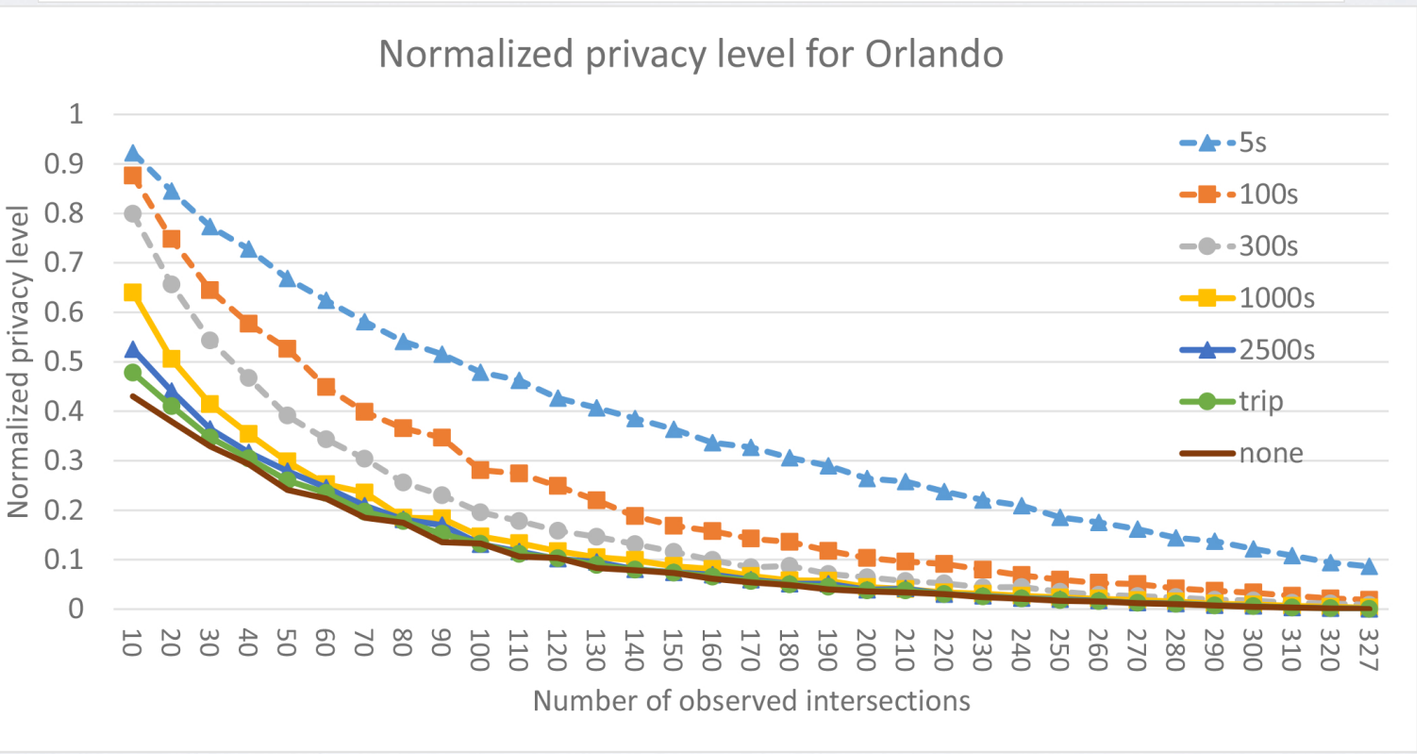
- **Everyone** can deploy a surveillance system

- Privacy cost model

- Need additional studies on pseudonym change strategy

LARGE-SCALE SCENARIO





PRIVACY-PRESERVING ROAD NETWORK?

BLACK HAT SOUND BYTES.

1. **Everyone** can deploy a surveillance system to track connected vehicles. It is **cheap** and **easy**.

2. Countermeasures exist to **mitigate** the risk.