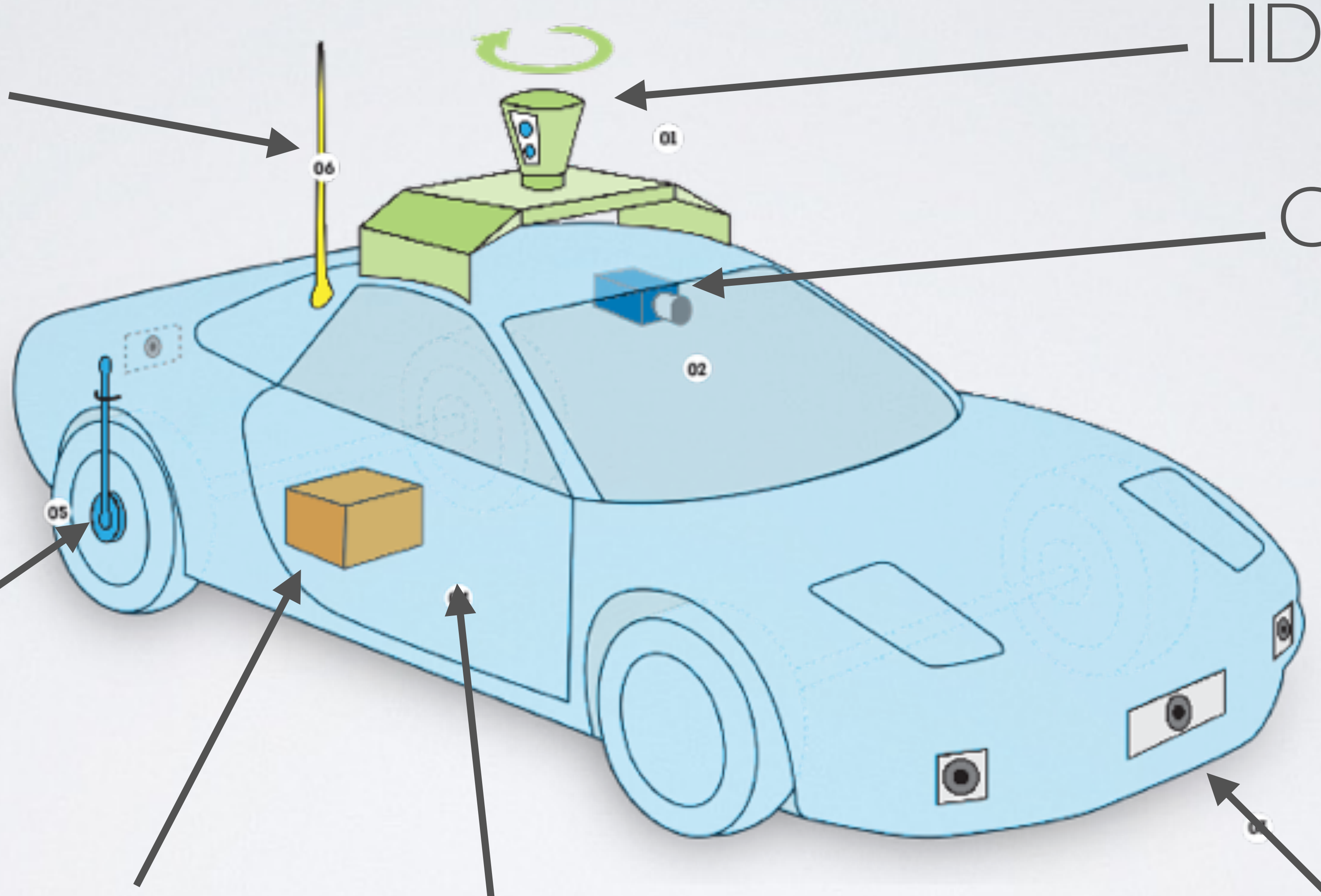
SELF-DRIVING AND CONNECTED CARS: FOOLING SENSORS AND TRACKING DRIVERS

Jonathan Petit

Security Innovation® THE APPLICATION SECURITY COMPANY

UNIVERSITY OF TWENTE.

AUTOMATED/CONNECTED VEHICLE



GPS, 802.11p

LIDAR

Camera

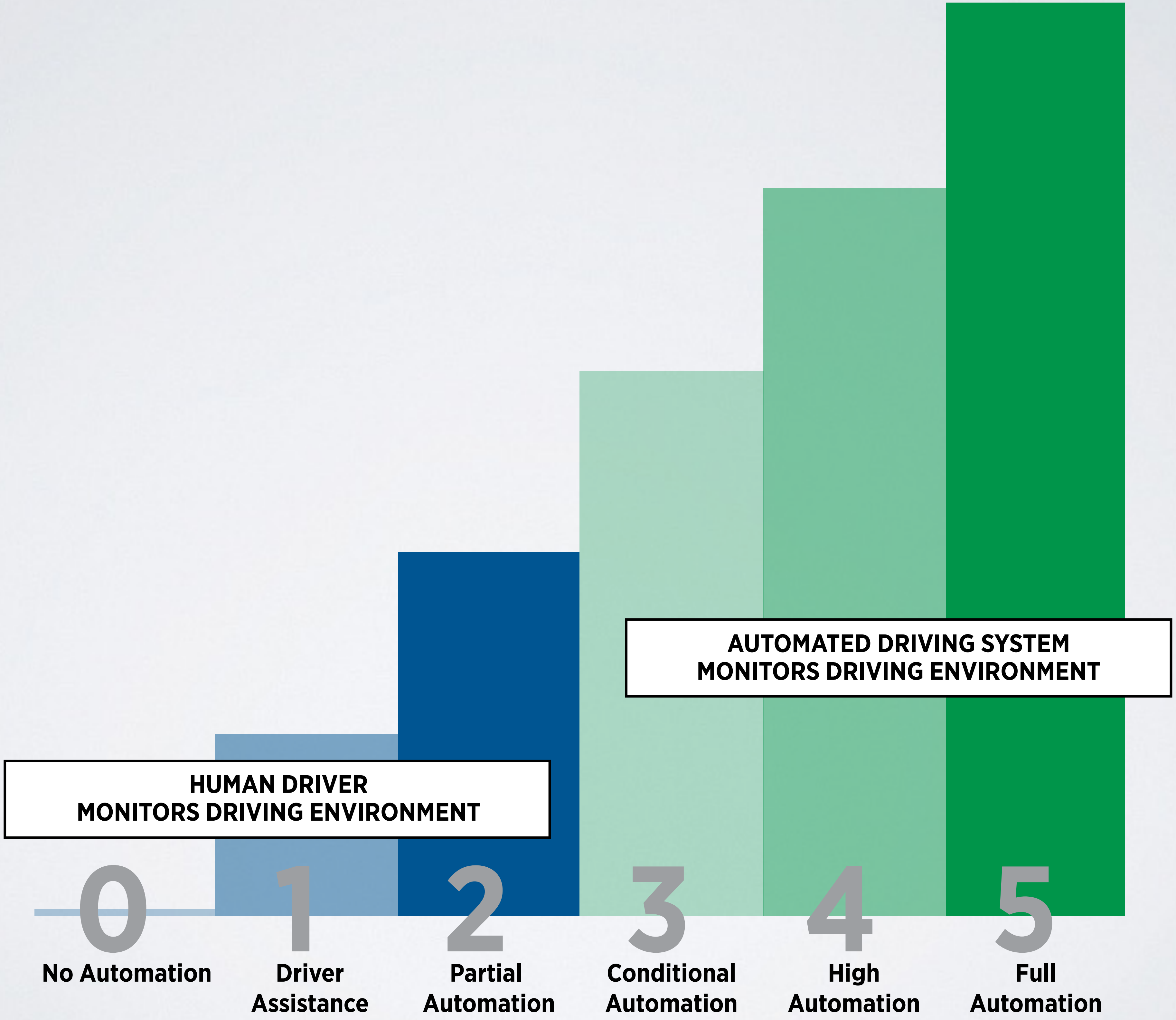
wheel encoder

On-Board Unit, emaps

ultrasonic sensors

RADAR

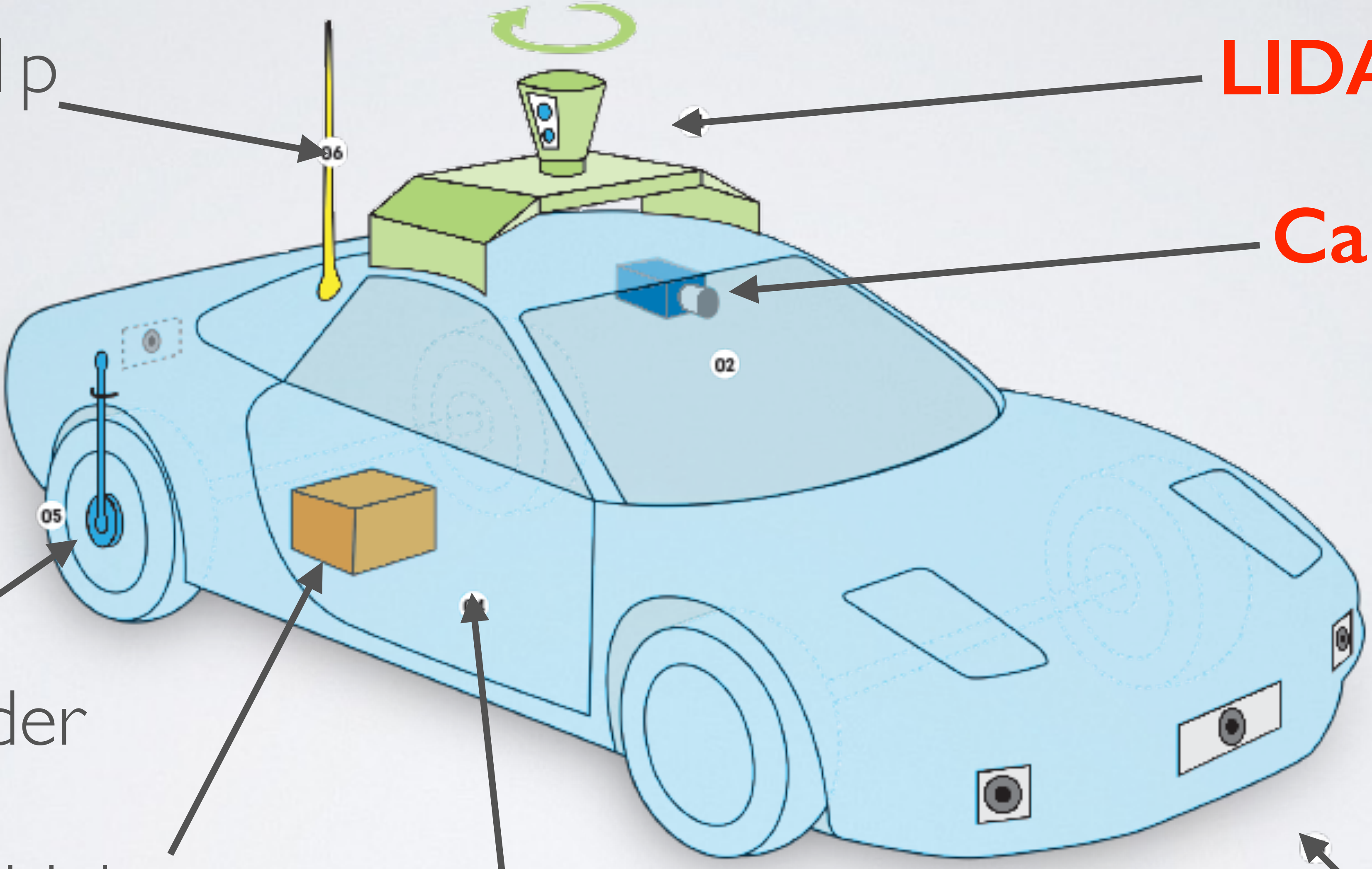
LEVELS OF DRIVING AUTOMATION (SAE J3016)



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

Jonathan Petit, Bas Stottelaar, Michael Feiri, Frank Kargl

ATTACKING AUTONOMOUS VEHICLE SENSORS



GPS, 802.11p

LIDAR

Camera

wheel encoder

On-Board Unit, emaps

ultrasonic sensors

RADAR

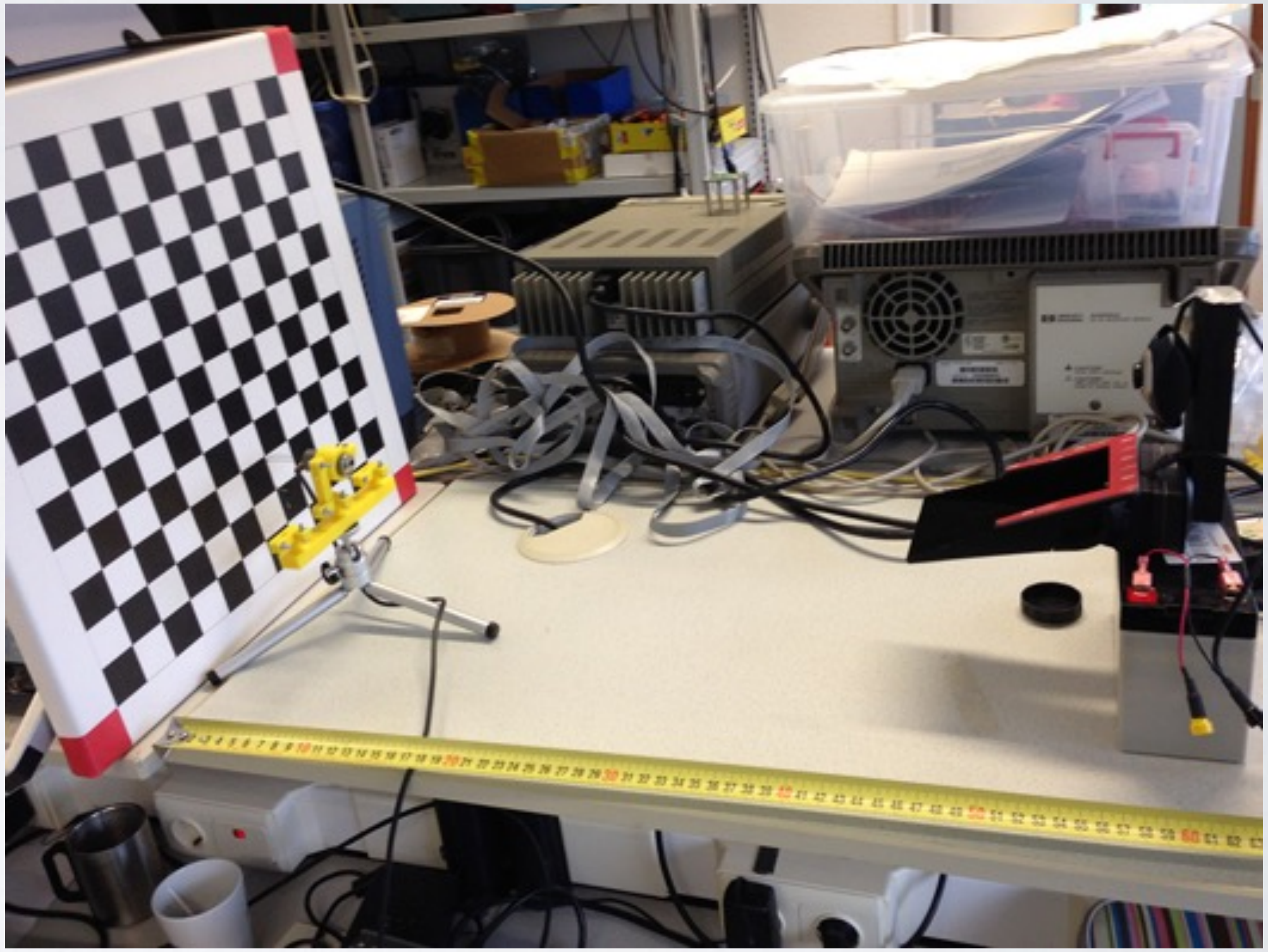
CAMERA

- MobilEye C2-270
- Features:
  - Lane departure
  - Rear collision alert
  - Pedestrian alert

Aptina MT9V024 CMOS
Red/Clear camera
752x480 at 60 FPS

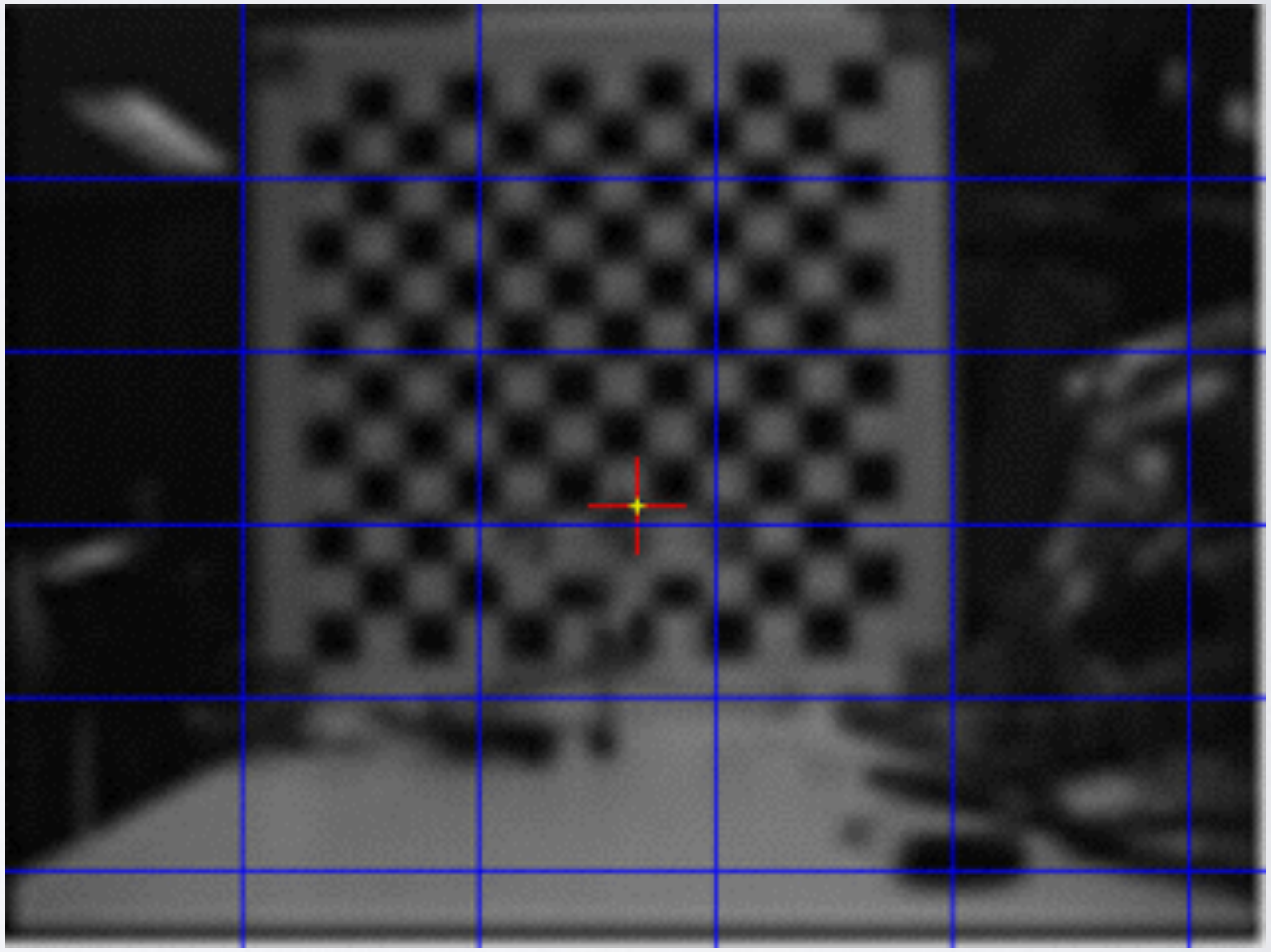
ATTACKING CAMERA

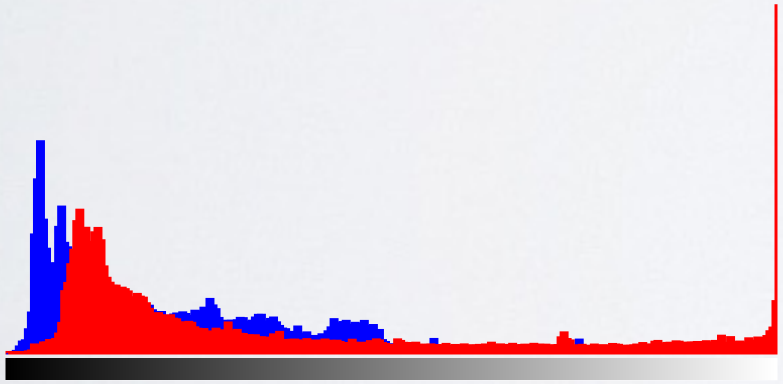
- Attacks:
  - Jamming
  - **Blinding**
  - Scenery attack
- Equipments:
  - Light sources (LED, laser)
  - Screen



ATTACKING CAMERA - SENSITIVITY

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

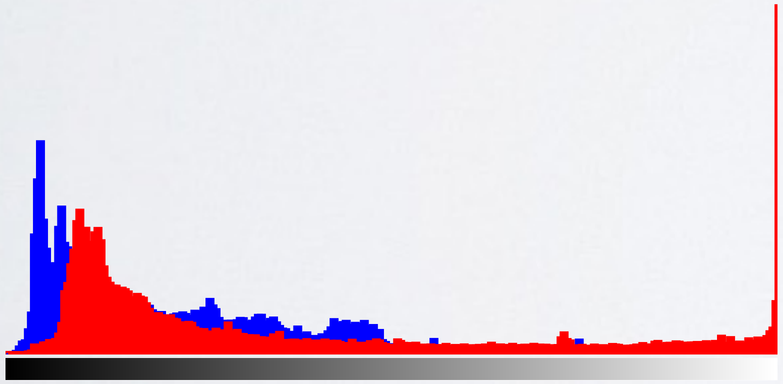




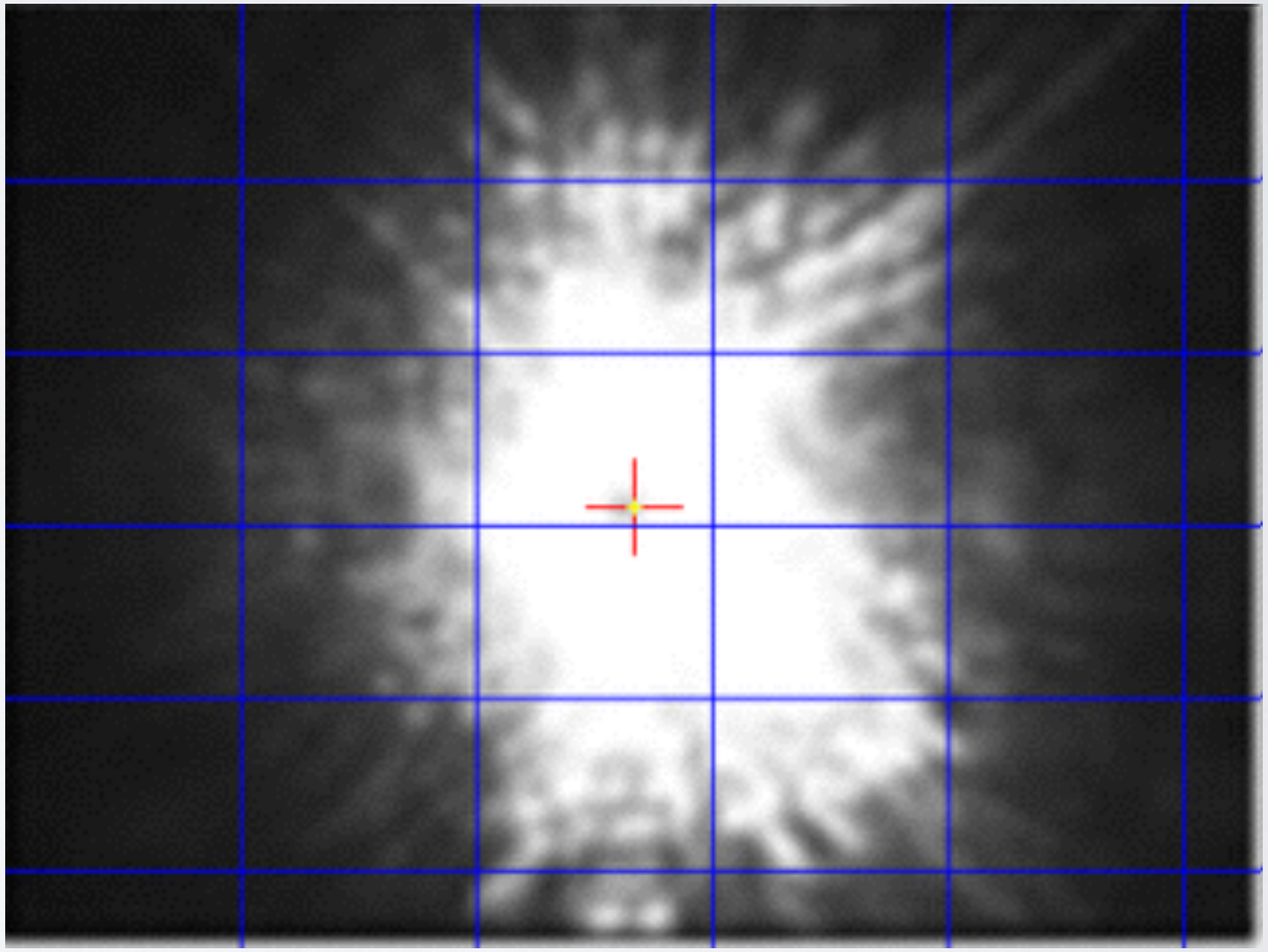
Tonal distribution

ATTACKING CAMERA - SENSITIVITY

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



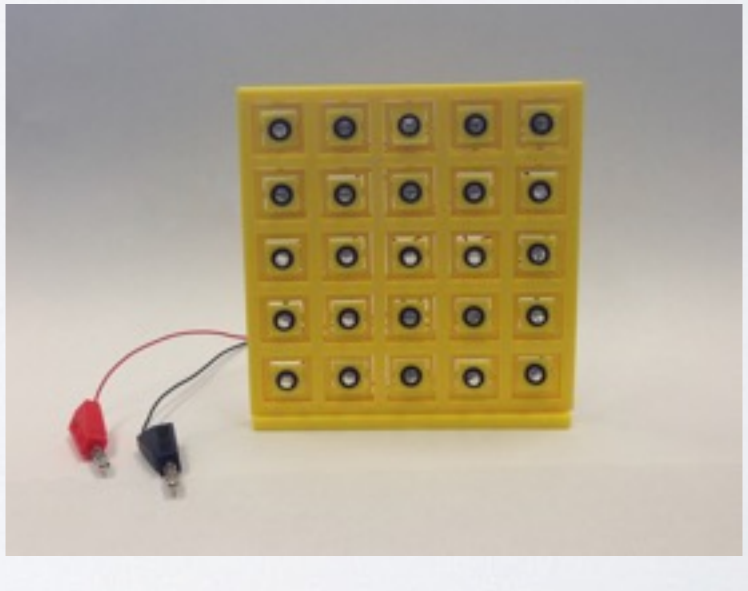
Tonal distribution



ATTACKING CAMERA - SENSITIVITY

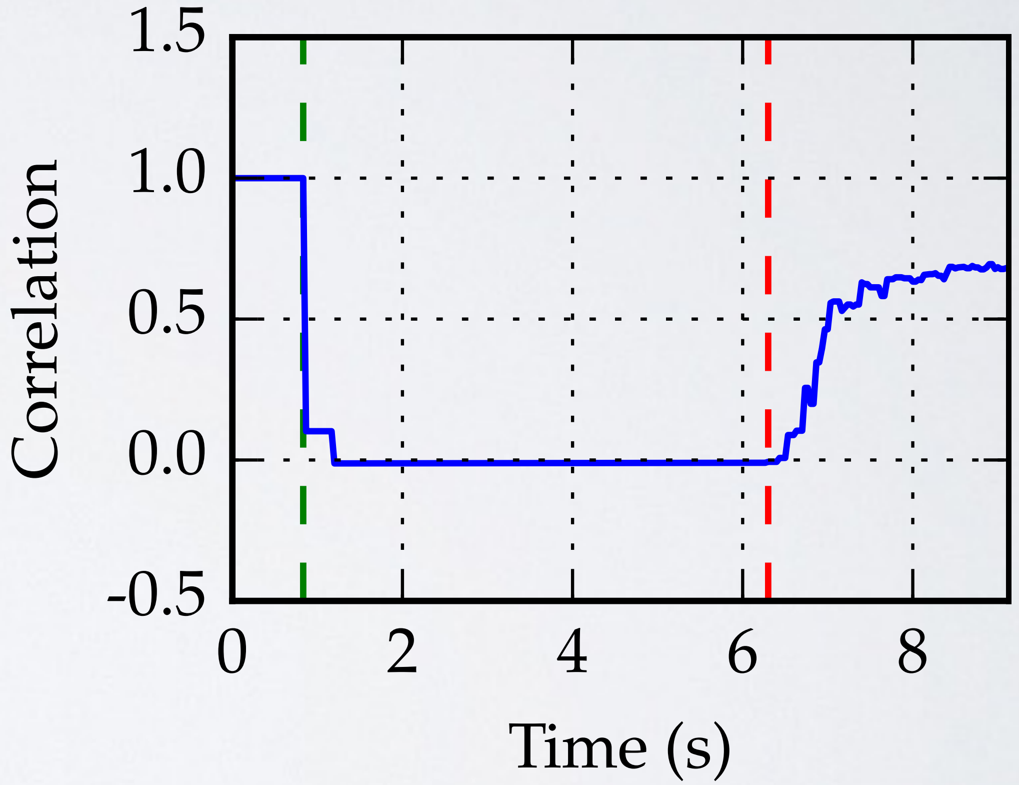
- LED 850nm
- LED 860nm
- LED 875nm
- LED 880nm

- Laser 905nm
- LED 940nm
- **Matrix LED 940nm**

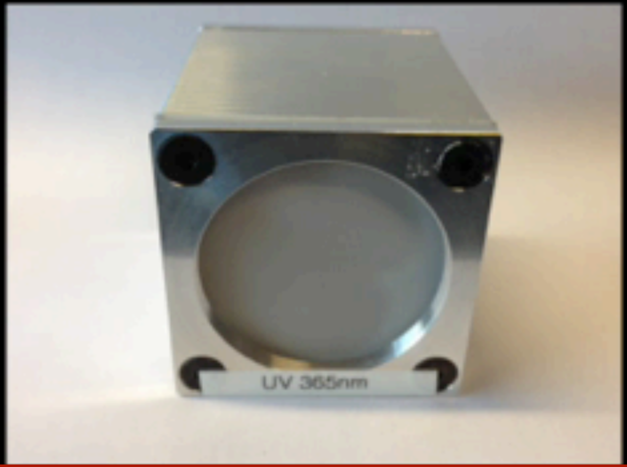


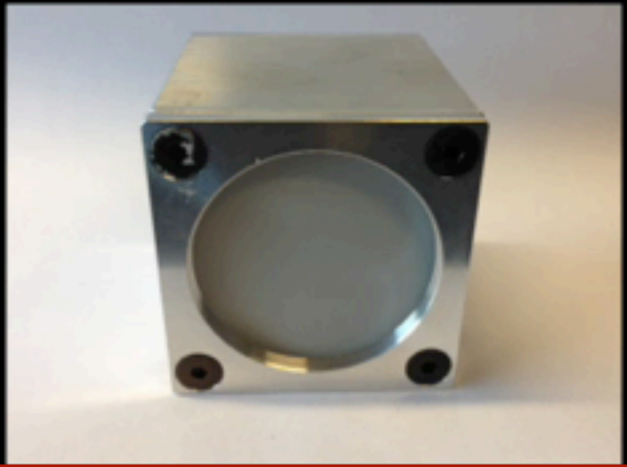
BLINDING CAMERA

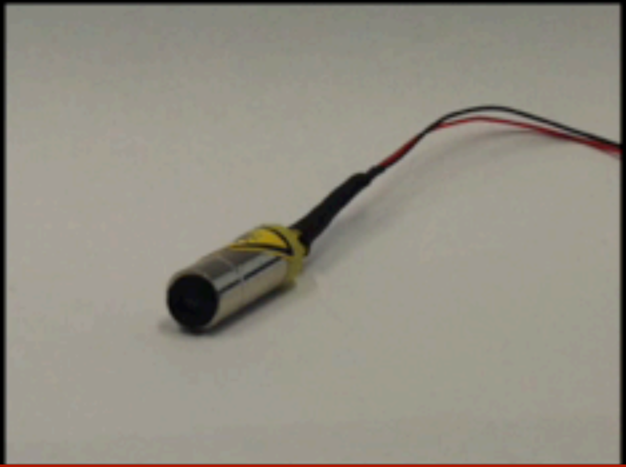
- Use auto exposure
- “Time to recover”



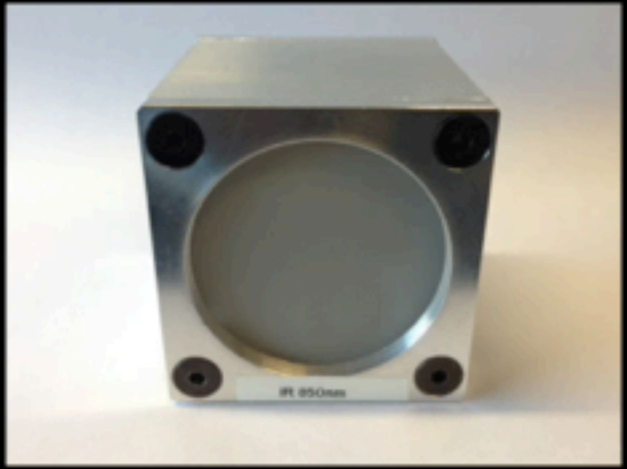
BLINDING CAMERA

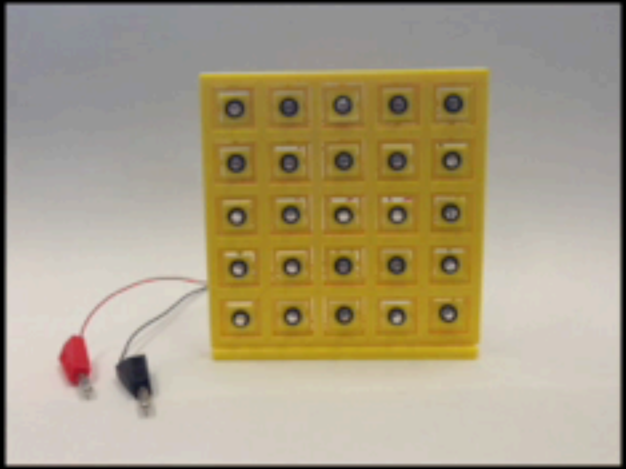






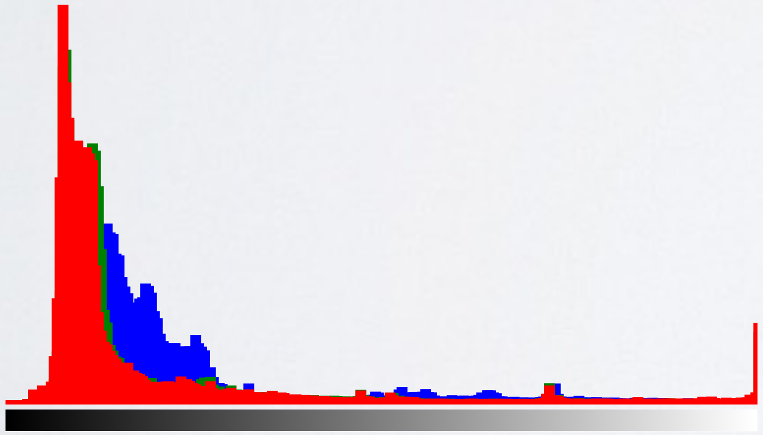
Video of different light sources and their impact on camera



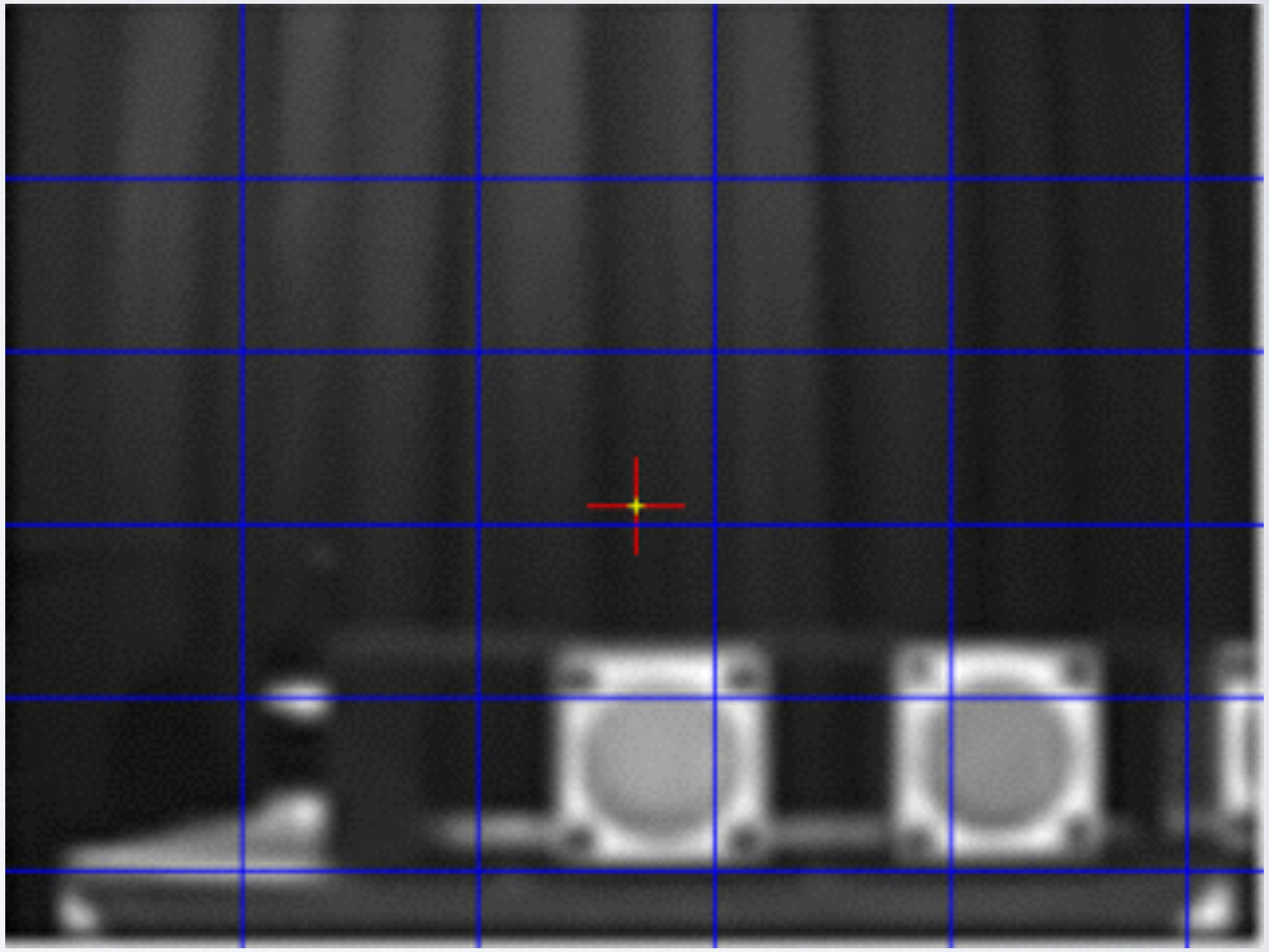


BLINDING CAMERA

- White spot, light, 50cm
- Affect background

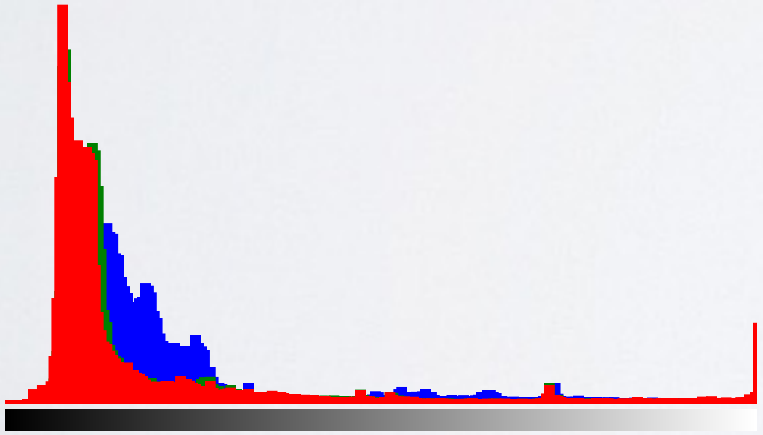


Tonal distribution

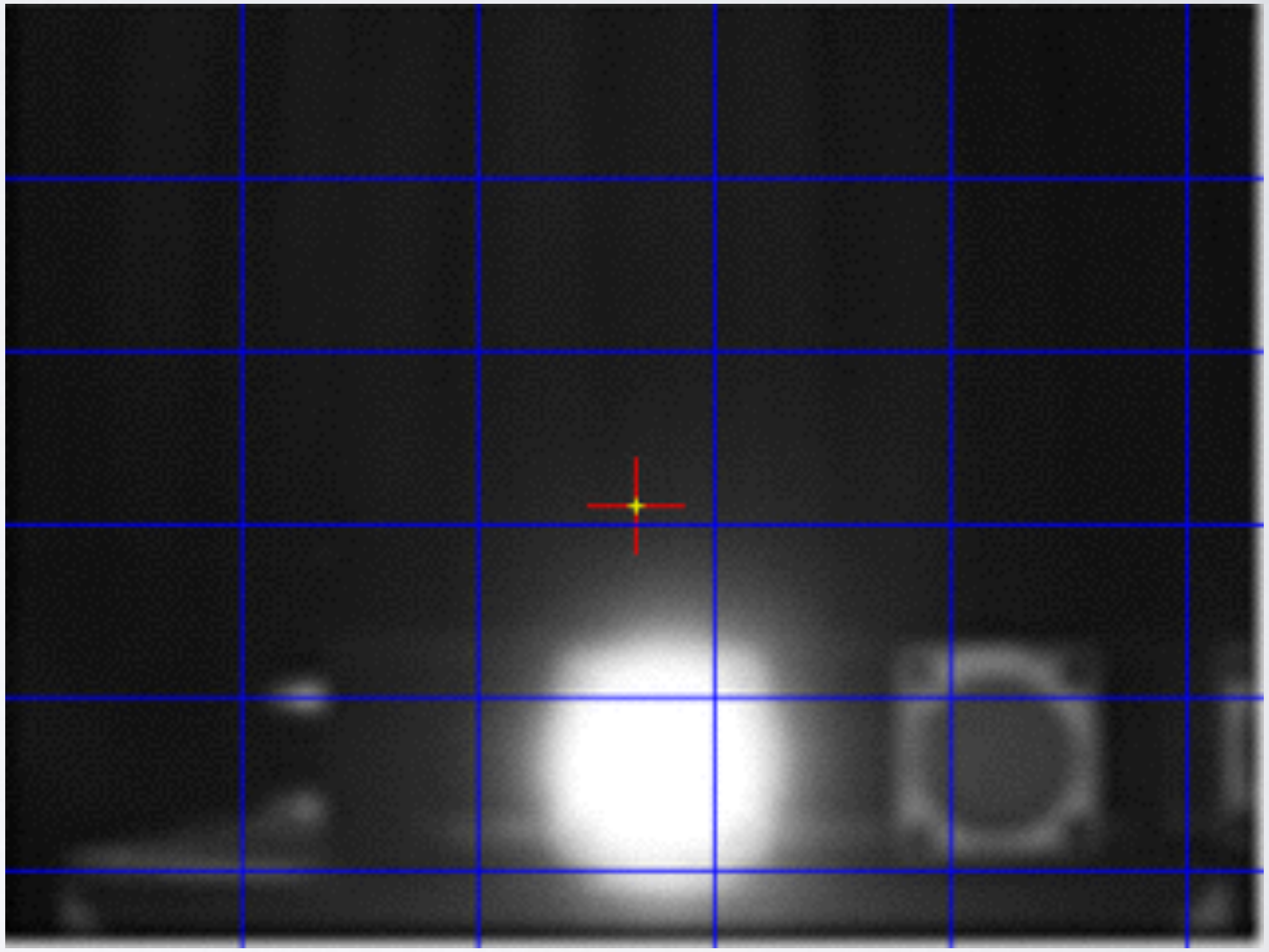


BLINDING CAMERA

- White spot, light, 50cm
- Affect background



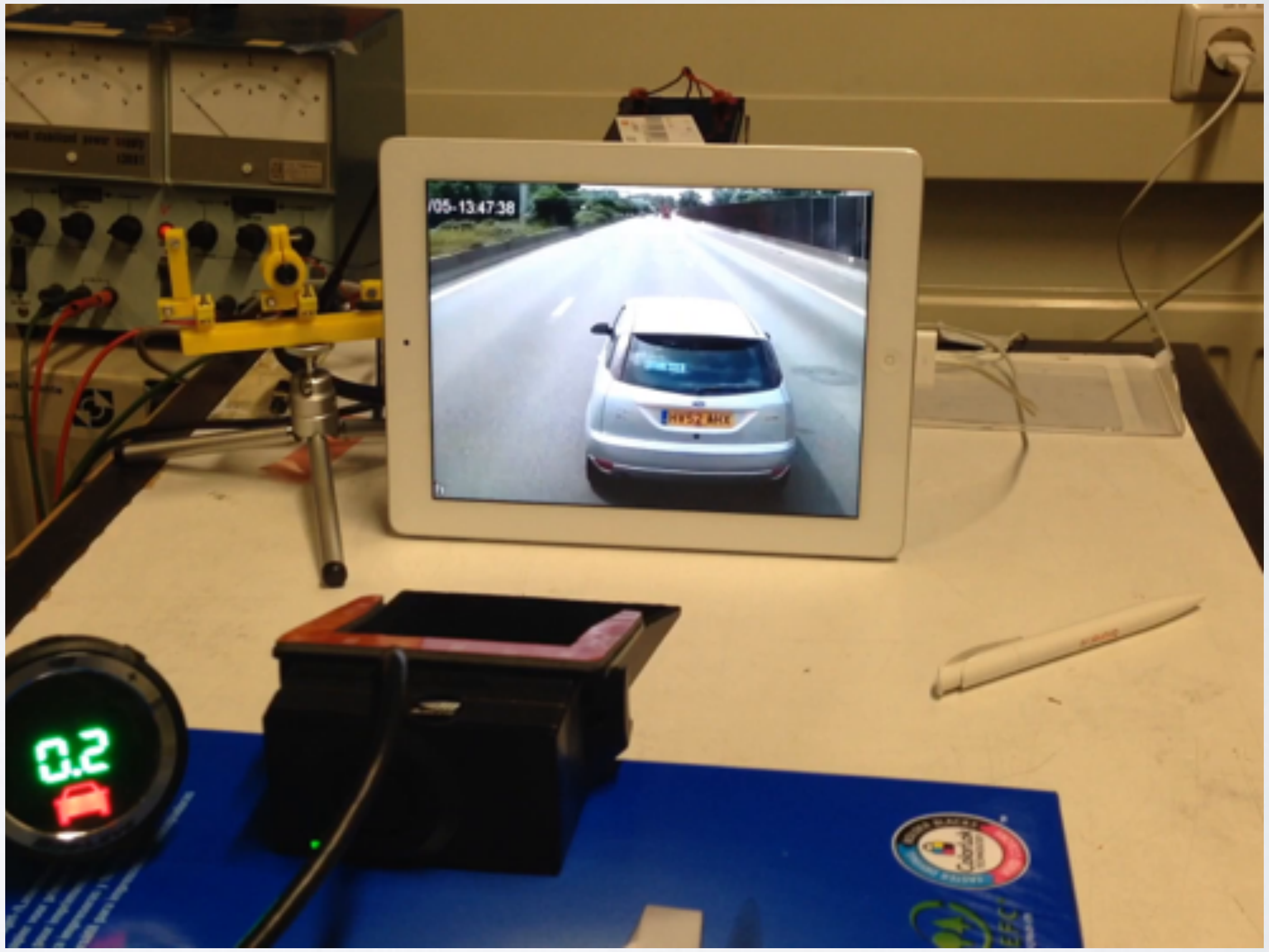
Tonal distribution



BLINDING CAMERA

Video of MobilEye C2-270 blinded by laser 650 nm

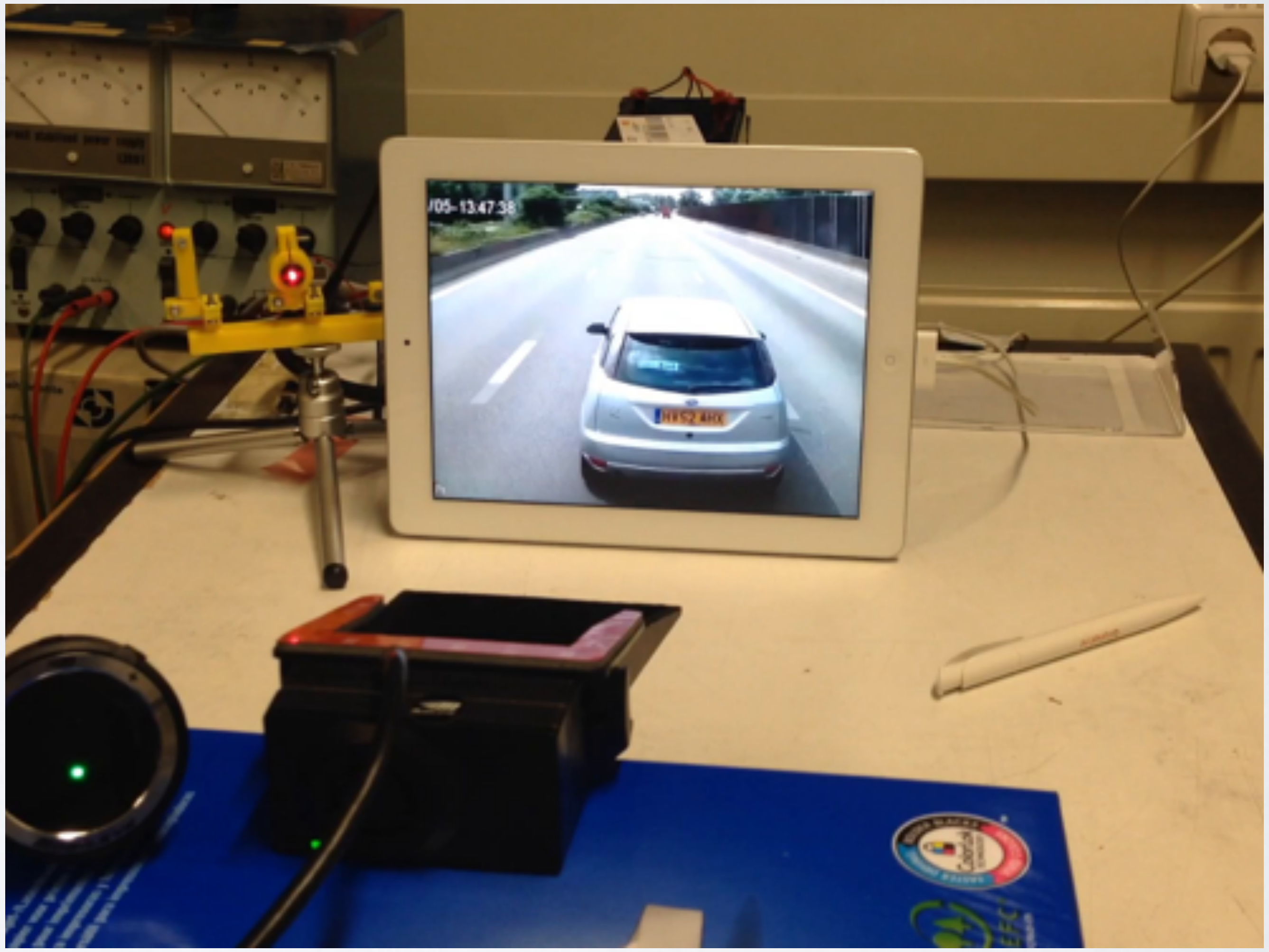
- Laser 650nm



BLINDING CAMERA

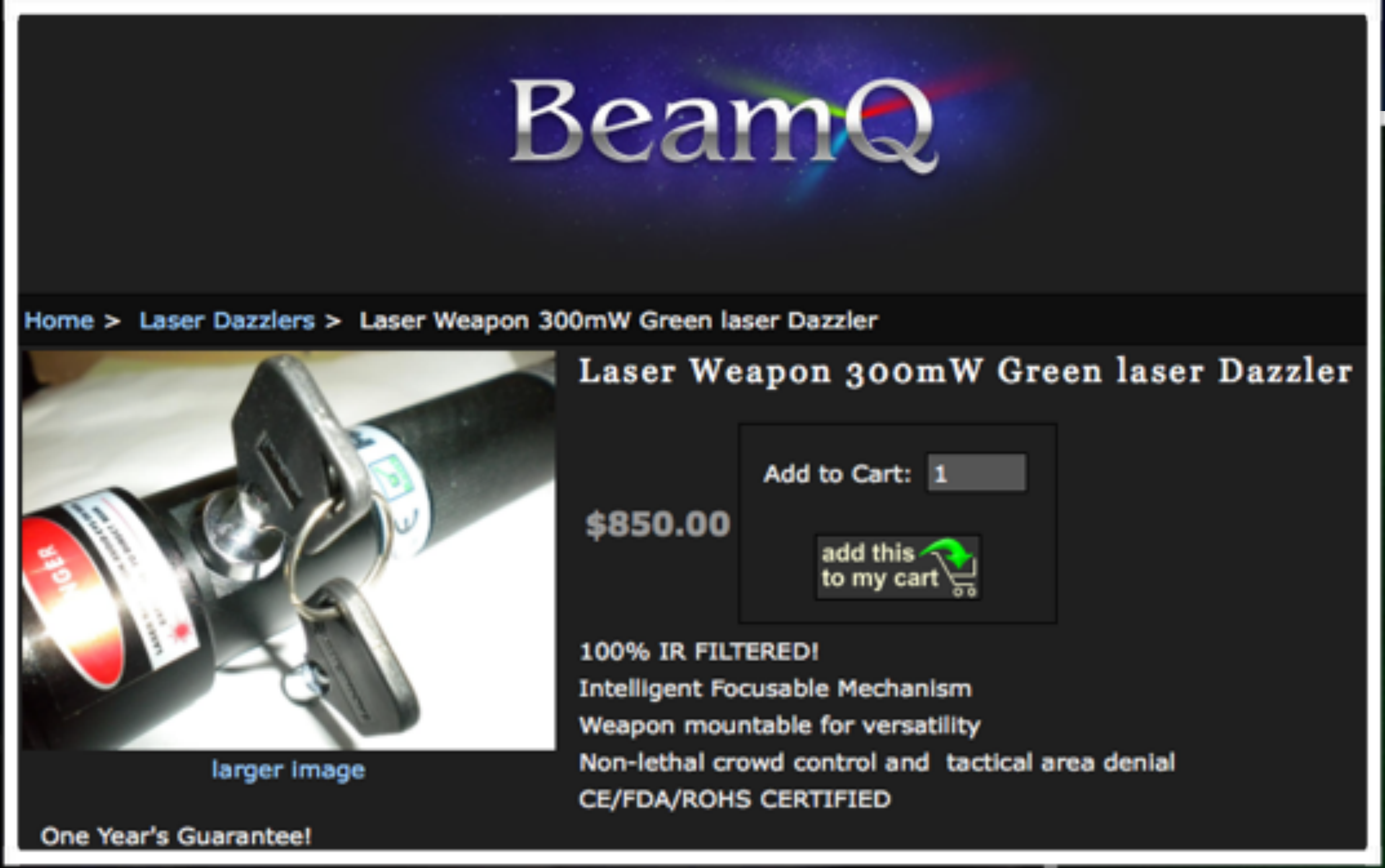
Video of MobilEye C2-270 blinded by laser 650 nm

- Laser 650nm



DAZZLER

DAZZLER



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

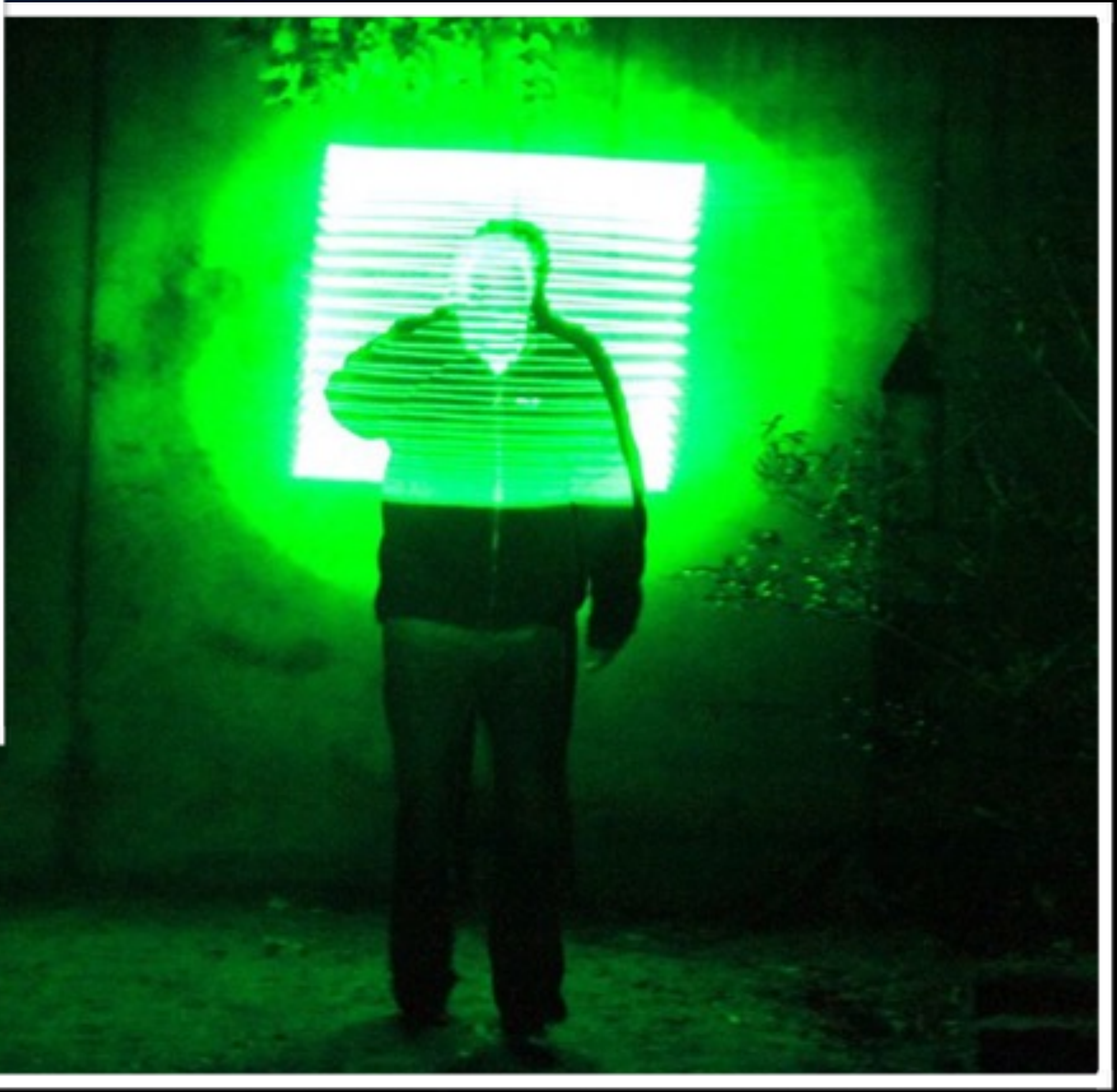
Laser Weapon 300mW Green laser Dazzler

$850.00

Add to Cart: 1

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!

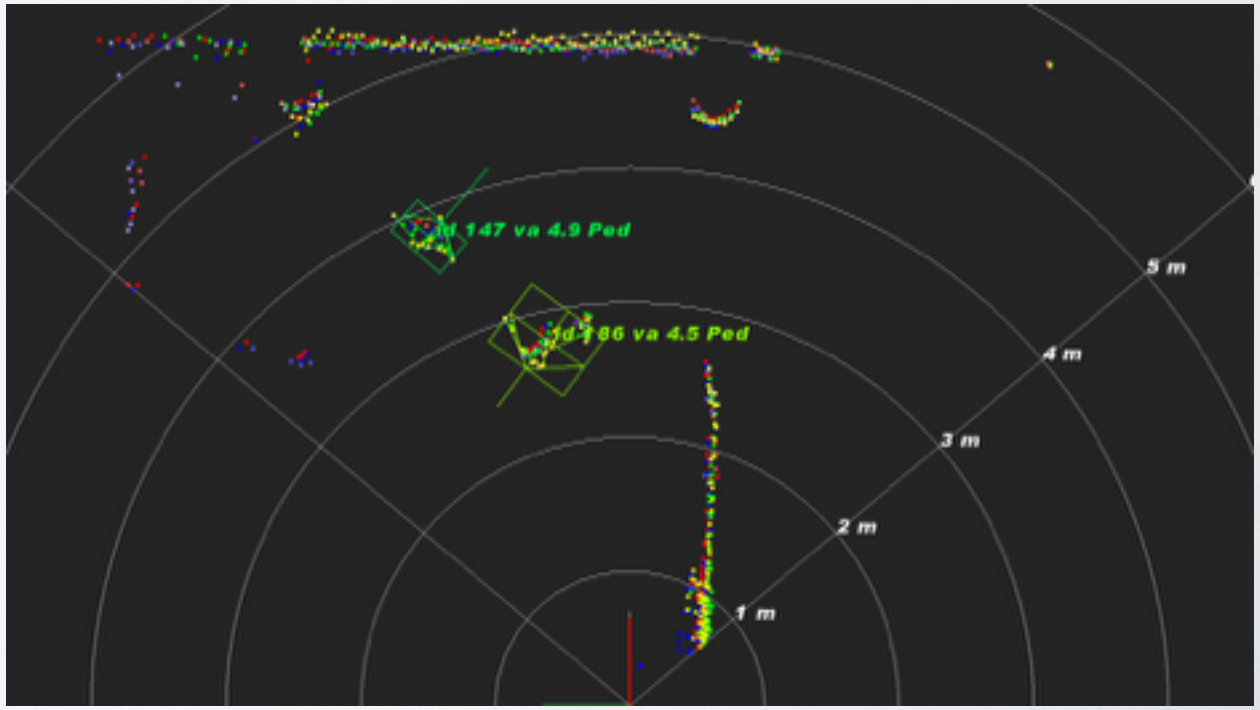


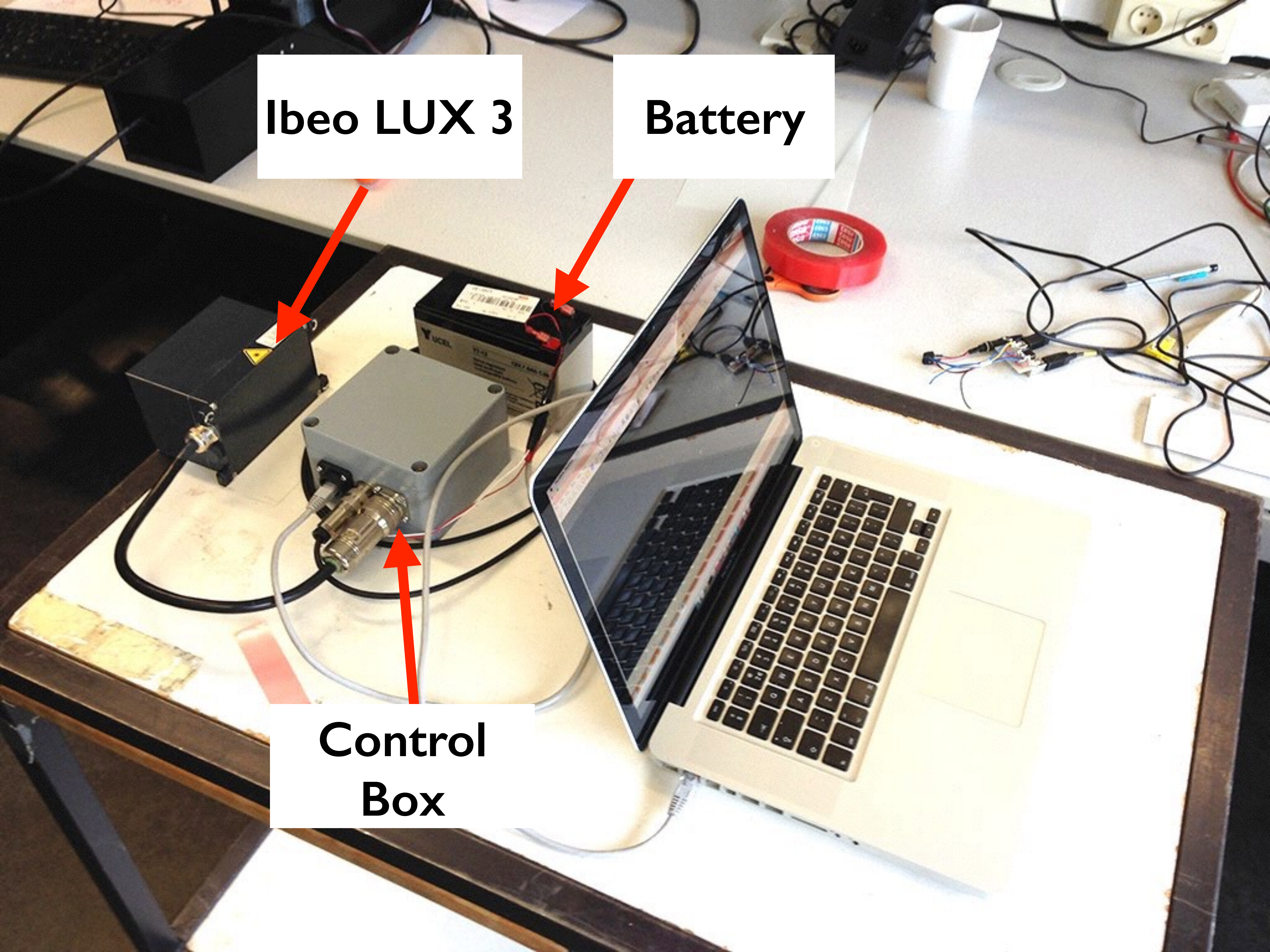
COUNTERMEASURES CAMERA

- 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**
  - 200 meters range
  - Viewing angle 110°
  - 4 layers
  - Up to 3 echoes
  - Scanning speeds: 12.5/25/50 Hz
  - Angular resolution: up to 0.125° horizontal
  - Distance resolution: 4 cm
- Detect object
- Object tracking



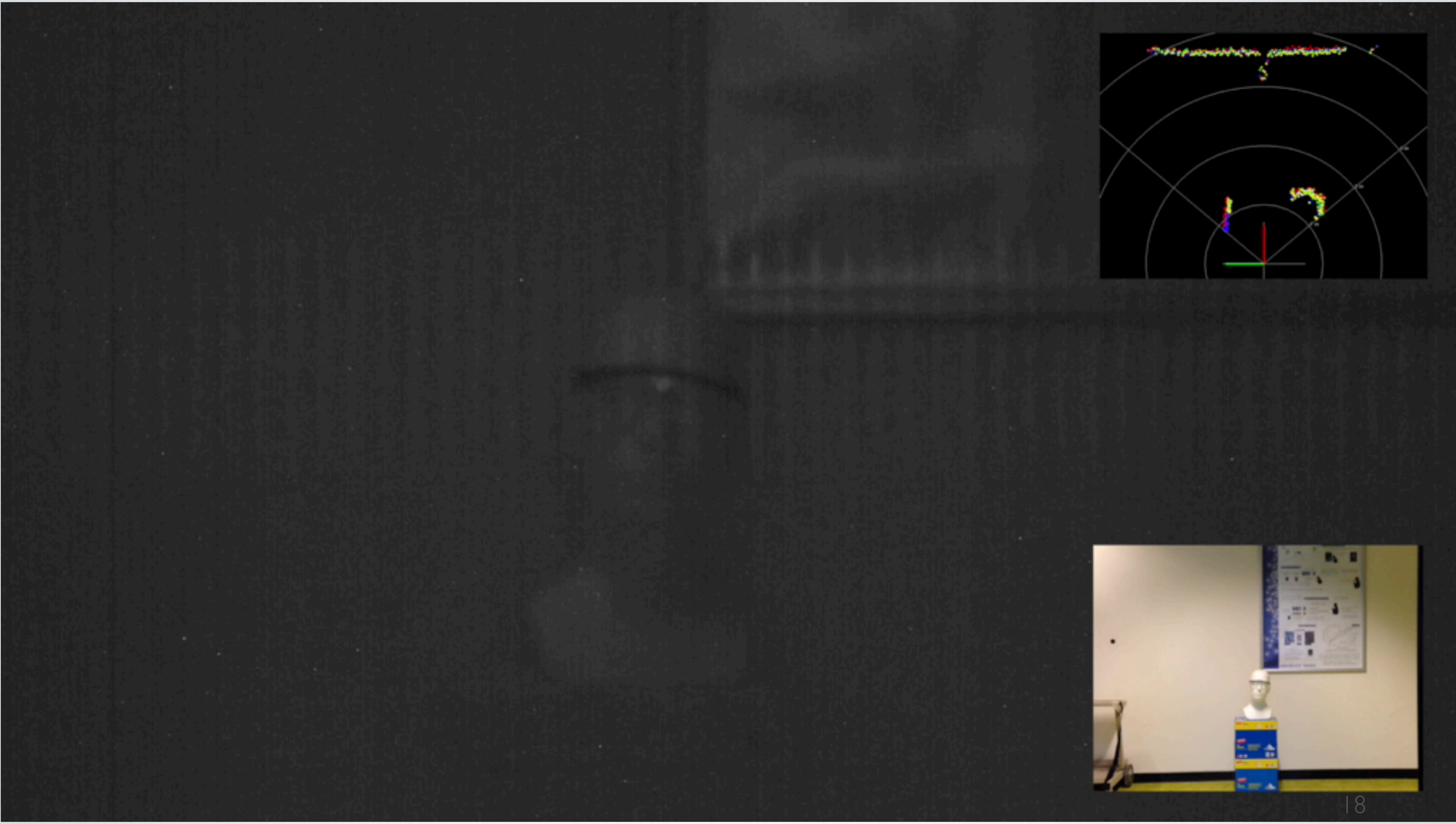


Ibeo LUX 3

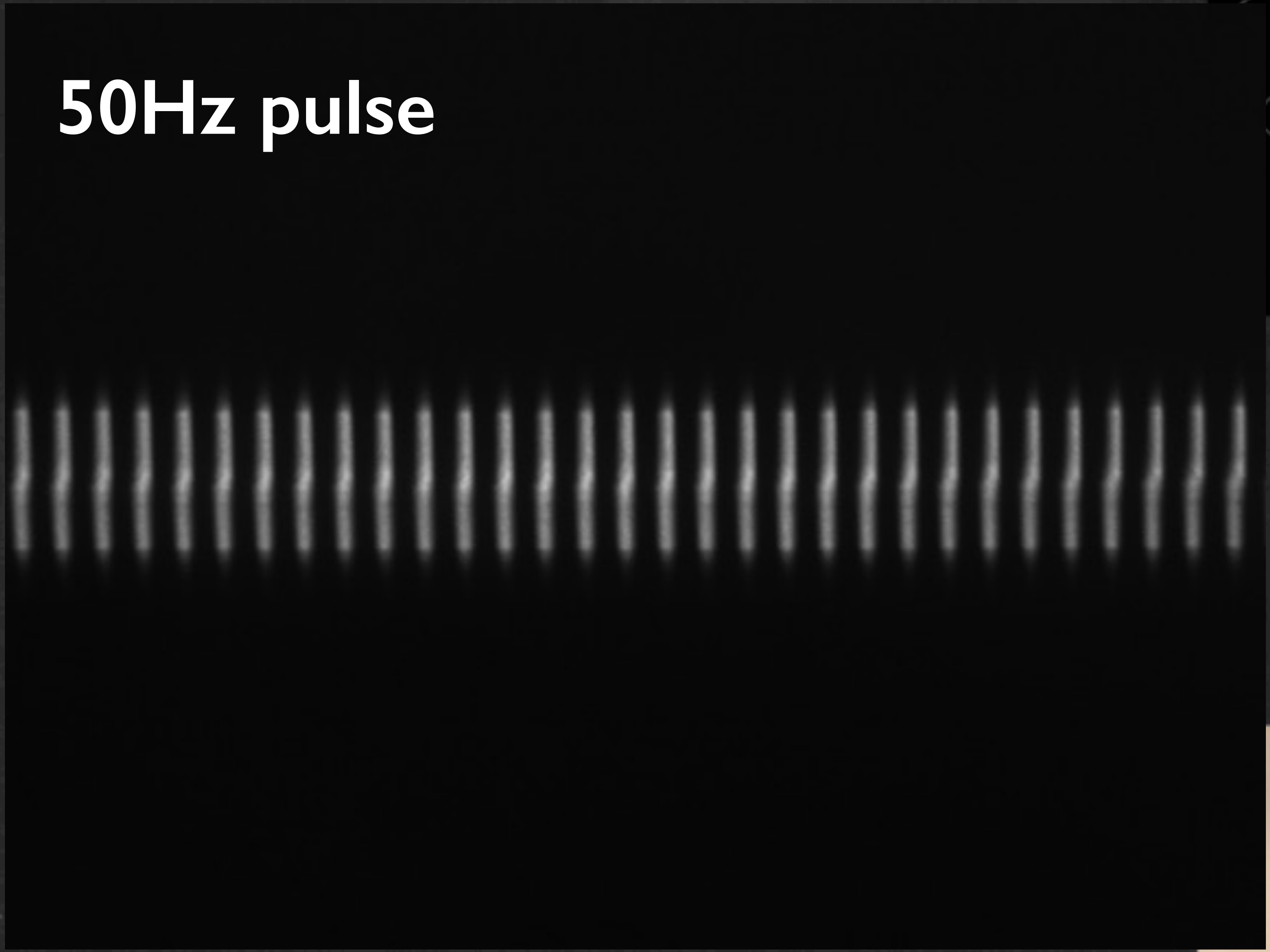
Battery

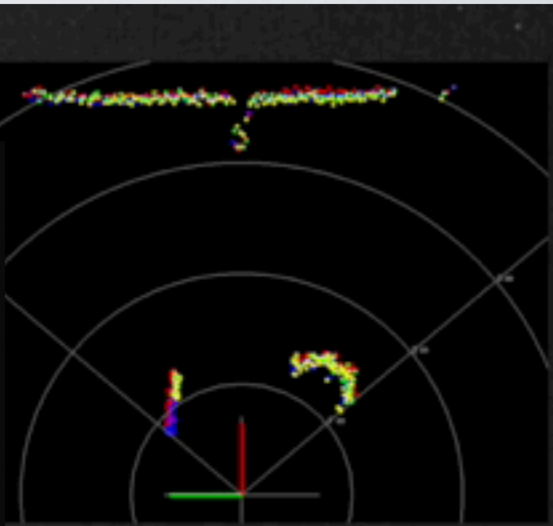
Control Box

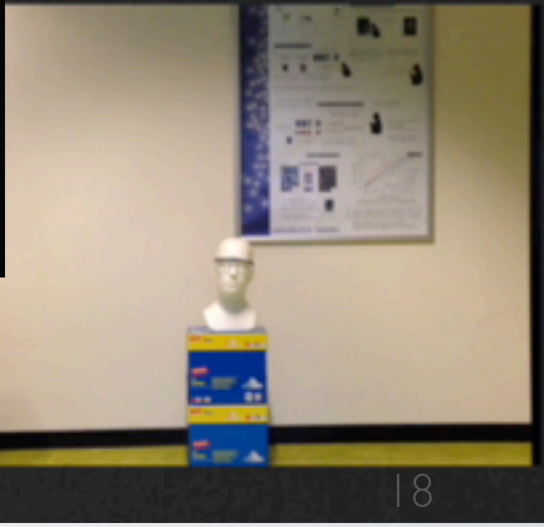
HOW DOES LIDAR WORK?



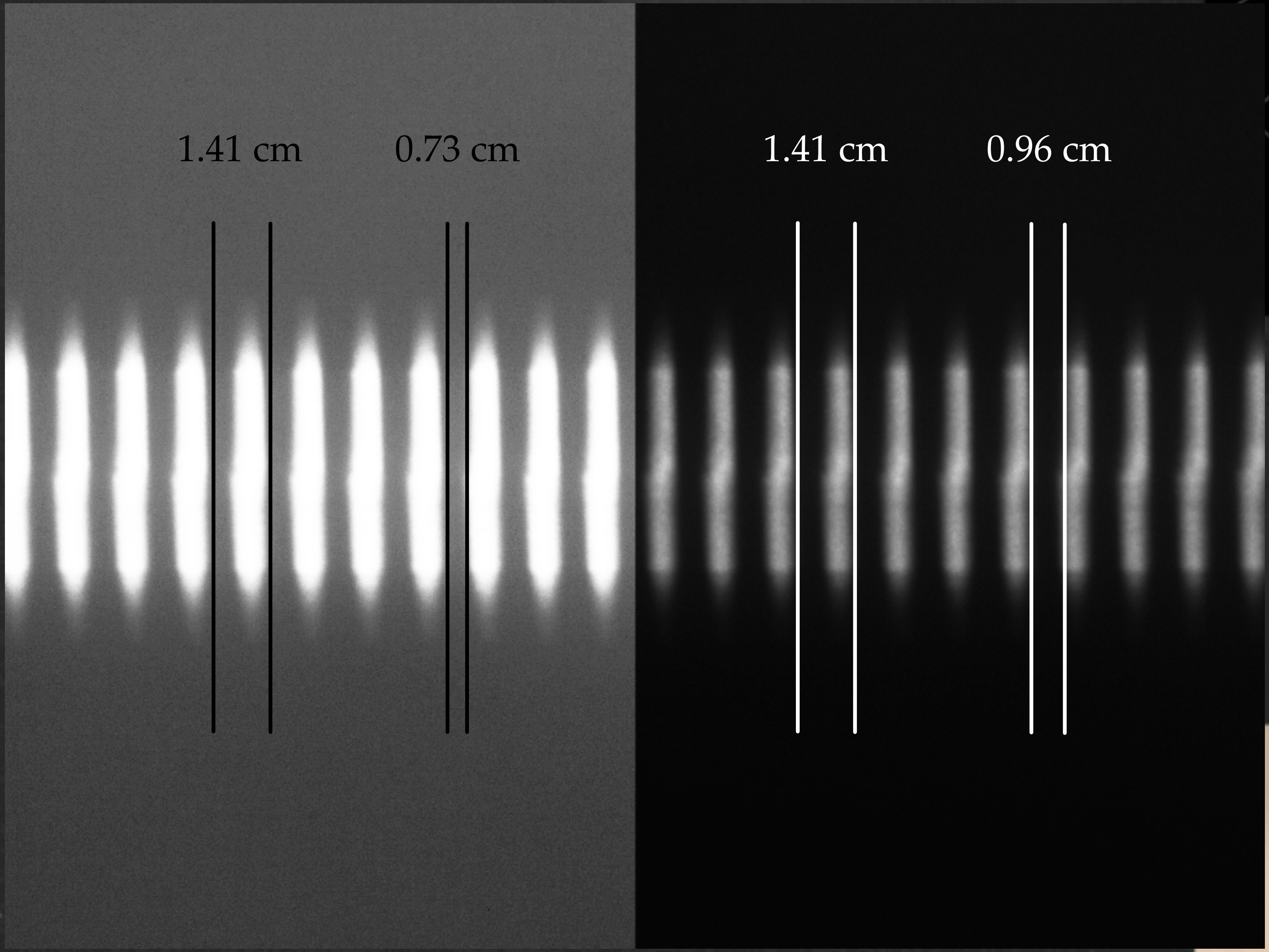
HOW DOES LIDAR WORK?

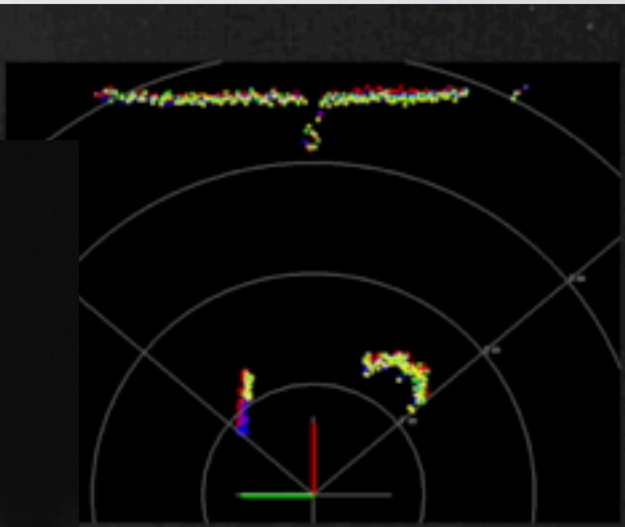


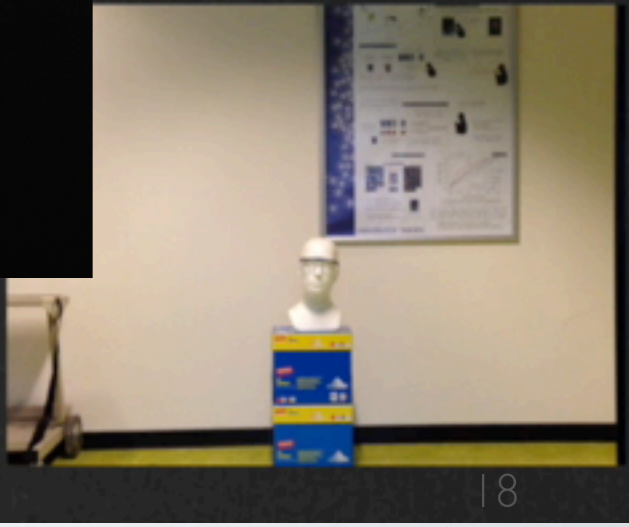




HOW DOES LIDAR WORK?



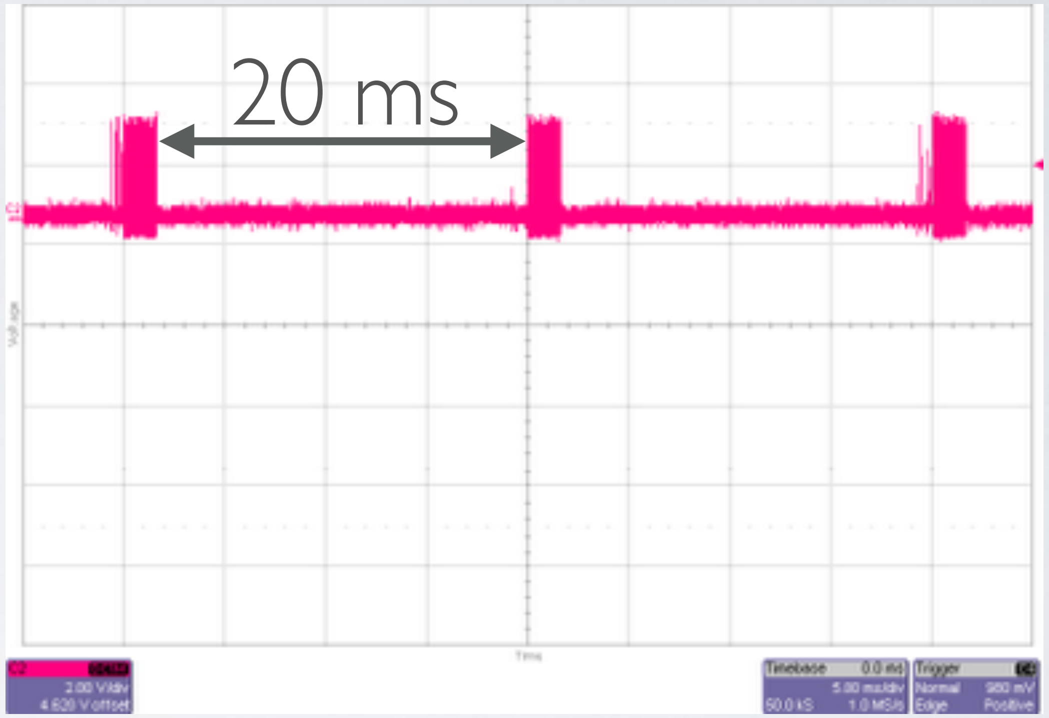




ATTACKING LIDAR

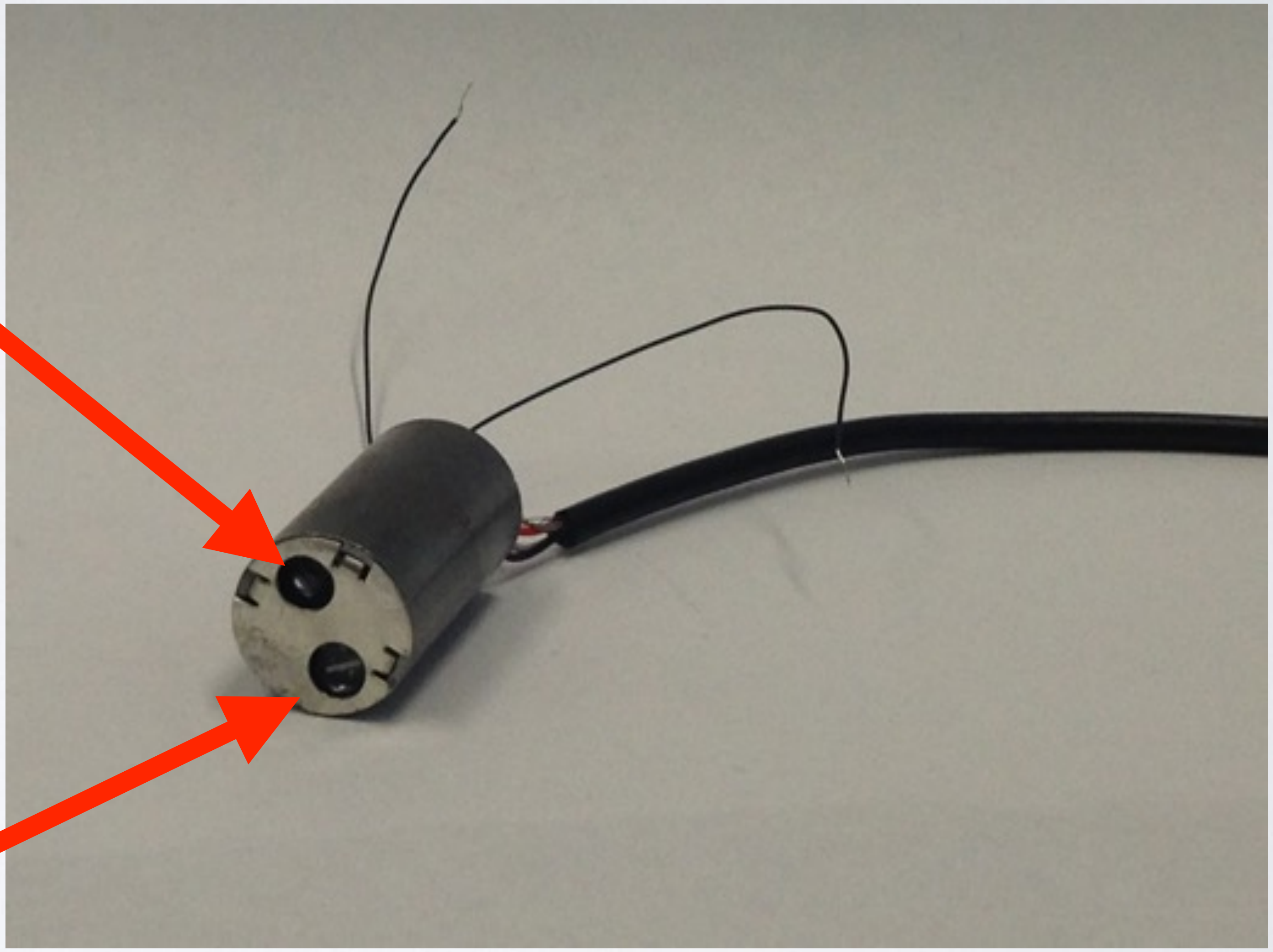
- Attacks:
  - Replay
  - Relay
  - Jamming
  - **Spoofing**
  - **Tracking**

- Equipments:
  - Receiver/Transmitter
  - Pulse generators



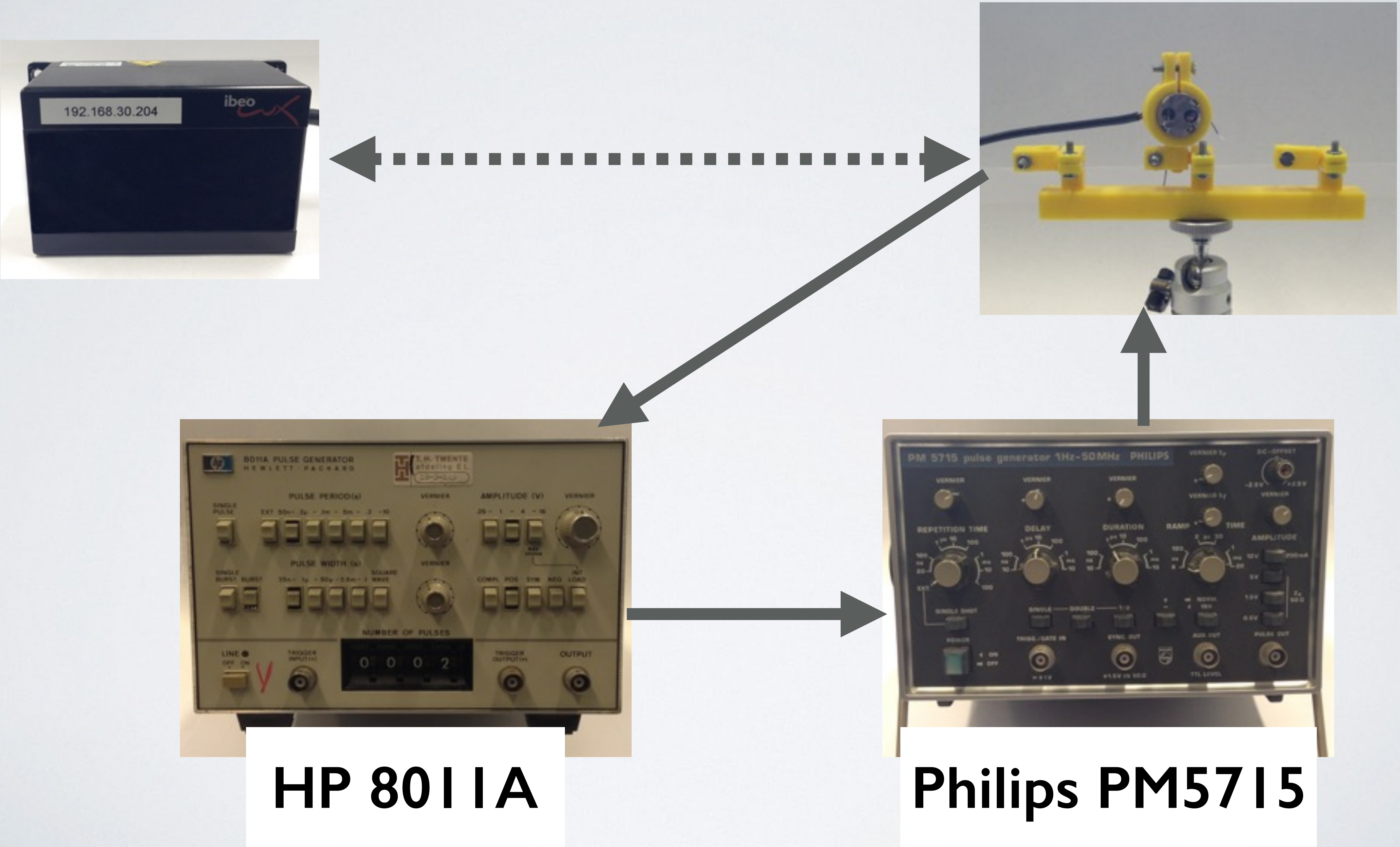
EQUIPMENT

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



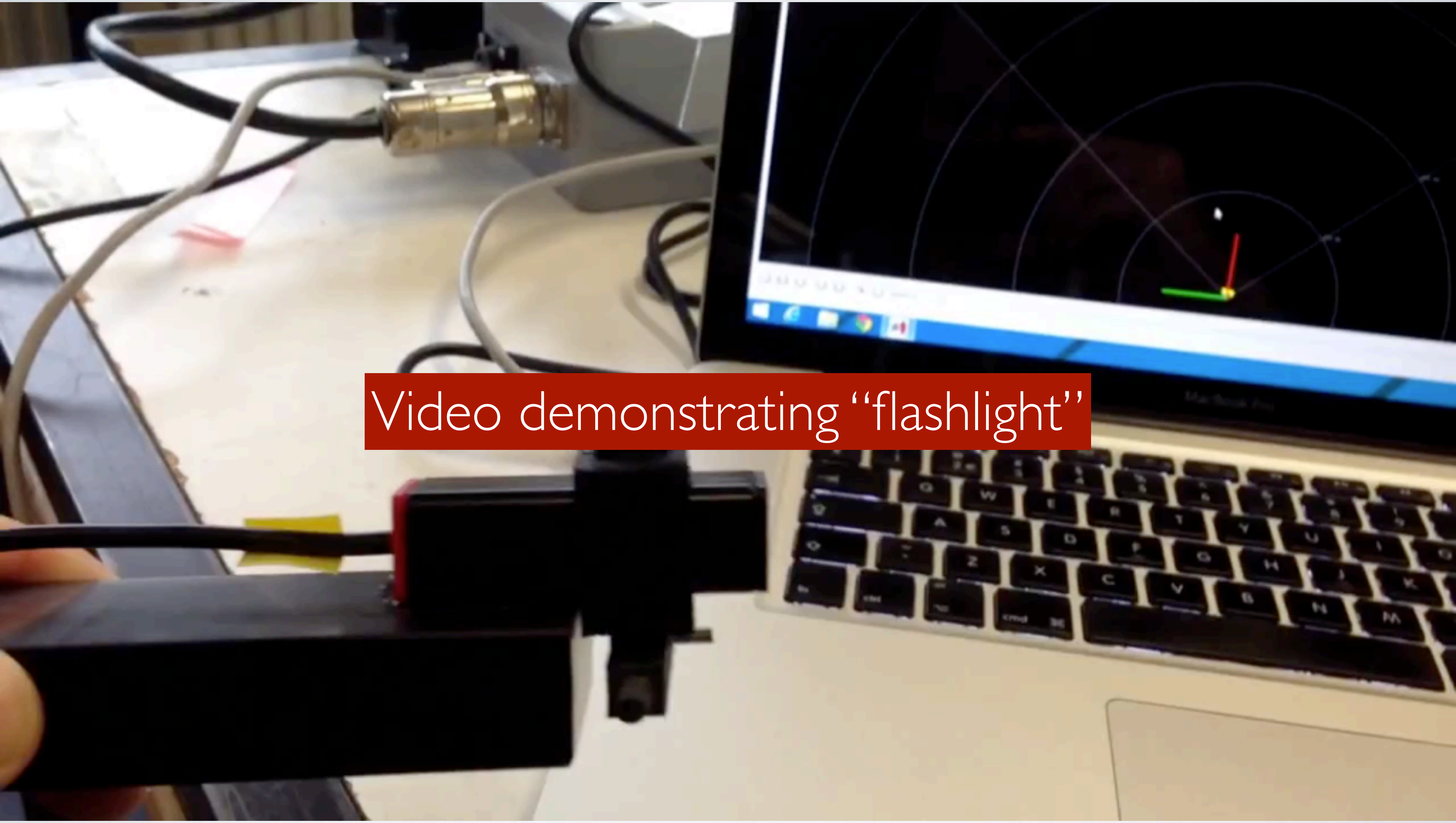
Receiving photodetector:
Osram SFH-213
($0.65)

SETUP



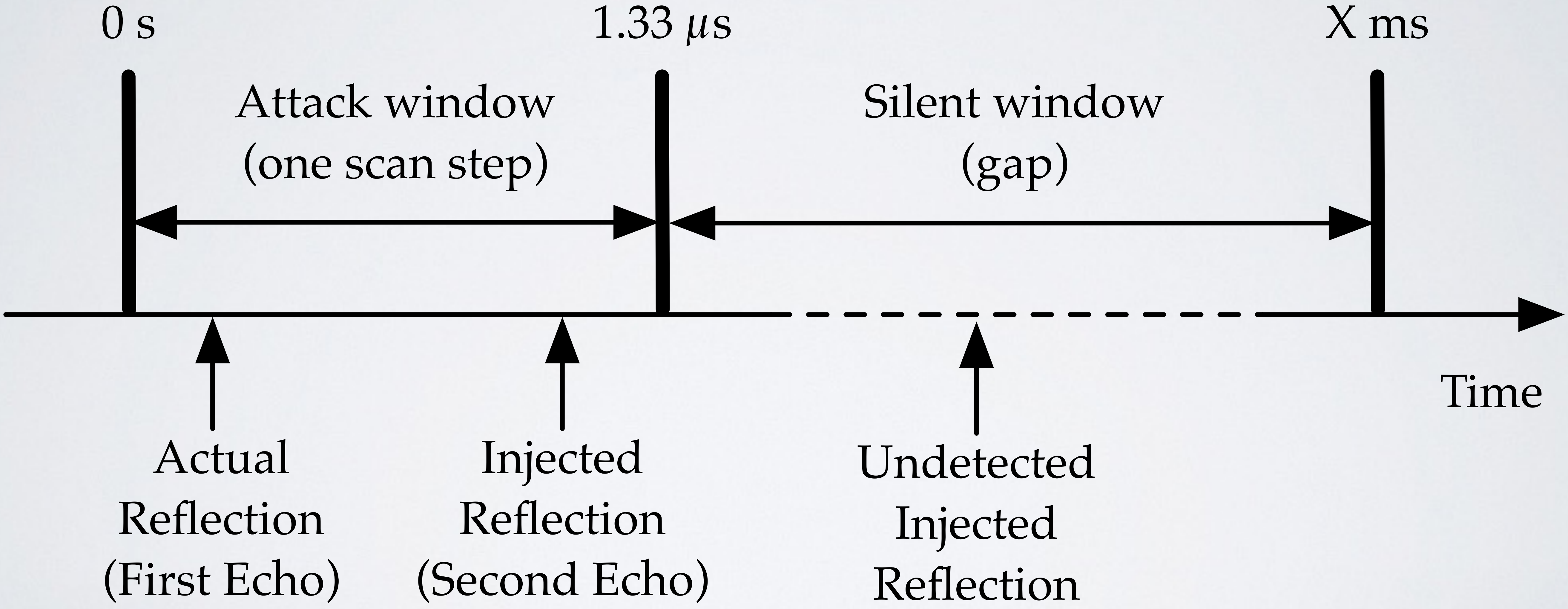
HP 8011A

Philips PM5715

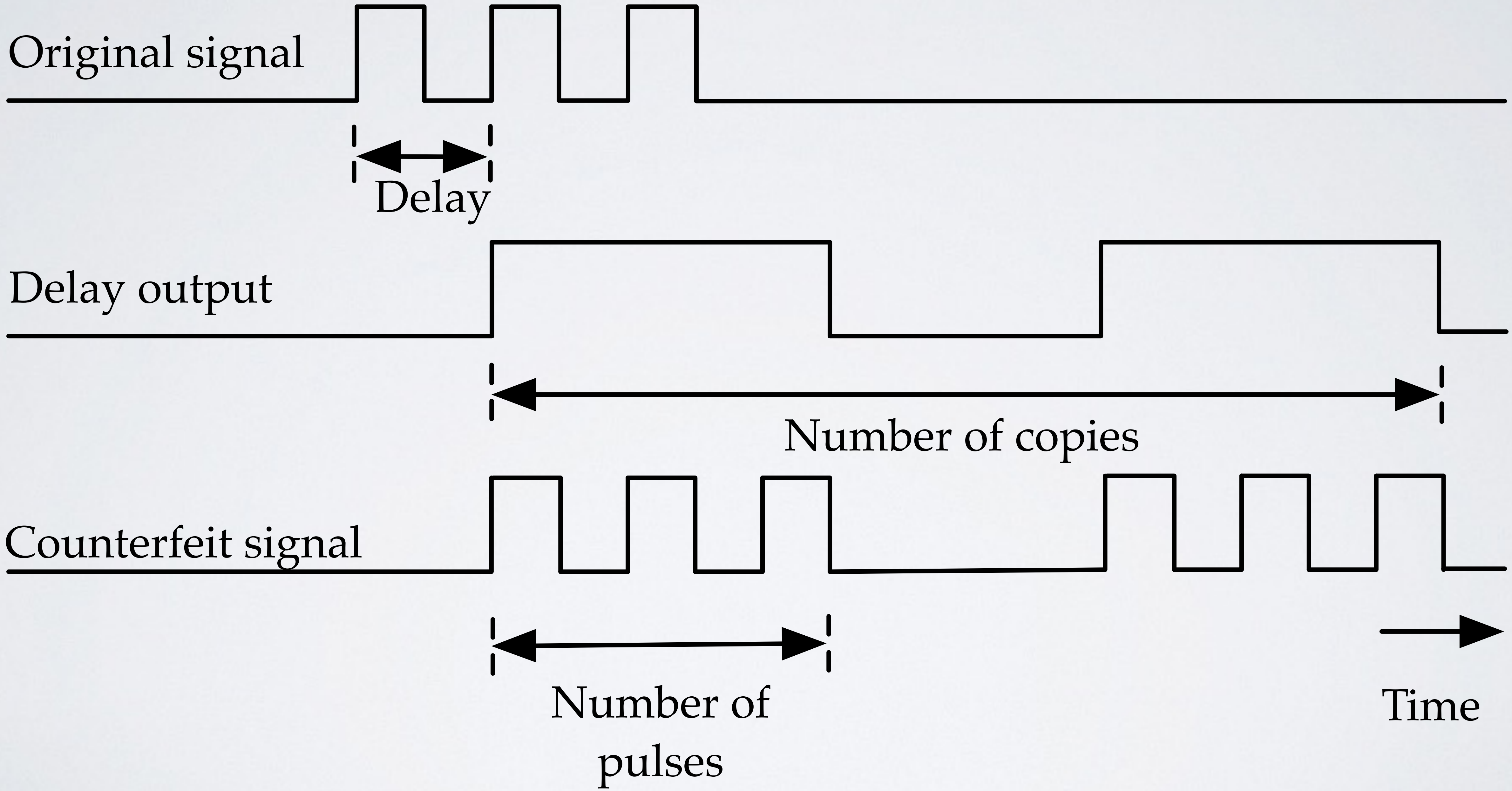


Video demonstrating “flashlight”

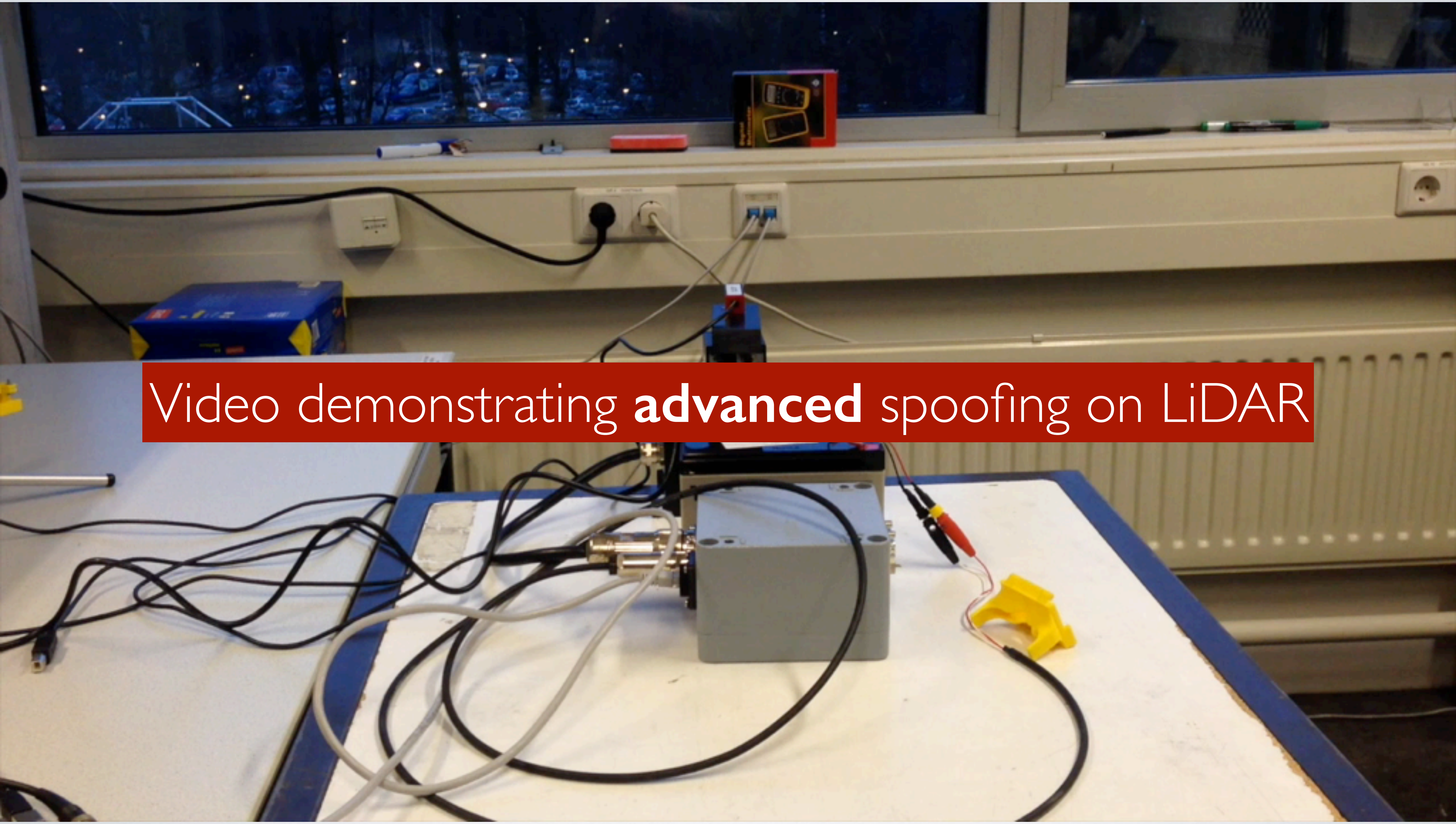
SPOOFING LIDAR (1/3)



SPOOFING LIDAR (2/3)



SPOOFING LIDAR (3/3)



Video demonstrating **advanced** spoofing on LiDAR

TRACKING LIDAR

Video demonstrating impact of spoofing on tracking box

COUNTERMEASURES LIDAR

- **Use multiple lasers with non-overlapping wavelengths for redundancy:**
  Ibeo: Possible, but currently not preferred by Ibeo

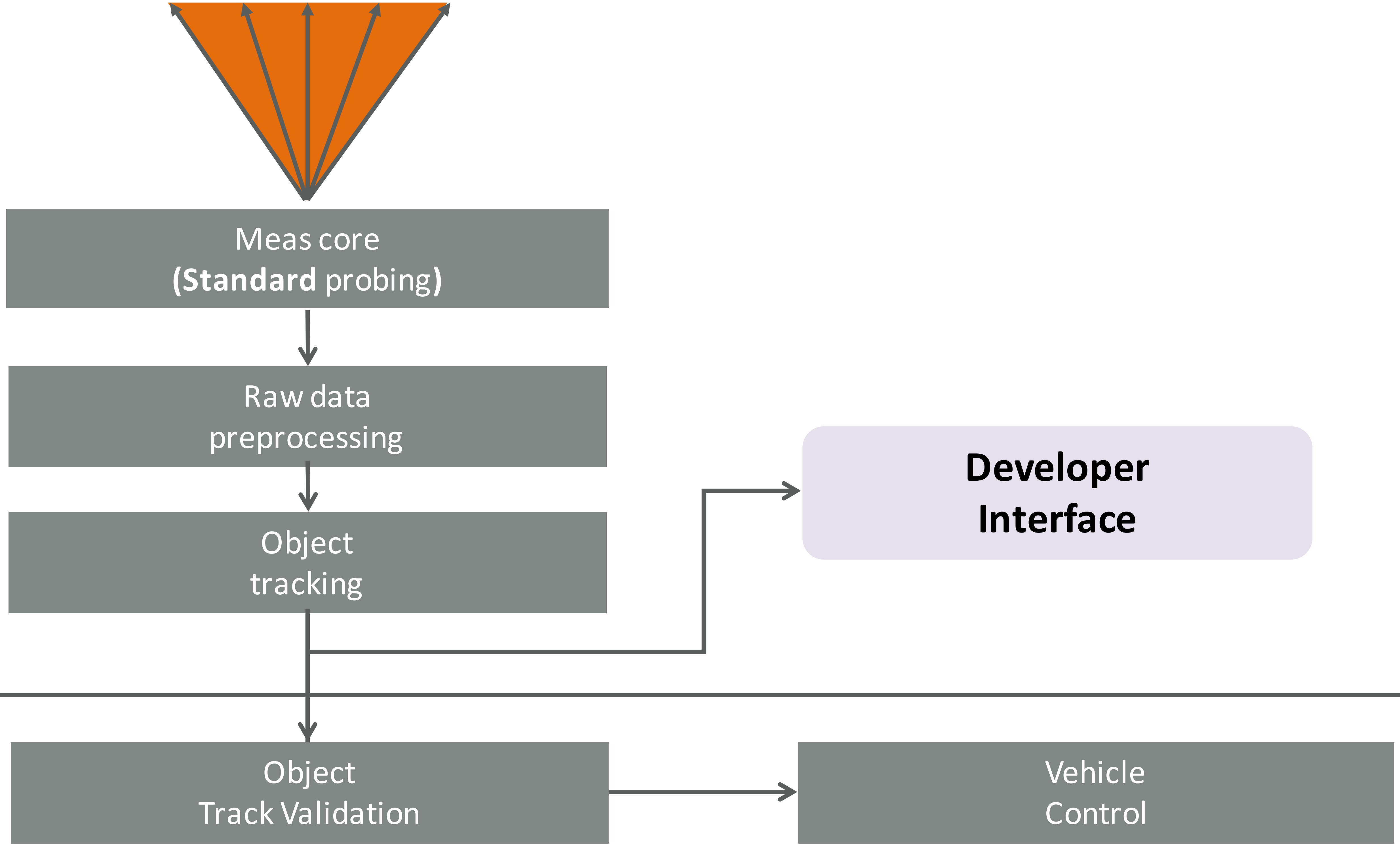
- **Shorten the pulse period by limiting the maximum range:**
  Ibeo: Today Ibeo adapts the maximum range according to the environmental situation

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

Confidential

Countermeasures LIDAR - System Setup Analyzed



Meas core

(**Standard** probing)

Raw data preprocessing

Object tracking

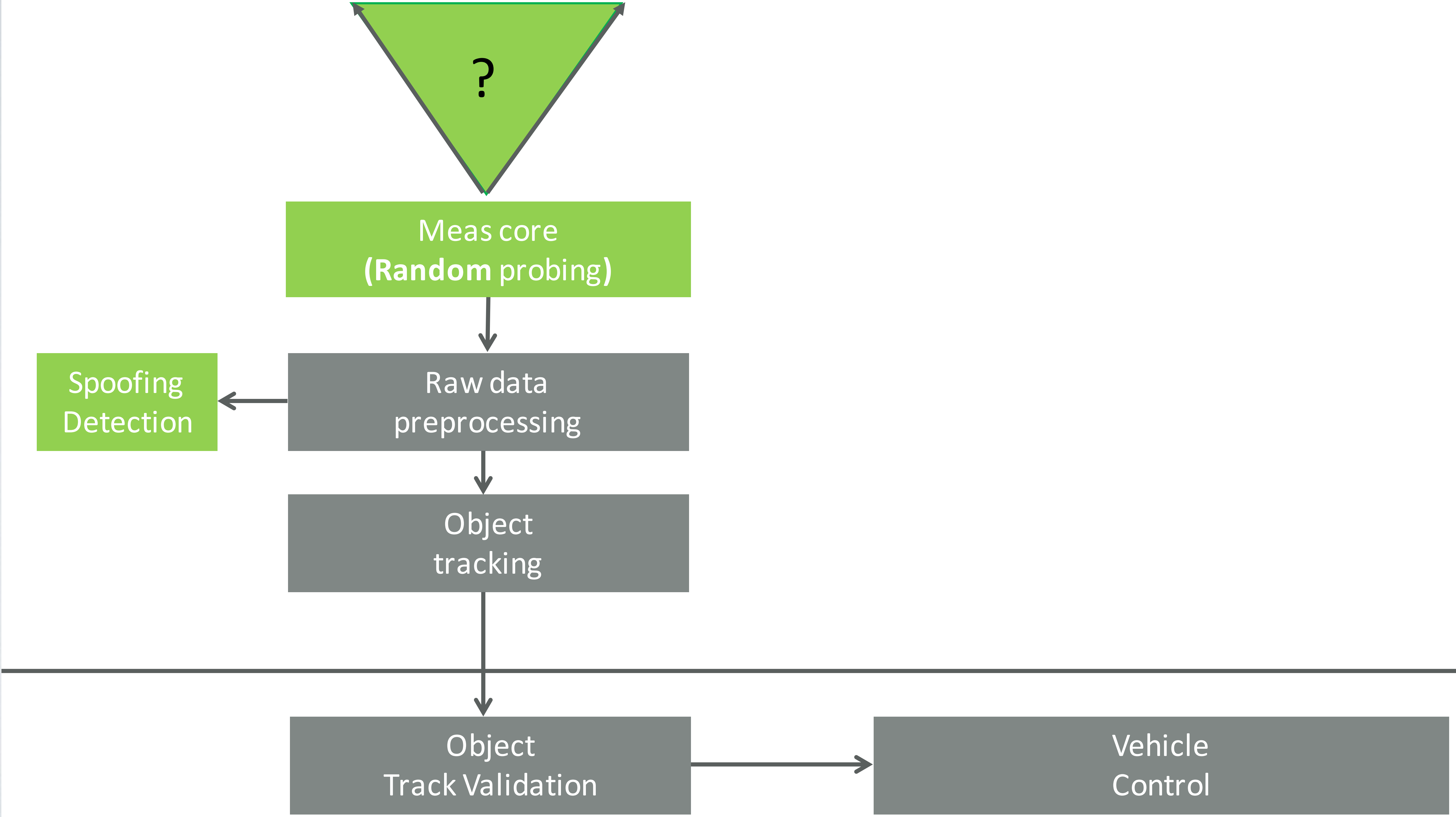
Developer Interface

Object Track Validation

Vehicle Control

Confidential

Countermeasures LIDAR - System Setup in Preparation



?

Meas core
(Random probing**)**

Raw data
preprocessing

Spoofing
Detection

Object
tracking

Object
Track Validation

Vehicle
Control

Confidential

BLACK HAT SOUND BYTES.

1. Fooling LiDAR on raw data level in laboratory environment is possible **<u>but</u>**

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

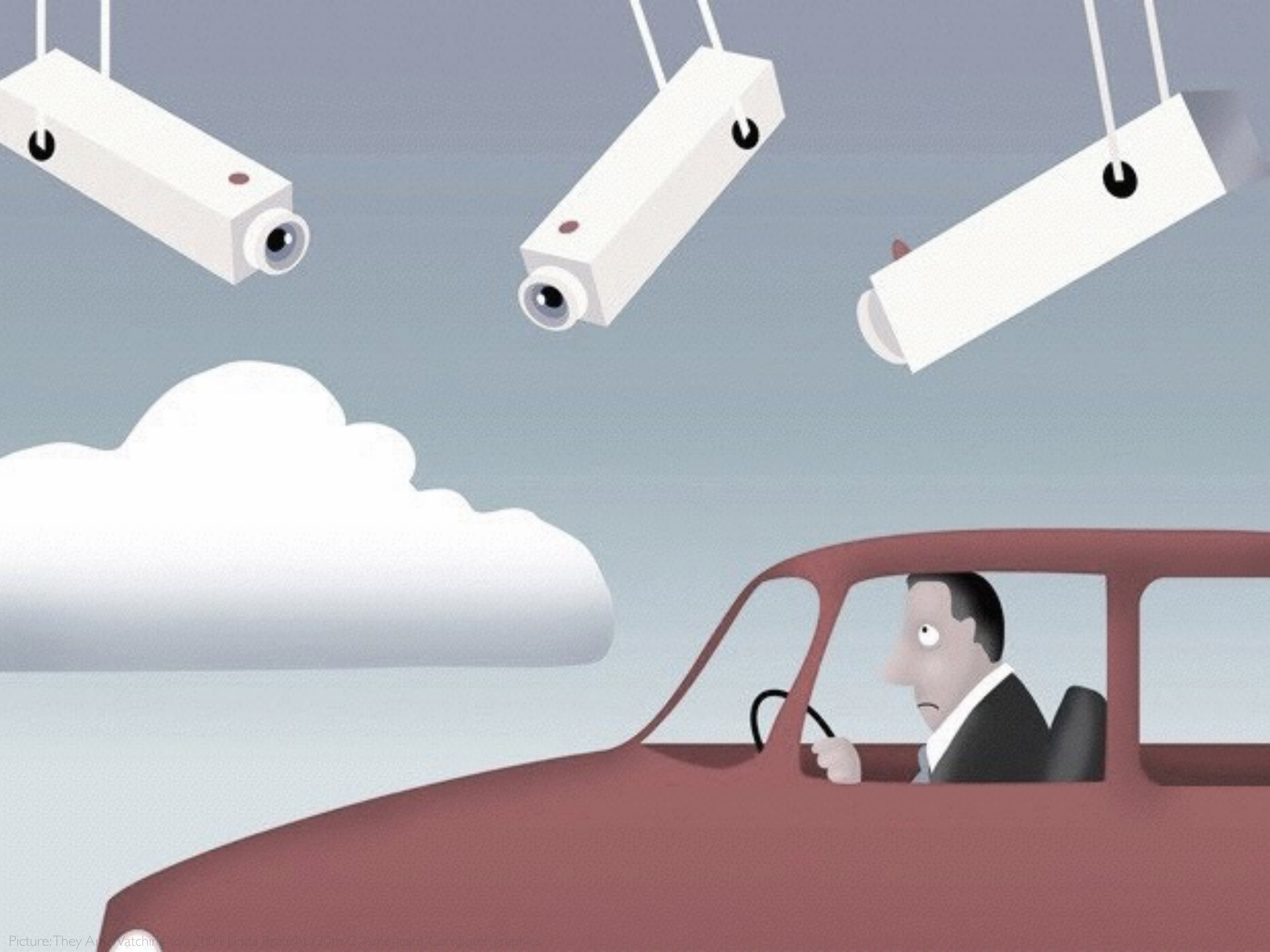
2. Fooling camera-based systems is **easy** and **cheap.**

3. Don’t trust automated vehicle sensors unless you implement countermeasures to mitigate such threats.

CONNECTED VEHICLES: SURVEILLANCE THREAT AND MITIGATIONS

Jonathan Petit, Djurre Broekhuis, Michael Feiri, Frank Kargl

Picture: They Are Watching You 2004 Linda Braucht (20th C. American) Computer graphics



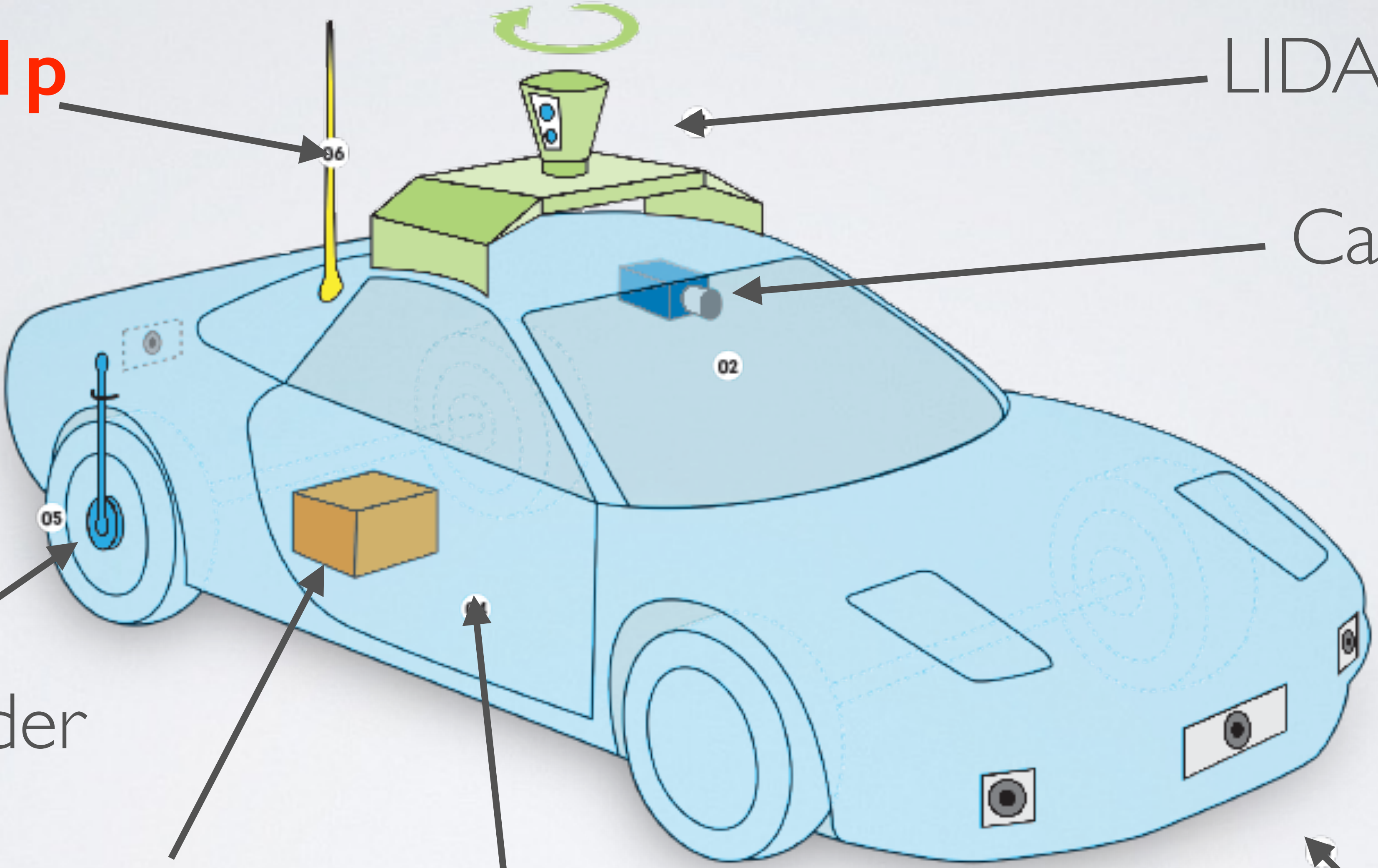
Picture: They Are Watching You 2004 Linda Braucht (20th C. American) Computer graphics

Picture: They Are Watching You 2004 Linda Braucht (20th C. American) Computer graphics

Picture: They Are Watching You 2004 Linda Braucht (20th C. American) Computer graphics

Picture: They Are Watching You 2004 Linda Braucht (20th C. American) Computer graphics

AUTOMATED/CONNECTED VEHICLE



GPS, **802.11p**

LIDAR

Camera

wheel encoder

On-Board Unit, emaps

ultrasonic sensors

RADAR

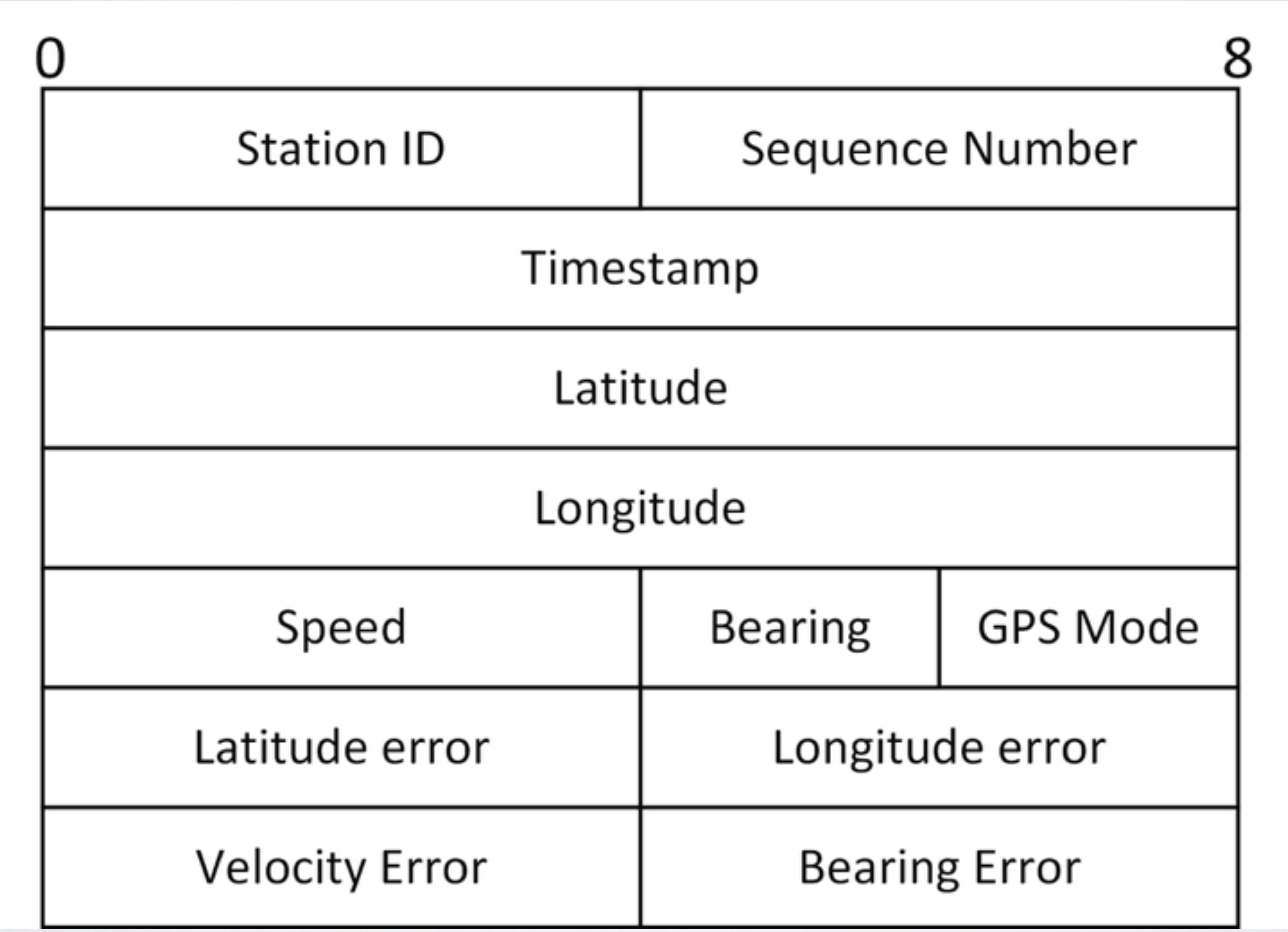
APPLICATION AREAS FOR V2X COMMUNICATION

Safety

Efficiency

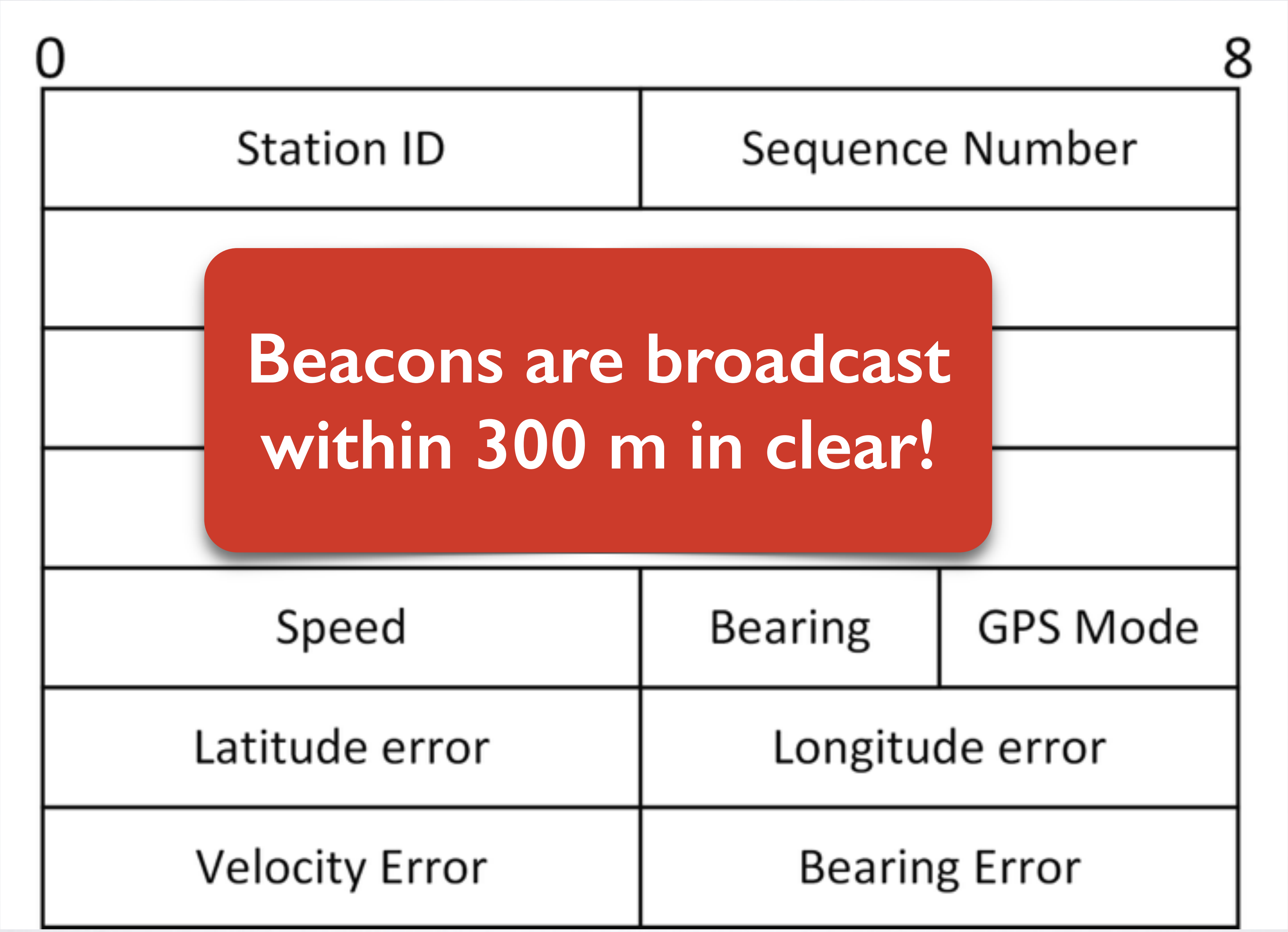
Comfort

CONTENT OF BEACON



<table>
<tr><td>0</td><td></td><td></td><td>8</td></tr>
<tr><td colspan="2">Station ID</td><td colspan="2">Sequence Number</td></tr>
<tr><td colspan="4">Timestamp</td></tr>
<tr><td colspan="4">Latitude</td></tr>
<tr><td colspan="4">Longitude</td></tr>
<tr><td colspan="2">Speed</td><td>Bearing</td><td>GPS Mode</td></tr>
<tr><td colspan="2">Latitude error</td><td colspan="2">Longitude error</td></tr>
<tr><td colspan="2">Velocity Error</td><td colspan="2">Bearing Error</td></tr>
</table>

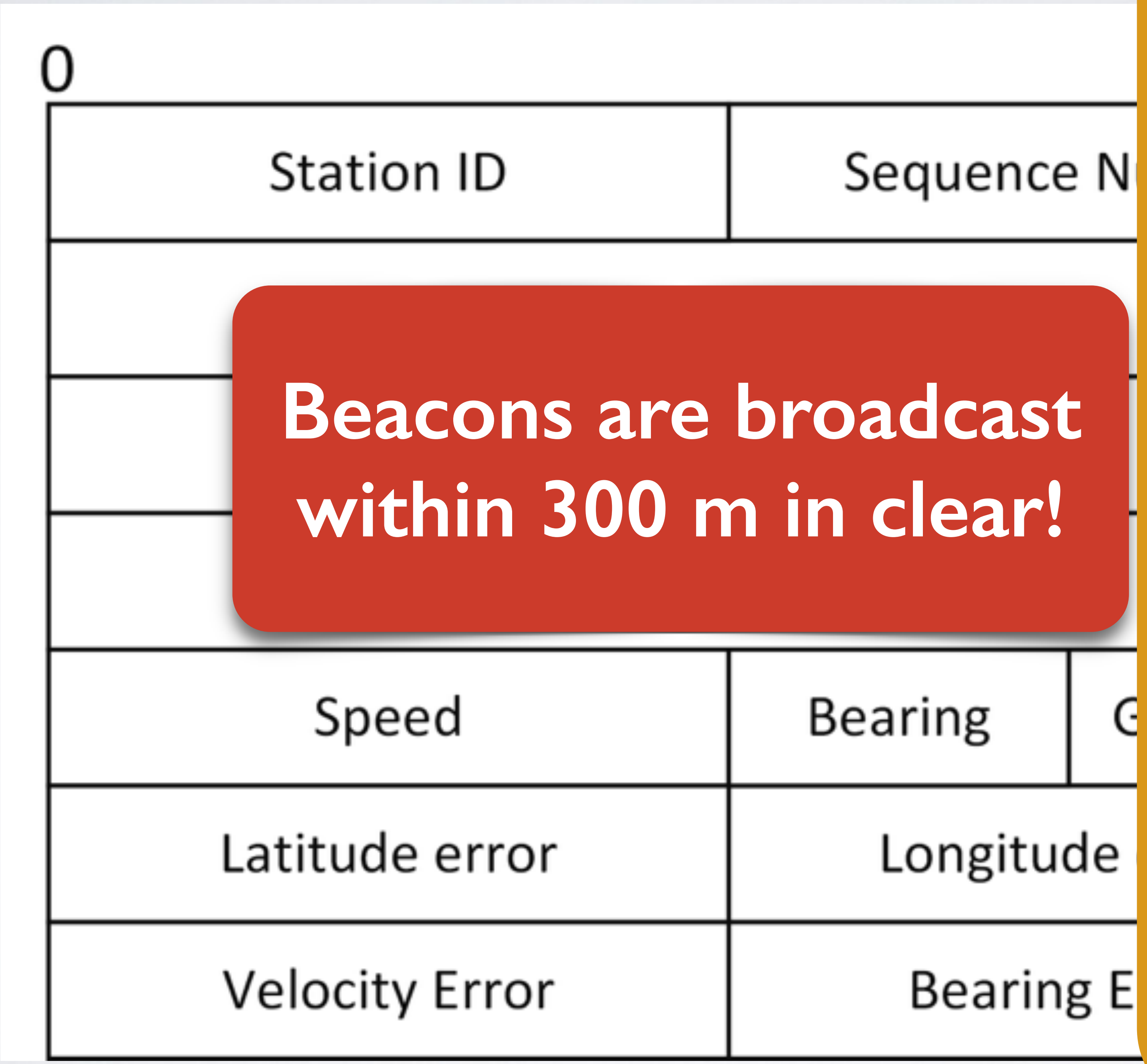
CONTENT OF BEACON



0		8
Station ID	Sequence Number	
Speed	Bearing	GPS Mode
Latitude error	Longitude error	
Velocity Error	Bearing Error	

Beacons are broadcast within 300 m in clear!

CONTENT OF BEACON



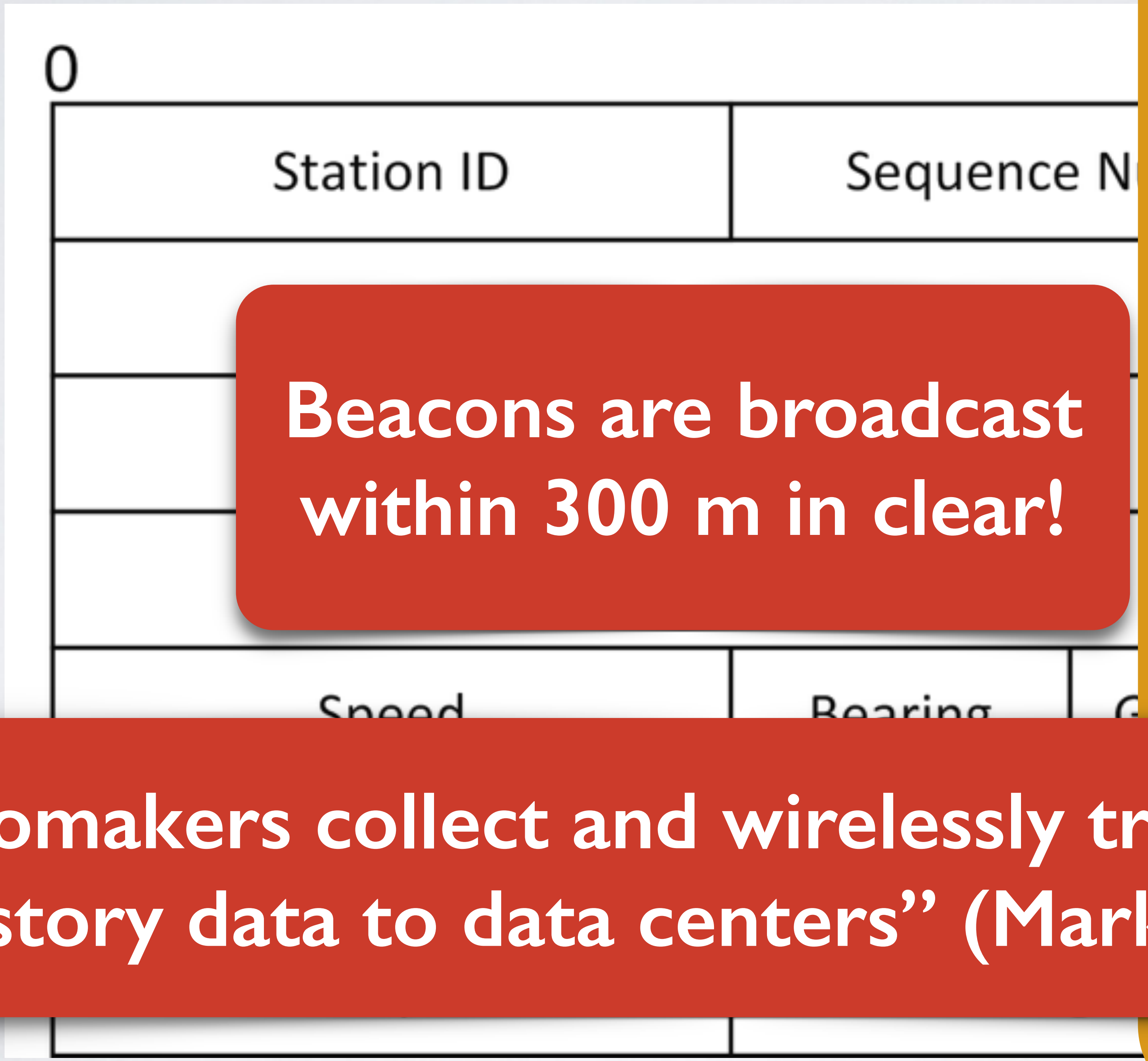
0

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

Beacons are broadcast within 300 m in clear!

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

CONTENT OF BEACON



0

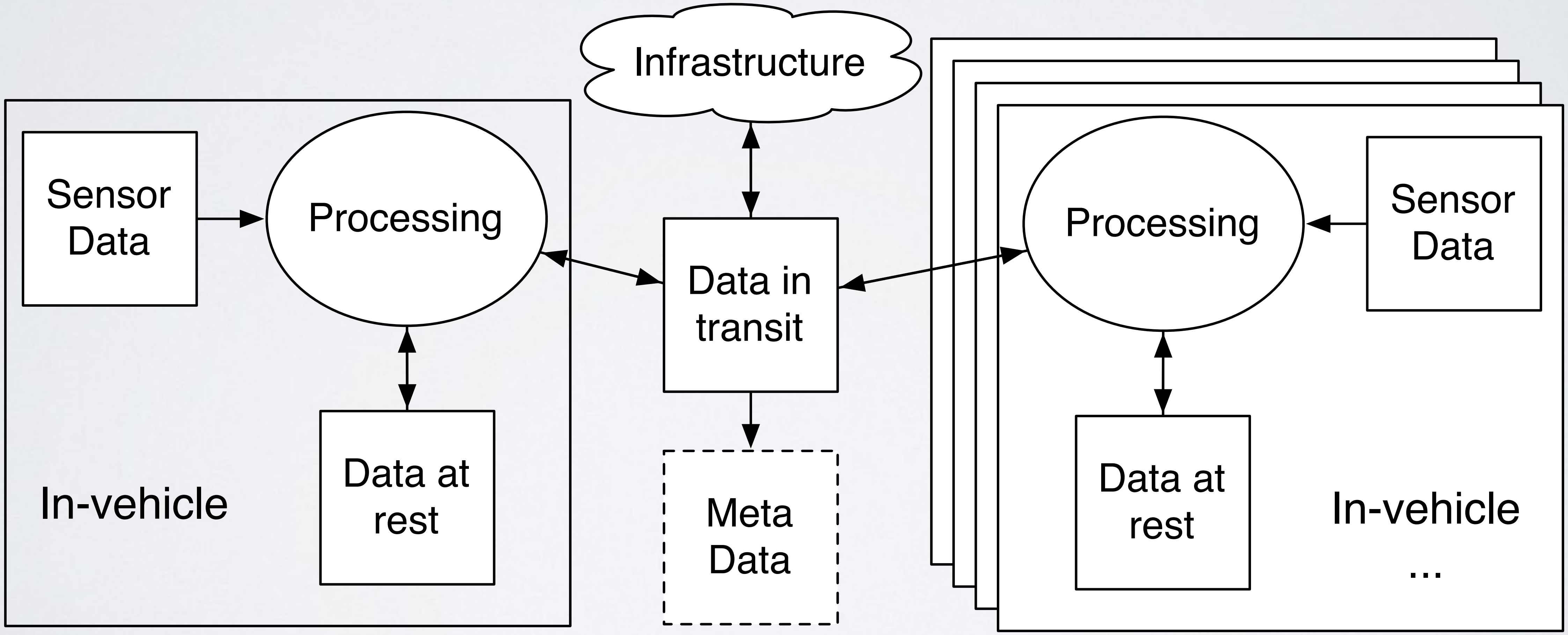
Station ID	Sequence N
Speed	Bearing

Beacons are broadcast within 300 m in clear!

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

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

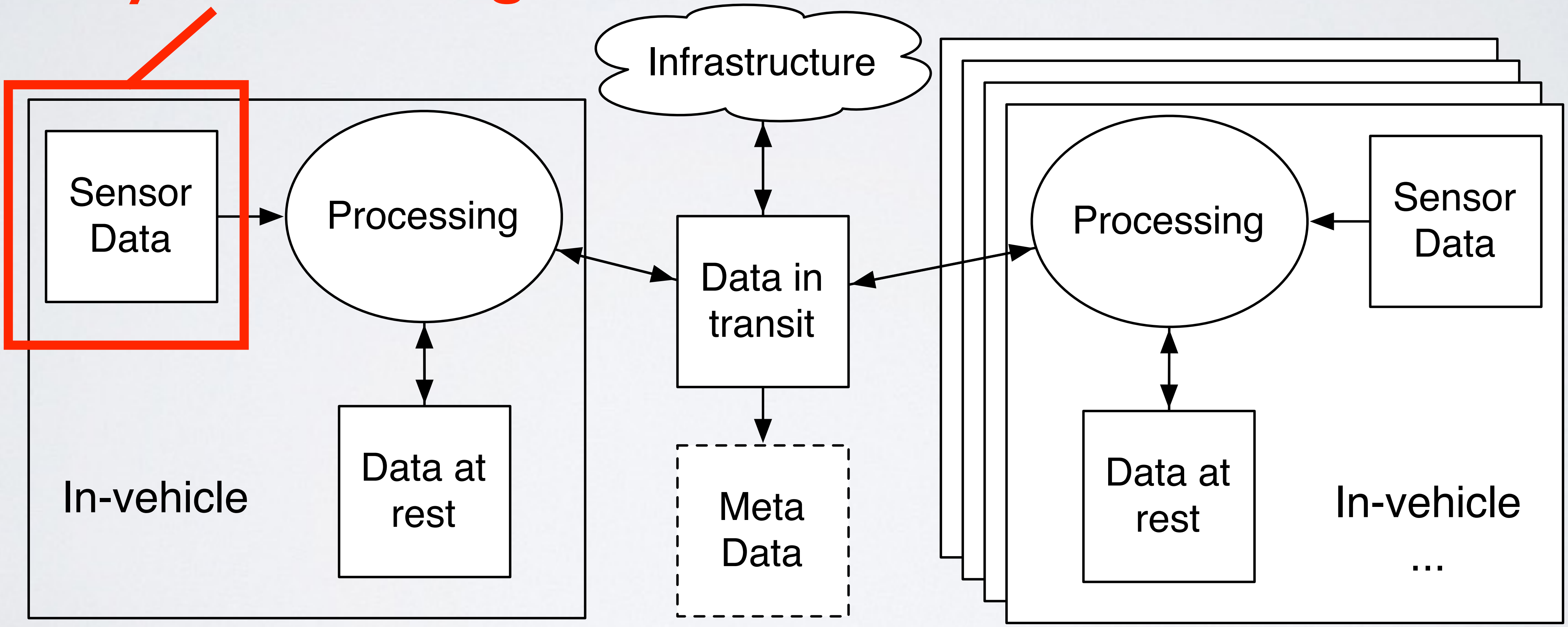
PRIVACY VIOLATIONS



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

PRIVACY VIOLATIONS

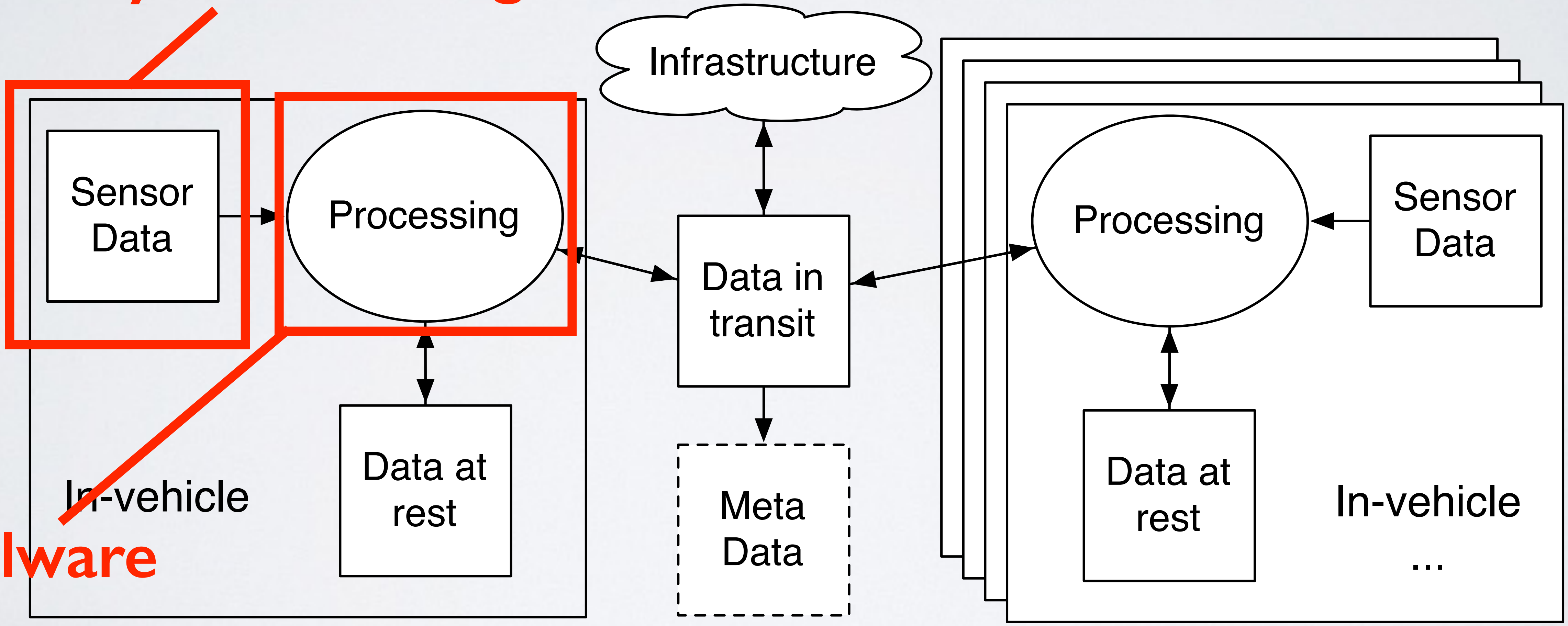
collect information about me, my car, and my surroundings



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

PRIVACY VIOLATIONS

collect information about
me, my car,
and my surroundings

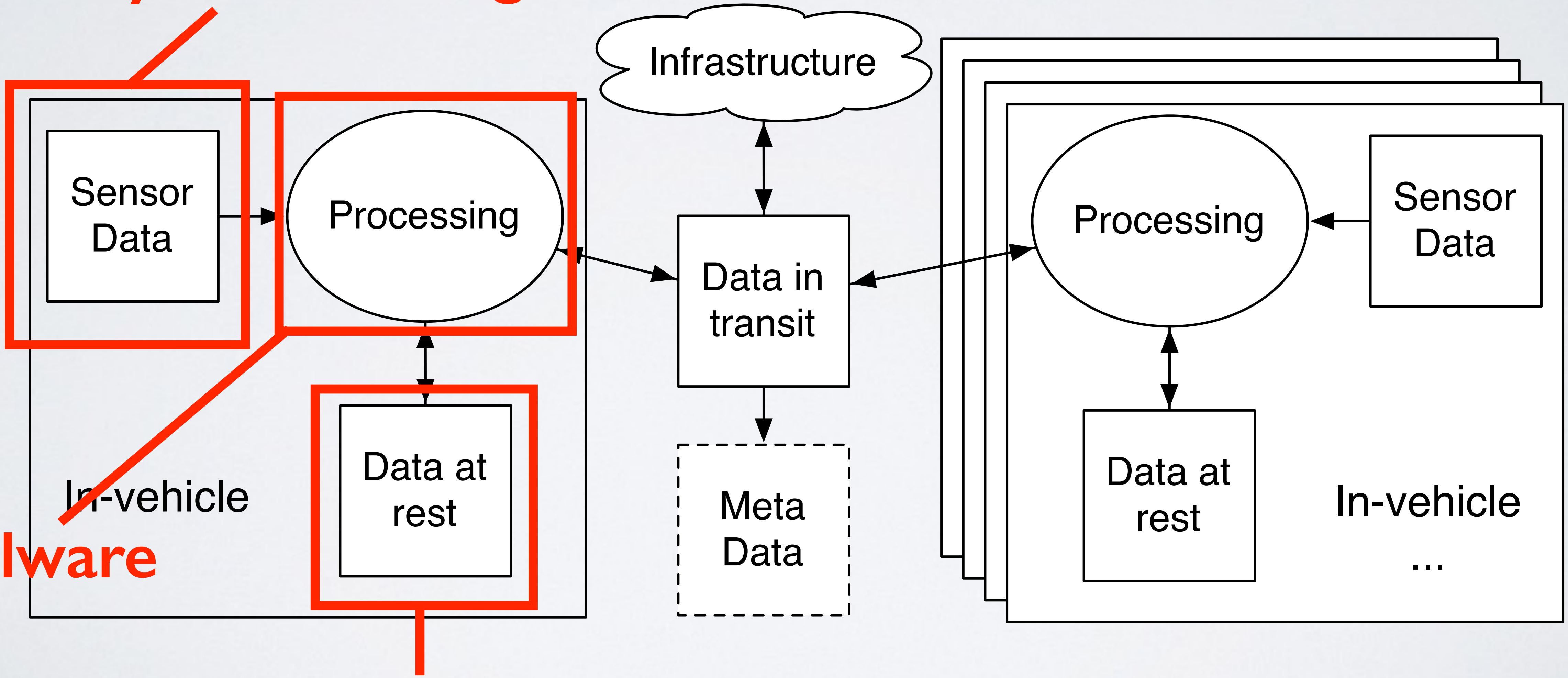


malware

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

PRIVACY VIOLATIONS

collect information about
me, my car,
and my surroundings

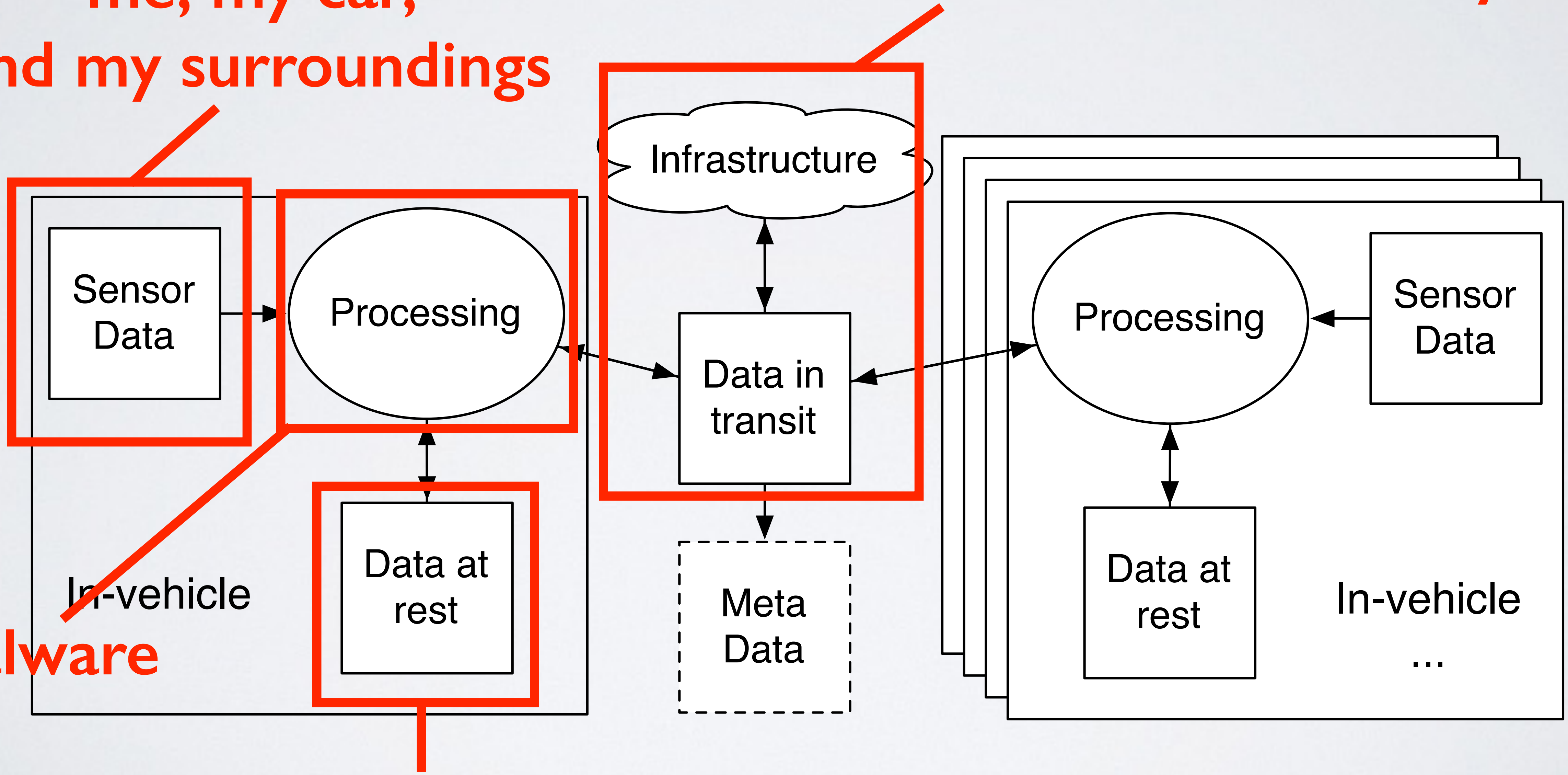


malware

store information

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

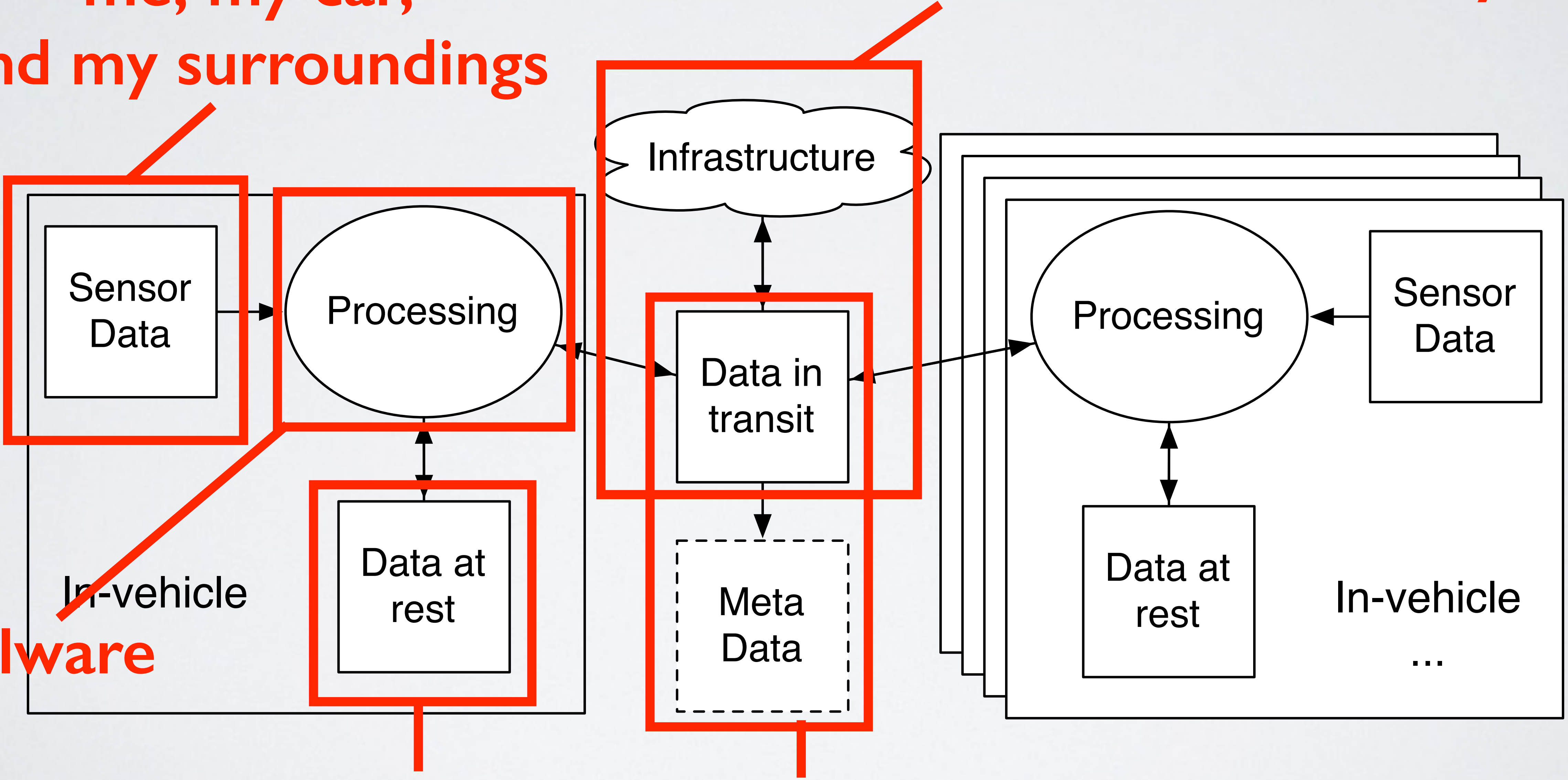
store information

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

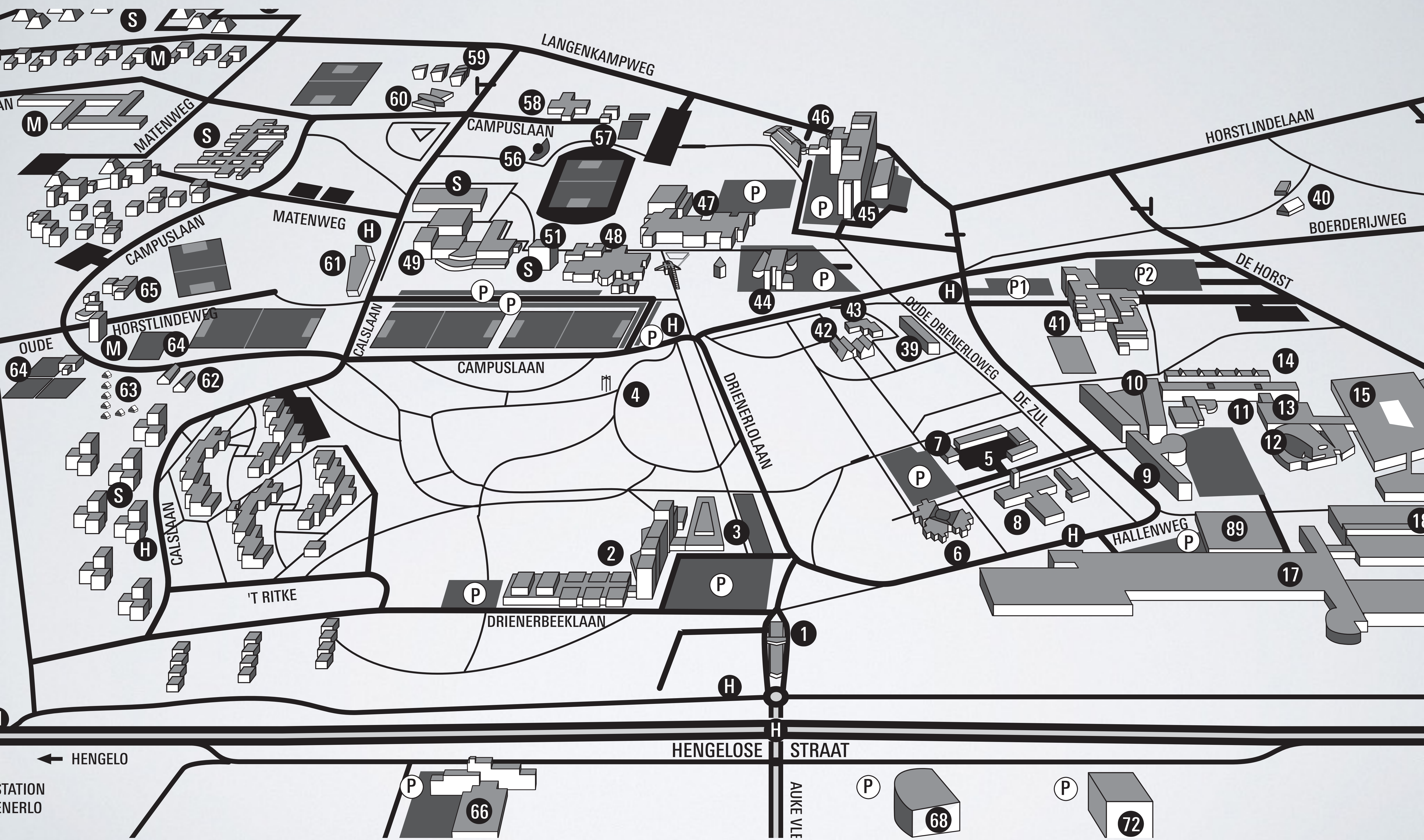


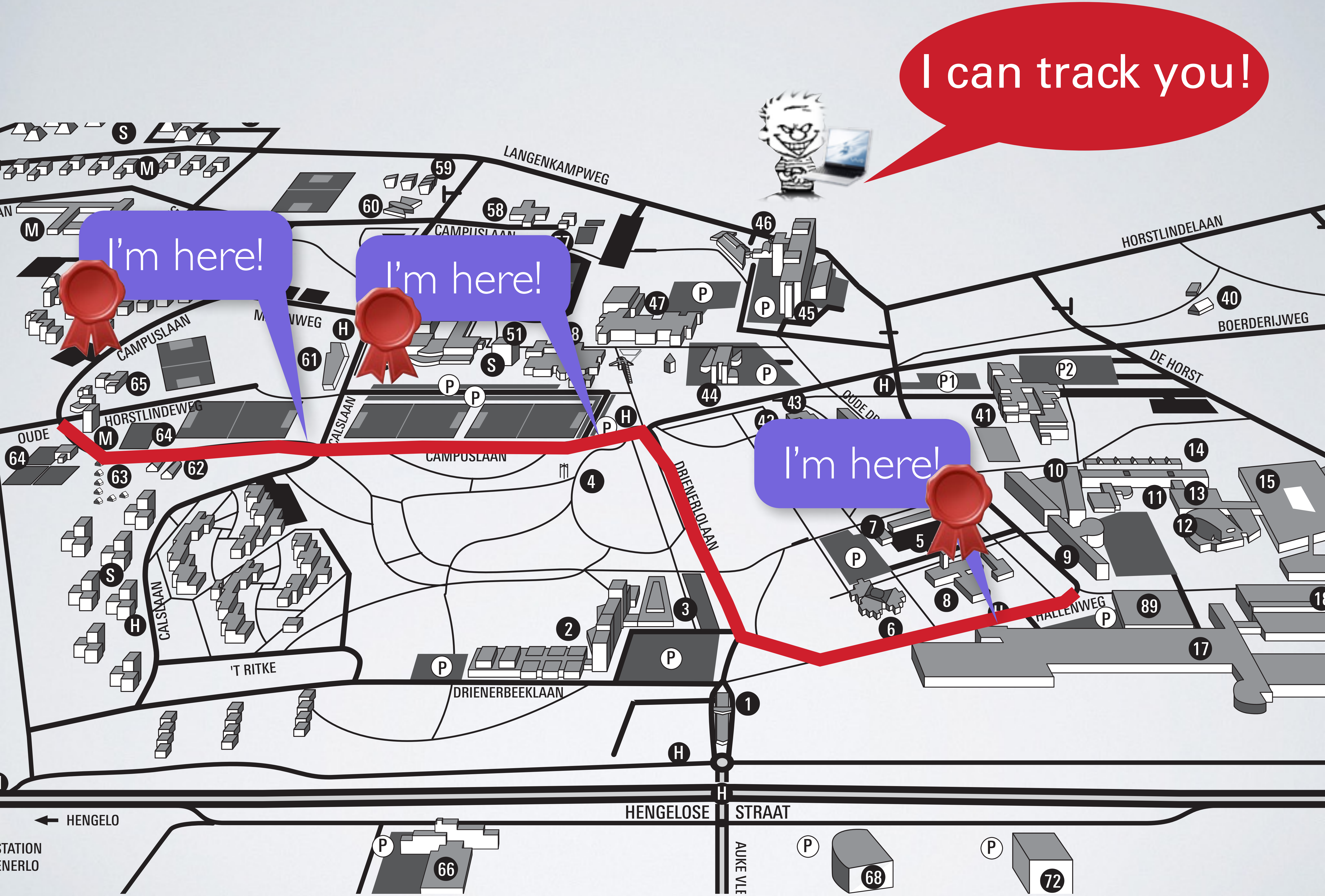
malware

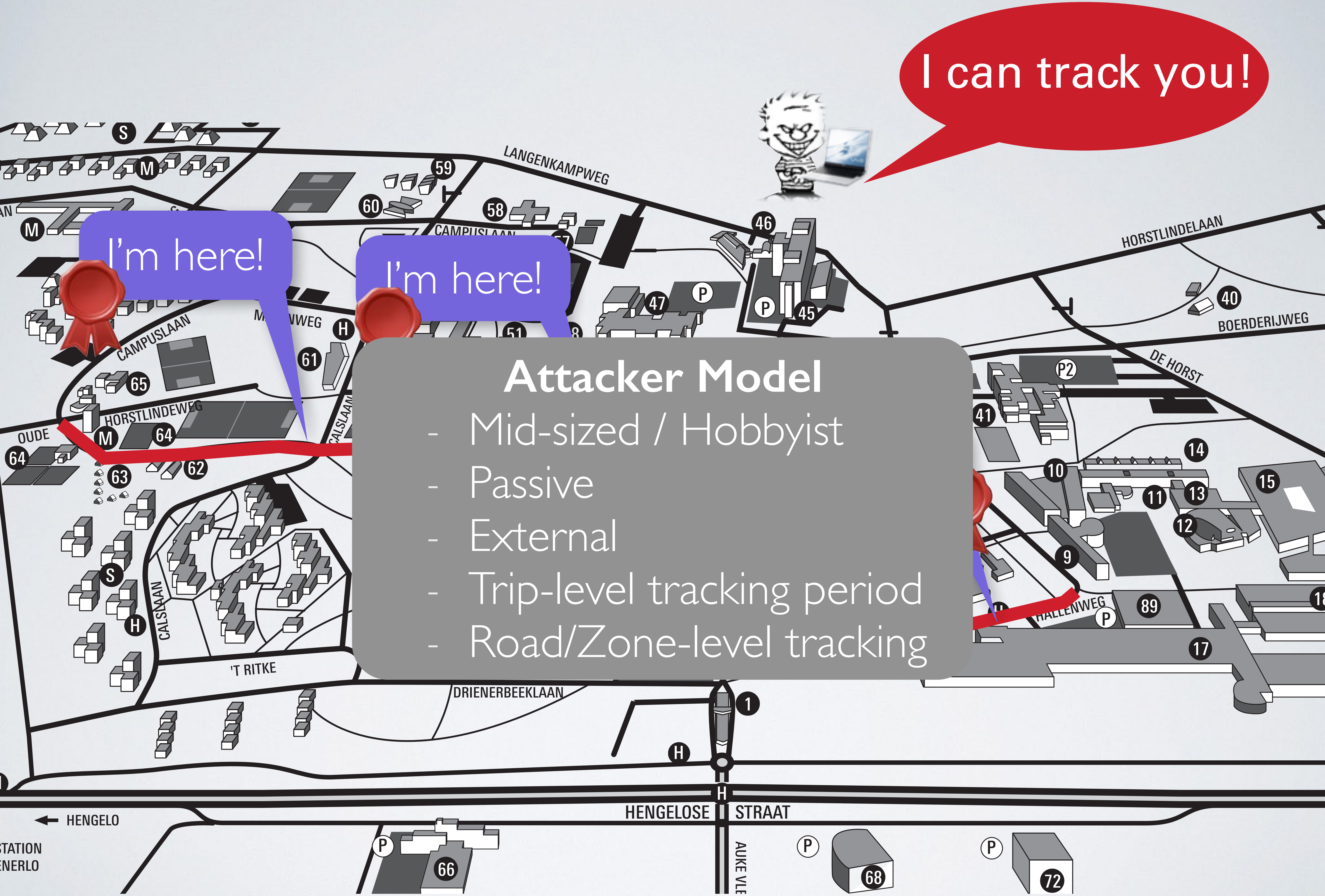
store information

privacy inferences

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


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


I can track you!
I'm here!
I'm here!
I'm here!
LANGENKAMPWEG
CAMPUSLAAN
CAMPUSLAAN
CAMPUSLAAN
HORSTLINDELAAN
BOERDERIJWEG
DE HORST
HORSTLINDEWEG
OUDE
CALSLAAN
CALSLAAN
DRIENERLOLAAN
OUDE DR
HALLENWEG
'T RITKE
DRIENERBEEKLAAN
HENGELOSE
STRAAT
HENGELO
STATION
ENERLO
AUKE VLE
P1
P2



Attacker Model

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

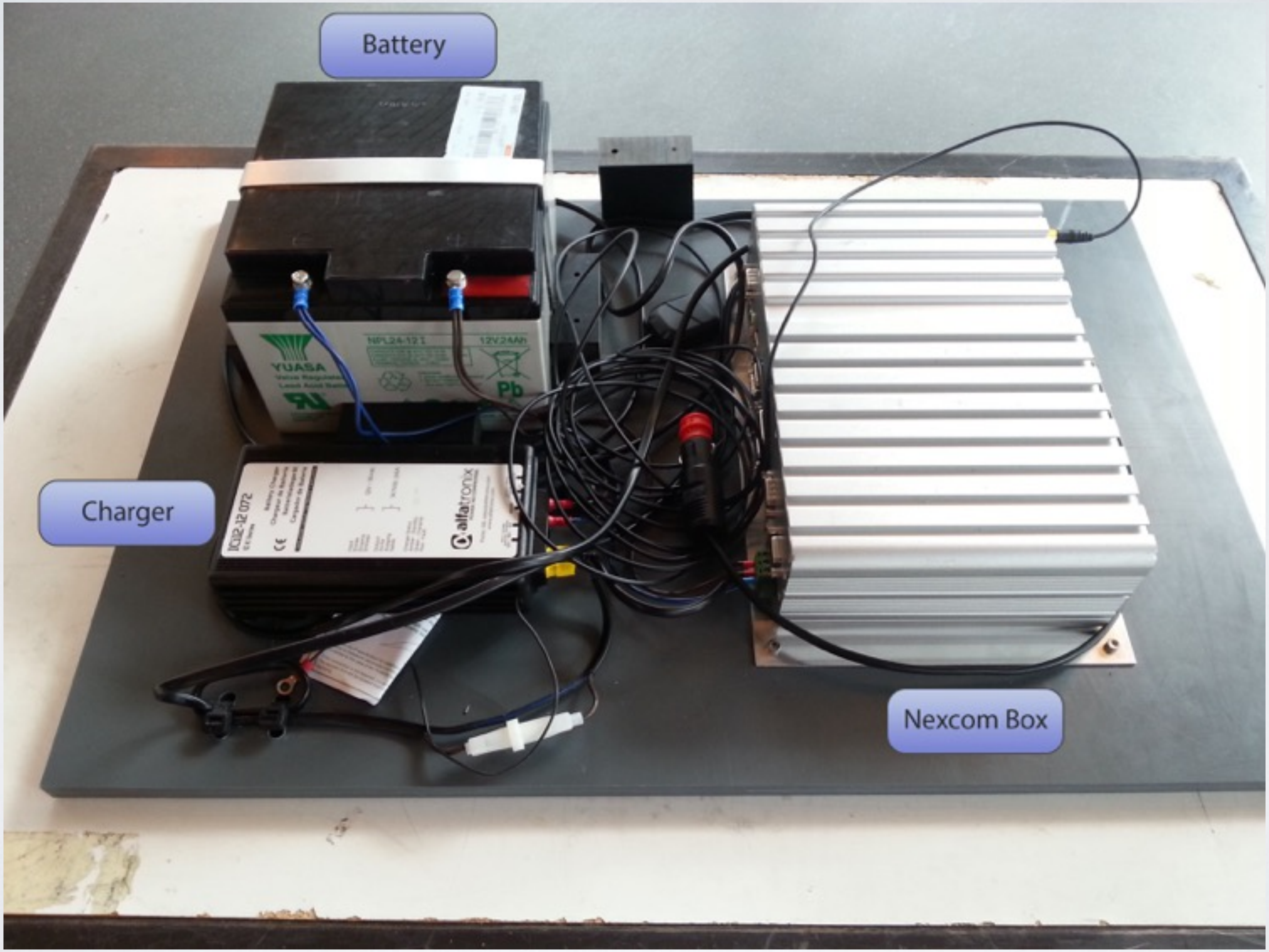
I can track you!
I'm here!
I'm here!
LANGENKAMPWEG
CAMPUSLAAN
HORSTLINDELAAN
BOERDERIJWEG
DE HORST
HORSTLINDEWEG
OUDE
CALSLAAN
'T RITKE
DRIENERBEEKLAAN
HALLENWEG
HENGELO
STATION
ENERLO

Attacker Model

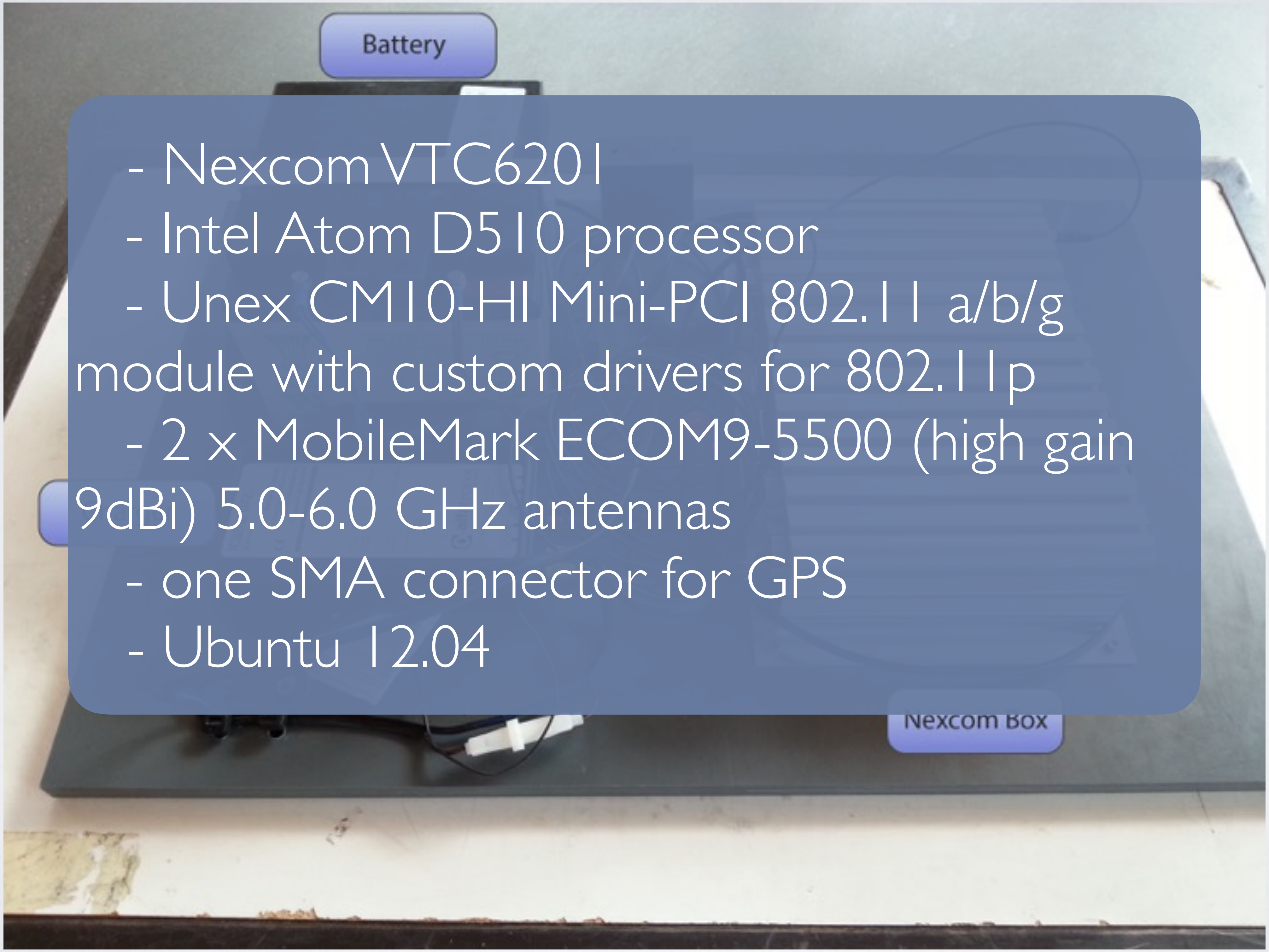
- Mid-sized / Hobbyist
- Passive
- External
- Trip-level tracking period
- Road/Zone-level tracking

Let's track the security guard vehicle!

EXPERIMENTAL SETUP (1/4)



EXPERIMENTAL SETUP (1/4)

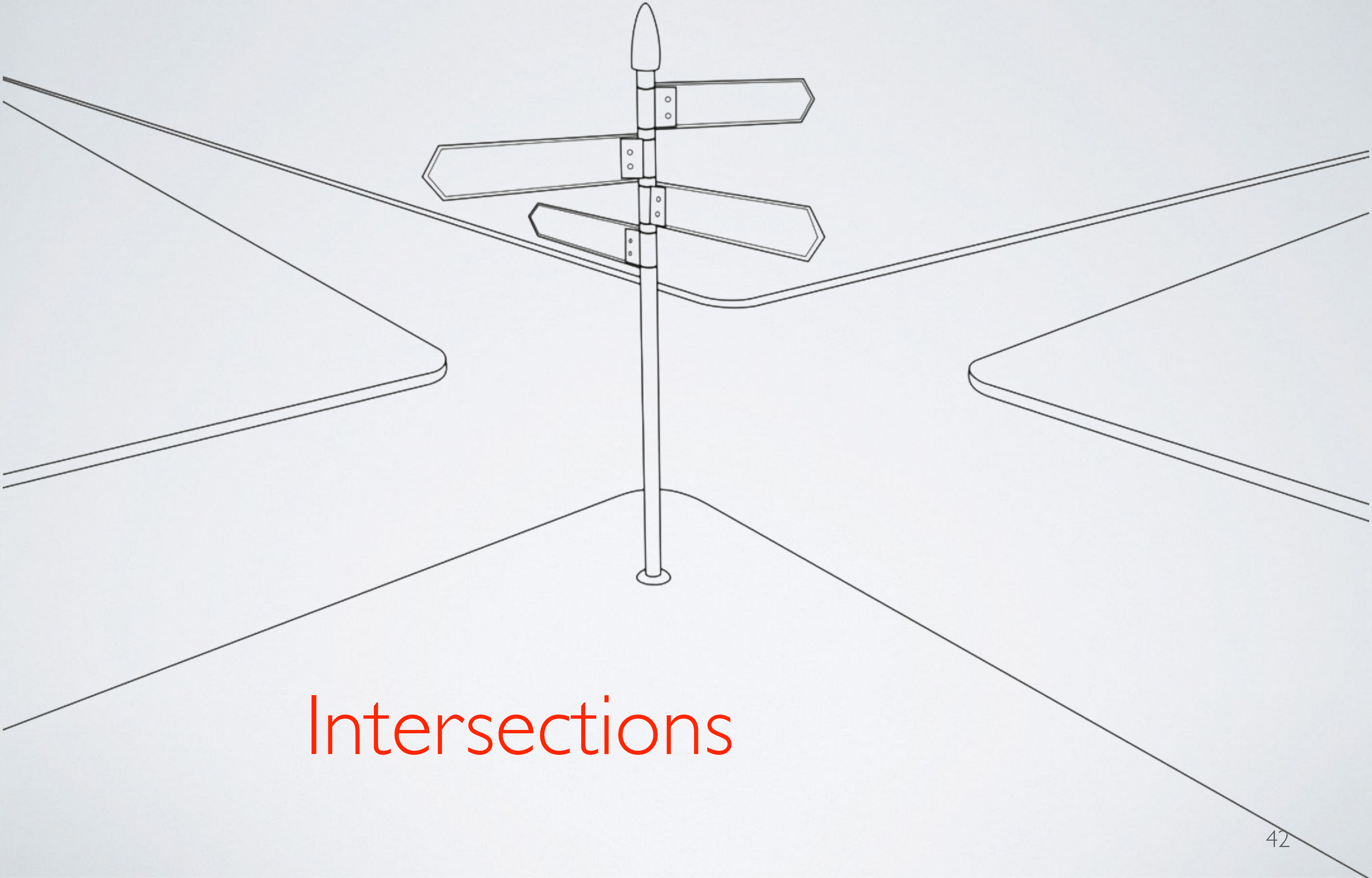


- Nexcom VTC6201
- Intel Atom D510 processor
- Unex CM10-HI Mini-PCI 802.11 a/b/g module with custom drivers for 802.11p
- 2 x MobileMark ECOM9-5500 (high gain 9dBi) 5.0-6.0 GHz antennas
- one SMA connector for GPS
- Ubuntu 12.04

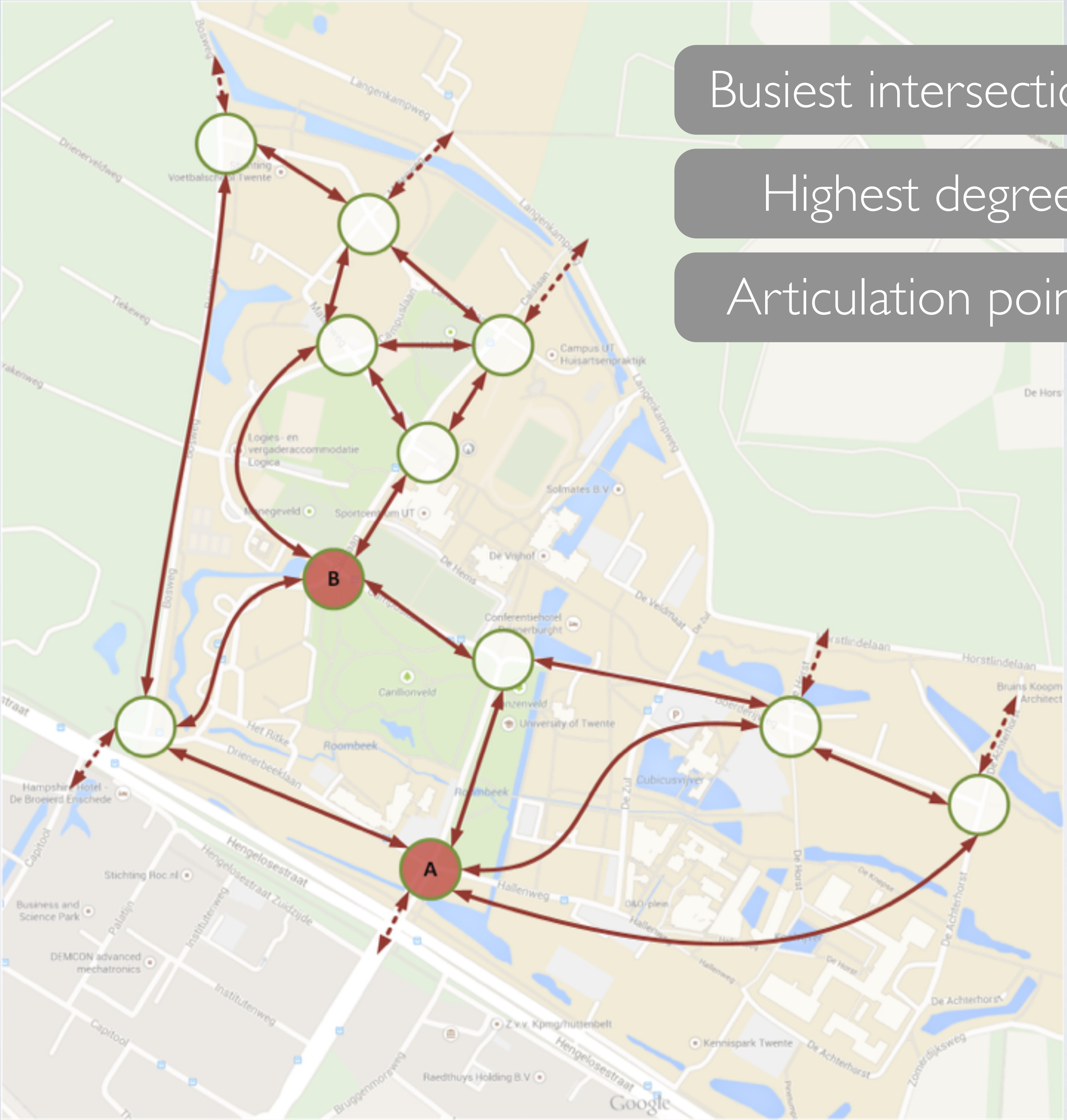
EXPERIMENTAL SETUP (2/4)

EXPERIMENTAL SETUP (3/4)

Where should an attacker deploy sniffing stations?



Intersections



Busiest intersections

Highest degree

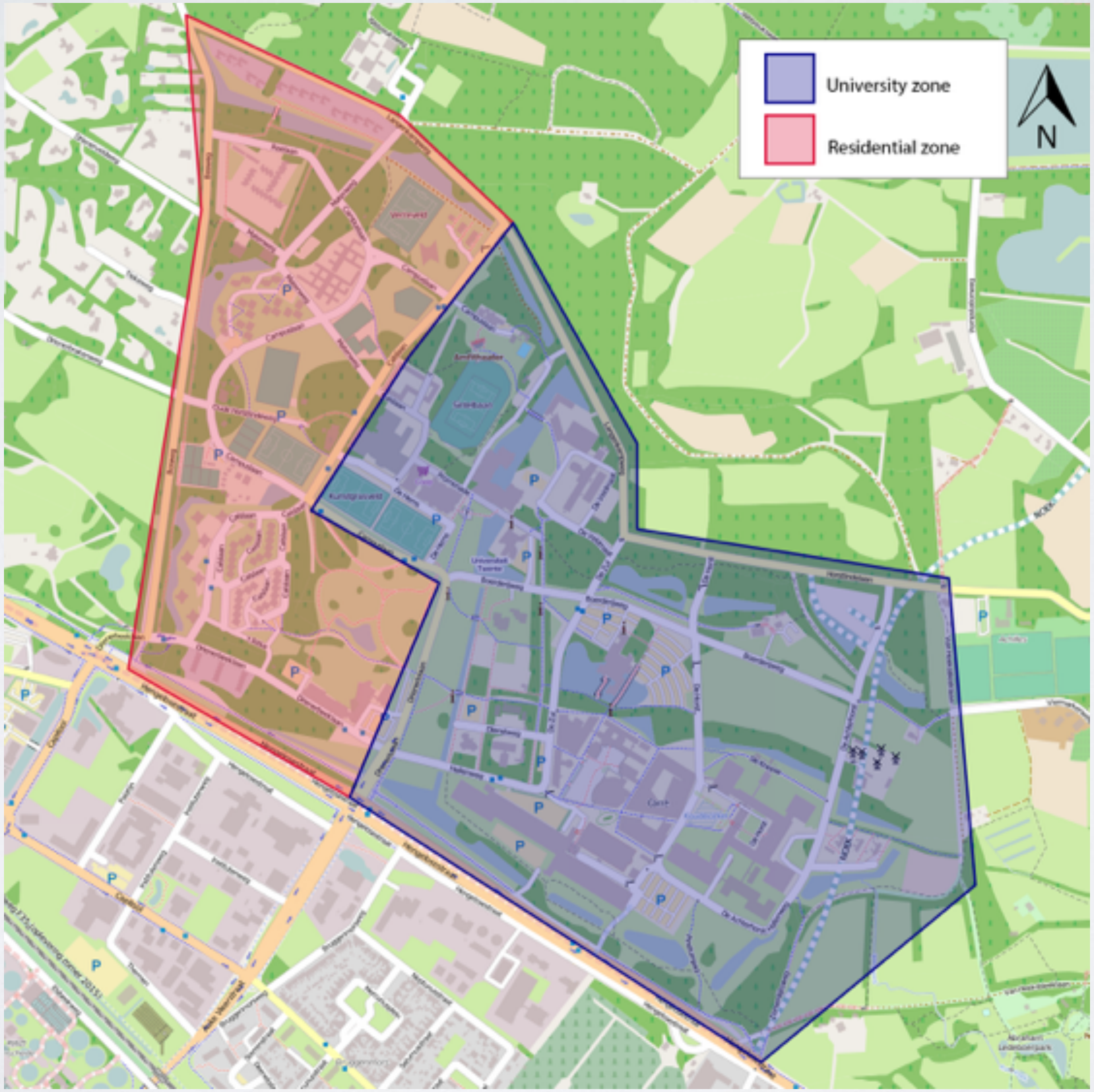
Articulation points

EXPERIMENTAL SETUP (4/4)

Intersection A
Ground floor
75 m from intersection
2 x Smarteq V09/54
antennas (9 dBi gain)

Intersection B
1st floor
110 m from intersection
2 x Smarteq V09/54
antennas (9 dBi gain)

ZONE-LEVEL TRACKING



The equipment was deployed for

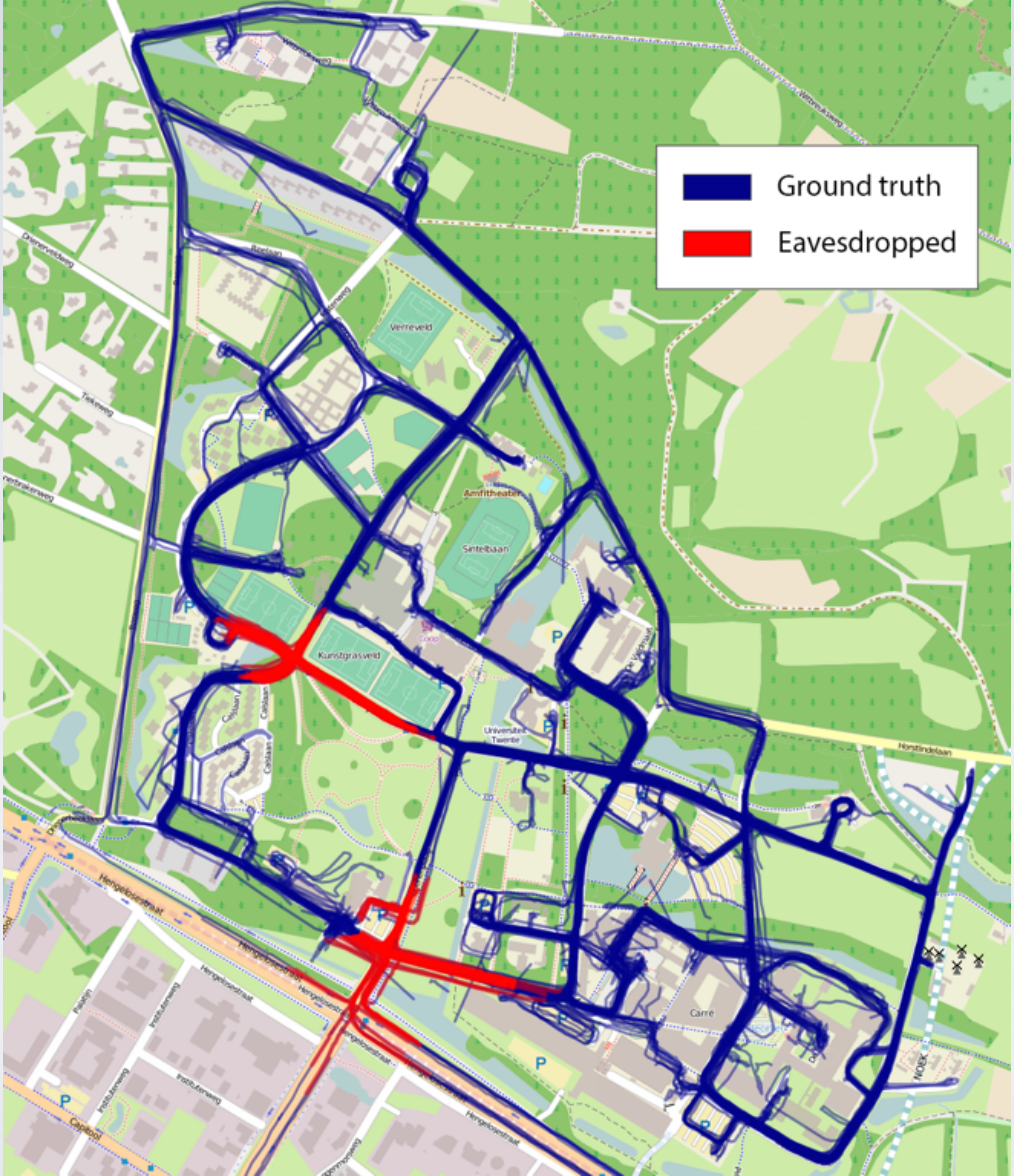
16 days

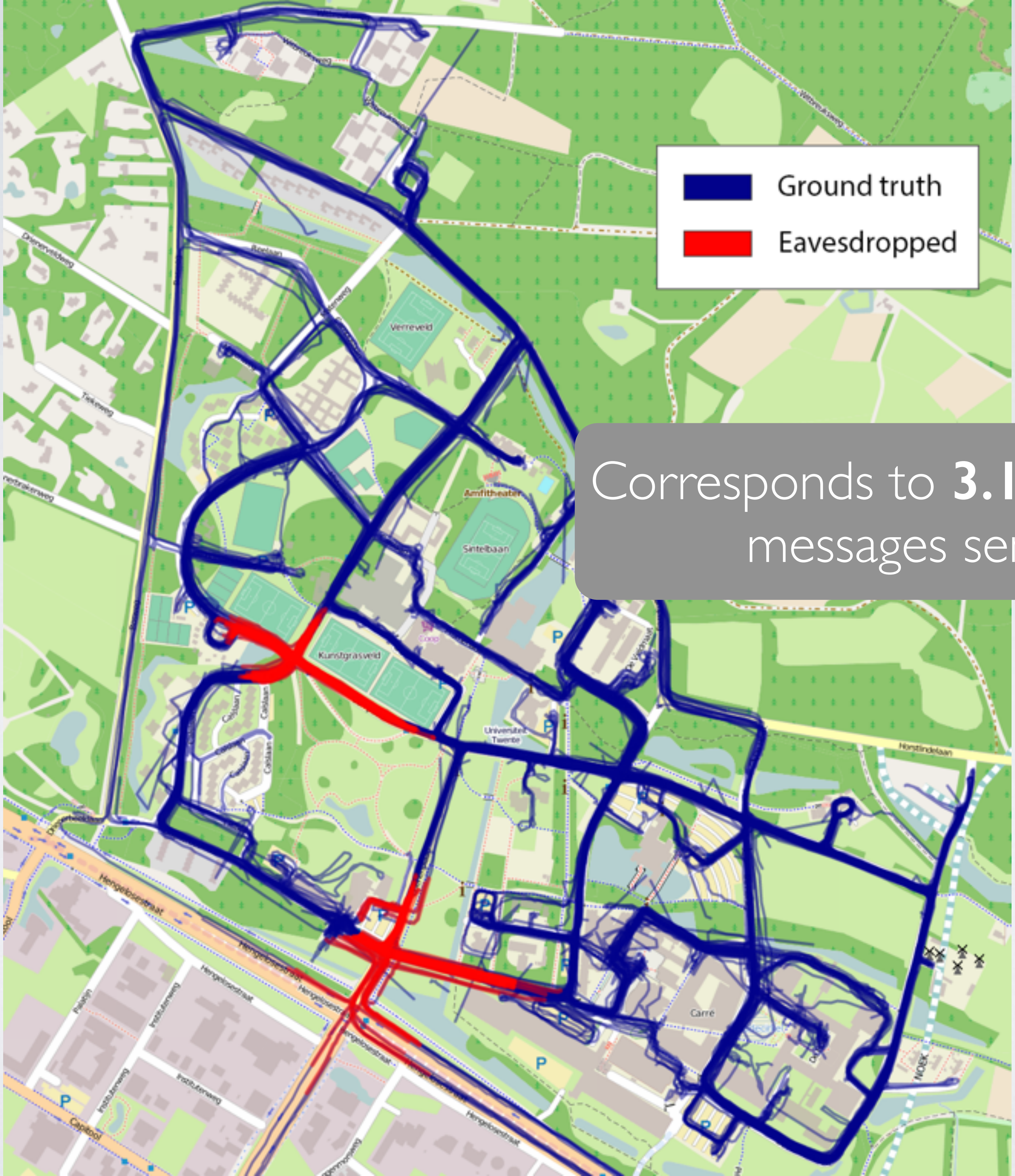
during which the vehicle transmitted

2,734,691 messages

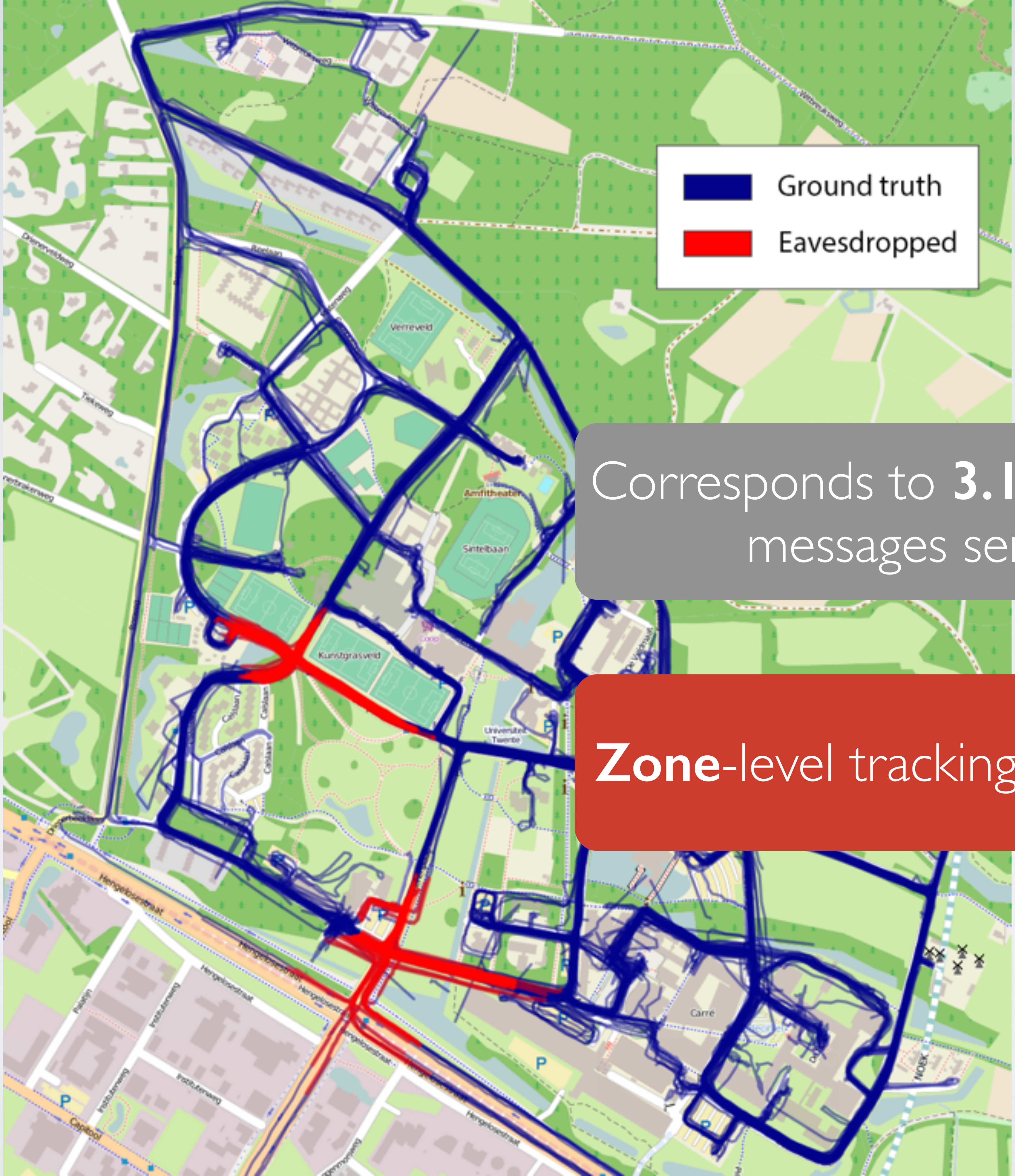
and we eavesdropped on

68,542 messages


Ground truth
Eavesdropped
Verreveld
Amfitheater
Sintelbaan
Kunstgrasveld
Universiteit Twente
Carre
Hengelosestraat
Horstlindelaan
Calslaan
Boelaan



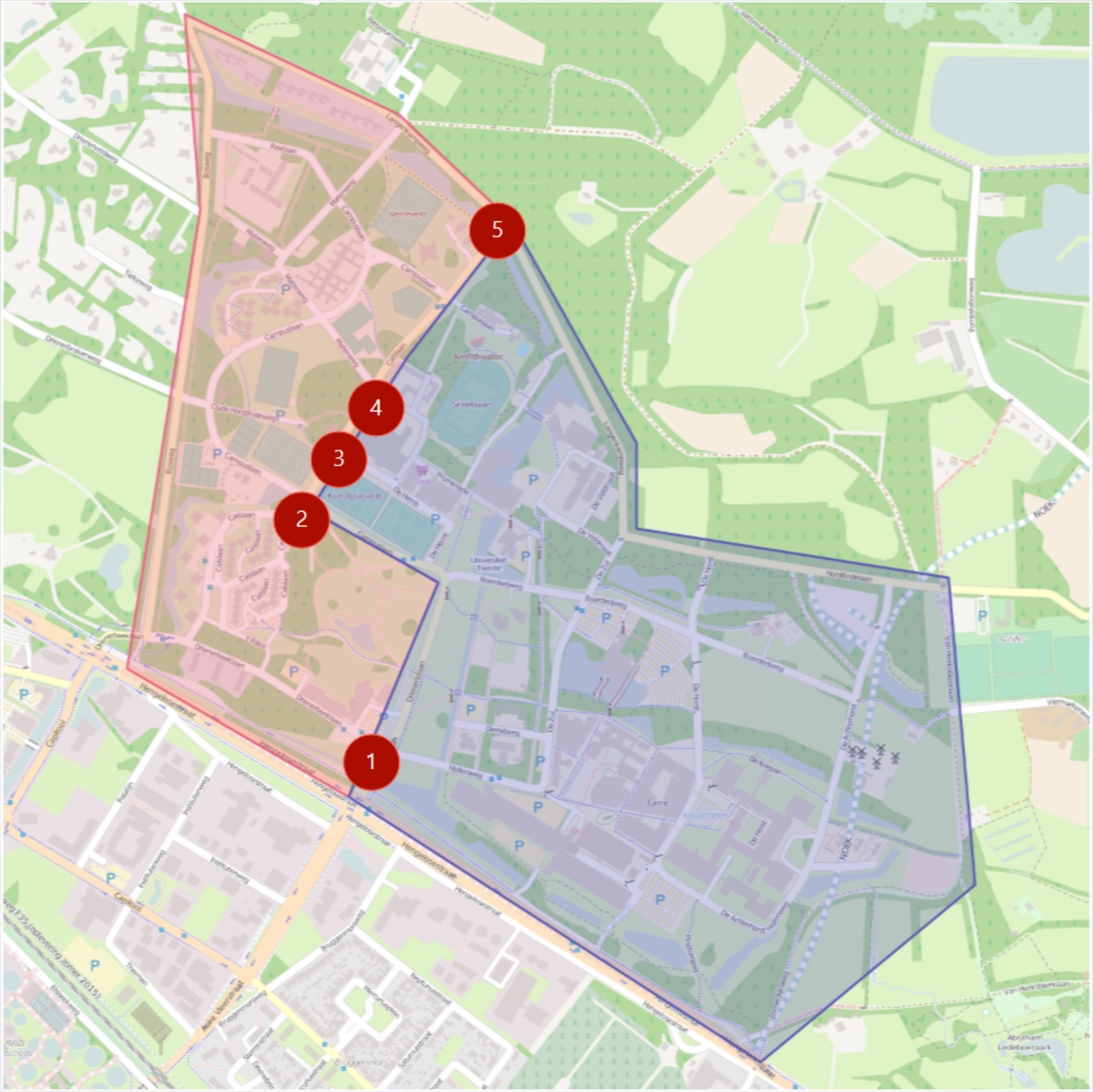
Corresponds to **3.17%** of all messages sent



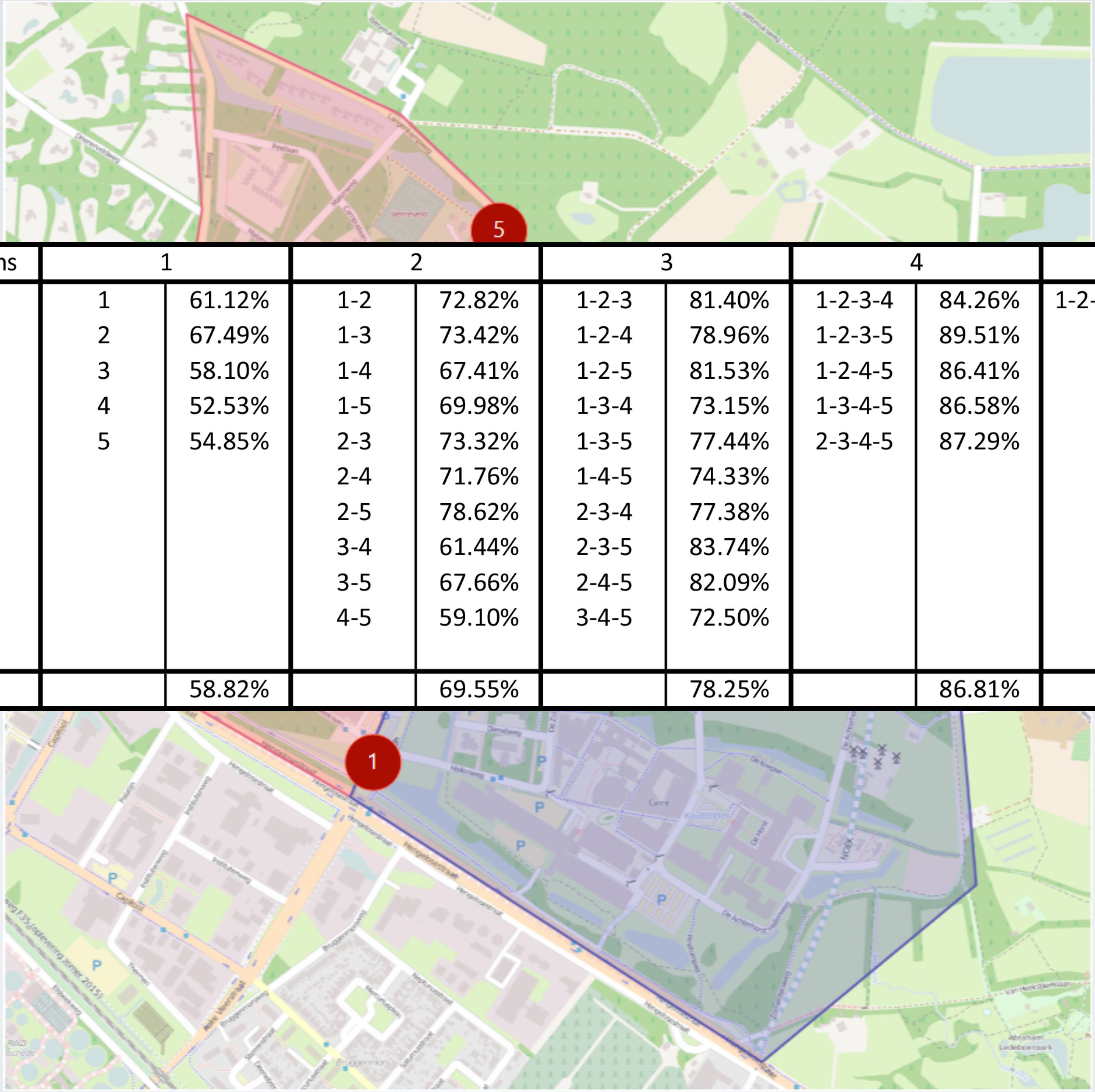
Corresponds to **3.17%** of all messages sent

Zone-level tracking: **72.82%**

TRACKING ACCURACY (MLZ)

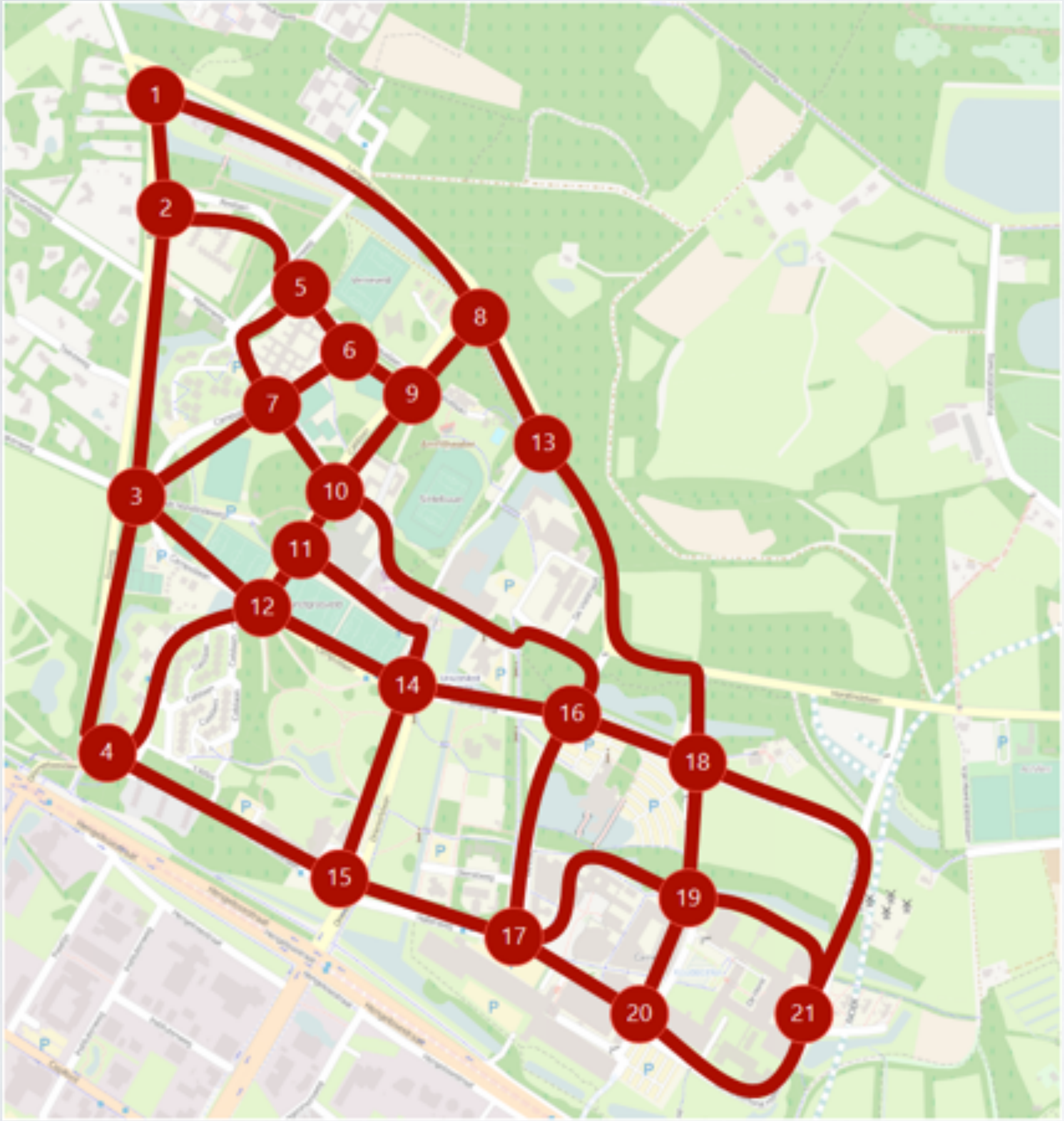


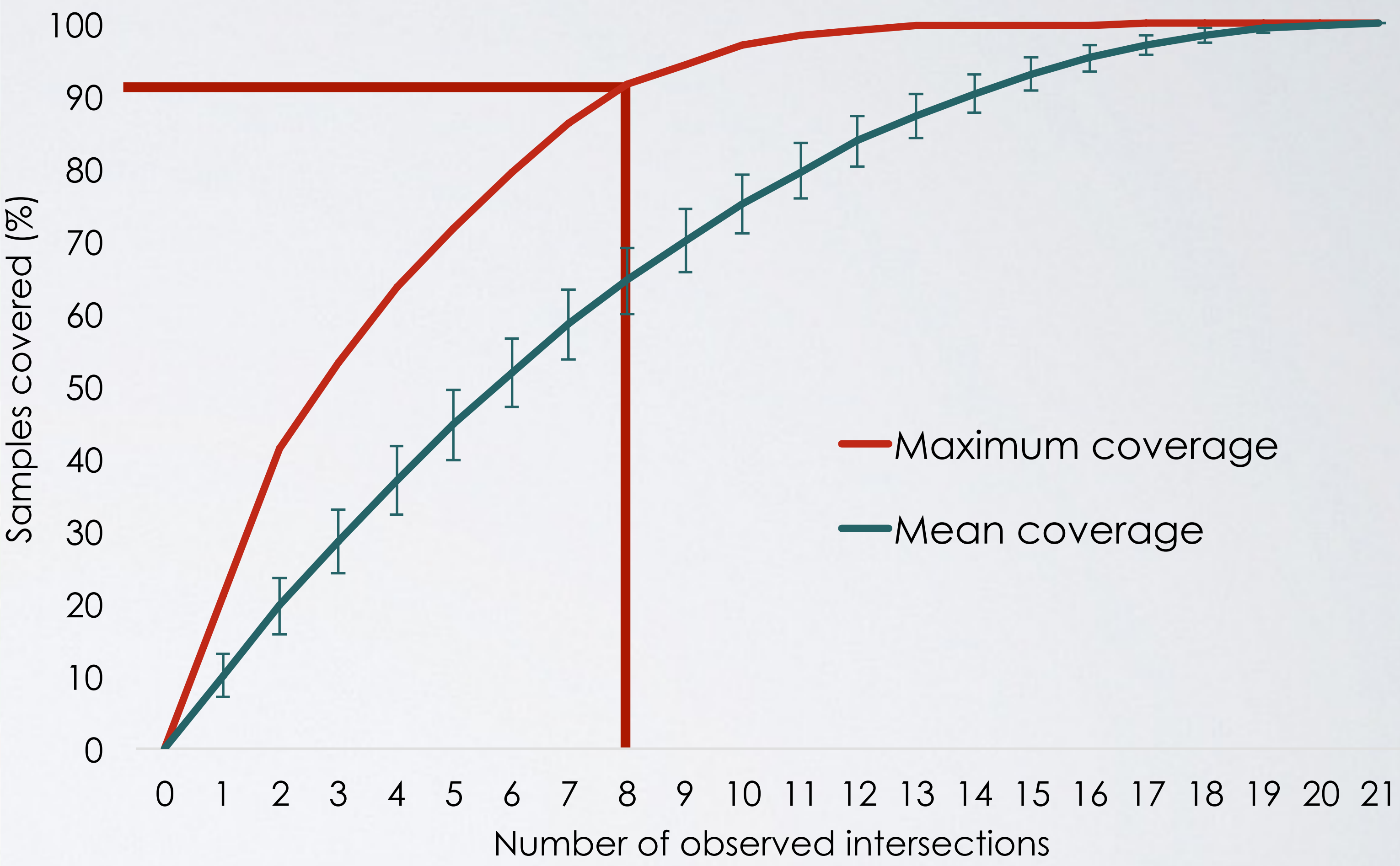
TRACKING ACCURACY (MLZ)



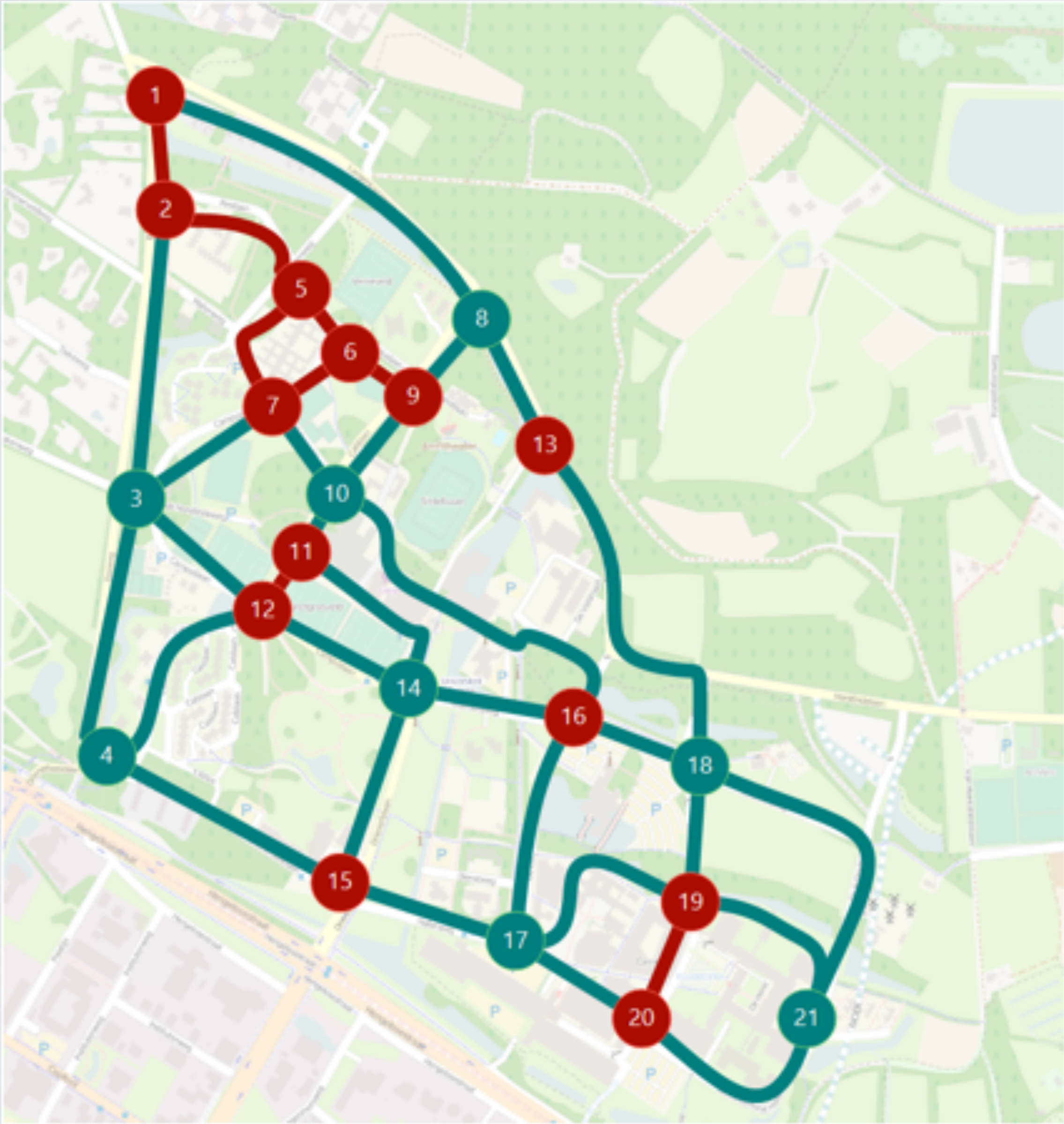
# of intersections	1		2		3		4		5	
	1	61.12%	1-2	72.82%	1-2-3	81.40%	1-2-3-4	84.26%	1-2-3-4-5	95.28%
	2	67.49%	1-3	73.42%	1-2-4	78.96%	1-2-3-5	89.51%		
	3	58.10%	1-4	67.41%	1-2-5	81.53%	1-2-4-5	86.41%		
	4	52.53%	1-5	69.98%	1-3-4	73.15%	1-3-4-5	86.58%		
	5	54.85%	2-3	73.32%	1-3-5	77.44%	2-3-4-5	87.29%		
			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%

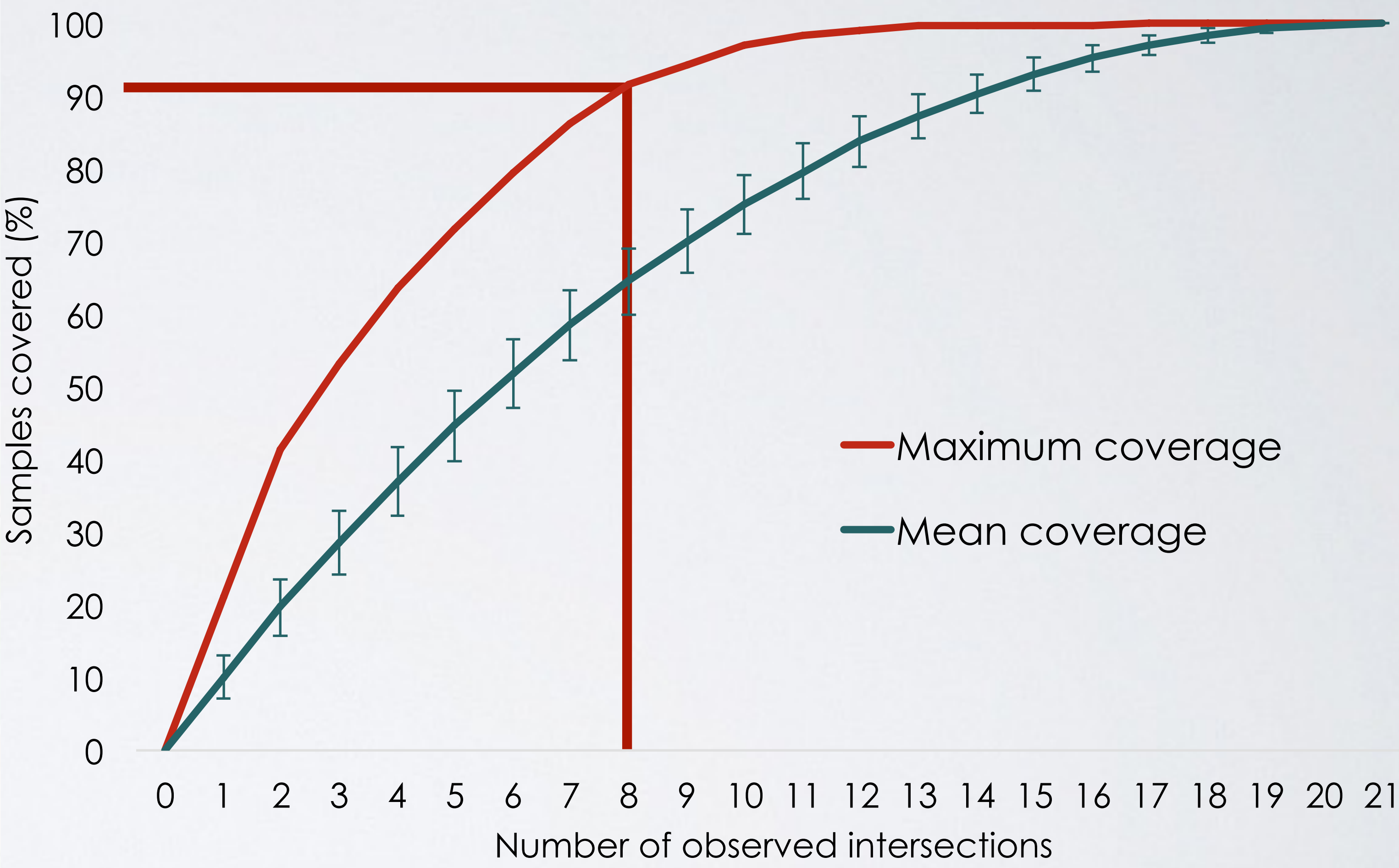
TRACKING ACCURACY (MLR)





TRACKING ACCURACY (MLR)





Can we

STOP

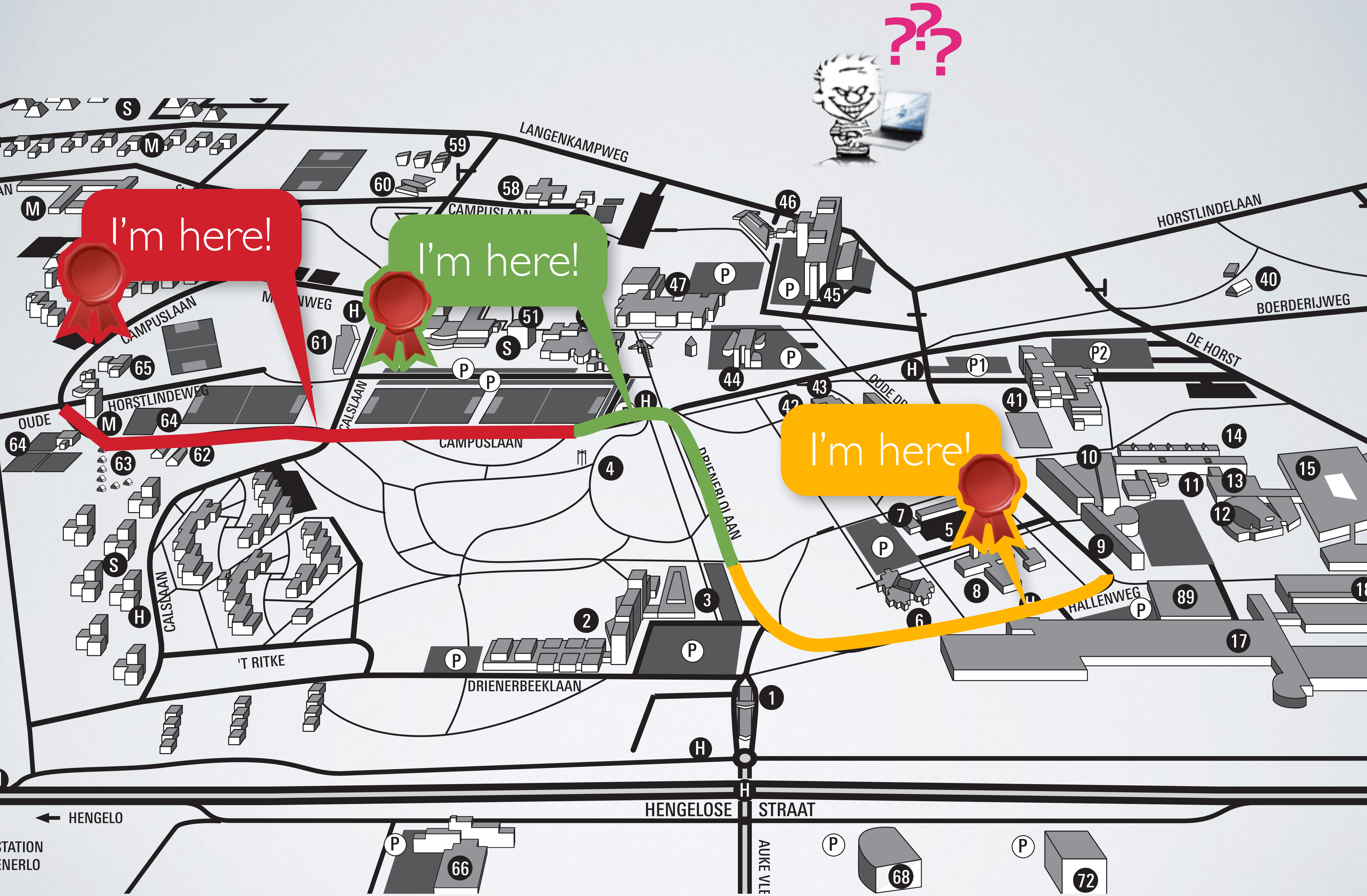
tracking?

CANDIDATE SOLUTIONS

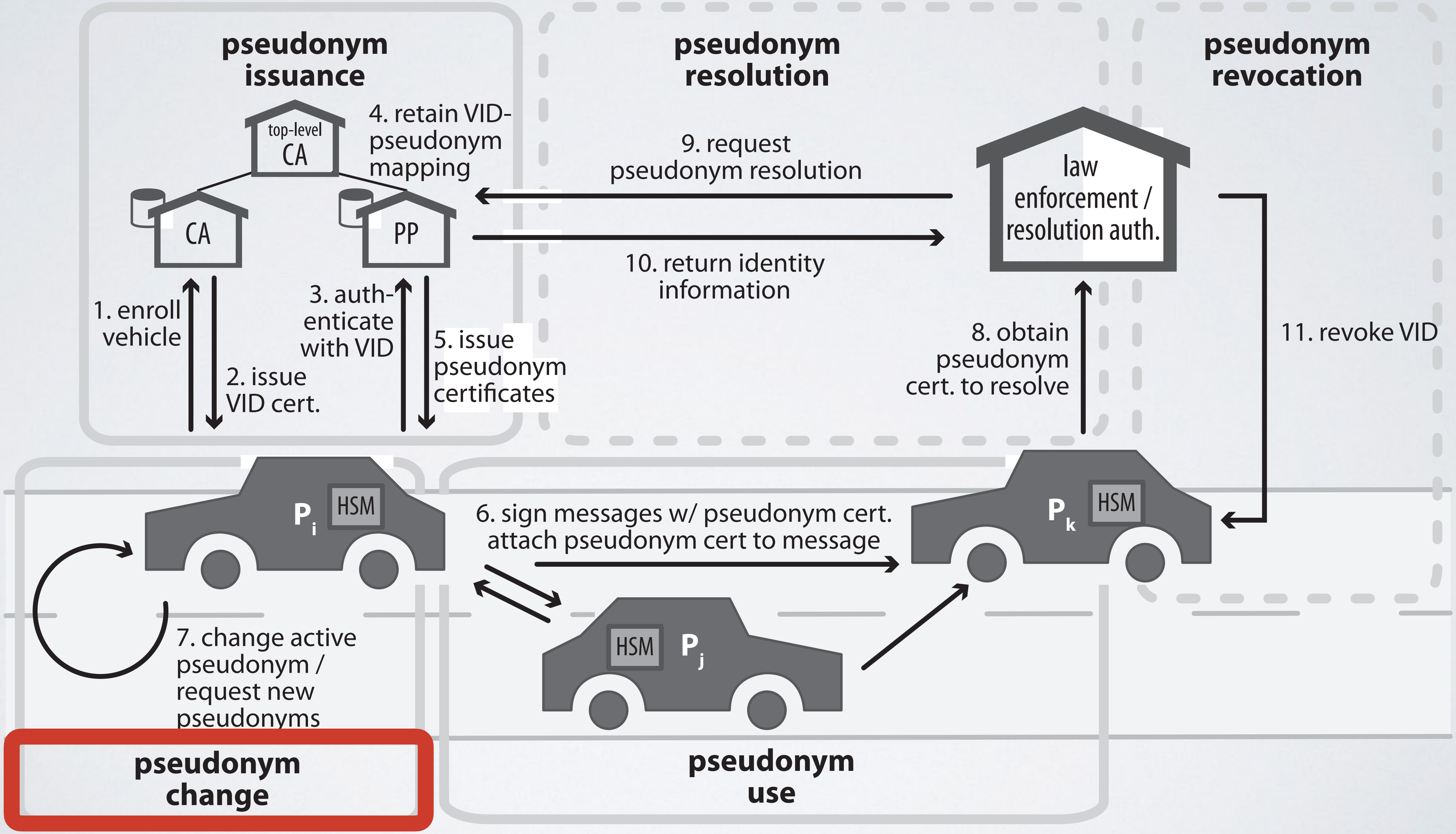
- Cloaking/Fuzzing location
- Anonymous credentials
- Encryption
- Opt-out
- **Pseudonyms**

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”


??
I'm here!
I'm here!
I'm here!
LANGENKAMPWEG
CAMPUSLAAN
HORSTLINDELAAN
BOERDERIJWEG
DE HORST
HORSTLINDEWEG
CALSLAAN
DRIENERLOLAAN
HALLENWEG
'T RITKE
DRIENERBEEKLAAN
HENGELOSE STRAAT
HENGELO
AUKE VLE
STATION
ENERLO
OUDE
P1
P2

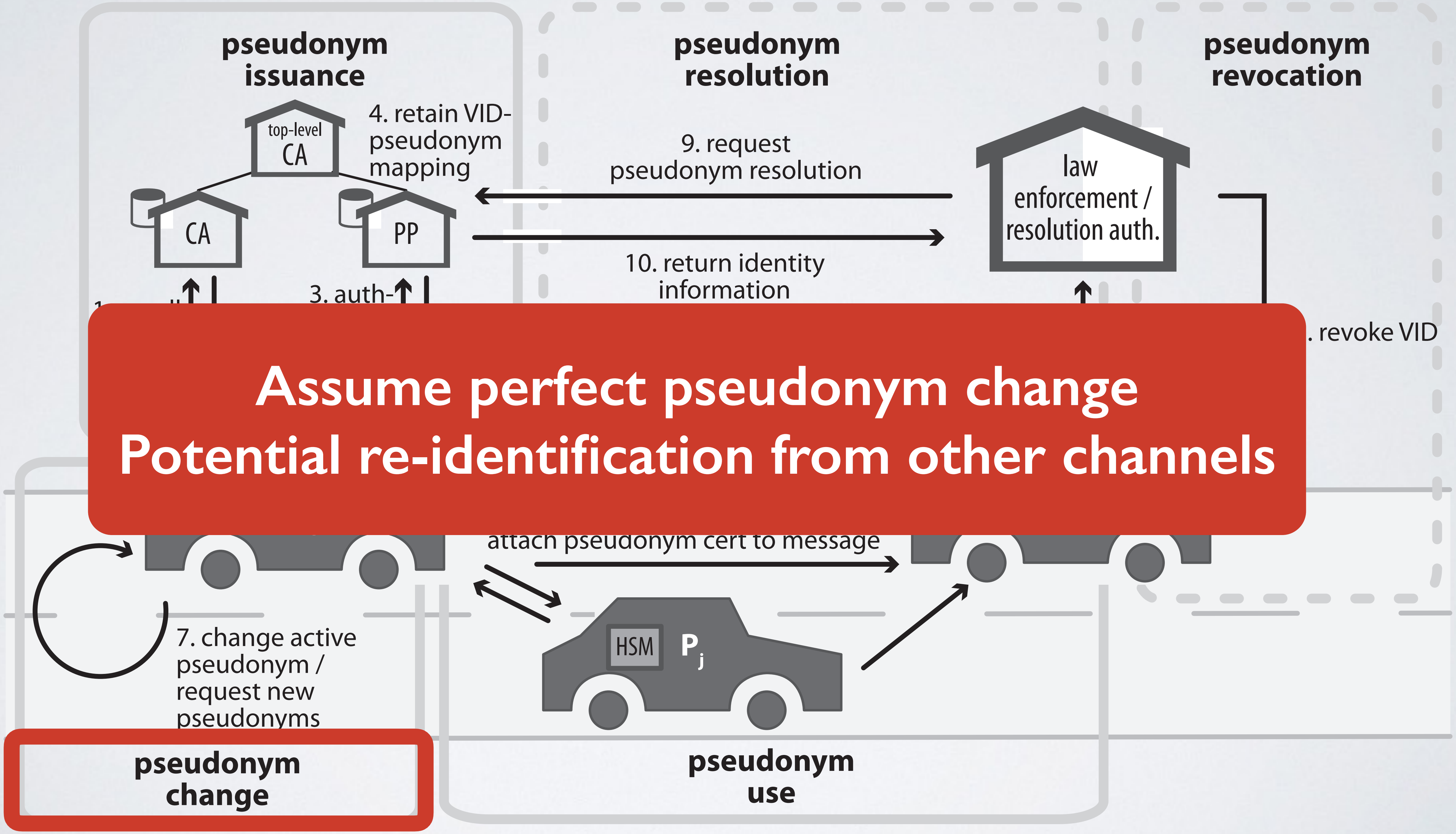
PSEUDONYM LIFECYCLE



pseudonym issuance
top-level CA
CA
PP
4. retain VID-pseudonym mapping
1. enroll vehicle
2. issue VID cert.
3. authenticate with VID
5. issue pseudonym certificates
pseudonym resolution
9. request pseudonym resolution
10. return identity information
pseudonym revocation
law enforcement / resolution auth.
8. obtain pseudonym cert. to resolve
11. revoke VID
P_i
HSM
P_j
HSM
P_k
HSM
6. sign messages w/ pseudonym cert. attach pseudonym cert to message
7. change active pseudonym / request new pseudonyms
pseudonym change
pseudonym use

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

PSEUDONYM LIFECYCLE


pseudonym issuance
top-level CA
CA
PP
4. retain VID-pseudonym mapping
3. auth-
pseudonym resolution
9. request pseudonym resolution
10. return identity information
law enforcement / resolution auth.
pseudonym revocation
. revoke VID
attach pseudonym cert to message
HSM
P_j
7. change active pseudonym / request new pseudonyms
pseudonym change
pseudonym use

Assume perfect pseudonym change

Potential re-identification from other channels

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

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

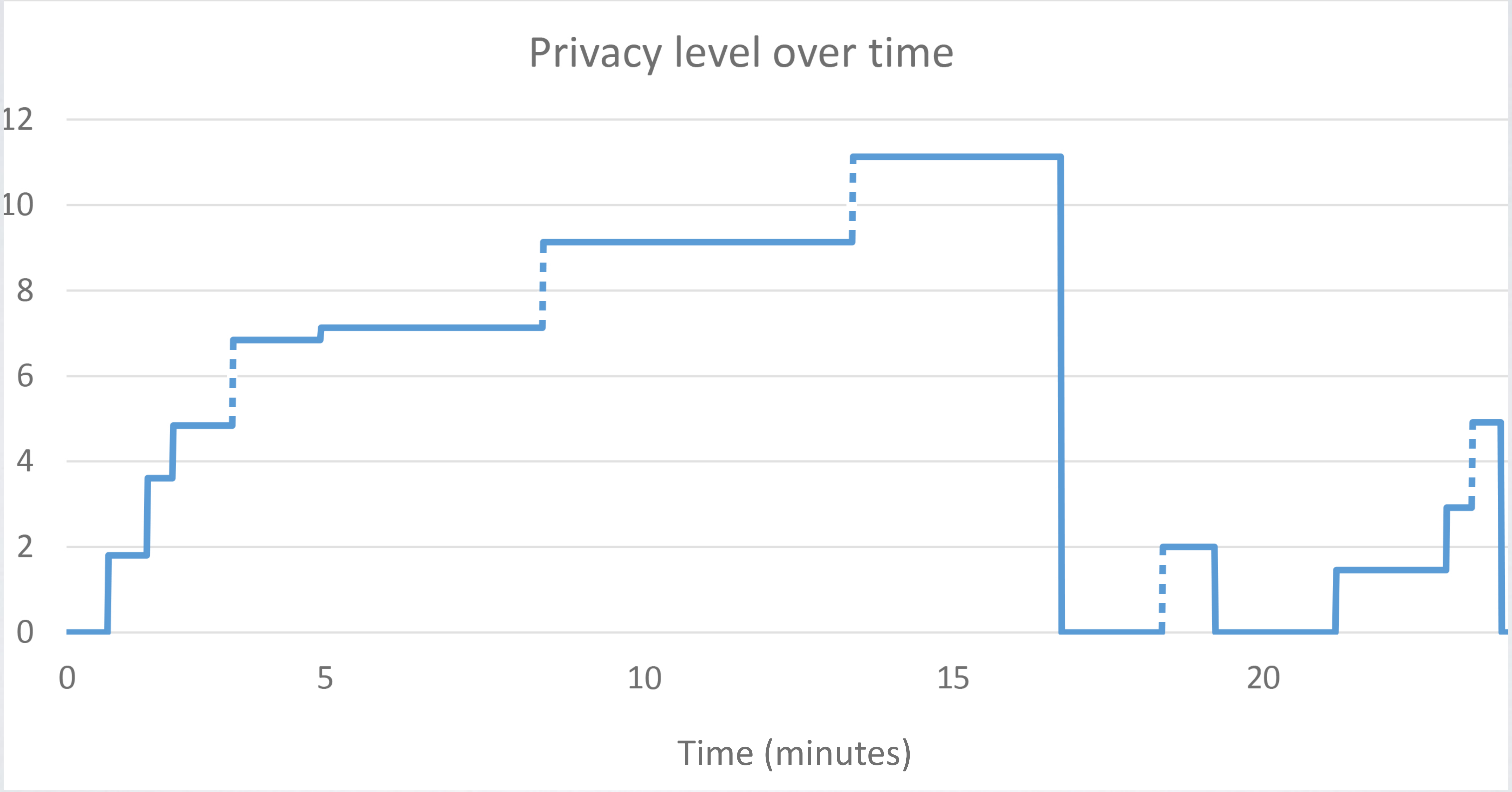
$$P_{road}(t) = \begin{cases} max(P_{road}(t-1) + \lambda(t_{last} - t), P_{dmax}) & \text{if } t \in T_{urs} \\ 0 & \text{if } t \in T_{obs} \end{cases}$$

Time since observation

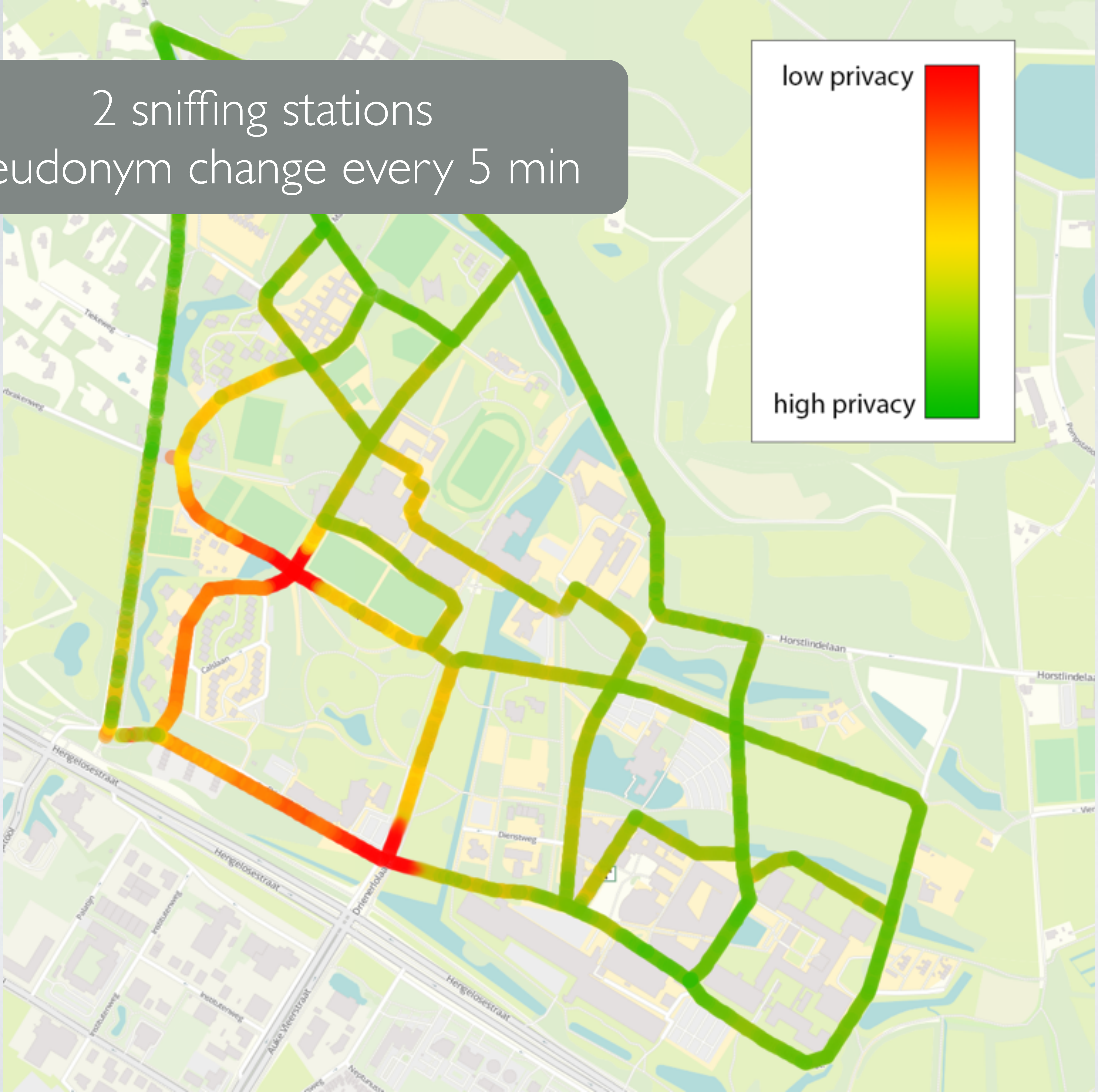
$$P(t) = P_{pnm}(t) + P_{int}(t) + P_{road}(t)$$

Total

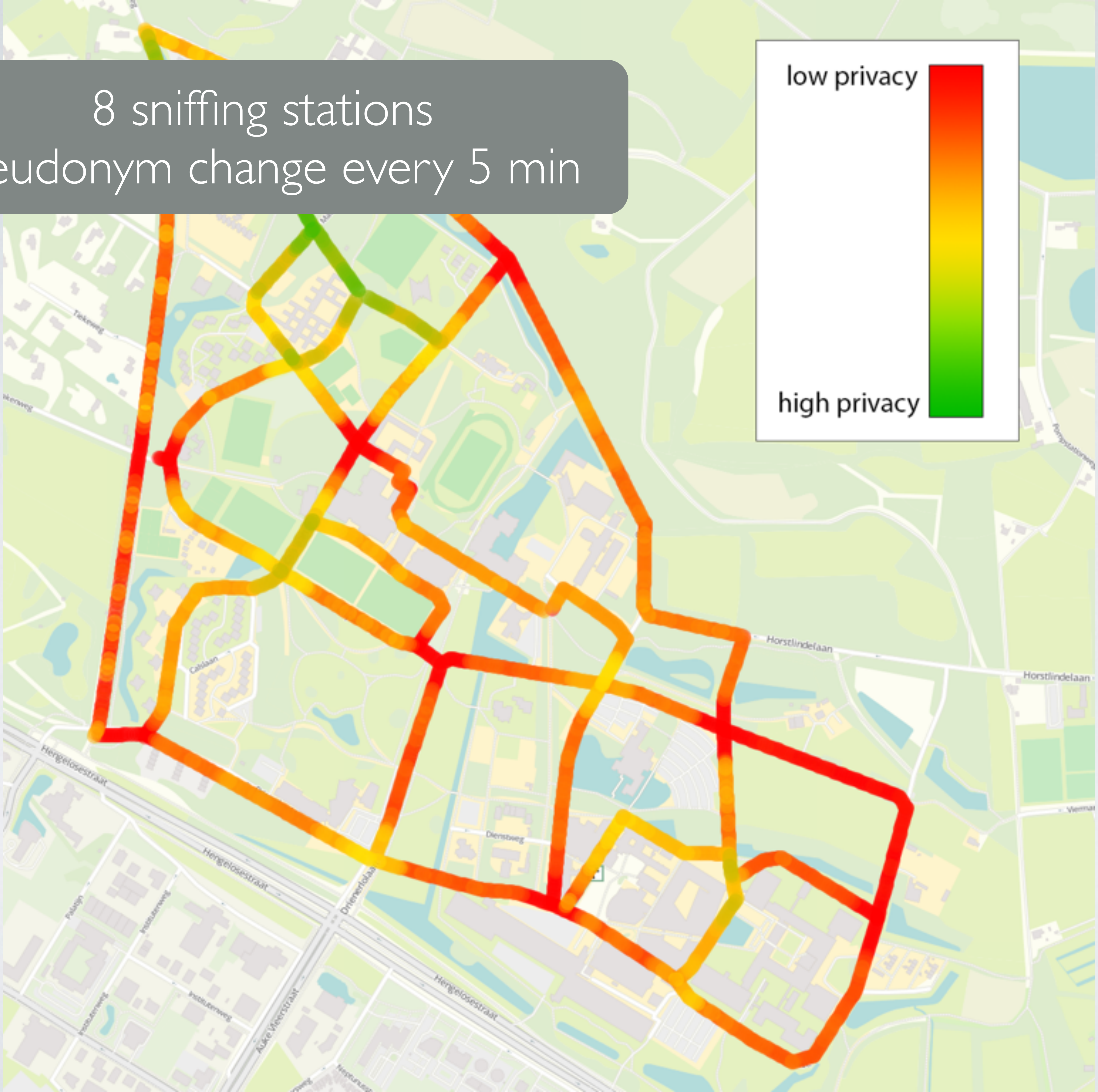
EVOLUTION OF PRIVACY LEVEL



2 sniffing stations
Pseudonym change every 5 min

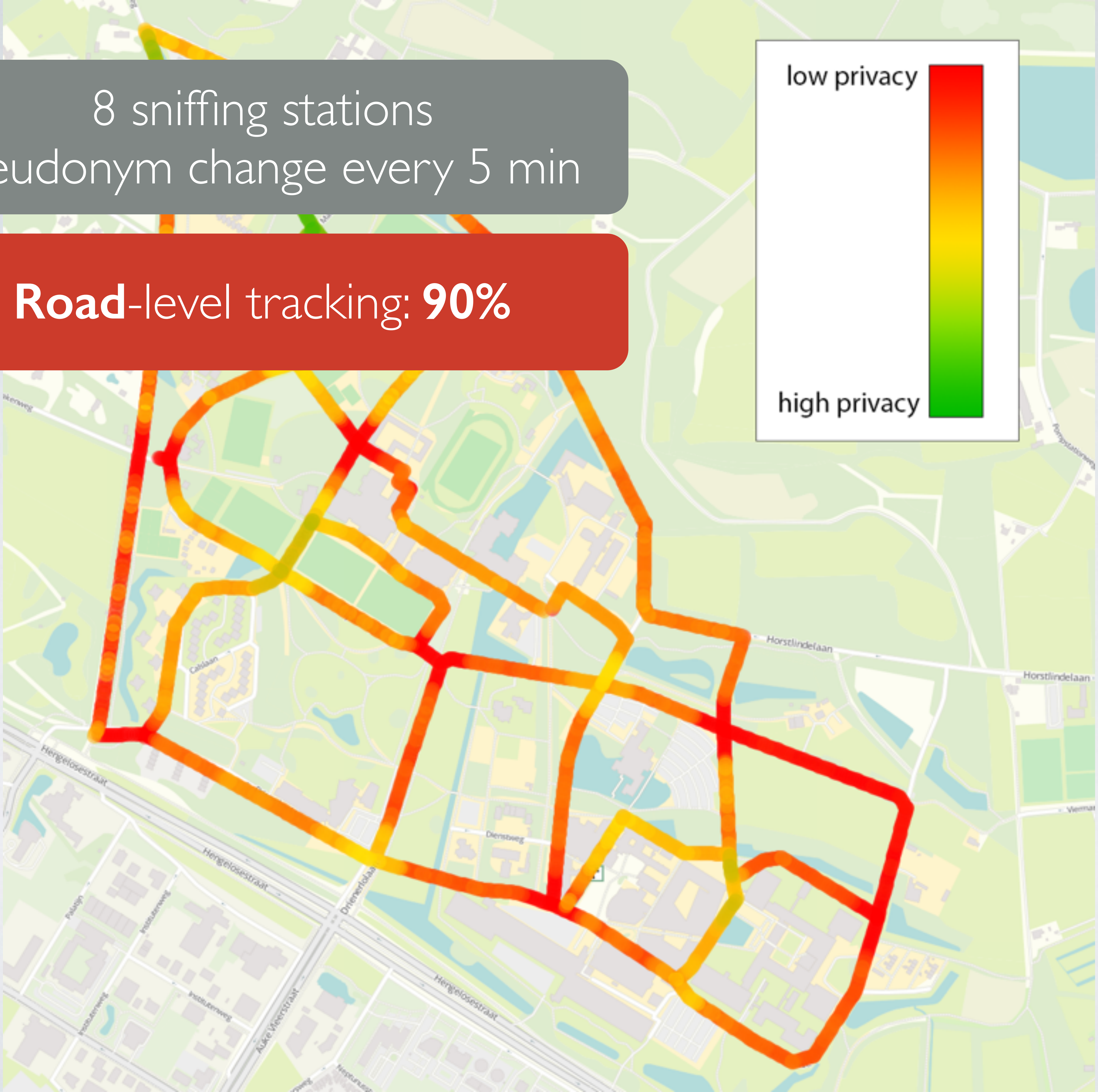


8 sniffing stations
Pseudonym change every 5 min

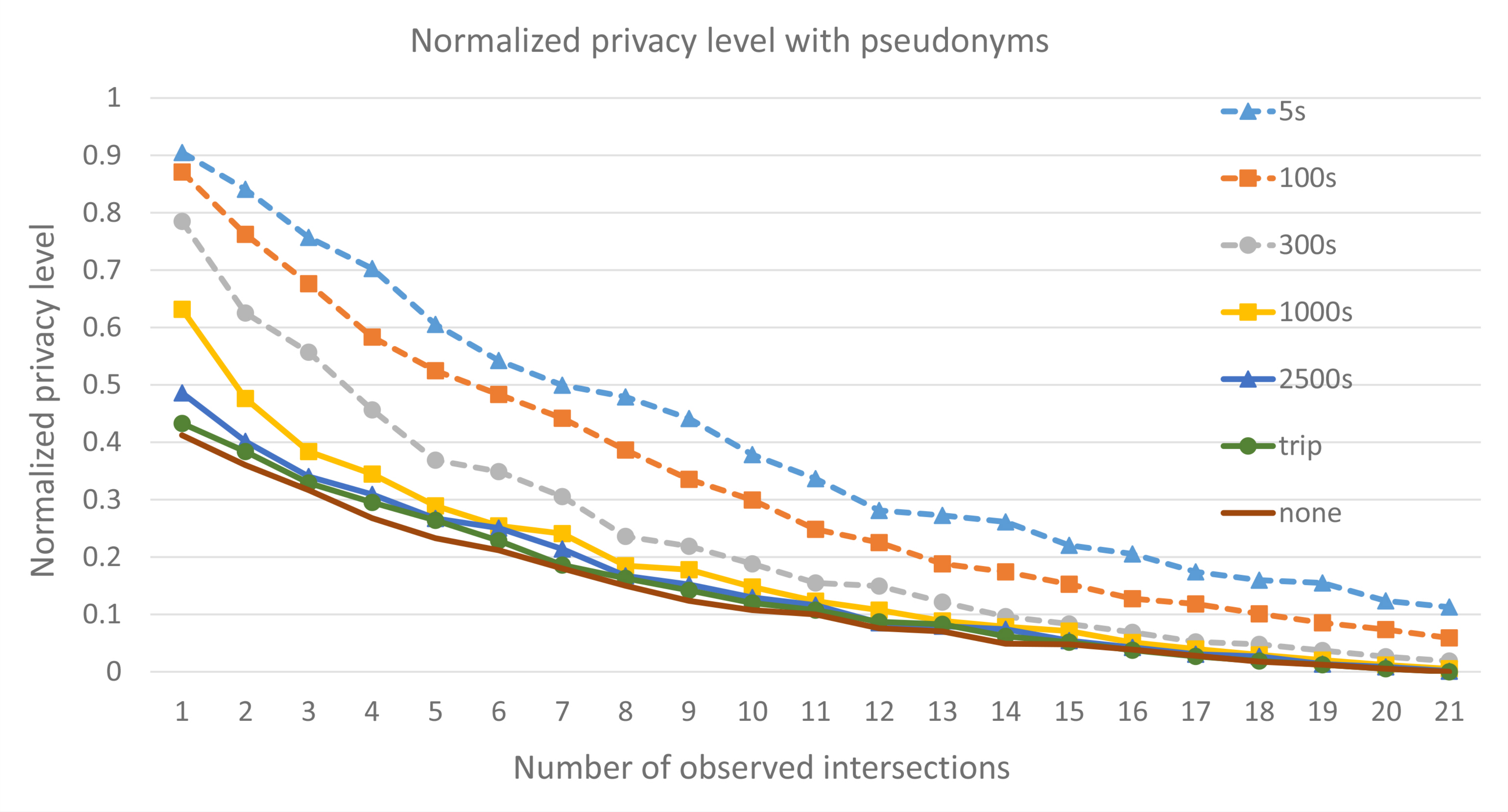


8 sniffing stations
Pseudonym change every 5 min

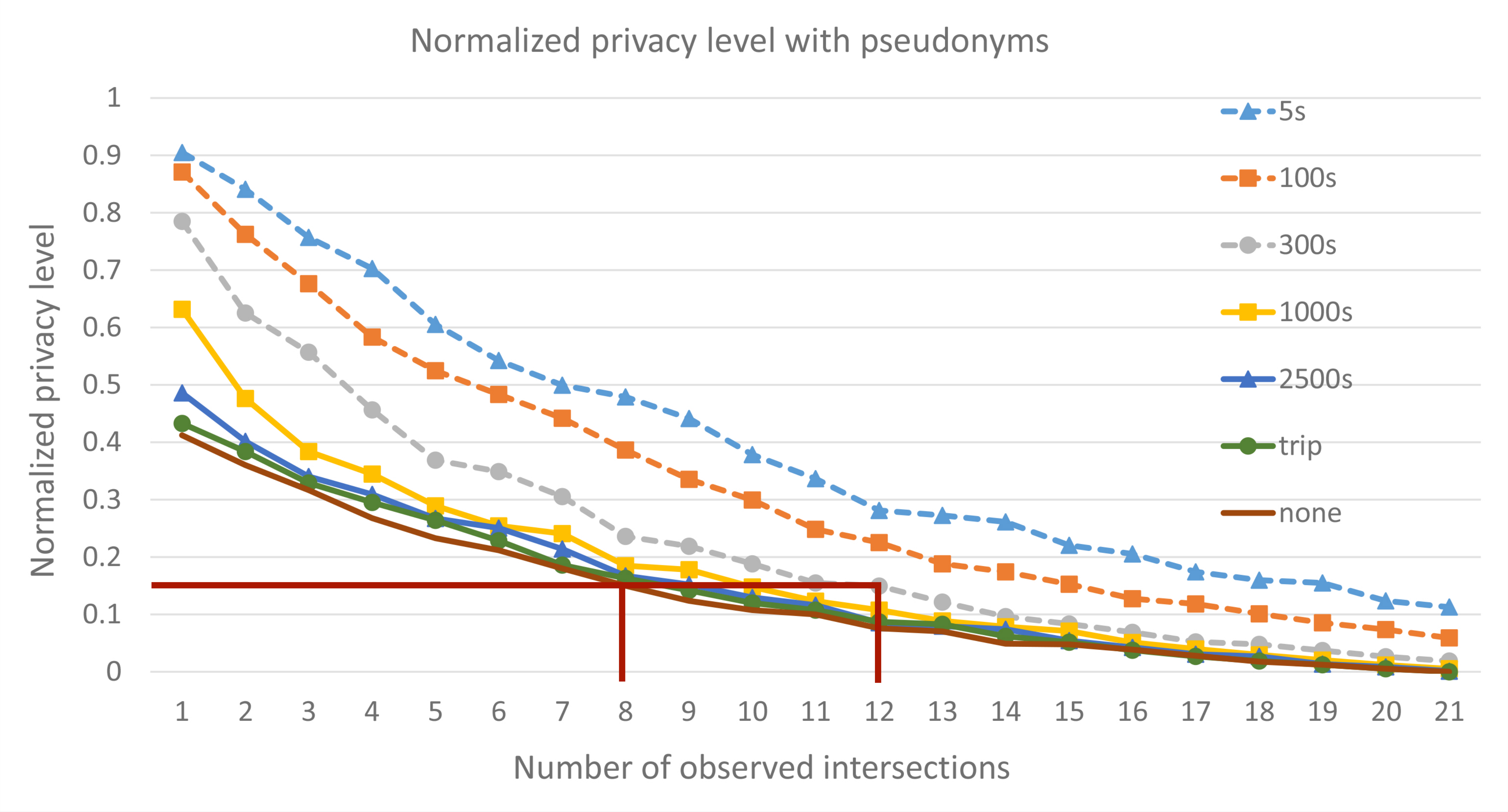
Road-level tracking: **90%**



PSEUDONYM CHANGE STRATEGIES



PSEUDONYM CHANGE STRATEGIES



COST MODEL

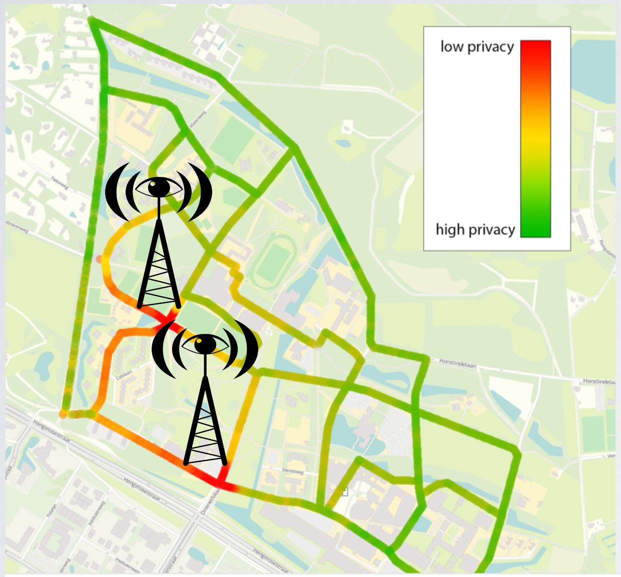
#observed intersection	Equipment Cost (€)
1	500
2	1000
8	4000
Full campus	10500

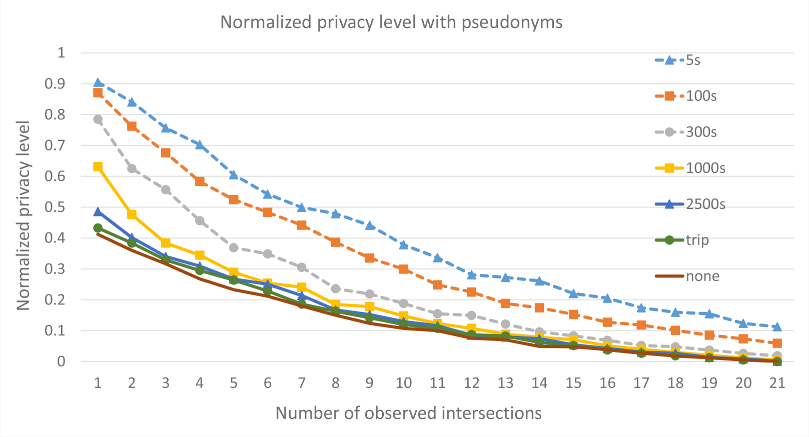
6000€/km^2

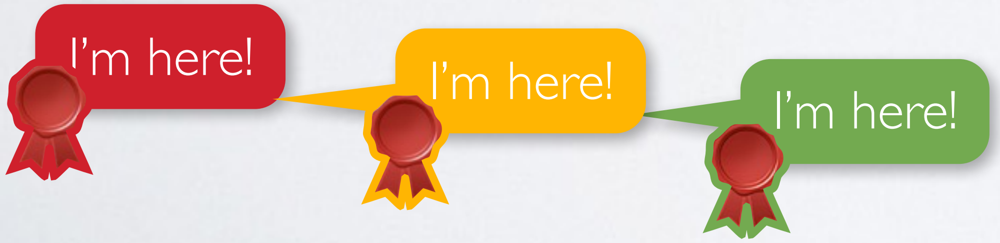
+ installation/operational/maintenance cost

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

CONCLUSION OF THE EXPERIMENT







Additional mitigations:
silent period, encrypted BSMs, …

Generalization
large-scale scenarios

Privacy-Preserving Road Networks?

BLACK HAT SOUND BYTES.

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

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

Questions & Answers

Jonathan Petit
jpetit@securityinnovation.com

Check out our white papers!

contain URL to results/videos!