Security Vulnerabilities of Autonomous, Unmanned and Driverless Vehicles

Zoz

PROTOTYPE THIS

PROTOTYPE THIS

Origins

Germany 1986

Ernst Dickmanns, VaMoRs

1995: Munich to Copenhagen in regular traffic, up to 175kph, vision only!

Europe

- UK: Nissan testing autonomous LEAFs in London since 2017
  - Jaguar Land Rover testing on public roads
  - Government promises £200 million research fund
- Sweden: Gothenburg driverless Volvo trials started Dec 2017 through 2018
  - Autonomous bus in northern Stockholm approved 2018
- Germany: BMW testing 40 vehicles in Munich
  - Promises to sell autonomous electric vehicle for autobahn in 2021
  - Autonomous bus trials in 2018 at Berlin hospital and Bad Birnach, Bavaria
- France: automated shuttles in Paris from 2017
  - Legislation to allow open road testing
- EU project AUTOPILOT: 2017-2019, 6 cities, €25,000,000

The Revolution Is Coming

- Advantages:
  - Energy efficiency
  - Time efficiency
  - New applications

The Revolution Is Coming

Civil Applications

Transportation

Oceanography

Mapping

Filmmaking

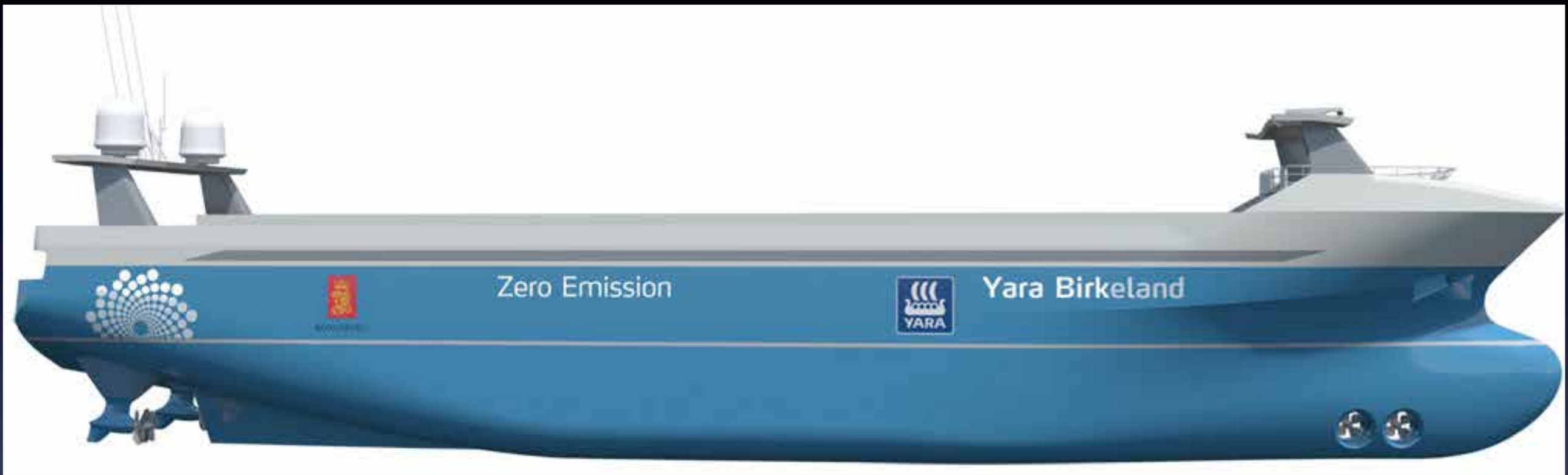
Powerline Inspection

Logistics

Civil Applications

- Unmanned cargo shipping
- 75% of maritime accidents caused by human error
- Major technical challenge: dealing with hardware failure on long voyages

Civil Applications

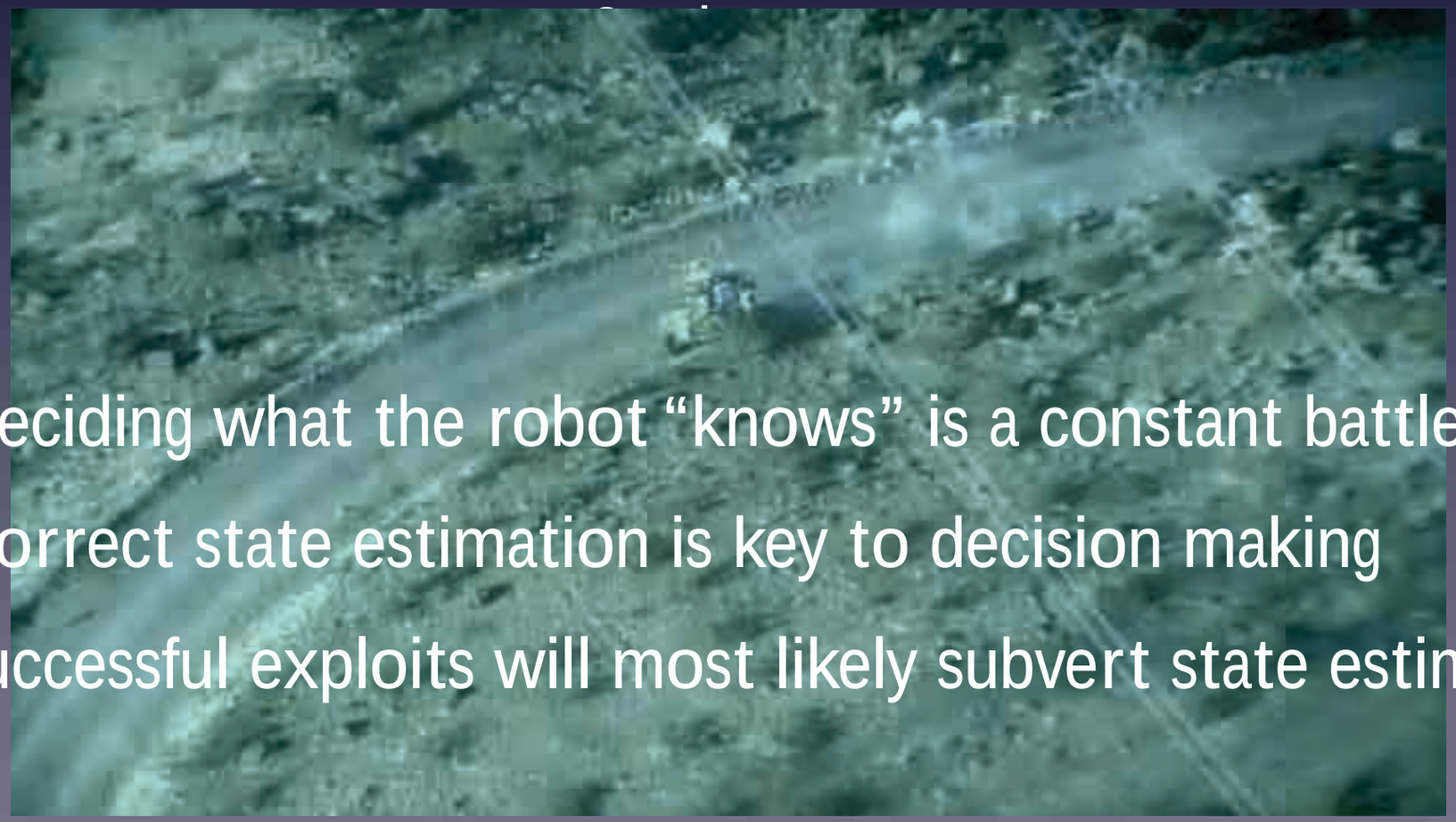


- Kongsberg Yara Birkeland
  - Zero emissions, autonomous capable
  - Replaces 40,000 annual truck trips
  - 2020: Manned operation & testing
  - 2021: Downcrewing
  - 2022: Fully autonomous operation

Civil Applications

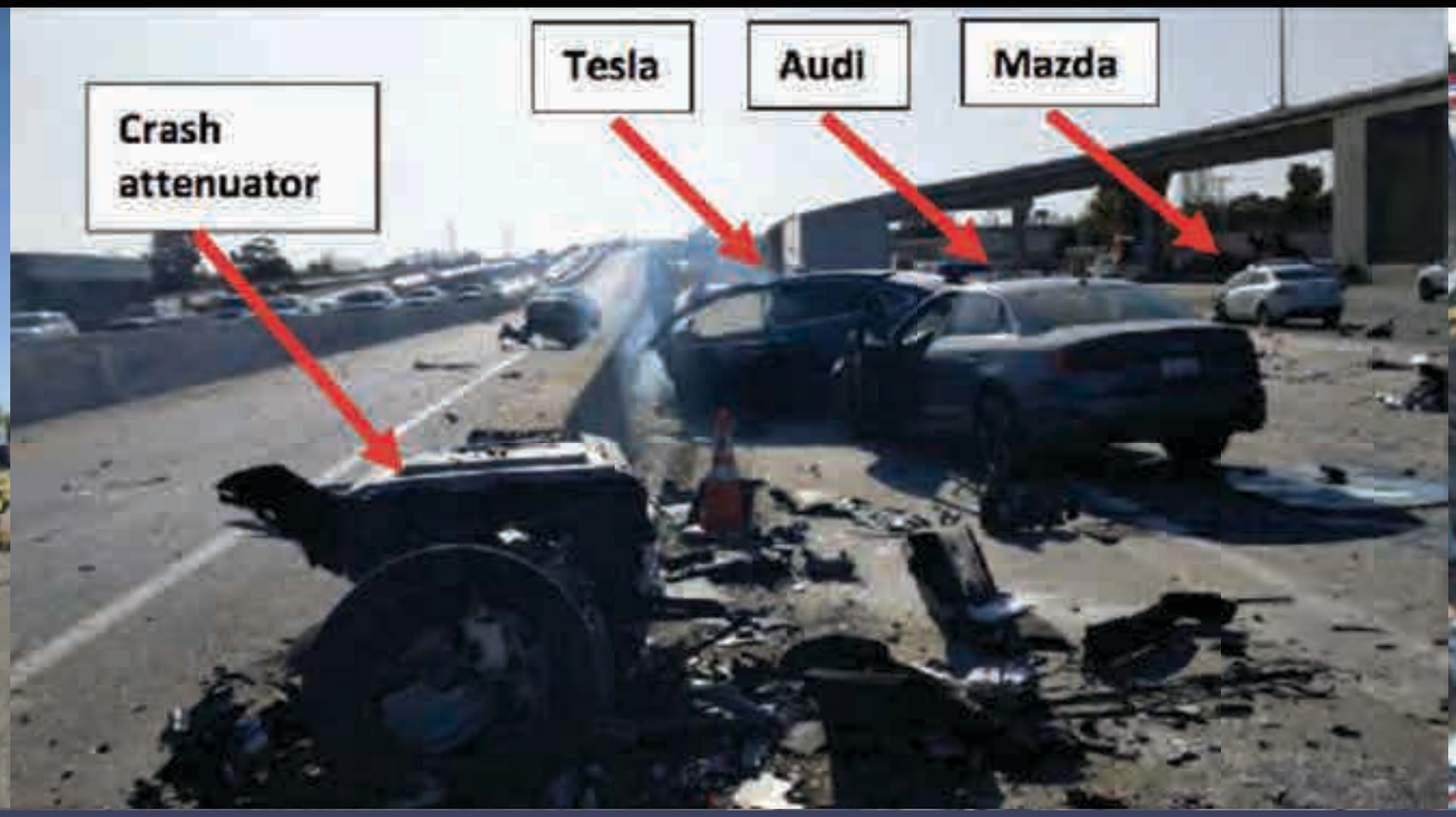
- Priorities:
  - Precision Agriculture
  - Self-Driving Cars
- Roadblocks:
  - Shared Infrastructure (Airspace, Roads)
  - Acceptance (Safety, Robustness)
- Let's Talk Failure!

Classic Failures



- Deciding what the robot “knows” is a constant battle
- Correct state estimation is key to decision making
- Successful exploits will most likely subvert state estimation

Classic Failures



Fatal Tesla Autopilot Accident
US-101, March 2018

- Dynamic cruise control + autosteer lane following
- 120 kph impact with previously damaged crash attenuator
- Vehicle selected poor lane markings over lead vehicle
- Fragile decision making & edge cases abound

Autonomous Vehicle Logic Structures

Activity Hierarchy

- Attacks lower in the stack defeat everything above
- More engineering effort spent on guaranteed robustness at lower levels
  - Lower layers may be juicier but harder targets

Autonomous Vehicle Logic Structures

Examples

Lifesaving Drone

Pizza Delivery

Mission Task Planners/ Reasoners	→	Dynamic “bombing run” planner, impact point estimator	Dispense pizza to credit card	←	Mission Task Planners/ Reasoners
Navigation & Localization	→	GPS waypoint circuit	Route planning from SLAM-generated sensor map	←	Navigation & Localization
Collision Avoidance	→	None!	Dynamic obstacle discrimination & avoidance	←	Collision Avoidance
Control Loops, Stability Maintenance	→	Autopilot PID loops tuned for environmental conditions	Balancing, weight shifting	←	Control Loops, Stability Maintenance

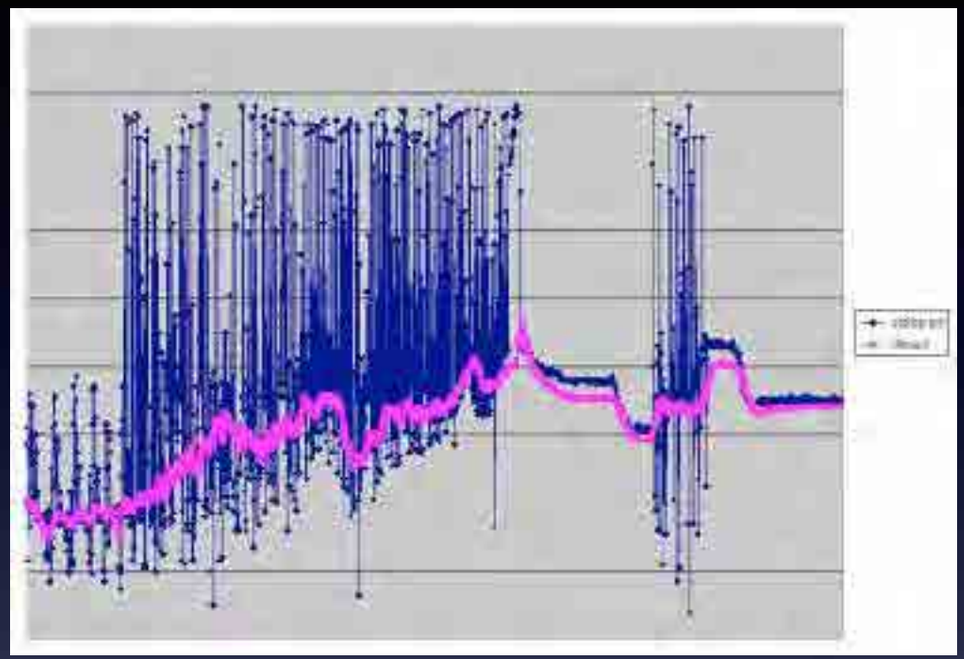
- Extremely vulnerable to collision
- High level logic depends on single sensor

- Vulnerable to redirection, trapping and map-confusion attacks

Sensors

- Active vs Passive
- Common sensors:
  - GPS
  - LIDAR
  - Cameras
  - Millimeter Wave Radar
  - Ultrasonic Transducers
  - Digital Compass
  - IMU
  - Wheel Encoders
  - Doppler Velocity Logger (subsurface)
  - Scanning SONAR (subsurface)
  - Pressure Transducers (air & subsurface)

Sensors



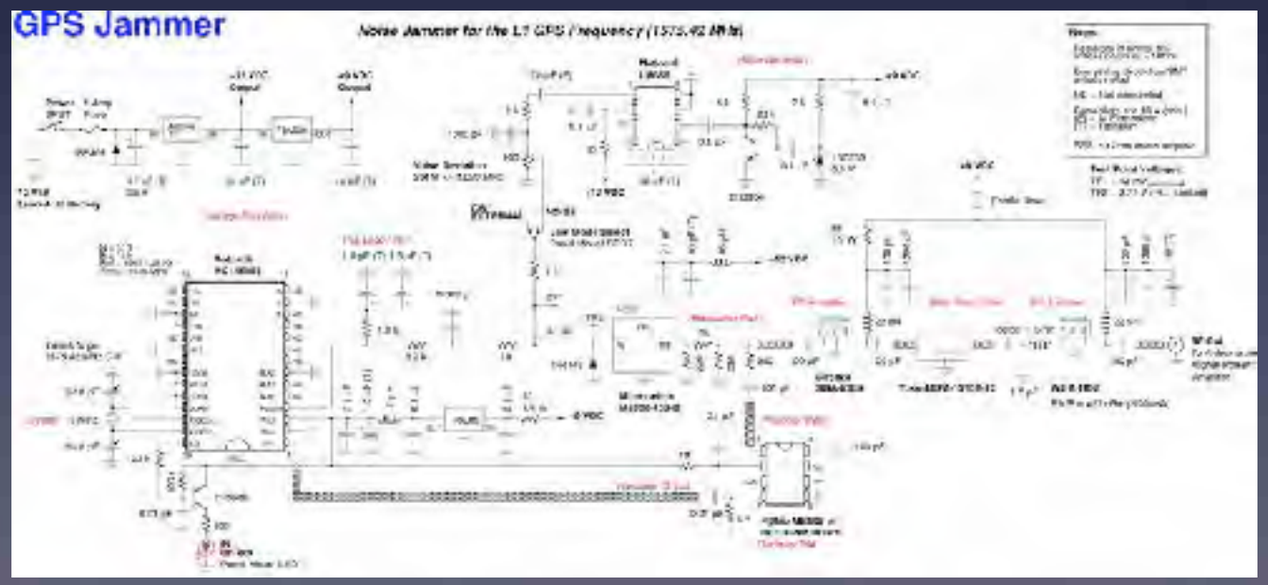
- Sources of uncertainty:
  - Noise
  - Drift
  - Latency & update rate
- Uncertainty must be modeled under assumptions
- Sensor fusion:
  - Fused/registered data can be more useful than separate
  - What to do when sensors disagree?
- Robot robustness may come down to:
  - How smart is it at discounting 1 bad/spoofed sensor?

Sensor Attacks

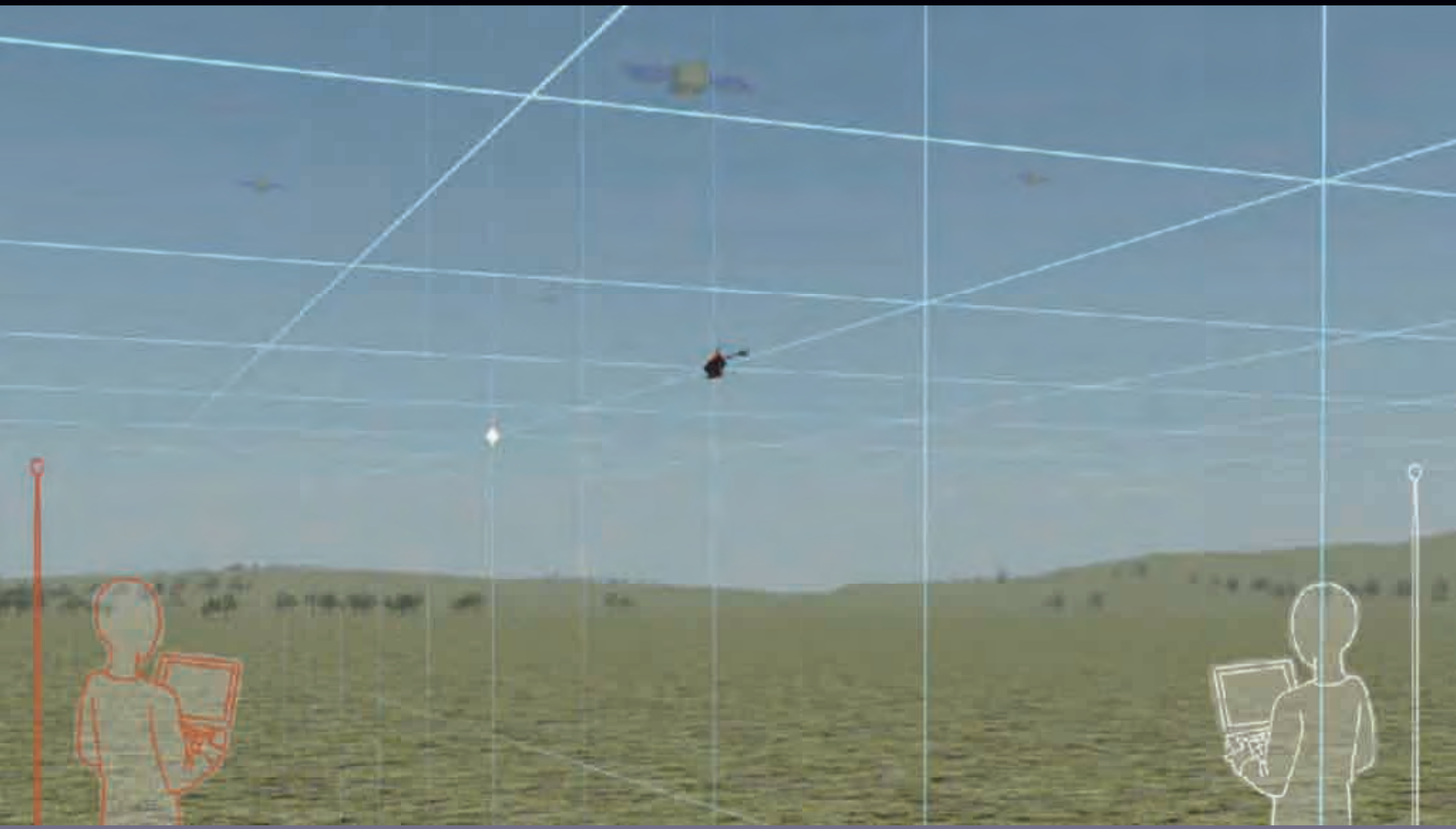
- 2 kinds:
  - Denial
    - Preventing sensor from recovering useful data
  - Spoofing
    - Causing sensor to retrieve specifically incorrect data
- Basic attack mode choice:
  - Attack sensors instantaneously
  - Attack aggregated sensor data

GPS

- Denial:
  - Jamming
- Spoofing:
  - Fake GPS satellite signals at higher power



GPS




آمریکا هیچ غلطی نمی تواند بکند
American Can Do No Wrong
اسرائیل باید از صحنه روزگار محو شود
Israel must be wiped out of the scene


RQ170 – هواپیمای پیشرفته جاسوسی آمریکا
تسلط مدافعان ایران اسلامی بر تحرکات شیطان بزرگ
اخبار شبکه یک


NOVA


02
MY RIDE

GPS

GPS

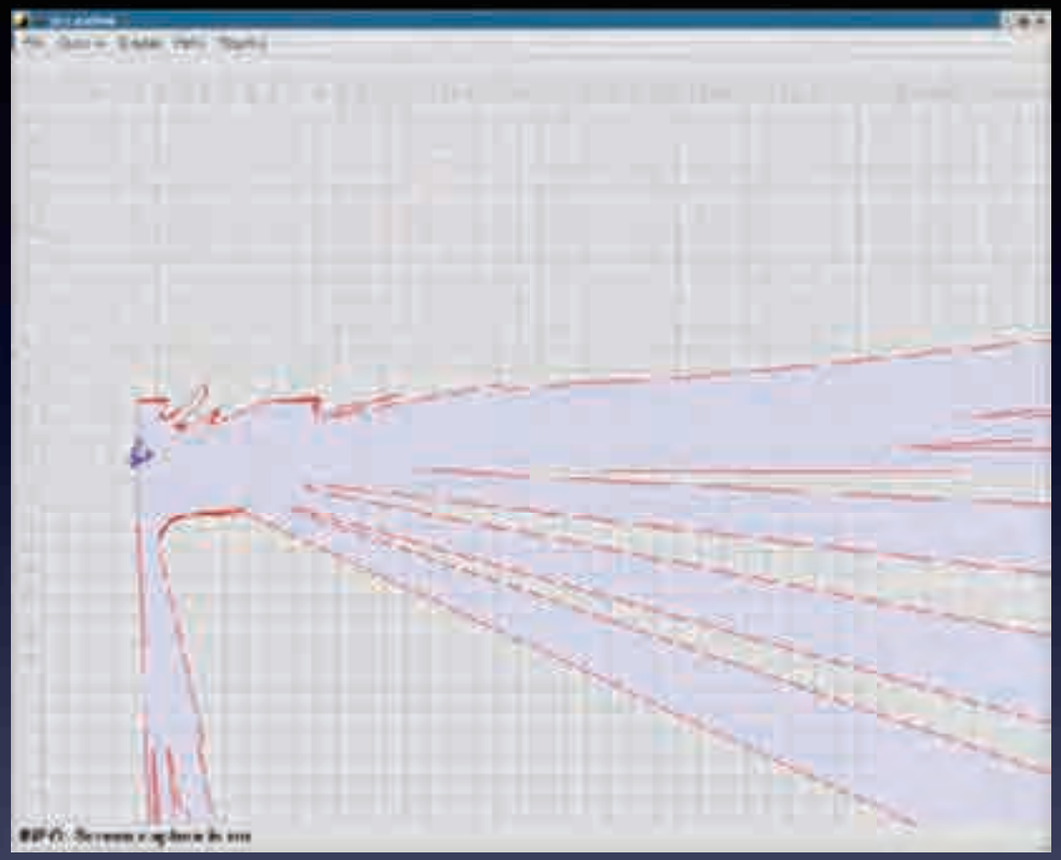
- Low Cost GPS Simulator Using BladeRF SDR
  - Qihoo360 Unicorn Team Huang & Yang, DEF CON 23

UAV Takedown!

LIDAR

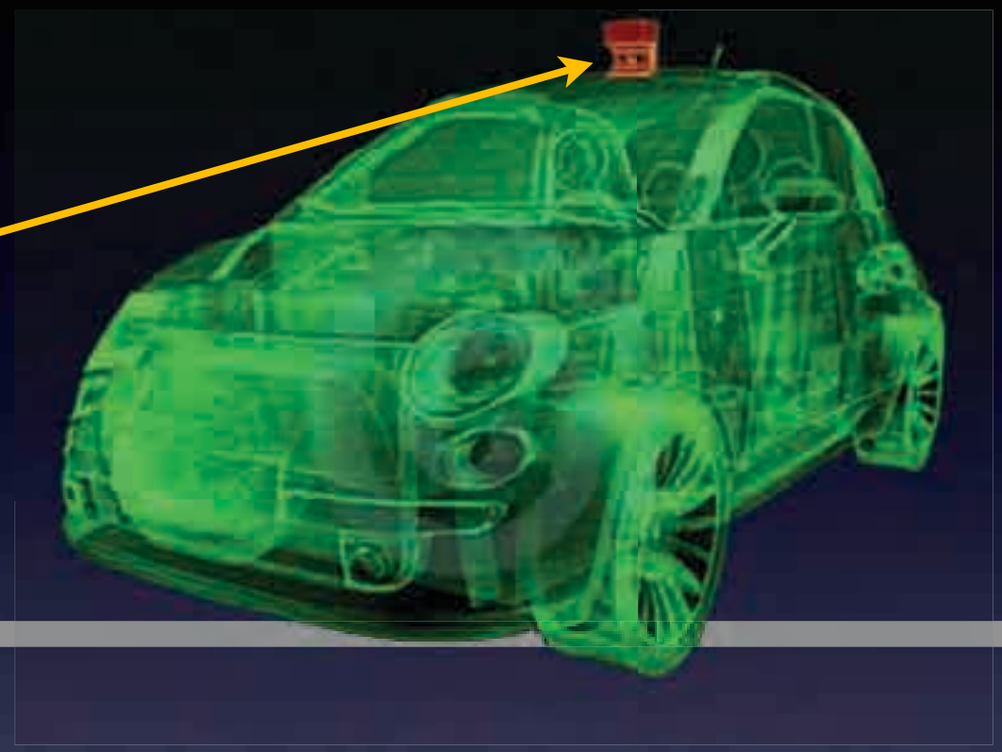
- Originally industrial monitoring sensors
- Mechanically scanned operation
- Primarily for collision avoidance & map building
- Denial:
  - Active overpowering
  - Preventing return signal
- Spoofing:
  - Manipulating absorbence/reflectivity
  - Active spoofing

LIDAR



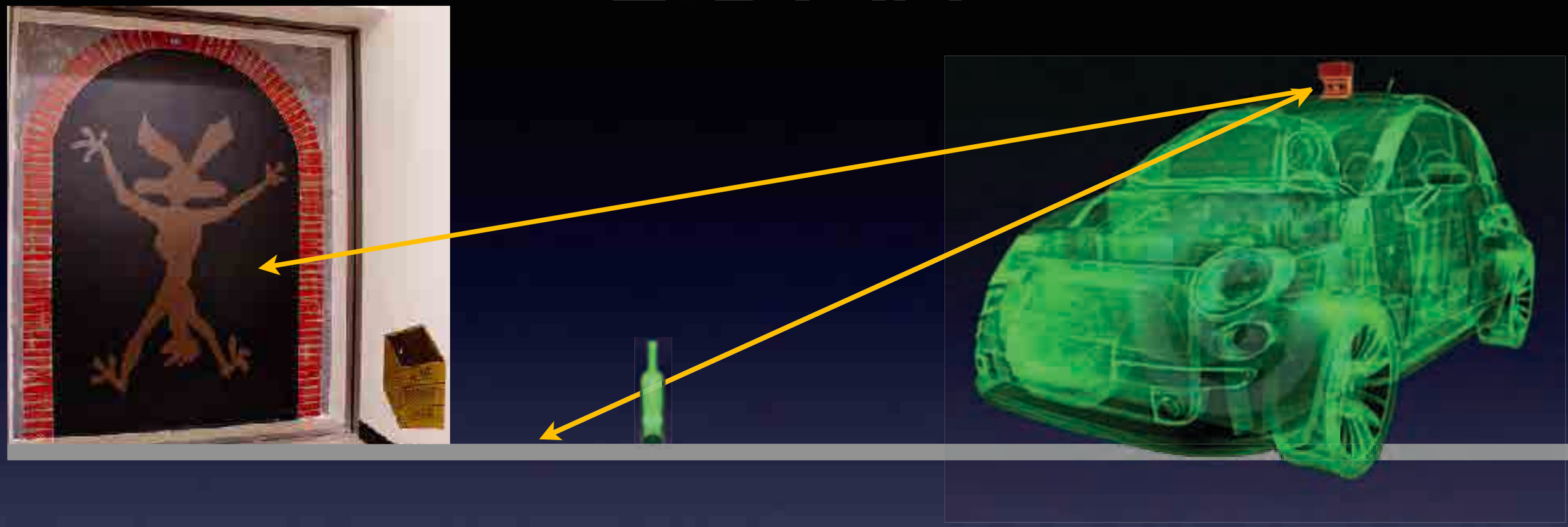
- 2D sensor highly orientation dependent
  - Inclines can look like obstacles
  - May miss low obstacles & discontinuities

LIDAR



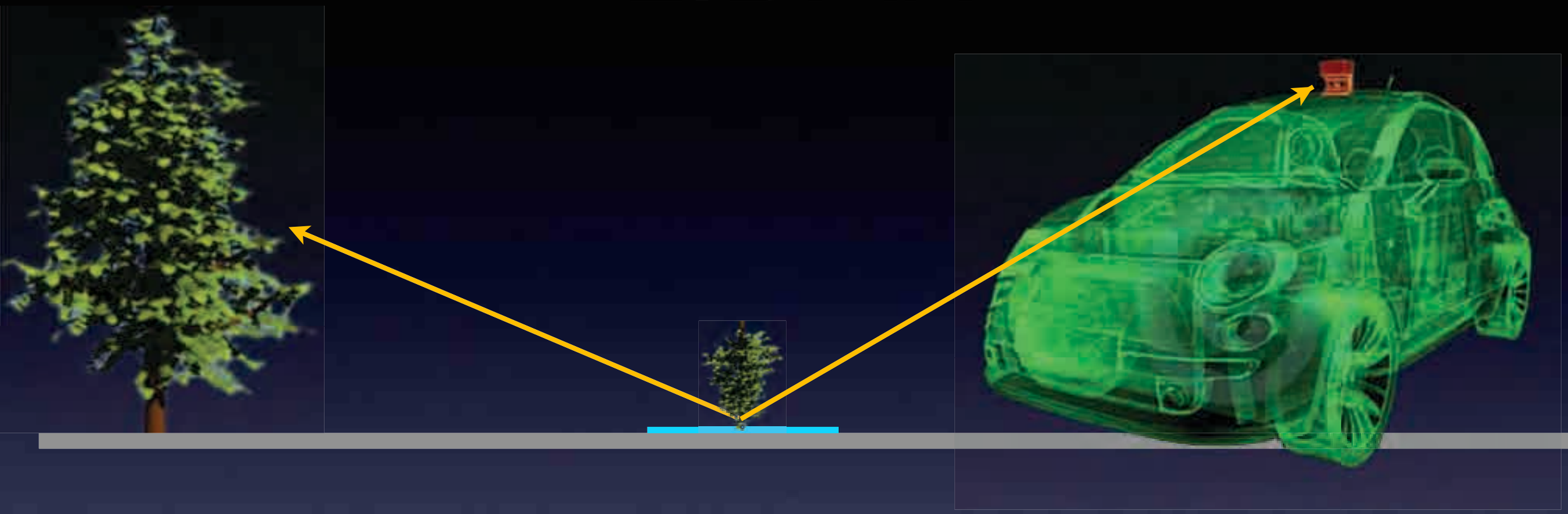
- Active emission sensor
  - Can only see what returns a signal
  - No return = nothing there
  - Most of the world returns no data

LIDAR



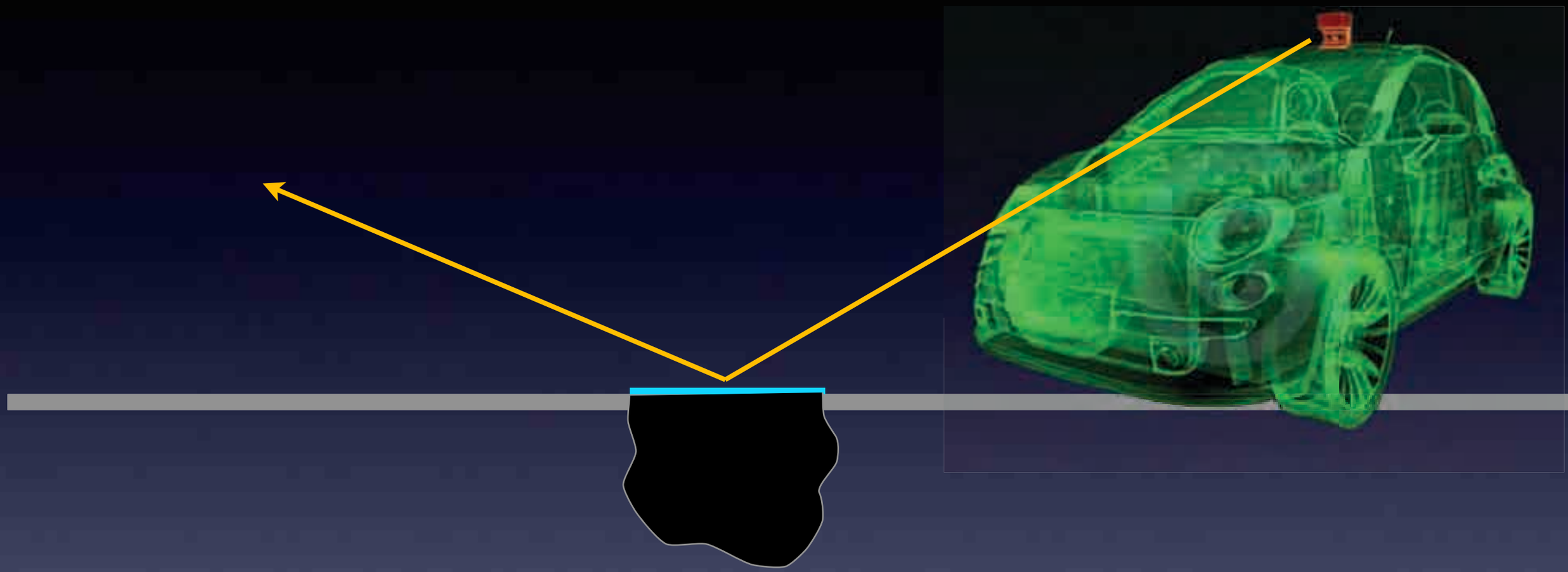
- Absorbent things look like nothing
  - Also transparent

LIDAR



- Reflective things can confuse laser
  - Faraway things brought near
  - Loss of return looks like ditch

LIDAR



- Reflective things can confuse laser
  - Faraway things brought near
  - Loss of return looks like ditch

Russian “Racal” GPS jammer

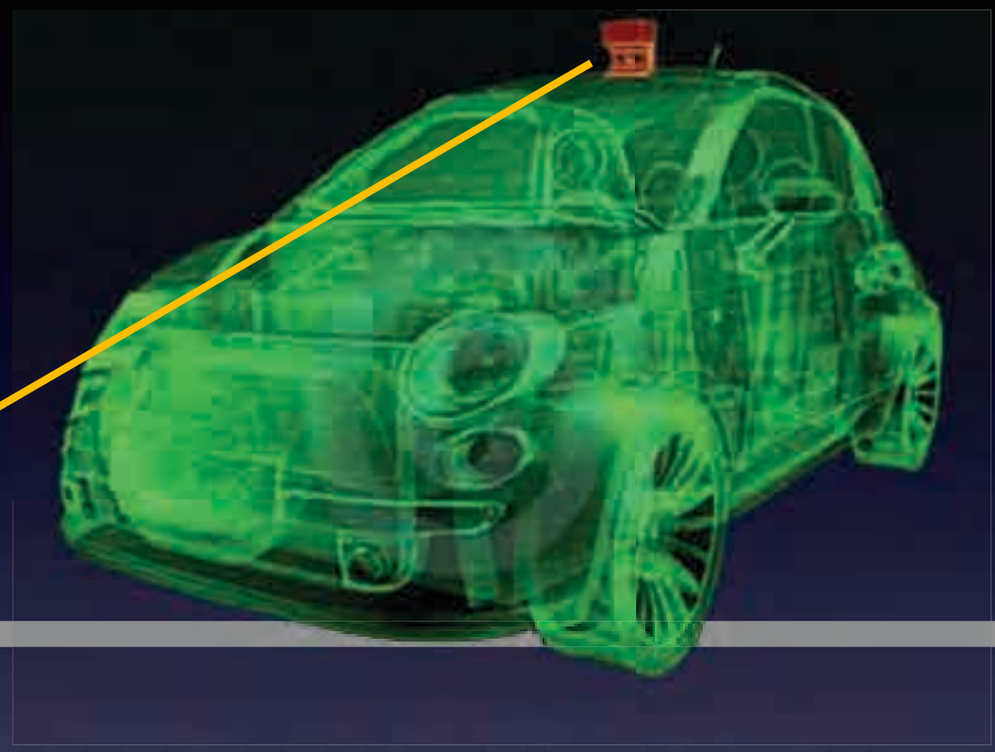
في اعتقادي ان إفشال هذه الإستراتيجية يعتمد على ثلاثة اشياء [illegible] راي عام مناهض للهجمات - ردع الجواسيس - تكتيكات التمويه والتضليل [وهي كالتالي .

[1] تكتيكات التمويه والتضليل هي مجموعة خبرات جمعتها من تجارب ين

- 1 لكشف نوايا ومهمة الطائرة يمكن من خلال جهاز " سكاي كرابر " روسي الصنع الدخول على موجات وترددات الطقرة بدون طيار والجهاز متوفر في الأسواق وبسعر 2595 دولار ويتطلب خبرة في الحاسوب .
- 2 إستخدام أجهزة تبث ترددات أو حزمة ترددات لأجل قطع الإتصال أو التشويش على الترددات التي تستخدم في السيطرة على الطائرة وقد كان للمجاهدين تجارب ناجحة باستخدام جهاز " الراكال " روسي الصنع .
- 3 وضع الزجاج العاكس فوق السيارة أو فوق المبنى أو تكسيره ونشره في المكان .
- 4 توزيع تشكيلة من القناصين المهرة لإصطياد الطقرات بدون طيار وخاصة الإستطلاعية لأنها تطير على علو منخفض 6 كيلو وما دون .
- 5 للتشويش على الإتصالات الألكترونية يمكن استخدام " دينموا " رفع المياة العادي وتزويده بعمود نحاسي بأكثر من 30 متر .
- 6 استخدام التشويش والتضليل بأجهزة الإتصال وتكون في وضع إتصال دائم وخاصة الأجهزة القديمة جدا حيث ان ذبذباتها قوية جدا ويمكن استخدام أشراك خداعية لجذب أجهزة البحث الألكتروني فأفكار بسيطة كالذي فعله الجيش اليوغسلافي عندما استخدموا أجهزة الميكروويف " الفرن " في جذب وتضليل صواريخ التيتو المزودة بأجهزة بحث كهرومغناطيسي .
- 7 التمويه العام وعدم استخدام المقرات الثابتة .
- 8 أخذ العلم بوجود الطائرة عبر شبكات إستطلاع موزعة بشكل جيد ثم التعميم على كافة التشكيلات بإيقاف كل التحركات في المنطقة .
- 9 الإختفاء عن الرؤية المباشرة وغير المباشرة وخاصة في الليل .
- 10 الإختفاء في الأماكن كثيفة الأشجار لأنها افضل وسيلة للإختفاء من الطقرات .
- 11 اللجوء إلى الأماكن غير المضاءة بأشعة الشمس كظل المباني والأشجار .

Use of reflective materials
to thwart laser designators

LIDAR

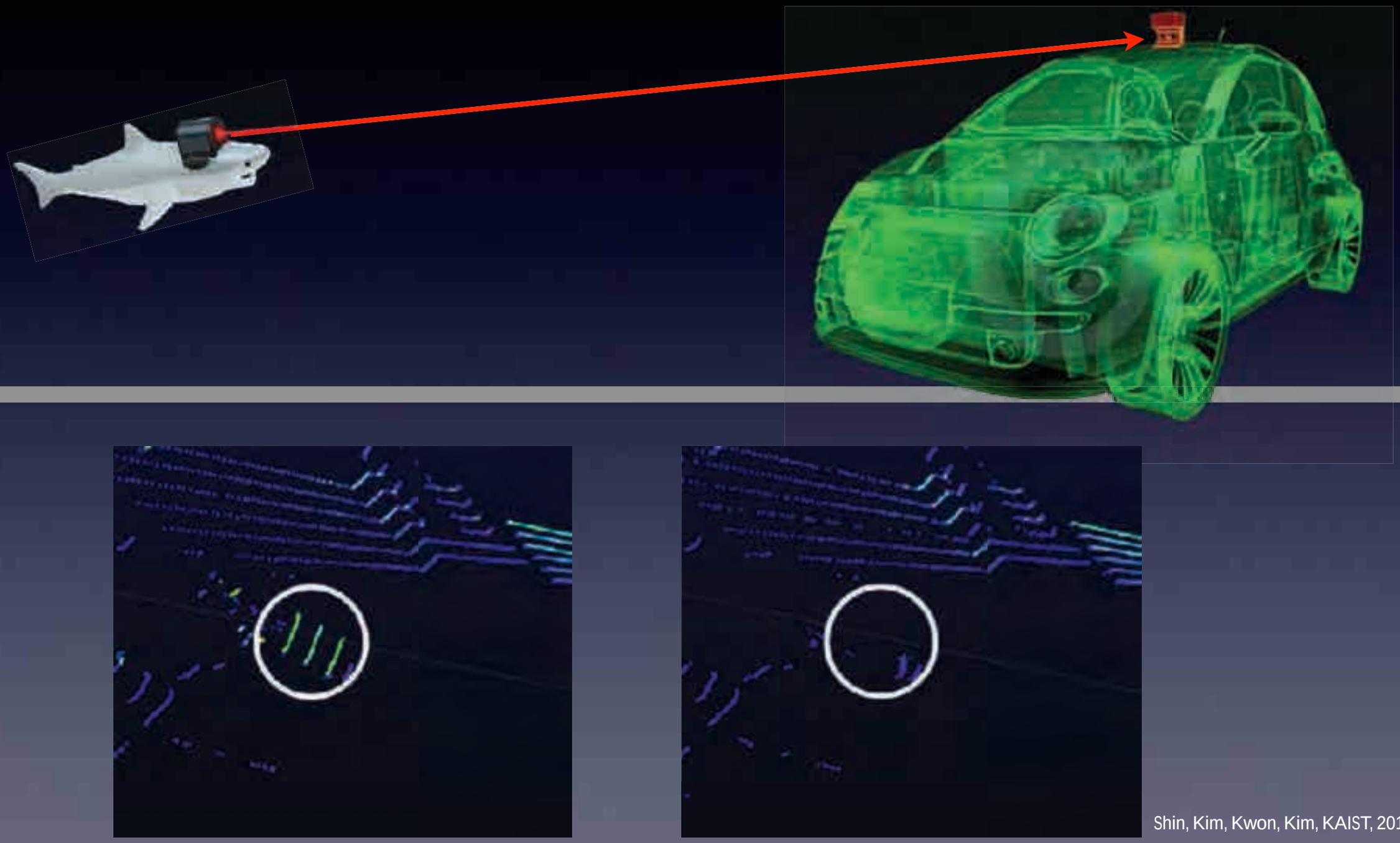


- Reflectance is also a feature
  - Road line detection
  - Can fake road markings invisibly to human

LIDAR

- Solid looking objects look solid

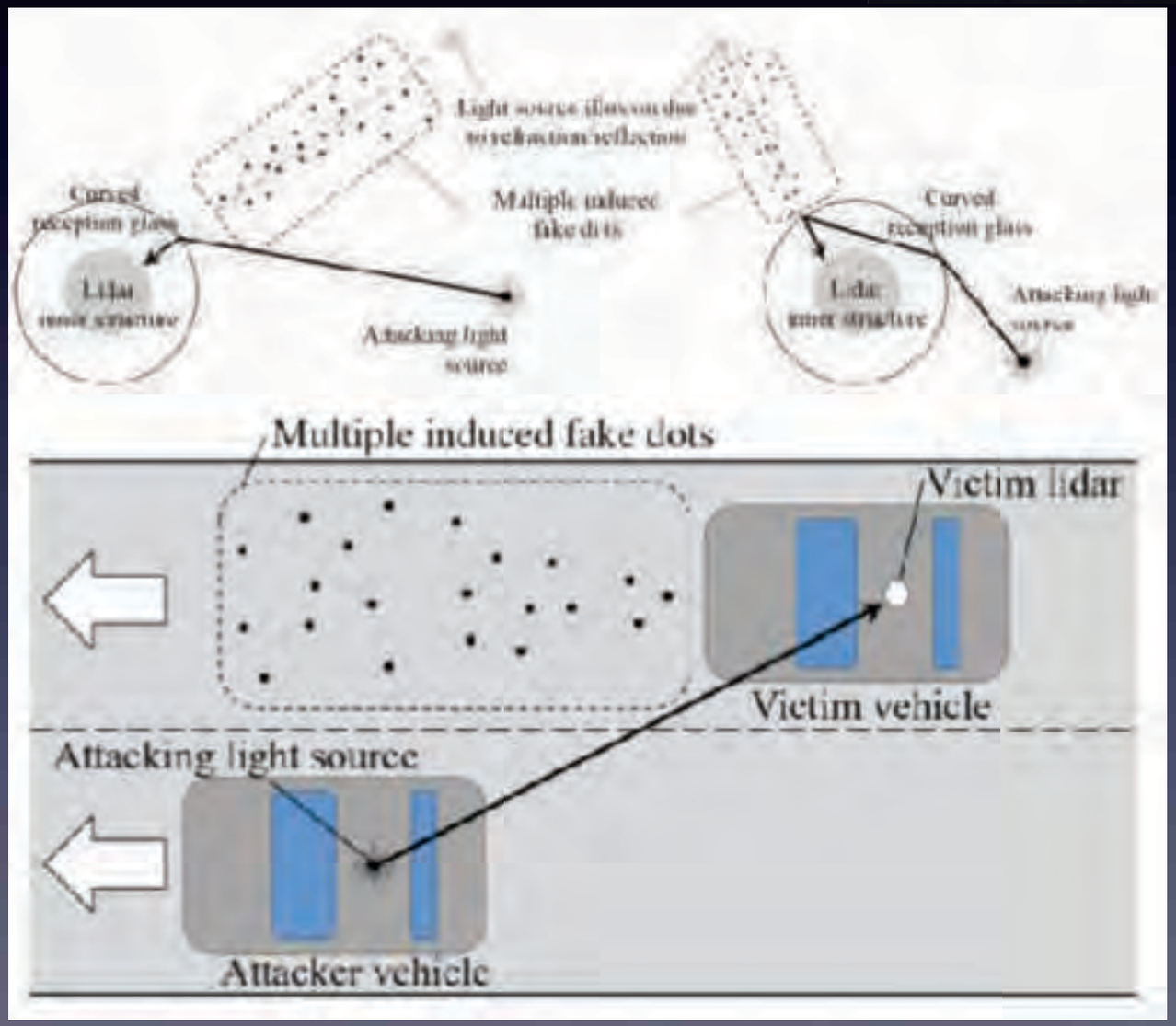
LIDAR



Shin, Kim, Kwon, Kim, KAIST, 2017

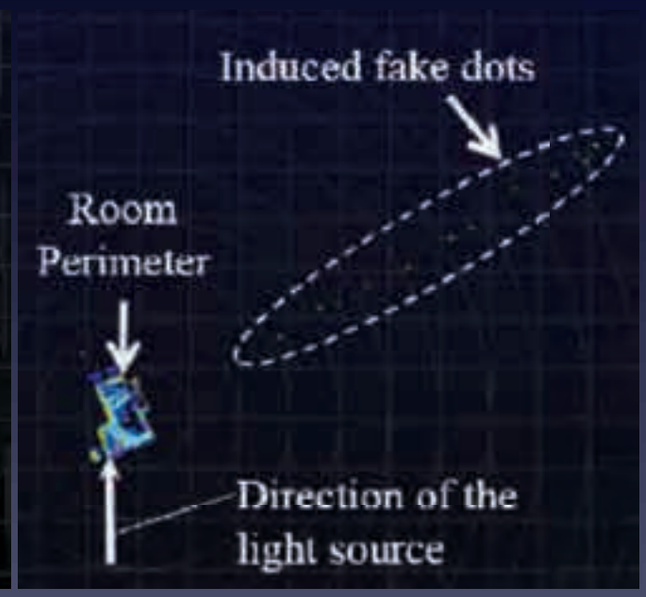
- Denial: strong source overpowers LIDAR in a certain area

LIDAR



WEAK

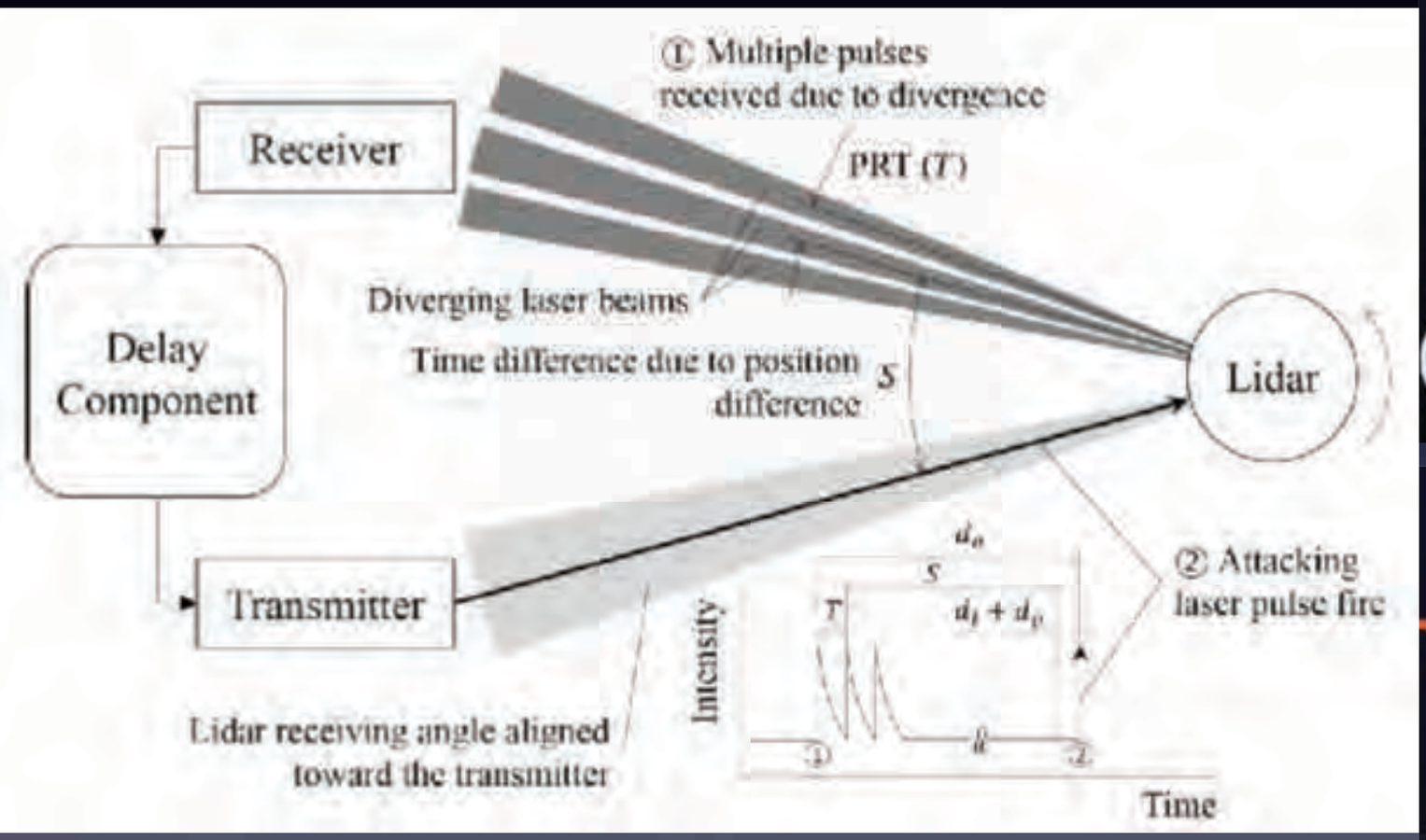
STRONG

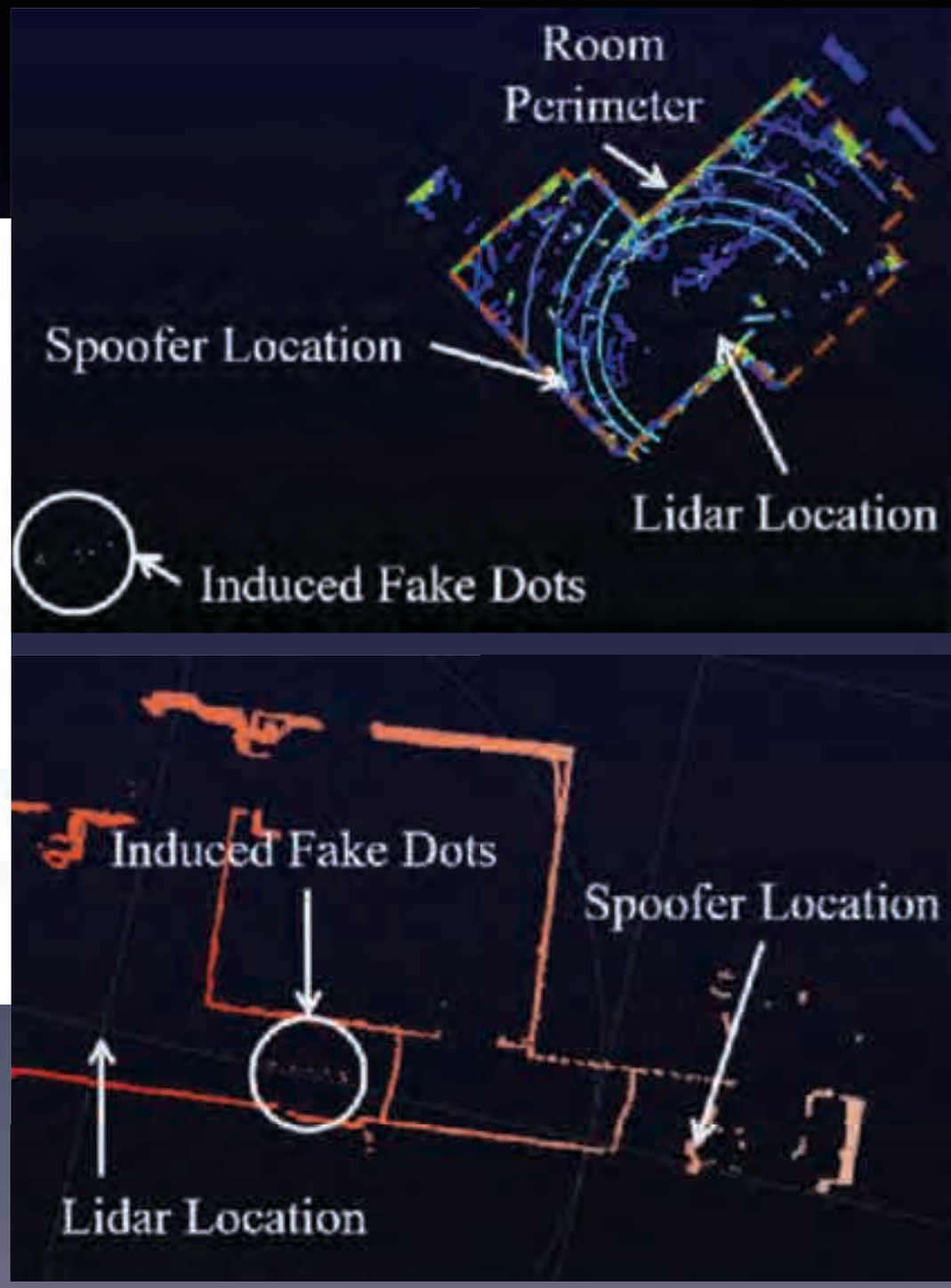


Shin, Kim, Kwon, Kim, KAIST, 2017

- Spoofing: weaker sources cause false returns
  - Can exploit curved glass refraction to alter location of false returns
  - Depends on source strength

LIDAR

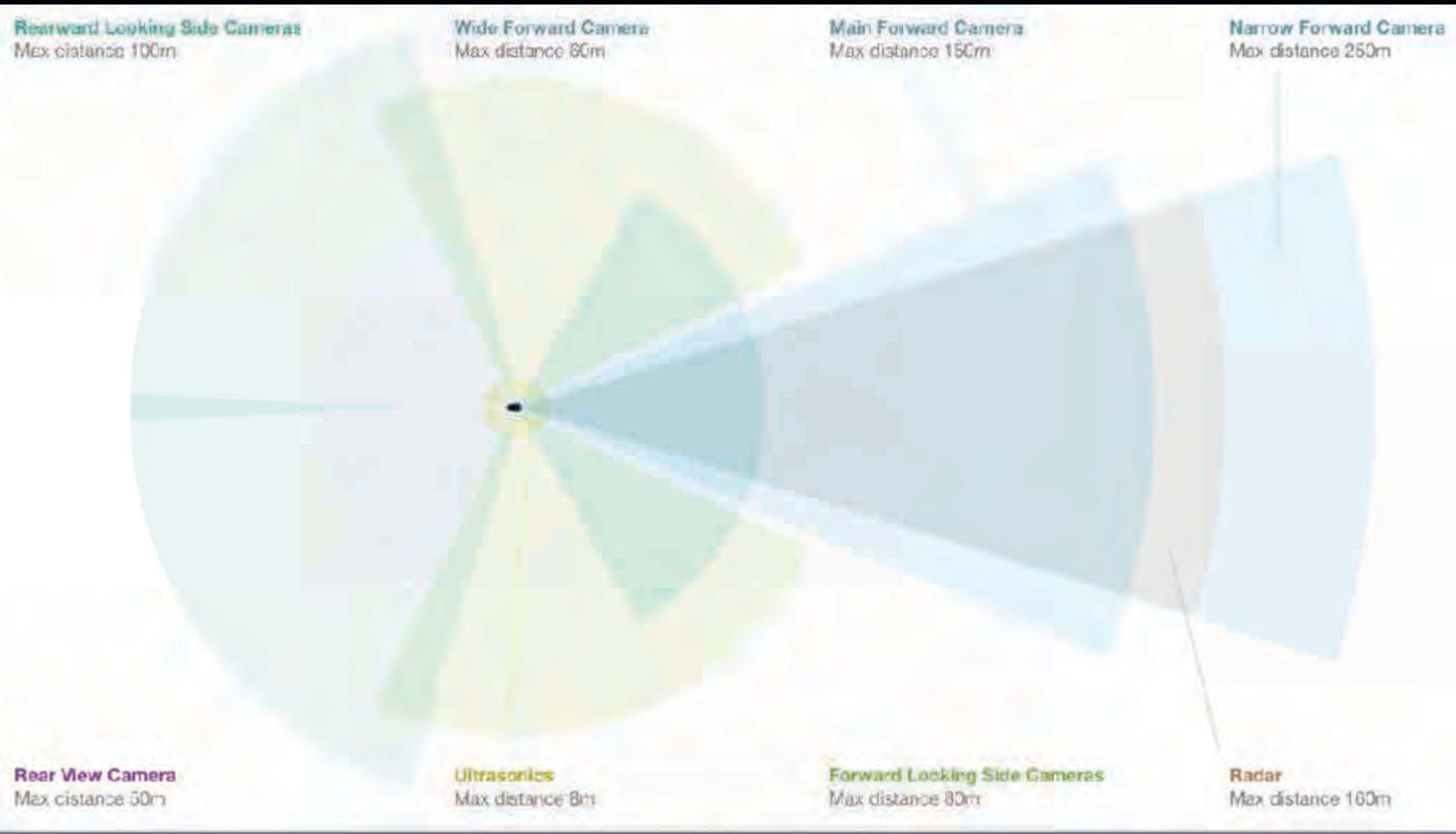




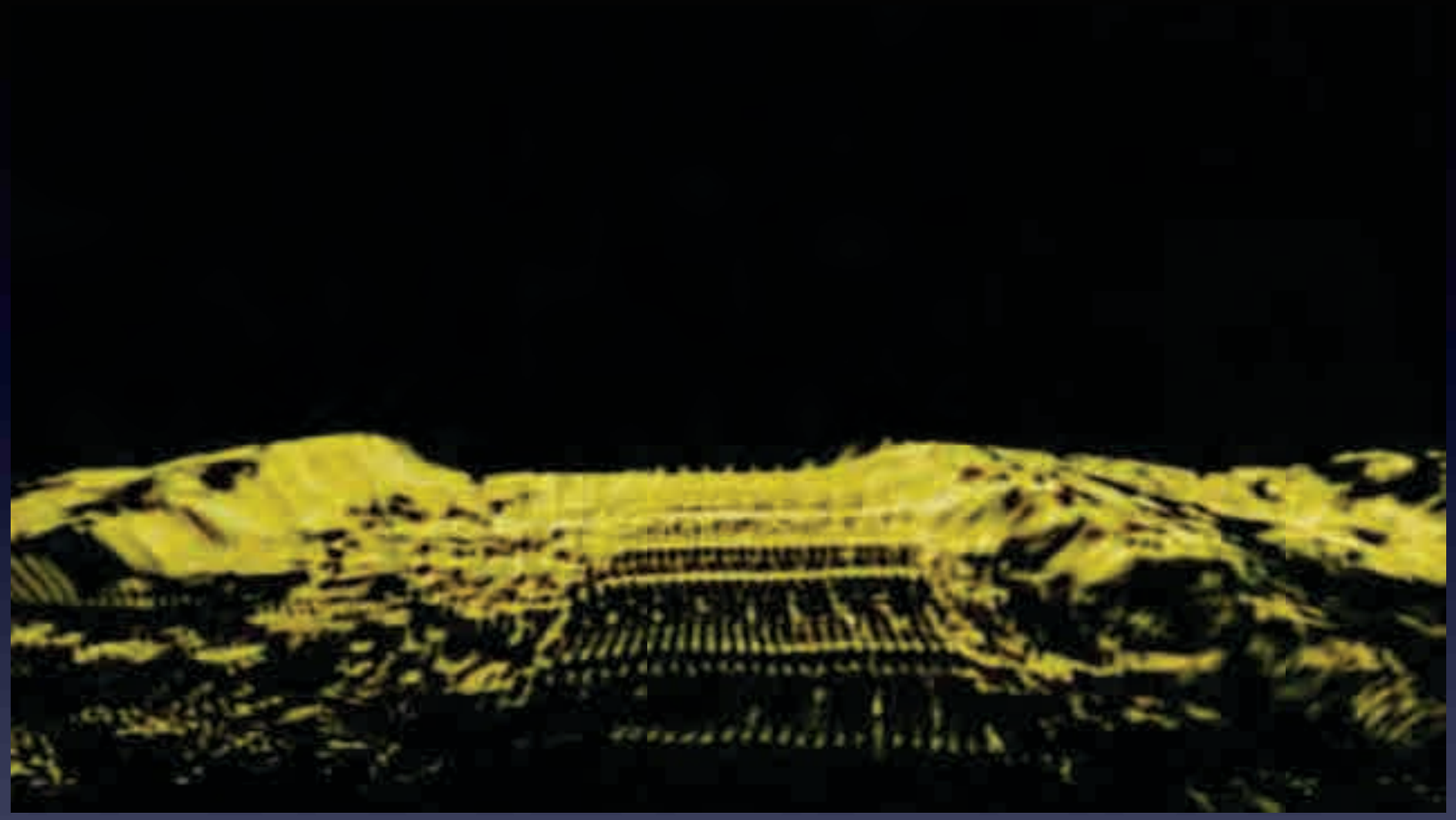
Shin, Kim, Kwon, Kim, KAIST, 2017

- Spoofing: Relay attack
  - Timing is critical for placement of fake returns

Tesla Autopilot



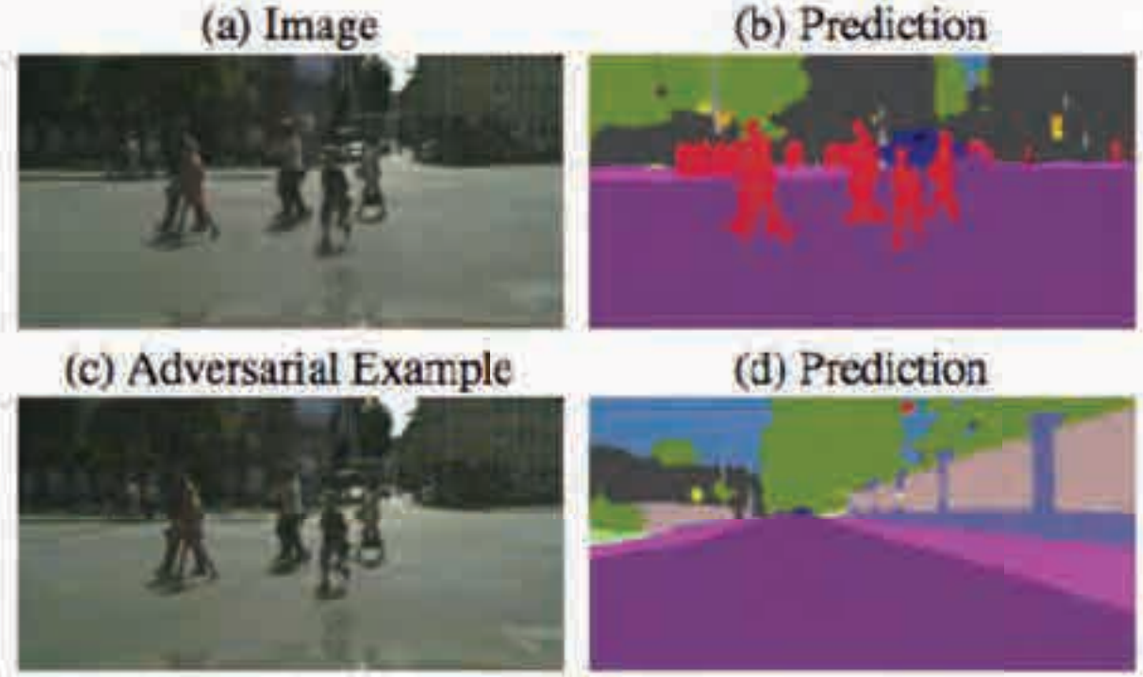
Cameras



- Specialized object detection (including signs and lane markings)
- Sometimes stereo for (noisy!) depth map
- Colorizing LIDAR
- Denial:
  - Easily dazzled
- Spoofing:
  - Camouflage techniques
  - Color assumptions
  - Repeating patterns

Cameras

Eykholt et al., 2018



Fischer et al., 2017

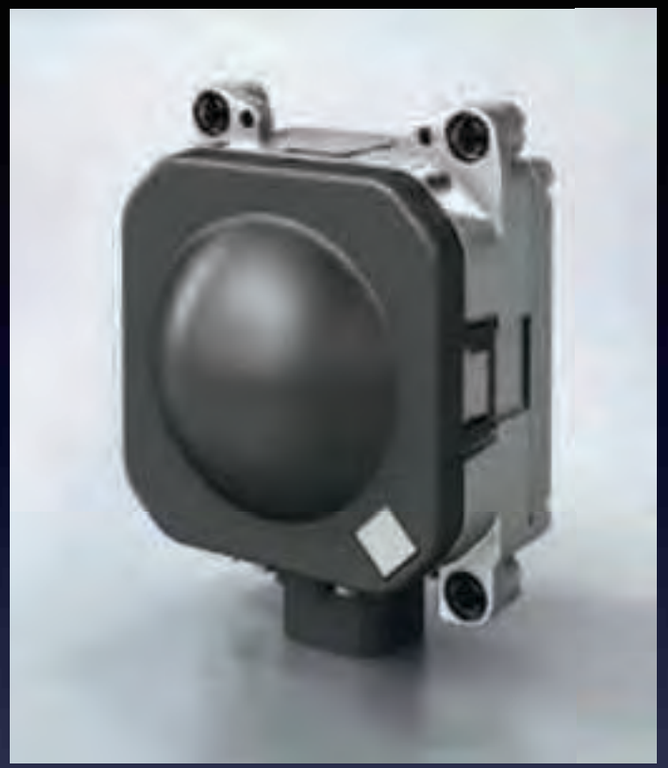
Athalye et al., 2018

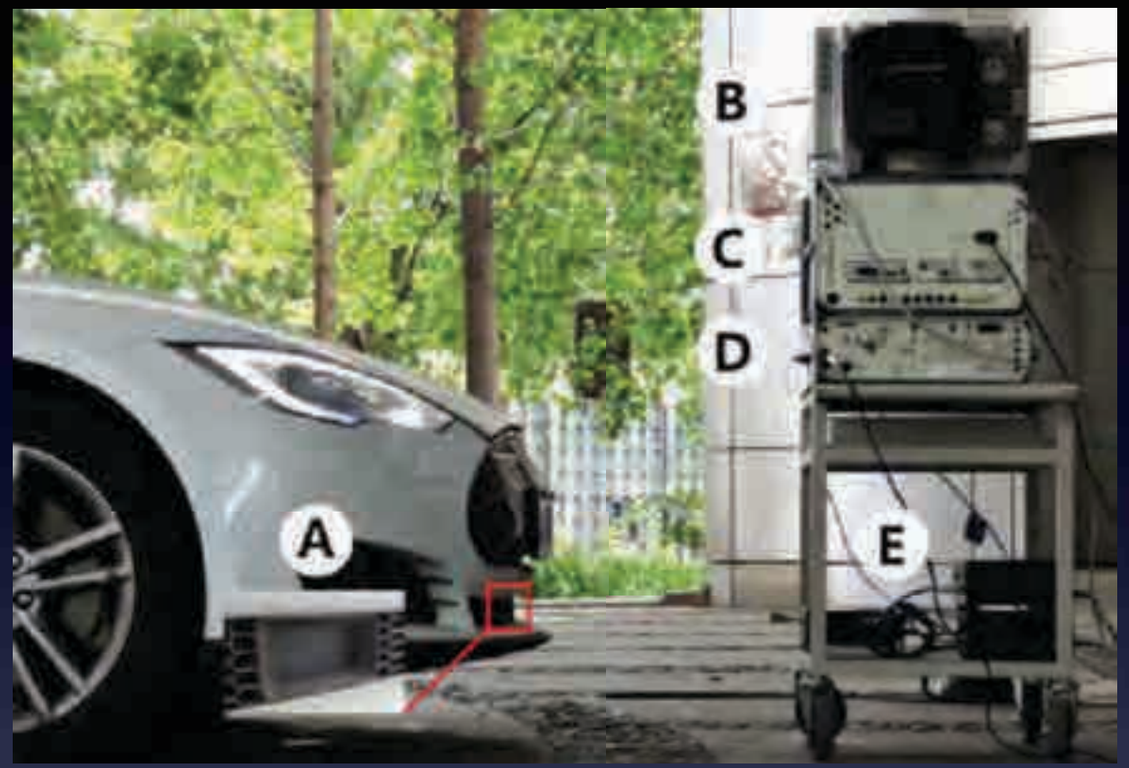
- Spoofing deep learning recognition models
  - Crafted adversarial examples
  - So far generally white box techniques
  - Do not currently work reliably in face of parametric distortions

MMW RADAR

- Collision avoidance
- Lower resolution than laser
- Most things very reflective
- Denial/spoofing:
  - Jamming
  - Chaff
  - Overhead signs

MMW RADAR





Oscilloscope

Signal Analyzer

Signal Generator

Harmonic Mixer
Frequency Multiplier

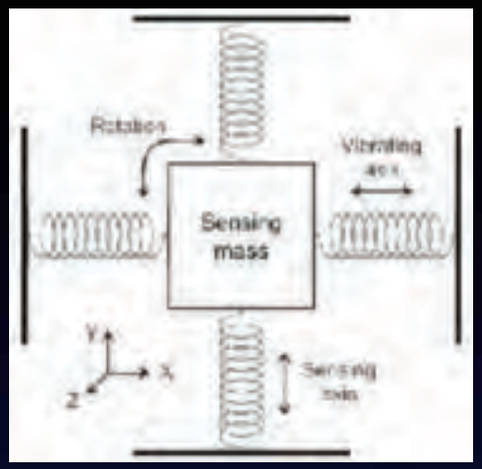
(a) Drive gear. (b) Autopilot. (c) Jammed.

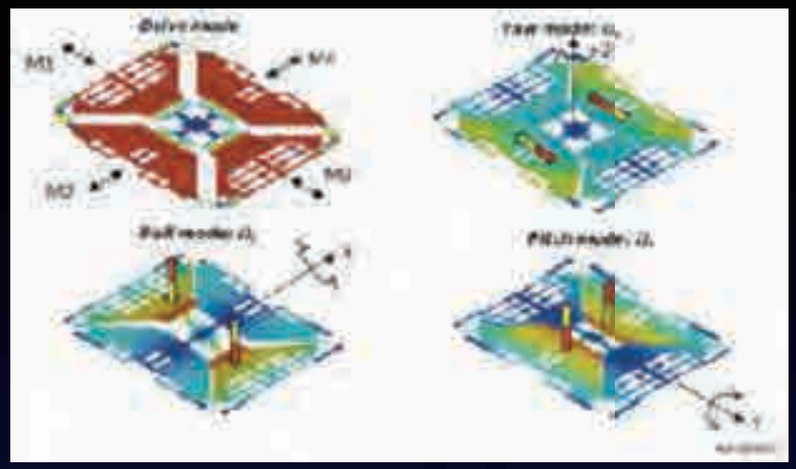
- Jamming: Contactless Sensor Attacks
  - Liu,Yan, Xu, DEF CON 24
  - Spoofing & relay attacks theorized but not performed

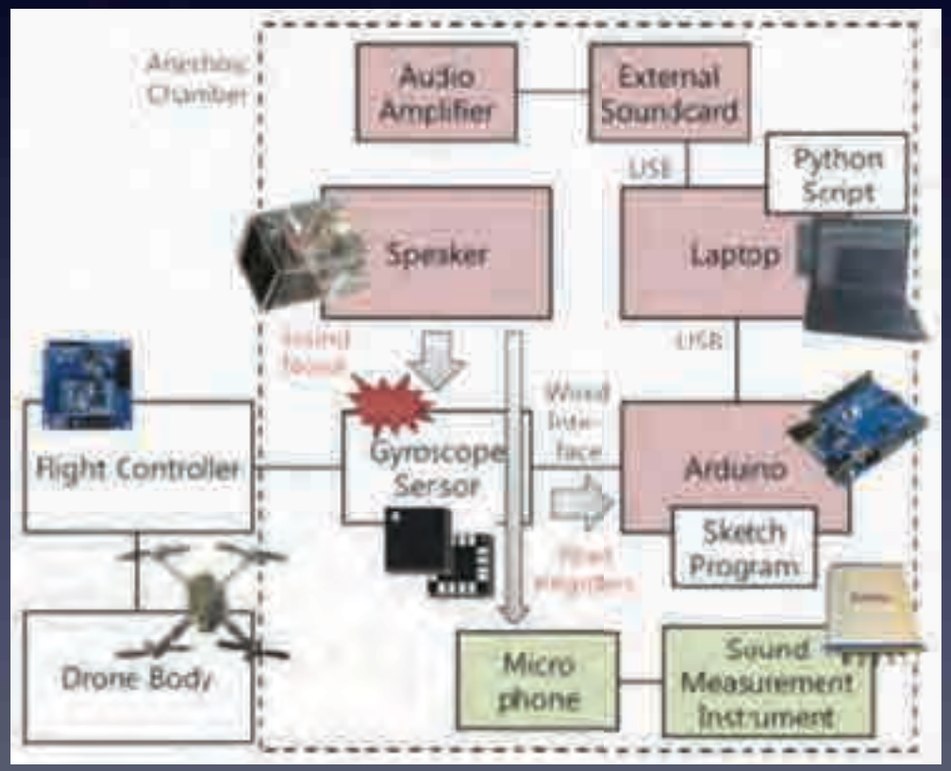
IMU & Compass

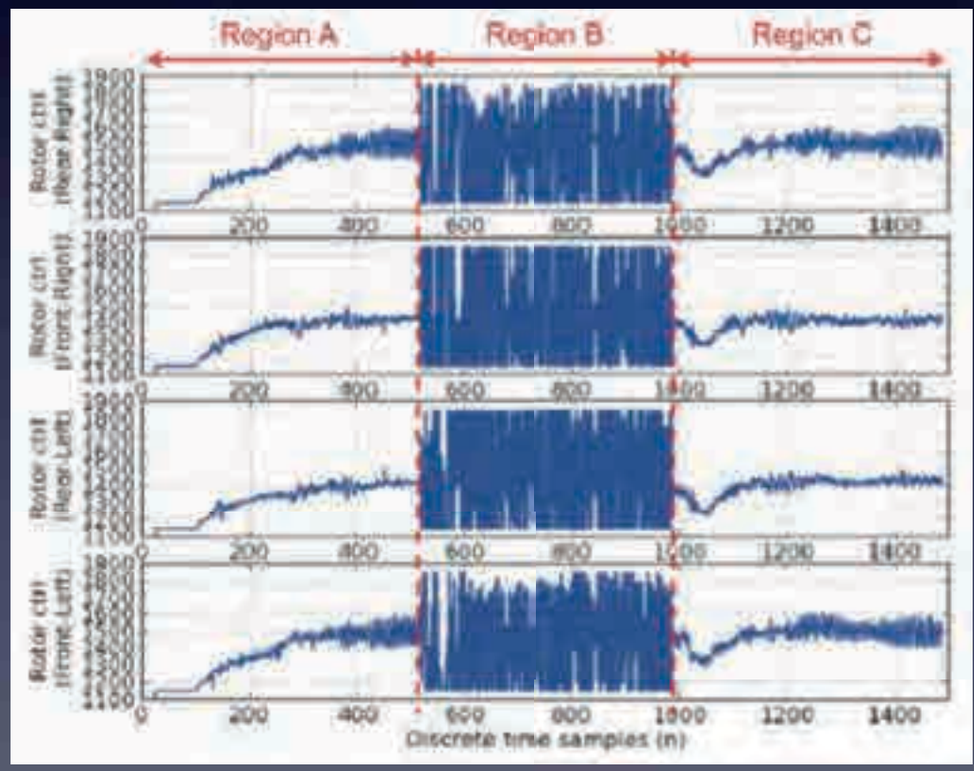
- Primary navigation sensor for some systems
- High fidelity models available
  - Typical cumulative error: 0.1% of distance traveled
- Denial/spoofing:
  - Extremely difficult to interfere with
  - Physical attacks with magnetic fields, thermal drift

IMU Acoustic Attacks









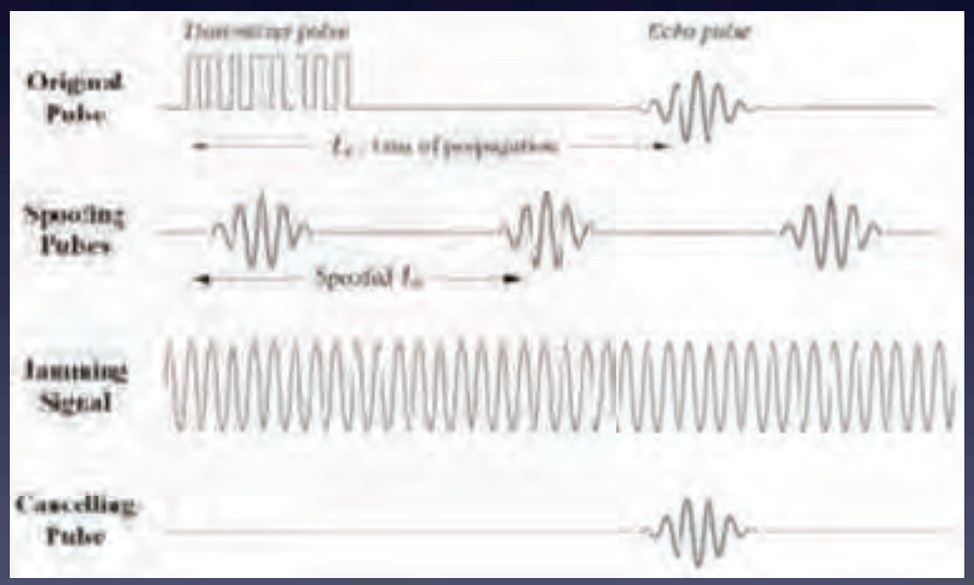
Son et al., KAIST, 2015

- MEMS gyroscope vibrates & has resonant frequency
  - Can be perturbed with external acoustic source
    - Similar to well-known attacks on spinning hard disks
  - Successfully POC'd by crashing flying multirotor UAV

Wheel Odometry

- Encoders
- Useful to know true speed & when stopped
- Attacks:
  - Change wheel diameter
  - Slippery surface
  - Removal may cause unpredictable behavior or stoppage

Ultrasonic Sensors



Contactless Sensor Attacks (Liu,Yan, Xu, DEF CON 24)

- Automated parking sensor
- Only used at low speed
- Attacks:
  - Jamming
  - Spoofing
  - Cancellation

Bond vs Robots

- GPS Jammer
- Smoke/Dust/Vapor
- Lightweight decoy obstacles
- Chaff
- Glass caltrops
- Oil slick

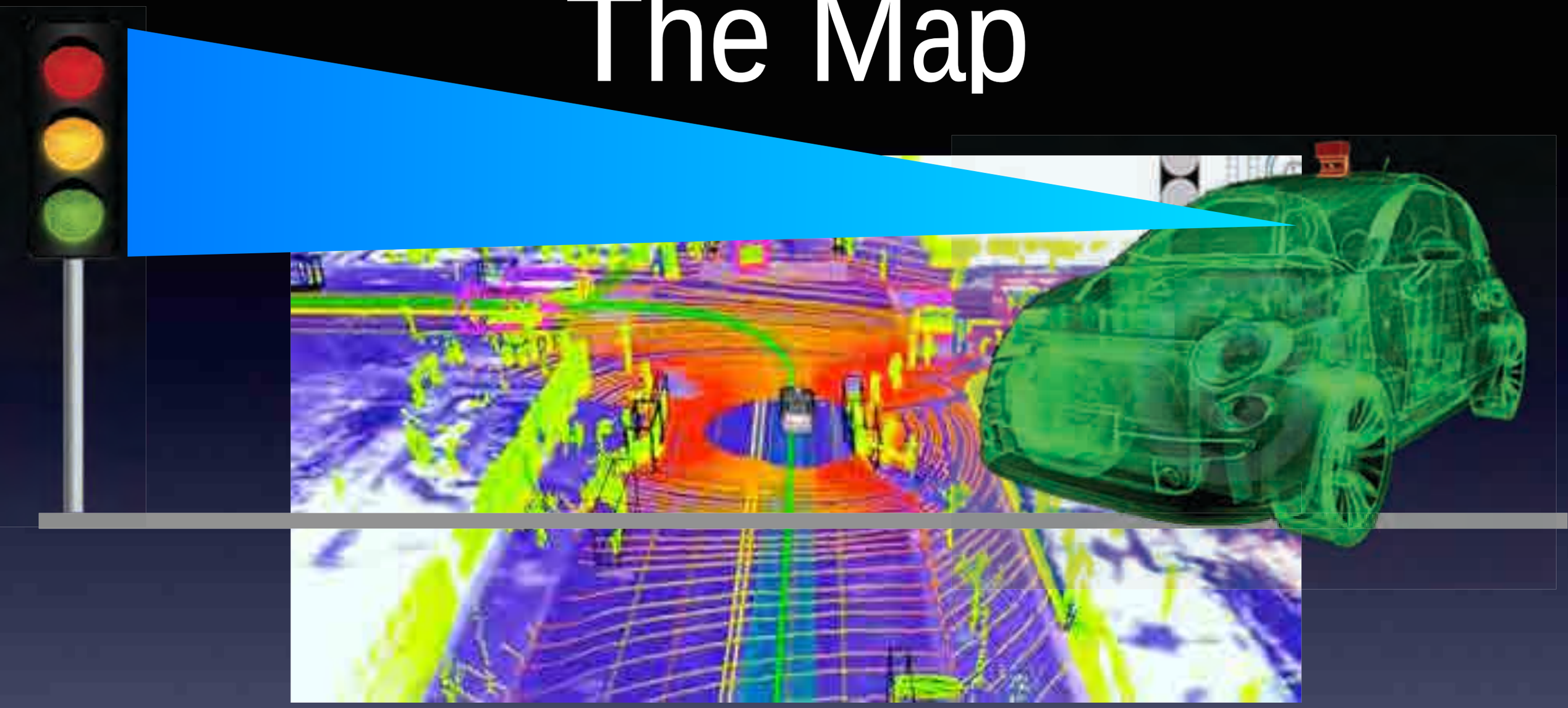
Bond vs Robots

- Active LIDAR Jammer/Spoofer
- Active Radar Jammer
- Acoustic Blaster
- Adversarial Turtle Dispenser

The Map

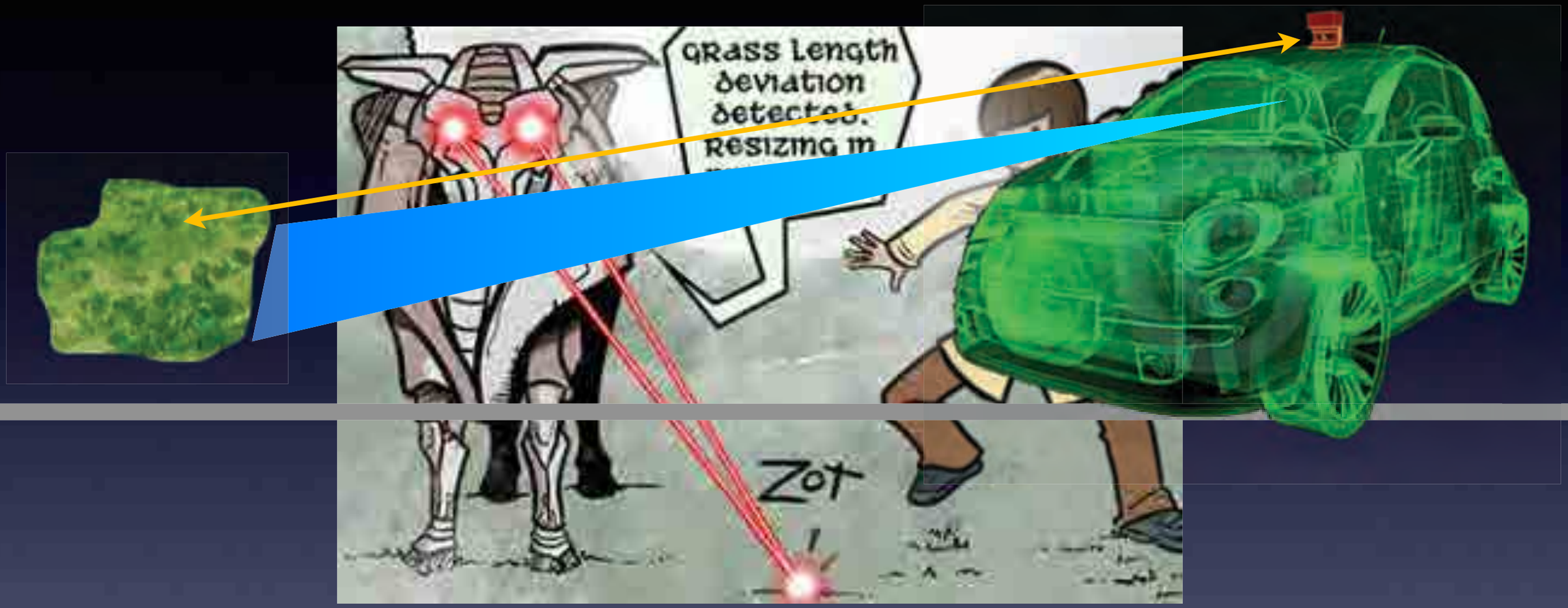
- Great emphasis on preacquired map data
- Often considered to be reference ground truth
- Reduces recognition load
  - Traffic lights
  - Vegetation
  - Other speed control & traffic management features

The Map



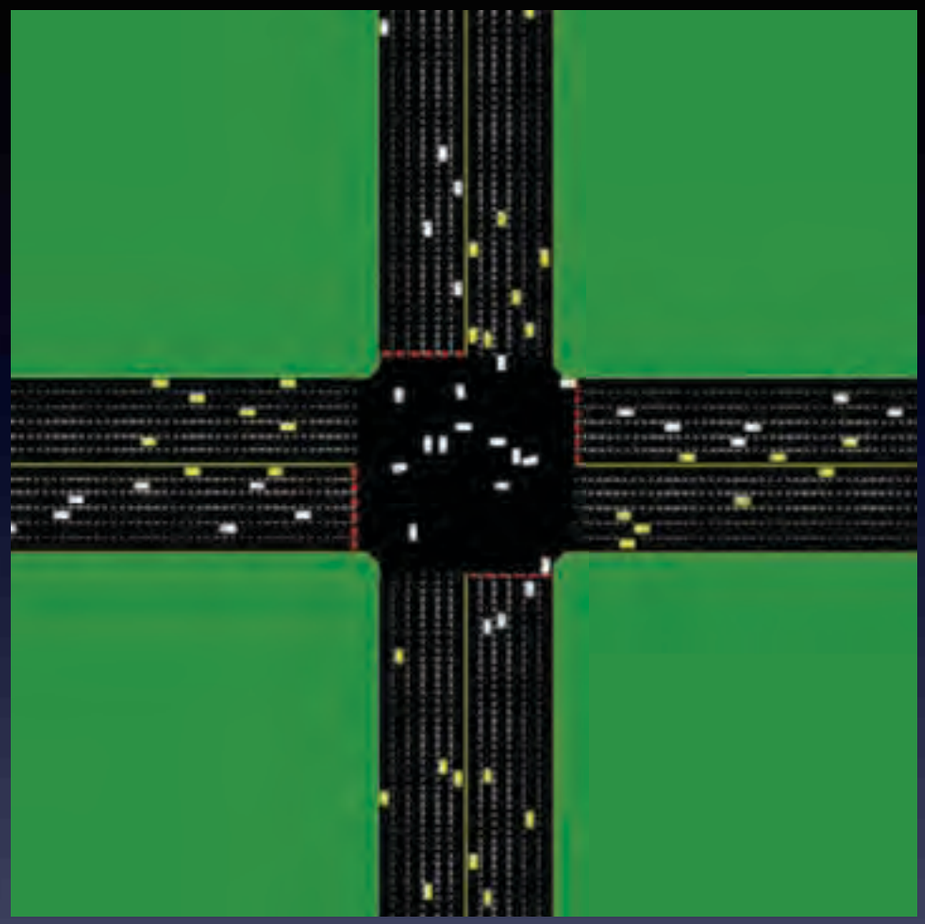
- Traffic lights
  - Camera knows where to look
  - Difference in robot vs human assumptions

The Map



- Vegetation
  - Colorized LIDAR
  - Transmission classifier
- Overhanging foliage
- Map dependence may exacerbate brittleness of discrimination rules

The Map



Peter Stone, UT Austin

- Map requires constant updates
- Local map:
  - Vulnerable to unexpected real world features
- Remote map:
  - Vulnerable to denial (4G jamming)
  - Vulnerable to spoofing (MITM attack, standard cellular intercept techniques)

Exploiting the Logic Structure

- Goal: Maximize uncertainty
  - Requiring manual assistance
  - Confusing/annoying occupants
  - Inconveniencing other road users
- Concentrate on fragile maneuvers
- Attacker has access to map too

Trapping/Redirecting

- Attacks at collision avoidance & navigation layers
- Force robot to postpone high level tasks
  - Moving obstacles
  - Obstacle swarms
  - Artificial stop signs
- Human driver wouldn’t notice, robot can’t ignore

Clobbering

- Goal: make robot run into something
- Subvert collision avoidance
  - Incapacitate vehicle
  - Damage/remove sensors
- Subtle map deviations
- Imitate light vegetation
- Simulate obstacles at speed
- Disguise entrance walls with reflective/absorbent material within GPS noise
- Dynamic obstacles under overhead signs

Would you buy a self-driving car that couldn't drive itself in 99 percent of the country? Or that knew nearly nothing about parking, couldn't be taken out in snow or heavy rain, and would drive straight over a gaping pothole?

If your answer is yes, then check out the Google Self-Driving Car, model year 2014.

— *MIT Technology Review, August 2014*

V2V

U.S. Department
of Transportation
**National Highway
Traffic Safety
Administration**

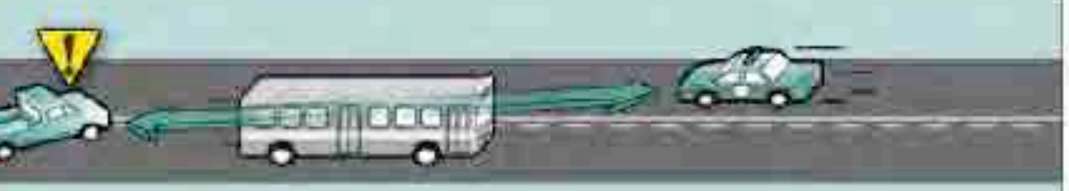
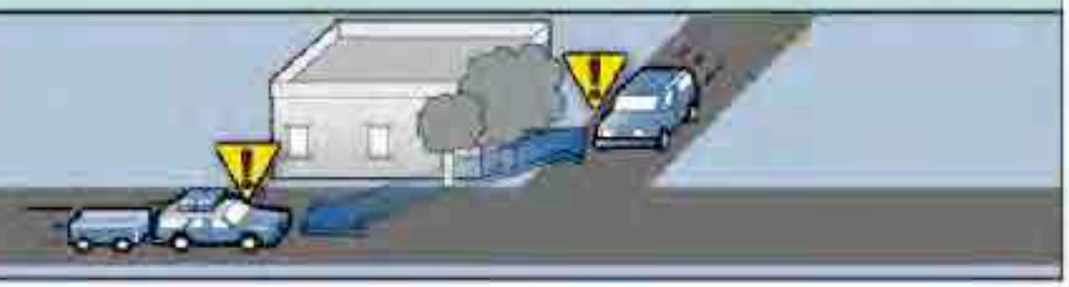
NHTSA
www.nhtsa.gov

DOT HS 812 014

August 2014

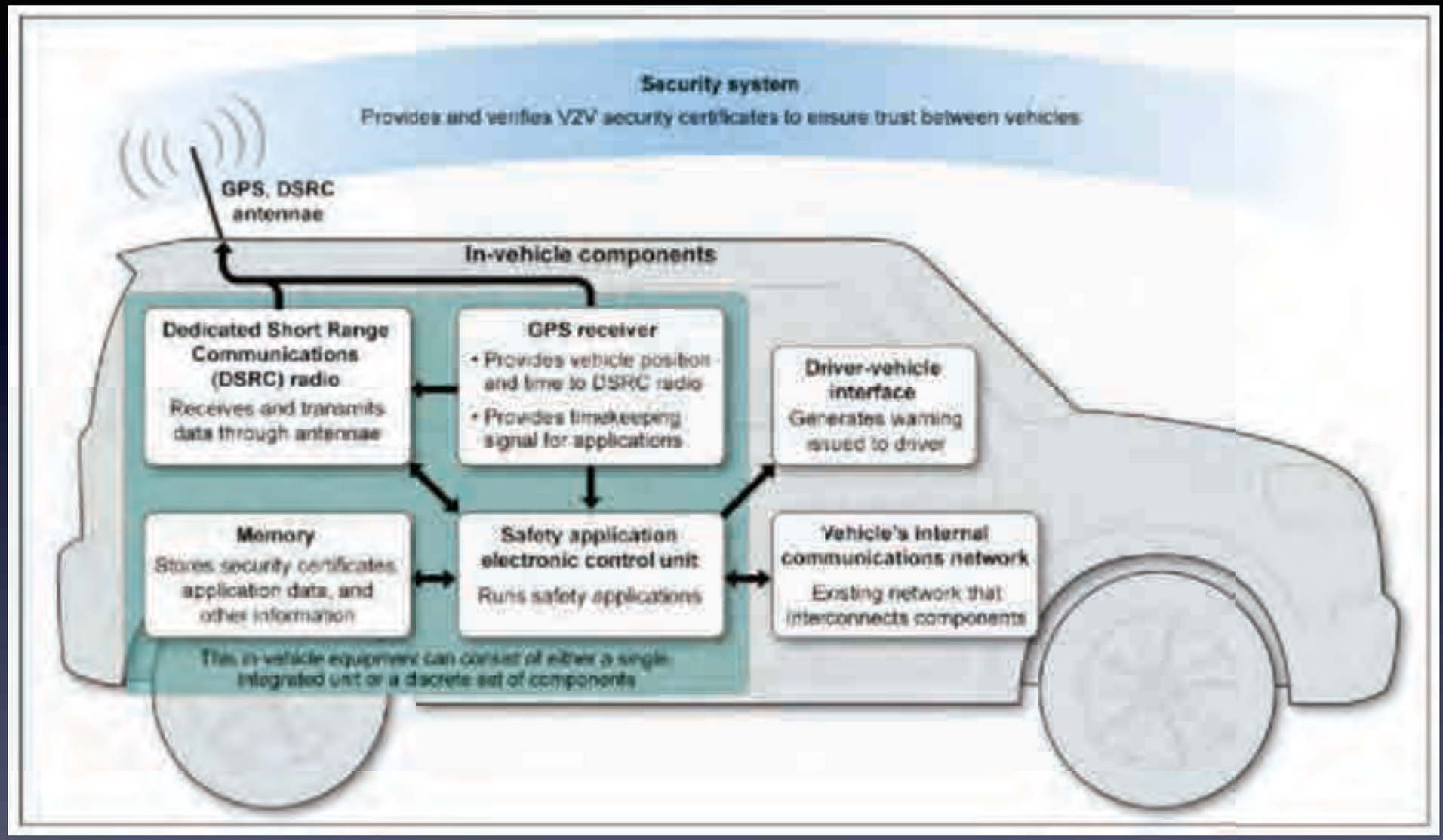
Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application

V2V Components

Scenario and warning type		Scenario example
Rear end collision scenarios	**Forward collision warning** Approaching a vehicle that is decelerating or stopped.	
	Emergency electronic brake light warning Approaching a vehicle stopped in roadway but not visible due to obstructions.	
Lane change scenarios	**Blind spot warning** Beginning lane departure that could encroach on the travel lane of another vehicle traveling in the same direction; can detect vehicles not yet in blind spot.	
	Do not pass warning Encroaching onto the travel lane of another vehicle traveling in opposite direction; can detect moving vehicles not yet in blind spot.	
Intersection scenario	**Blind intersection warning** Encroaching onto the travel lane of another vehicle with whom driver is crossing paths at a blind intersection or an intersection without a traffic signal.	

- Just warnings for now!

V2V Components



- Both on-board and roadside communicators
- DSRC: Omnidirectional, 300m range, 200-500 bytes
- Basic Safety Message (BSM) protocol
  - Not encrypted
  - PKI authenticated (signed via certificates)

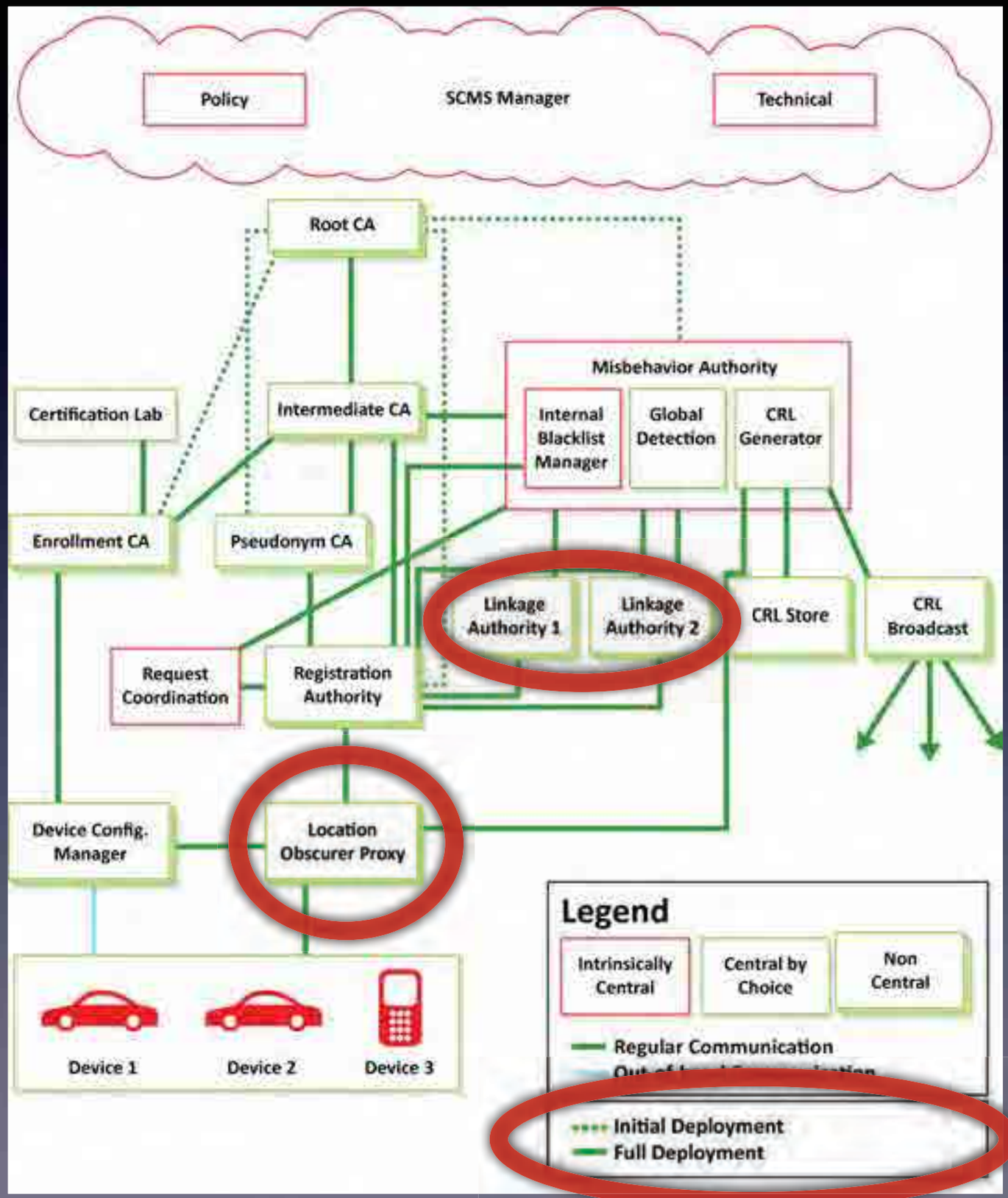
V2V Transmissions

Table V-1 Contents of BSM Part I[3,4]

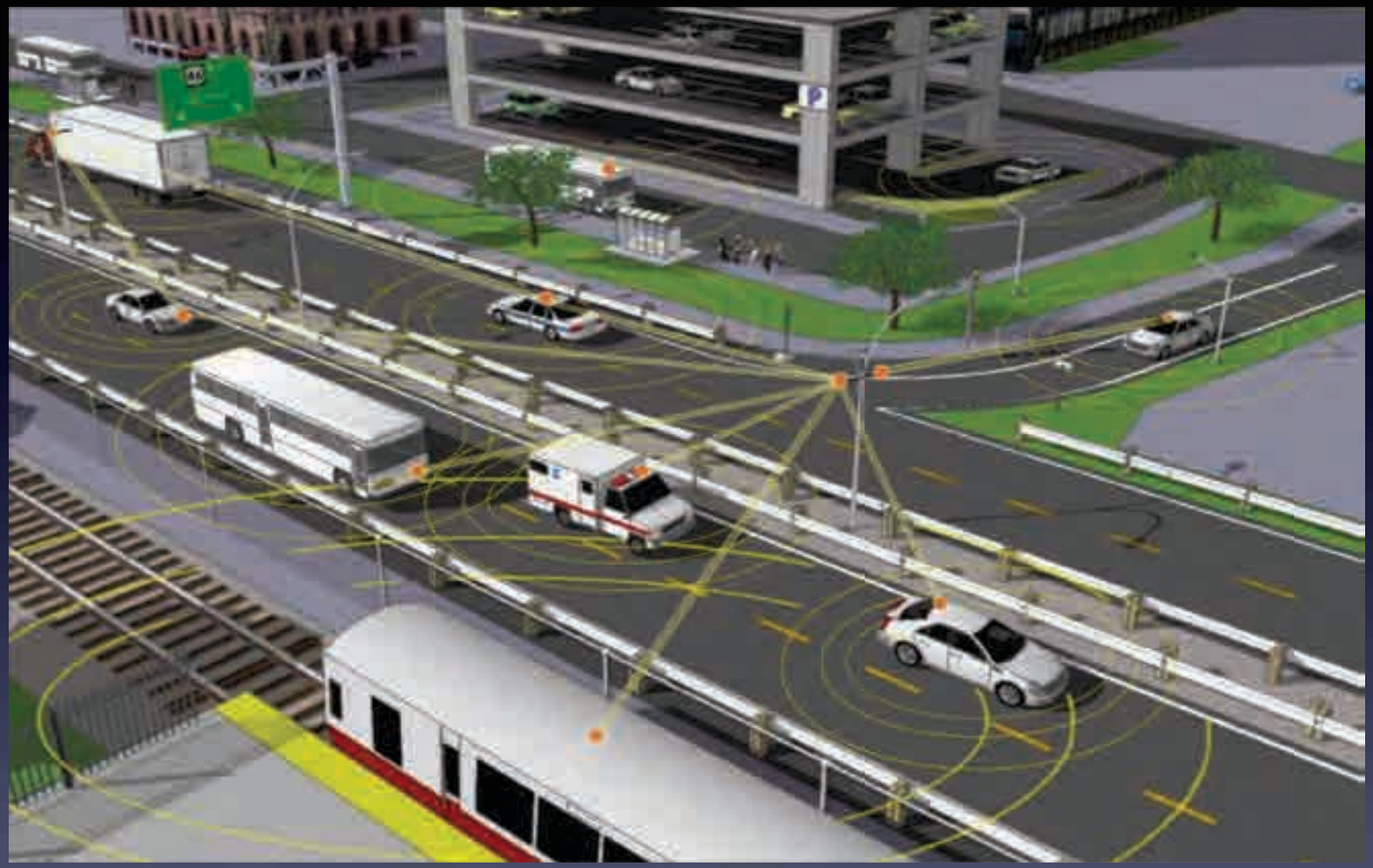
Part I	
Data Frame (DF)	**Data Element (DE)**
Position (DF)	
	Latitude*
	Elevation*
	Longitude*
	Positional accuracy*
Motion (DF)	
	Transmission state*
	Speed
	Steering wheel angle
	Heading*
	Longitudinal acceleration*
	Vertical acceleration
	Lateral acceleration
	Yaw rate*
	Brake applied status
	Traction control state
	Stability control status
	Auxiliary brake status
	Brake status not available
	Antilock brake status
	Brake boost applied
Vehicle size (DF)	
	Vehicle width
	Vehicle length
	*Required in Safety Pilot Model Deployment

- Part I: Core
  - Part II: Appended when changed, vehicle-specific
  - Note unencrypted GPS
    - Spoofing feedback?

V2V Security

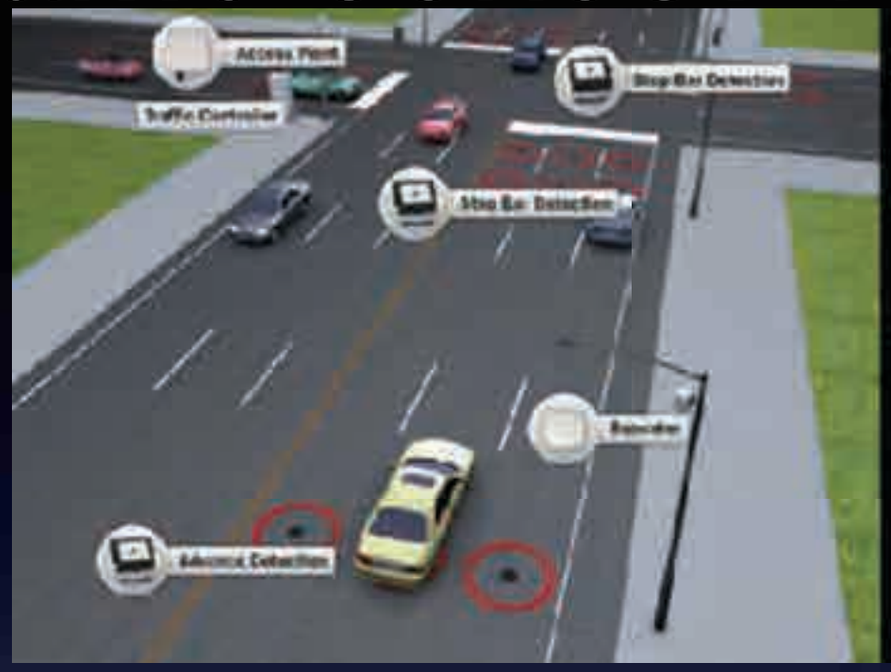


V2V Bottom Lines

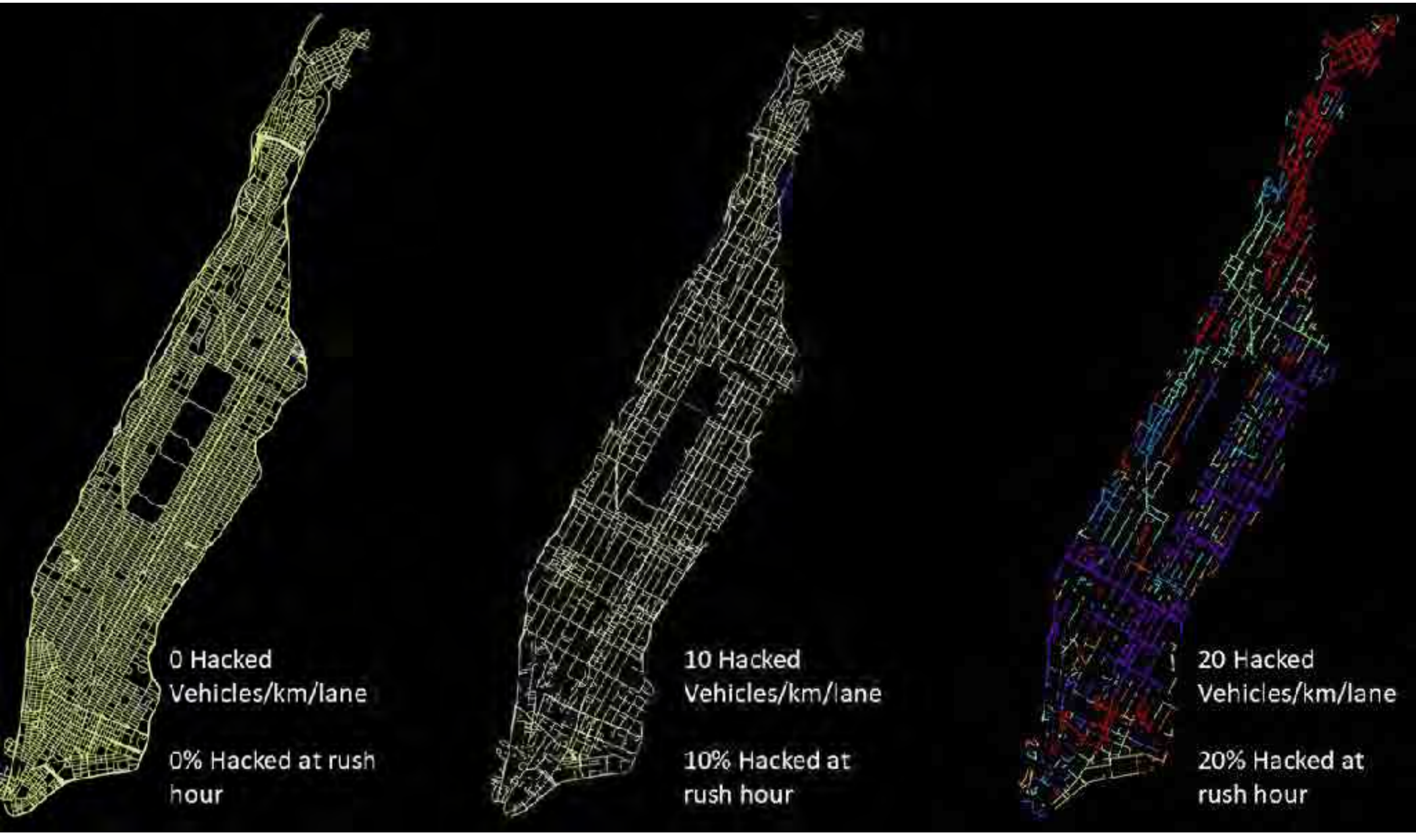


- Careful rollout: 11 year development
- Slow & steady rollout: 37 years to full fleet
- Tracking/Privacy more immediate concern than other malicious attacks
- Standard PKI concerns, many yet TBD
- No direct control imminent (robots might get there first)

Traffic Sensor Flaws



- V2V/V2I aims to avoid mistakes of current traffic sensors
  - Hacking US Traffic Control Systems, Cesar Cerrudo @IOActive, DEF CON 22
    - No encryption/authentication, wireless transmission in cleartext
    - Firmware updates neither encrypted nor signed
- No doubt will make others!


0 Hacked
Vehicles/km/lane
0% Hacked at rush
hour
10 Hacked
Vehicles/km/lane
10% Hacked at
rush hour
20 Hacked
Vehicles/km/lane
20% Hacked at
rush hour

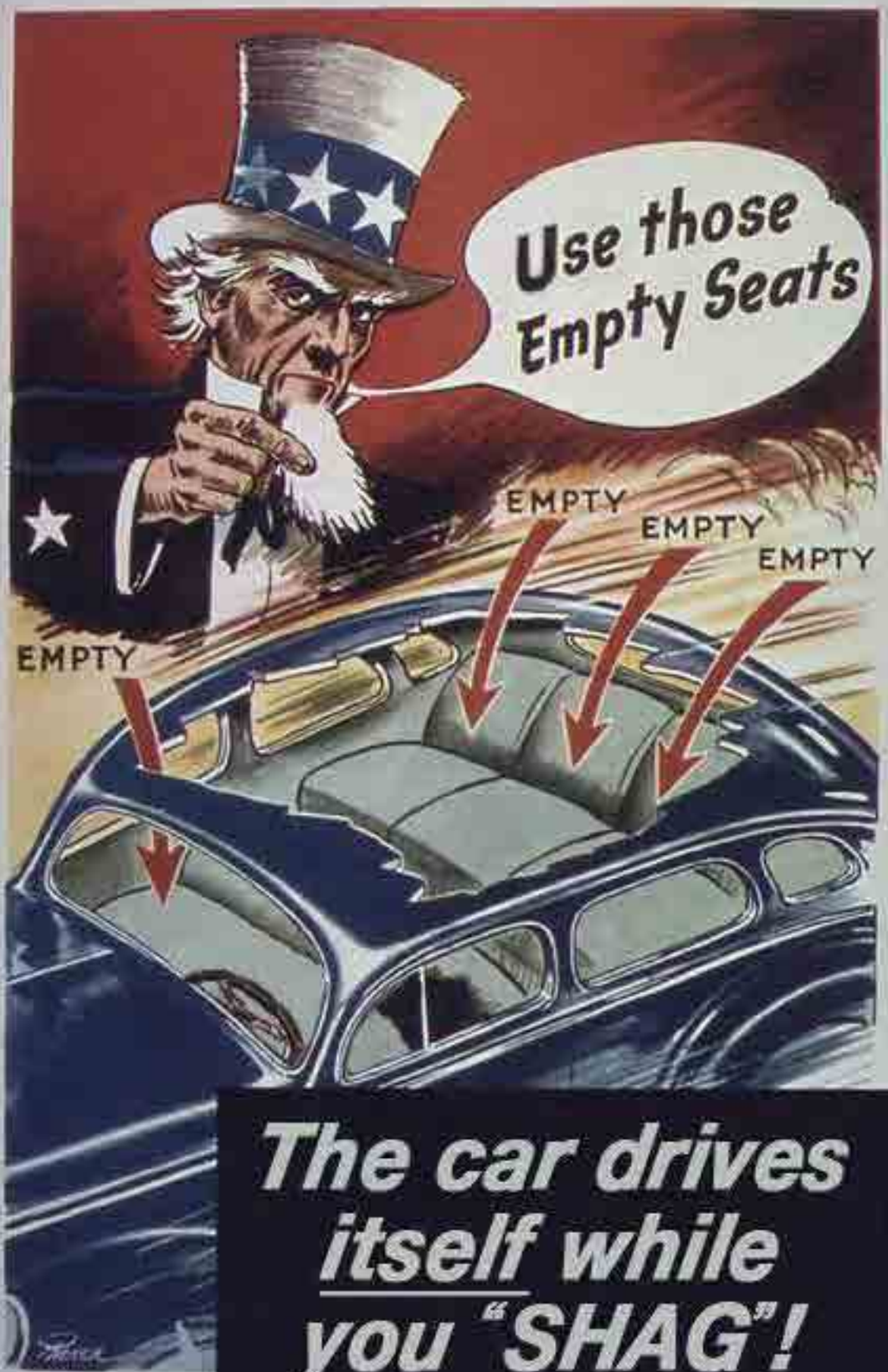
Remember...

Driverless vehicles are cool!

Don’t do any of these things!

~~Don’t hassle the Hoff!~~

Don’t hax0r the Bots!


Use those Empty Seats
EMPTY
EMPTY
EMPTY
EMPTY
The car drives itself while you "SHAG"!