Sensor Spoofing: Attacks and Consequences

Yasser Shoukry

Resilient Cyber-Physical Systems Lab
Department of Electrical and Computer Engineering
University of Maryland, College Park

A. JAMES CLARK
SCHOOL OF ENGINEERING

Sensors in IoT

Sensors in IoT

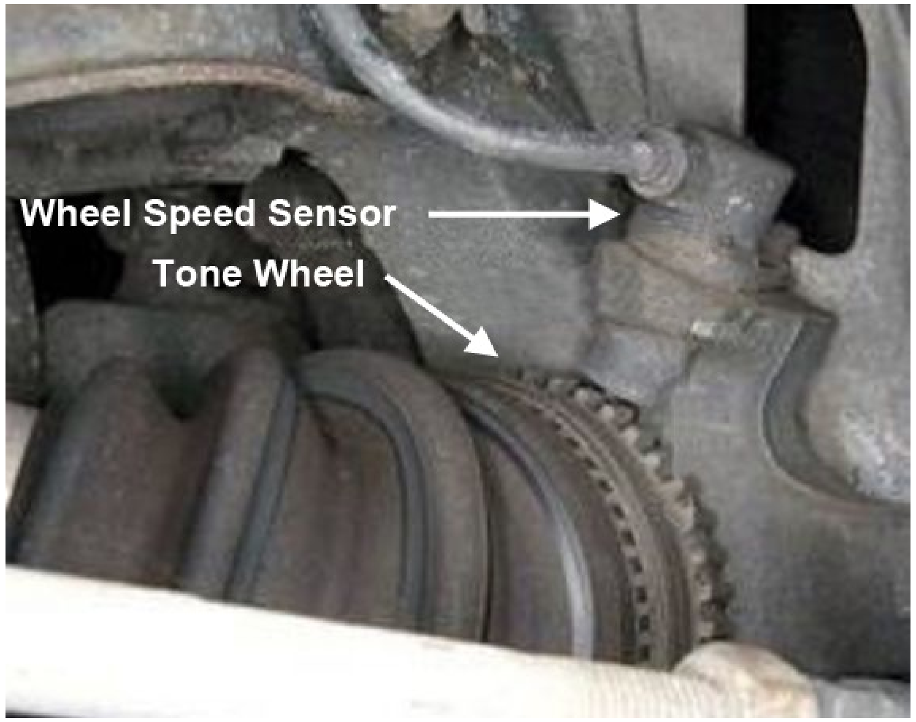
Type 1: Physical Spoofing Attacks (Attacks from the Environment)

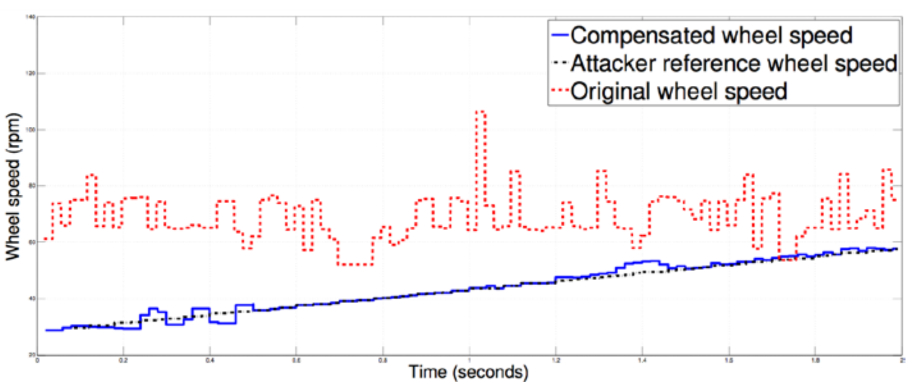
Message #1: Physical Attacks on IoT sensors are feasible

GPS Spoofing Attacks: Navigation

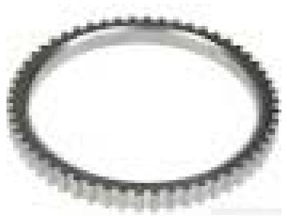
Mark L. Psiaki (Cornell) and Todd E. Humphreys (UT Austin)

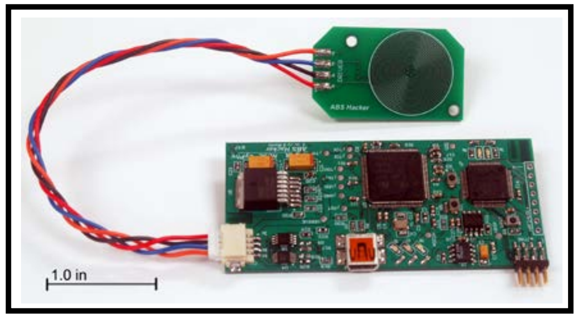
Spoofing Attacks: Automotive Systems



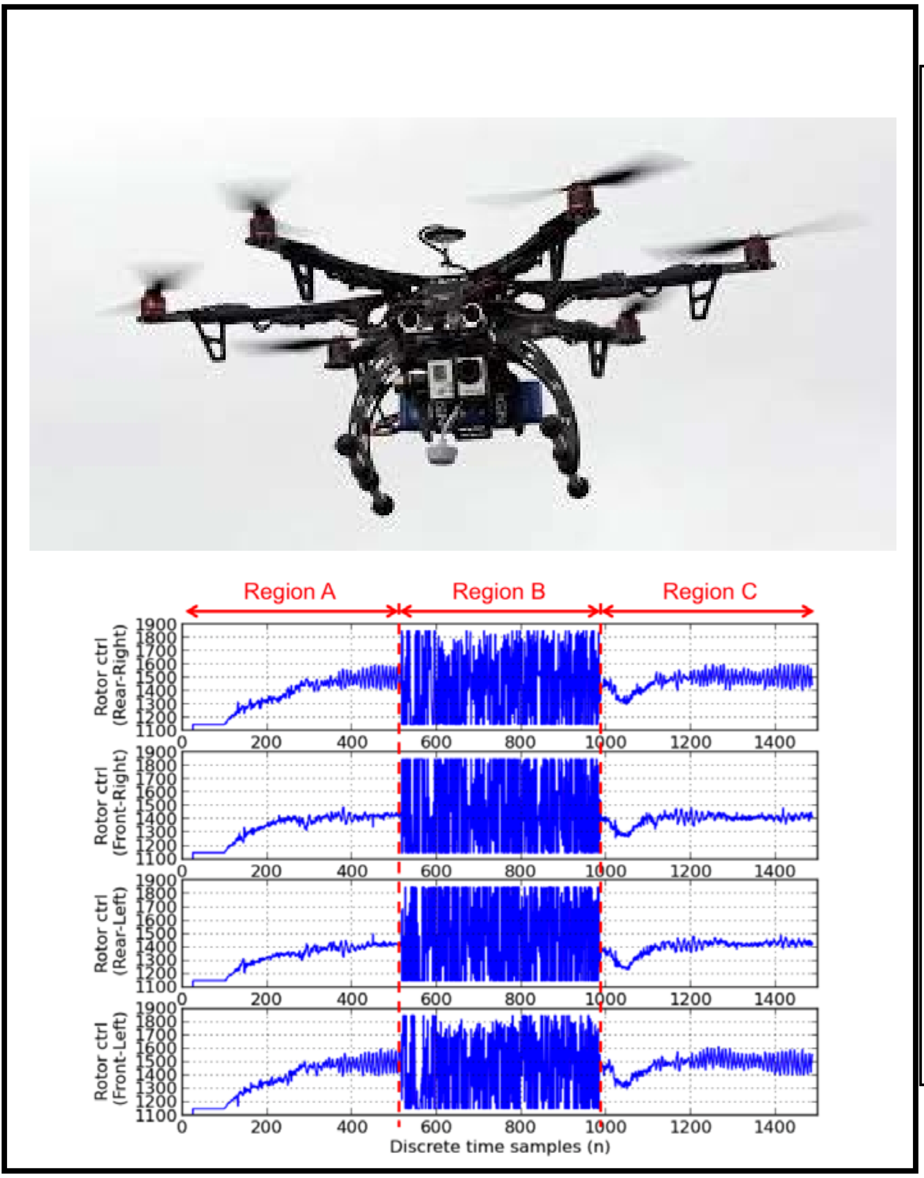


Y. Shoukry, et. al, “Noninvasive Spoofing Attacks for Anti-Lock Braking Systems,” CHES 2013





Spoofing Attacks: Quadrotors

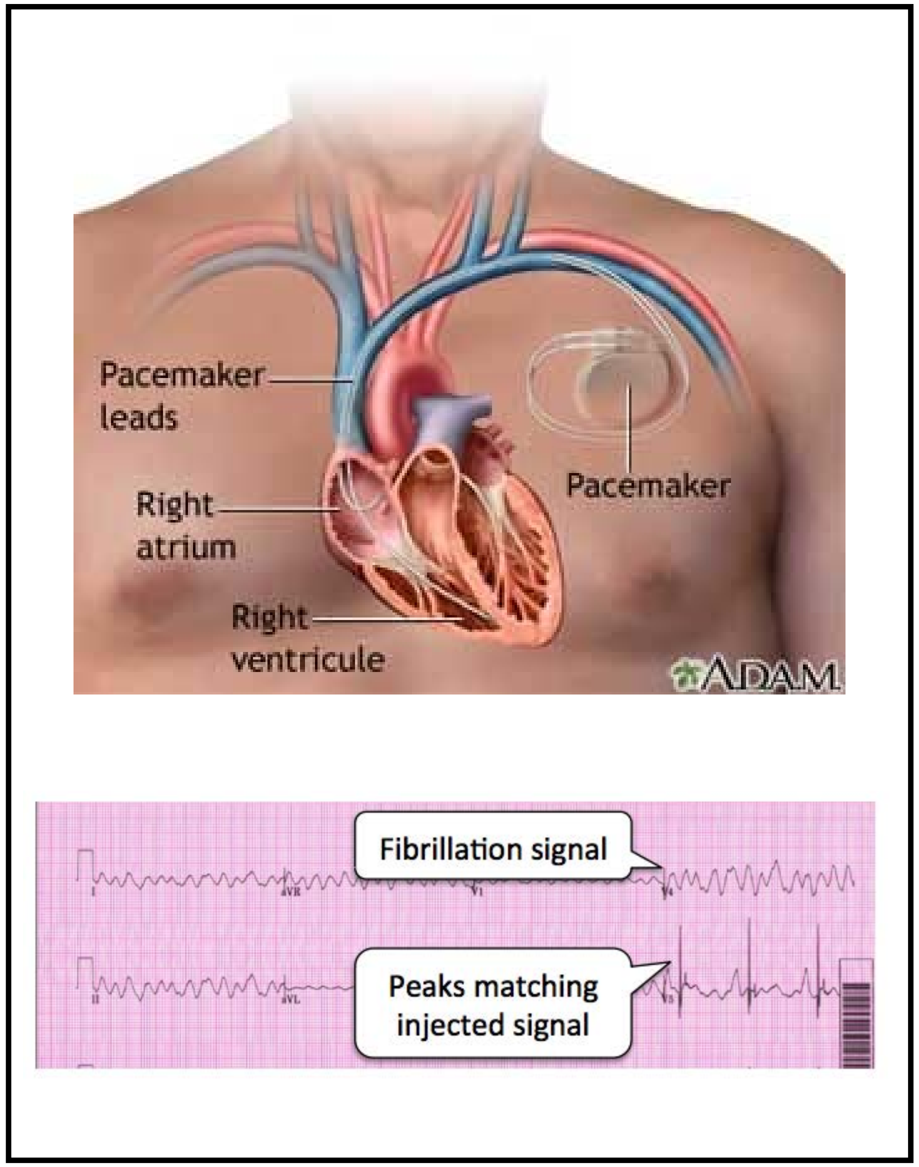


Y. Son, et. al, “Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors,” USENIX Security 2015.

Spoofing Attacks: Power Grid

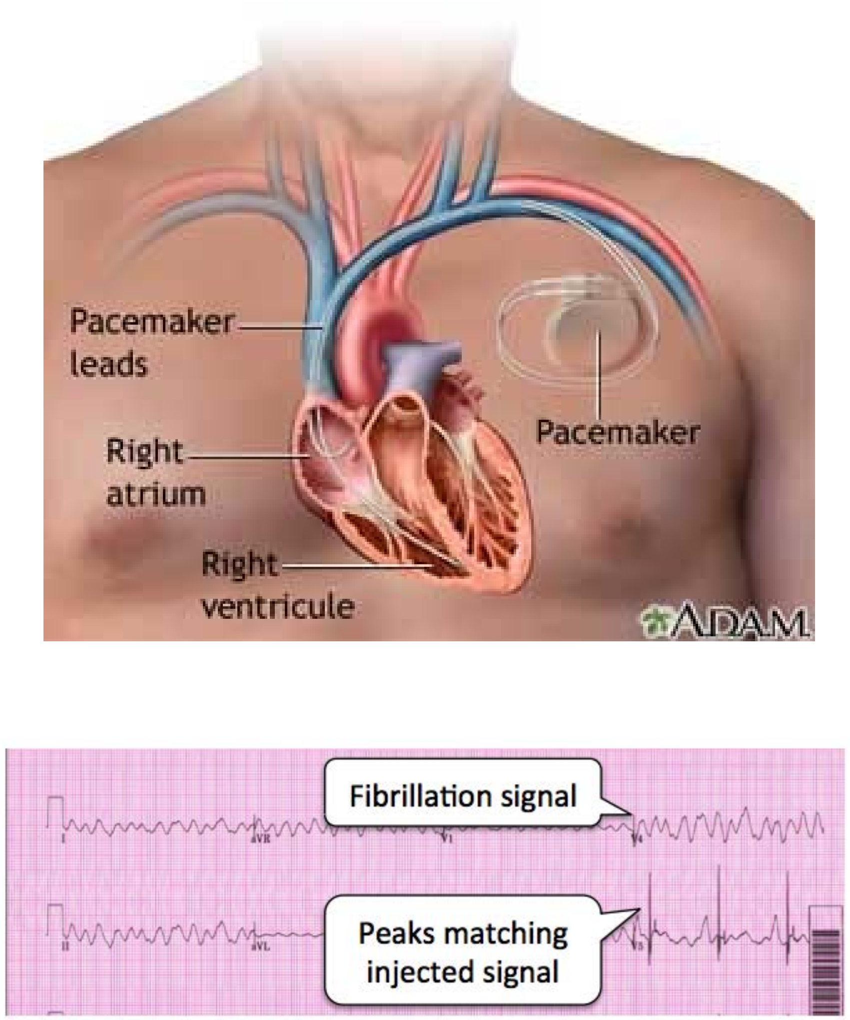
- Power grid consists of multiple generators and loads.
- These generators MUST be synchronized to maintain the stability of the power grid
- Phasor Measurement Units (PMU) are used to measure the phase differences between generators
- Two attack vectors:
  - GPS attacks (used for time-sync)
  - False data injection attacks

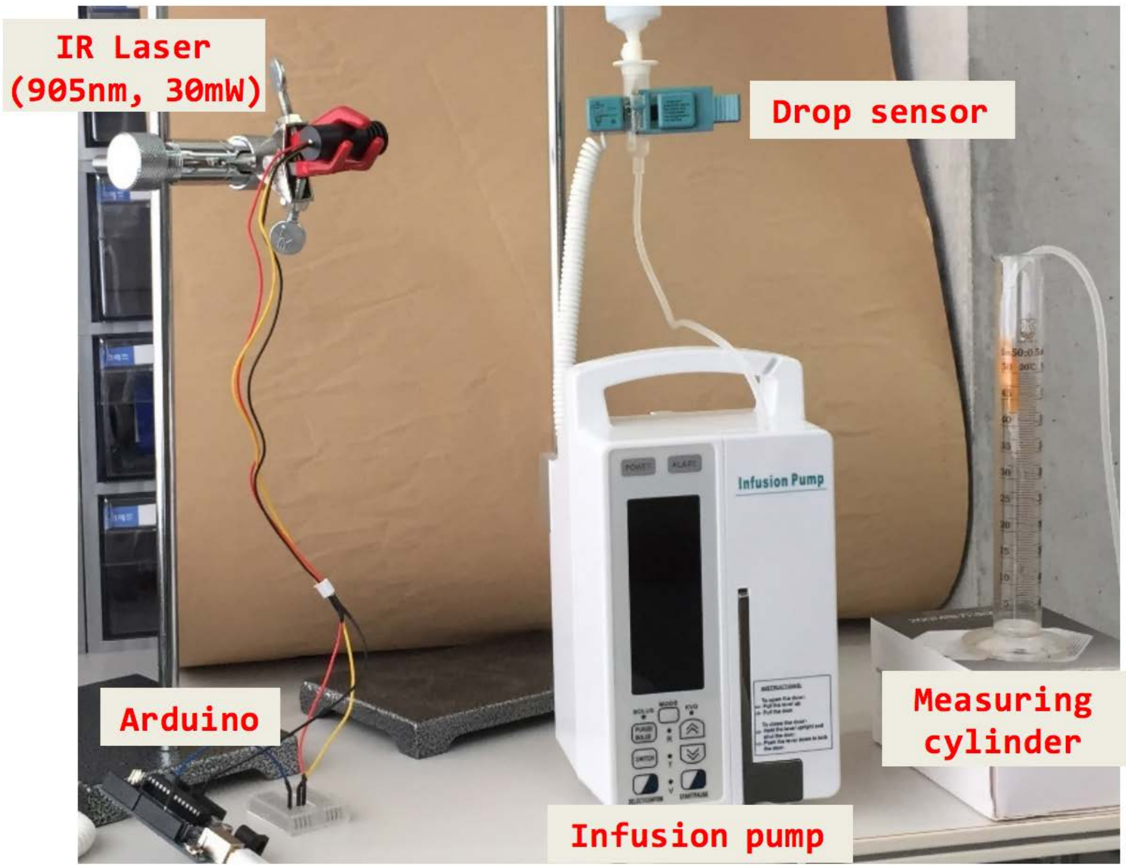
Spoofing Attacks: Medical Devices



D. Kune, et. al, “Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors,” IEEE S&P 2013.

Spoofing Attacks: Medical Devices



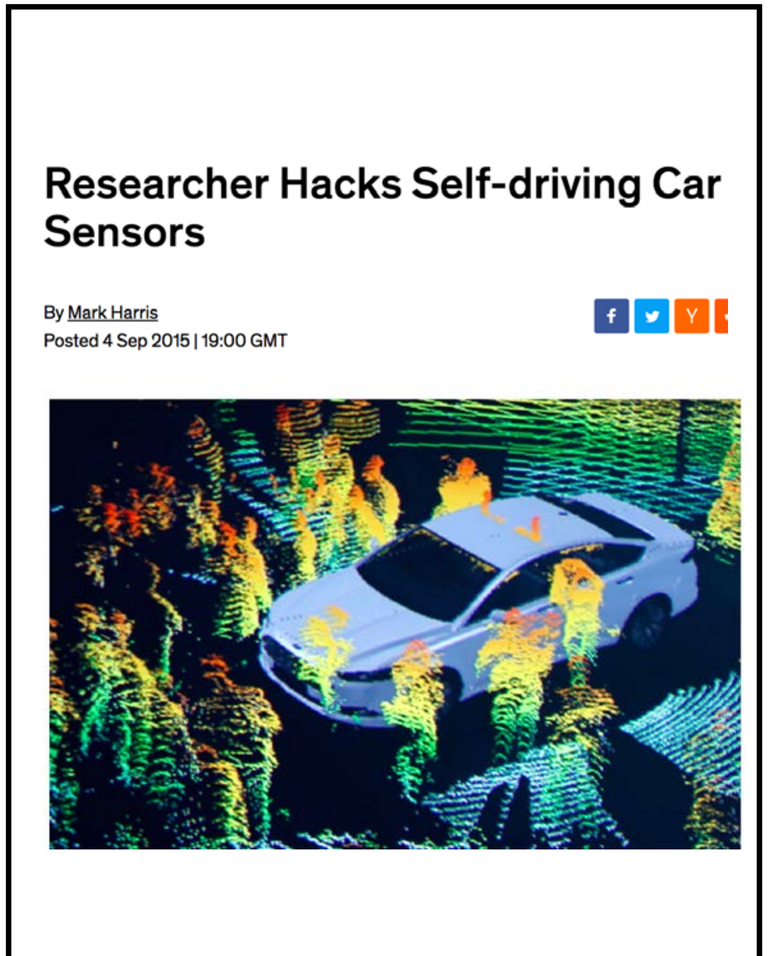


Under/Over infusion

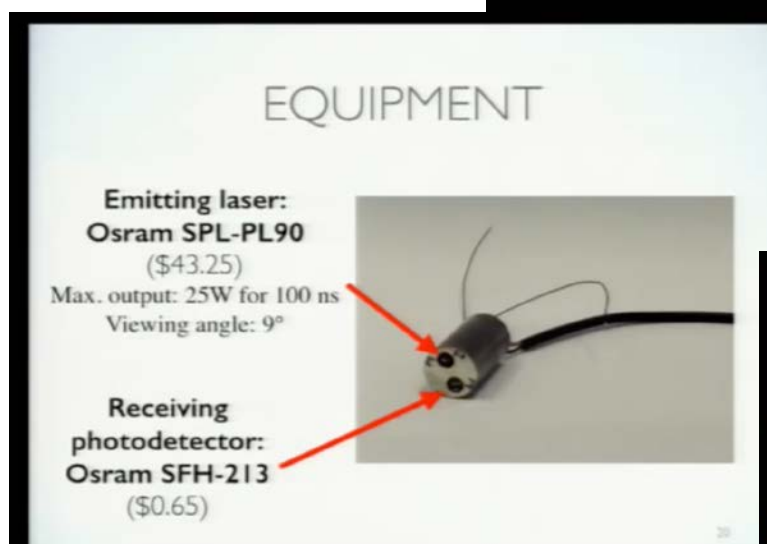
D. Kune, et. al, "Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors," IEEE S&P 2013.

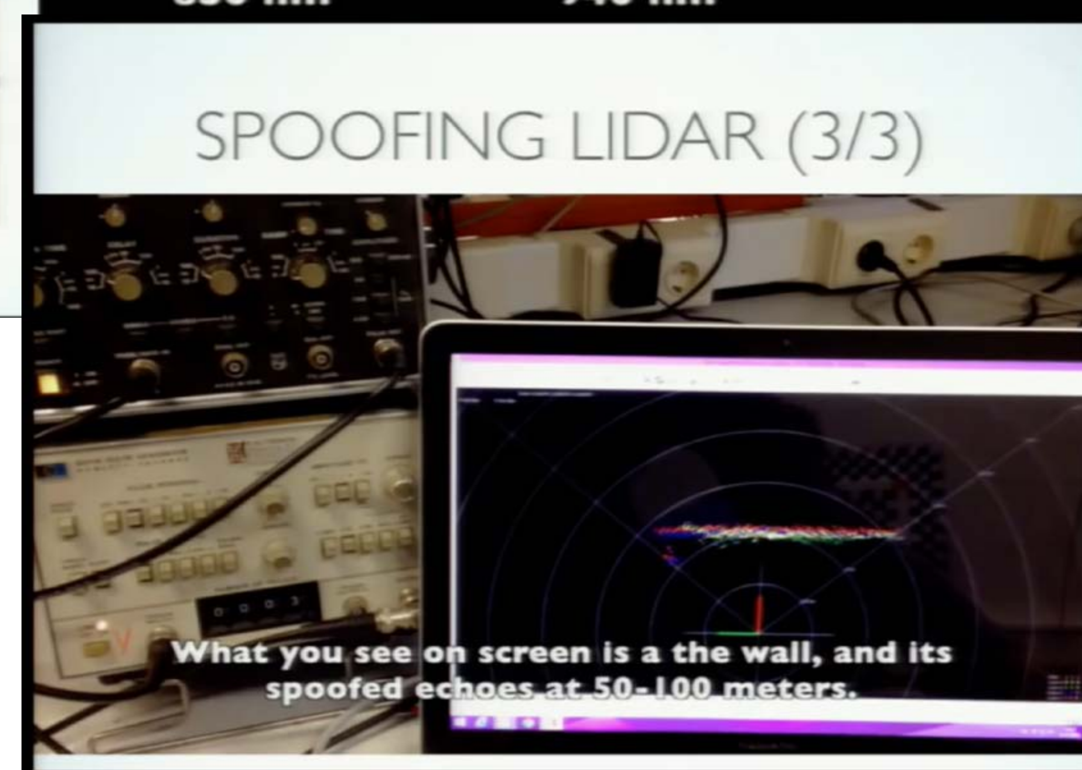
Y. Park, et. al, "This Ain't Your Dose: Sensor Spoofing Attack on Medical Infusion Pump," WOOT 2016.

Spoofing Attacks: Self-Driving Cars



J. Petit, et. al, “Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR” blackhat 2015.



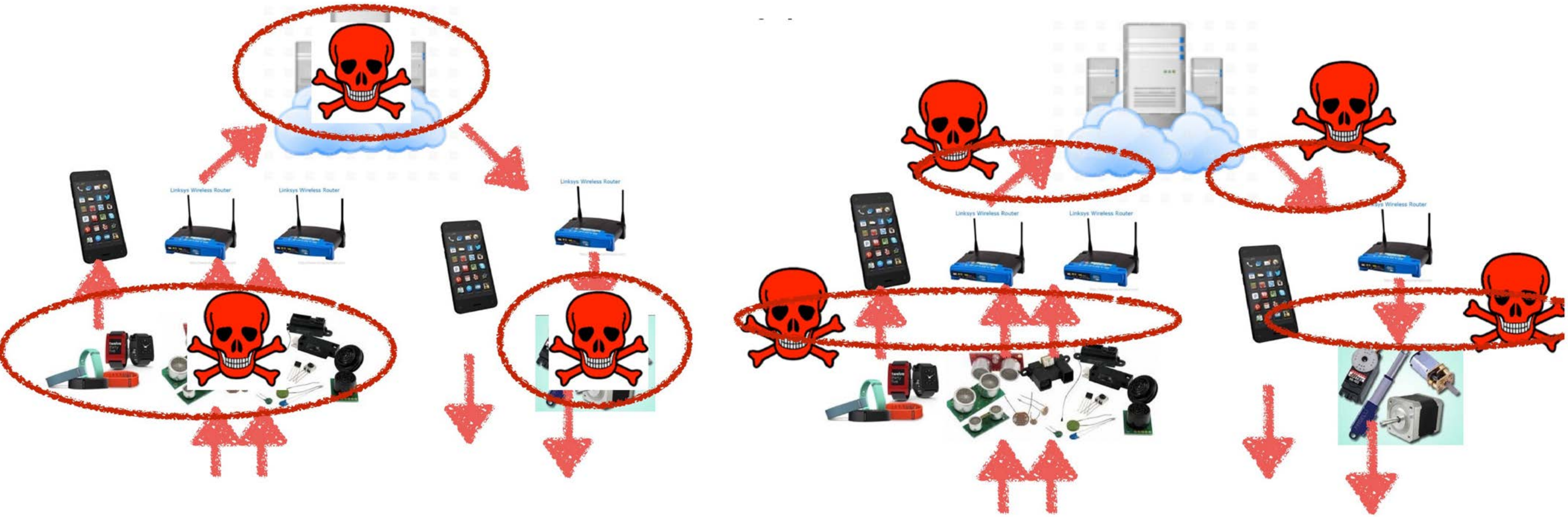


Black Hat talk: https://www.youtube.com/watch?v=C29UGFsIWVI

Message #1: Physical Attacks on IoT sensors are feasible

Message #1.1: information-security offers no defense against these attacks!

Type II: Cyber Attacks (Software or Communication)



Message #1: Physical Attacks on IoT sensors are feasible, but cyber attacks maybe easier, but leads to the same consequences

Message #1.1: information-security offers no defense against these attacks!

Beyond Sensor Physical Spoofing

Beyond Sensor Physical Spoofing

Message #1: Physical Attacks on IoT sensors are feasible, but cyber attacks maybe easier but leads to the same consequences

Message #1.1: information-security offers no defense against these attacks!

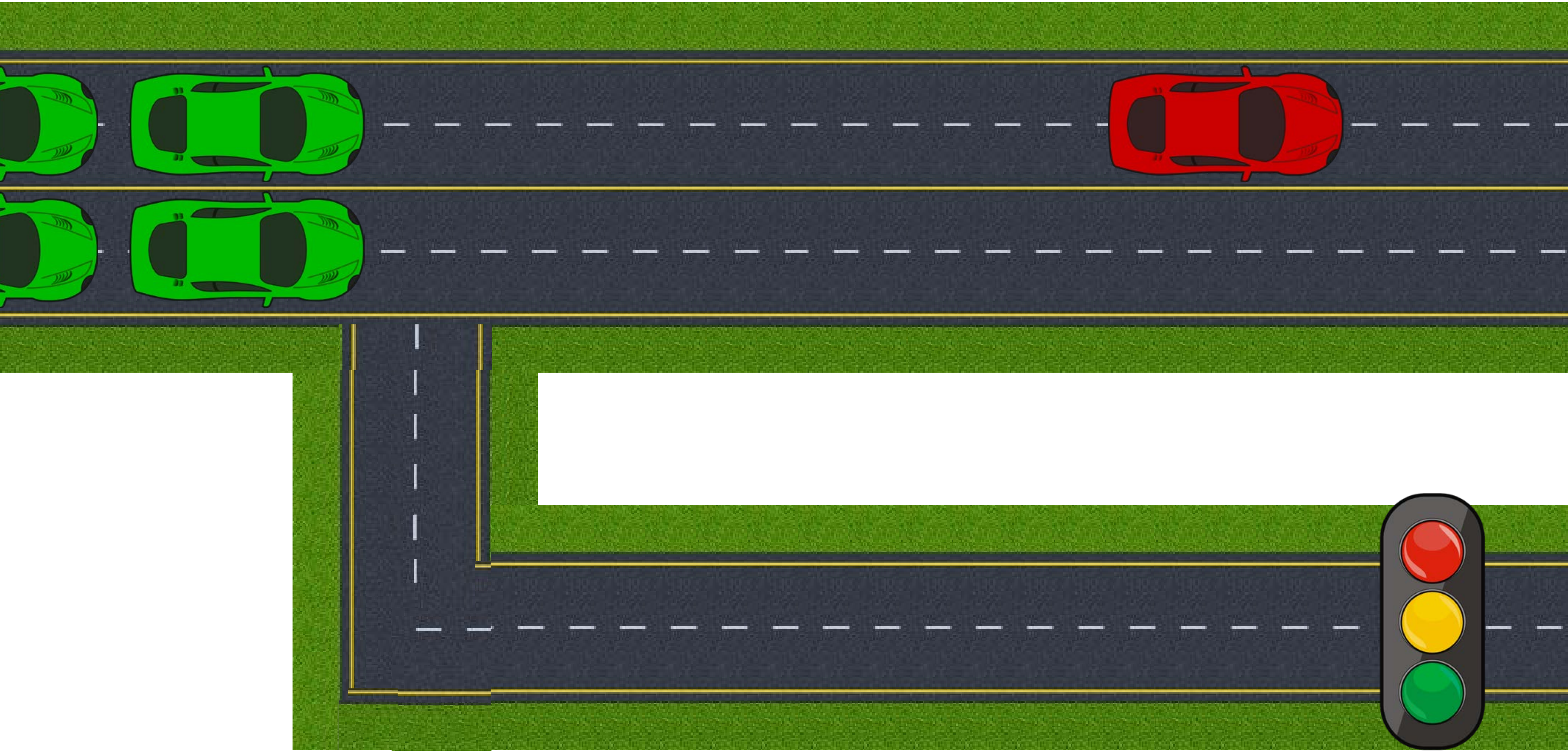
Attack Consequences ?

Are they always catastrophic?

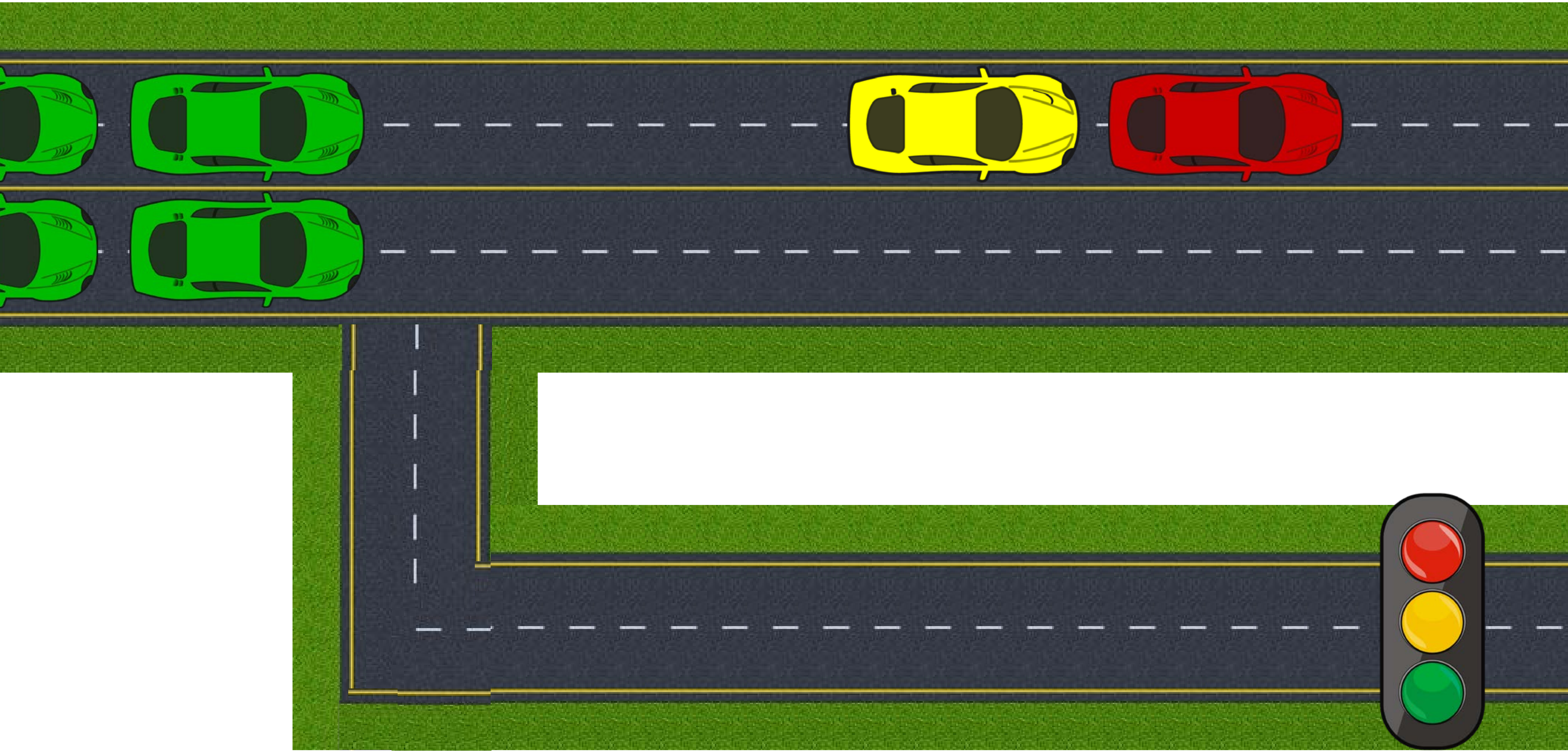
How many sensors a hacker need to attack

Message #2: Attacks on small sets of IoT sensors can lead to catastrophic consequences

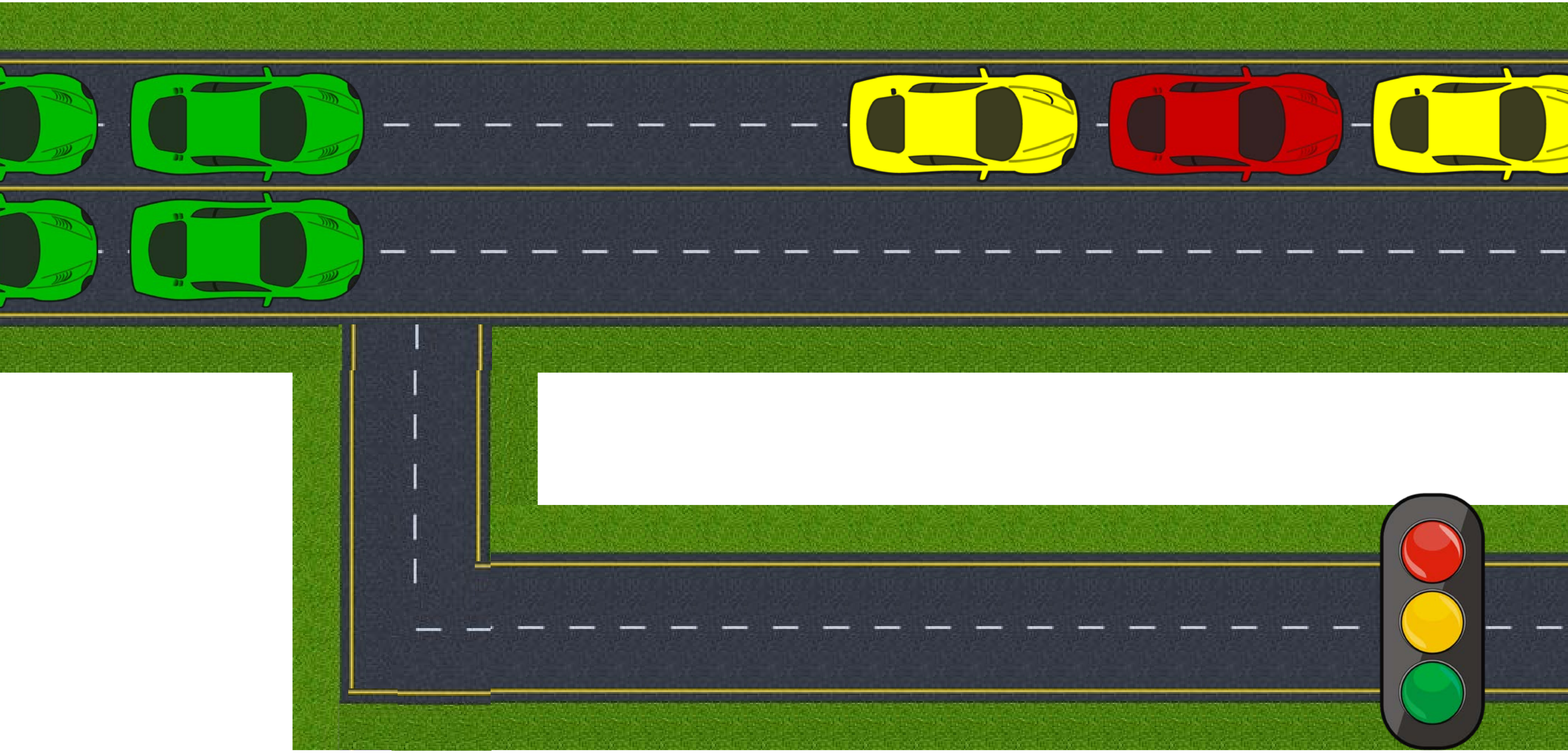
Smart Traffic System



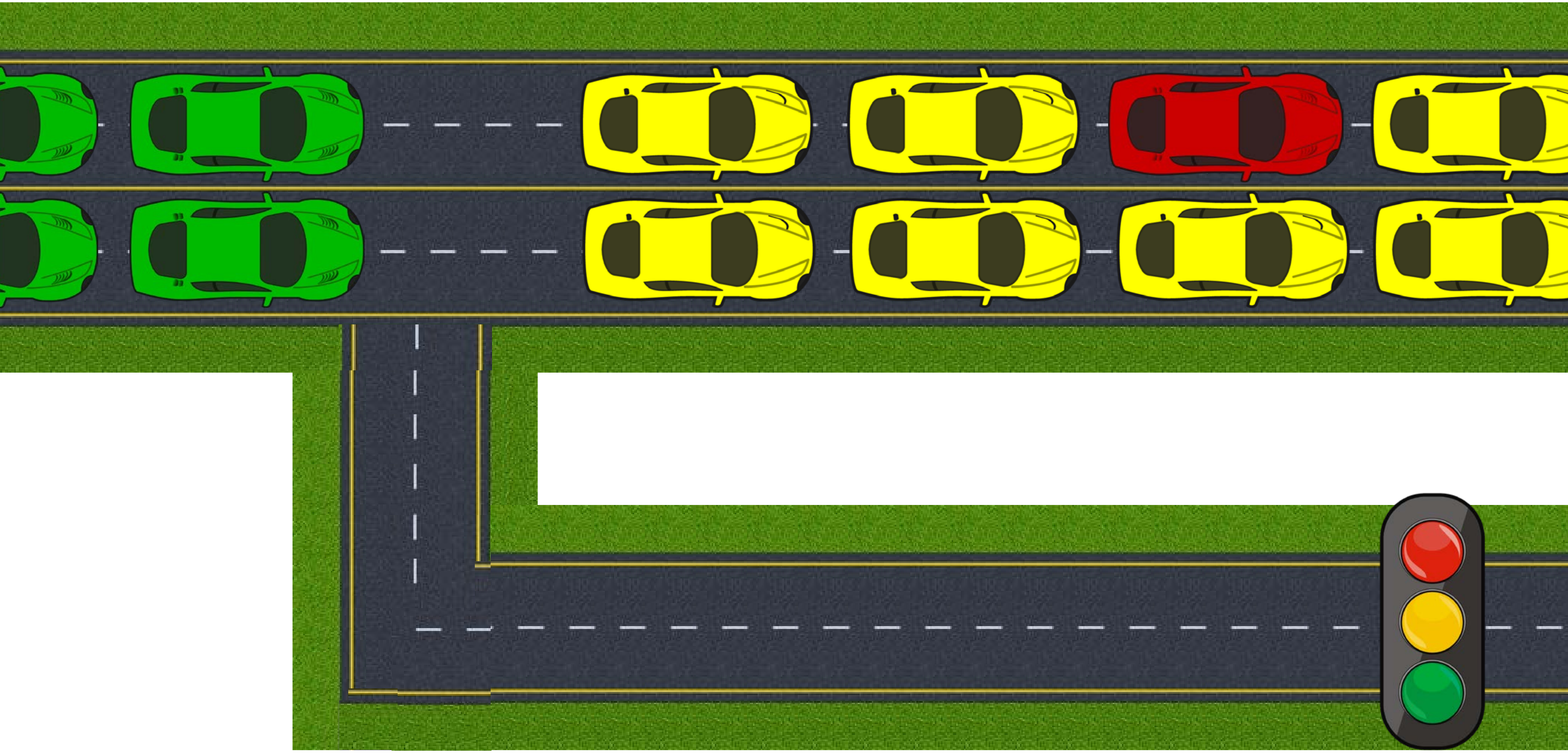
Smart Traffic System



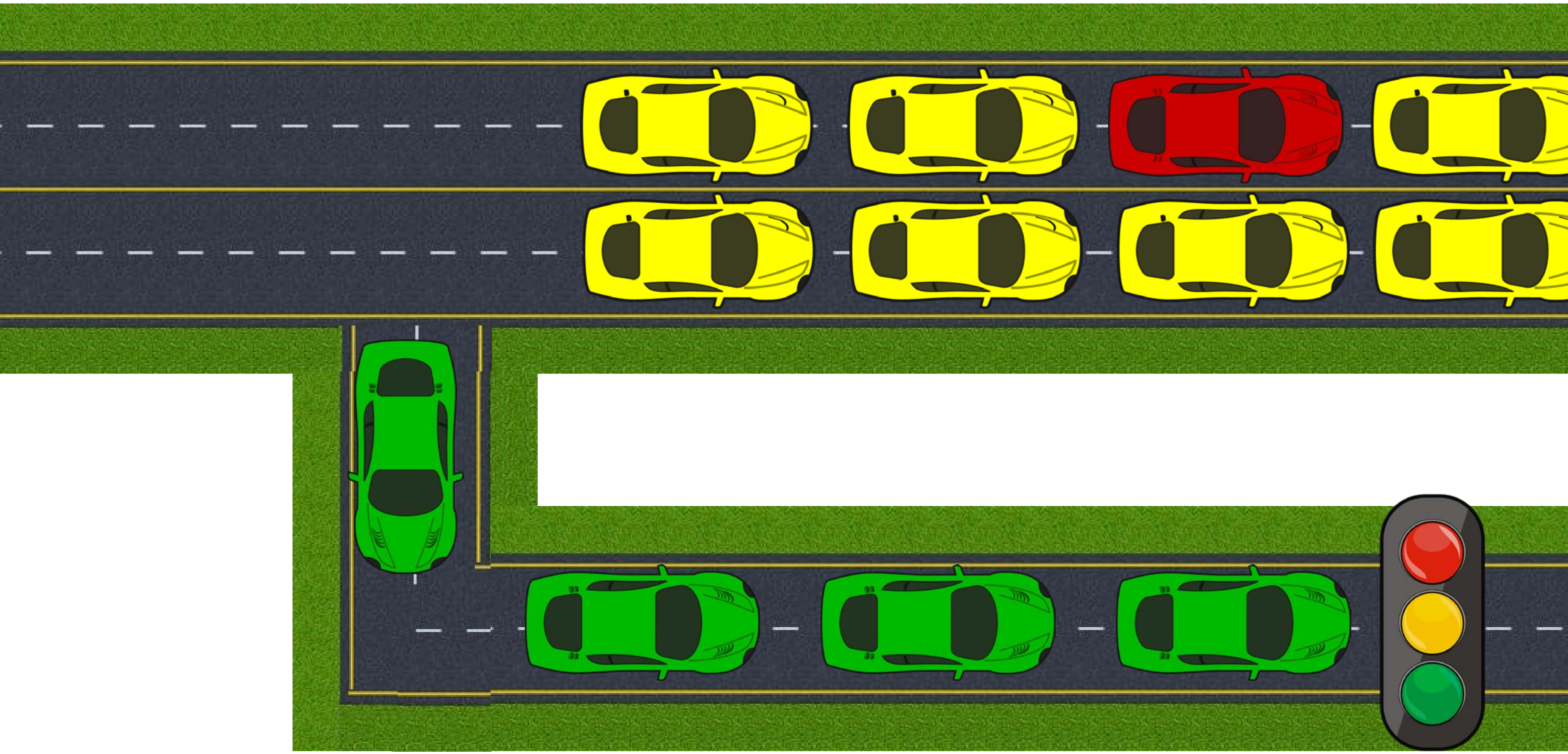
Smart Traffic System



Smart Traffic System

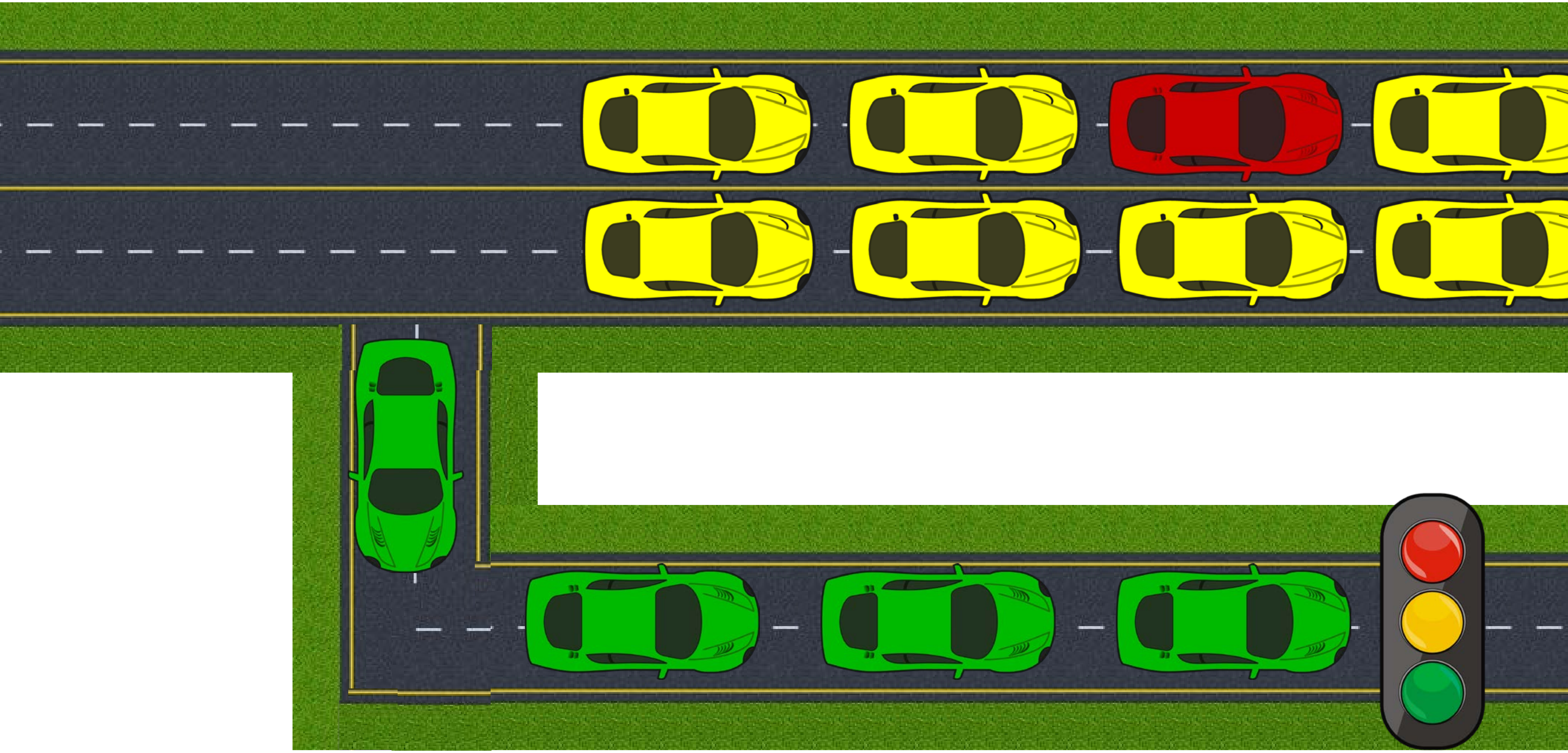


Smart Traffic System



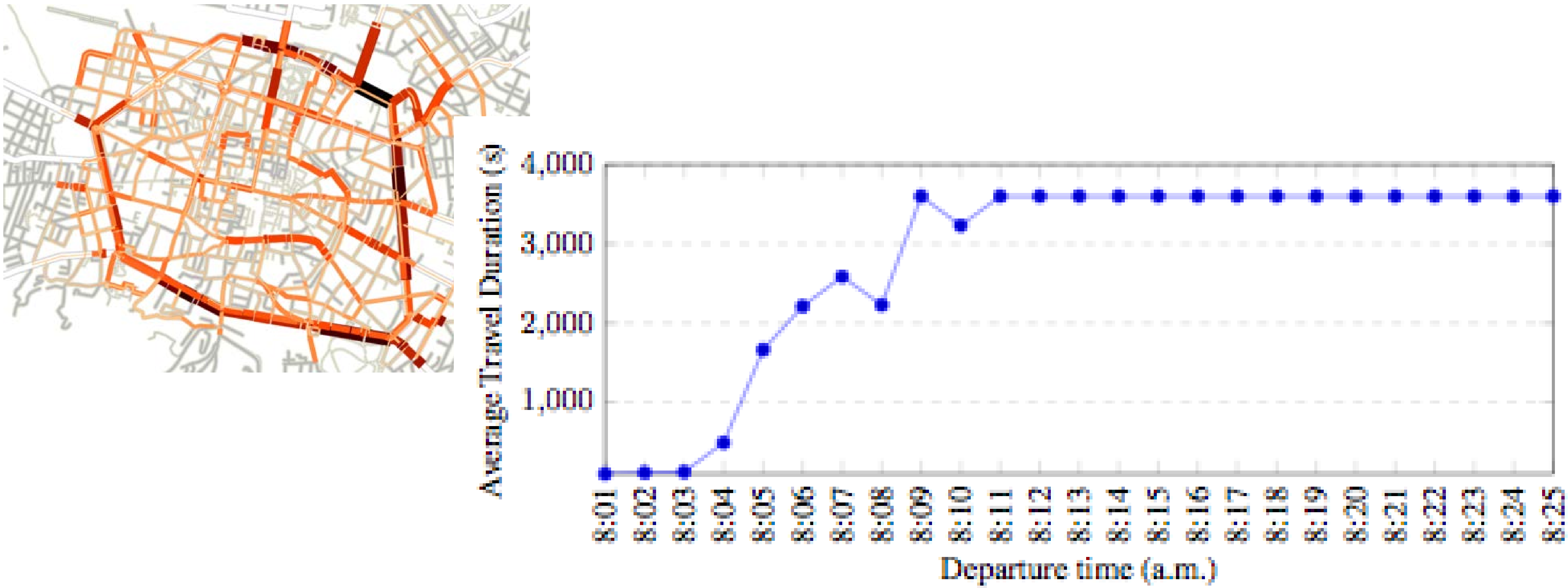
Smart Traffic System

One malicious car can disturb the whole system



Smart Traffic System

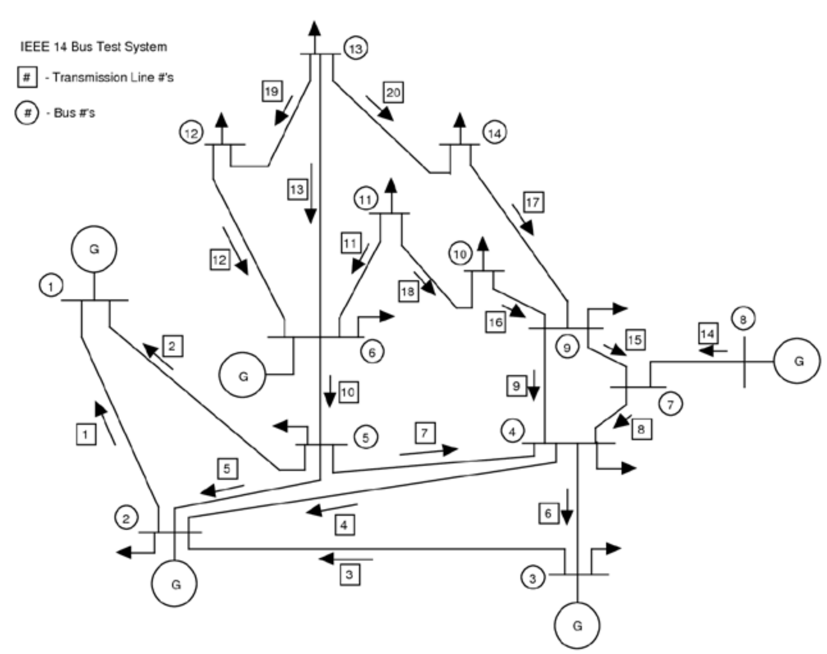
Simulation using traffic data sets and urban simulators (SUMO) supports the same conclusion



Without attacks, average travel time is 4 minute

GPS Spoofing Attacks: Power Grid

- Attacks on PMUs are “unobservable” by current anomaly detection units.
- Some PMUs are more critical than others.
- In certain scenarios, attacking one PMU is enough to destabilize portions of the grid

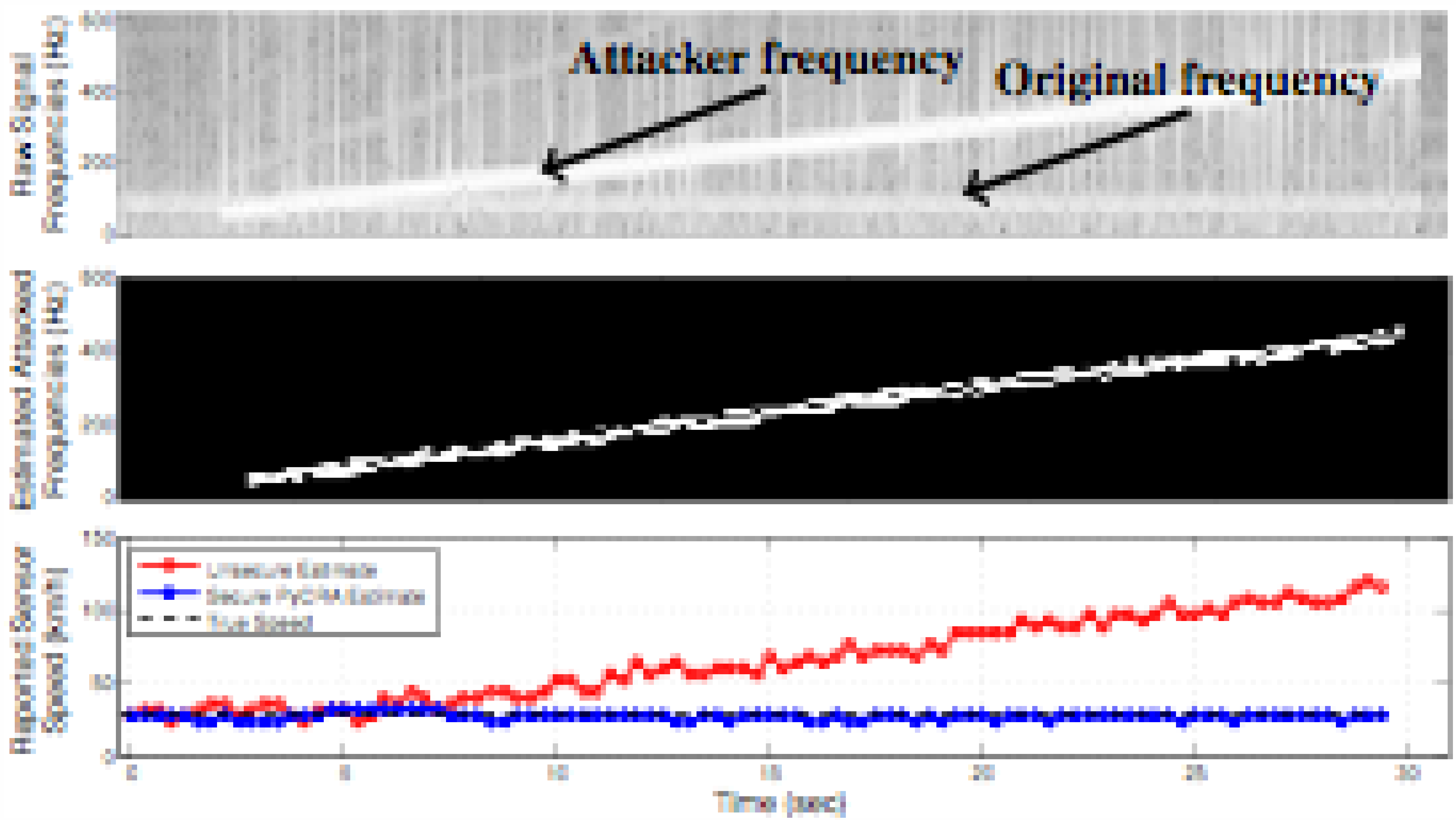


Physical Layer Countermeasures

Message #3: Hardening the physics of the sensors is hard but needed

Physical Authentication

Physical Authentication



Data Analytics Countermeasures

Message #4: Data analytics techniques that leverage heterogeneous redundancy in information seems a feasible solution

Resilient Data Analytics: Automotive

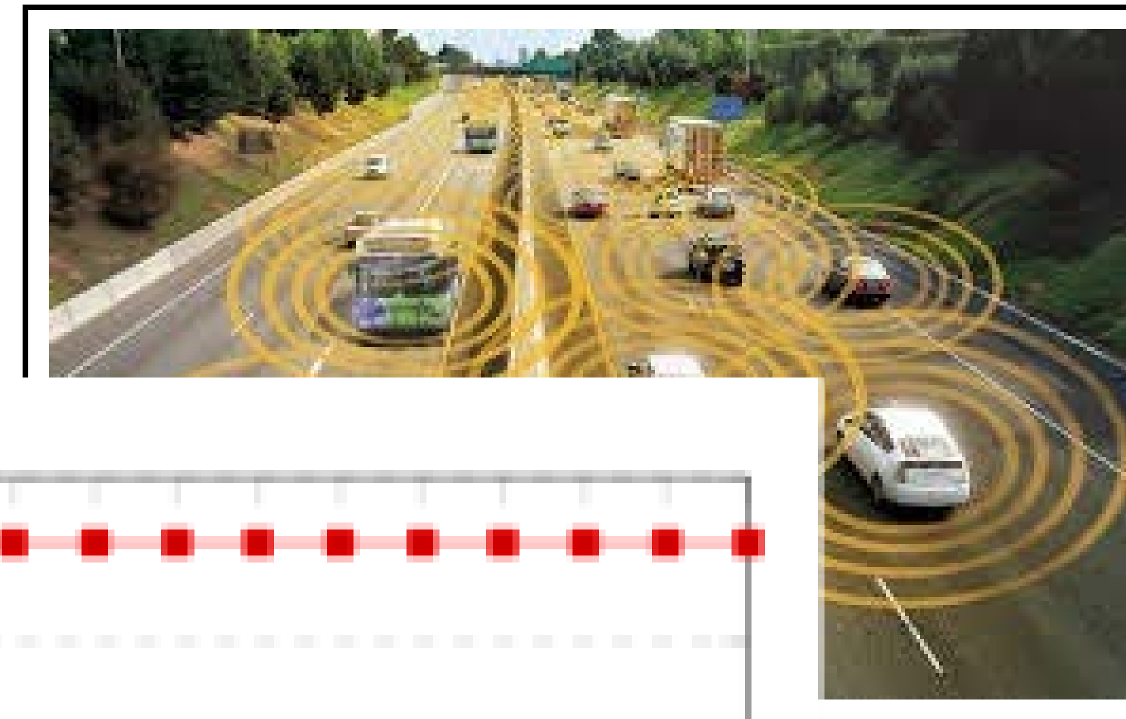
Miroslav Pajic (Duke)

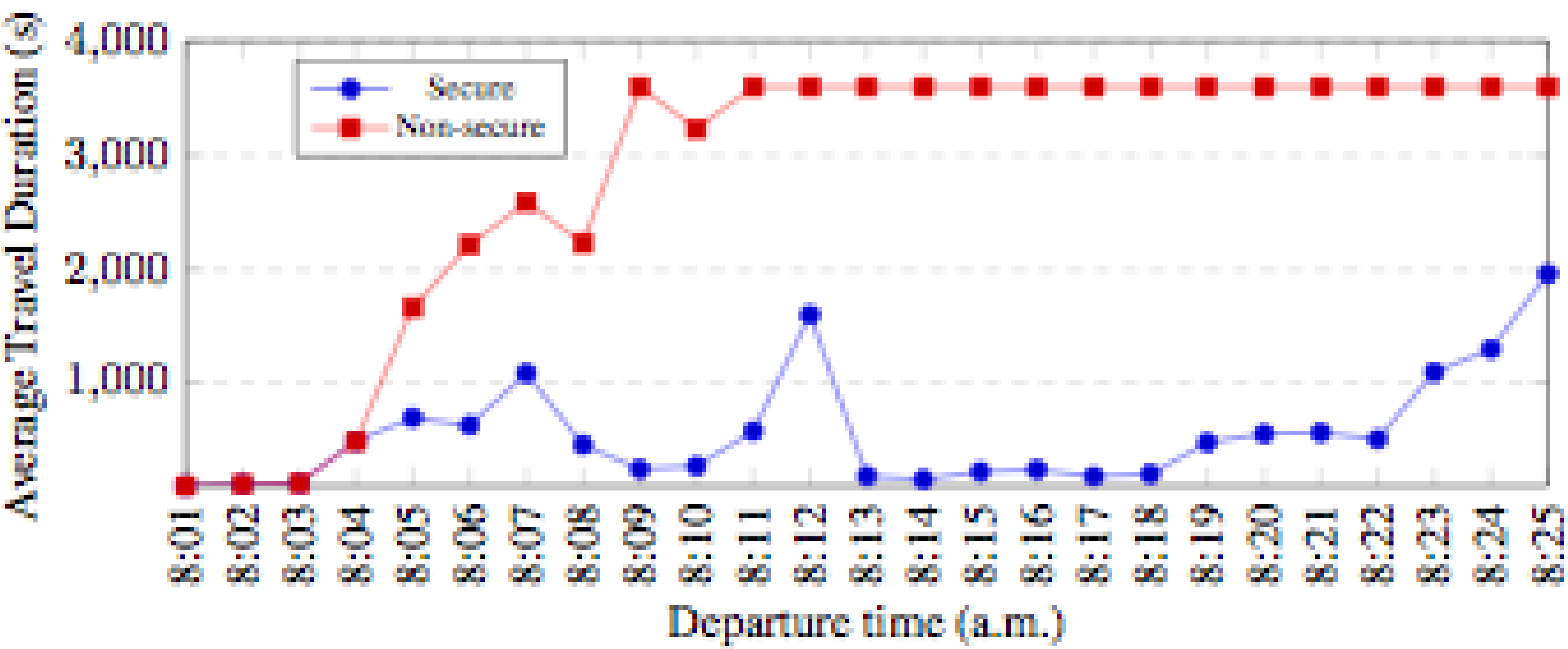
Nicola Bezzo (UVa)

Resilient Data Analytics: Quadrotors

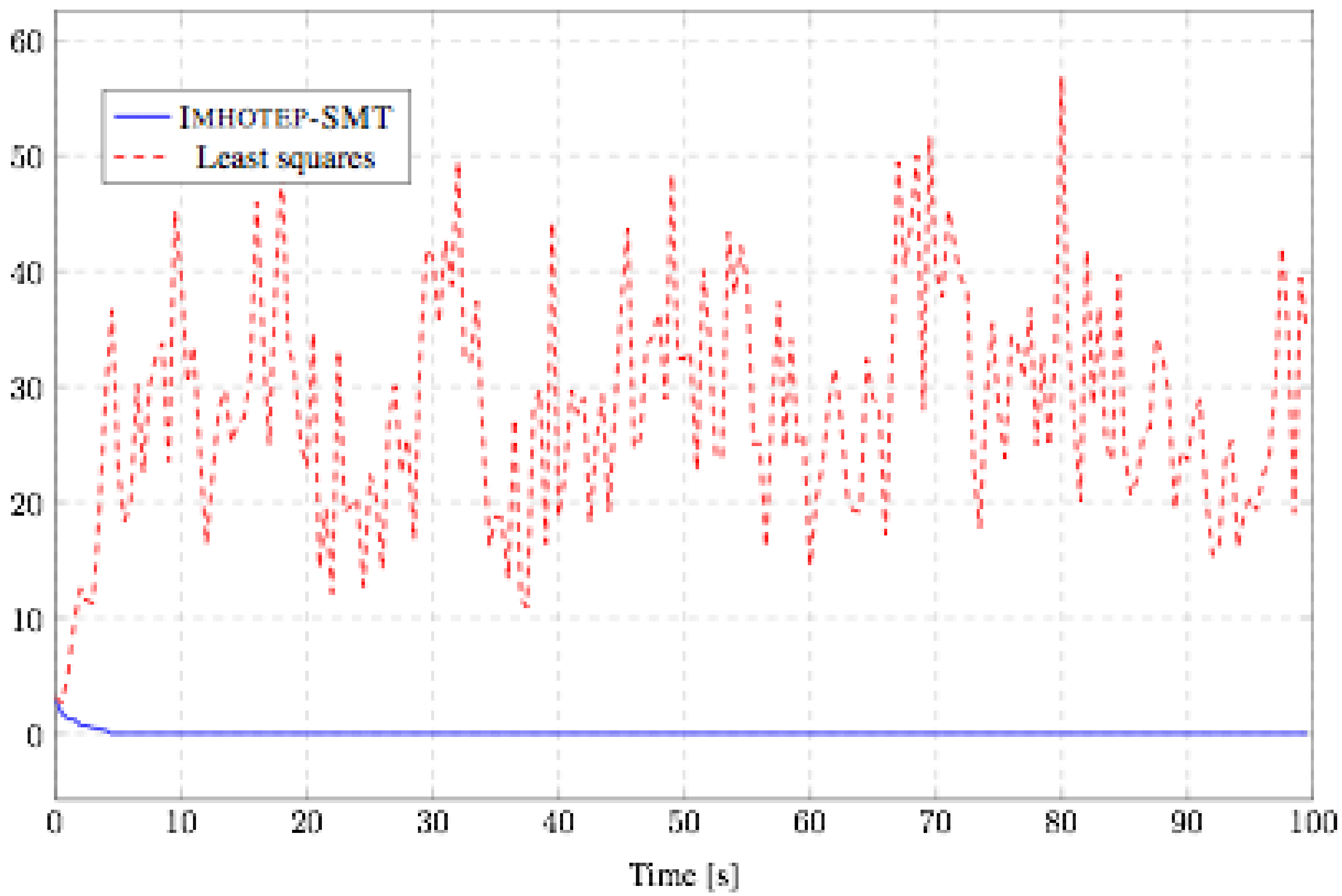
Resilient Data Analytics: Quadrotors

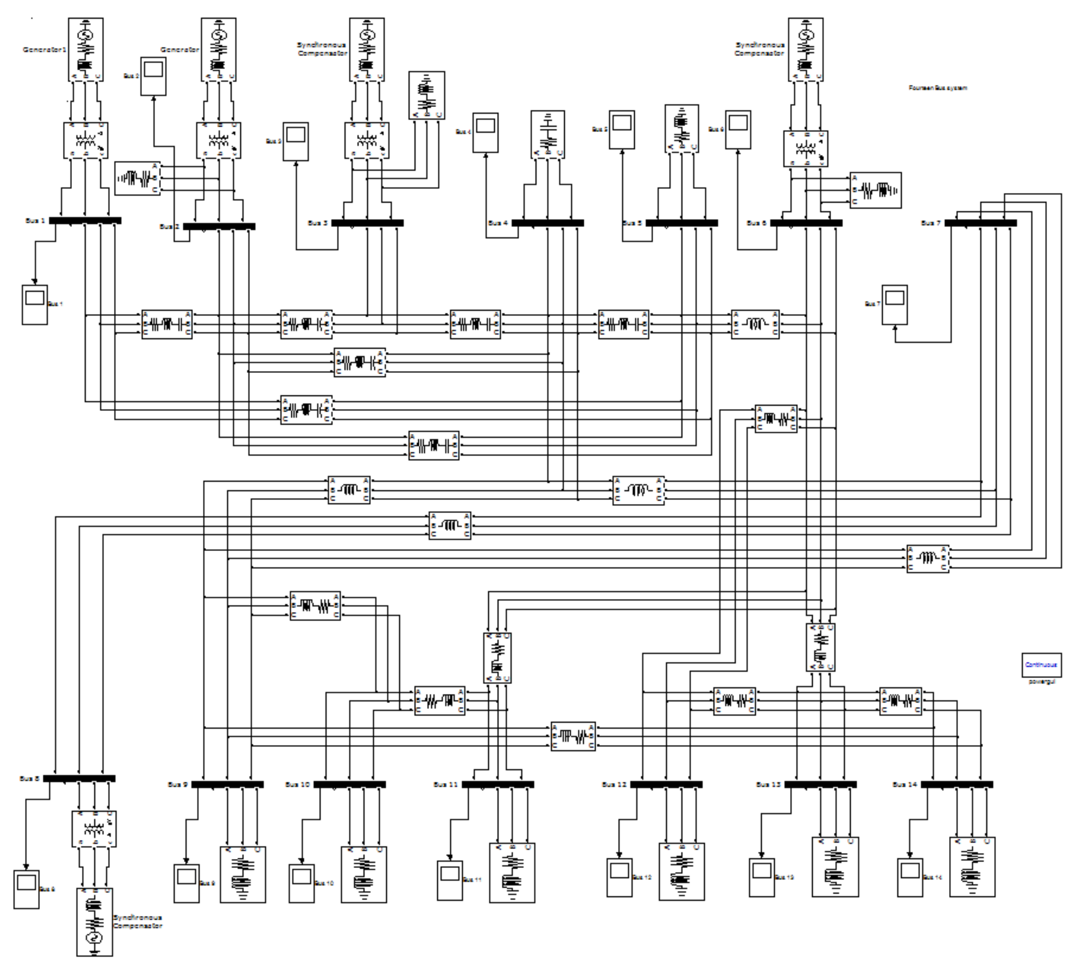
Resilient Data Analytics: Traffic Systems





Resilient Data Analytics: Power Systems



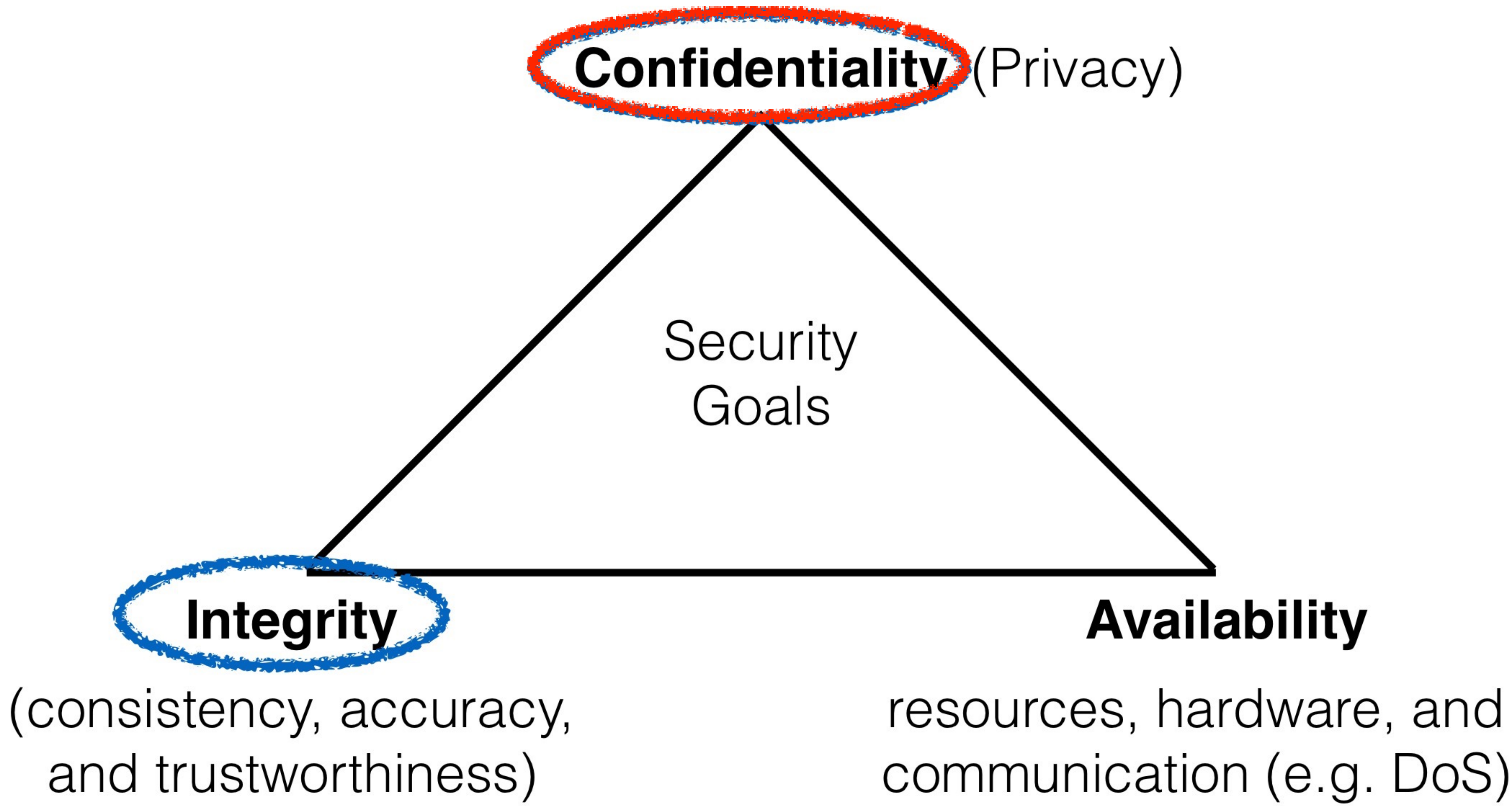


Message #4: Data analytics techniques that leverage heterogeneous redundancy in information seems a feasible solution but what about Big-data, how to handle massive amounts of data to find discrepancies?

Message #4: Data analytics techniques that leverage heterogeneous redundancy in information seems a feasible solution but what about Big-data, how to handle massive amounts of data to find discrepancies?

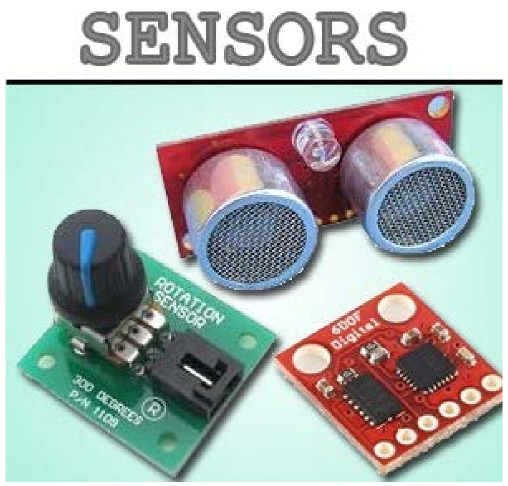
Open research problem!

CIA Security Triad



Message #5: Sensor information can be used to infer much more than what is expected

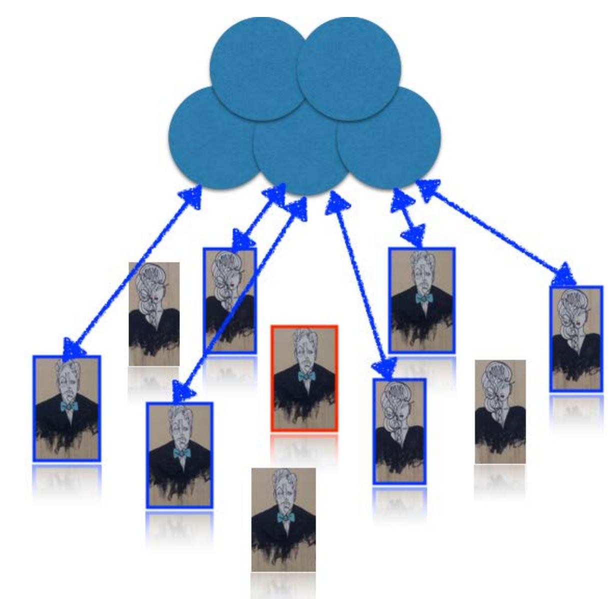
Sensor Privacy



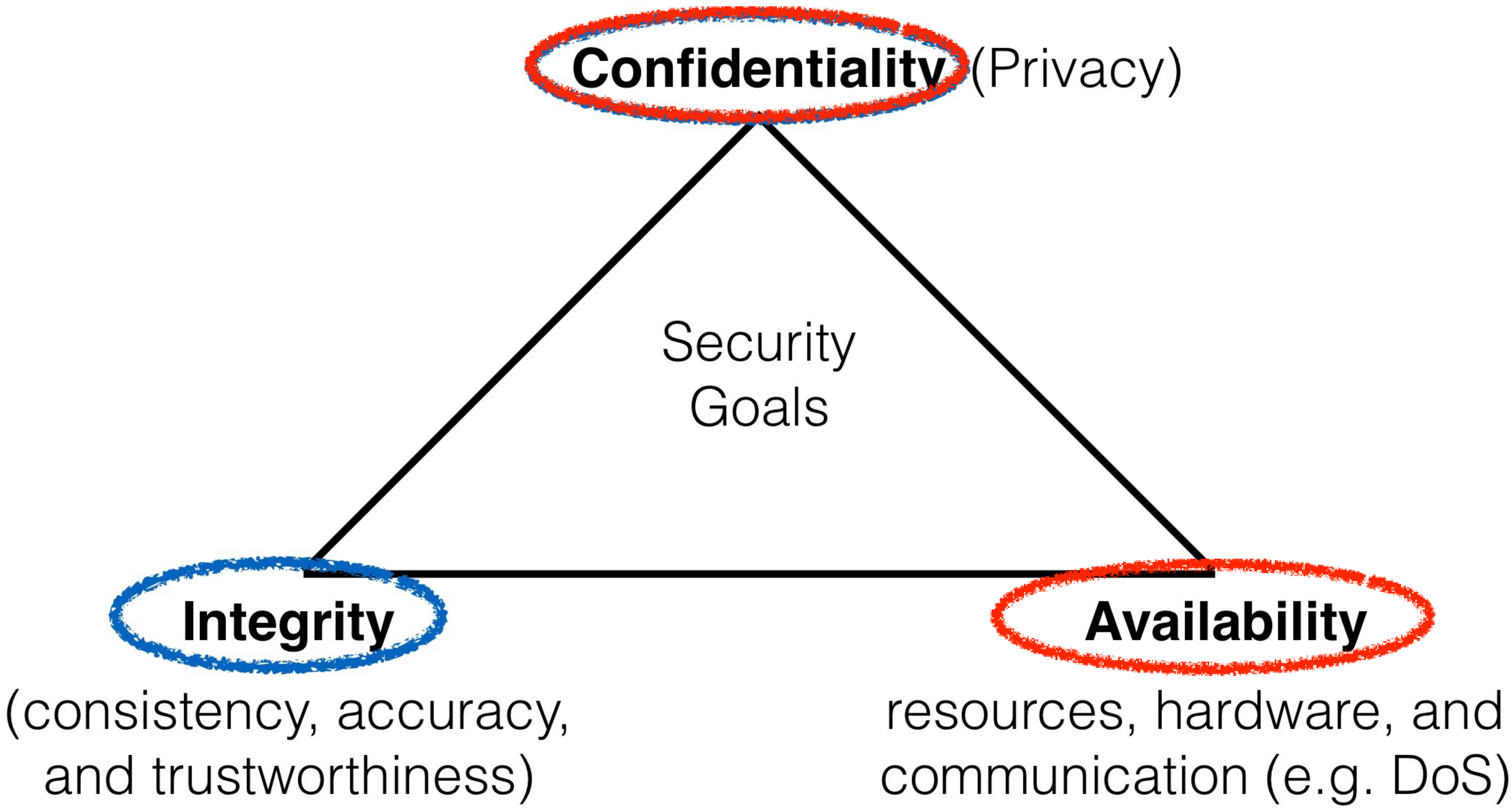
Smart meter	Electricity Usage	TV watching habits [Greveler11, Enev11]
Gyroscope (smart phones)	Orientation	Speech, Passwords [Michalevsky'15]
Barometer (smart phones)	Pressure	Location [Martin'15]
GPS	Location	Religion, health habits

Privacy-Aware Data Analytics

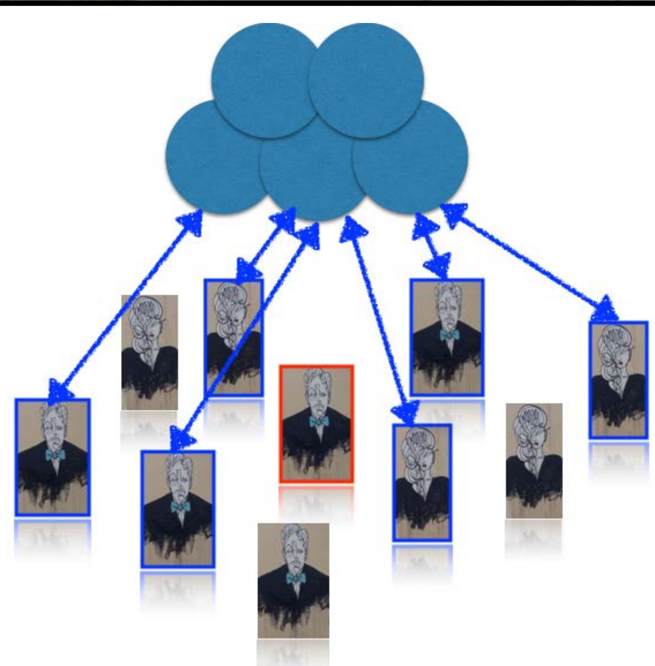
- Beyond cryptography (securing the communication channel is enough)
- Differential privacy is a technique that corrupts the data before sharing it with the cloud
- Not always the answer. In some scenarios ss.
    - Example: localization in smart cities.



CIA Security Triad



Message #6: DoS attacks on sensor information can be harmful as well



Summary

- Attacks on IoT sensors are feasible
- Attacks on small sets of IoT sensors can lead to catastrophic consequences
- Hardening the physics of the sensors is hard but needed
- Data analytics techniques that leverage heterogeneous redundancy in information seems a feasible solution
- Privacy-aware data analytics is also needed to solicit participation from users.