POLITECNICO
MILANO 1863

DIPARTIMENTO DI ELETTRONICA
INFORMAZIONE E BIOINGEGNERIA

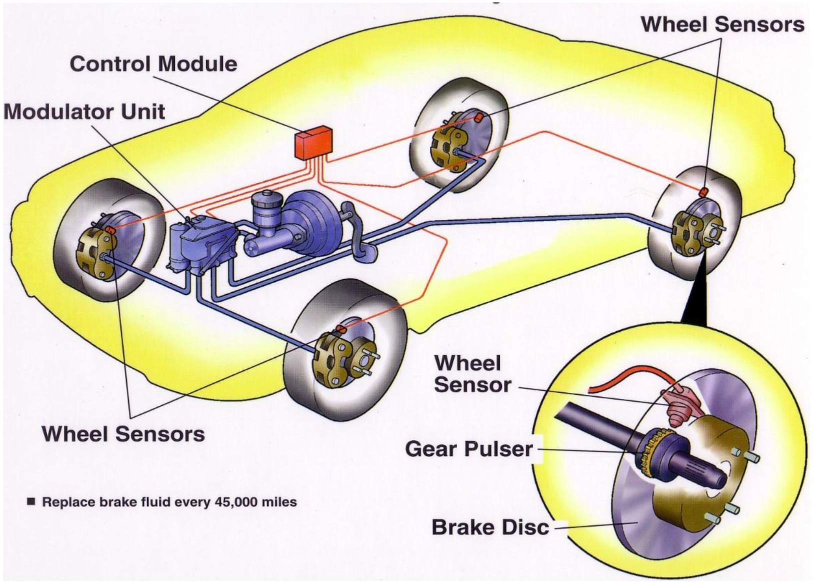
POLITECNICO MILANO 1863
NECST laboratory

Automotive Security

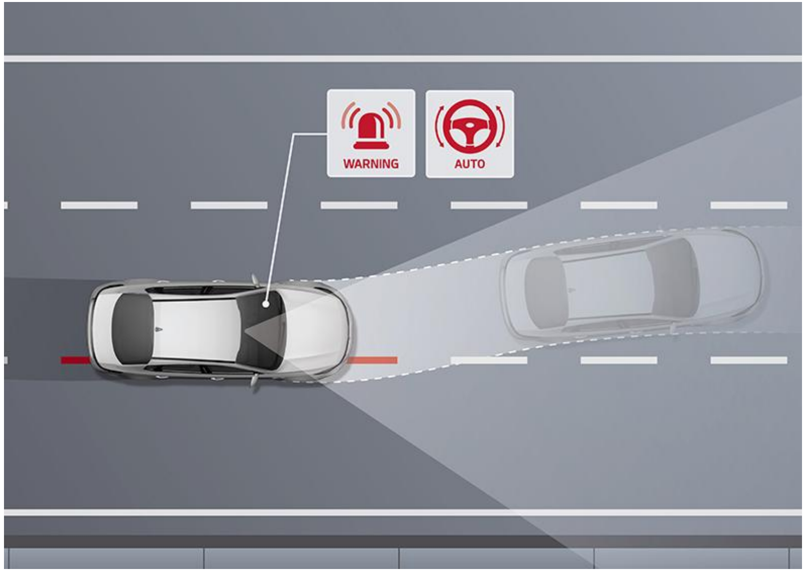
Automotive Development

What Developed? - Safety

ABS

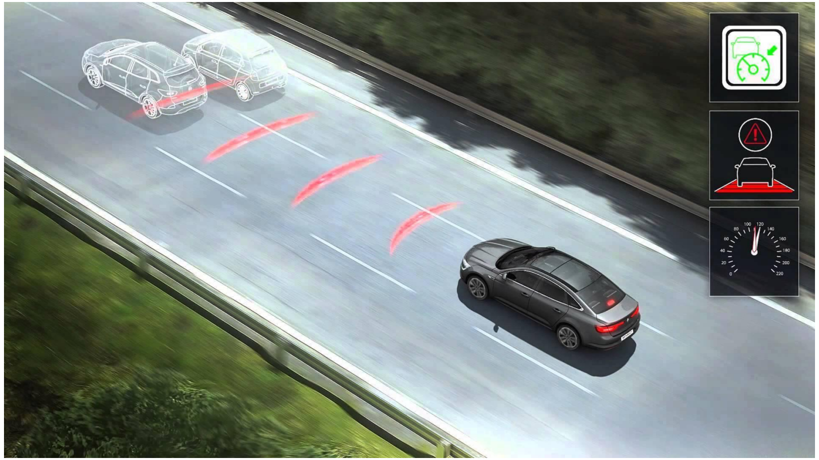


Lane Assist



What Developed? - Comfort

Cruise Control



Adjustable Settings

What Developed? - Communication

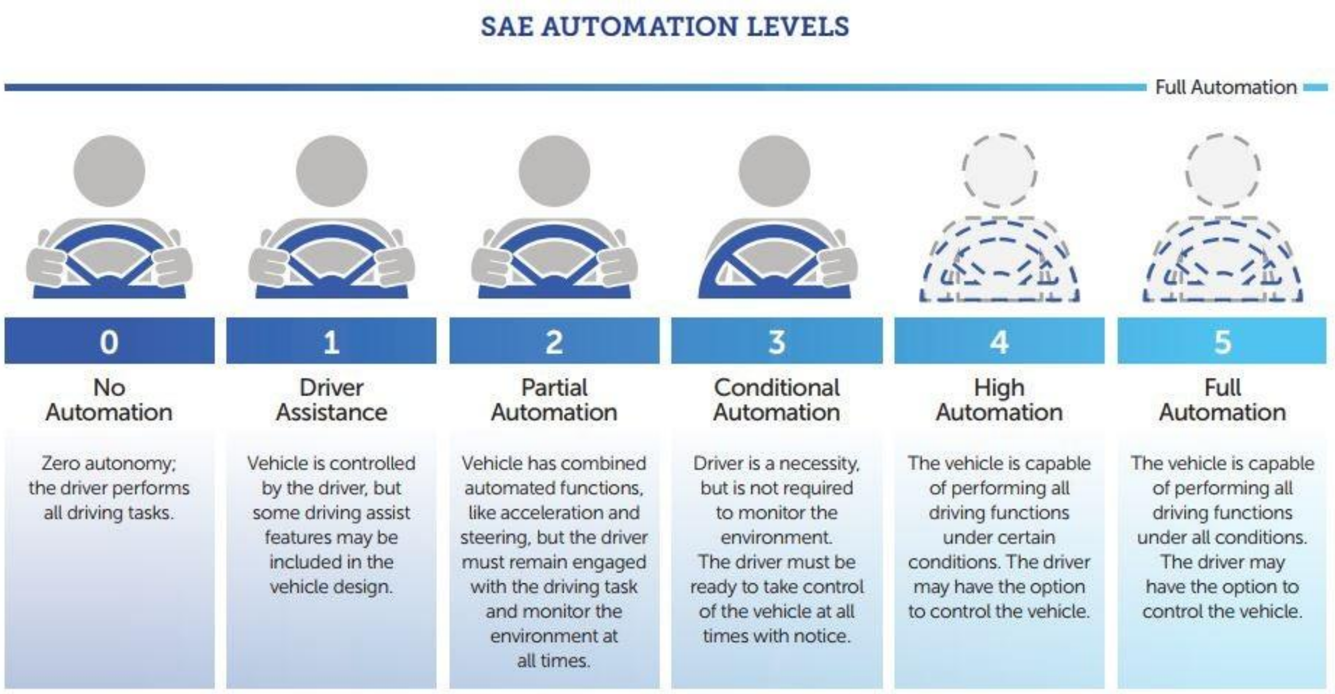
Local Communication

Remote Communication

DSRC

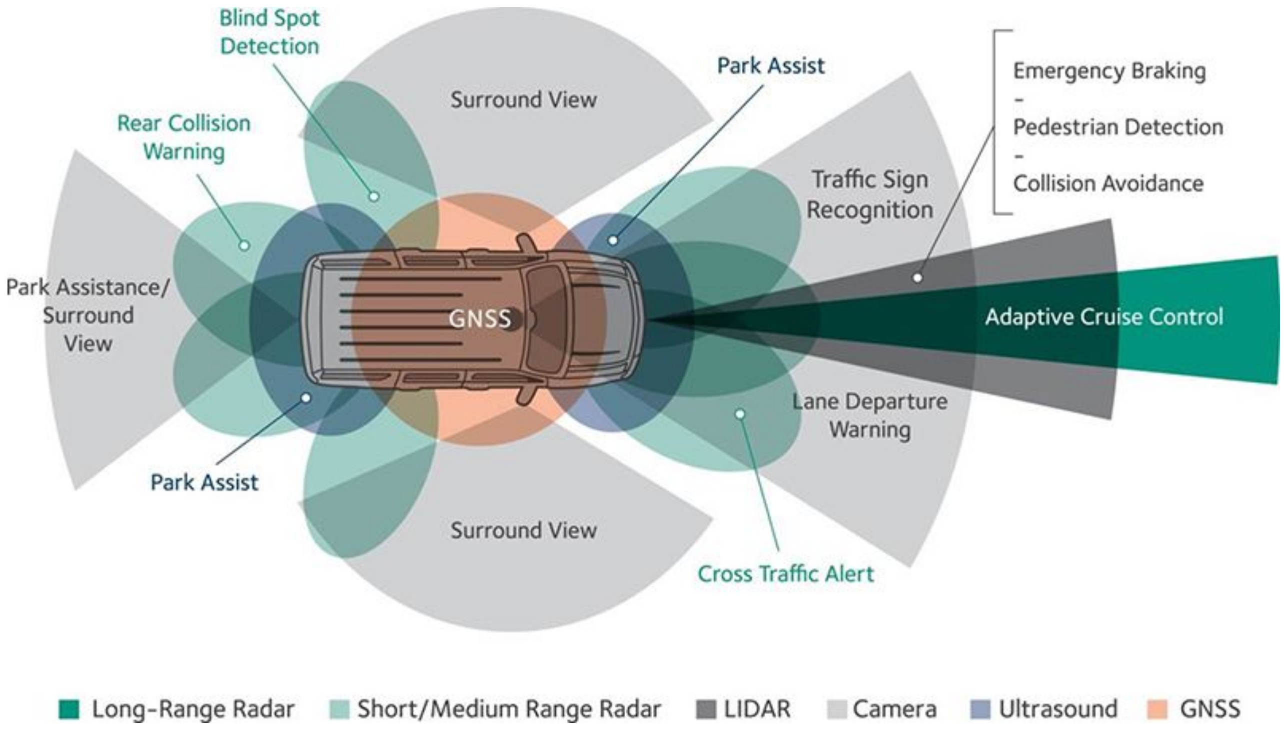
What Developed? - Aftermarket Devices

Future – Autonomous Driving



How? (1)

How? (1)

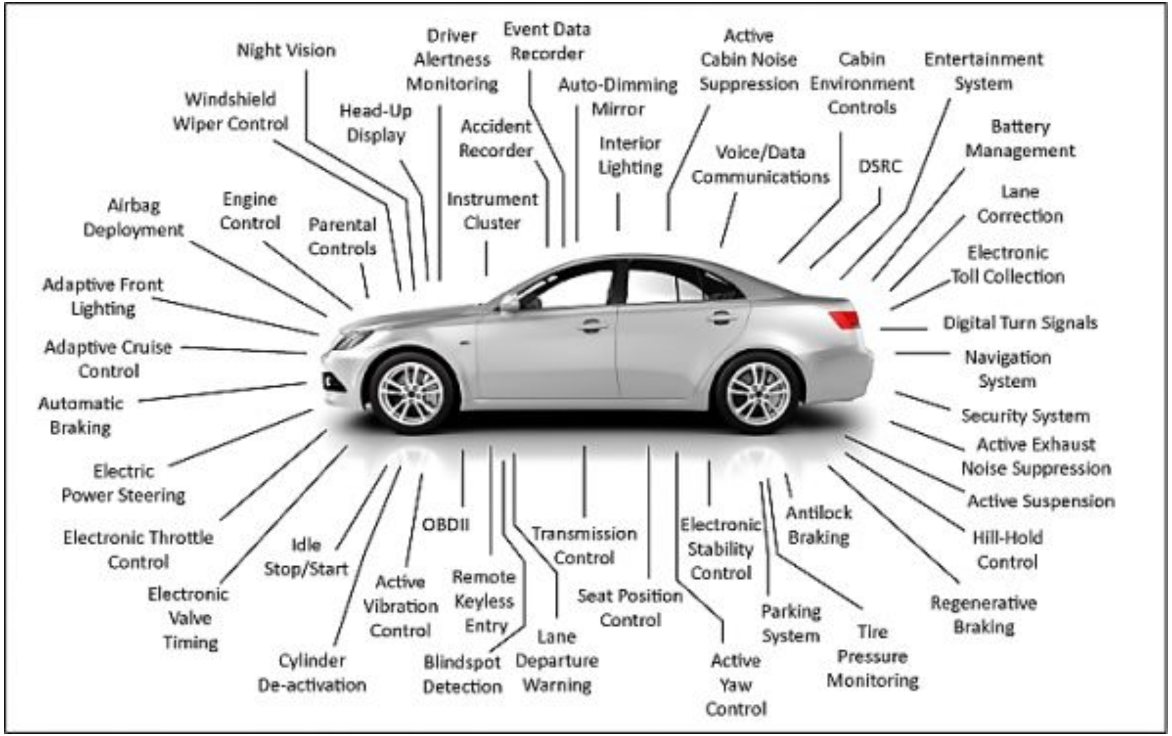


Blind Spot Detection
Surround View
Park Assist
Emergency Braking
-
Pedestrian Detection
-
Collision Avoidance
Rear Collision Warning
Traffic Sign Recognition
Park Assistance/ Surround View
GNSS
Adaptive Cruise Control
Lane Departure Warning
Park Assist
Surround View
Cross Traffic Alert
Long-Range Radar
Short/Medium Range Radar
LIDAR
Camera
Ultrasound
GNSS

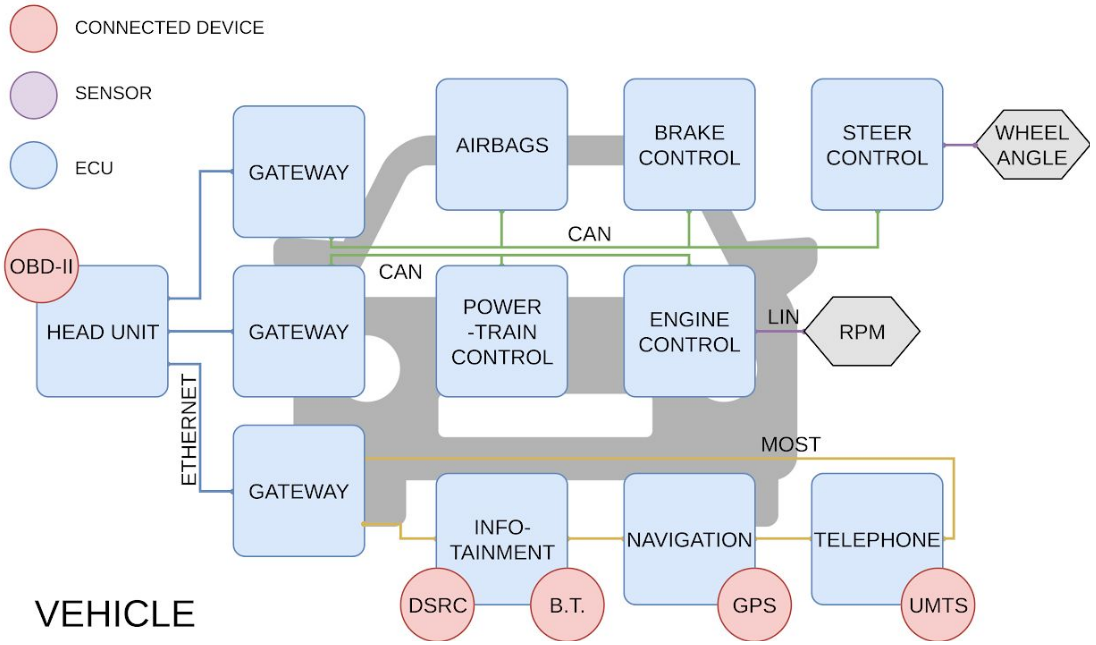
How? (2)


C-V2X
Intelligently connecting the car to surroundings and cloud
V2V
Vehicle-to-vehicle
e.g. collision avoidance safety systems
V2P
Vehicle-to-pedestrian
e.g. safety alerts to pedestrians, bicyclists
V2N
Vehicle-to-network
e.g. real-time traffic / routing, cloud services
V2I
Vehicle-to-infrastructure
e.g. traffic signal timing/priority

A LOT of Devices

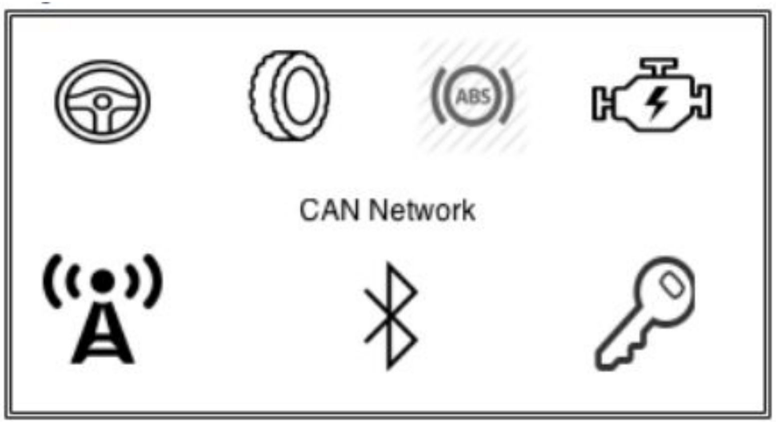


Structure of the vehicle

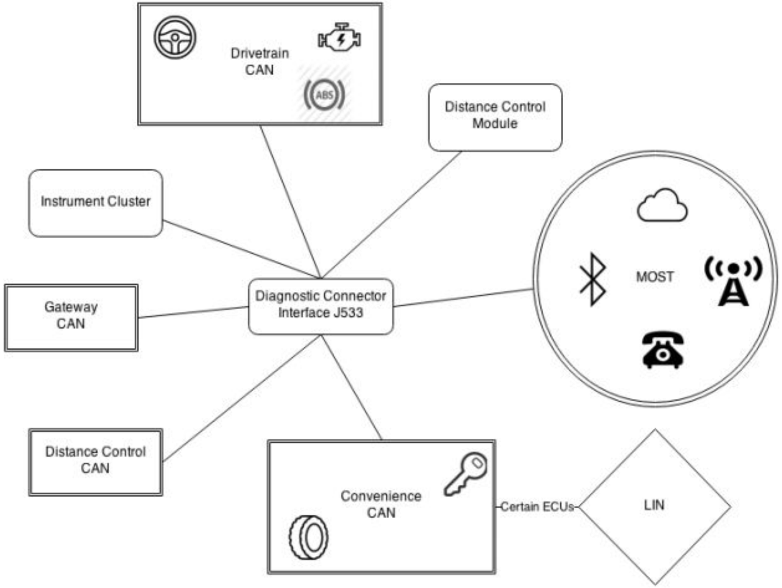


Structure of the vehicle

2010 Infiniti G37



2014 Audi A8



Subnetworks

CAN - Controller Area Network: Standard, Real-Time, Cheap

FlexRay: Expensive, Real-Time

MOST - Media Oriented System Network: High Bandwidth

LIN - Local Interconnect Network: Cheap, for sensors

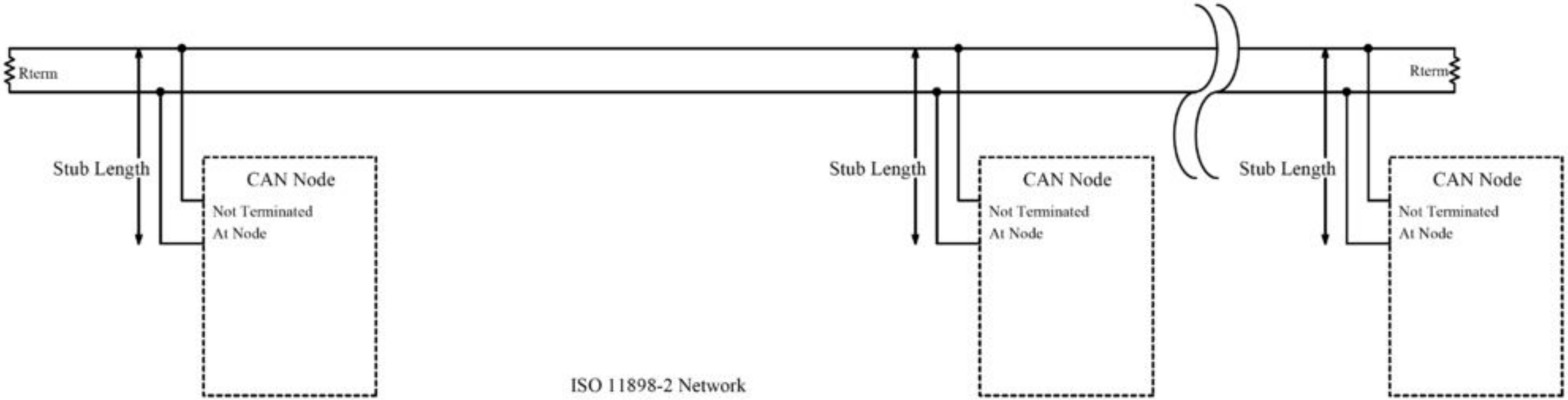
Automotive Ethernet: Higher layer communication

Controller Area Network

- Developed by Bosch in 1980’s
- Current de-facto standard
- Data Link and Physical layers
- Developed with focus on safety:
    - No issues with electromagnetic interferences
    - Broadcast nature
    - Arbitration focused on favouring most important messages

CAN

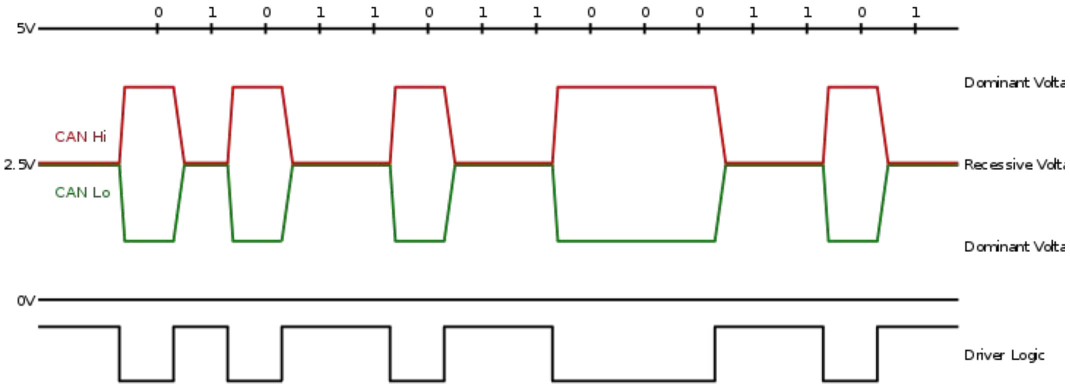
- Multi Master
- Broadcast
- Bus topology

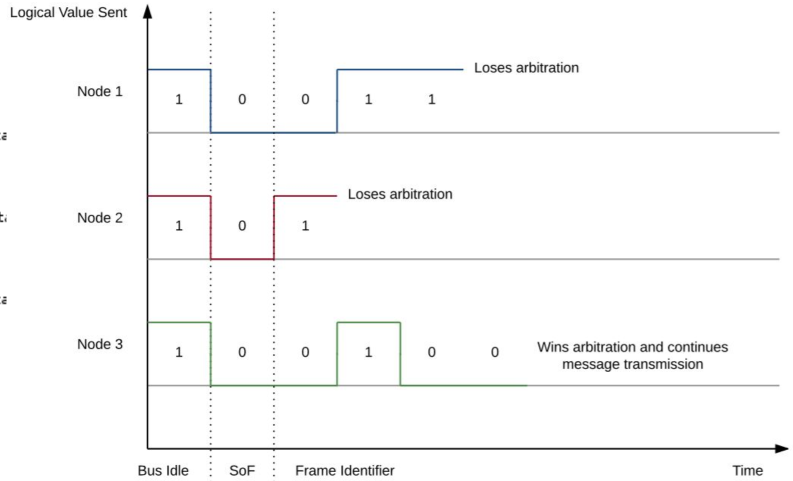


CAN

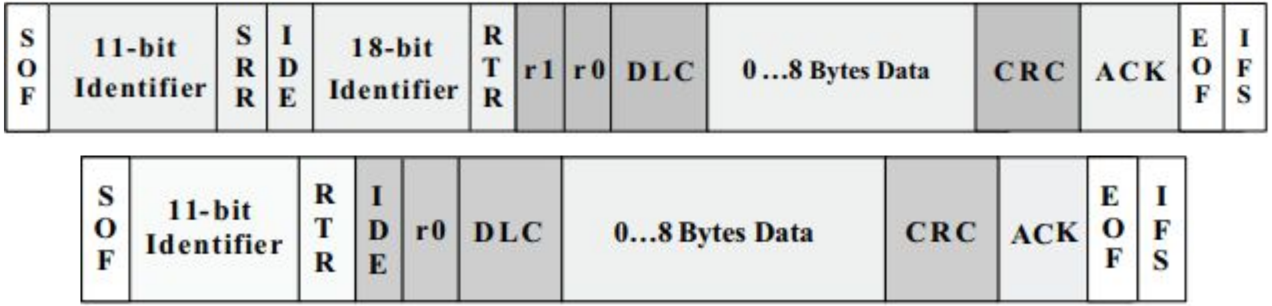
Physical layer: Differential signaling over two wires

Data Link Layer: CSMA/BA -> This enables Real-Time



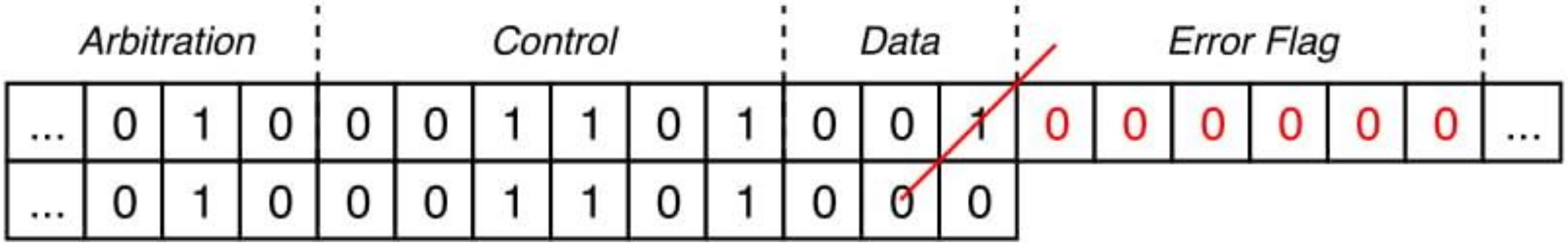


Data/Remote Frames



Meaning of Data Field and ID meanings are Proprietary for the most part

Error/Overload Frames



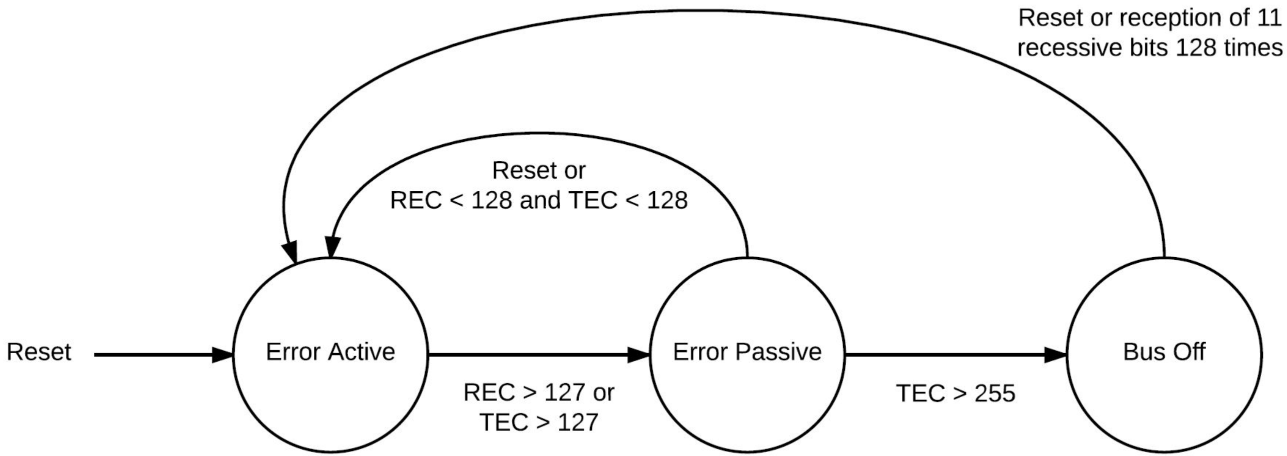
Error Handling:

Bit, Stuff, CRC, Form or Acknowledgment Errors are possible

Fault Confinement:

- Units can be in Error Active, Error Passive or Bus Off state
- Two Error Counters, Transmit and Receive
- Error Counter increases by 8 every time an error occurs
- When Transmit counter reaches 128 the unit goes into Error Passive state
- When it reaches 256 the units shuts down the CAN controller

Error Handling: Fault Confinement



OBD-II (On Board Diagnostics)

Mandatory in many countries, almost always present

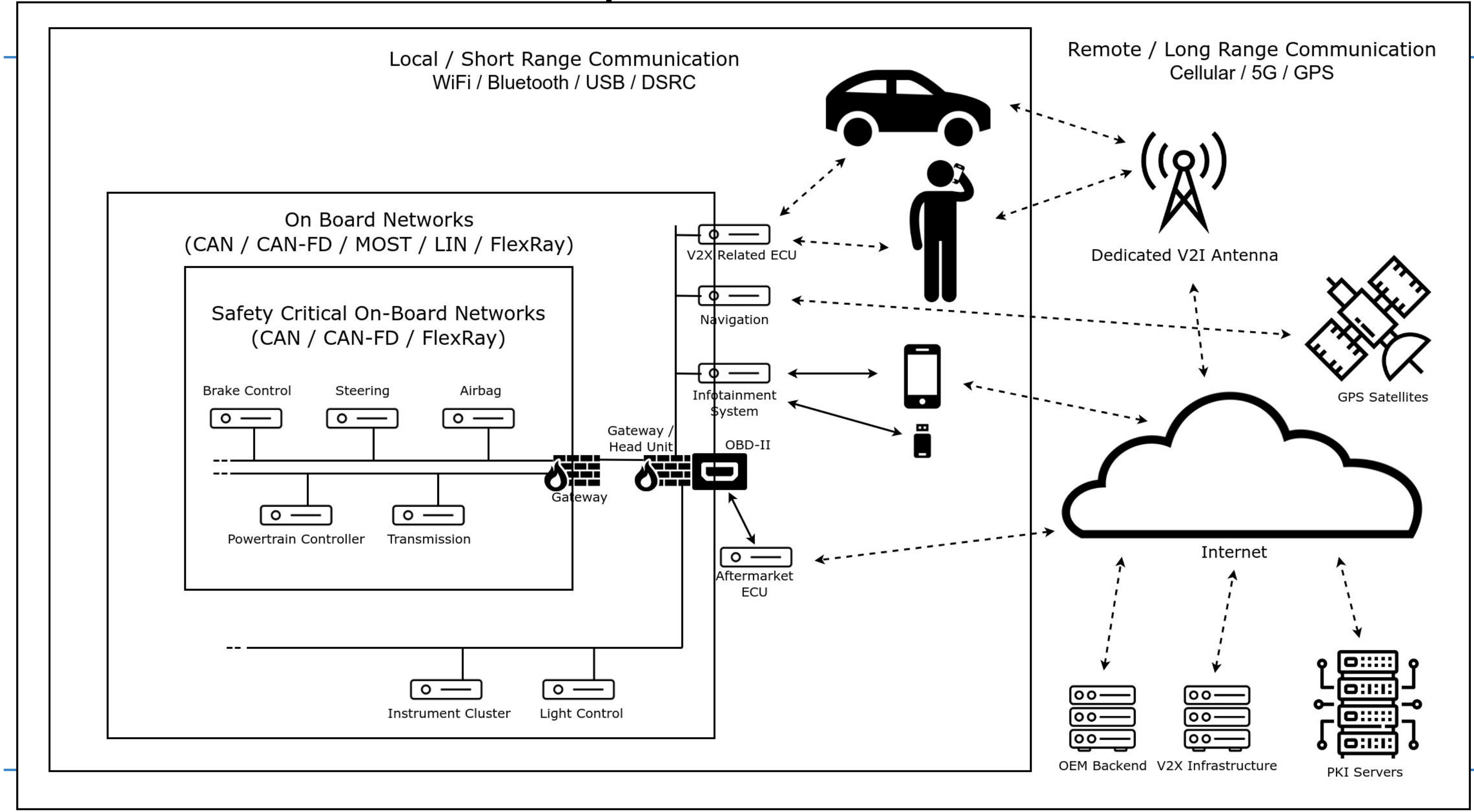
System to enable reporting and self-diagnostics of the whole network

OBD-II PIDs

Codes used to request data from the various Units

00	0	4	PIDs supported [01 - 20]				Bit encoded [A7..D0] == [PID $01..PID $20] See below
01	1	4	Monitor status since DTCs cleared. (Includes malfunction indicator lamp (MIL) status and number of DTCs.)				Bit encoded. See below
02	2	2	Freeze DTC				
03	3	2	Fuel system status				Bit encoded. See below
04	4	1	Calculated engine load	0	100	%	$\frac{100}{255}A$ (or $\frac{A}{2.55}$)
05	5	1	Engine coolant temperature	-40	215	°C	$A-40$
06	6	1	Short term fuel trim—Bank 1	-100 (Reduce Fuel: Too Rich)	99.2 (Add Fuel: Too Lean)	%	$\frac{100}{128}A-100$ (or $\frac{A}{1.28}-100$)
07	7	1	Long term fuel trim—Bank 1				
08	8	1	Short term fuel trim—Bank 2				
09	9	1	Long term fuel trim—Bank 2				
0A	10	1	Fuel pressure (gauge pressure)	0	765	kPa	$3A$
0B	11	1	Intake manifold absolute pressure	0	255	kPa	A
0C	12	2	Engine RPM	0	16,383.75	rpm	$\frac{256A+B}{4}$
0D	13	1	Vehicle speed	0	255	km/h	A
0E	14	1	Timing advance	-64	63.5	° before TDC	$\frac{A}{2}-64$
0F	15	1	Intake air temperature	-40	215	°C	$A-40$
10	16	2	MAF air flow rate	0	655.35	grams/sec	$\frac{256A+B}{100}$
11	17	1	Throttle position	0	100	%	$\frac{100}{255}A$

Complete Overview



Security, at last… Some History

Hoppe et al. - 2008 - Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study

- Connect wirelessly to the tpms system
- Reverse engineer the data
- Spoof tpms messages

Some History

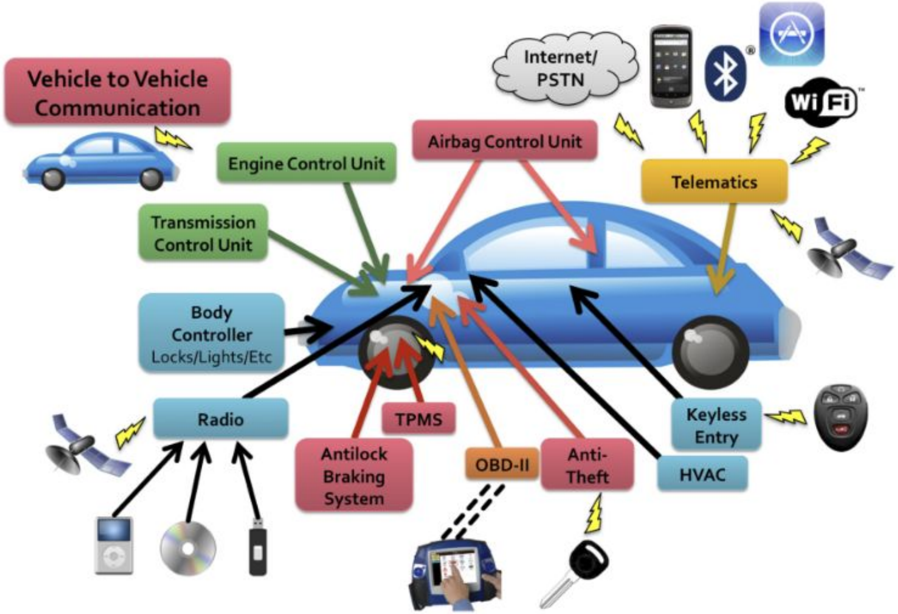
Koscher et al. - 2010 - Experimental Security Analysis of a Modern Automobile

- Connect physically to the internal networks
- Reverse engineer the IDs
- Study the possibilities:
  - DoS
  - Lock brakes
  - Stop engine
  - Modify panel cluster

Some History

Checkoway et al. - 2011 - Comprehensive Experimental Analyses of Automotive Attack Surfaces

- Detect all attack surfaces available
- Analyze some to understand the functioning
- Exploit and re-flash the firewall of some



Some History

Miller & Valasek - 2013 - Adventures in Automotive Networks and Control Units

- In depth study of possibilities through physical connection

Some History

Miller & Valasek - 2015 - Remote Exploitation of an Unaltered Passenger Vehicle

- First completely remote attack to a real world vehicle

Some History

KeenLab - 2016/18 - Security Analysis of a Tesla S / Security Analysis of a BMW

Automotive Risks

- Safety
- Privacy
- Financial
- Functional

Attack Goals

C.I.A. Triad

- Confidentiality
- Integrity
- Availability

Confidentiality

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Integrity

Data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle.This means that data cannot be modified in an unauthorized or undetected manner.

Availability

For any information system to serve its purpose, the information must be available when it is needed.

Attack Goals

- Confidentiality -> Sniffing
- Integrity -> Spoofing
- Availability -> Denial of Service

Sniffing

“Eavesdrop” conversations/data moving through a channel

e.g., MITM

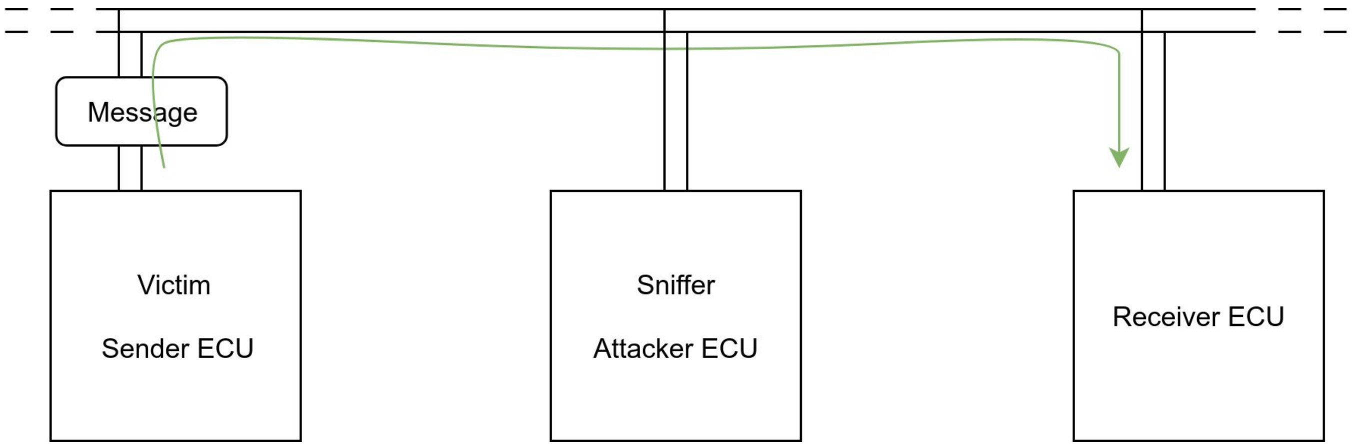
Spoofing

A spoofing attack is a situation in which a person or program successfully masquerades as another by falsifying data, to gain an illegitimate advantage

Denial of Service

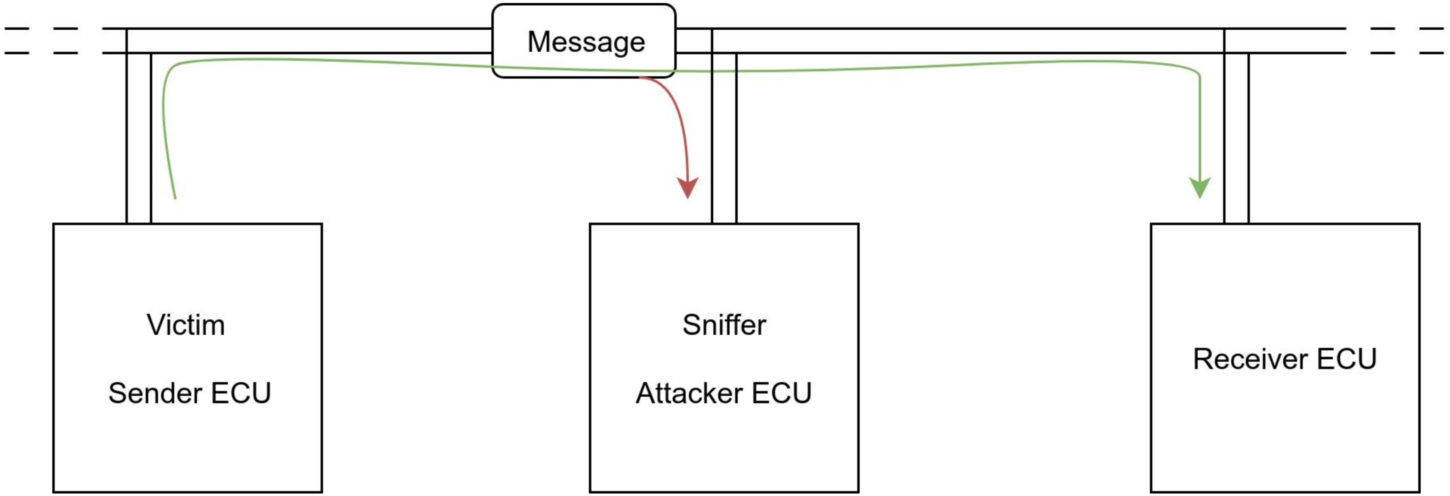
A denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the network.

Automotive CAN Attacks - Sniffing



Automotive CAN Attacks - Sniffing

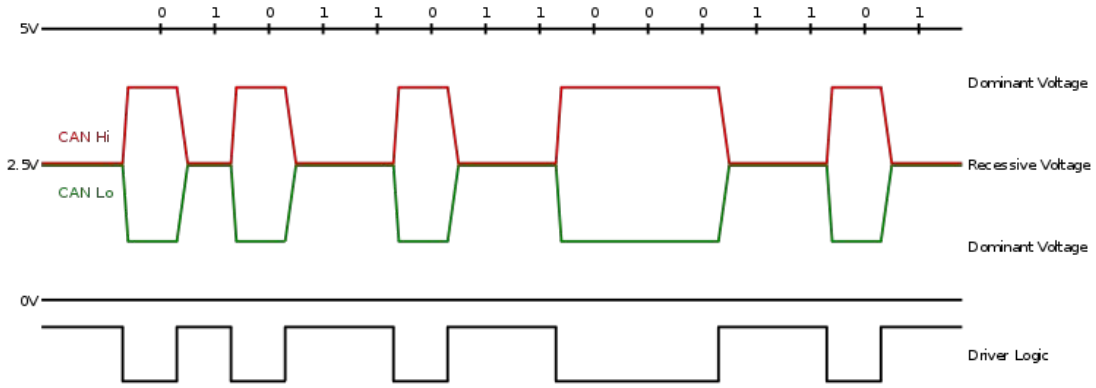
Extremely Hard to detect, but also kinda useless



Automotive CAN Attacks - DoS

Recessive is deleted by Dominant Bit

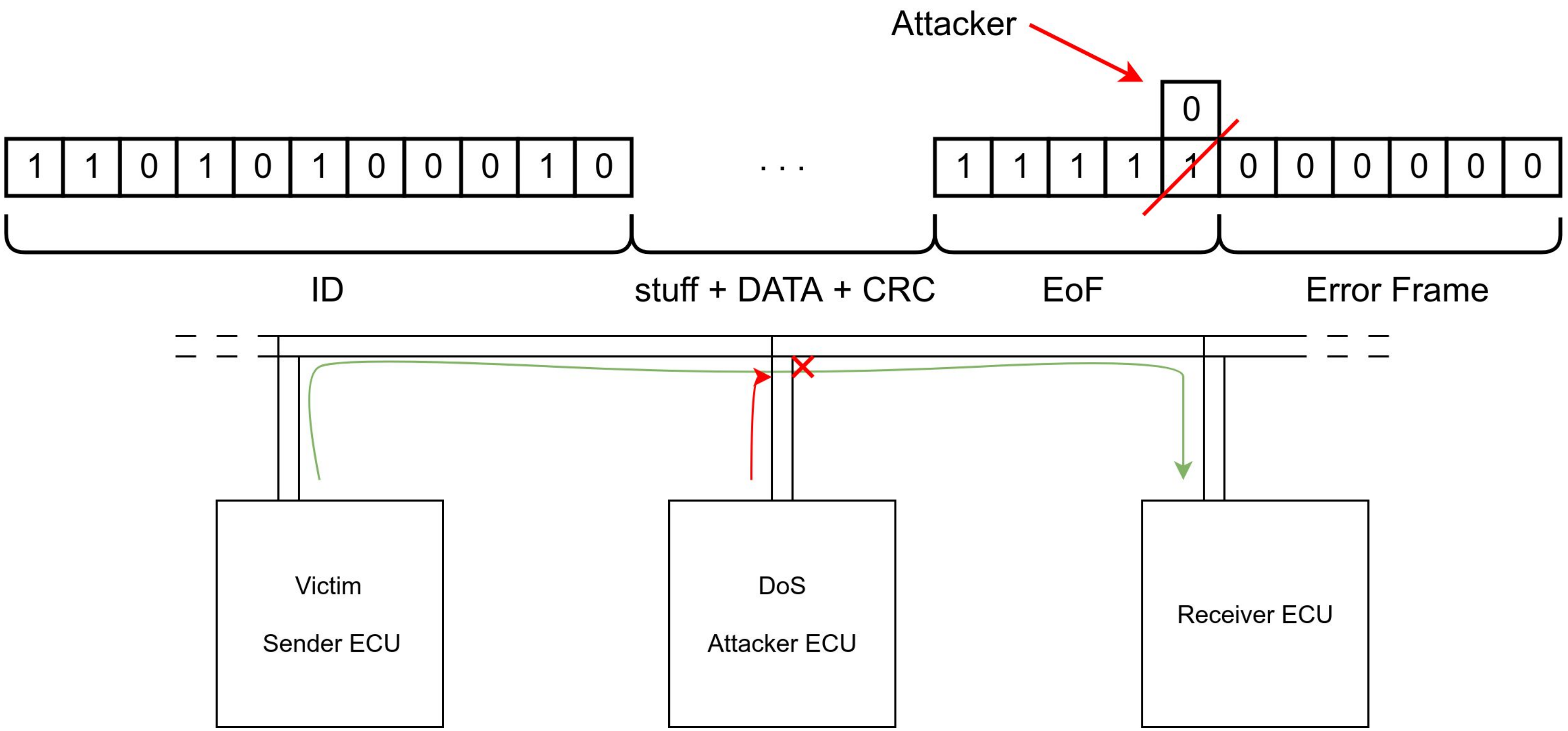
CSMA/BA property: An attacker can ALWAYS win arbitration



Automotive CAN Attacks - Targeted DoS

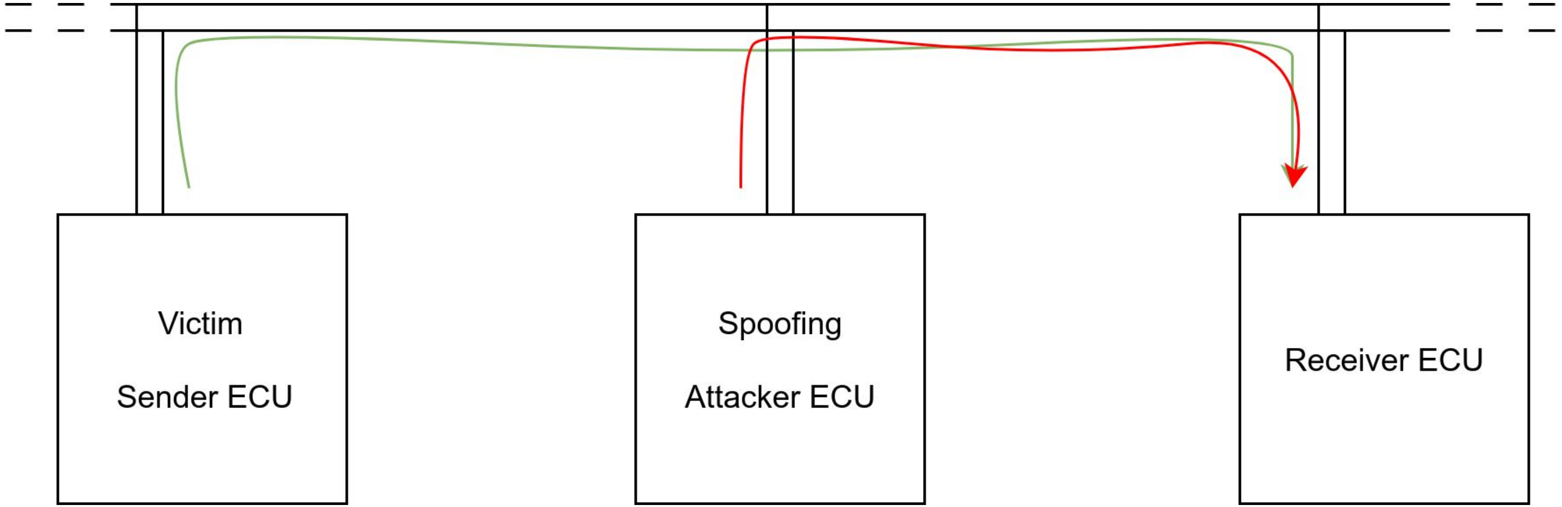
But what if the attacker wants to shut down only one ECU?

Automotive CAN Attacks - Targeted DoS



Automotive CAN Attacks - Spoofing

Pretty straightforward, sending messages with any ID is accepted in CAN. Even ones owned by other ECUs.
A basic receiver accepts ALL messages.



Countermeasures? Defenses?

Required at different levels:

1) Secure External communication
2) Secure Coding / Secure Hardware
3) Automotive-specific countermeasures

Countermeasures

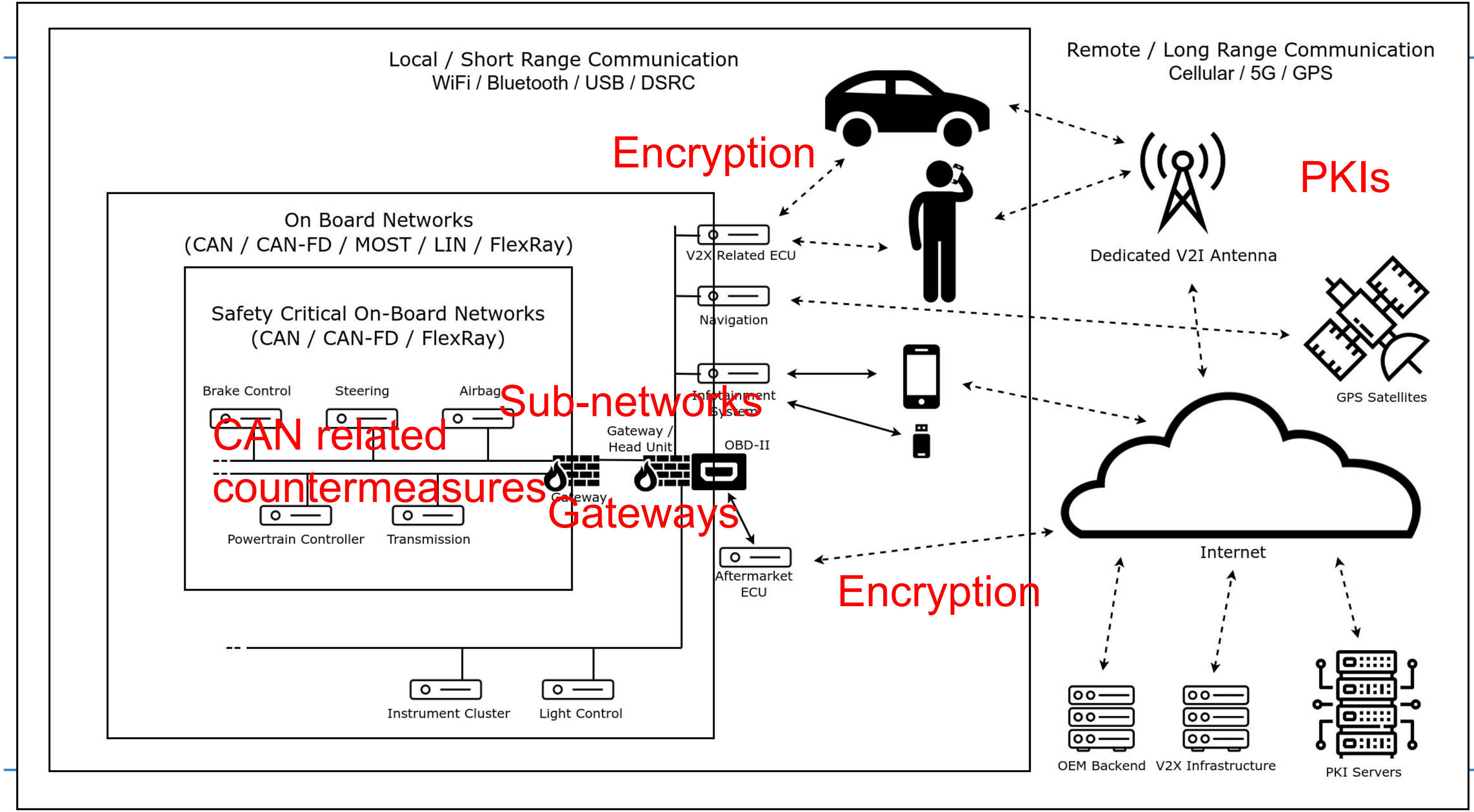
Authentication protocols

Intrusion Detection Systems

Subnetworks+Secure Gateways

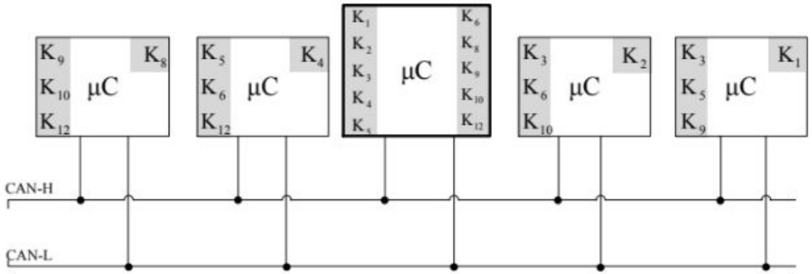
Intrusion “Reaction” Systems

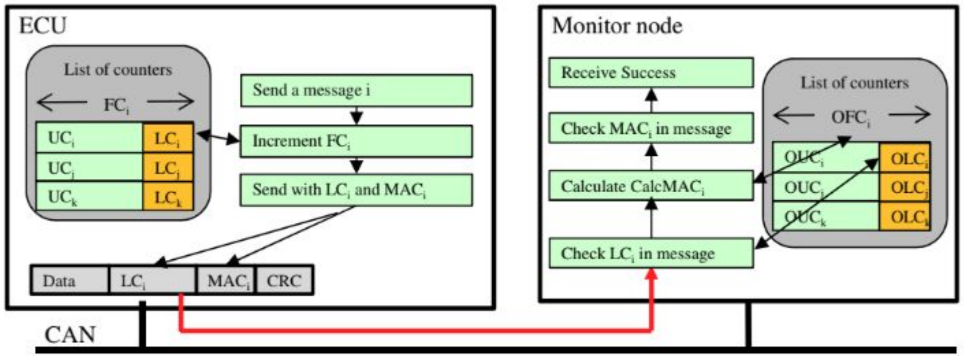
Countermeasures

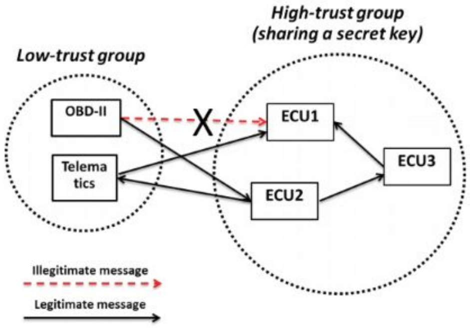


Authentication Protocols

1) MAC/HMAC
2) Backward compatible
3) Centralized/Distributed
4) Key Distribution
5) Security Level







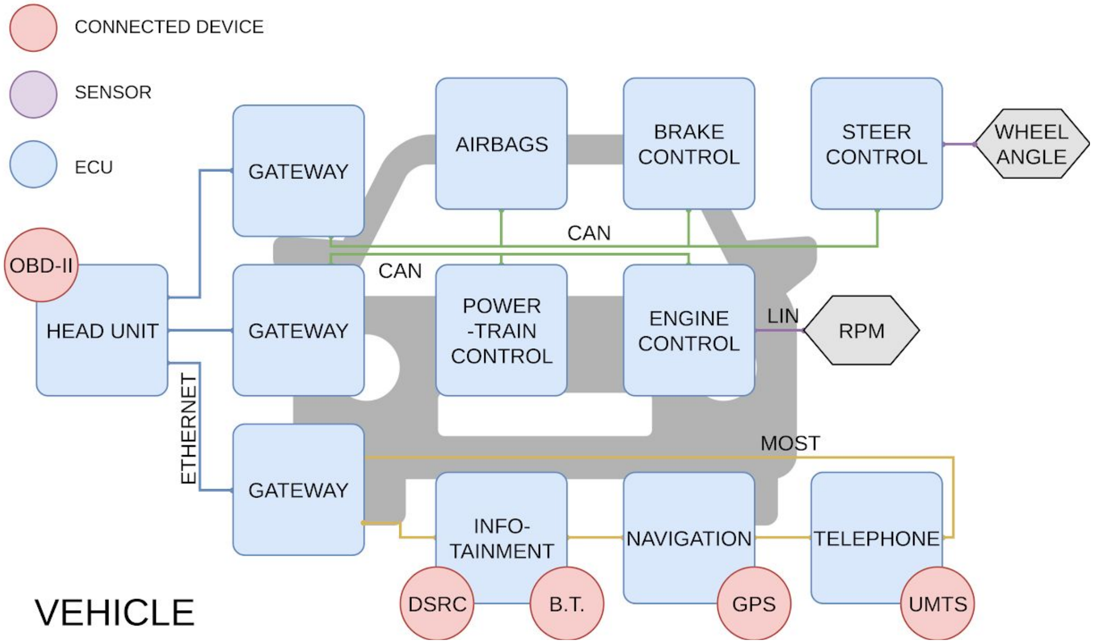
Intrusion Detection Systems

1) Frequency Based
    a) Issues related to the acceptable errors
2) Specification Based
    a) Physical specifications (e.g., Voltages/Power, …)
    b) Logical specifications (value ranges, ID ownership)
    c) Logical “differential” specifications (speed + rpm + gear)
    d) Issues related to the strength of rules
3) Data-Sequence Based
    a) Based on the change of data from the previous history
    b) Often ML based
        i) meh
    c) Still issues related to the strength of rules

+ What do i do AFTER???

Subnetworks + Secure Gateways

1) smart subdivision
2) Gateways = Firewalls



Intrusion Reaction Systems

1) Shut Down the attacker? -> Dangerous, also how do I tell?
2) Send Alert? -> to who, “hey driver u’r being PwNeD?”
3) Switch to a less “technology-reliant” mode?
4) Change IDs

Intrusion Detection+Reaction Systems

Parrot (2016):
Is someone sending my IDs? -> react and shut them down.

I will always win the “battle” even if both will increase the Transmit Error Counter, because at a certain point the attacker’s “error flag” will be passive.

Algorithm 1 The *Parrot* pseudo code

```
procedure MAIN()
    InitializeDefenseSystem()
    while parrotOnGuard do
        if suspectFound then
            # identified a spoofed message with my
            # ID
            ENGAGE(spoofedID)
procedure ENGAGE(SPOOFEDID)
    # continue as long as we either intercepted
    # the spoofed message or give up
    while suspectFound and !collisionDetected do
        transmitNDmessages(ND)
procedure TRANSMITNDMESSAGES(ND)
    bound = ND
    for (i=0 ; i < bound ; i++) do:
        transmitDmessage()
        # After identifying a potential collision we
        # enter the final stage of our counter-attack,
        # and reset the flags to allow new suspect
        # identification.
        if collisionDetected then:
            collisionDetected=False
            suspectFound=False
            # transmit exactly 15 more Dmessages
            bound=i+16
```

Defenses vs Attacks:

1) Sniffing -> no real solution
2) Spoofing -> Authentication Protocols (but limited)
3) Spoofing -> Intrusion Detection Systems combinations
4) DoS -> No real solution :((yet kinda less useful than others)
5) DoS + Spoofing -> Ouch! But there are solutions

Defenses vs Attacks:

DoS + Spoofing

First the attacker shuts down the ECU that sends the wanted signal (Targeted DoS)

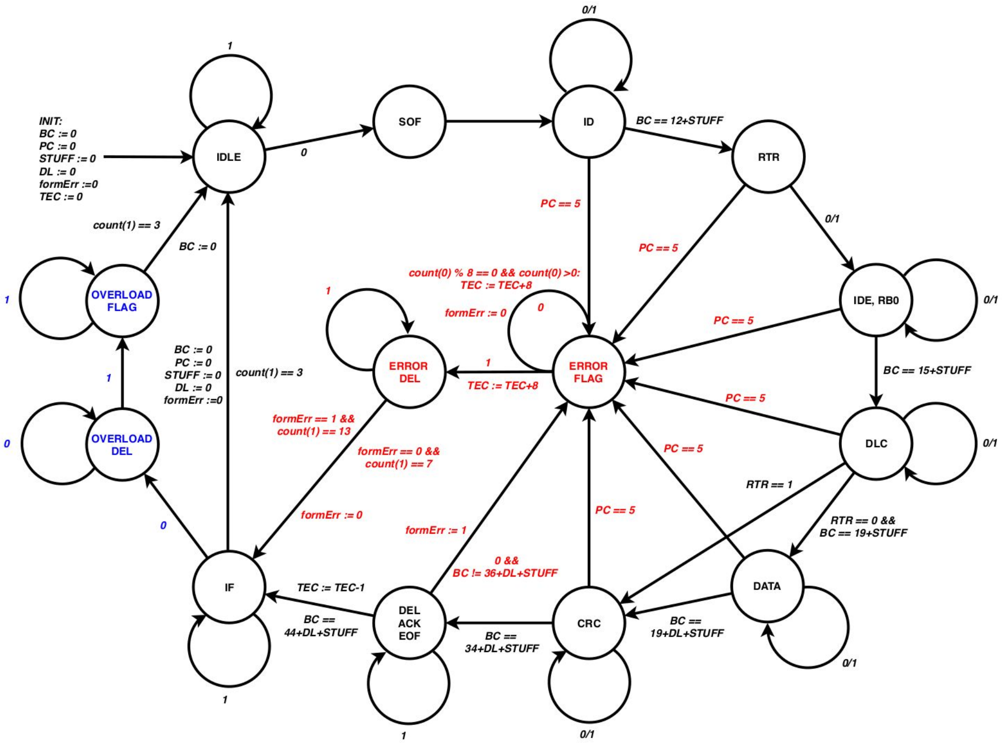
Then he sends forged messages on behalf of such ECU, undisturbed.

Hard to detect with frequency, specification or data-sequence based attacks.

Defenses vs Attacks: CopyCAN

How do we detect it?

We can detect the victim ECU going in “bus off” state. The IDs related to said ECU cannot be sent anymore.



POLITECNICO MILANO 1863

DIPARTIMENTO DI ELETTRONICA INFORMAZIONE E BIOINGEGNERIA

POLITECNICO MILANO 1863 NECST laboratory

Secure Positioning: RKES and GPS

Remote Passive Keyless Entry/Start Systems

How do they work?

1) The vehicle periodically sends a message asking for the key
2) When the key receives it, through RFID it responds
3) The vehicle opens the doors/ignites the engine

Remote Passive Keyless Entry/Start Systems

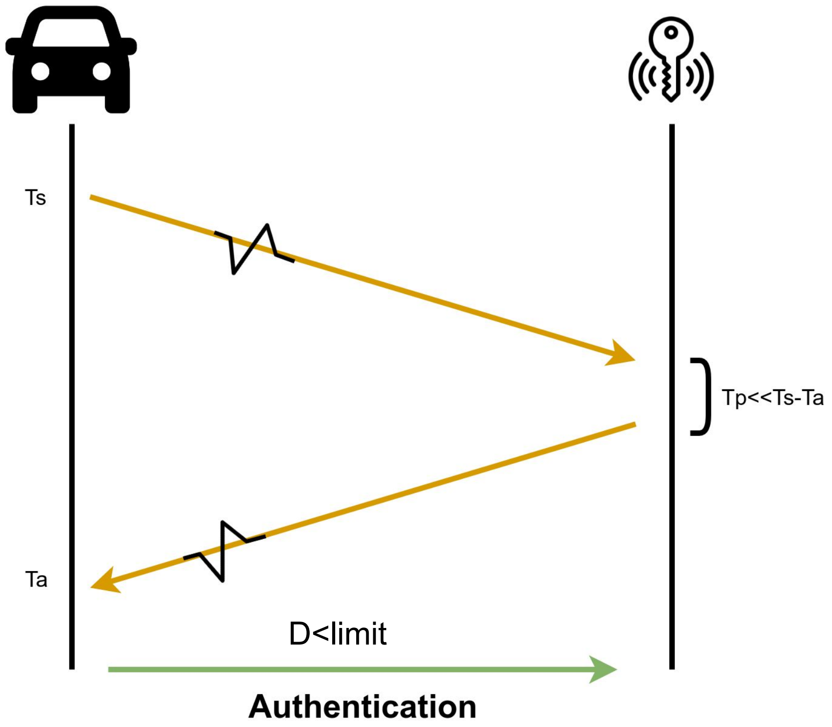
Does it need security? -> Well it is a substitute of the key, so yeah

Does it implement security measures? -> yes

Is it secure? ...

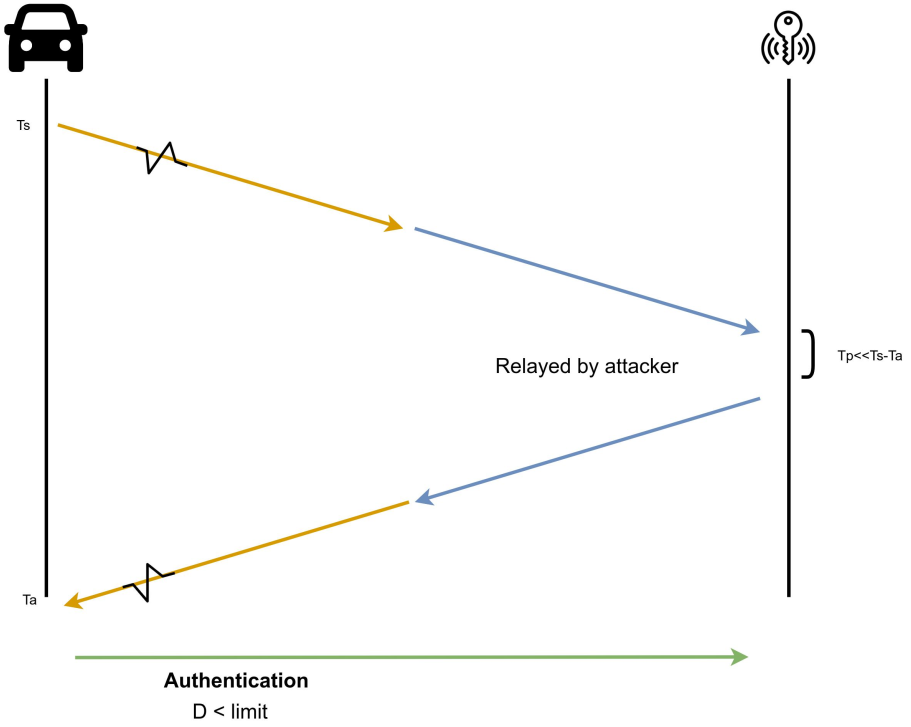

CAR
THEFT

How does RKES work?



$$D = (Ta - Ts - Tp) * c/2$$

What does an attacker want?



Generally to fake the key to be close to the car even if it isn't. In this way the car will start.

How is it secured?

IDM - Indirect Distance Measurement

1) NFC/RFID
2) RSSI (Received Signal Strength Indication) Measurement
3) Phase Measurement
4) AoA (Angle of Arrival) Measurement

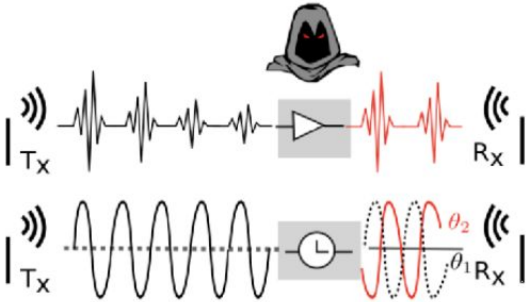
…

DDM - Direct Distant Measurement (Time-of-Flight)

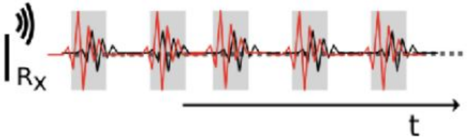
Most secure because basically uncheatable

Known Attacks

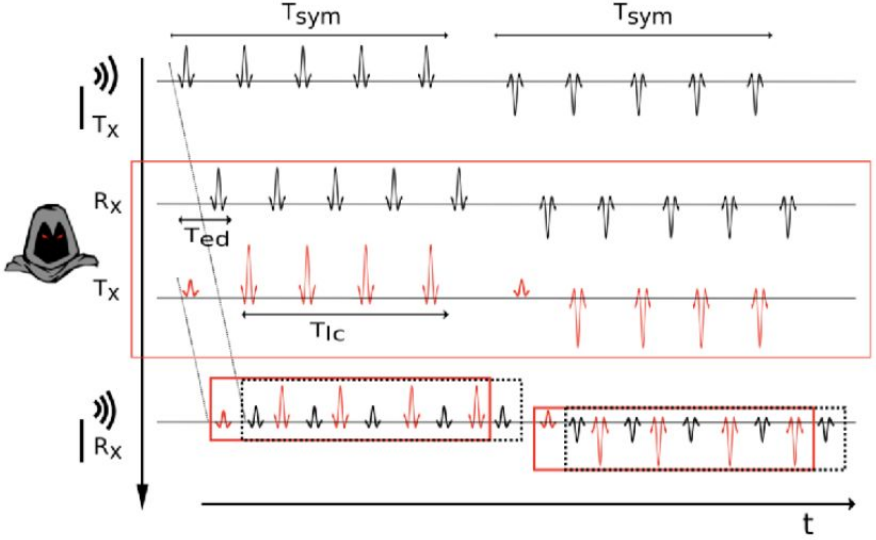
Simple Relay, Phase Relay, Signal Amplification, Early Detect / Late Commit, Cicada, Preamble Advance, …



a) Relay Attack

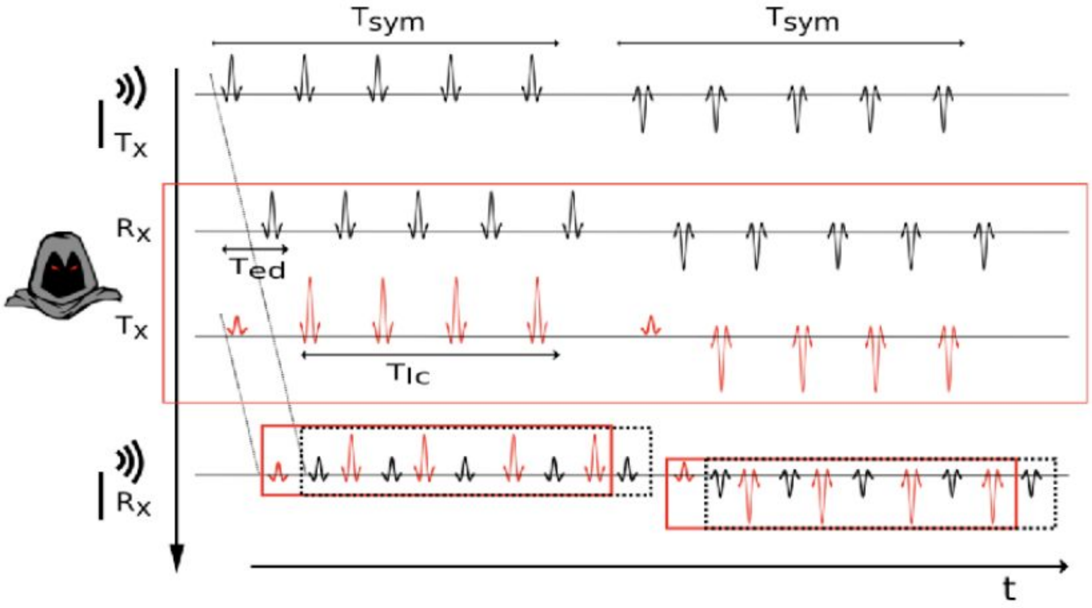


b) Cicada Attack



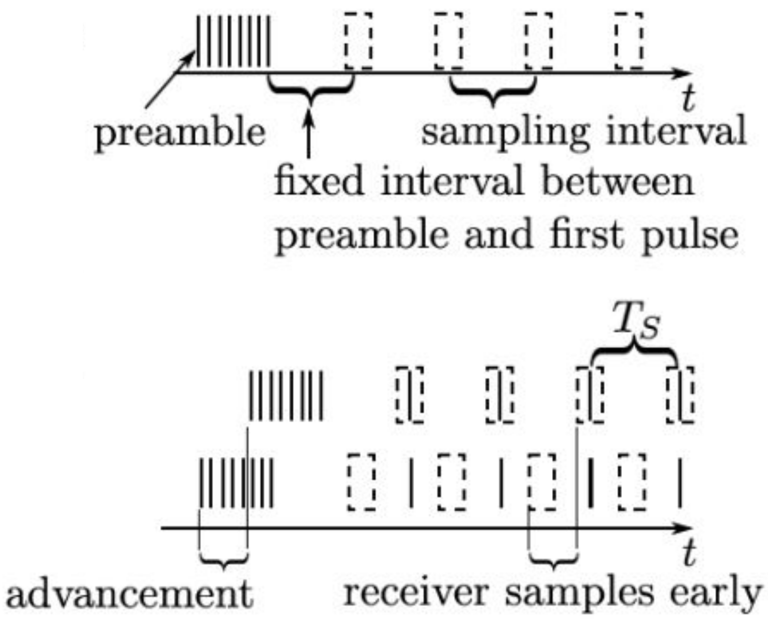
c) ED/LC Attack

Known Attacks: Early Detect/Late Commit

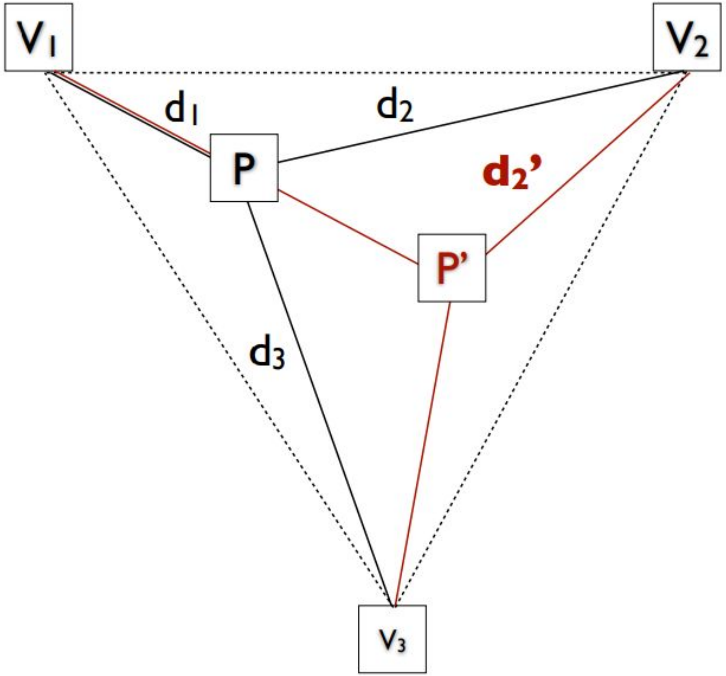


c) ED/LC Attack

Solution: Preamble!

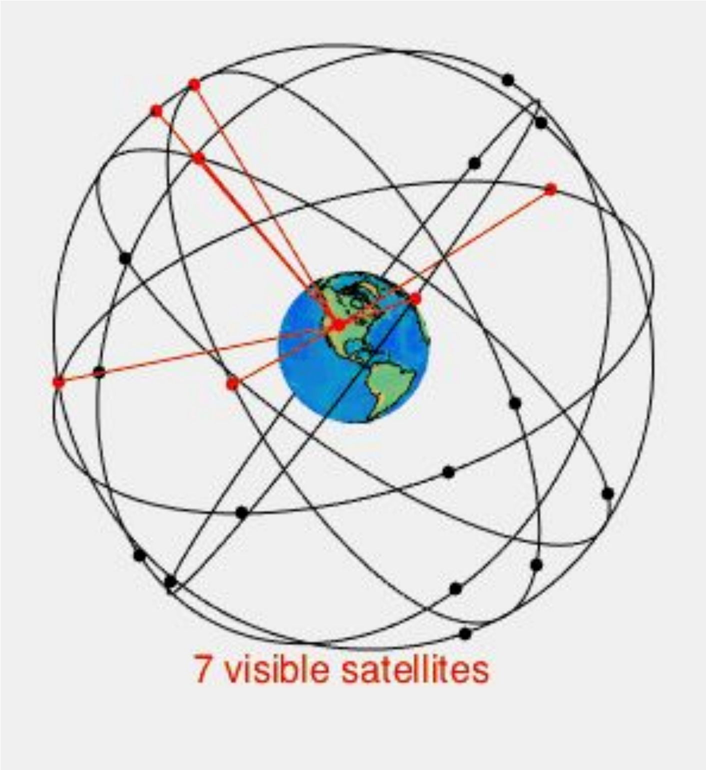


Triangulation OK! (Short Range)



P→P' => d2'<d2

Long Range Positioning: GPS / GNSS



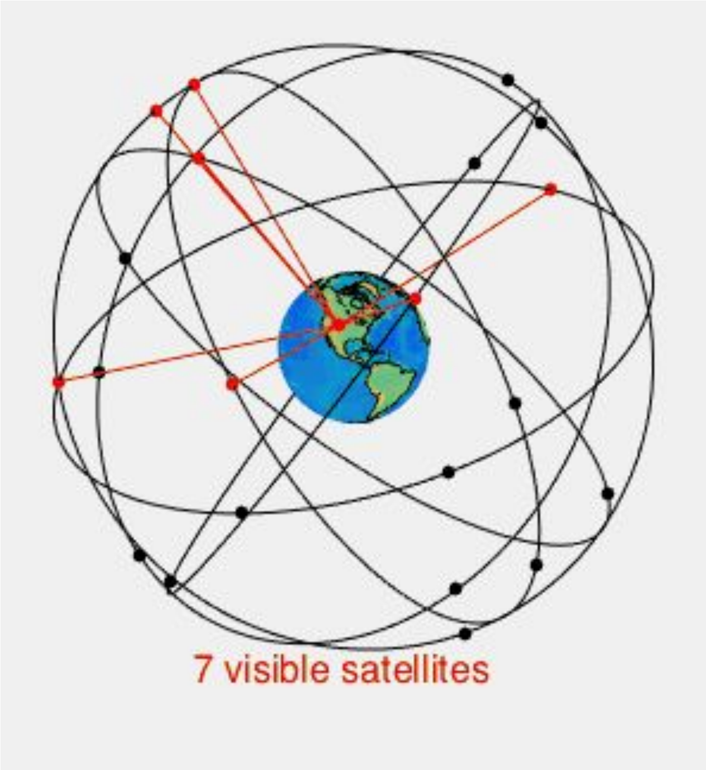
24 satellites at 20.200 Km

Each satellite sends its location and PRECISE time of transmission

GPS receiver measures the distance from each satellite

Receiver uses trilateration to calculate its position

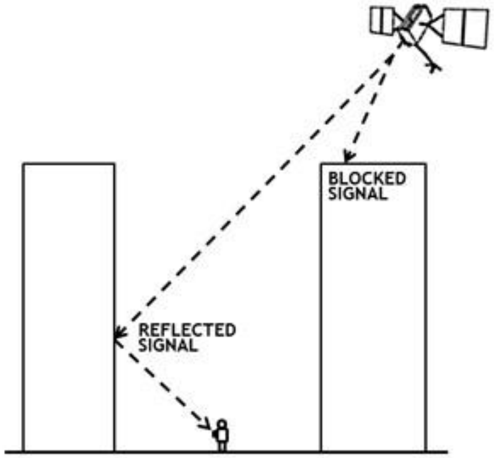
GPS Encryption



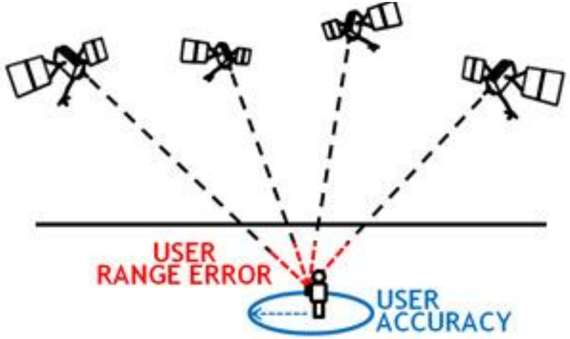
GPS is encrypted ONLY for military purposes.

Why? - hard to keep the secret a secret
- all satellites has to know all keys
- can’t create 10000000000 keys

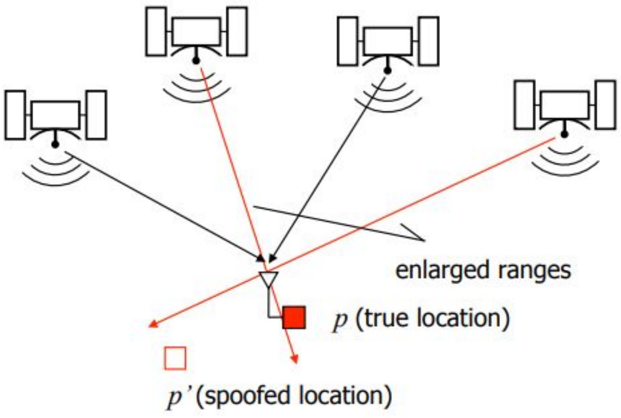
GPS Precision



The government commits to broadcasting the GPS signal in space with a global average user range error (URE) of ≤7.8 m (25.6 ft.), with 95% probability. Actual performance exceeds the specification. On May 11, 2016, the global average URE was ≤0.715 m (2.3 ft.), 95% of the time.



GPS Spoofing



The attacker:

Modifies the navigation message contents

or

Manipulates the time of arrival

(Military GPS can only be delayed)

GNSS Countermeasures

Changing the protocol:

- Authentication of messages -> can still be delayed
- Direct Sequence Spread Spectrum -> requires secred shared keys

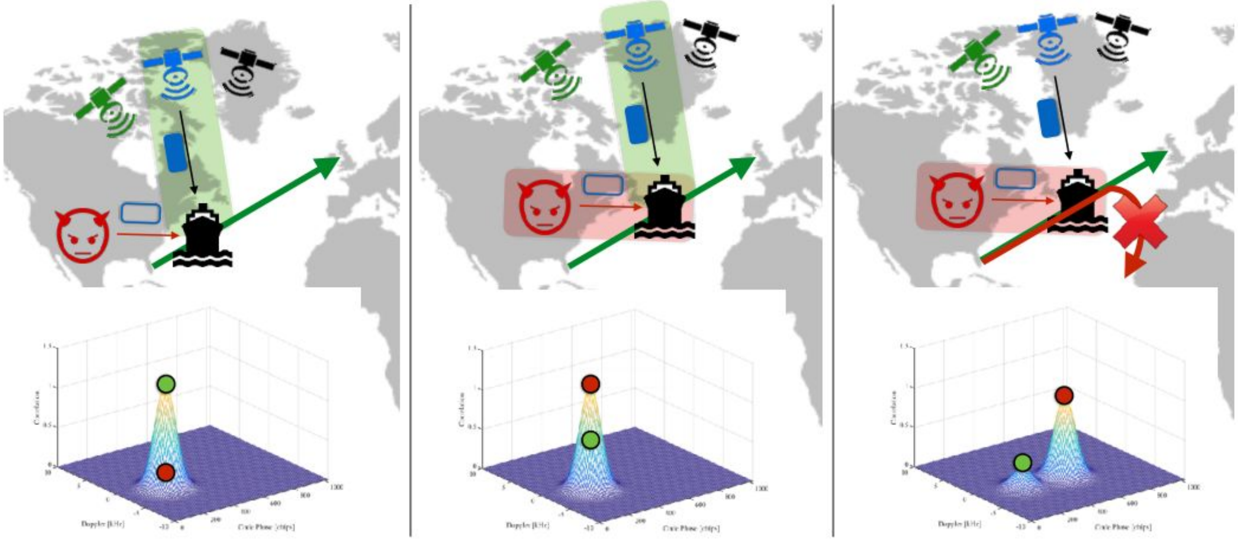
Not changing the protocol:

- Noise level, # of satelites…
- Spatial Diversity (AoA...)

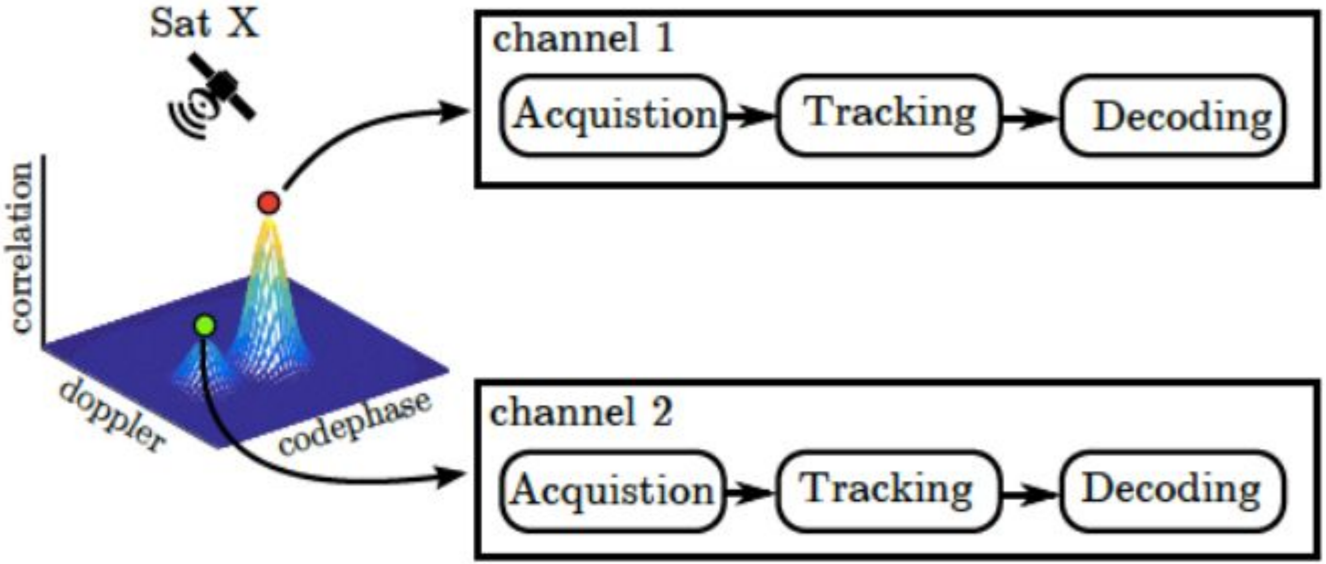
More or less feasible...

GNSS Seamless Takeover Attack

...But counterable

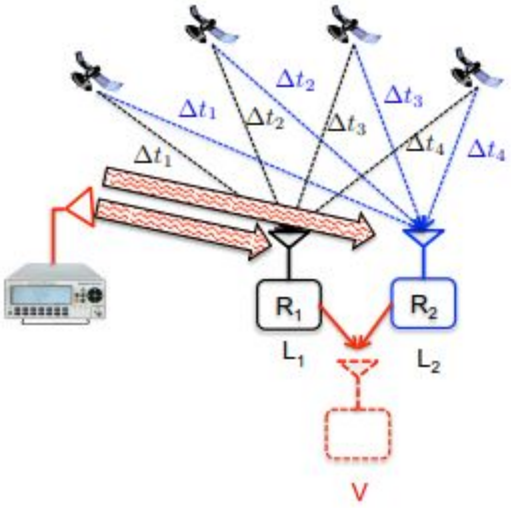


Detection with one receiver: SPREE



Detection with multiple receivers:

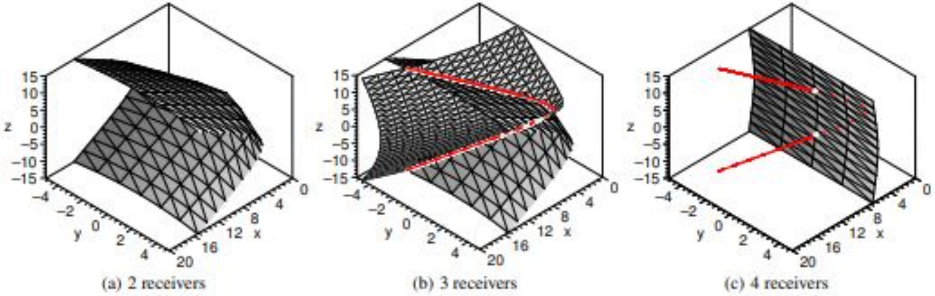
Leverage spatial diversity



If d(R1,R2) is known
=> spoofing detection

Detection with multiple receivers:

Spatial diversity and number of nodes constraint the attacker



	Spoofing to one location	Spoofing to multiple locations (preserved formation)	
n	Civ. & Mil. GPS	Civilian GPS	Military GPS
1	$P_i^A \in \mathbb{R}^3$	-	-
2	$P_i^A \in \mathbb{R}^3$	set of hyperboloids	one hyperboloid
3	$P_i^A \in \mathbb{R}^3$	set of intersections of two hyperboloids	intersection of two hyperboloids
4	$P_i^A \in \mathbb{R}^3$	set of 2 points	2 points
≥ 5	$P_i^A \in \mathbb{R}^3$	set of points	1 point

Thanks

For any question please write to <stefano.longari@polimi.it>

Thanks to ETH zurich and Srdjan Čapkun for some contents of the slides