POLITECNICO
MILANO 1863

DIPARTIMENTO DI ELETTRONICA
INFORMAZIONE E BIOINGEGNERIA

POLITECNICO MILANO 1863
NECST laboratory

Automotive Security

Stefano Longari

Stefano.longari@polimi.it

Program of these two lessons:

- Introduction to the automotive context
- Automotive (CAN) Attacks
- Automotive (CAN) Countermeasures
- Secure Positioning Systems
- Exercises

Automotive Ecosystem Players:

Automotive Manufacturers

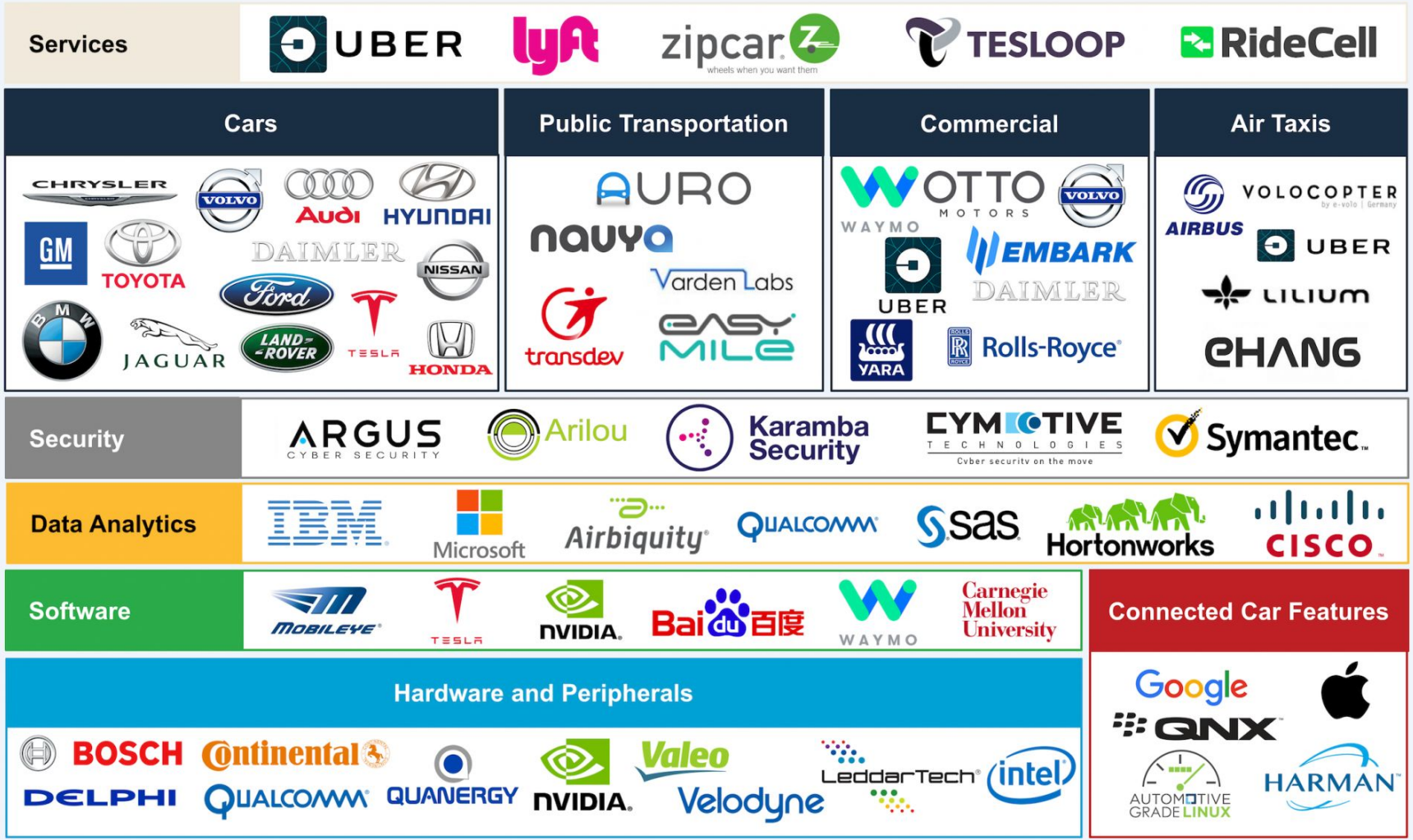
Original Equipment Manufacturers

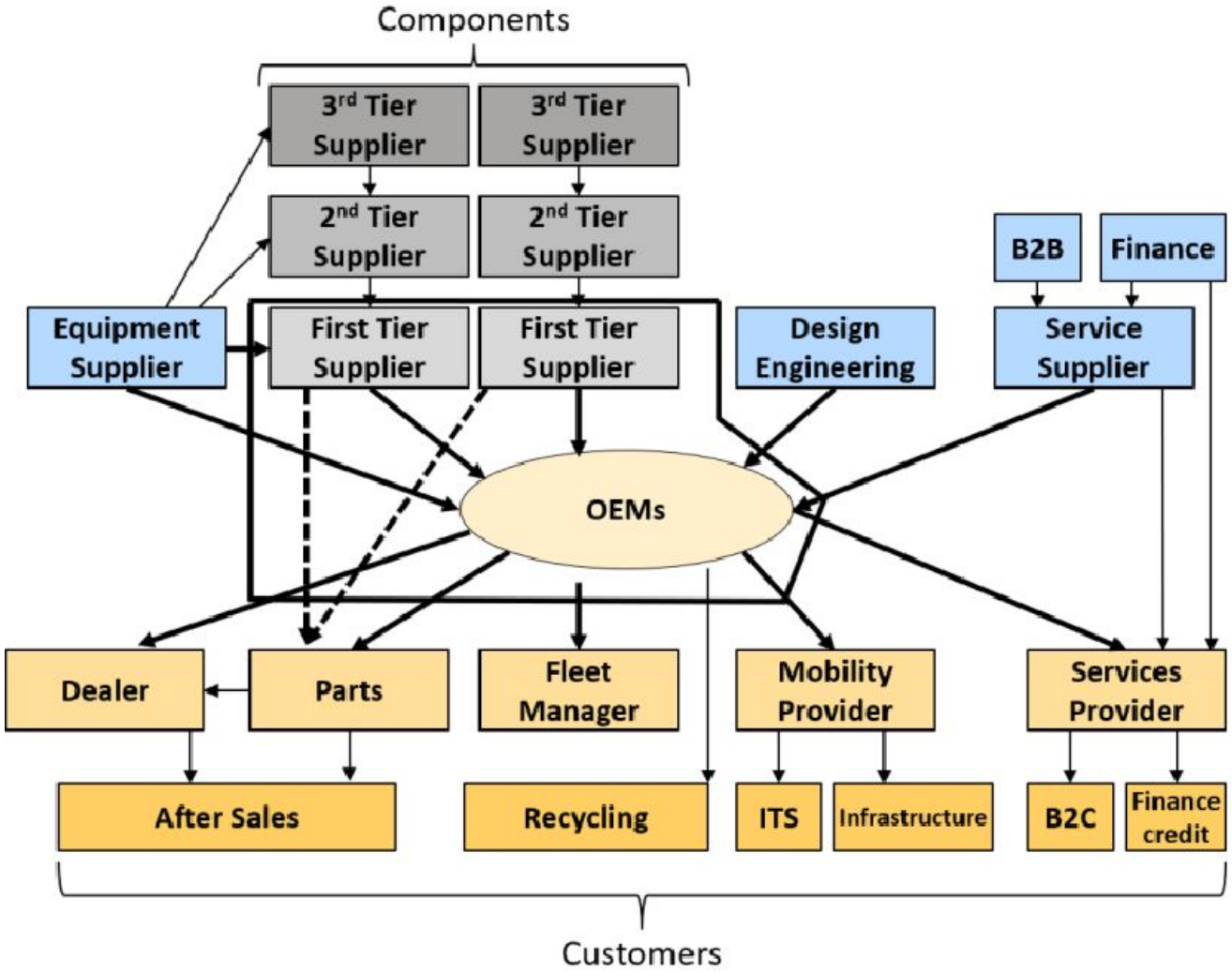
Processor/Semiconductor/Board Companies

Regulations and State requirements

Fleet management companies (Uber, Taxis, Truck hauling companies, Postal services, Rental etc…)

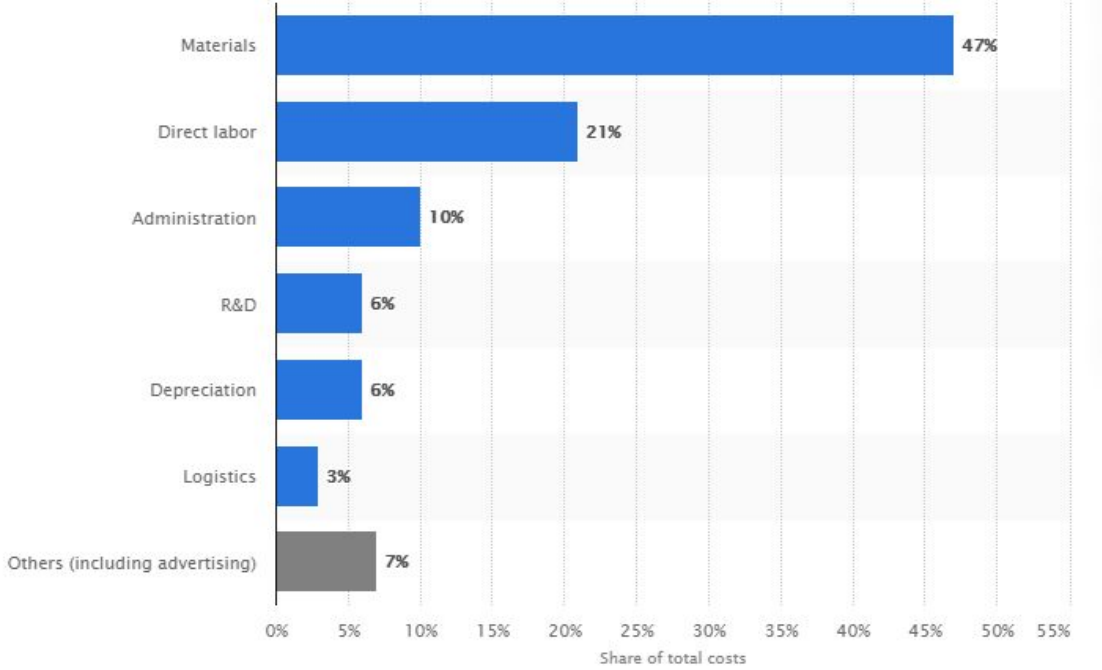
All these players have a role in the development of new vehicles


Services
UBER
lyft
zipcar
wheels when you want them
TESLOOP
RideCell
Cars
CHRYSLER
VOLVO
Audi
HYUNDAI
GM
TOYOTA
DAIMLER
NISSAN
Ford
TESLA
BMW
JAGUAR
LAND ROVER
HONDA
Public Transportation
AURO
navya
Varden Labs
transdev
easy MILE
Commercial
OTTO
MOTORS
VOLVO
WAYMO
EMBARK
UBER
DAIMLER
YARA
Rolls-Royce
Air Taxis
VOLOCOPTER
by e-volo | Germany
AIRBUS
UBER
LILIUM
EHANG
Security
ARGUS
CYBER SECURITY
Arilou
Karamba Security
CYMOTIVE
TECHNOLOGIES
Cyber security on the move
Symantec
Data Analytics
IBM
Microsoft
Airbiquity
QUALCOMM
sas
Hortonworks
CISCO
Software
MOBILEYE
TESLA
NVIDIA
Baidu 百度
WAYMO
Carnegie Mellon University
Connected Car Features
Google
QNX
AUTOMOTIVE GRADE LINUX
HARMAN
Hardware and Peripherals
BOSCH
Continental
DELPHI
QUALCOMM
QUANERGY
NVIDIA
Valeo
Velodyne
LeddarTech
intel


Components
3rd Tier Supplier
3rd Tier Supplier
2nd Tier Supplier
2nd Tier Supplier
B2B
Finance
Equipment Supplier
First Tier Supplier
First Tier Supplier
Design Engineering
Service Supplier
OEMs
Dealer
Parts
Fleet Manager
Mobility Provider
Services Provider
After Sales
Recycling
ITS
Infrastructure
B2C
Finance credit
Customers

Costs and profits

Profit per vehicle: around 3k$



Details: Worldwide; 2015

https://www.statista.com/statistics/744910/cost-breakdown-of-car-production-by-segment/
https://www.zaginvestor.com/tesla-profit-per-vehicle/

Latest Vehicle Advancements: Safety

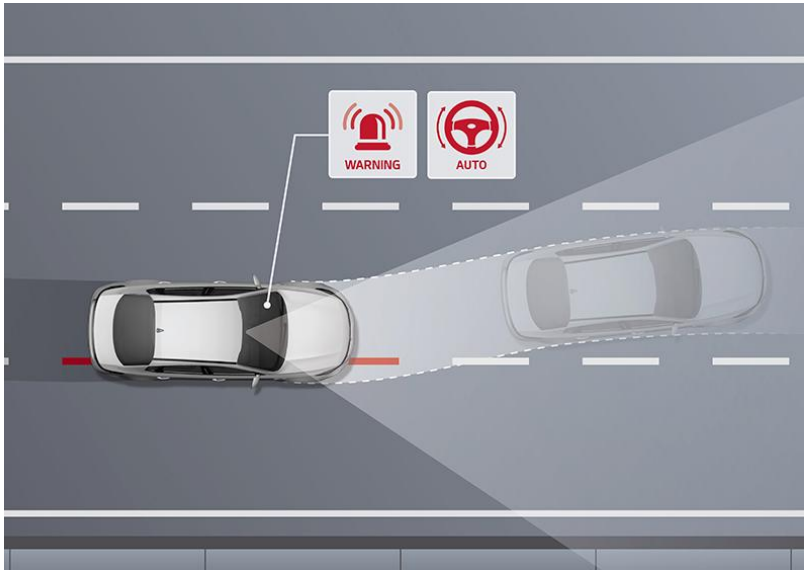
Pedestrian Detection and braking systems

Latest Vehicle Advancements: Safety

Drowsiness detection

Latest Vehicle Advancements: Safety

Lane Assist

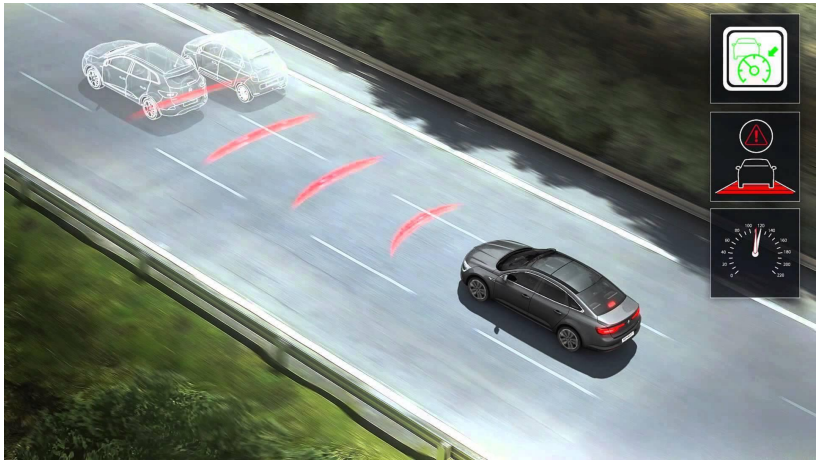


Latest Vehicle Advancements: Safety

Emergency Call

Latest Vehicle Advancements: Comfort

Adaptive Cruise Control

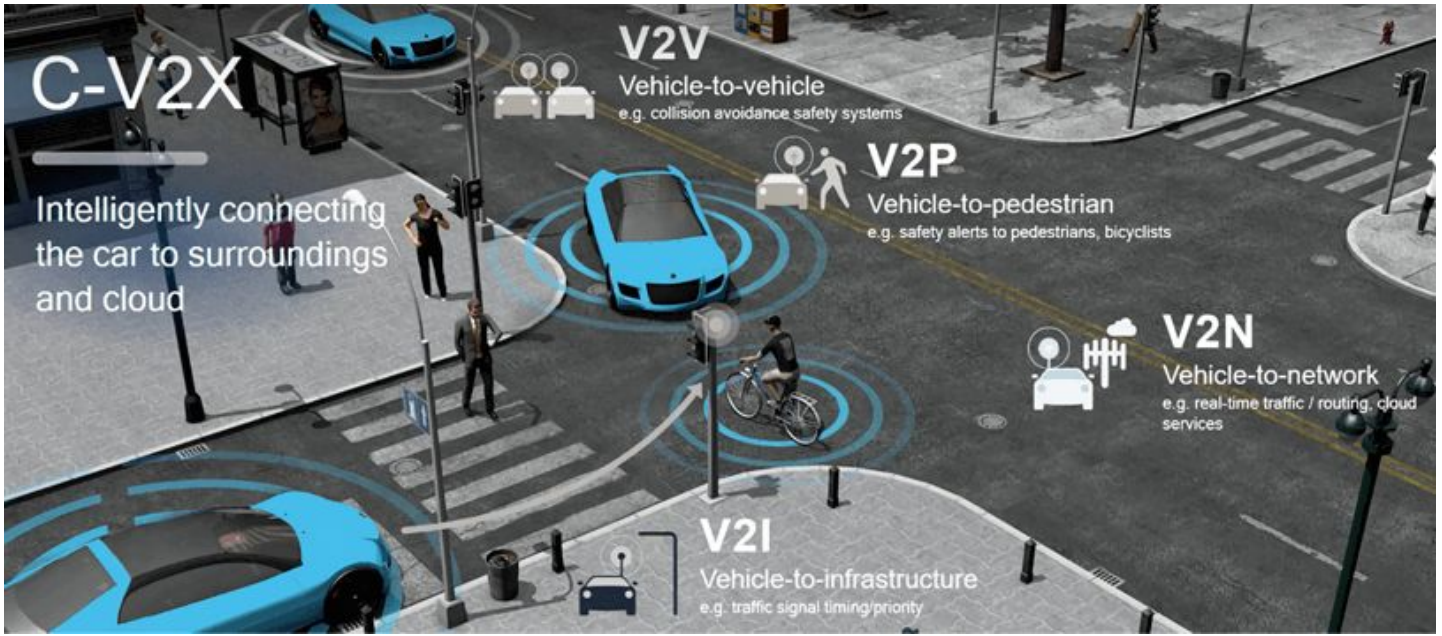


Latest Vehicle Advancements: Comfort

Personalized adjustable settings

Latest Vehicle Advancements: Communication

V2X

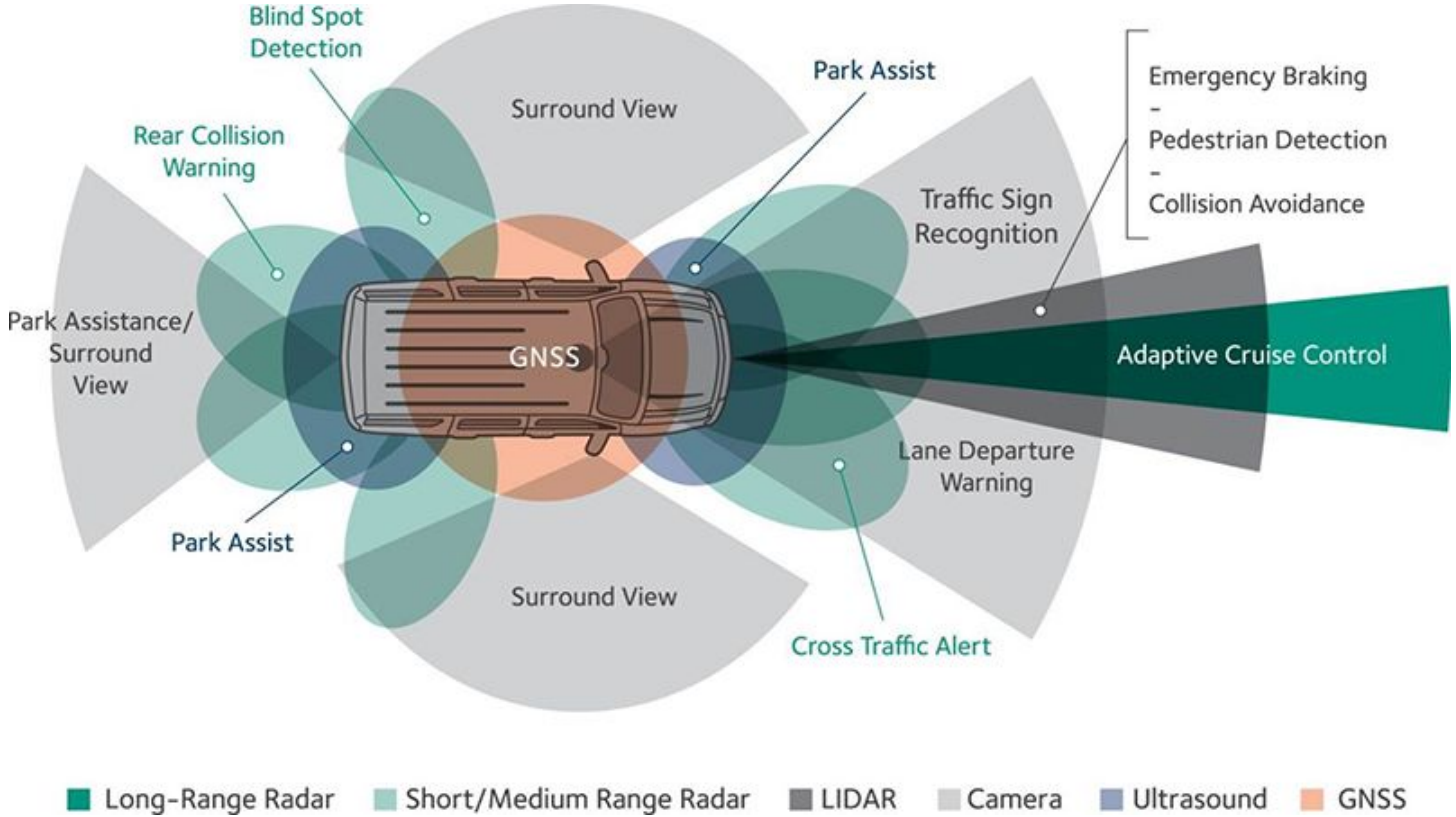


Latest Vehicle Advancements: Communication

Aftermarket Devices

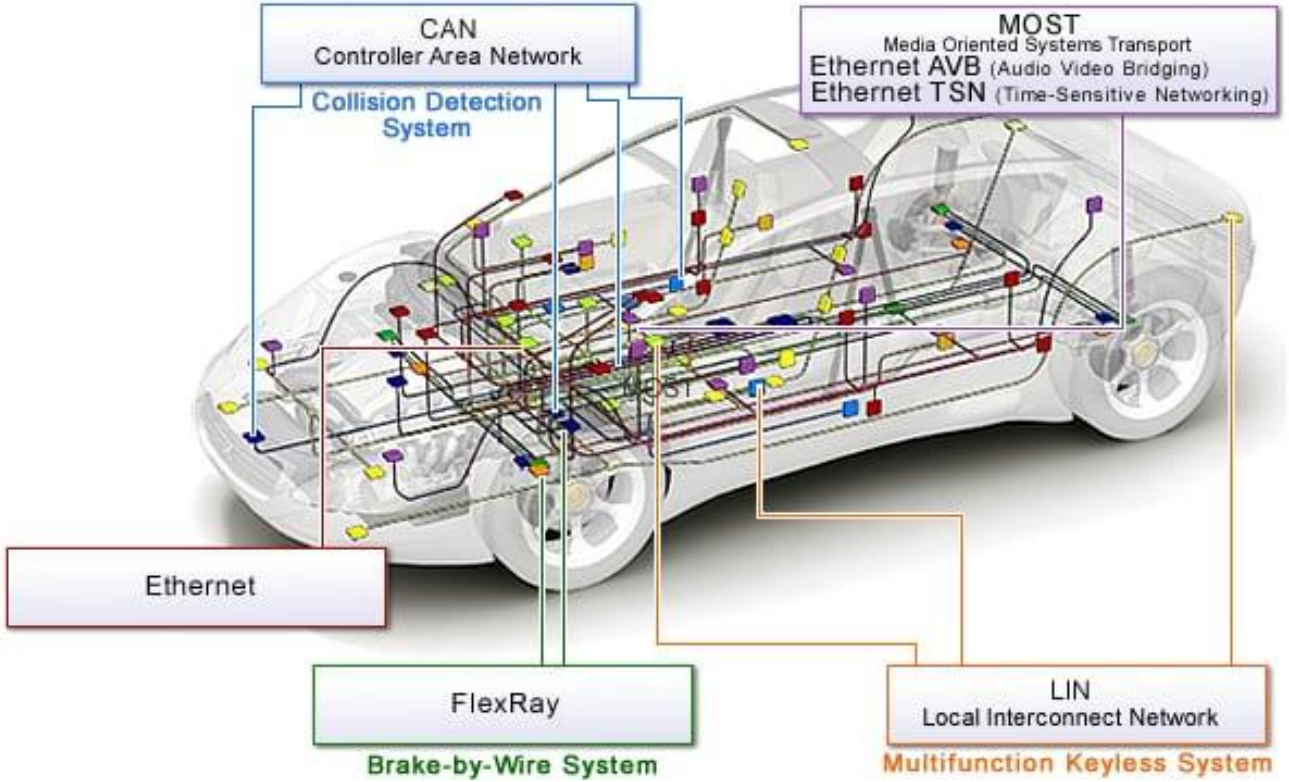
Future Vehicle Advancements

Technologies to get there: External Sensors



Technologies to get there: External Sensors

Technologies to get there: On-board networks

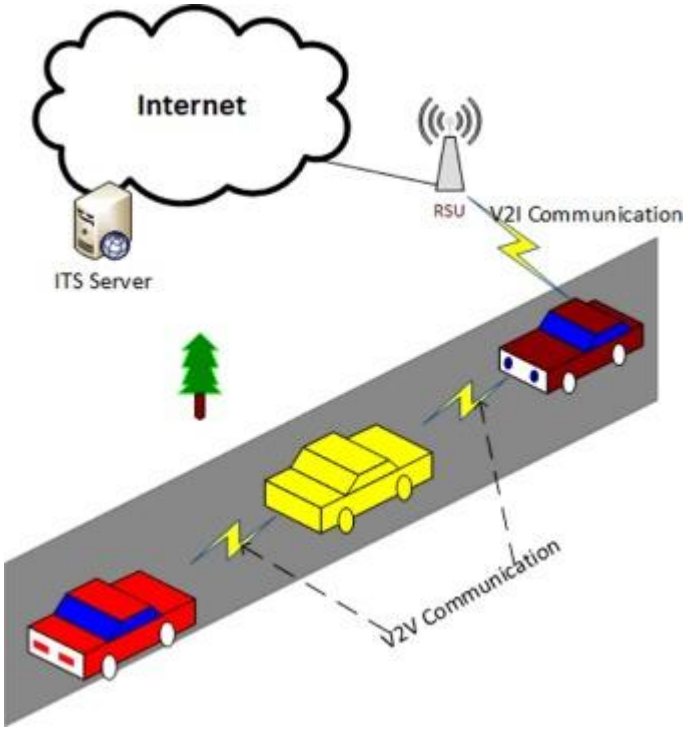


Technologies to get there: Communication Networks

Local Communication **Remote Communication**

DSRC

Technologies to get there: Communication Networks



Sending and receiving traffic data

Sending status updates

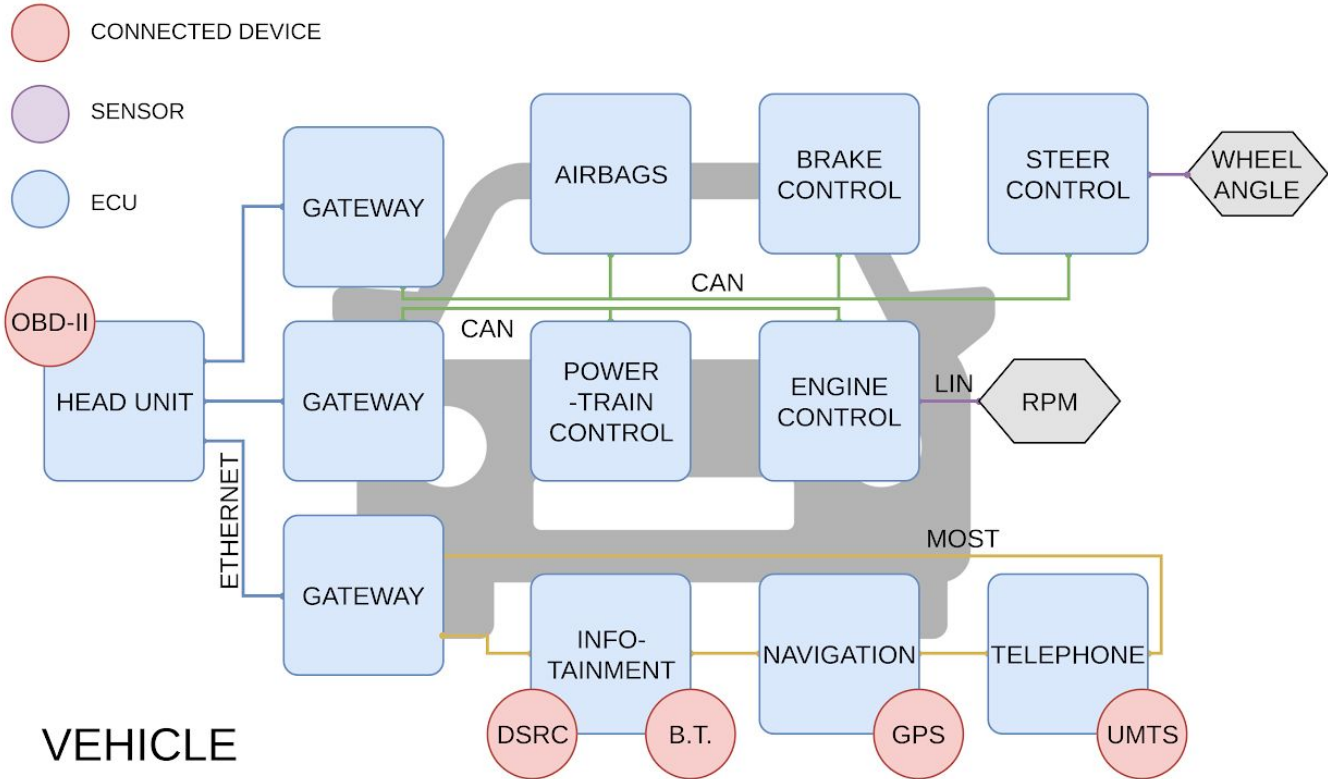
Receiving software updates

Phone calls

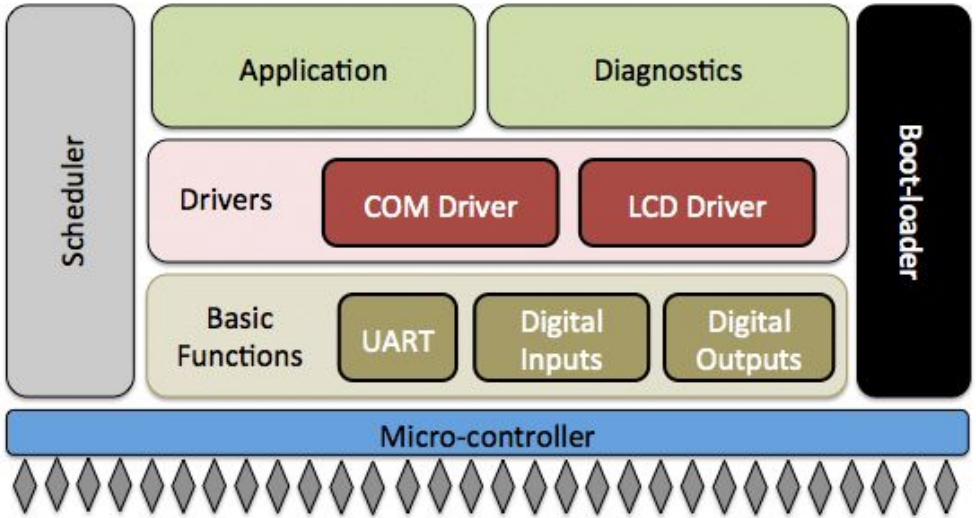
Internet navigation

…

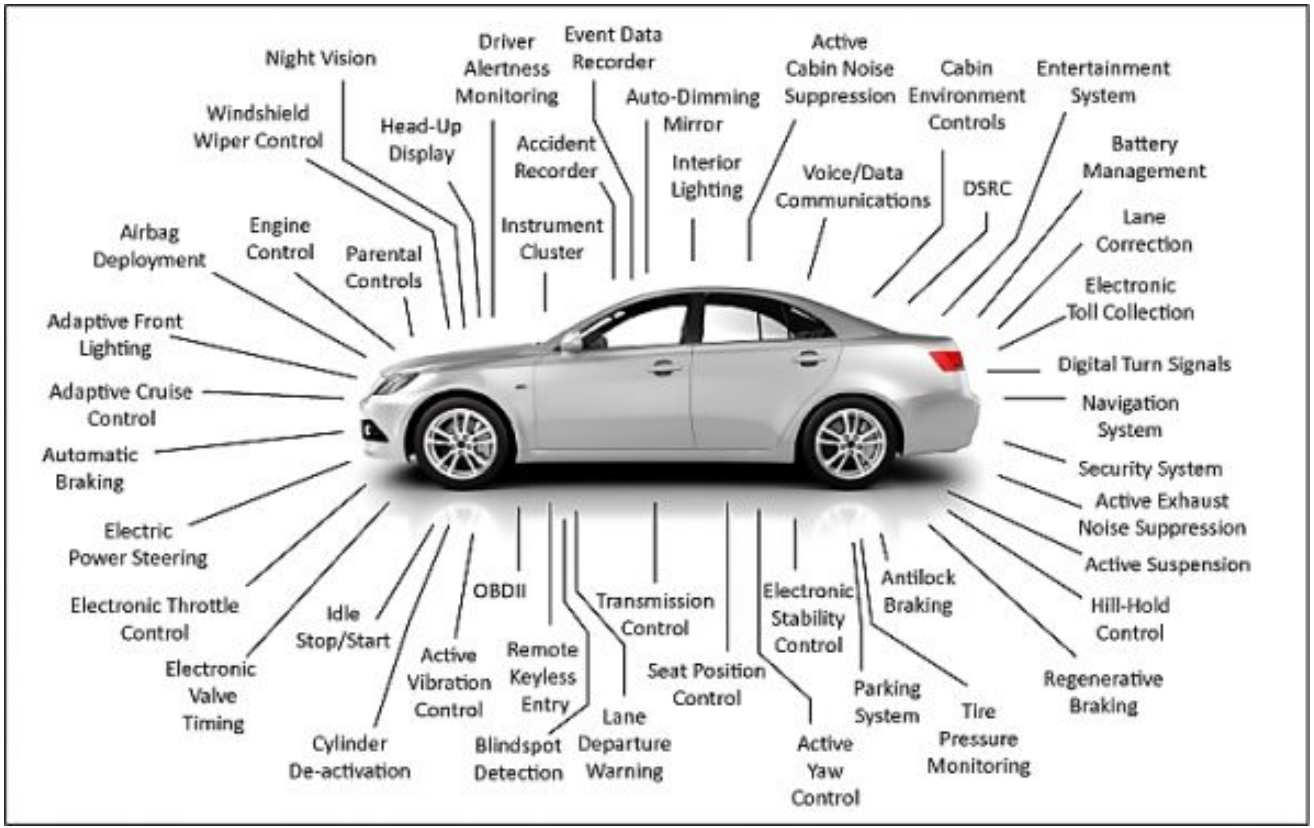
Technologies to get there: On-board networks

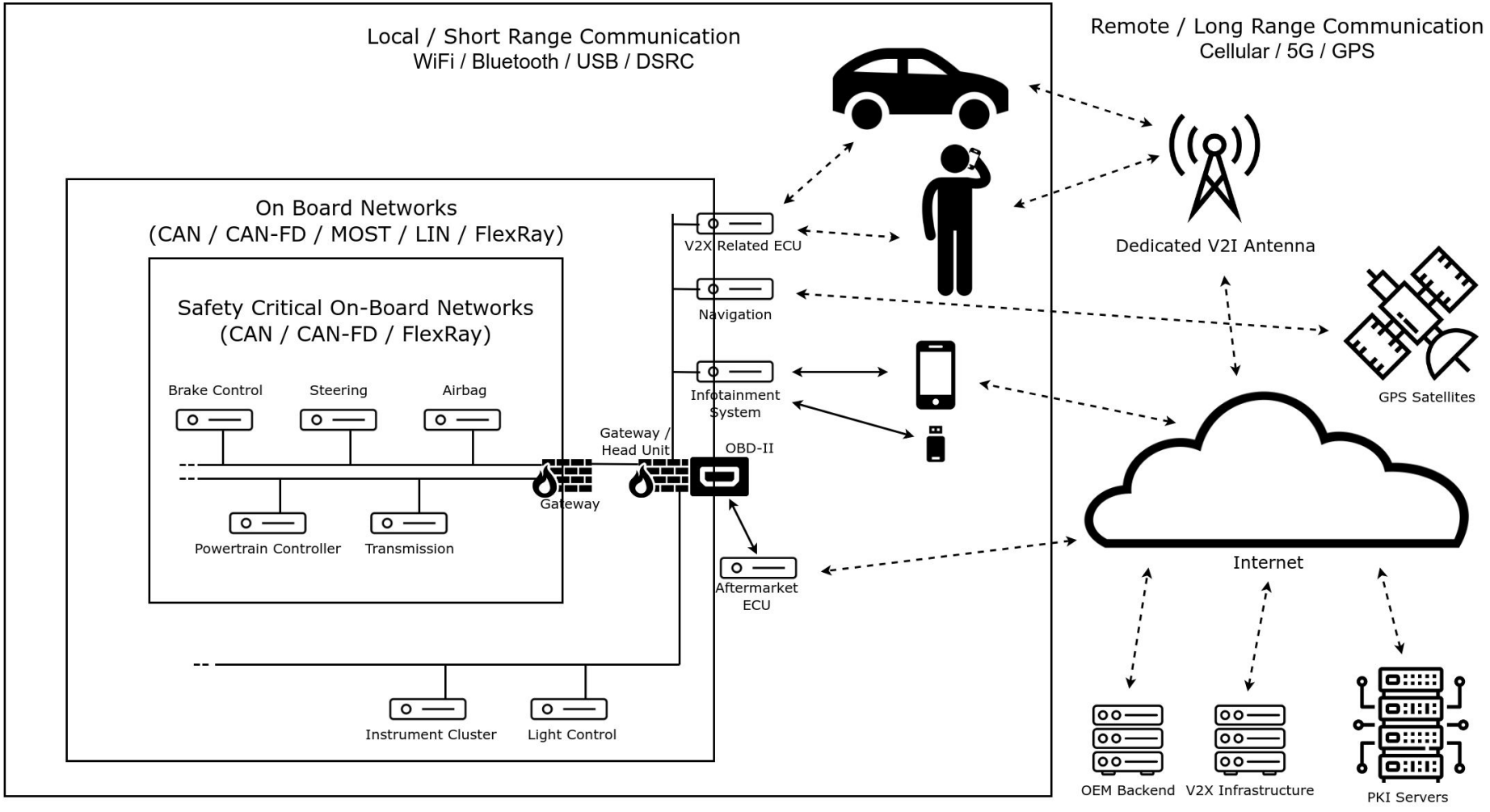


Technologies to get there: ECUs



Overview of intra vehicle devices




Local / Short Range Communication
WiFi / Bluetooth / USB / DSRC
Remote / Long Range Communication
Cellular / 5G / GPS
On Board Networks
(CAN / CAN-FD / MOST / LIN / FlexRay)
Safety Critical On-Board Networks
(CAN / CAN-FD / FlexRay)
Brake Control
Steering
Airbag
Powertrain Controller
Transmission
Gateway
Gateway /
Head Unit
OBD-II
V2X Related ECU
Navigation
Infotainment
System
Aftermarket
ECU
Instrument Cluster
Light Control
Dedicated V2I Antenna
GPS Satellites
Internet
OEM Backend
V2X Infrastructure
PKI Servers

POLITECNICO
MILANO 1863

DIPARTIMENTO DI ELETTRONICA
INFORMAZIONE E BIOINGEGNERIA

POLITECNICO MILANO 1863
NECST laboratory

CAN NETWORKS

Most common on-board subnetworks

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

CAN-FD - “faster” CAN, basically identical, carries more data

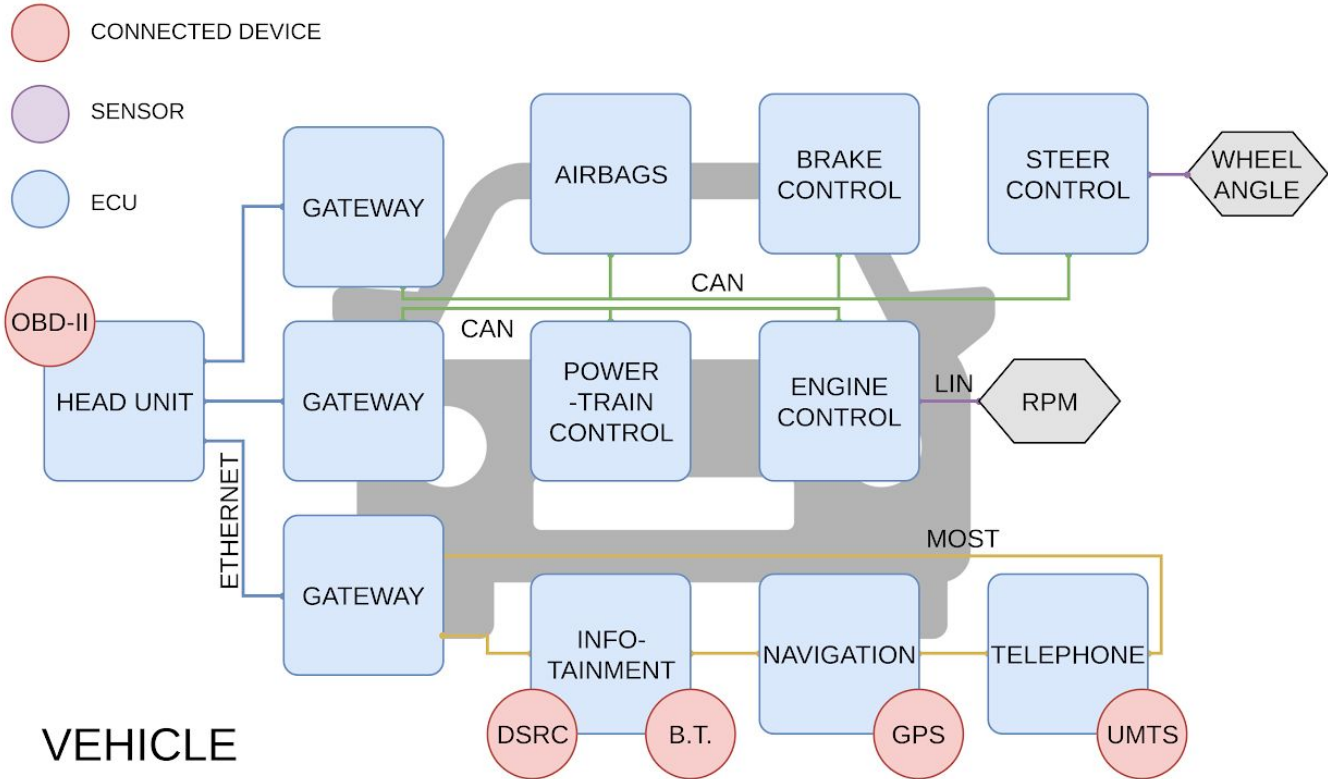
FlexRay: Expensive, Real-Time

MOST - Media Oriented System Network: High Bandwidth

LIN - Local Interconnect Network: Cheap, for sensors

Automotive Ethernet: Higher speed than CAN, already used in other contexts

Most common on-board subnetworks

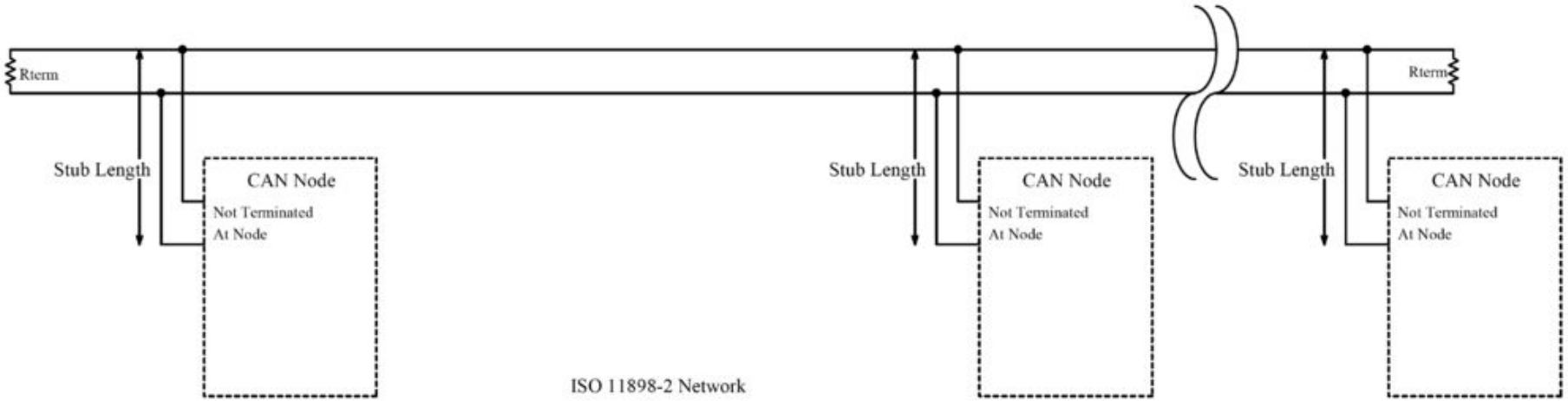


Controller Area Network

- 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
- Max network length of 40 meters
- Max baud rate 1Mbps (usually 500/250kbps)

Controller Area Network

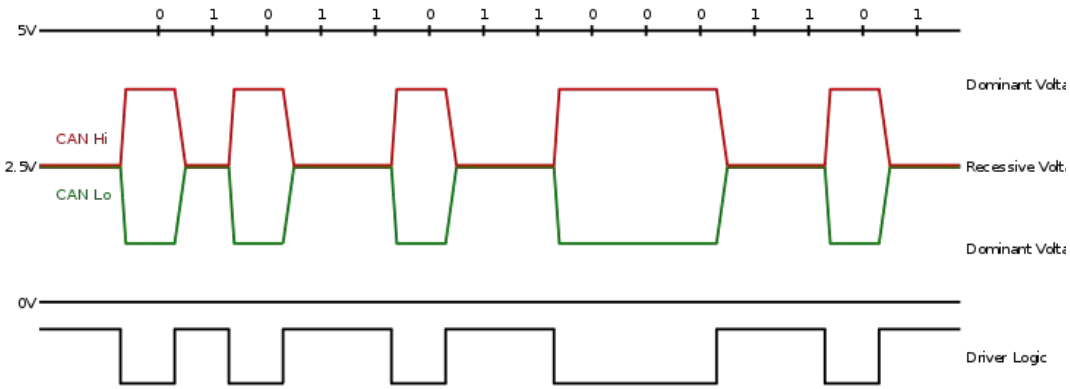
- Multi Master
- Broadcast
- Bus topology

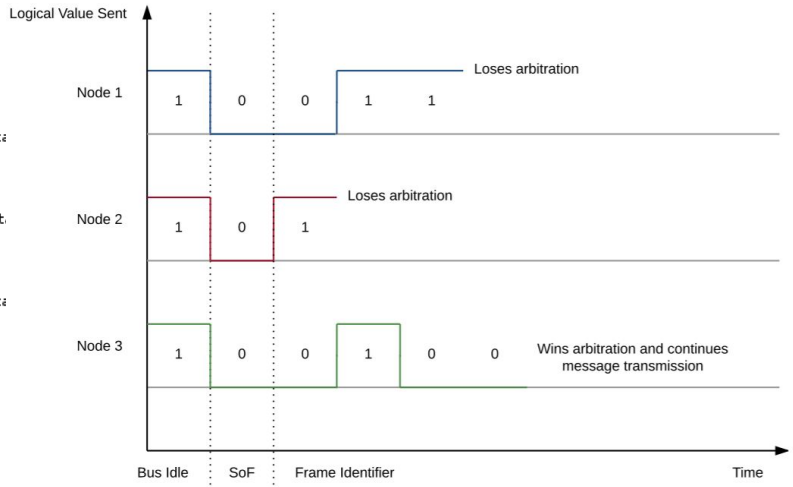


Controller Area Network

Physical layer: Differential signaling over two wires

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





Controller Area Network: Frames

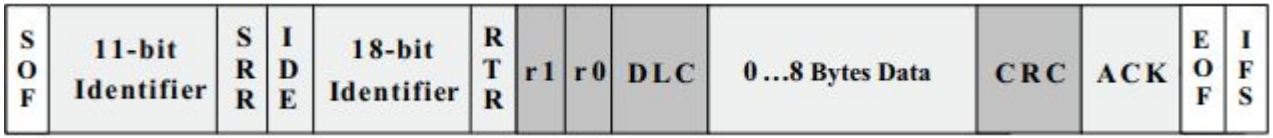
- Data Frames
- Remote Frames
- Error Frames
- Overload Frames

Controller Area Network: Data Frames

Base Frame format: 11 bit ID (2^11 2048 possible IDs)

Extended Frame format: 29 bit ID (2^29 = 536870912 possible IDs)

8 data bytes (64 for CAN-FD)



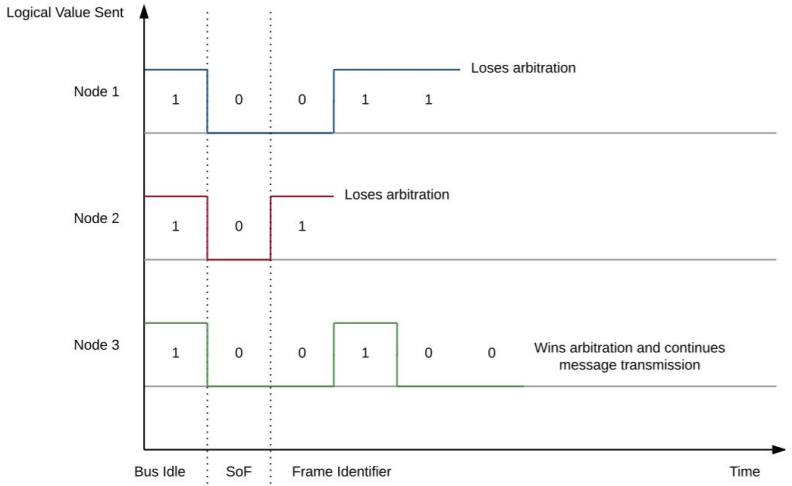
Controller Area Network: Data Frames

(Wikipedia)

Field name	Length (bits)	Purpose
Start-of-frame	1	Denotes the start of frame transmission
Identifier (green)	11	A (unique) identifier which also represents the message priority
Remote transmission request (RTR) (blue)	1	Must be dominant (0) for data frames and recessive (1) for remote request frames (see Remote Frame, below)
Identifier extension bit (IDE)	1	Must be dominant (0) for base frame format with 11-bit identifiers
Reserved bit (r0)	1	Reserved bit. Must be dominant (0), but accepted as either dominant or recessive.
Data length code (DLC) (yellow)	4	Number of bytes of data (0–8 bytes)[a]
Data field (red)	0–64 (0-8 bytes)	Data to be transmitted (length in bytes dictated by DLC field)
CRC	15	Cyclic redundancy check
CRC delimiter	1	Must be recessive (1)
ACK slot	1	Transmitter sends recessive (1) and any receiver can assert a dominant (0)
ACK delimiter	1	Must be recessive (1)
End-of-frame (EOF)	7	Must be recessive (1)

Controller Area Network: Data Frames

IDs enable priority as seen before



Lower ID = higher priority, hence messages with high real time requirements are associated to lower IDs

Controller Area Network: Data Frames

Each ECU “owns” a set of IDs

No other ECU can use those IDs

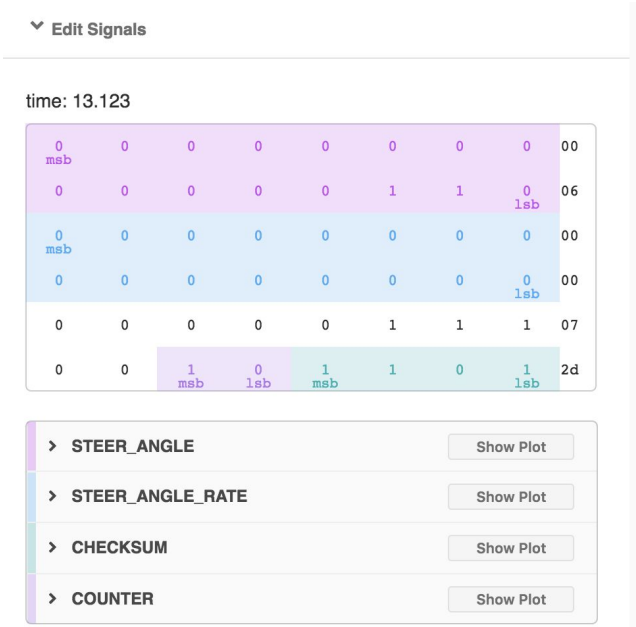
Data field of each ID has a fixed meaning

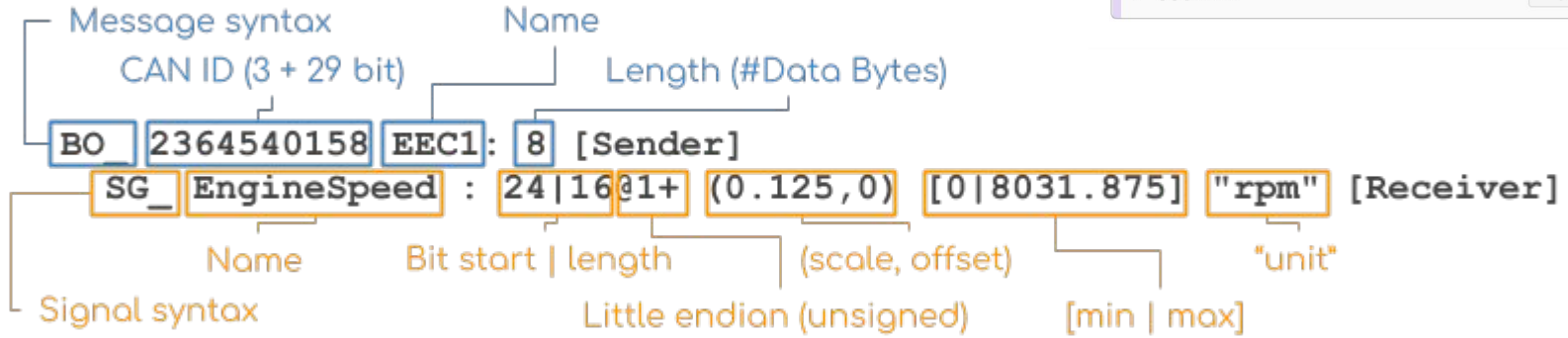
Each ECU “subscribes” to a list of IDs and knows the meaning of their data

Majority of packets are periodic

Controller Area Network: Data

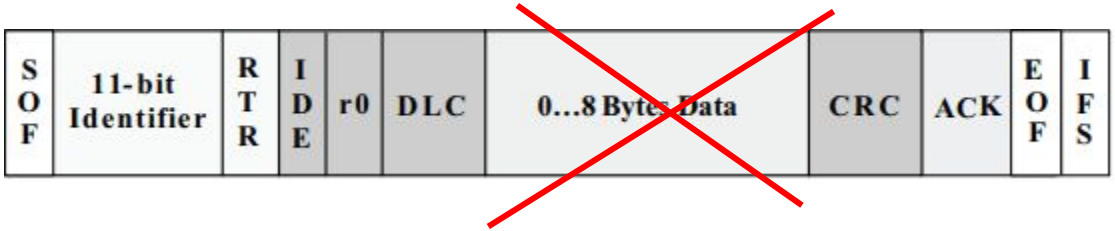
DBC files (proprietary) describe well what's inside the data field of each ID





Controller Area Network: Remote Frames

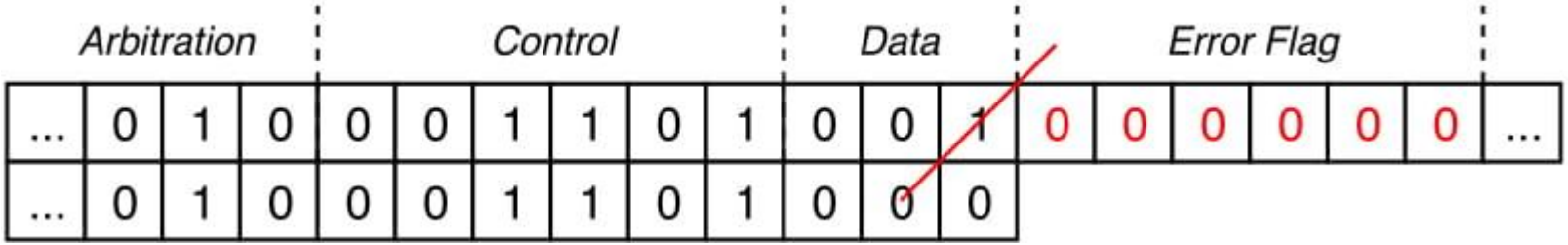
Data frames used for requests. Not often seen.



Controller Area Network: Error Frames

6 bit time sequences of zeroes or ones. Used to say that the current data/remote frame has to be considered not valid

Reasons:
Sender ECU sent a wrong bit
Receiver ECU reads something non CAN-compliant
Conflict on the bus



Controller Area Network: Overload Frames

Error frames sent while bus is idle to request a pause from transmission - not often used in newer ECUs

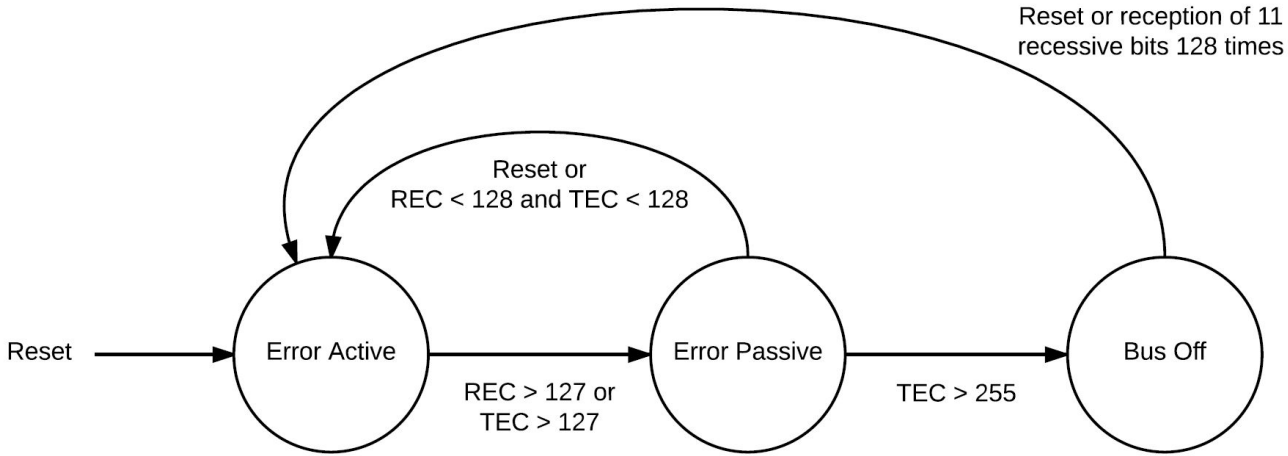
Controller Area Network: Error Handling

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 any counter reaches 128 the unit goes into Error Passive state
- When the transmit error counter reaches 256 the units shuts down the CAN controller

Controller Area Network: Fault Confinement

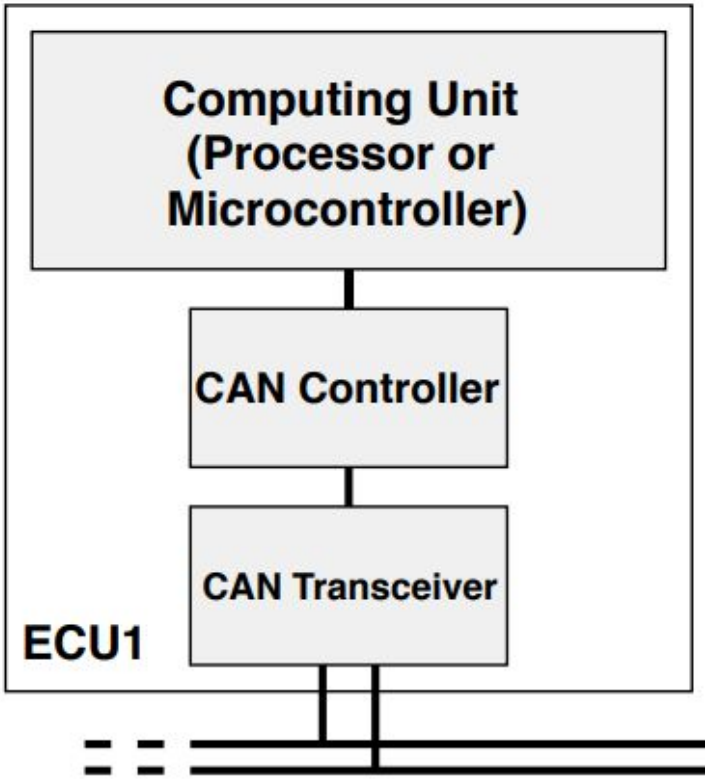


Controller Area Network

Processor is the application layer

CAN controller reads the bits and translates them in actual packets with meaning

CAN transceiver translates only electric signals in bits and vice-versa



Controller Area Network: Example Log

Only data frames (and remote, rarely). All others are “removed” by the CAN transceiver in advance.

https://www.sciencedirect.com/science/article/pii/S2352340920300433

CAN higher layers: OBD-II diagnostics

Mandatory in many countries, almost always present

Enables reporting and self-diagnostics of the whole network

PID (hex)	PID (Dec)	Data bytes returned	Description	Min value	Max value	Units	Formula[a]
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 speed	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	Mass air flow sensor (MAF) air flow rate	0	655.35	grams/sec	$\frac{256A + B}{100}$
11	17	1	Throttle position	0	100	%	$\frac{100}{255}A$

CAN higher layers: ISO-TP

Enables Multi-packet Messaging

Used for OBD-II diagnostics too

Type	Code	Description
Single frame	0	The single frame transferred contains the complete payload of up to 7 bytes (normal addressing) or 6 bytes (extended addressing)
First frame	1	The first frame of a longer multi-frame message packet, used when more than 6/7 bytes of data segmented must be communicated. The first frame contains the length of the full packet, along with the initial data.
Consecutive frame	2	A frame containing subsequent data for a multi-frame packet
Flow control frame	3	the response from the receiver, acknowledging a First-frame segment. It lays down the parameters for the transmission of further consecutive frames.
	4..15	Reserved

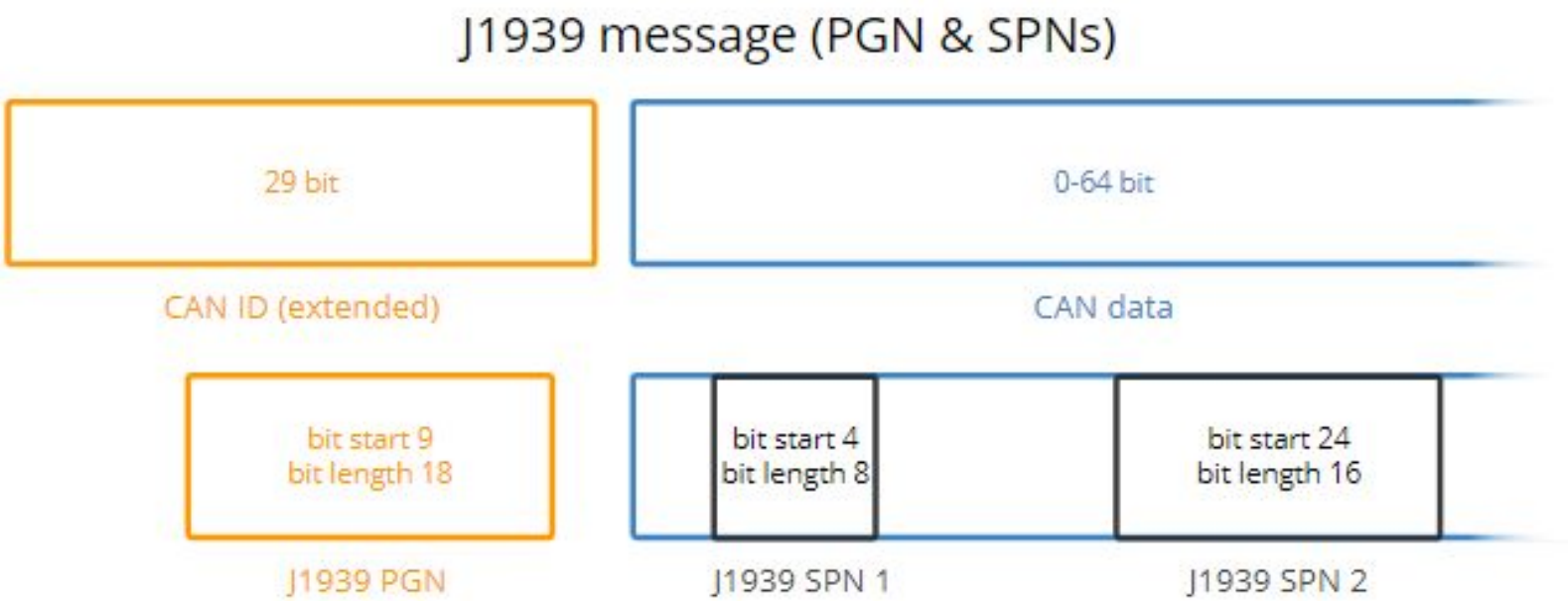
CAN higher layers: J1939

Higher Layer Protocol that uses CAN as a transfer protocol.

Used mainly by “bigger” vehicles (Agricultural, Buses, Ships, Military…)

Its main scope is to enable messaging longer than 8 bytes (i.e. sent in multiple CAN packets)

CAN higher layers: J1939



CAN higher layers: J1939

PGN61444 - Electronic Engine Controller 1 - EEC1

Transmission Repetition Rate: Engine speed dependent
Data Length: 8 bytes
Data Page: 0
PDU Format: 240
PDU Specific: 4
Default Priority: 3
Parameter Group Number: 61444 (0x00F004)

Bit Start/Byte	Length	SPN ID	SPN Description
1.1	4 bits	899	Engine Torque Mode
2	1 byte	512	Driver's Demand Engine - % Torque
3	1 byte	513	Actual Engine - Percent Torque
4-5	2 bytes	190	Engine Speed
6	1 byte	1483	SA of Controlling Device for Engine Control
7.1	4 bits	1675	Engine Starter Mode
8	1 byte	2432	Engine Demand - Percent Torque

CAN higher layers: J1939

CAN ID	Data bytes
0CF00401	FF FF FF 68 13 FF FF FF

PGN	61444
SPN	190
Bit start	24
Bit length	16
Resolution	0.125 rpm/bit
Offset	0
Min	0
Max	8031.875

CAN higher layers: J1939

Messages can be also multi-packet:

In the first packet we receive the layout (PGN + number of successive packets)

Each successive packet has the first data byte used to count and the other 7 carry data.

CAN higher layers: Unified Diagnostic Services

Diagnostic communication protocol widely used to ask specific ECUs to answer diagnostic questions, make diagnostic tests, and similar.

The majority of the “requests” are accessible only once authenticated with the ECU

POLITECNICO
MILANO 1863

DIPARTIMENTO DI ELETTRONICA
INFORMAZIONE E BIOINGEGNERIA

POLITECNICO MILANO 1863
NECST laboratory

AUTOMOTIVE ATTACKS

Automotive Attacks: History

- Hoppe et al 2008 - Tire pressure monitoring
- Koscher et al. 2010 - On-board attacks
- Checkoway et al 2011 - Remote attack surfaces
- Miller & Valasek 2013/15/16 - Actual attacks

Automotive Attacks: History

Automotive Attacks: History

Automotive Attacks

Risks	Goals (CIA triad)
Safety	Confidentiality
Privacy	Integrity
Financial	Availability

Confidentiality

Information is not made available or disclosed to unauthorized individuals, entities, or processes

Integrity

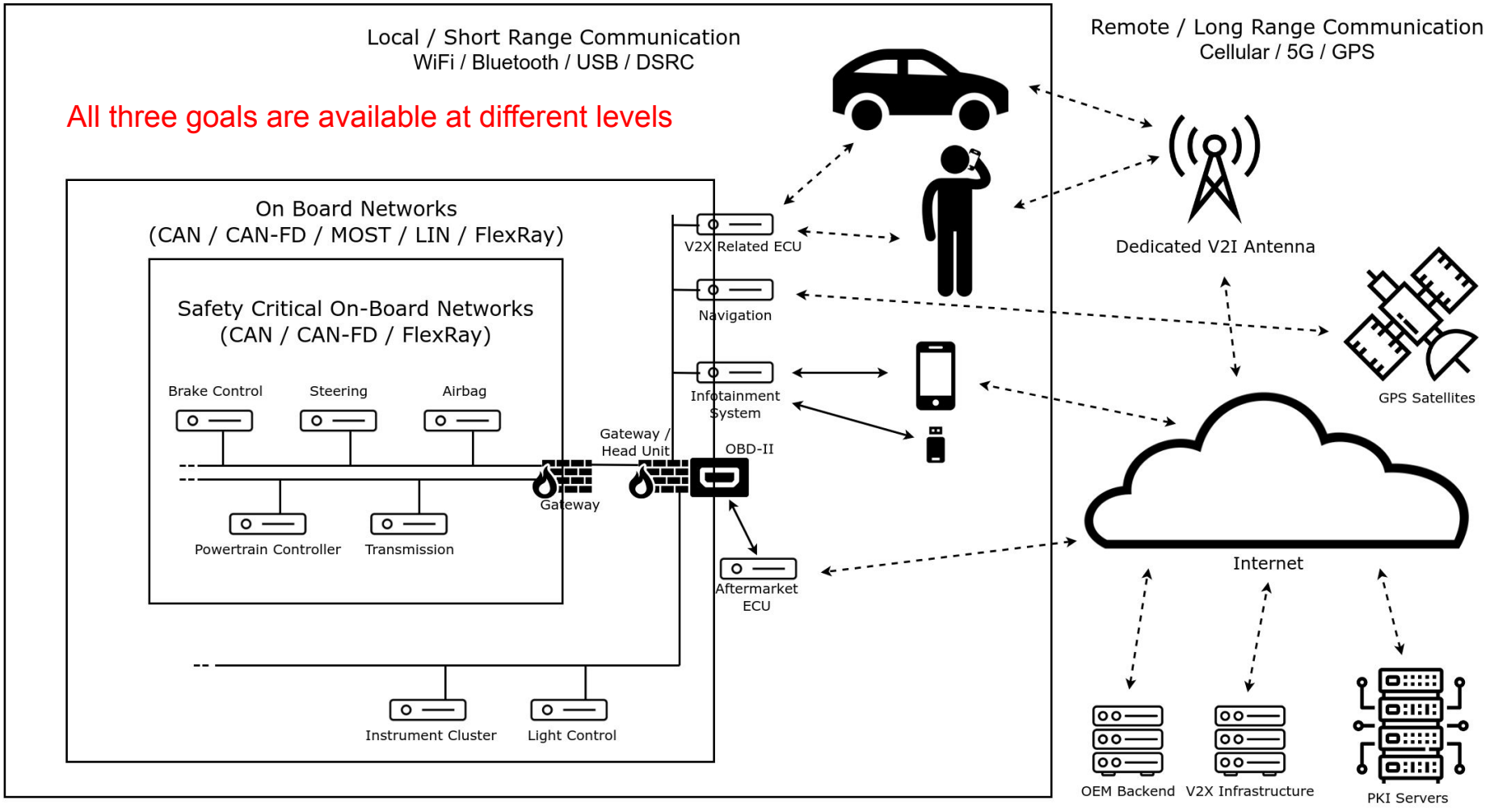
Assuring the accuracy and completeness of data over its entire lifecycle.This means that data cannot be modified in an unauthorized or undetected manner.

Availability

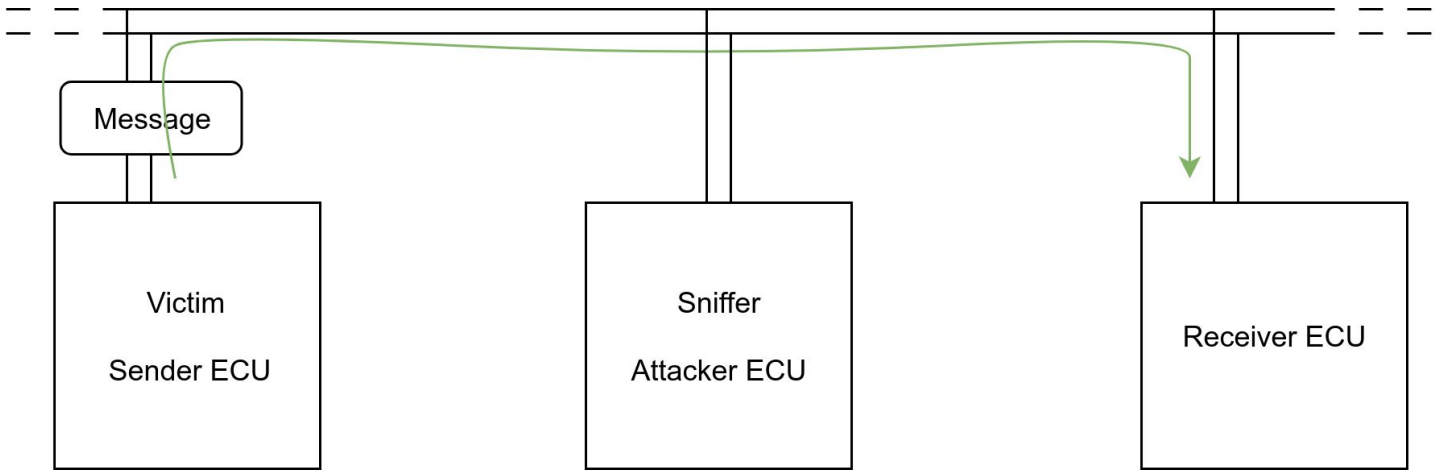
For any information system to serve its purpose, the information must be available when it is needed.

Attack Goals

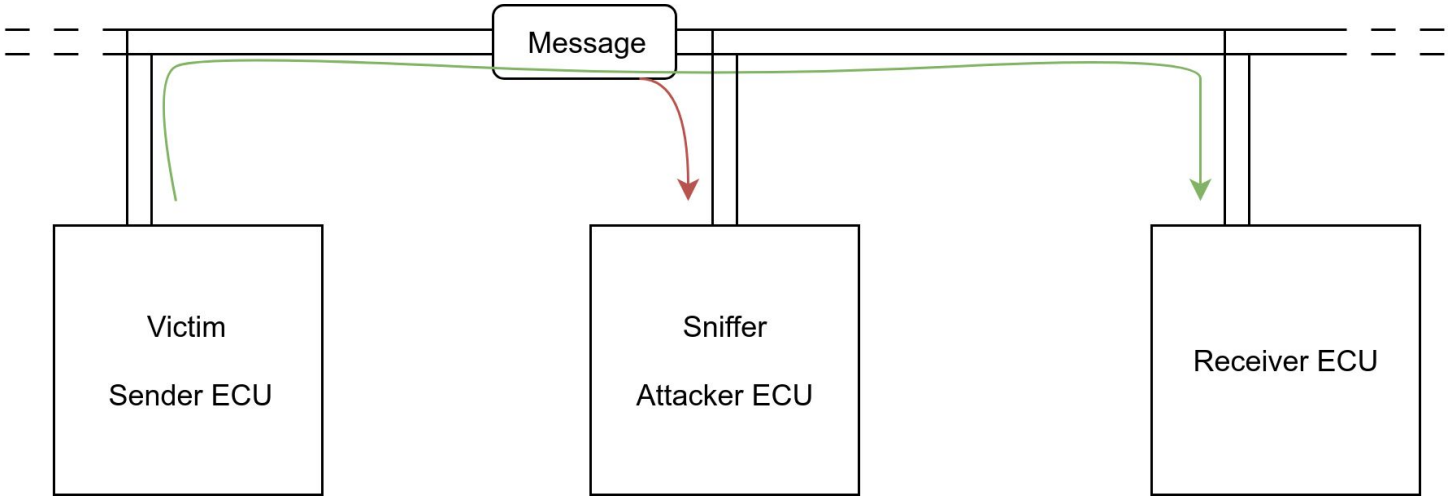
● Confidentiality	->	Sniffing
● Integrity	->	Spoofing
● Availability	->	Denial of Service


Local / Short Range Communication
WiFi / Bluetooth / USB / DSRC
Remote / Long Range Communication
Cellular / 5G / GPS
All three goals are available at different levels
On Board Networks
(CAN / CAN-FD / MOST / LIN / FlexRay)
Safety Critical On-Board Networks
(CAN / CAN-FD / FlexRay)
Brake Control
Steering
Airbag
Powertrain Controller
Transmission
Gateway
Gateway /
Head Unit
OBD-II
V2X Related ECU
Navigation
Infotainment
System
Aftermarket
ECU
Instrument Cluster
Light Control
Dedicated V2I Antenna
GPS Satellites
Internet
OEM Backend
V2X Infrastructure
PKI Servers

CAN Sniffing



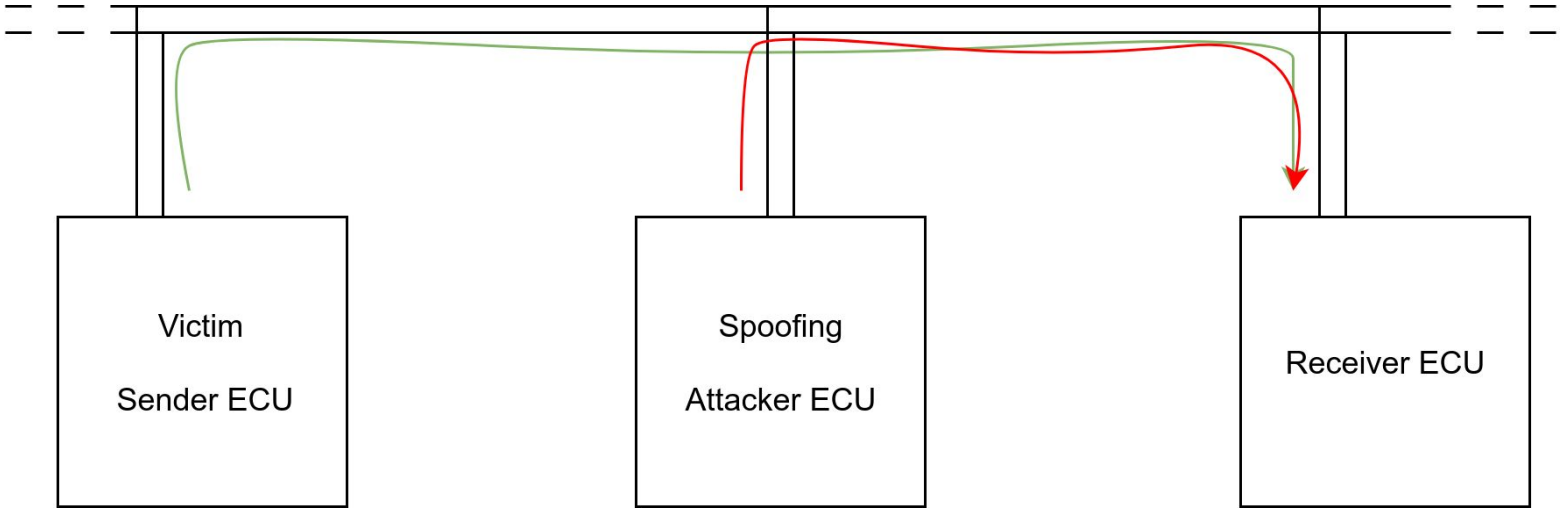
CAN Sniffing



CAN Spoofing

Pretty straightforward, sending messages with any ID is accepted in CAN. Even ones owned by other ECUs.

A basic receiver accepts ALL messages.



CAN Spoofing

Common spoofing attacks:

1) Masquerade

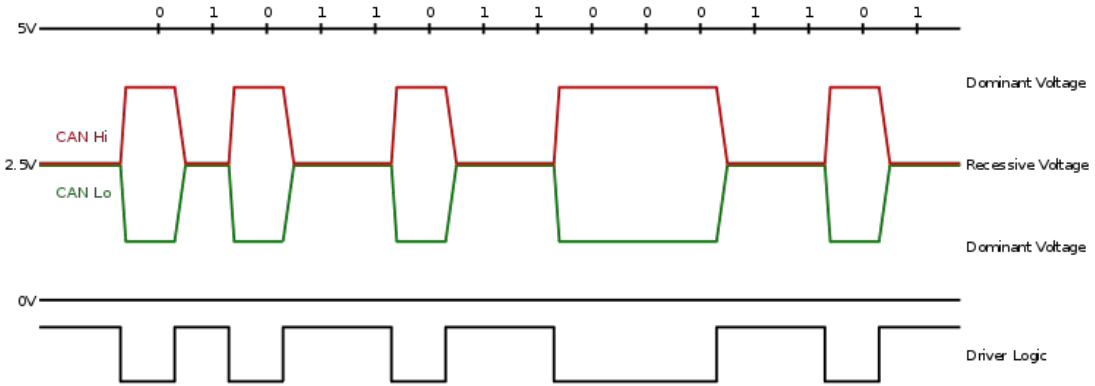
2) Replay

3) Fuzzing

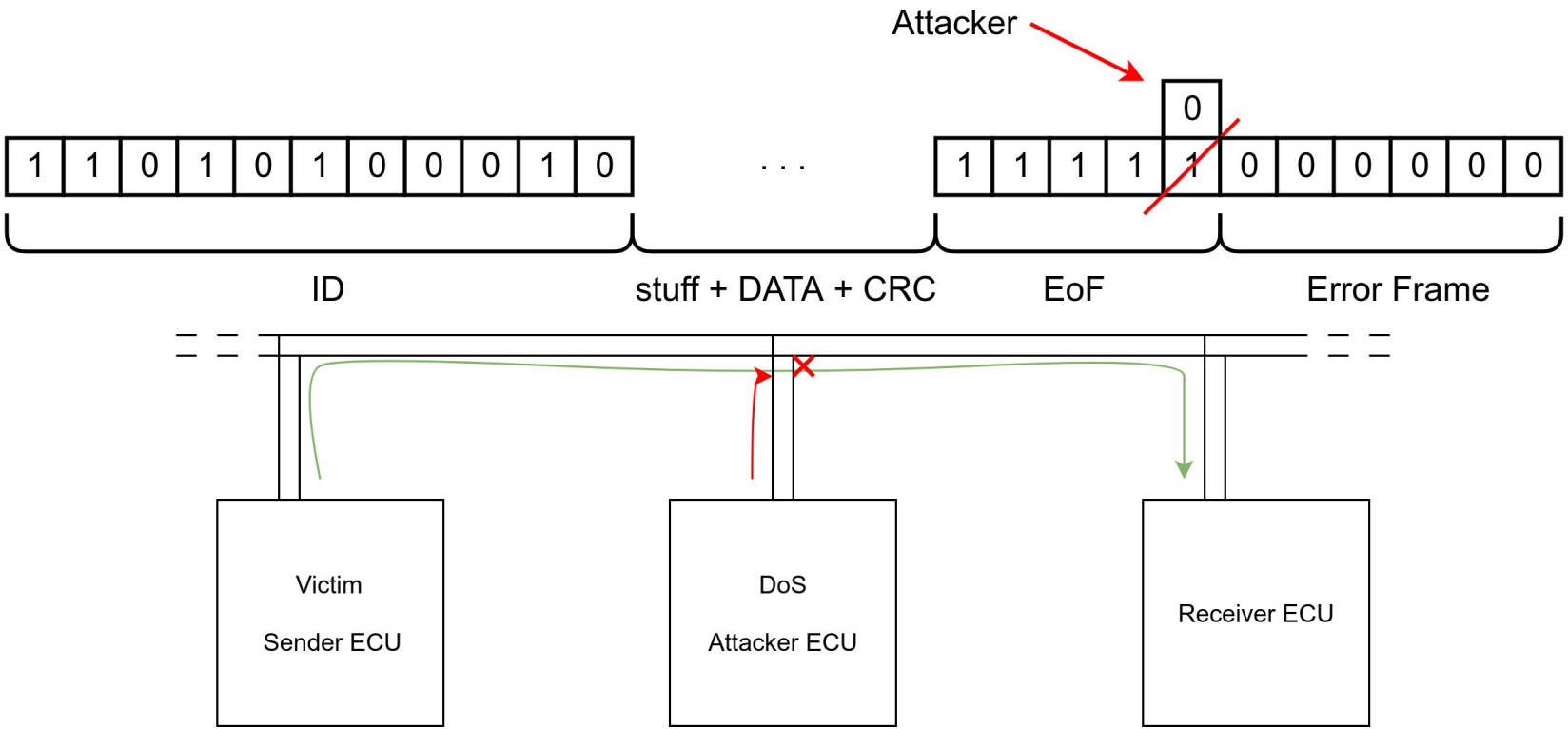
CAN Denial of Service

Recessive is deleted by Dominant Bit

CSMA/BA property: An attacker can ALWAYS win arbitration



CAN Targeted Denial of Service



CAN Practical attack examples

http://illmatics.com/car_hacking.pdf

http://illmatics.com/Remote%20Car%20Hacking.pdf

http://illmatics.com/can%20message%20injection.pdf

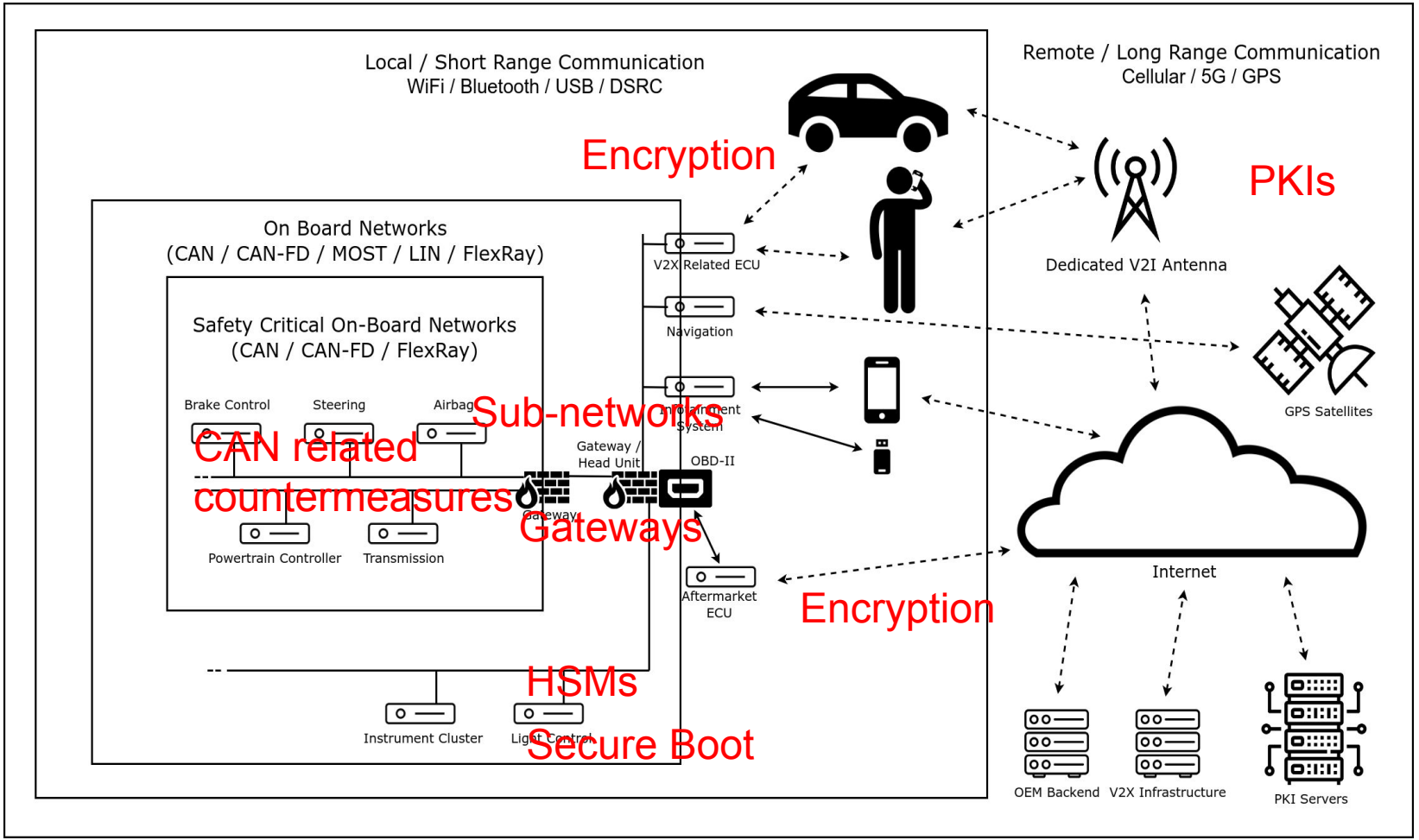
https://docs.google.com/presentation/d/1Js82wcBiDPJHvLL2d6lOWGITZh-tIF8E-OhghtL80PE/edit?usp=sharing

POLITECNICO
MILANO 1863

DIPARTIMENTO DI ELETTRONICA
INFORMAZIONE E BIOINGEGNERIA

POLITECNICO MILANO 1863
NECST laboratory

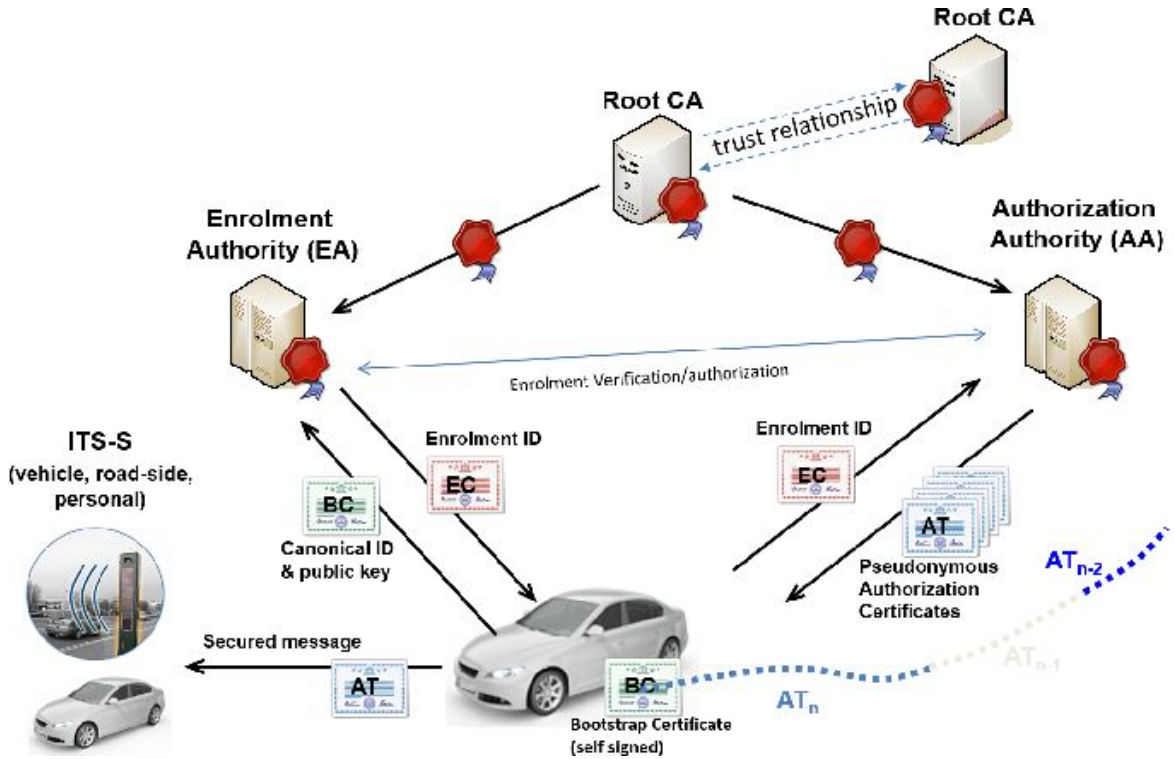
COUNTERMEASURES


Local / Short Range Communication
WiFi / Bluetooth / USB / DSRC
Remote / Long Range Communication
Cellular / 5G / GPS
Encryption
PKIs
On Board Networks
(CAN / CAN-FD / MOST / LIN / FlexRay)
V2X Related ECU
Dedicated V2I Antenna
Navigation
Safety Critical On-Board Networks
(CAN / CAN-FD / FlexRay)
Brake Control
Steering
Airbag
Infotainment System
GPS Satellites
Sub-networks
CAN related countermeasures
Gateway / Head Unit
OBD-II
Gateway
Gateways
Powertrain Controller
Transmission
Internet
Aftermarket ECU
Encryption
HSMs
Secure Boot
Instrument Cluster
Light Control
OEM Backend
V2X Infrastructure
PKI Servers

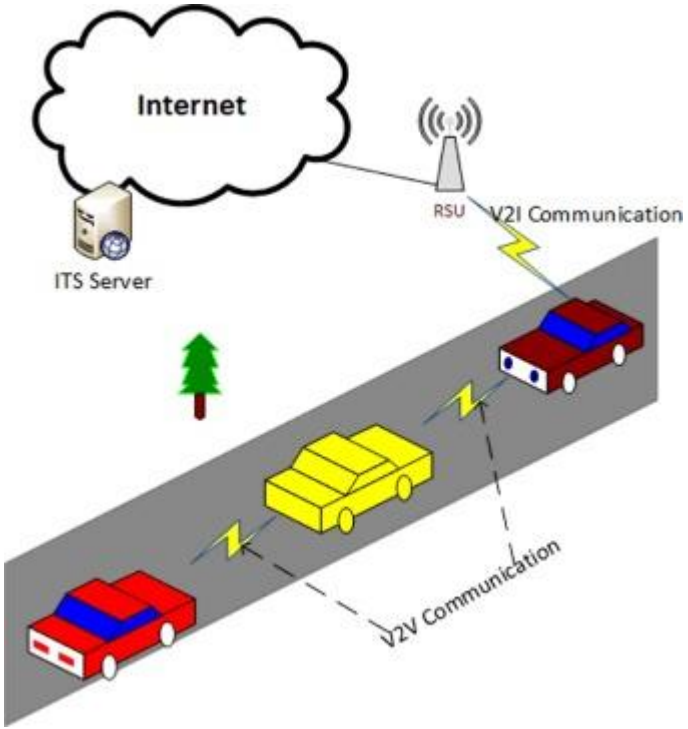
PKI

Requires Pseudonyms (privacy)

Ensures sender's entity



PKI



Sending and receiving traffic data

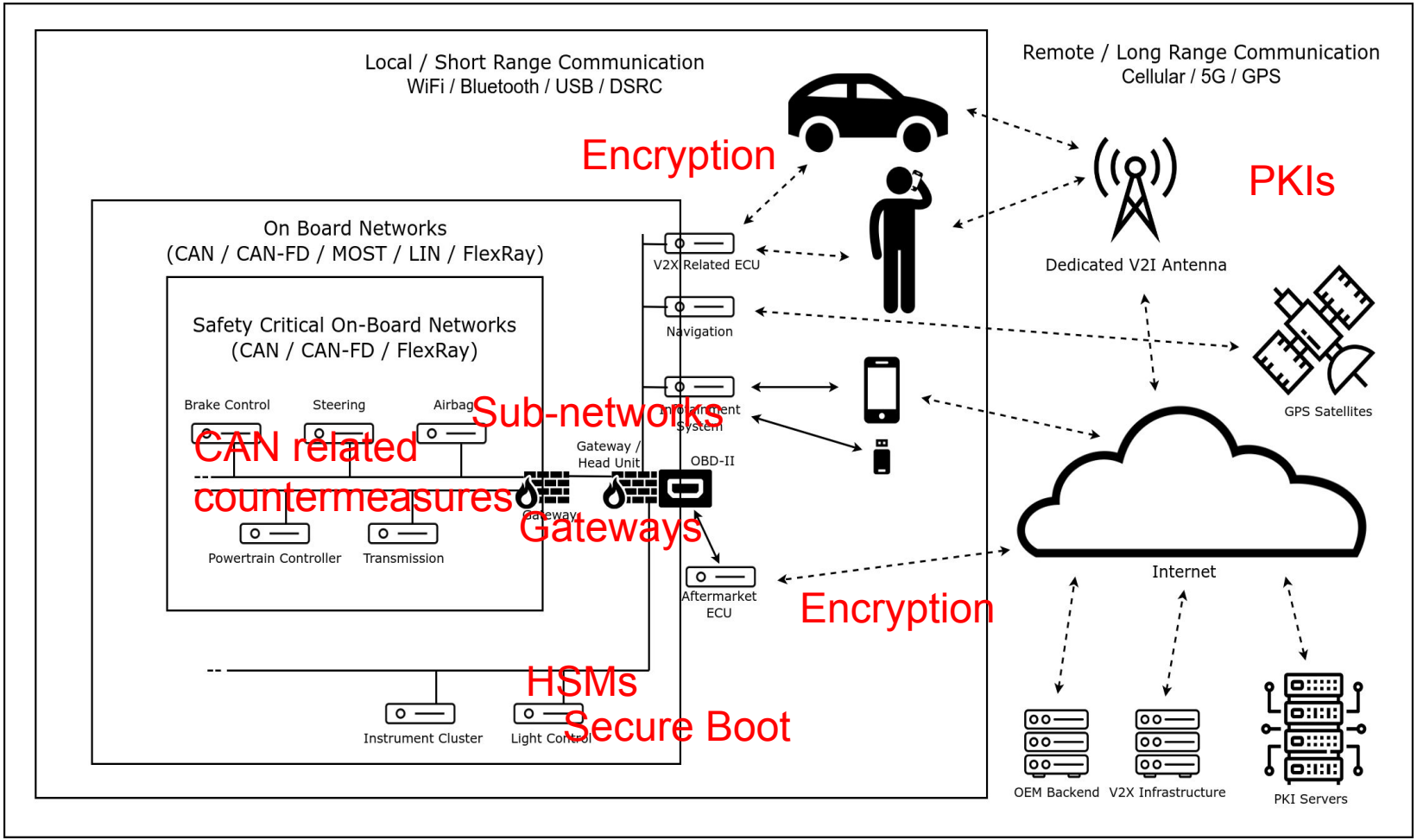
Sending status updates

Receiving software updates

Phone calls

Internet navigation

…


Local / Short Range Communication
WiFi / Bluetooth / USB / DSRC
Remote / Long Range Communication
Cellular / 5G / GPS
Encryption
PKIs
On Board Networks
(CAN / CAN-FD / MOST / LIN / FlexRay)
V2X Related ECU
Dedicated V2I Antenna
Navigation
Safety Critical On-Board Networks
(CAN / CAN-FD / FlexRay)
Brake Control
Steering
Airbag
Sub-networks
CAN related
countermeasures
Gateway /
Head Unit
OBD-II
GPS Satellites
Gateway
Gateways
Powertrain Controller
Transmission
Aftermarket
ECU
Encryption
Internet
HSMs
Secure Boot
Instrument Cluster
Light Control
OEM Backend
V2X Infrastructure
PKI Servers

ECU security (Secure Boot)

Secure Boot:

1) Trusted code written in production in read only memory
2) Start of execution always from trusted code
3) Trusted code verifies other code through PKI or hash (potentially updated)
4) Other code gets executed

Pro: avoids easy flashing of ECUs

Cons: valid only for the specific ECU on which it is implemented

ECU security (Hardware Security Module)

1) Makes the cryptographic computation
2) Stores keys safely
3) Doesn’t let the ECU communicate directly with the (untrusted) network

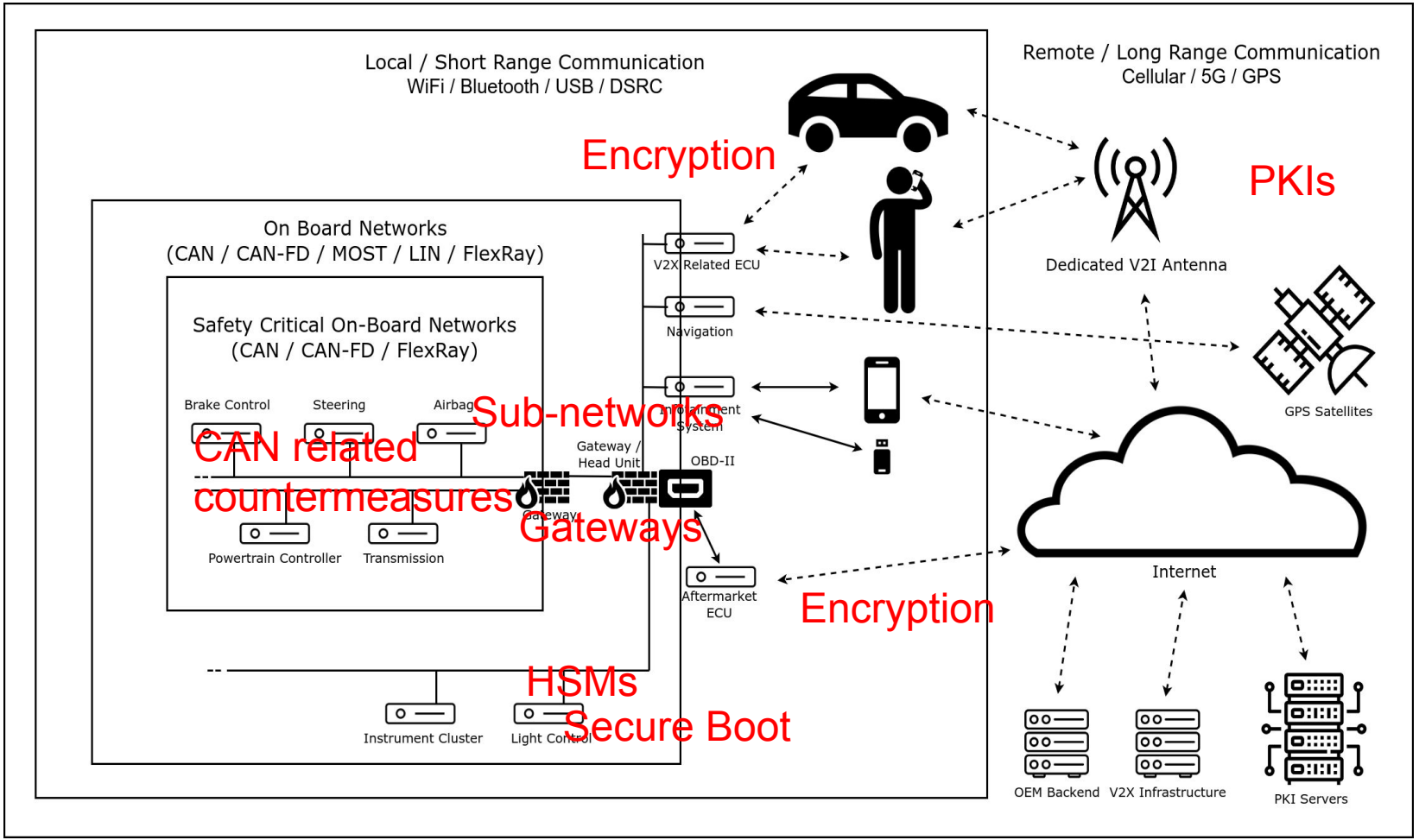
Pros: Increases security of the specific device by shielding it from external threats

Cons: Costs

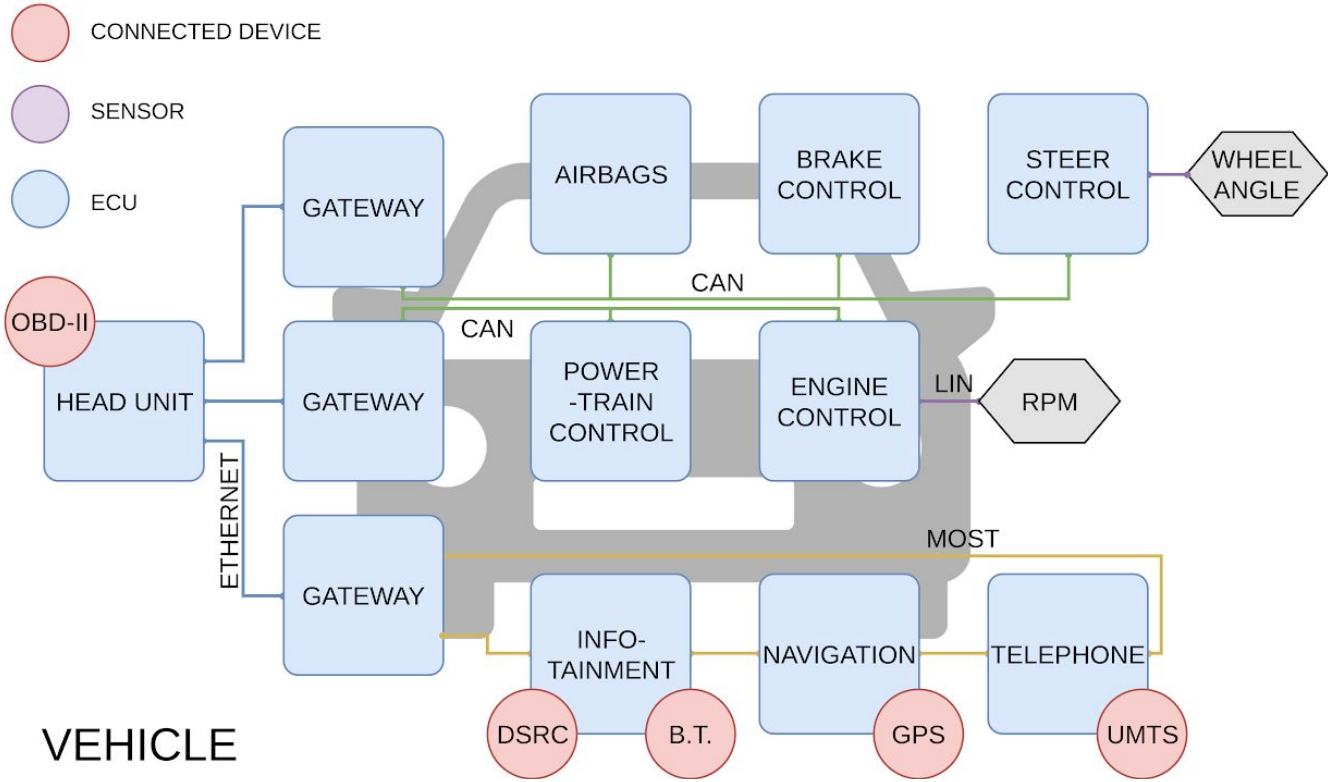
ECU security (OTA secure software updates)

Important to mention, although implemented by the previous technologies.

Enables patching of detected vulnerabilities without recalling the vehicles (Jeep Hack costs were estimated in the tens to hundred millions $ for FCA, since 1.4 million vehicles were recalled)


Local / Short Range Communication
WiFi / Bluetooth / USB / DSRC
Remote / Long Range Communication
Cellular / 5G / GPS
Encryption
PKIs
On Board Networks
(CAN / CAN-FD / MOST / LIN / FlexRay)
V2X Related ECU
Dedicated V2I Antenna
Navigation
Safety Critical On-Board Networks
(CAN / CAN-FD / FlexRay)
Brake Control
Steering
Airbag
Sub-networks
CAN related
countermeasures
Gateway /
Head Unit
OBD-II
GPS Satellites
Gateway
Gateways
Powertrain Controller
Transmission
Aftermarket
ECU
Encryption
Internet
HSMs
Secure Boot
Instrument Cluster
Light Control
OEM Backend
V2X Infrastructure
PKI Servers

Gateways, subnetworks, firewalls



Gateways, subnetworks, firewalls

Gateways divide one subnetwork from the other, and firewalls (in the GW) avoid unwanted packets to reach critical locations

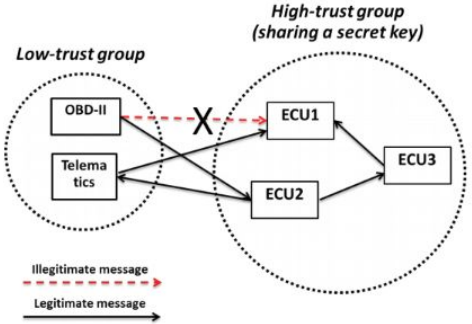
Subnetworks are divided so that critical ECUs are not in contact with externally connected ones

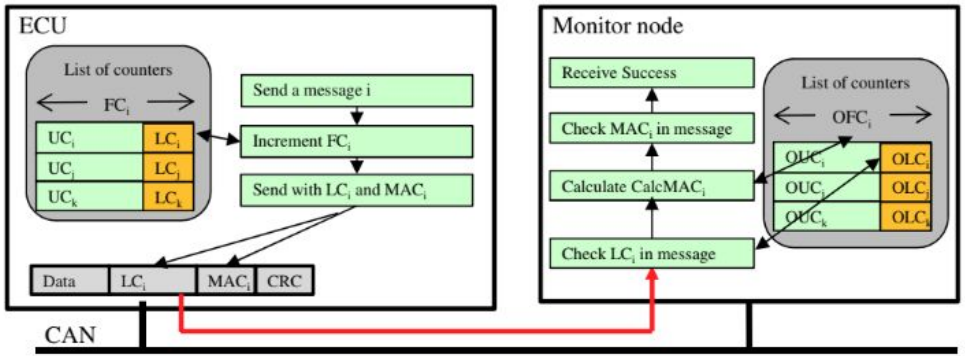
Pros: Gateways are required anyway to translate one kind of network packets to another. Only a small amount are required for the whole network

Cons: Do not defend from packets meant to pass in that GW (e.g.,)

On-board Network Security: Authentication Protocols

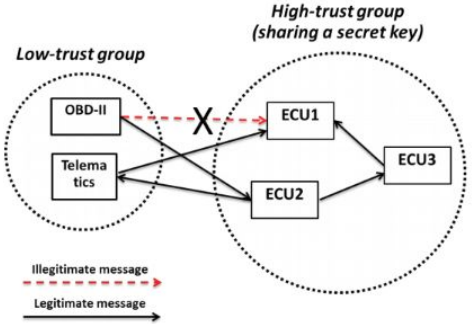
Encrypt / Authenticate the message passing on the CAN (or other) bus

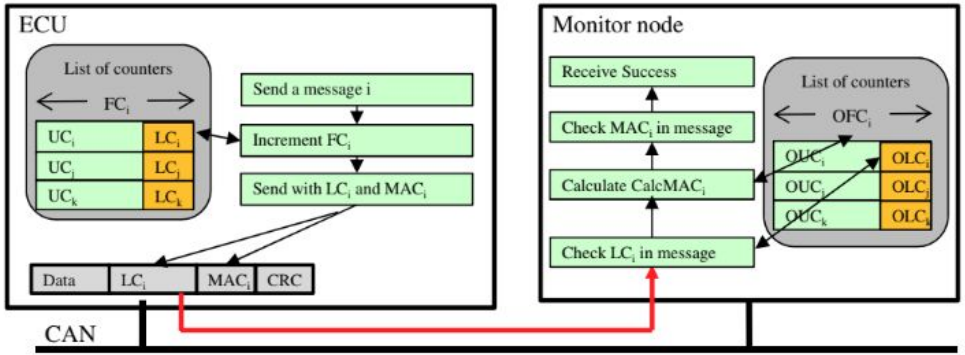




On-board Network Security: Authentication Protocols

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

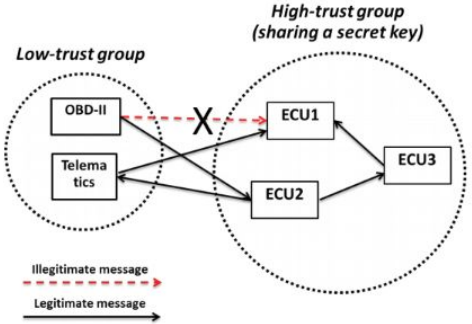


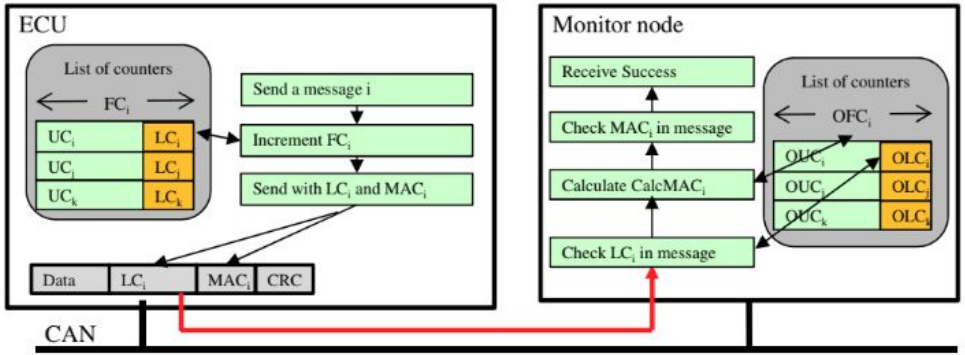


On-board Network Security: Authentication Protocols

Pros: Relatively high security measure, especially if uses an HSM to store keys

Cons: Expensive, slows computation, Increases message overhead/numbers





Generally used only for firmware updates and not even often.

On-board Network Security: Intrusion Detection

A singular (or a small amount) of devices that can read network traffic and analyze it to detect inconsistencies.

On-board Network Security: Intrusion Detection

Frequency Based IDSs:

+ CAN data is usually periodic, and when they are not, they are still sent at a specific frequency
+ Attackers often need to “overwrite” the messages sent by an ECU to convince another one of something (see Miller & Valasek speed)
- If the attacker can send the “writer” off the bus frequency can be kept identical

On-board Network Security: Intrusion Detection

Specification-based IDSs:

a) Physical specifications (e.g., Voltages/Power, …)
b) Logical specifications (ID ownership)
c) Protocol properties (Detect bus-off victim)

\+ Make it impossible for the attacker to exploit some specific vulnerabilities (e.g. buffer overflows due to too high values, Sending an ID from an ECU that was not supposed to send it)

\- Extremely case-specific, hard to generalize. May require testing per-vehicle

On-board Network Security: Intrusion Detection

Payload-based IDSs:

a) Data related rules (e.g., some bits may have fixed values)
b) Multi-value analysis (e.g., speed + rpm + gear)
c) Time-series analysis (e.g., speed increase not realistic)
d) Machine-Learning based rules

\+ Impossible for the attacker to send non-protocol compliant requests
\+ Extremely complex for the attacker to comply to all the rules while being able to implement a meaningful attack
\- Computationally expensive
\- Hard to find rules strict enough and at the same time without false positives

On-board Network Security: Intrusion Reaction

1) Shut Down the attacker? -> Dangerous, also how do I tell?
2) Send Alert? -> to who?
3) Switch to a less “technology-reliant” driving mode?
4) Change IDs
5) Send data to data analysts to patch the problem ←

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 -> CopyCAN and similar (see slides)

https://docs.google.com/presentation/d/1Js82wcBiDPJHvLL2d6lOWGlTZh-tIF8E-OhghtL80PE/edit?usp=sharing

Overall security solution (best case) :

1) Threat analysis is done in advance, while designing the vehicle
2) Penetration testing is done on all ECUs (unrealistic, the most safety critical ones at least)
3) Firewalls are always implemented in gateways, and threat analysis defines the best networks layouts
4) ECUs that expect to have software updates (infotainment system, safety critical ones) are either implemented with an HSM or with a secure implementation of key storage and PKIs
5) An IDS is implemented on board, or part of the data are sent remotely to be analyzed by a more powerful one
6) A teams studies the alerts being sent by different vehicles, understand the current threats and implements patches.

Overall security solution (best case) :

Pros:
Costs are contained
Overall known attacks are (more or less) unfeasible
The reactions can be implemented also on vehicles already on the road

Cons:
The attack being implemented on a specific vehicle is not always stoppable
The patch for an attack may arrive after months

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, it responds through RFID
3) The vehicle opens the doors/ignites the engine

Remote Passive Keyless Entry/Start Systems

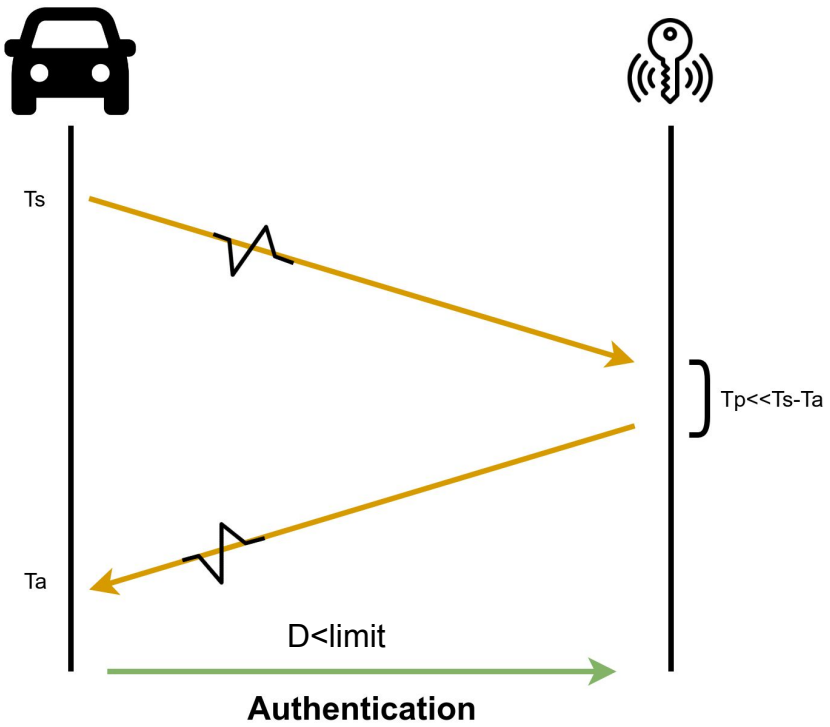
Does it need security? -> Well it is a substitute of the key, so yeah

Does it implement security measures? -> yes

Is it secure? ...


CAR
THEFT

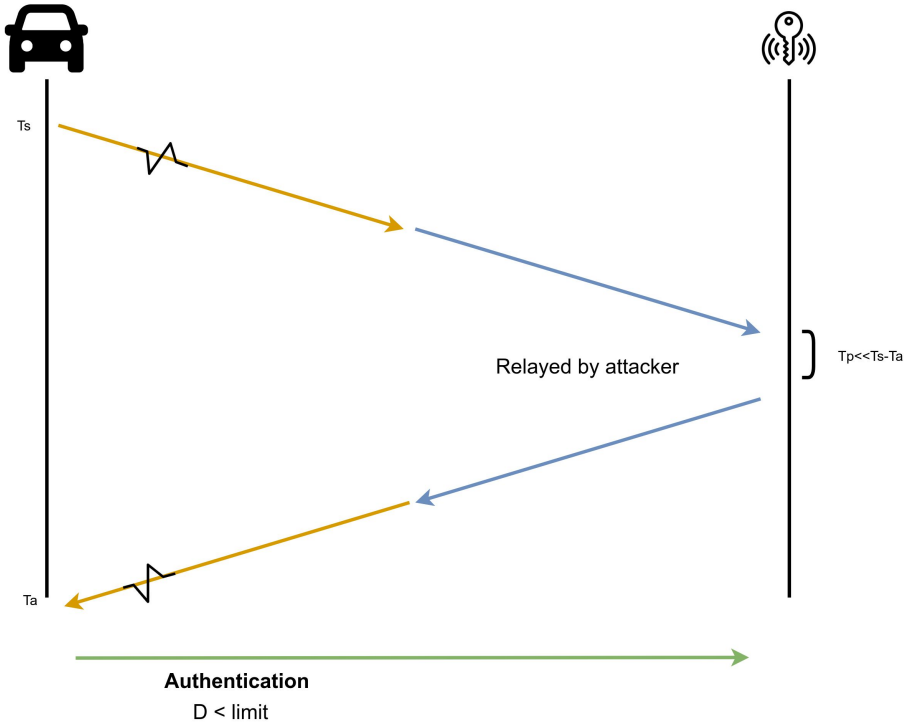
How does RKES work?



1) Single code
2) Rolling code
3) Manufacturer specific global codes
4) Challenge Response

Periodic
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

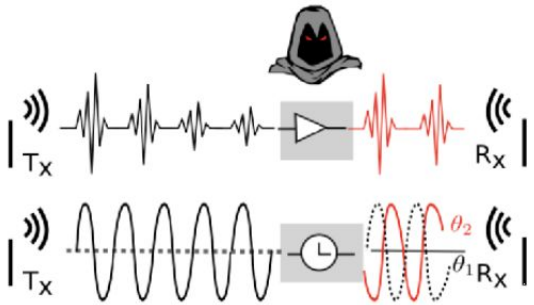
…

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

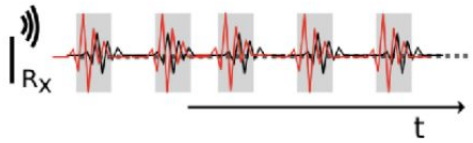
Most secure because basically uncheatable

Known Attacks

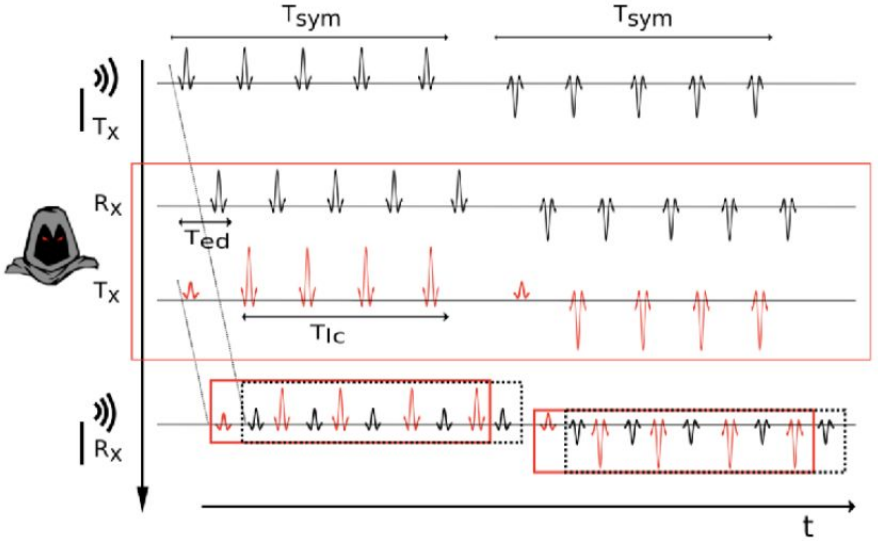
Simple Relay, Phase Relay, Signal Amplification, Early Detect / Late Commit, Cicada, Preamble Advance, …



a) Relay Attack

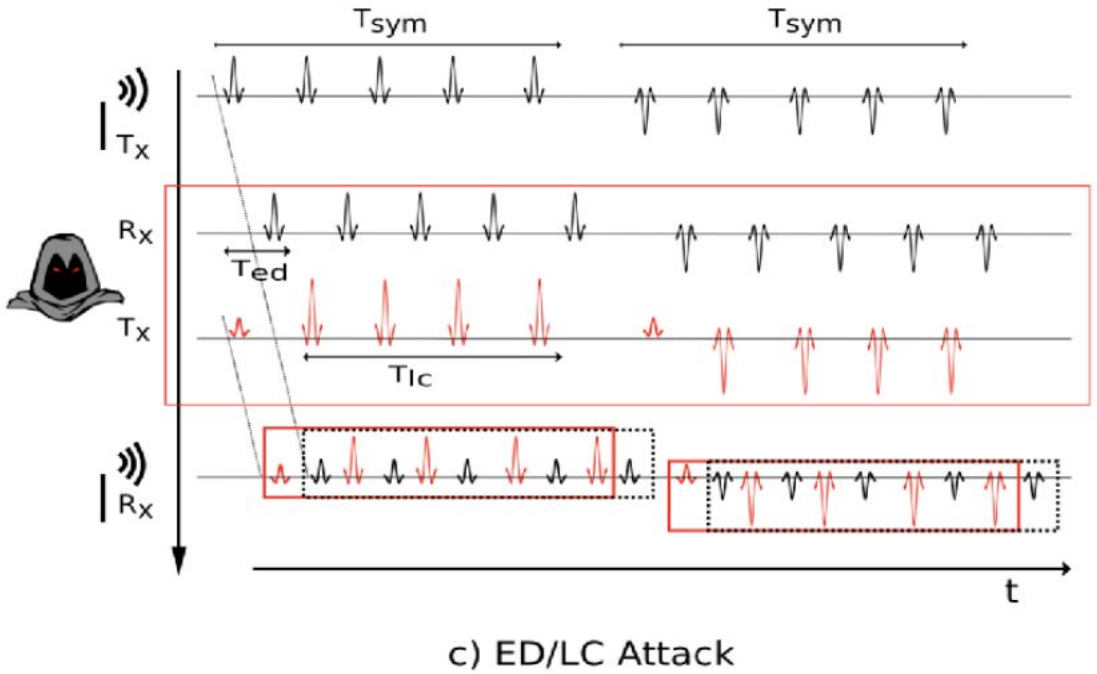


b) Cicada Attack



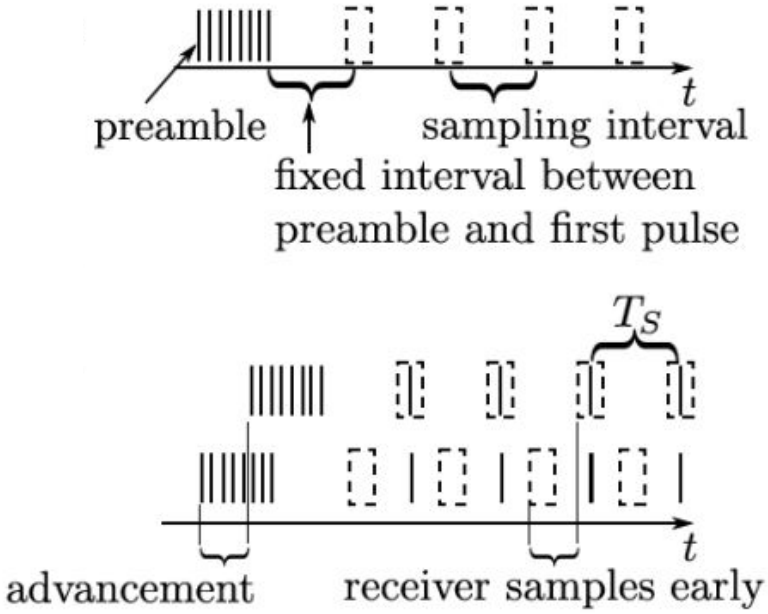
c) ED/LC Attack

Known Attacks: Early Detect/Late Commit

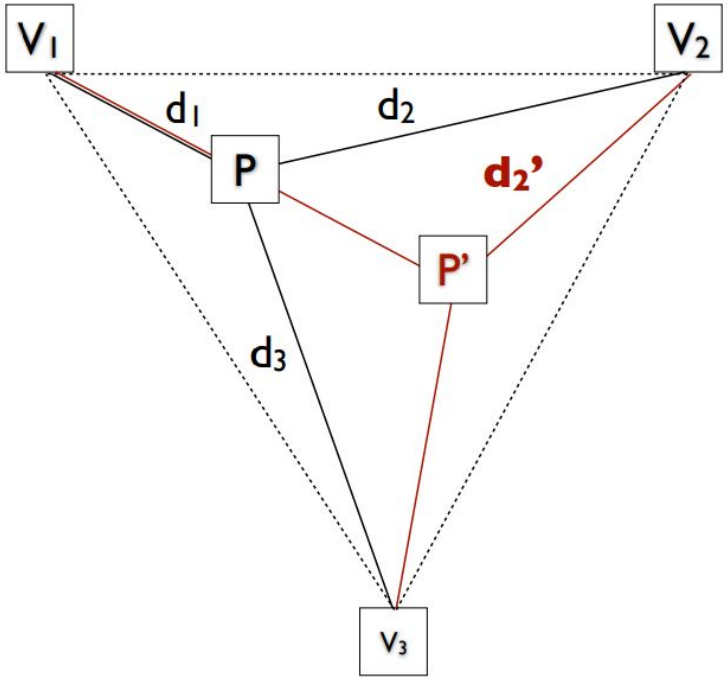


c) ED/LC Attack

Solution: Preamble!

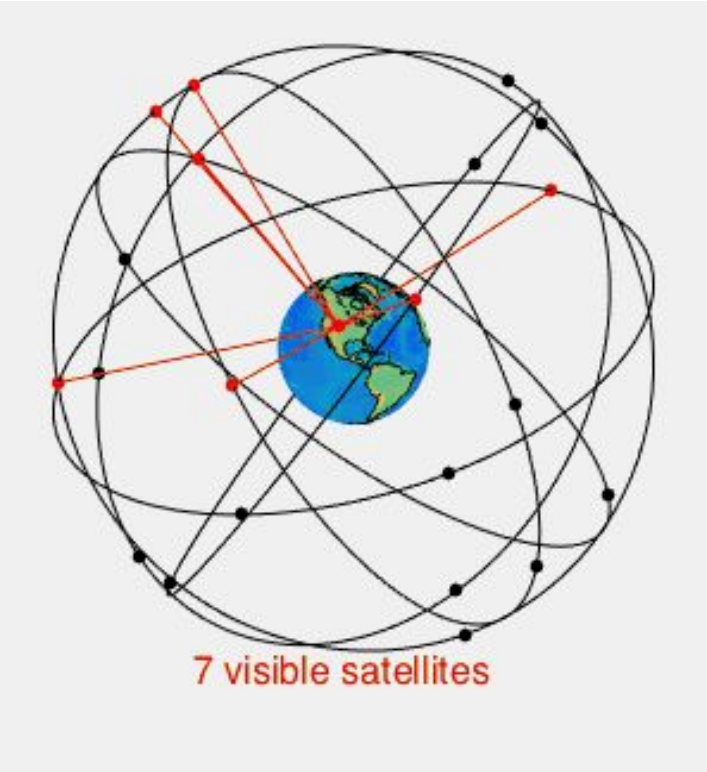


Triangulation OK! (Short Range)



P→P' => d2'<d2

Long Range Positioning: GPS / GNSS



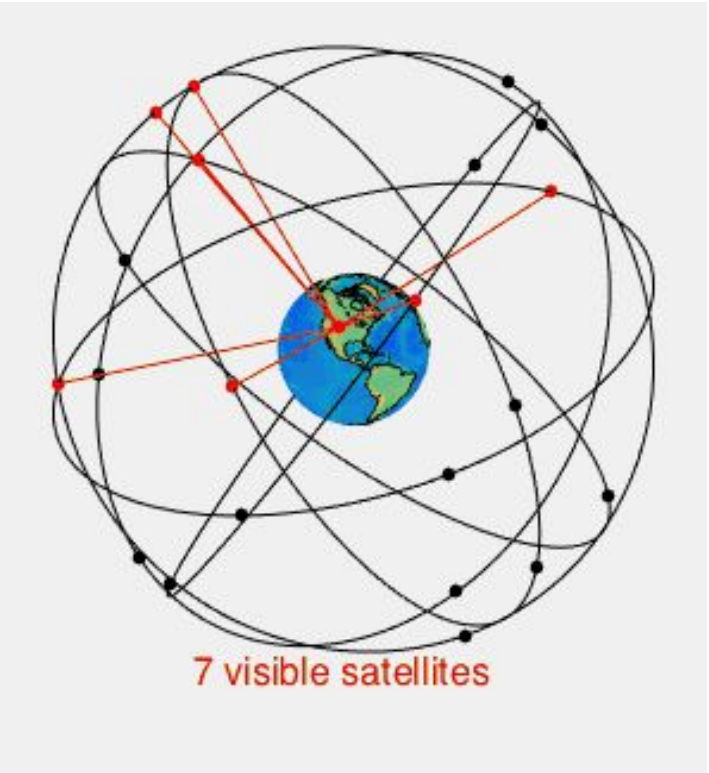
24 satellites at 20.200 Km

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

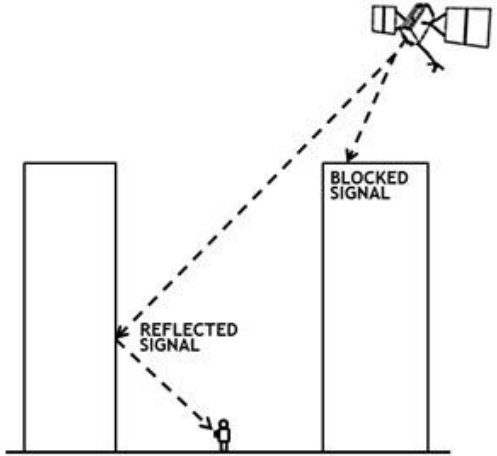
GPS Encryption



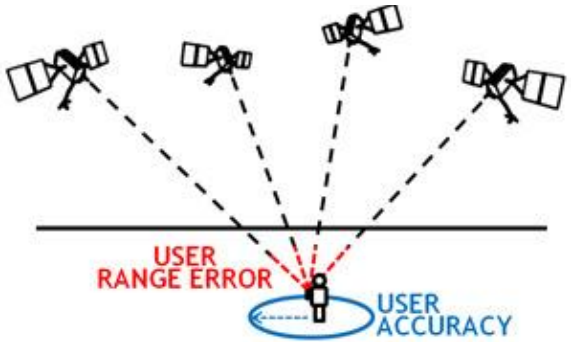
GPS is encrypted ONLY for military purposes.

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

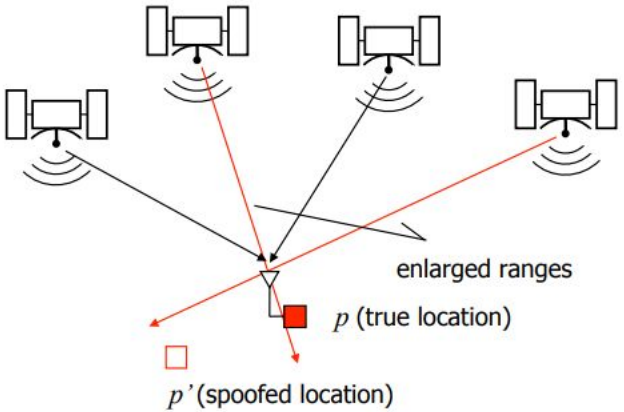
GPS Precision



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

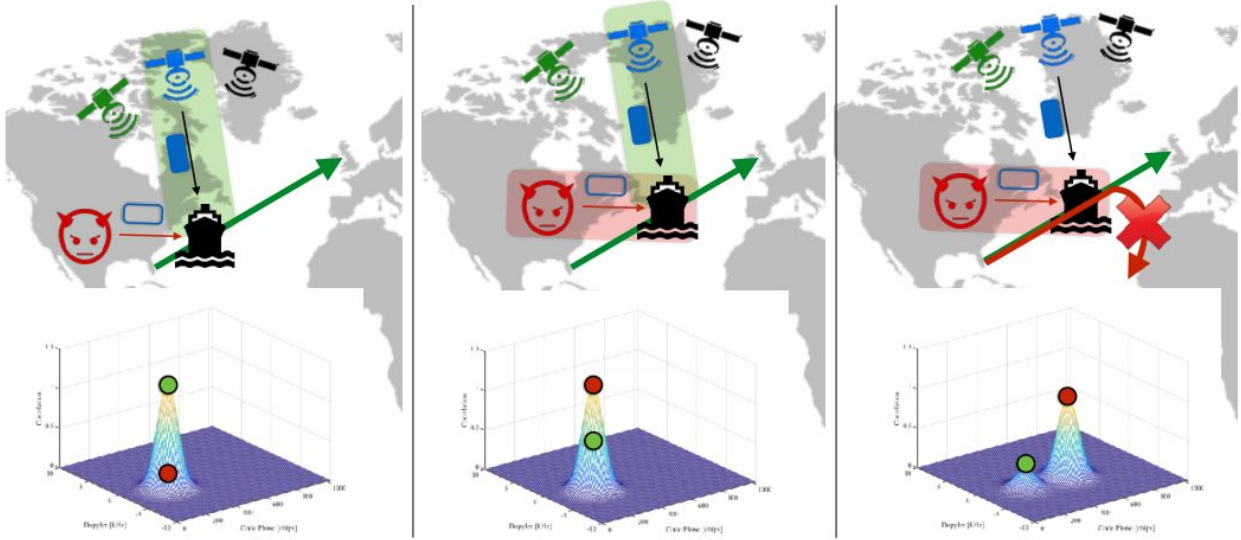
Not changing the protocol:

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

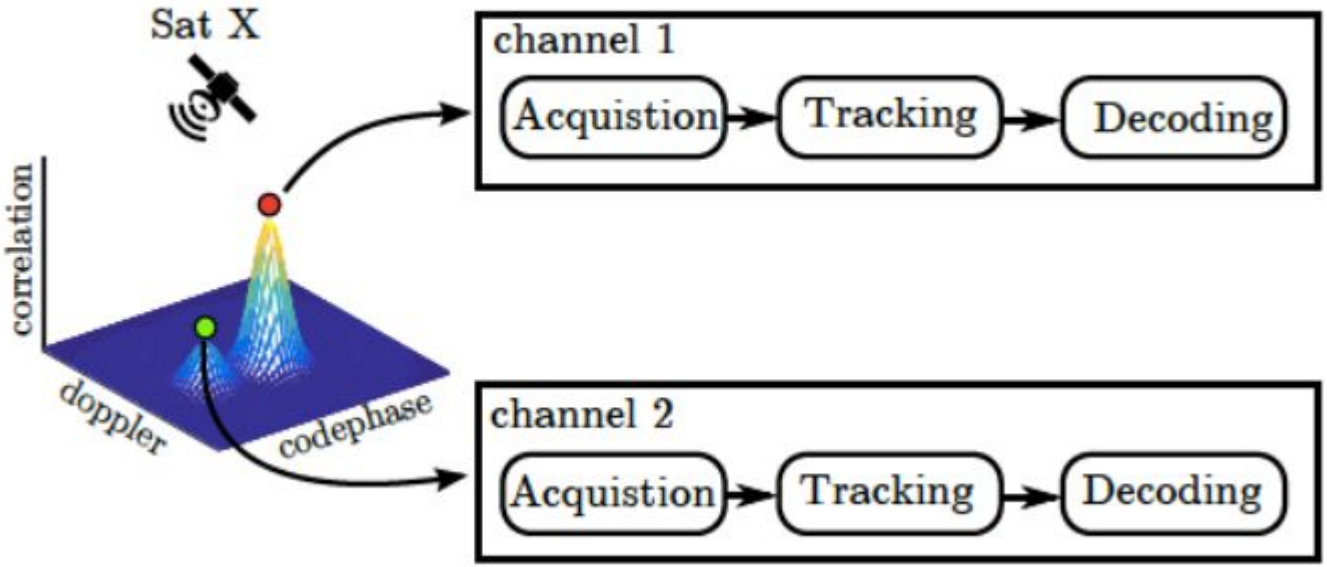
More or less feasible...

GNSS Seamless Takeover Attack

...But counterable

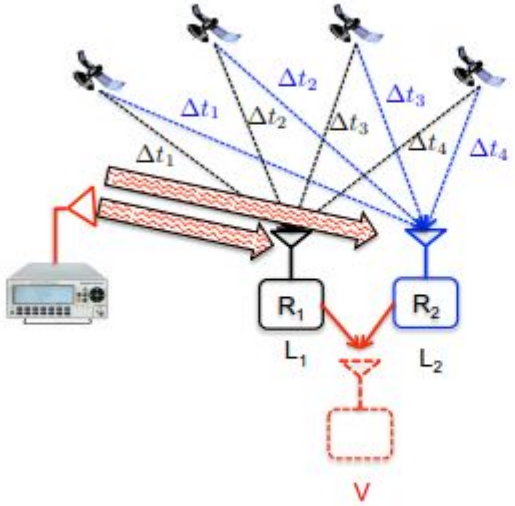


Detection with one receiver: SPREE



Detection with multiple receivers:

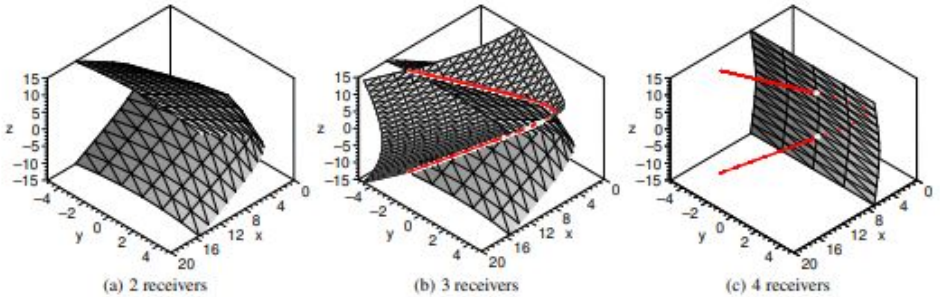
Leverage spatial diversity



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

Detection with multiple receivers:

Spatial diversity and number of nodes constraint the attacker



(a) 2 receivers (b) 3 receivers (c) 4 receivers

	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

POLITECNICO
MILANO 1863

DIPARTIMENTO DI ELETTRONICA
INFORMAZIONE E BIOINGEGNERIA

POLITECNICO MILANO 1863
NECST laboratory

EXERCISE

Go to this link and download the dataset: (password to decrypt: cefriel2020)
https://drive.google.com/file/d/19rYU4nNGR9YloQ3u7qmdbmQBYq6W9IR8/view?usp=sharing

Answer the following questions:
1) which IDs are present in the datasets (same IDs for all datasets)
2) what is the frequency of each ID in the noattack.csv dataset?
3) which attack is being implemented on each log?
4) what IDs are being attacked?
5) what is the goal of the attacker? (if feasible to understand)
6) implement a detector for the specific kind of attack on the specific log