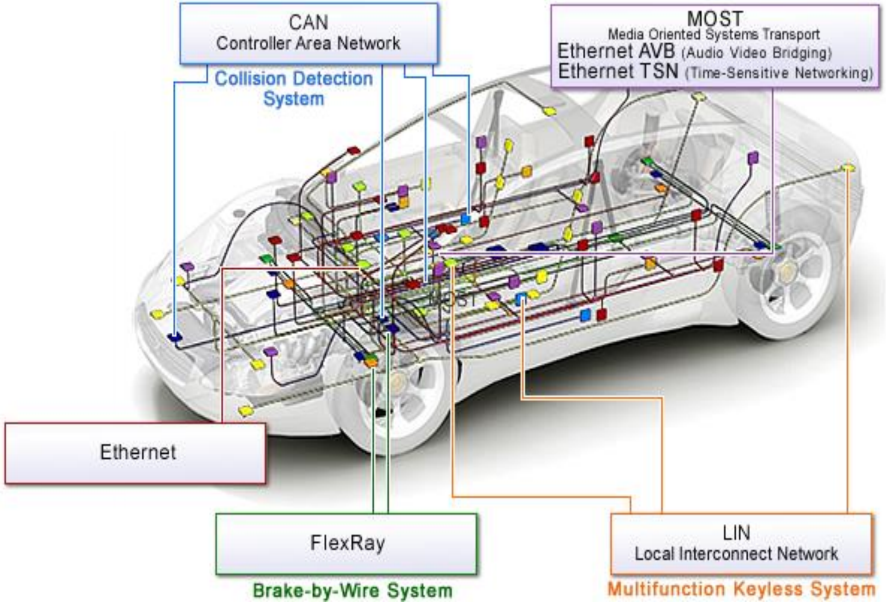
Design and implementation of an intrusion detection system (IDS) for in-vehicle networks

Presented by: *Noräs Salman*
Credits to my thesis partner: *Marco Bresch*

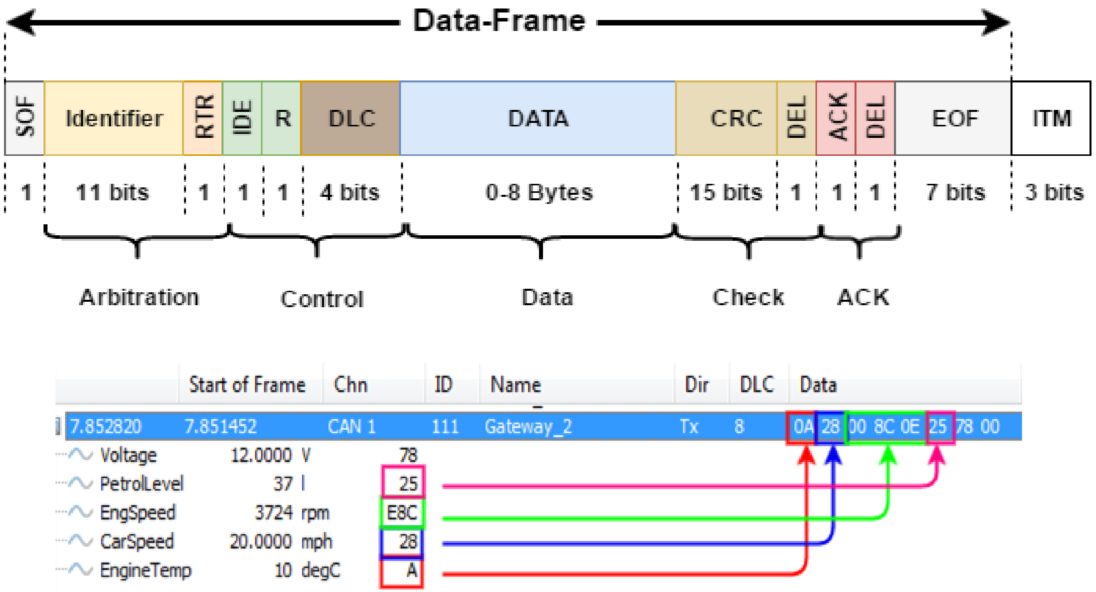
Brief background: in-vehicle networks

- Controller Area Network (CAN)
- MOST
- FlexRay
- LIN
- Ethernet



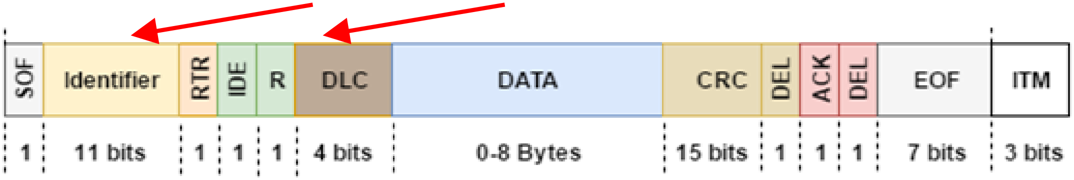
Brief background: CAN (frames & signals)

- Very well defined frame that carries multiple signals.

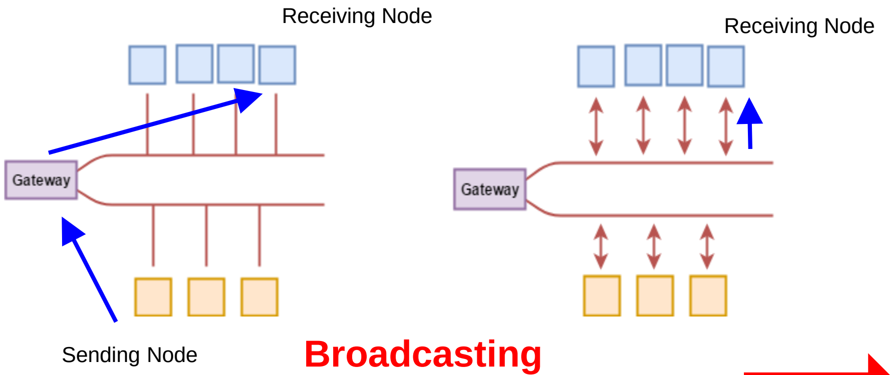


Brief background: CAN (signal database)

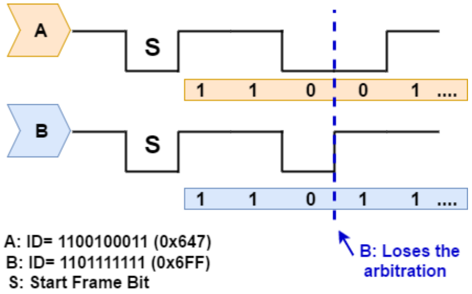
Name	ID	ID-Format	DLC [...	Tx Method	Cycle Time	Transmitter
Console_1	0x1A0	CAN Standard	4	not_used	20	Console
Console_2	0x1A1	CAN Standard	2	not_used	500	Console
DebugMsg1	0x100	CAN Standard	8	not_used	2	-- No Transmit...
Diag_Request	0x700	CAN Standard	8	not_used	2	-- No Transmit...
Diag_Response	0x600	CAN Standard	8	not_used	2	-- No Transmit...
DiagRequest	0x606	CAN Standard	8	not_used	2	-- No Transmit...
DiagResponse_DoorLeft	0x607	CAN Standard	8	not_used	2	DOOR_le
DiagResponse_Motor	0x601	CAN Standard	8	not_used	2	Gateway
DOOR_l	0x1F0	CAN Standard	1	not_used	30	DOOR_le
DOOR_r	0x1F1	CAN Standard	1	not_used	30	DOOR_ri
Gateway_1	0x110	CAN Standard	3	not_used	100	Gateway
Gateway_2	0x111	CAN Standard	8	not_used	2	Gateway
NM_Console	0x41A	CAN Standard	4	not_used	2	Console
NM_DOORleft	0x41B	CAN Standard	4	not_used	2	DOOR_le
NM_DOORright	0x41C	CAN Standard	4	not_used	2	DOOR_ri
NM_Gateway	0x41D	CAN Standard	4	not_used	2	Gateway
TP_Console	0x604	CAN Standard	6	not_used	2	Console
TP_Dashboard	0x605	CAN Standard	6	not_used	2	Dashboard



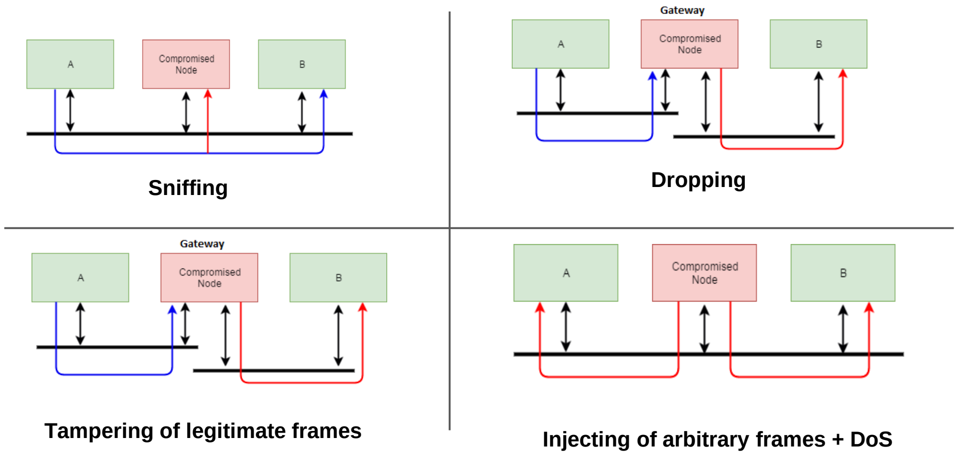
Brief background: CAN security



Broadcasting



Collision Avoidance



Mission briefing

Scientific Questions:

- How is an in-vehicle network IDS designed?
- How to design its rules?
- Limitations and challenges?

→ **Implementation** of an prototype IDS which can detect attacks on the network

Scope:

No prevention and no alarming of attacks, focused on the Controller Area Network

Preceding ideas, efforts and research (defense)

How to defend against in-vehicle networks attacks?

- **Encryption of communication**
- **Cryptographic signatures / certificates**
- **Intrusion Detection Systems**
  - Machine learning approaches
  - Specification-based
  - Anomaly-based

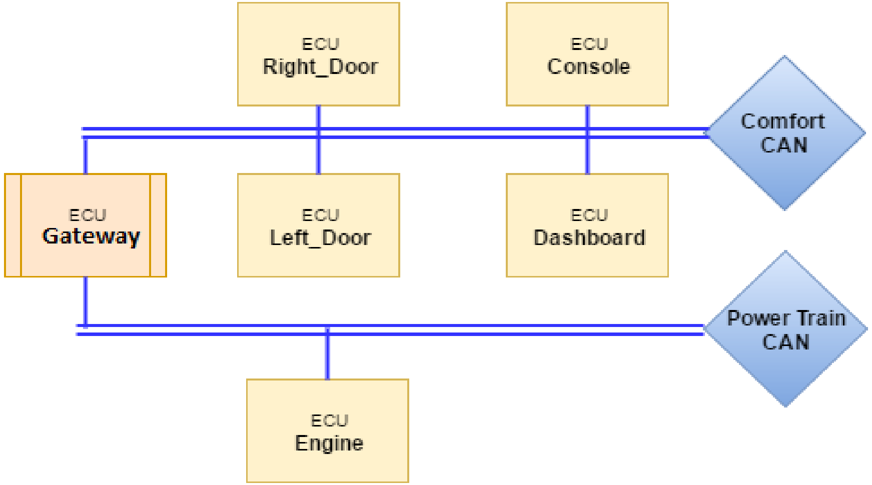
Previous research is **dominated** by anomaly-based solutions

Setup (Simulated network)

- Safer to start with.
- Easy to add nodes
- Can overwrite ECU code.

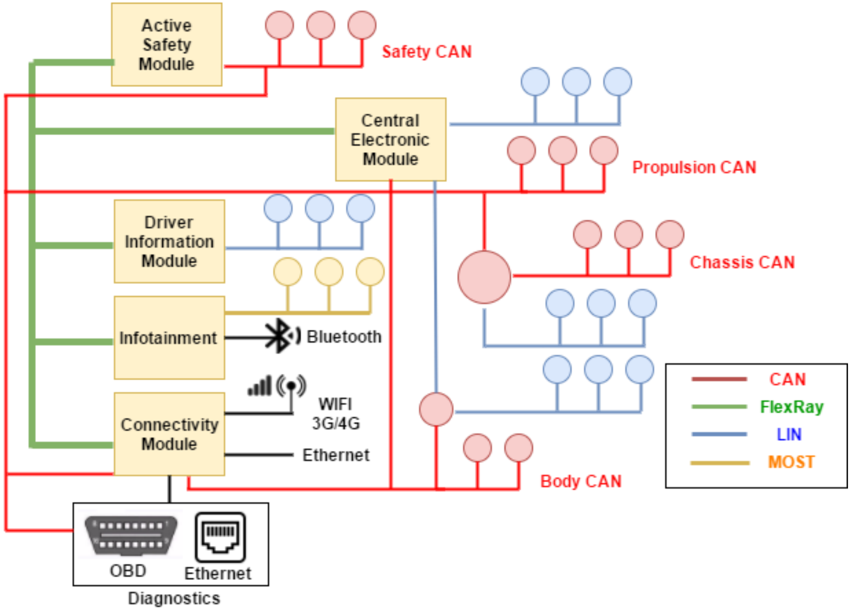
Nodes we add:

IDS **Attacker**



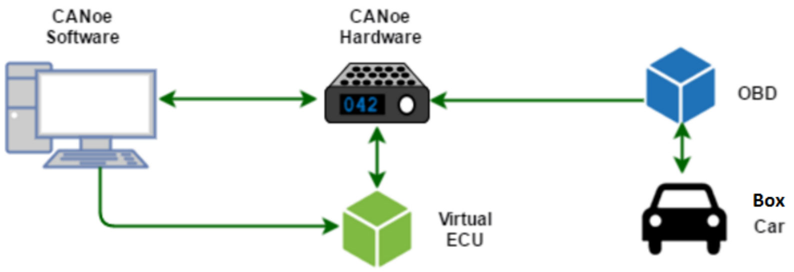
Setup (Box car)

- More complicated topology



Setup (Box car)

- **Can’t overwrite** the code for any ECU
- Connected to **only one domain** at a time.
- We can add more **(virtual)** nodes.

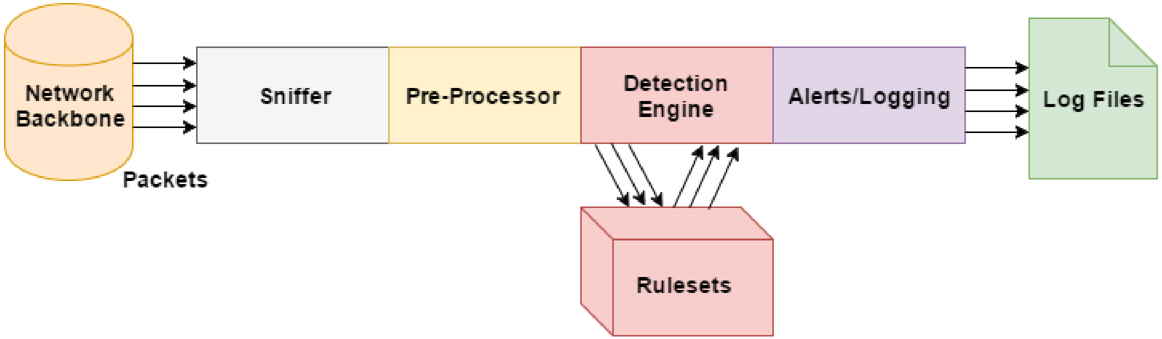


Virtual nodes we add:

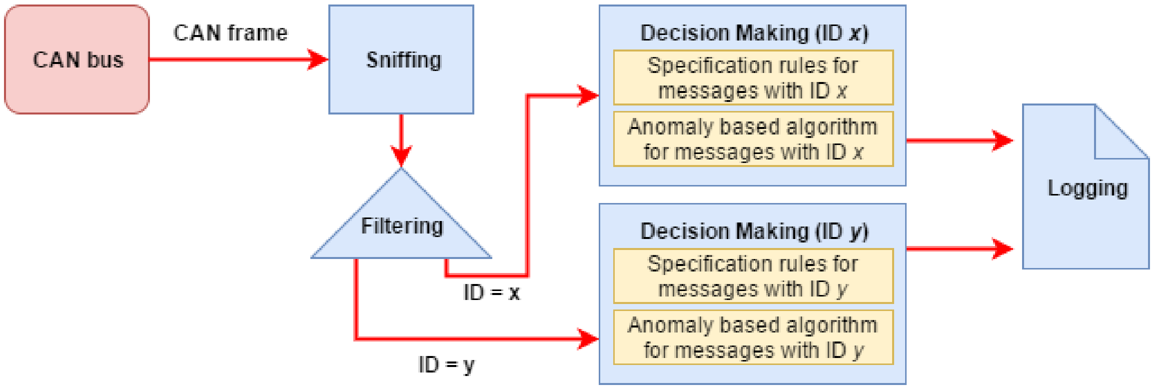
IDS

Attacker

Design



Snort (Computer System)



Our design (in-vehicle IDS)

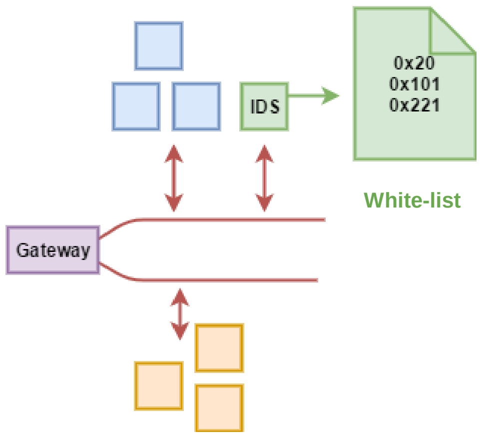
Implementation

- **Specification-based rules**
  - Malformed frame detection
  - Unauthorized message detection
- **Anomaly-based algorithms**
  - Plausibility detection (Detect sudden shifts in speed signal values)
  - Frequency change detection (Generic way to detect message injection)

Specification-based detection

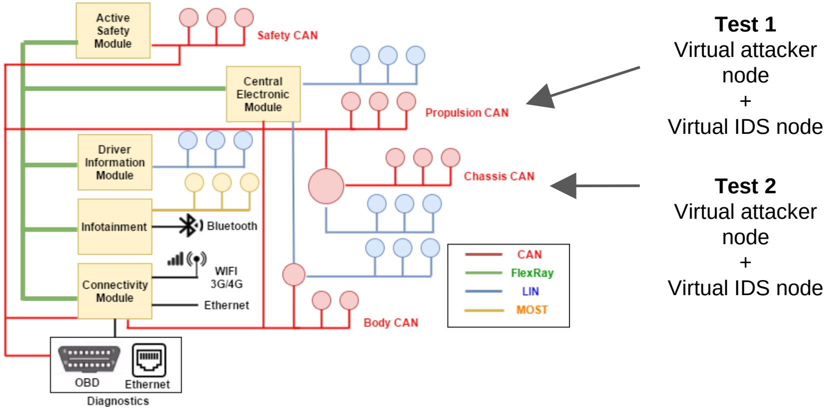
- Malformed frame detection
  - Rules extracted from signal database and compared directly.
- Unauthorized message detection
  - White-list extracted from the signal database.

Specification	Rule
The message carries three signals each signal is 8 bits or less	$DLC = 3$
Signal x is 8 bits maximum	$0 \leqslant x.value \leqslant 255$
Signal y is 8 bits maximum	$0 \leqslant y.value \leqslant 255$
Signal z is 5 bits maximum	$0 \leqslant z.value \leqslant 31$



Results (Specification-based detection)

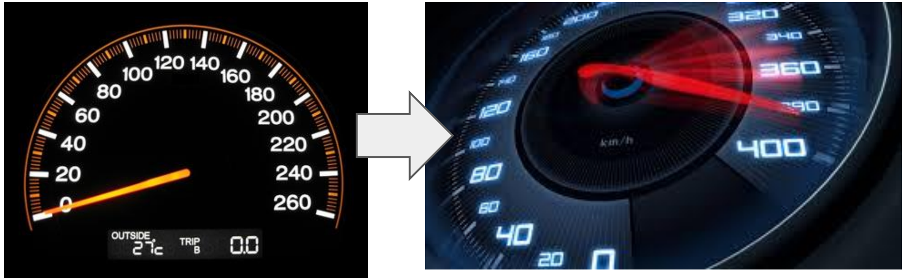
- Performed attacks on different domains for evaluation
- The results were as expected → 100% Detection rate



Parameter changed	Detection rate
Data length (DLC)	100% detection rate
Signal bit length	100% detection rate
Constant signal byte value	100% detection rate
Unauthorized messages	100% detection rate

Anomaly based detection (plausibility detection)

- We focused on **speed signals**
- It's not normal to see the speedometer jump from 30 km/h to 200 km/h in one second.
- Change in value between two consecutive messages **has a threshold** that depends on the acceleration capabilities and the driver’s behaviour.



Anomaly based detection (plausibility detection)

Extracting a threshold (Use case)

- Acceleration simulation.
- 4000 messages (20 seconds)
- Speed difference between (t) and (t-1)

Speed value difference (raw)	Samples (message)	Total percentage
1	3114	77.85%
2	638	15.95%
3	230	5.75%
4	6	0.15%
5,6,7,8,9	0	0.0%
10	1	0.025%
11	1	0.025%
12,13	0	0.0%
14	1	0.025%
15	1	0.025%
16	1	0.025%
17	3	0.075%
18	3	0.075%
19	1	0.025%

Threshold = **20 (raw) ≈ 16 (km/h)**

Algorithm simplified

x = abs(speed(t)-speed(t-1))

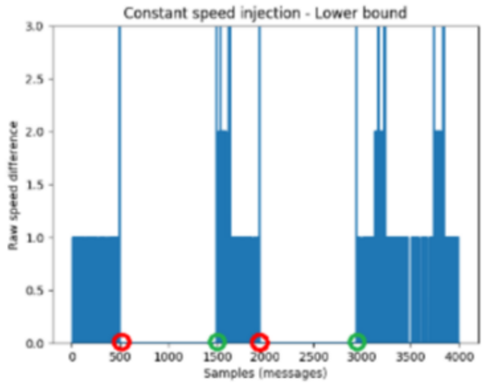
if (x >= threshold)
→ raise an alarm

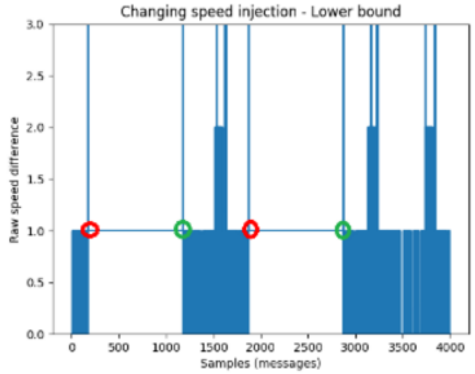
Results (plausibility detection)

Two tests

- Constant speed injection
  - Injected speed value is constant during the attack
- Stealth speed injection
  - Injected speed value is changing during the attack

We can detect the start and the end of the attack





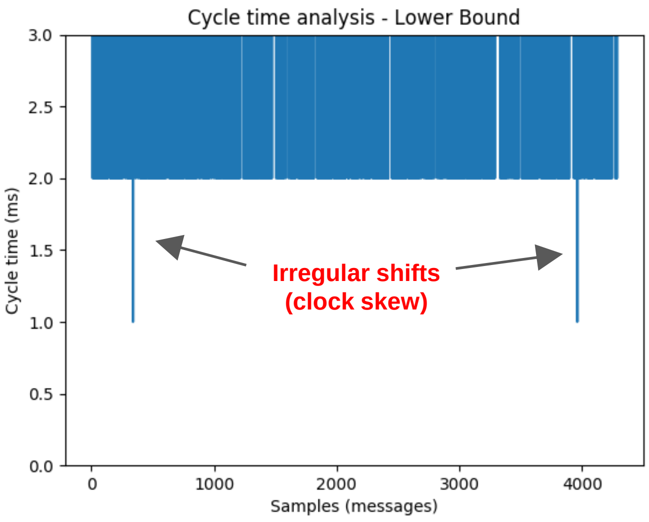
Anomaly based detection (frequency detection)

- The cycle time is defined in the signal database.
- This was not enough because it resulted in false detections.
- Solution: *(Double check)*

Algorithm simplified

First check → Second check →

```
attack = false
if( (T(m_t)-T(m_{t-1}) < cycle_time){
        attack =true
        attack_count++
        if (attack_count > 1)
                → raise an alarm
}
if(!attack  && count>0){
        attack_count=0
}
```



The message here has 2 ms as cycle time

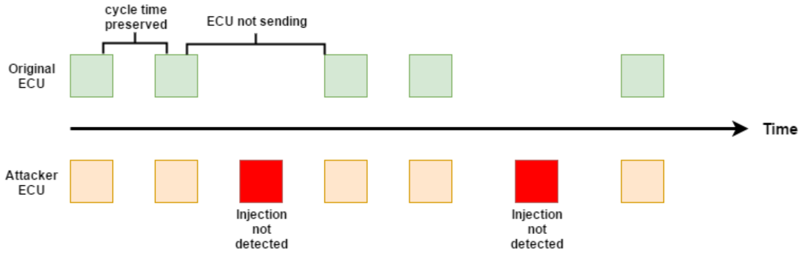
Results (Frequency change detection)

Two tests

- Cycle time effect
- Aggressive injection (Dos)

Original cycle time	Injected cycle time	Detection rate
15 (ms)	15 (ms)	Average detection (14.32%)
5 (ms)	5 (ms)	Average detection (96.67%)
2 (ms)	$t \leq 2$ (ms)	Average detection (99.98%)

Identical cycle time



Injected messages	Detection rate
1000	998 (99.8%)
10000	9998 (99.98%)
100000	99998 (99.998%)
n	n-2 $\frac{(n-2)*100}{n}\%$

Aggressive injection

Original cycle time	Injected cycle time	Detection rate
15 (ms)	$t \leq 14$ (ms)	n-2 of n injected messages
5 (ms)	$t \leq 4$ (ms)	
2 (ms)	$t \leq 2$ (ms)	

Smaller cycle time

Challenges and limitations

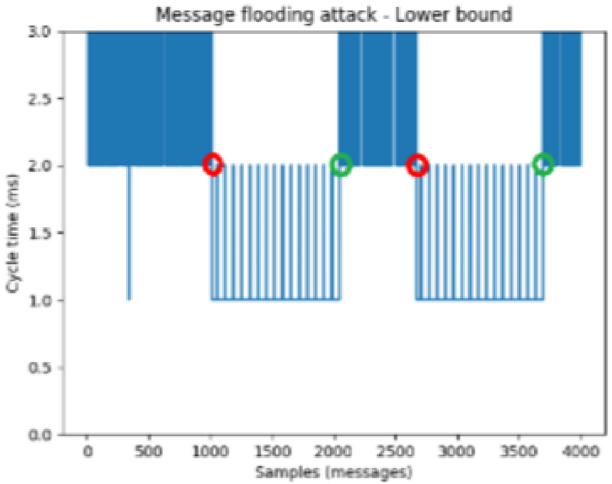
- Hardware constraints
    - ECUs have limited capabilities, but we didn’t have a problem with that.
- IDS node placement = cost
    - We suggest placing an IDS node in each domain for full coverage and lower load.
- Data selection
    - Plausibility detection should depend on acceleration capabilities, we only used a simulation
- Log storage? rule update?

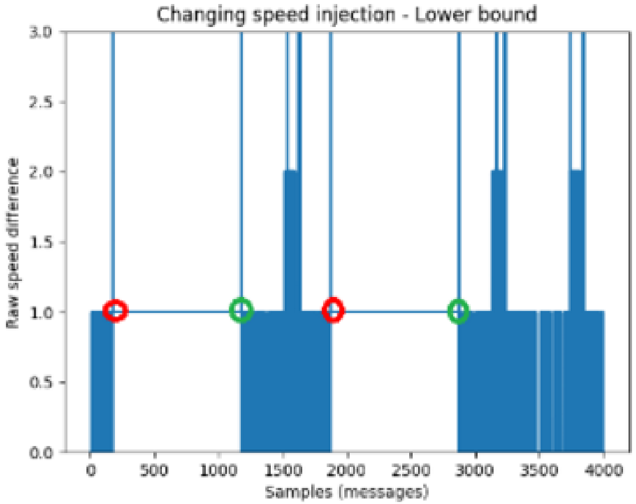
Summary

- Security is a problem in modern vehicles.
- We designed and implement an IDS system using distributed IDS nodes (ECUs) around the different domains.
- Each IDS node has a combination of :
    - Specification based rules
    - Anomaly based algorithms
- No false positives
- Challenges for future research.

Thank you for listening

Frequency detection vs plausibility detection





Monitors the message frequency
Detects the whole attack

Monitors the signal's value
Detects the beginning and the end of an attack