Risk assessment and security countermeasures for vehicular instrument clusters

Horatiu Gurban Bogdan Groza Pal-Stefan Murvay

Faculty of Automatics and Computers,
Politehnica University of Timisoara,
Romania

June 25, 2018

Universitatea Politehnica Timișoara

Objectives of our work:

- Establish the impact of attacks on vehicular ICs
- Design and implement an IDS to protect against adversarial actions

Research funded by:

CSEAMAN - Cryptographic Security for Automotive Embedded Systems and Networks,

young teams research grant of the Romanian National Authority for Scientific Research and Innovation, CNCS-UEFISCDI, project number PN-II-RU-TE-2014-4-1501 (2015-2017).

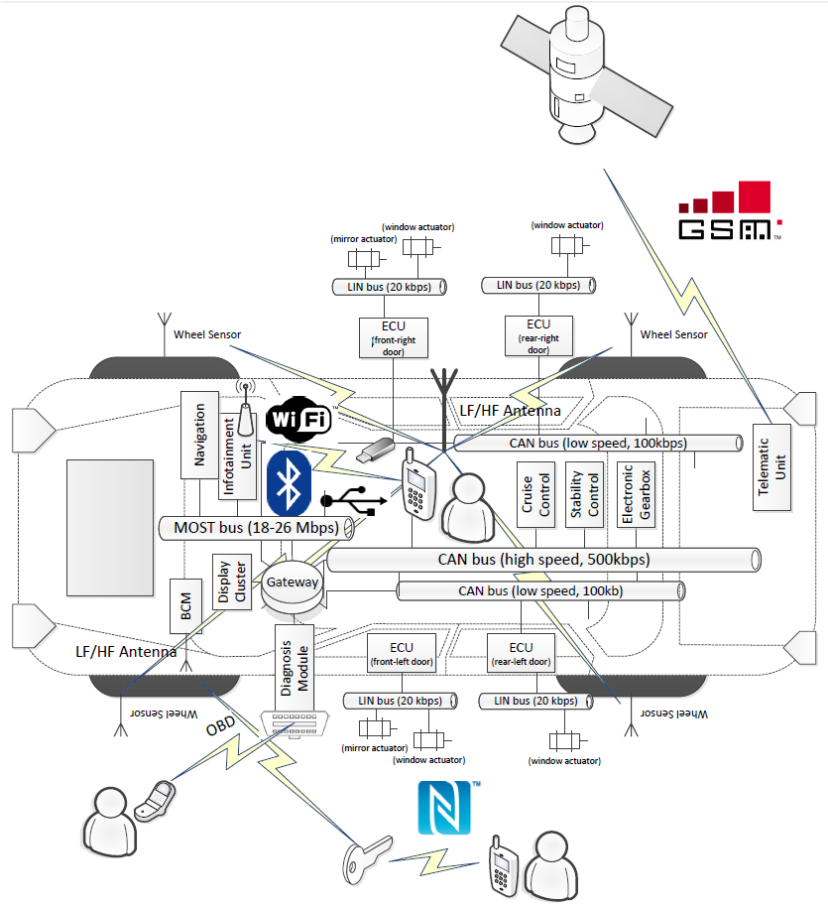
http://www.aut.upt.ro/~bgroza/cseaman.html

Modern vehicle interconnectivity

Vehicles evolved from mechanical devices into complex electro-mechanical systems loaded with software

- 100+ ECUs
- > 10 million lines of code
- Electronics + software

  =40% production cost
- 5-7 busses on various technologies
  - CAN,
  - FlexRay
  - BroadRReach (Ethernet),
  - LIN,
  - MOST, etc
- Several wireless interfaces
  - Bluetooth, WiFi, 4G

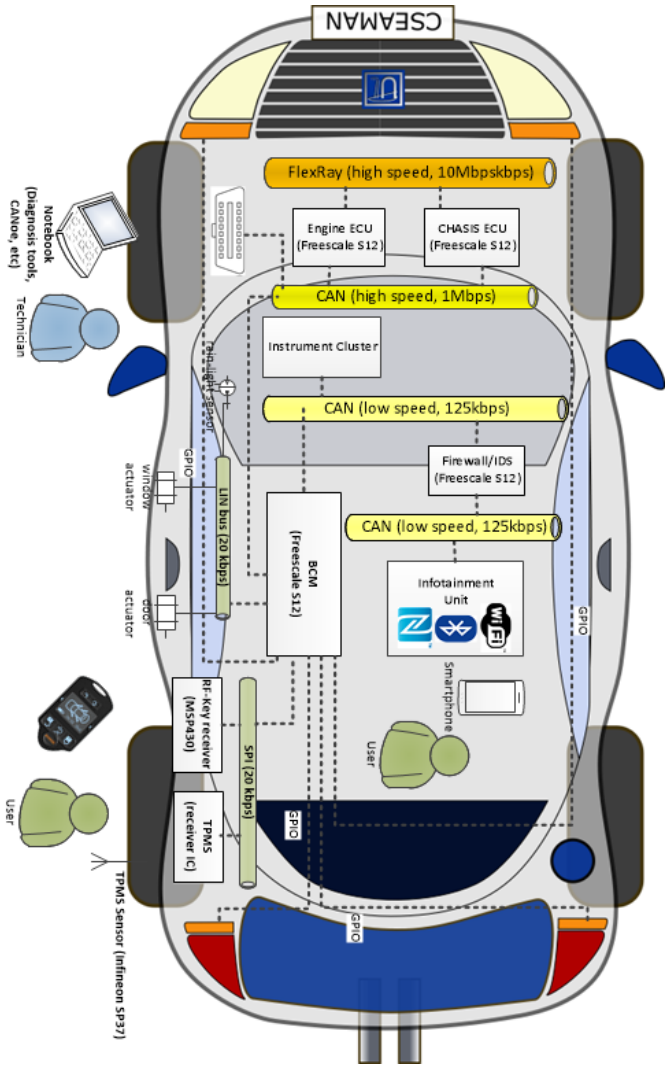


Taxonomy of ECU-related functionalities

- ECU grouping by functionalities:
  - *body*
    - interior/exterior lighting, wind-shield wipers/washers, window lift, Heating Ventilation and Air Conditioning (HVAC), door locks, immobilizer, etc.
    - Main controller – BCM (Body Control Module (BCM)
  - chassis
    - braking, steering, suspension, restraint, stability control, etc.
  - powertrain and transmission
    - fuel injection, emission control and gear shift.
    - real-time nature of power-train related subsystems makes them susceptible to DoS attacks
  - infotainment and telematics
    - offers interfaces to user-held devices, e.g., mobile phone, tablets, etc; remote vehicle diagnosis via mobile telecommunication technologies, e.g., 4G

Automotive communications standards

- CAN (Controller Area Network)
  - fault tolerant, low-speed version, max 125kbps (ISO11898-3)
  - high-speed , max 1Mbps (ISO11898-2)
  - CAN-FD (Flexible Data-Rate), max 2.5 Mbps
- FlexRay
  - Fulfill communication req. of X-by-Wire
  - fault tolerant, high-speed, deterministic, max 2ch at 10Mbps
- LIN (Local Interconnect Network)
  - Low cost serial communication interface
  - based on a master-slave architecture
  - Connect peripheral sensors and actuators - max 20 kbps
- None of these communication layers has any kind of security except for std. CRC codes
- Wireless transmission standards
  - WiFi and Bluetooth
  - adds new challenges from the security perspective



Generic software modules provided by ECUs

- Diagnostics Services (all the life-cycle stages of the automobile)
  - fault identification, software update, parametrization, calibration and identification of irregular conditions
  - Key Word Protocol (KWP, ISO 14230-3) and the Unified Diagnostic Services (UDS, ISO 14229-1 and UDS on CAN ISO 15765-3).
  - Diagnosis services that are used to take control of the ECU functionalities
    - Read/Write memory by address/identifier (0x22 , 0x23 , 0x2E , 0x3D),
    - Device Control/Input-Output Control (0x2F),
    - Request Upload/Download (0x34),

- Failure Diagnostics
  - mandatory to monitor the electrical functions and to implement a plausibility check for sensors and actuator functions
  - the extended information is used during software development, verification and validation stages, repair shops when the cause of a failure needs further investigation
  - falsely reported DTC can lead to inhibition of some functionalities for other module

- XCP - Universal Measurement and Calibration Protocol
  - used for writing parameter calibration values and for acquiring ECUs internal parameters at runtime

Network topologies

- No standardization, each manufacturers has it's own type of network topology

- Position of the IC is critical since corrupted nodes may exist, e.g., outside access may be facilitated via Onboard diagnostics (OBD) port

2014 Toyota Prius

- Single CAN bus along with ADAS, safety, powertrain and body control modules, *Toyota's DLC3 (Data Link Connector 3)*

2010 FORD Escape

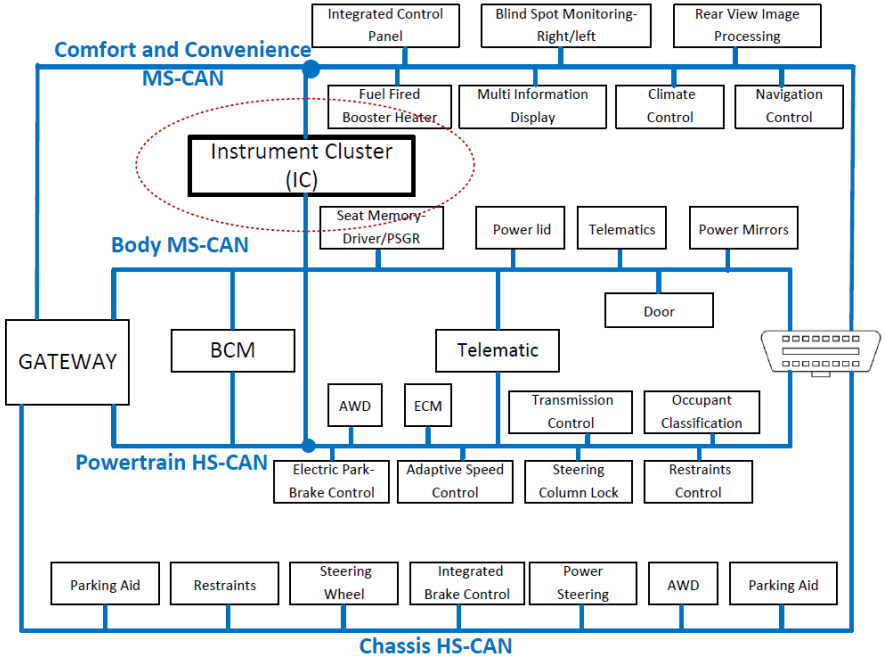
- Two CAN sub networks which also accommodate traffic for ADAS, safety, powertrain, comfort body and *multimedia* nodes, *DLC*

2014 Ford Fusion

- single CAN network: *Accessory Protocol Interface Module (APIM),* Audio Control Module (ACM), GPS and AM/FM/Satelite Radio, FCDM, ADSPM (audio digital processing) and the Gateway module

Network topologies

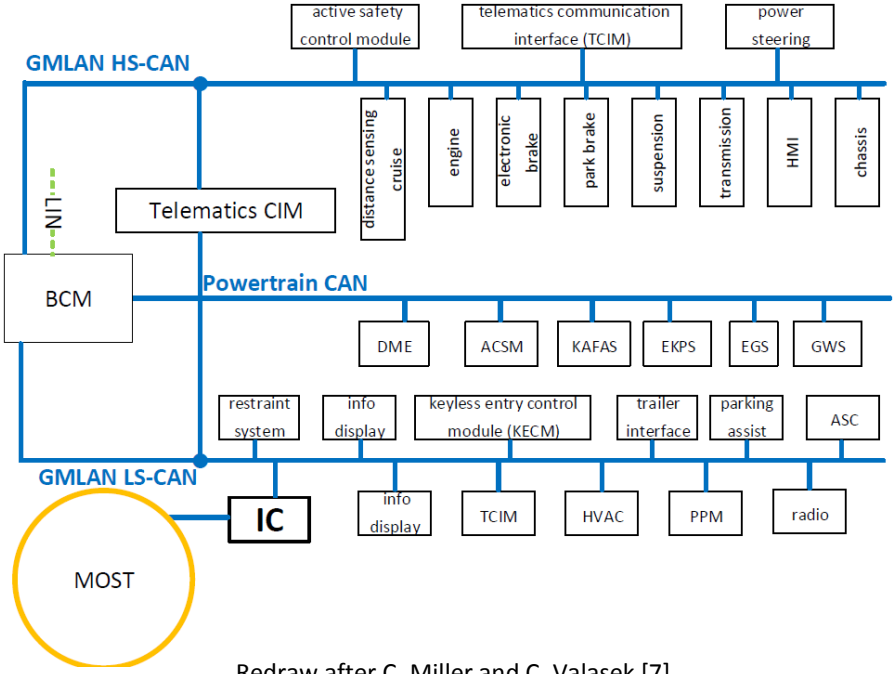
2014 Range Rover Evoque



Redraw after C. Miller and C. Valasek [7]

- powertrain system
- comfort and convenience systems

2015 Cadillac Escalade AWD



Redraw after C. Miller and C. Valasek [7]

- low speed CAN (LS-CAN) - body, comfort, ADAS and multimedia systems, etc.
- MOST network

Embedded platforms behind ICs

class	CPU model and characteristics
low-end	*NXP Qorivva MPC56xxS family: MPC5645S*, 32bit e200z4d core, 125 MHz, 64KB RAM, 2MB FLASH, 64KB EEPROM
middle-end	*Renesas RH850/D1M family*, 32bit RH850G3M core, 240 MHz, 512KB RAM, 5MB Flash, 64KB EEPROM *Cypress Traveo S6J3200*, 32bit ARM Cortex-R5F core, 240 MHz, 512KB RAM, 2112KB Flash, 64KB EEPROM
high-end	*NXP i.MX 6 family: MCIMX6QP6AVT1AA*, 4x 32bit ARM Cortex-A9 cores, 1 GHz, 512KB RAM, GPU 2D Vivante GC320, GPU 2D Vivante GC355, GPU 3D Vivante GC2000+ *Renesas R-Car H2 SoC Family: R8A77950*, 4xARM Cortex-A57, 4xARM Cortex-A53, 1xARM Cortex-R7 cores, Max. 1.6 GHz, ext. RAM, ext. Flash, ext. EEPROM *NVIDIA Tegra 3 SoC*, 32bit 4x ARM Cortex A9 cores, 1.4 Ghz MHz, 520MHz GeForce GPU, ext. RAM, ext. Flash, ext. EEPROM

Proposed µC by automotive semiconductor suppliers : Renesas, STMicroelectronics, NXP and NVIDIA

- 32bit architecture, with one to four cores
- clock speeds in 100-200MHz range (classical gauges, hybrid implementation), 1GHz (full LCD)
- Architecture with different cores with different clock speeds

=>sufficient computational resources for implementing more demanding security functions, e.g., cryptography

Reported attacks

- display arbitrary messages on the IC, falsify the speedometer and fuel level information and adjust the display brightness (replay attacks based on packet sniffing and fuzzing**)**, **Koscher et al.[5]**
  - DoS attacks have also been performed by disabling communication from the ECM (a case in which the reported speed drops to 0 MPH) and by disabling communication from the BCM (a case in which the speed freezes to the last received value).

- falsify the status of door locks, speedometer, tachometer, odometer and on board navigation (CAN network impersonation attacks), **Miller and Valasek[6]**
  - Attacks based on diagnostic services have been also employed to falsify the reported fuel level

- IC flooding attack on a Scania truck using CAN diagnostic messages **[12]**
  - Makes some functionalities unavailable (IC filled with warnings) and prevents heart beat messages from being sent (due lower priority) leading to the malfunction of all the IC indicators

- falsify the speedometer and odometer information, replay attacks based on packet sniffing and fuzzing, **Hoder et al**.**[14]**

Any attack can be performed when gaining physical access to the network

Risk assessment for the IC

Risk of a threat is based on two components:

the impact of the threat and **the difficulty** in mounting the attack

The impact of the threat:

- **safety** - the impact of an attack on the physical integrity of the driver, passengers of the car and on other traffic participants
- **financial** - the cost associated to the damage
- **operational** - the impact on the functional integrity of the vehicle and the consequences over other vehicles in traffic

impact

$$I = \alpha_{Sf} I_{Sf} + \alpha_{Fin} I_{Fin} + \alpha_{Op} I_{Op}$$

risk of the attack

$$R = I \times \beta_{\text{dif}}{}^{-1}$$

- β_{dif} = 14 similar to the work in [17] in order to have a common scale in evaluating the risk

Impact

	Safety	Financial	Operational
0	no injury	none	no operational impact
1	light	10$	impacts operation but is indiscernible to driver and causes little performance concerns
2	severe	100$	discernible to driver but insignificant to other vehicles
3	life threatening	1.000$	noticeable impact both for the driver and other vehicles
4	fatal	10.000$ or above	significant impact for driver and other vehicles in traffic

Attack severity classification and rating

impact

$$I = \alpha_{Sf} I_{Sf} + \alpha_{Fin} I_{Fin} + \alpha_{Op} I_{Op}$$

α_{Sf}	α_{Fin}	α_{Op}
8	4	2

Coefficients for impact similar to [8]

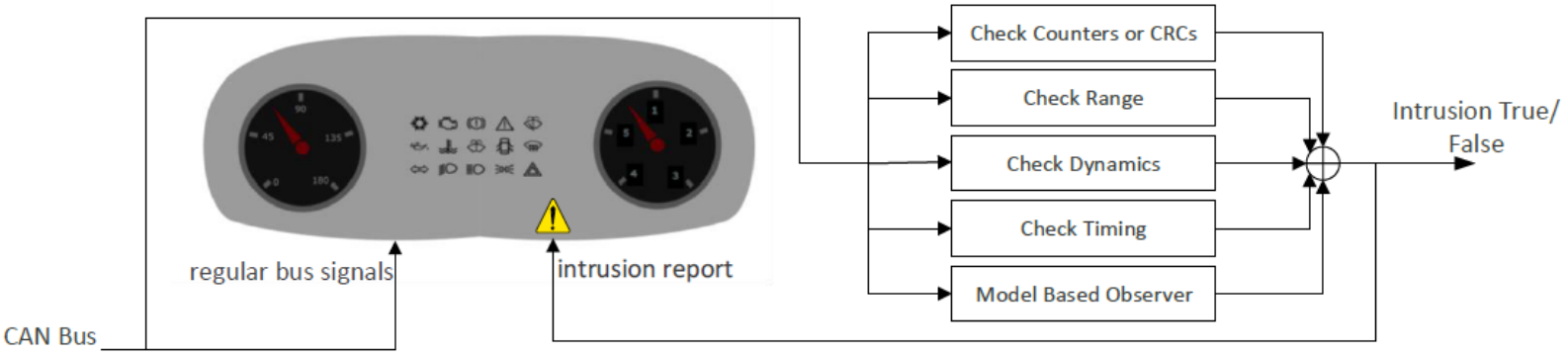
We partly base our assessment of security risks on the methodology from:

[15] Henniger et al., Security requirements for automotive on-board networks,
[16] Othmane et al., Incorporating attacker capabilities in risk estimation and mitigation
[17] B. Groza et al., Designing security for in-vehicle networks: a body control module (BCM) centered viewpoint

QUANTITATIVE RISK ANALYSIS FOR ATTACKS ON SEVERAL IC FUNCTIONALITIES

IC indicator	I_{Sf}	I_{Fin}	I_{Op}	I	Risk	Comments
Adaptive Cruise Control On	4	4	4	56	**4**	turning the indicator on or off misleads the driver to assume that the vehicle keeps a safe distance from the vehicle in front
Parking brake fault	3	4	1-3	46	**3.28**	parking on a steep surface can lead to life threatening situations
Parking brake applied	3	4	1-3	46	**3.28**	critical when parking on a ramp
Speedometer	1-3	4	1-3	46	**3.28**	false speed reports may cause accidents, e.g., unaware speeding driver
ABS system fault	1-3	1-3	1-3	42	**3**	without ABS the braking distances increases and vehicle manoeuvrability is reduced in case of wheel lockup
Brake pad wear	3	3	1-3	42	**3**	increased braking distance, malfunctions of other braking system components
ESP system fault	1-3	1-3	1-3	42	**3**	disabled ESP leads to reduced vehicle manoeuvrability
Engine fault	1-3	3	1-3	42	**3**	unreported errors can lead to engine malfunction
Forward Collision Warning	3	3	1-3	42	**3**	critical when the car is not equipped with autonomous braking
Low tire pressure	3	3	1-3	42	**3**	increased fuel consumption, increased braking distance and poor vehicle control, tire blowout in case of over-inflated tire
Low brake fluid level/fault	3	3	1-3	42	**3**	unreported malfunction of a safety critical system
Pedestrian Warning	3	3	1-3	42	**3**	pedestrian warning is critical in case of distracted drivers
Traction Control disabled	1-3	1-3	1-3	42	**3**	disabled traction control unit leads to reduced vehicle manoeuvrability
Lane Departure Warning	3	3	1-3	42	**3**	lane departure warning systems reduces the road departure crashes by 30% [21]
Light bulbs failure	3	3	1-2	40	**2.85**	lights malfunction reduces the visibility of the car to other drivers, brake/turn lights malfunction at high speeds increase the reaction time for other cars increasing risks of accidents
Front/Rear fog lights On	3	3	1-2	40	**2.85**	disabling rear fog lights reduces the visibility of the car
Headlight Low beams On	3	3	1-2	40	**2.85**	inactive low beams reduces the visibility of the car
Blind Spot Monitor (BSM) Warning	3	3	1	38	**2.71**	critical from the safety perspective, on the US highways 1 in 25 deaths is due to lane changes and merges [19]
Airbag/belt tensioning system fault	1-4	0	1	34	**2.43**	increased risk of fatal injuries in case of accident, the airbags reduces mortality by 63%
Airbag disabled	1-4	0	0	34	**2.43**	wrong assumption regarding the airbag status can lead to life threatening situations, e.g., (airbag deployment in case of front-mounted baby carrier)
Oil pressure low	1-2	3	1-3	34	**2.43**	low oil pressure can lead to engine malfunction
Seat belt not fastened	3	1	2	32	**2.29**	increased risk of fatal injuries in case of accident, the usage of seat belts reduces the mortality by 72%
Alternator fault	1-2	2	1-3	30	**2.14**	alternator is unable to charge the battery, driverpassengers in danger when extreme conditions, e.g., snowstorm, desert, etc.
Low coolant level	1-2	3	1	30	**2.14**	can lead to engine malfunction
Engine coolant temperature	1-2	2	1-3	30	**2.14**	unreported high engine temperature may lead to engine damage or falsely reported high temperature can make the driver stop the car
Low battery charge	1-2	2	1-3	30	**2.14**	driver/passengers in danger when extreme conditions, e.g., snowstorm, desert, etc.
Fuel level	1-2	2	2	28	**2**	car runs out of fuel in extreme conditions, e.g., snowstorm, desert, etc.
Low fuel level	1-2	2	2	28	**2**	driver/passengers in danger when extreme conditions, e.g., snowstorm, desert, etc.
Open doors/trunk	2	2	1	26	**1.86**	opened door while driving represents a serious threat to car occupants
Park Assist Activated	1	2	3	22	**1.57**	minor threat
Tachometer	1	1	1-3	18	**1.28**	fuel consumption may not be optimal with manual gear shifts
Headlight High beams On	1	1	1-2	16	**1.14**	blinding other drivers may increase the risk of accident
Odometer	0	3	1	14	**1**	odometer tampering is used to increase the resale value

Security countermeasures - IDS for vehicular ICs



Intrusion detection mechanisms

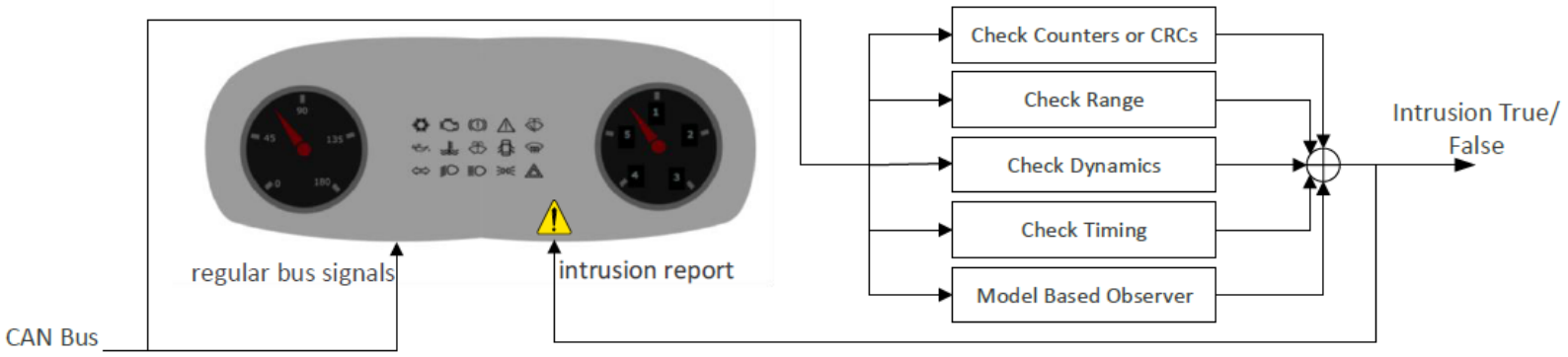
Specification-based anomaly detection for CAN communication based on CAN specification :

- monitoring of frame timeout, CRC/counter fault and invalid values
- timing checks of the periodic frames, minimum interval between periodic and event-triggered frames as well as consistency checks of signals values where interrelations exist

Diagnostics attack detection - signature-based

Model based observer can be used to estimate values and compare them to the reported values. Simplified models can be employed to identify an attack over certain values.

Security countermeasures - IDS for vehicular ICs



Intrusion detection mechanisms

Actions undertaken by the IDS includes **informative actions (alarms)** and **attack mitigation actions**.

Informative actions - *informing the driver* about possible intrusion (IC notification) and/or *informing the automotive maker/fleet owner* when telematics systems are employed.

Attack mitigation actions - changing the system state, e.g., switching to limp mode or shutdown

Security countermeasures - Intrusion detection rules

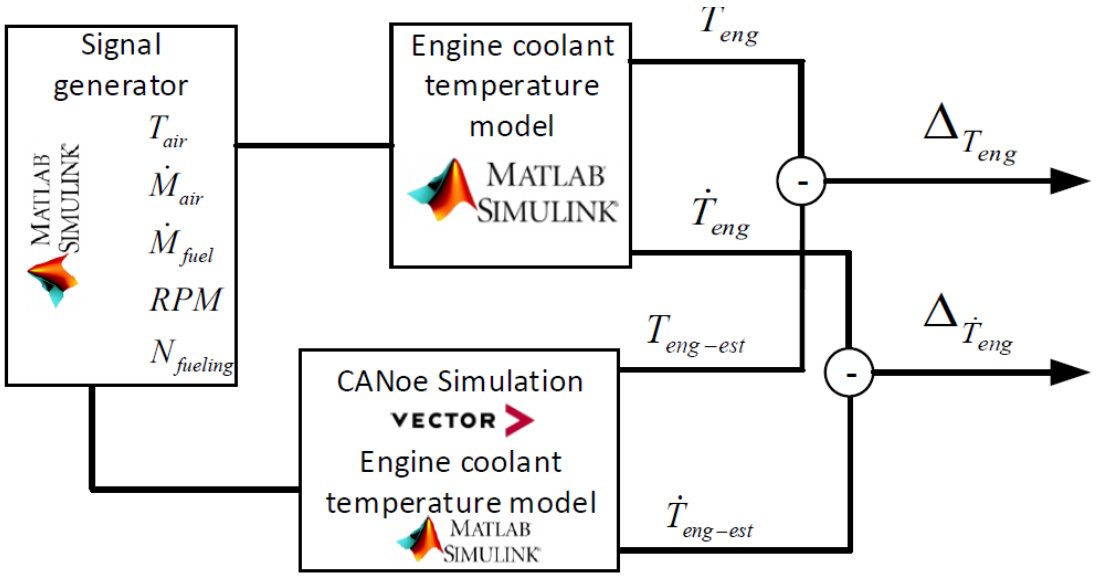
Functionality	Simplified model for detection
Fuel level	$FLev_{est}[t] = FLev_{CAN}[t-1] - h(ICon_{CAN}[t] + ICon_{CAN}[t-1])/2,\ |FLev_{CAN}[t] - FLev_{est}[t]| < \varepsilon_{FLev}$
Fuel warning	$FLev_{CAN}[t] < Thr_{FLev}$ and $Fuelwarning_{CAN} = ON$
TPMS	$Z_a = (\omega_1[t]/\omega_2[t]) - (\omega_4[t]/\omega_3[t]),\ Z_d = (\omega_2[t]/\omega_4[t]) - (\omega_1[t]/\omega_3[t]),$ $|Z_a| < \varepsilon_{TPMS}$ or $|Z_d| < \varepsilon_{TPMS}, |P_i[t] - P_{ref}|/P_{ref} < 0.3, \forall i \in \{1,2,3,4\},$
under-inflated identification:	$Z_a < 0$ and $Z_d < 0$ - rear left, $Z_a < 0$ and $Z_d > 0$ - front right, $Z_a > 0$ and $Z_d < 0$ - front left, $Z_a > 0$ and $Z_d > 0$ - rear right
RPM, speed, gear	$\|[(ArV[t]Tr[t]336.13)/Td] - RPM[t]| < \varepsilon$
Speed	$V_{est}[t] = V_{CAN}[t-1] + h(a_{CAN}[t-1] + a_{CAN}[t])/2$ $|V_{CAN}[t] - V_{est}[t]| < \varepsilon_V$
Cruise control	$|sp_V - V[t]| < \varepsilon_{SPV},\ D_{FrontCar}[t] > min_{dist}$
Engine coolant temperature	$|T_{eng\,est} - T_{eng}| < \varepsilon_{T_{eng}},\ \dot{Q}_{eng} = \dot{Q}_{rej} - \dot{Q}_{air} - \dot{Q}_{rad}$, $\dot{Q}_{rej} = (ap_{factor} \times \dot{M}_{air} + bp_{factor}) \times (N_{fueling}/N_{cyl}) \times \dot{M}_{fuel} \times Q_{LHV}$, $\dot{Q}_{air} = h_{eng} \times A_{eng} \times (T_{eng} - T_{air})$, $\dot{Q}_{rad} = \dot{M}_c \times C_c \times (T_{eng} - T_{eng\_in}),\ \dot{M}_c = A_{Thermostat} \times C_{coolflow} \times RPM$

Intrusion detection rules for certain functionalities

Intrusion detection rules

- **fuel warning model** is correlated with the fuel level model which uses the instant fuel consumption rate provided by the IC trip computer to easily inferred the fuel level
- **Tire Pressure** Monitoring System (TPMS) - indirect TPMS for validating the data received from the sensors
- **vehicle speed** can also be calculated based on the previous vehicle speed value and the average acceleration
- The car's **transmission expression** linking *the vehicle speed, motor rotational speed* and selected *gear* can be employed to identify a masquerade attack on CAN frames

Security countermeasures - Test environment

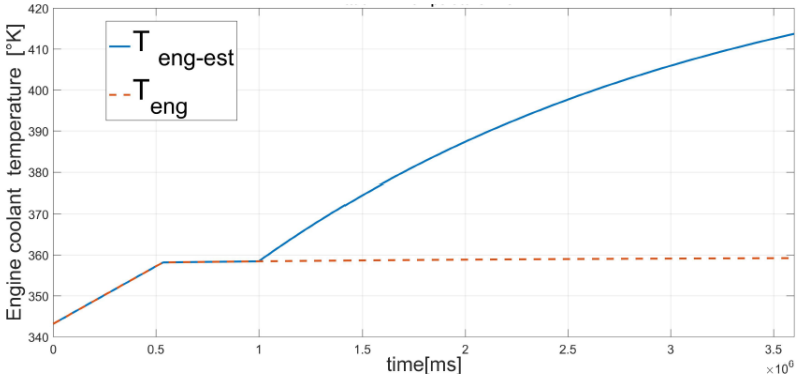


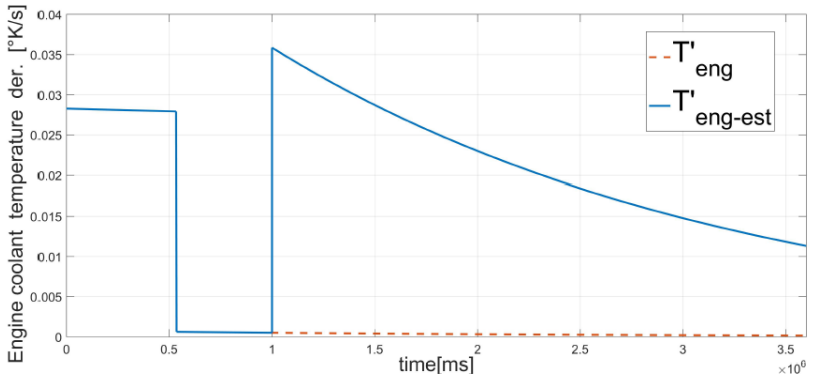
Test environment for engine coolant temperature model IDS

Engine coolant temperature model [23] employs information available from production Engine Control Modules (ECM) to compute the engine coolant temperature

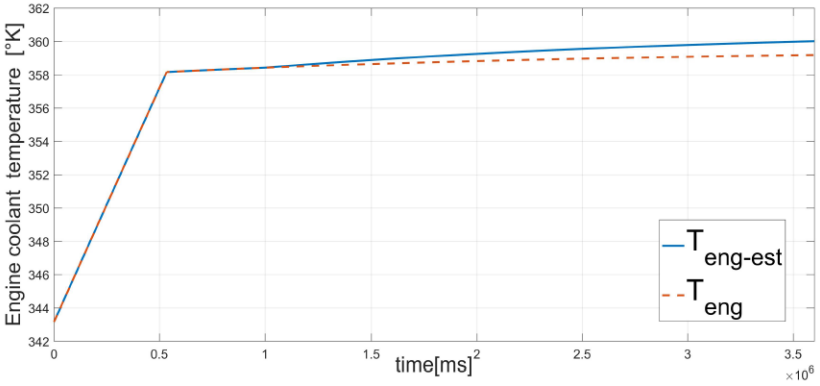
- engine ECU provides the measured engine coolant temperature and it's derivative
- IDS implement an observer for the engine coolant temperature by computing it along with its derivative
- IDS monitors if the difference between these values exceed some fixed thresholds

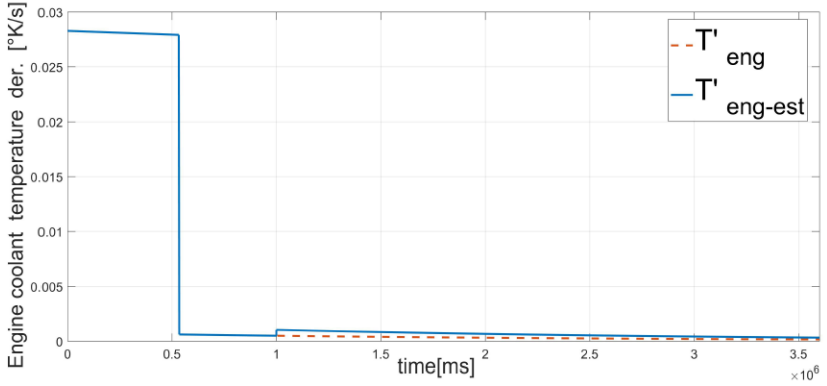
Security countermeasures - Experimental results



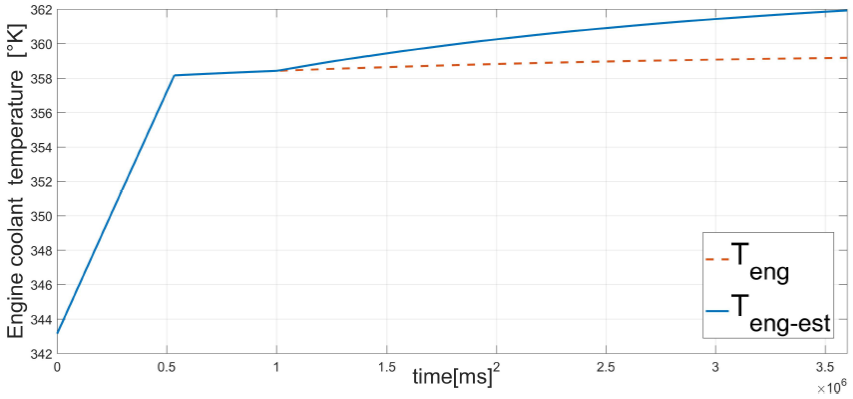


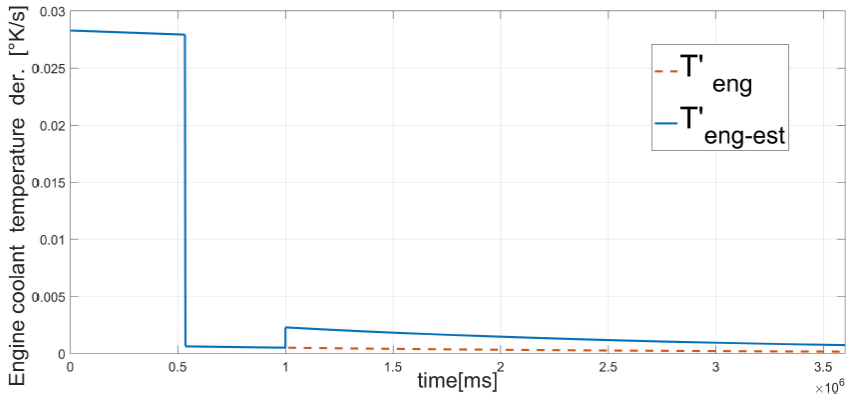
T_{eng} and $\dot{T}_{eng}$ in case of $\dot{M}_{fuel}$ signal attack



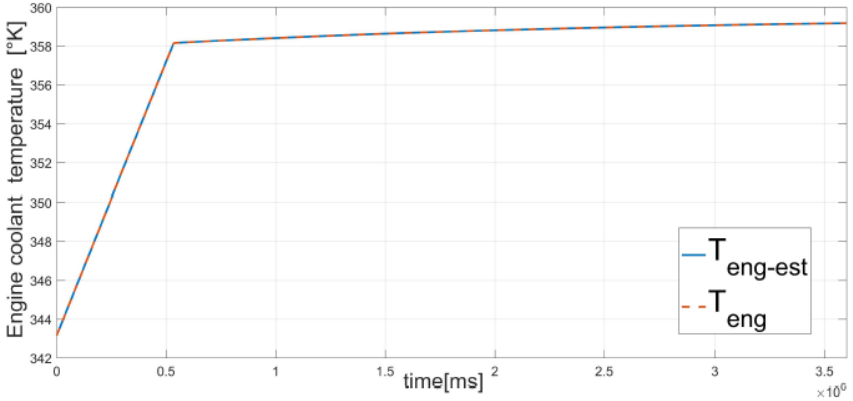


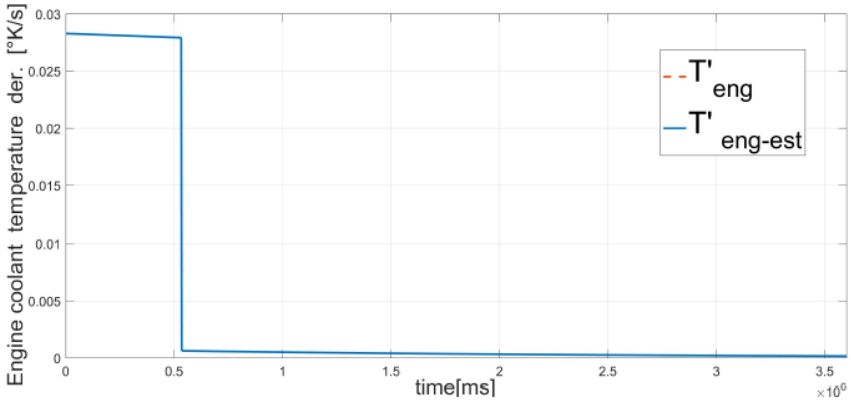
T_{eng} and $\dot{T}_{eng}$ in case of $\dot{M}_{air}$ signal attack



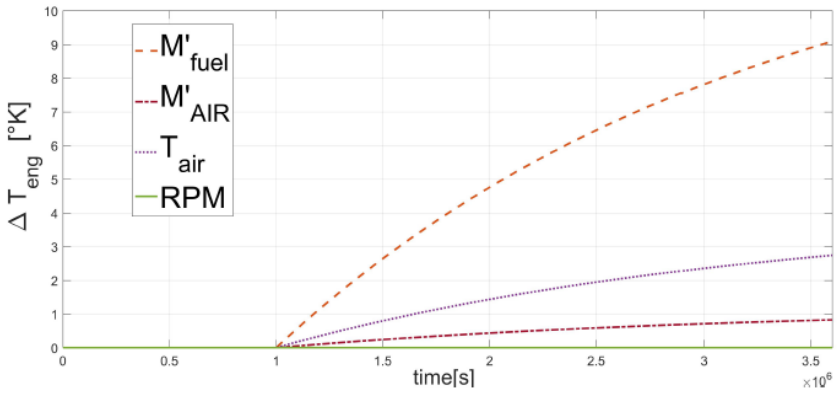


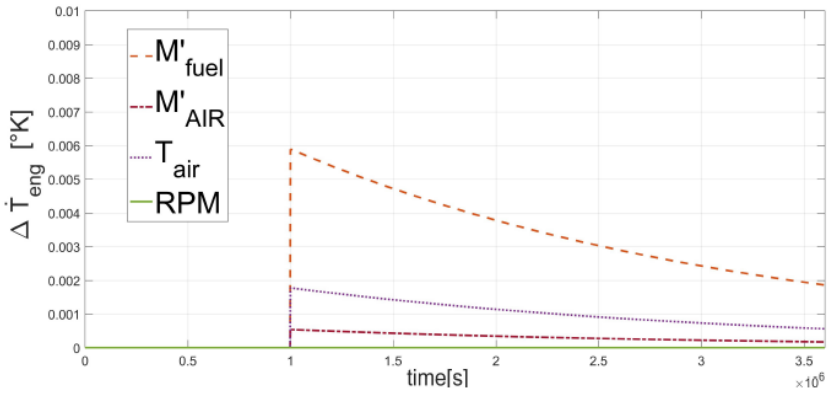
T_{eng} and $\dot{T}_{eng}$ in case of T_{air} signal attack





T_{eng} and $\dot{T}_{eng}$ in case of RPM signal attack





$\Delta_{T_{eng}}$ and $\Delta_{\dot{T}_{eng}}$ in case of $\dot{M}_{fuel}$, $\dot{M}_{air}$, T_{air} and *RPM* signal attack

- False reports of coolant temperature will be easily identified for $\dot{M}_{fuel}$ and $\dot{M}_{air}$ signals attack
- For T_{air} and *RPM the* $\Delta_{T_{eng}}$ and $\Delta_{\dot{T}_{eng}}$ are small and setting $\varepsilon_{T_{eng}}$ and $\varepsilon_{\dot{T}_{eng}}$ to identify this attack attempts will make the IDS susceptible to *false positive attack detection*

Conclusion

- Serious consequences can take place from wrong information sent to the driver from the instrument cluster
- Comprehensive risk analysis for vehicular ICs tries to bring a crisper image over the impact of security threats
- IDS may help to prevent spoofed messages from corrupted CAN nodes
- Our proof-of-concept implementation shows that simple detection rules can be used in addition to a model-based observer

http://www.aut.upt.ro/~bgroza/cseaman.html