Anomaly And Intrusion Detection Algorithms for CAN-bus Networking Security in Automotive Applications

Automotive SPIN Italia
21° WORKSHOP on AUTOMOTIVE SOFTWARE & SYSTEMS – 30/05/2023

P. Dini [1] , S. Saponara [1], **C. Rosadini** [2], W. Nesci [2], and S. Chiarelli [2]

[1] Department of Information Engineering – University of Pisa
[2] Marelli Europe S.p.A

Agenda

- Background
- Detection Engines
  - Rule-Based
  - Fingerprinting Voltage-based
  - Fingerprinting Time-based
- Combining Detection Engines
- Characterization Setup

UNECE WP.29 – R155

R155 - Cybersecurity

- Establish a Cybersecurity Management System (**CSMS**), which ensures security is adequately considered during development, production and post-production phases
- Manage vehicle cyber risks
- Securing vehicles by design to mitigate risks along the value chain
- Detecting and responding to security incidents across vehicle fleet

January 2021
- Enter into force

July 2022
- Mandatory for new vehicle types

July 2024
- Mandatory for new vehicle produced

7.3.7. The vehicle manufacturer shall implement measures for the vehicle type to:

(a) Detect and prevent cyber-attacks against vehicles of the vehicle type;

(b) Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type;

(c) Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.

Can be achieved by a combination of

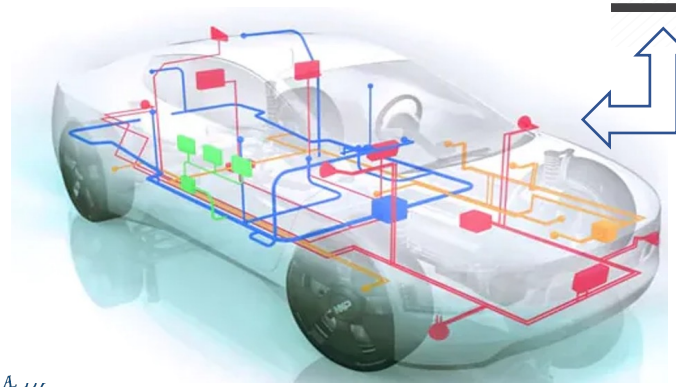
- onboard solutions to detect in-vehicle attacks
- offboard systems for fleet-wide collection and analysis

Rule-Based Approach

Rules' Expert

Rules' Database

In-Vehicle
CAN Network



condition

Code 1

Code 2

Rules Check

Result's Analysis

Advantages
- easy to interpret
- deterministic

Disadvantages
- high experience requirement
- limited to known attacks
- low flexibility to new scenarios
- often easy to trick

PATENTED

"Procedimento di monitoraggio di traffico dati in una rete di autoveicolo o motoveicolo.", **IT201600111869A1**

Rule-Based: detection capability (R155 coverage)

IDS Rule-Based

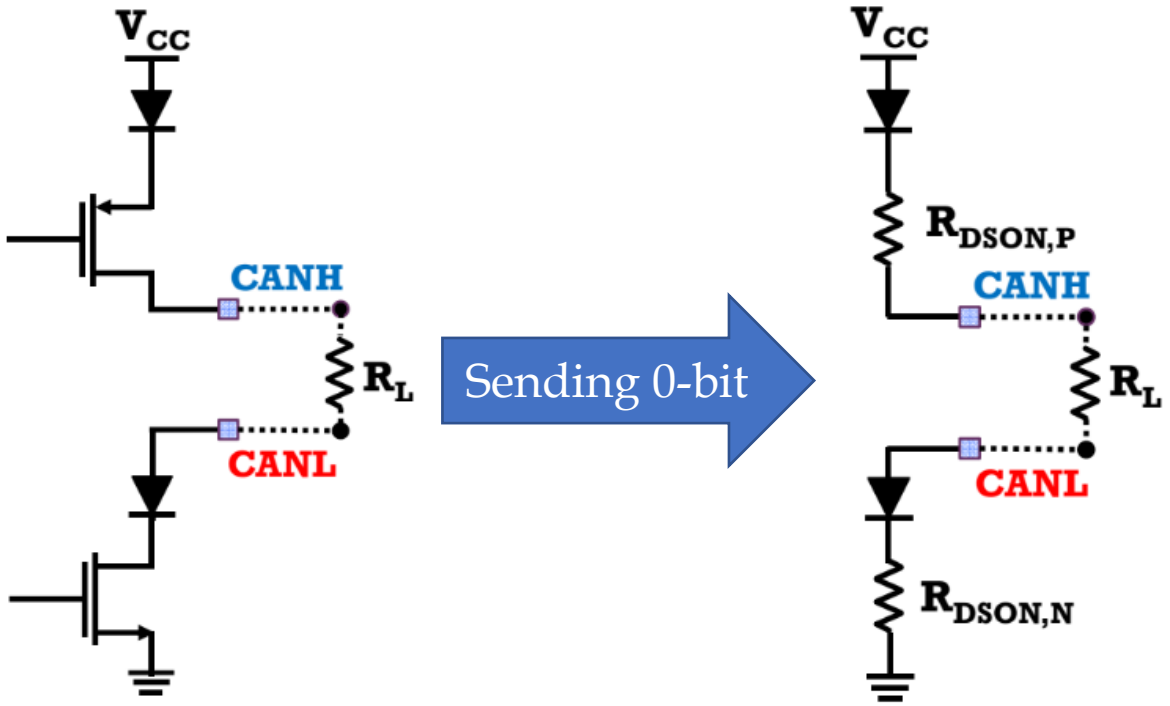
4.3.2 Threats to vehicles regarding their communication channels		Attack performed by					
		Added ECU		Replaced ECU		Reprogrammed ECU	
High level and sub-level descriptions of vulnerability/ threat	Example of vulnerability or attack method	w/ dbc mod*	w/o dbc mod	w/ dbc mod*	w/o dbc mod	w/ dbc mod*	w/o dbc mod
Spoofing of messages or data received by the vehicle	Spoofing of messages by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)	IDS		IDS		IDS	
	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)	IDS		IDS		IDS	
Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data	Communications channels permit code injection, for example tampered software binary might be injected into the communication stream						
	Communications channels permit manipulate of vehicle held data/code						
	Communications channels permit overwrite of vehicle held data/code						
	Communications channels permit erasure of vehicle held data/code						
	Communications channels permit introduction of data/code to the vehicle (write data code)						
Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks	Accepting information from an unreliable or untrusted source	IDS		IDS		IDS	
	Man in the middle attack/ session hijacking	IDS		IDS		IDS	
	Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway	IDS		IDS		IDS	
Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders	Interception of information / interfering radiations / monitoring communications						
	Gaining unauthorized access to files or data	IDS	IDS	IDS	IDS	IDS	IDS
Denial of service attacks via communication channels to disrupt vehicle functions	Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	IDS		IDS		IDS	IDS
	Black hole attack, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles	IDS					
An unprivileged user is able to gain privileged access to vehicle systems	An unprivileged user is able to gain privileged access, for example root access	IDS	IDS	IDS	IDS	IDS	IDS
Viruses embedded in communication media are able to infect vehicle systems	Virus embedded in communication media infects vehicle systems						
Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content	Malicious internal (e.g. CAN) messages	IDS		IDS		IDS	
	Malicious V2X messages, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)	N/A	N/A	N/A	N/A	N/A	N/A
	Malicious diagnostic messages	IDS	IDS	IDS	IDS	IDS	IDS
	Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier)	IDS		IDS		IDS	

IN SUPREMÆ DIGNITATIS 1343

MARELLI

Unicity of CAN ECUs/Devices – Voltage Levels

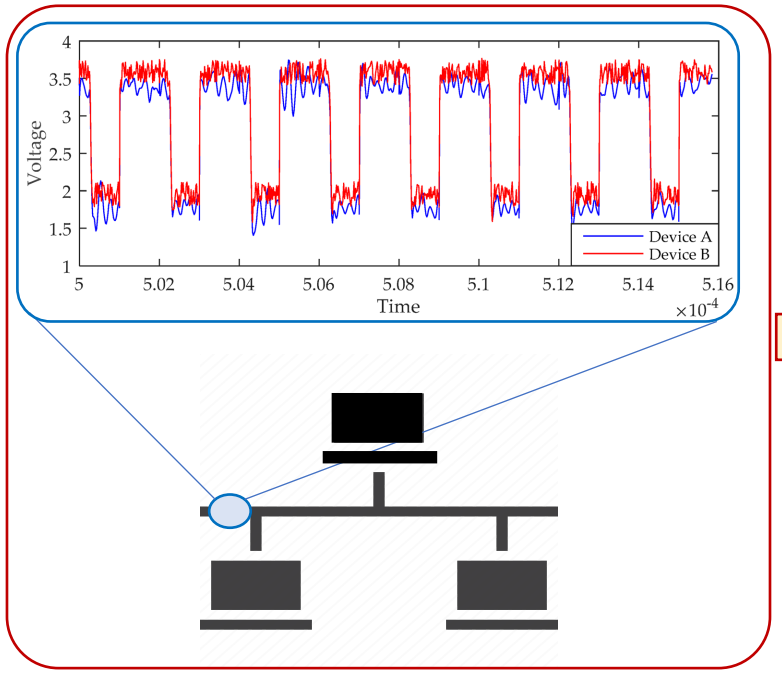
Basic Concept from Simplified Model of a CAN Transceiver



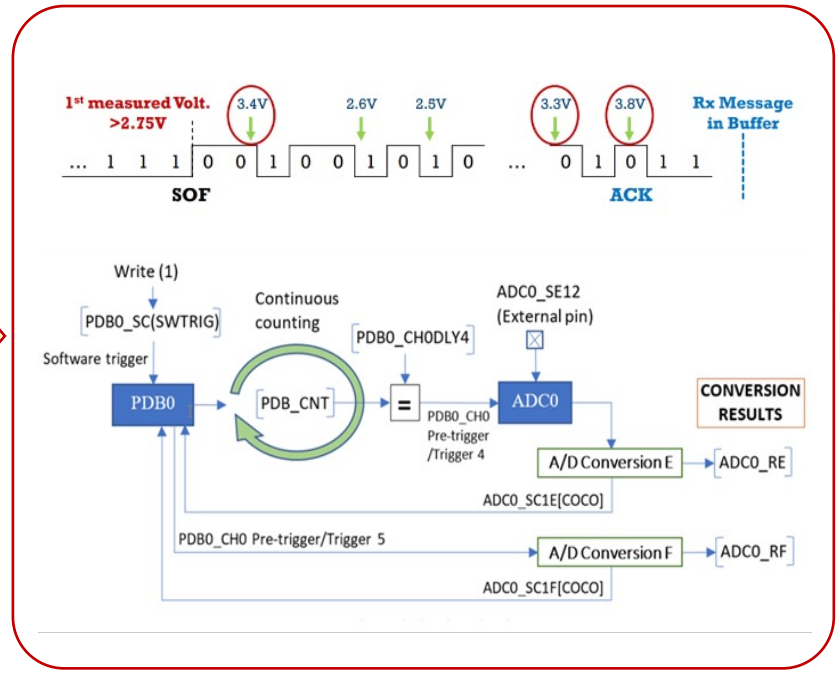
- $V_{cc_k} = V_{cc_0} + \Delta V_{cc_k}$
- $R_{ds,ECU_i} \neq R_{ds,ECU_j}$
- $V_{L/H,ECU_i} \neq V_{L/H,ECU_j}$
- $\Delta V_{ECU_i} \neq \Delta V_{ECU_j}$

- Different ECUs have tiny differences in the voltage of electrical signals which depends on the hardware and production process, even though the ECU are the same model
- The unique signatures of electrical signals could be used as fingerprints for detecting intrusions as well as identifying the source ECU of the attack

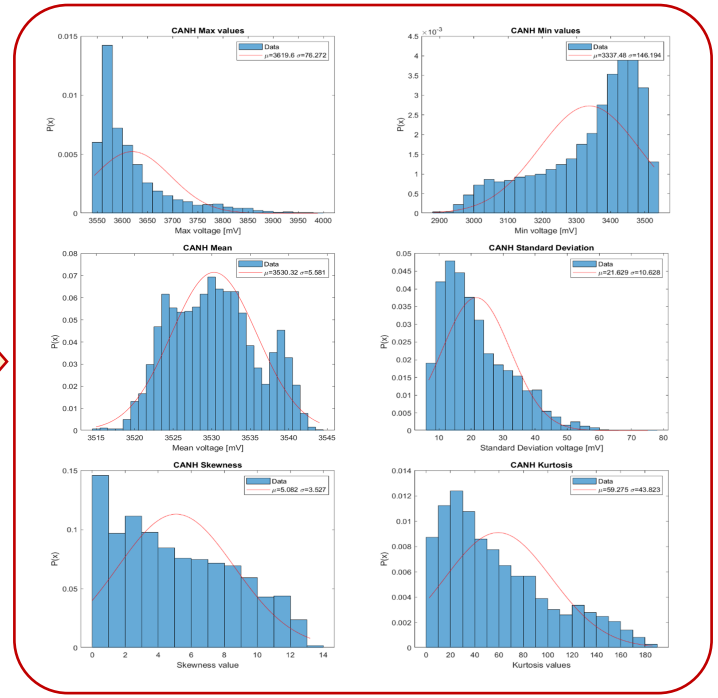
Voltage Fingerprinting Approach



Monitoring the Physical Layer of CAN_H & CAN_L



Opportune Sampling Phase on dedicated ECU/device

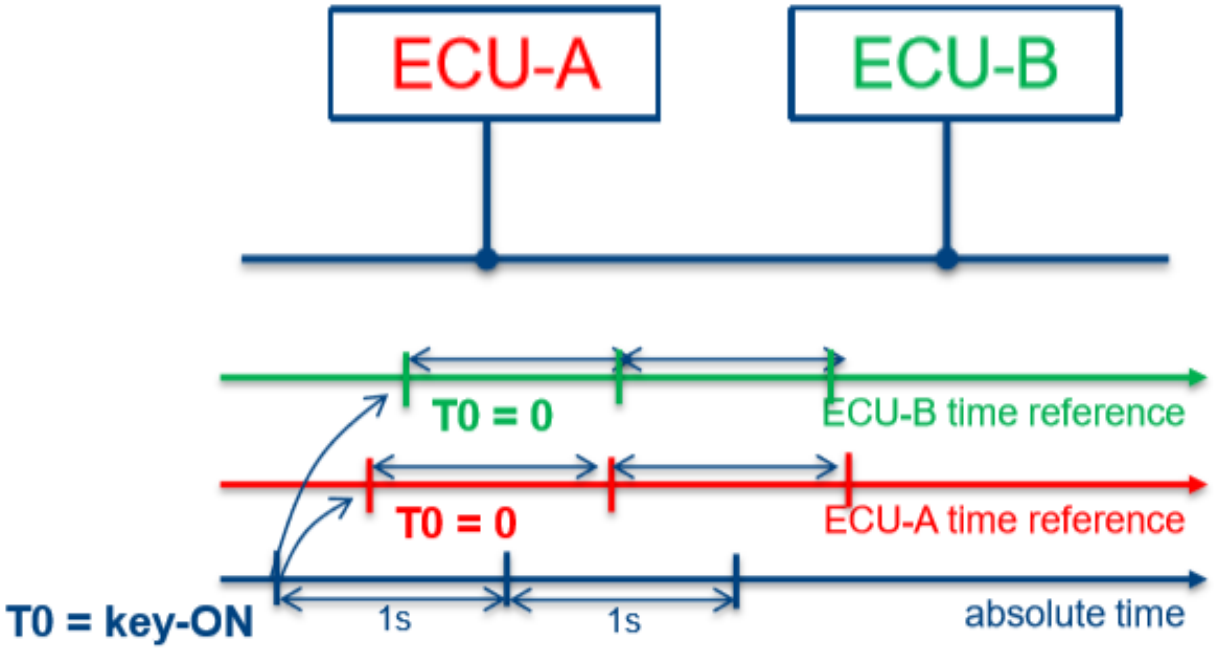


Check of Features by Specialized Algorithm

PATENTED

- "Method For Protection From Cyber Attacks To A Vehicle, And Corresponding Device." **U.S. Patent Applications No. 17/664,960** and **No. 17/804,010**.

Unicity of CAN ECUs/Devices – Internal Clock

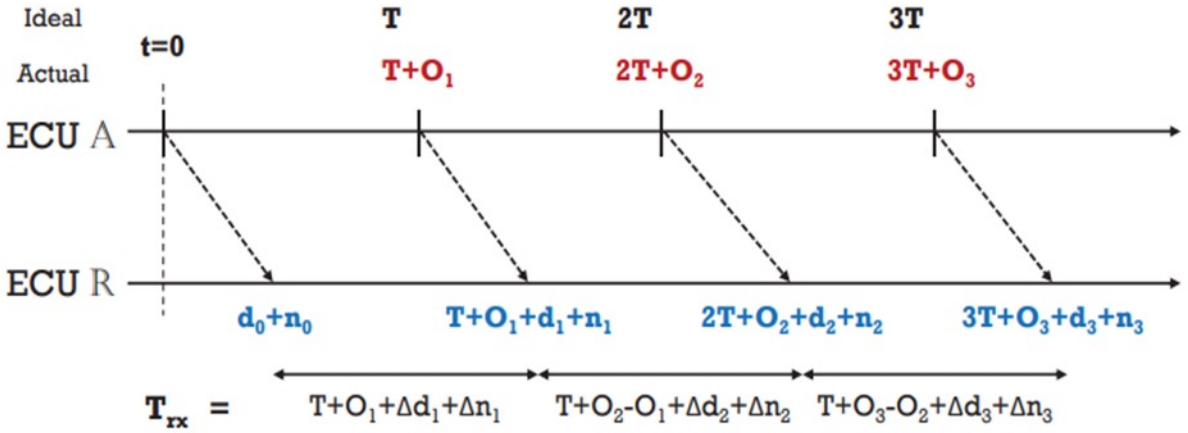


- All µC need a square wave (clock) to sequence their operations.
- The square wave is produced by an oscillator external to the µC.
- Typical oscillator: quartz with frequency ~10MHz.
- Internal clock multiplier that rise up to frequency to ~100MHz
- The µC uses the internal clock to define "time-line".

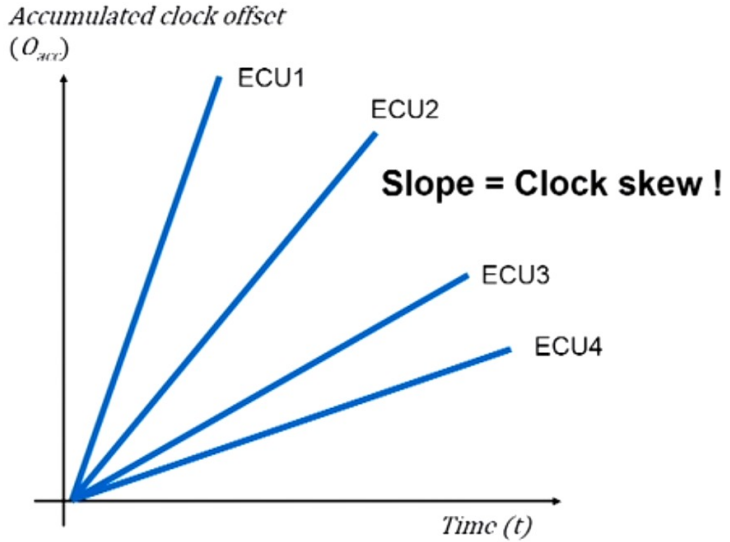
- ECU-A and ECU-B time references start at different absolute instants.
- ECU-A time runs slower than absolute time.
- ECU-B time runs faster than absolute time.

- **Technical Fact (HW/SW):**
  - **each ECU has its own key-on-time**
  - **every ECU has its own ref. time**

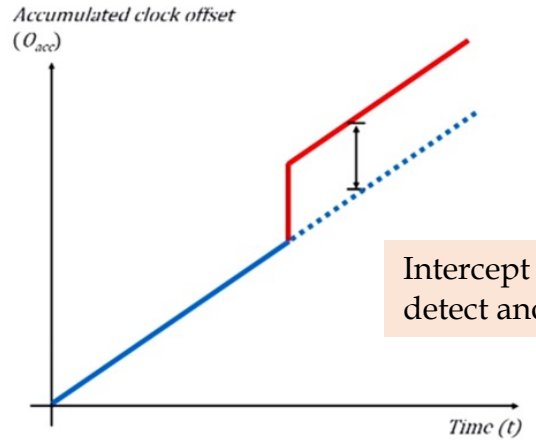
Timing Fingerprinting Approach



Modeling the Clock-Skew of each ECUs

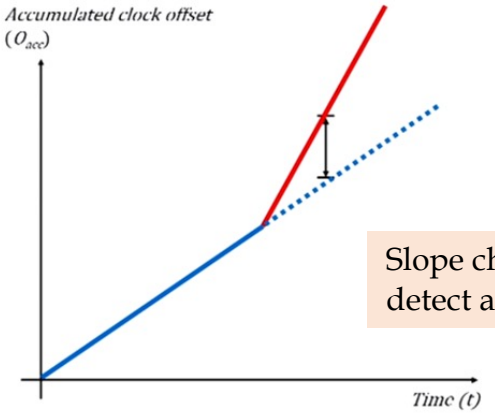


Detection of Fabrication Attack



Intercept changing
detect anomaly device

Detection of Masquerade Attack



Slope changing
detect anomaly period

PATENTED

"Method For Protection From Cyber Attacks To A Vehicle Based Upon Time Analysis, And Corresponding Device." **U.S. Patent Application No. 17/929,370**.

Rule-Based + Fingerprinting: detection capability (R155 coverage)

IDS Rule-Based
FP Time-based
FP Voltage-Based

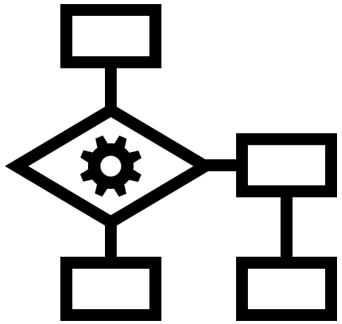
4.3.2 Threats to vehicles regarding their communication channels		Attack performed by					
		Added ECU		Replaced ECU		Reprogrammed ECU	
High level and sub-level descriptions of vulnerability/ threat	Example of vulnerability or attack method	w/ dbc mod*	w/o dbc mod	w/ dbc mod*	w/o dbc mod	w/ dbc mod*	w/o dbc mod
Spoofing of messages or data received by the vehicle	Spoofing of messages by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)	FP	FP	FP	FP	FP	FP
	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)	FP	FP	FP	FP	FP	FP
Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data	Communications channels permit code injection, for example tampered software binary might be injected into the communication stream			FP	FP	FP	FP
	Communications channels permit manipulate of vehicle held data/code			FP	FP	FP	FP
	Communications channels permit overwrite of vehicle held data/code			FP	FP	FP	FP
	Communications channels permit erasure of vehicle held data/code			FP	FP	FP	FP
	Communications channels permit introduction of data/code to the vehicle (write data code)			FP	FP	FP	FP
Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks	Accepting information from an unreliable or untrusted source	FP	FP	FP	FP	FP	FP
	Man in the middle attack/ session hijacking	FP	FP	FP	FP	FP	FP
	Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway	IDS FP	FP	FP FP	FP FP	FP FP	FP FP
Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders	Interception of information / interfering radiations / monitoring communications						
	Gaining unauthorized access to files or data	IDS	IDS	FP	FP	FP	FP
Denial of service attacks via communication channels to disrupt vehicle functions	Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	FP	FP	FP	FP	FP	FP
	Black hole attack, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles	IDS					
An unprivileged user is able to gain privileged access to vehicle systems	An unprivileged user is able to gain privileged access, for example root access	IDS	IDS	FP	FP	FP	FP
Viruses embedded in communication media are able to infect vehicle systems	Virus embedded in communication media infects vehicle systems						
Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content	Malicious internal (e.g. CAN) messages	FP	FP	FP	FP	FP	FP
	Malicious V2X messages, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)	N/A	N/A	N/A	N/A	N/A	N/A
	Malicious diagnostic messages	IDS	IDS	FP	FP	FP	FP
	Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier)	FP	FP	FP	FP	FP	FP

IN SUPREMÆ DIGNITATIS 1343

MARELLI

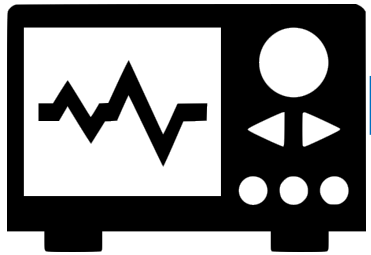
Needs for Approaches Merging

Rule-based



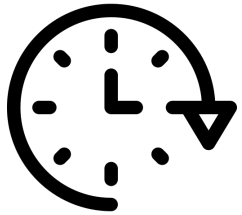
- Fast Anomaly Check
- Issue with Nodes Suspension
- No Source Detection Capability

Voltage FP



- Medium Speed in Anomaly Check
- Great with Nodes changing
- Bit high computational cost

Timing FP

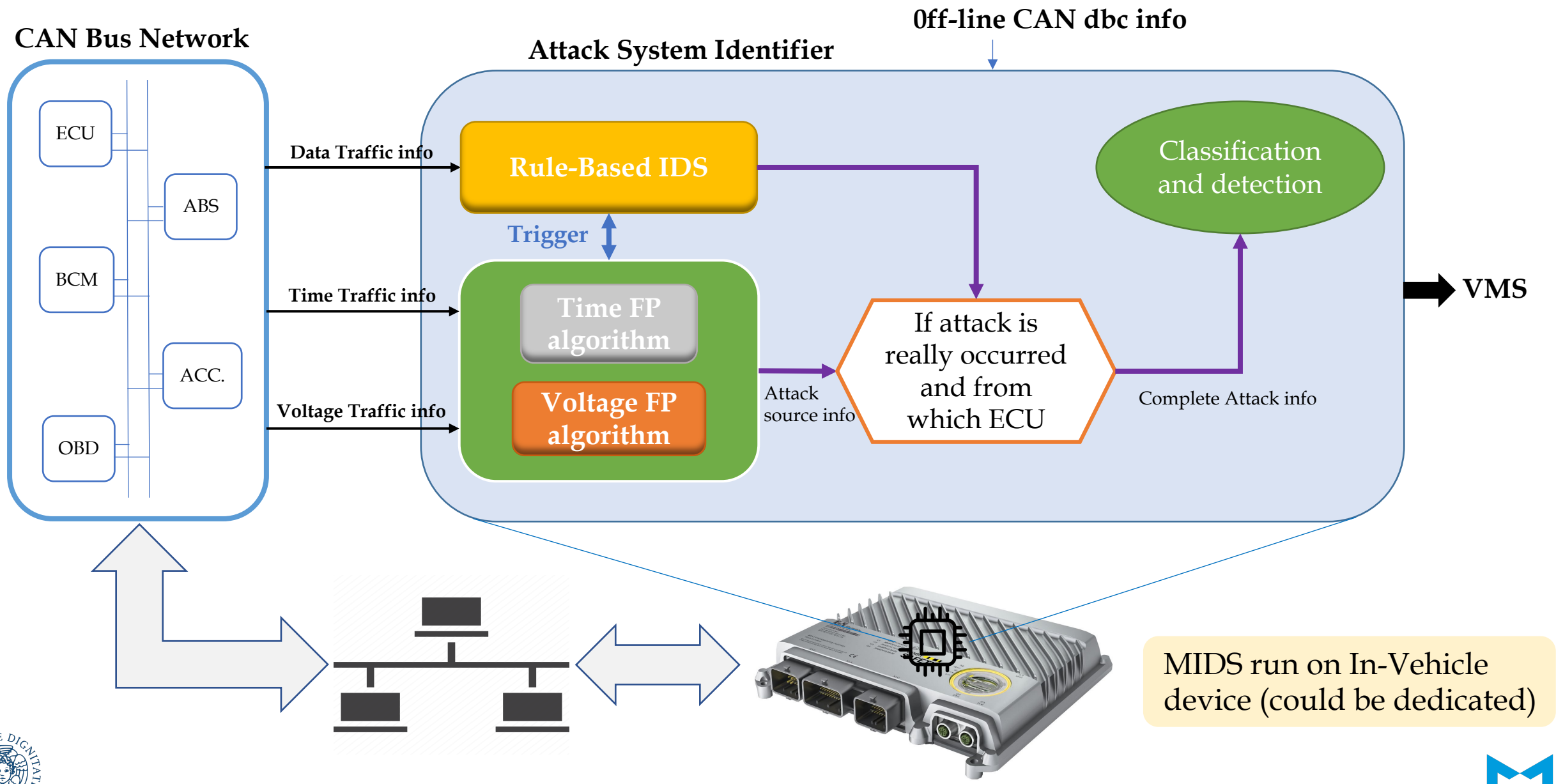


- Slow in Anomaly Check
- Issue with External Node recognition
- Great with Node suspension

Integration of Algorithms

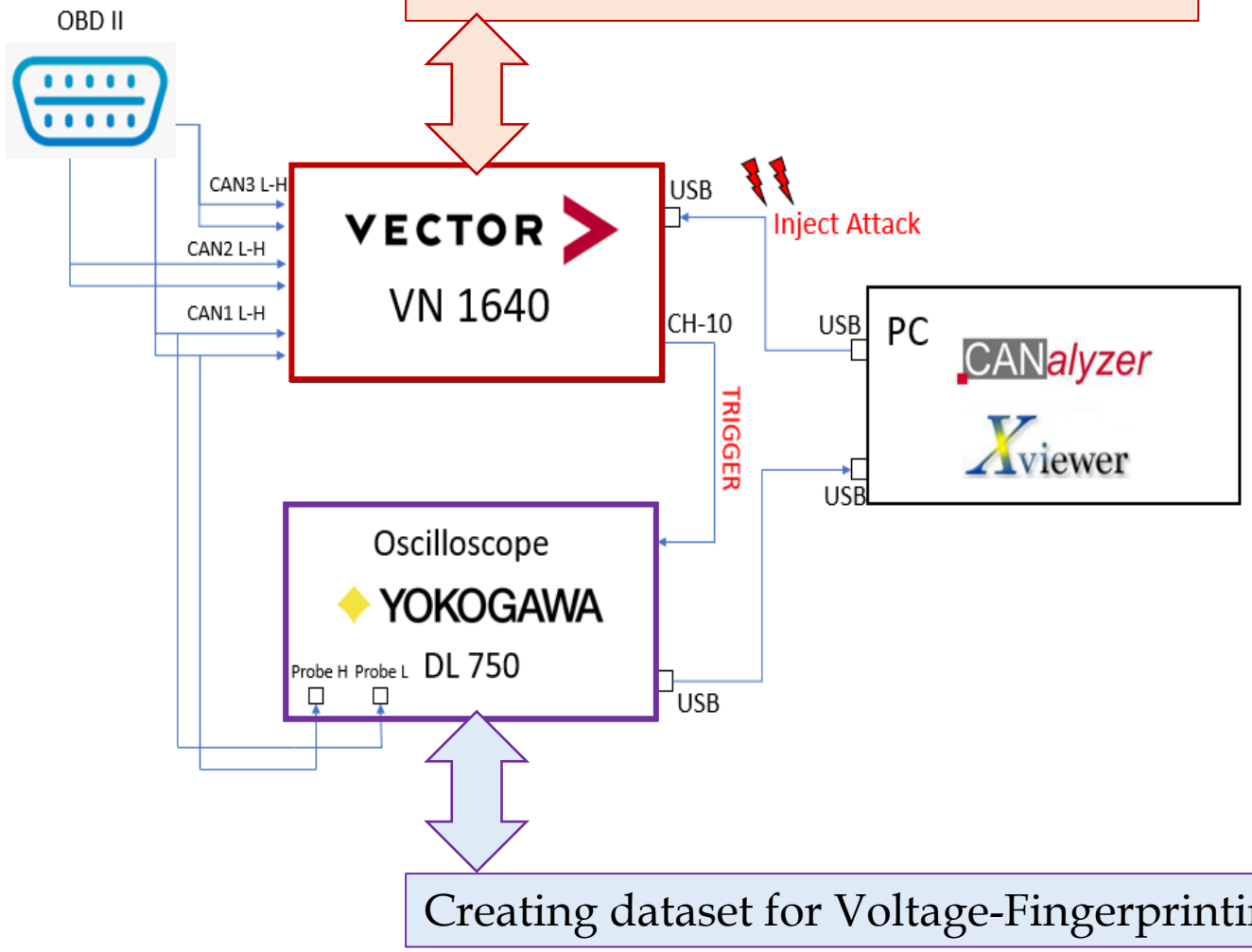
- Fast Anomaly Check
- Great with Nodes changing
- Great with Node suspension
- Decreasing of FP ratio
- ....

Multifeatured IDS



Validation Setup – Real Data Collection

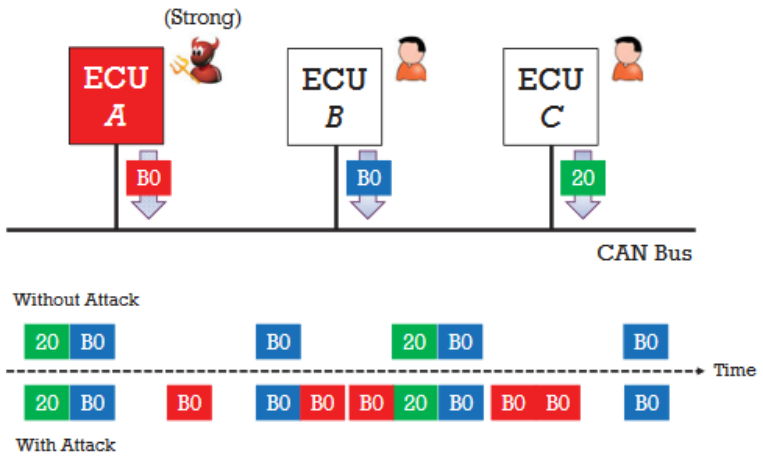
Creating dataset for Rule-based IDS
And Time-Fingerprinting



Creating dataset for Voltage-Fingerprinting

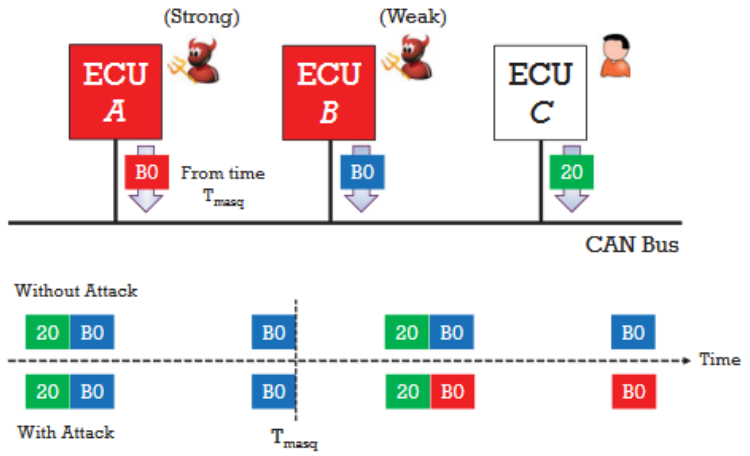
Validation Setup – Reference Attack Models

Fabrication Attack



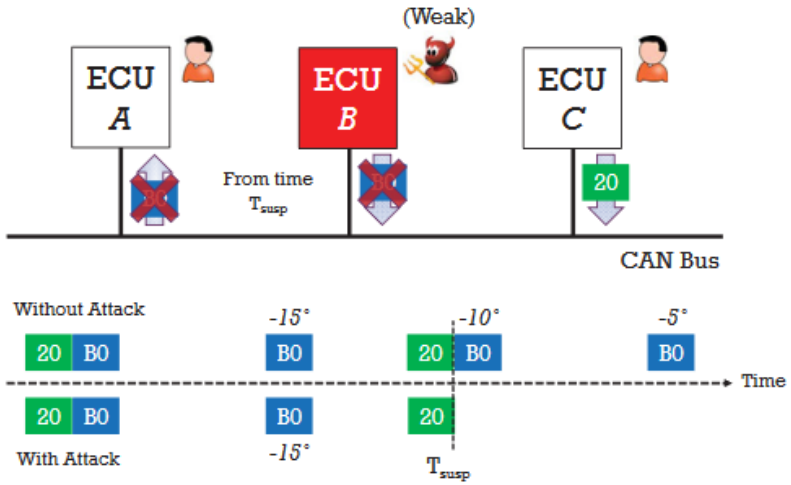
Adversary fabricates and injects messages with forged ID, DLC, and data.

Masquerade Attack



Adversary is able to manipulate an ECU, exploiting another compromised.

Suspension Attack



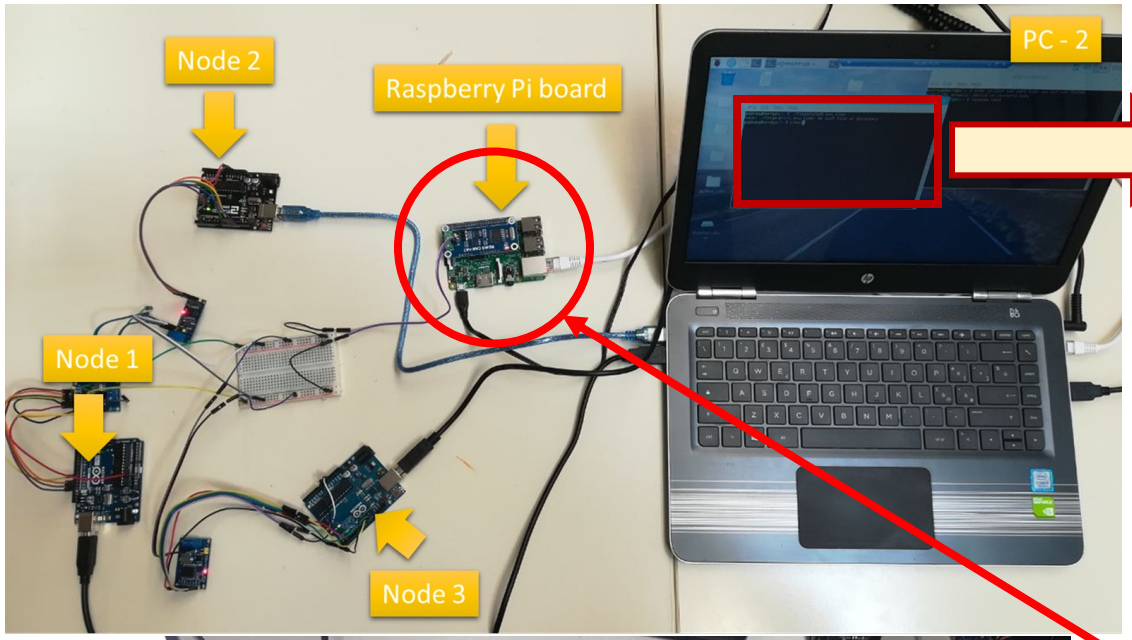
Adversary is able to stop/suspend ECU and its data traffic.

- **Weak Attacker**: the attacker is assumed to be able to stop/suspend the ECU from transmitting certain messages or listen only mode. Cannot inject any fabricated messages.
- **Strong Attacker**: the attacker is assumed to have full control of it and access to memory data. In addiction to what a weak attacker can do, this attacker controlling a fully compromised ECU can mount attacks by injecting arbitrary attack message.

IN SUPREMÆ DIGNITATIS 1343

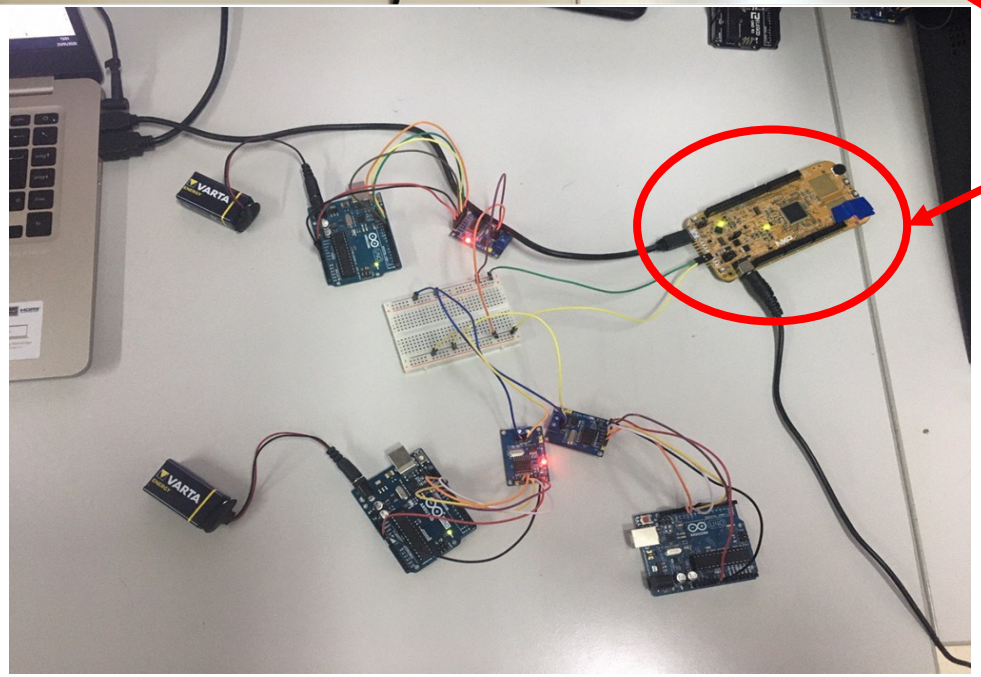
MARELLI

Validation Setup – Analysis & Testing



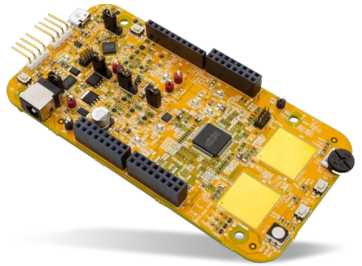

```
Console  Tasks  Peripheral Registers Values  Problems  Exe
<terminated> can_pal_s32k144_new_debug_flash_pemicro [GDB PEMicro Interface
P&E Semihosting Console

media clock Status ID 0x120 0.845391

media clock Status ID 0x1FC 0.693206

media clock Status ID 0x1EF 0.845407

media clock Status ID 0x2EF 0.842347

**** inizio analisi ON-LINE ****
ID 0x120 --> fuori intervallo di confidenza --> 0.134432
ID 0x120 --> fuori intervallo di confidenza --> 0.134432
ID 0x1EF --> fuori intervallo di confidenza --> 0.536141
ID 0x1EF --> fuori intervallo di confidenza --> 0.536141
ID 0x1FC --> fuori intervallo di confidenza --> 0.693263
ID 0x1EF --> fuori intervallo di confidenza --> 0.226902
ID 0x1EF --> fuori intervallo di confidenza --> 0.226902
ID 0x1FC --> fuori intervallo di confidenza --> 0.772793
ID 0x1EF --> fuori intervallo di confidenza --> 0.072190
ID 0x1EF --> fuori intervallo di confidenza --> 0.072190
ID 0x1EF --> fuori intervallo di confidenza --> 0.536141
ID 0x1EF --> fuori intervallo di confidenza --> 0.536141
ID 0x120 --> fuori intervallo di confidenza --> 0.359808
ID 0x1EF --> fuori intervallo di confidenza --> 0.226902
ID 0x1EF --> fuori intervallo di confidenza --> 0.226902
ID 0x120 --> fuori intervallo di confidenza --> 0.359808
ID 0x120 --> fuori intervallo di confidenza --> 0.536156
ID 0x1EF --> fuori intervallo di confidenza --> 0.763058
ID 0x1EF --> fuori intervallo di confidenza --> 0.763058
ID 0x120 --> fuori intervallo di confidenza --> 0.536156
ID 0x120 --> fuori intervallo di confidenza --> 0.536156
```

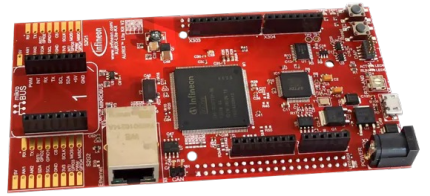
- easy for tuning phase
- on-line test
- representative configuration

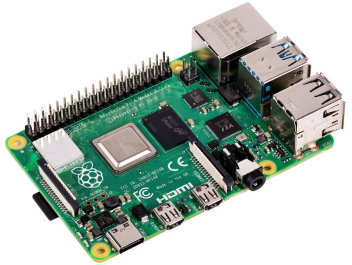


Test/Comparison for different Embedded Systems

NXP infineon RaspberryPi

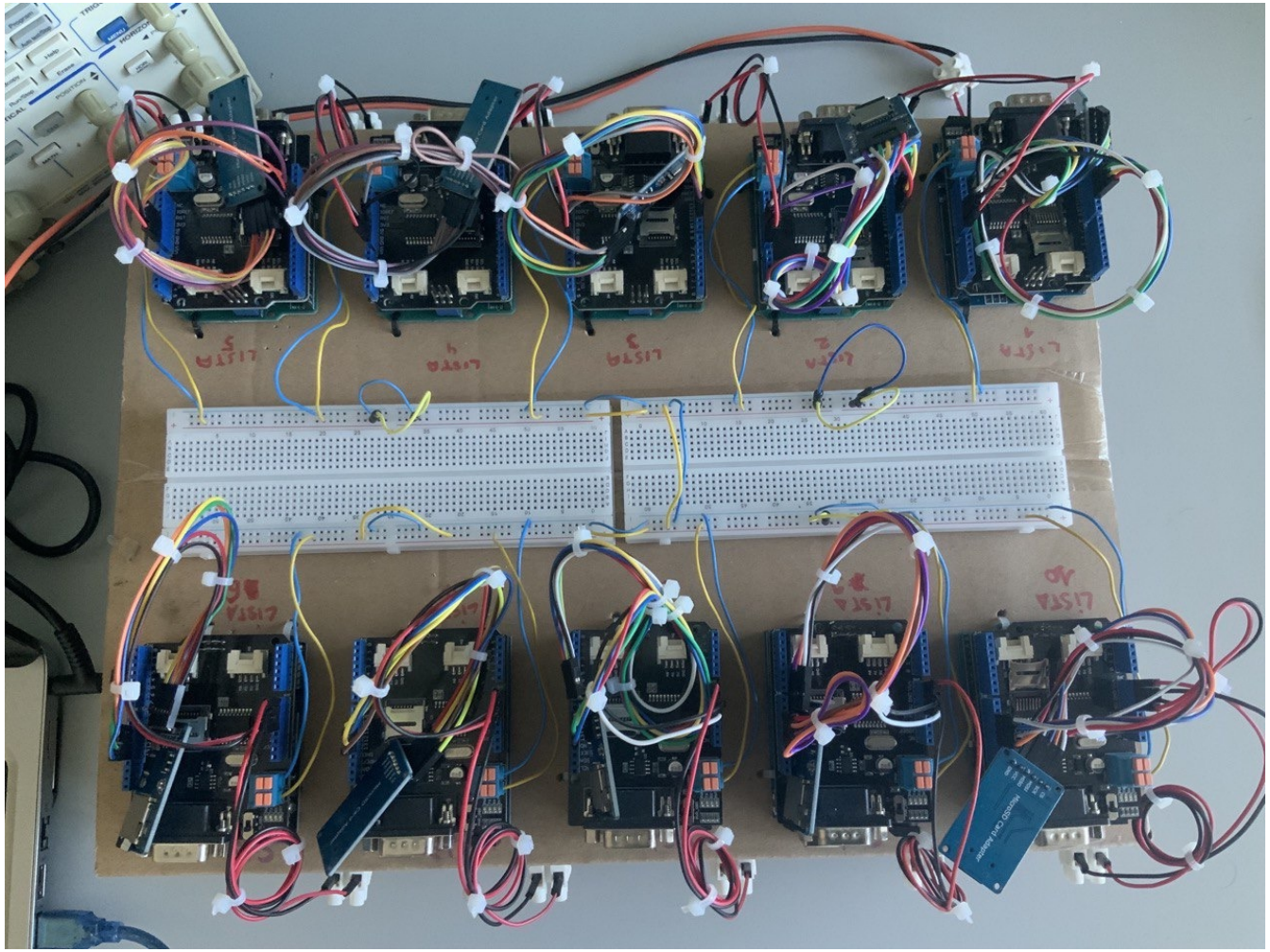






Validation Setup – Test Bench Improvement

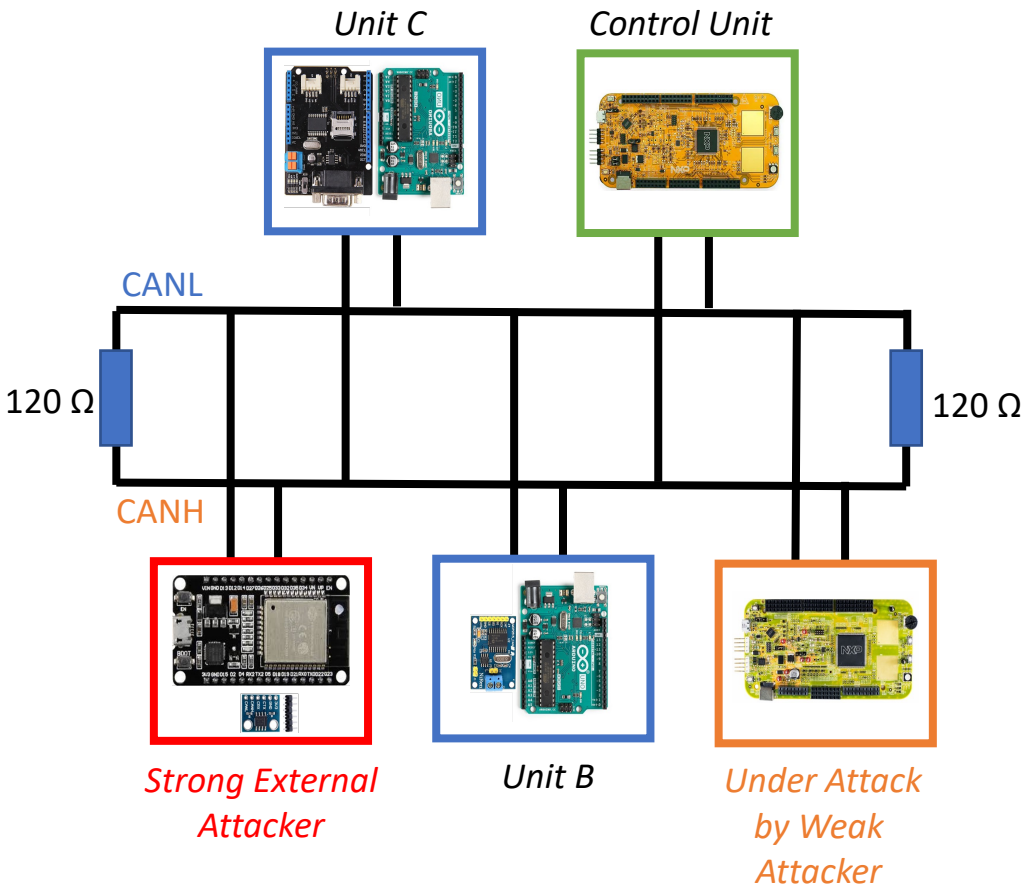
Test directly on real demonstrator



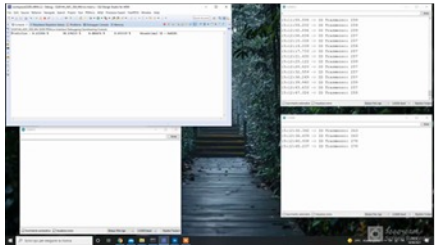
- Use of Prototyping Tools
  (Arduino EVB, SD cards, Plug-in Shields)
- Increased flexibility in validation
  of algorithms
- Increase in measurable physical layers
- Acceptable operational limitations
  (respect of high-rate periodicity)

Validation of Rule-Based + Time-Based

Attack Simulation Setup

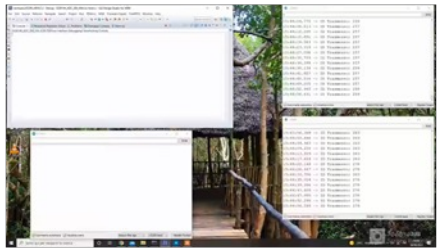


Replay Attack



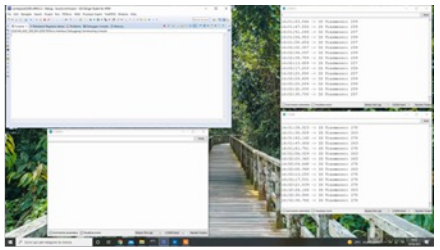
Every time a message with an ID belongs to *Unit A* is sent, the *Strong Attacker* replies on the bus with a message with the same ID sent by Unit A but different data frame

Impersonation Attack

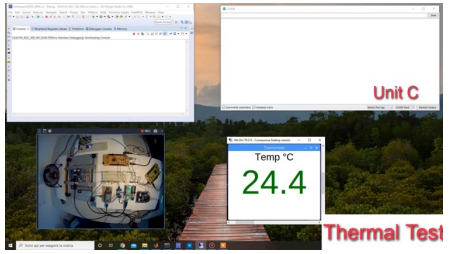


Unit A is under attack of *Weak Attacker*. It stops sending any message. *Strong Attacker* sends *Unit A* ID messages to impersonate the unit weakly compromised.

Injection Attack



Strong Attacker uses just high frequency messages with ID=0x00 in order to occupy the bus wining all arbitration phase. The other units can not communicate between them.



Thermal Test

The test was carried out between 25°C ÷ 83°C.
Every 5°C increment, 4 messages are sent on the bus

	Unit C is the sender			
	Classified as A	**Classified as B**	**Classified as C**	**Classified as Unk**
Mean **score**	0.4%	0.01%	99.3%	0.3%
Std Dev **score**	0.1%	0.01%	0.3%	0.2%
N. of times **score** ≥ 67%	0	0	48	0
N. of times **score** ≥ 90%	0	0	48	0

Thanks for your Attention!