Anomaly Detection for Dependable RISC-V-based Systems in Safety-Critical Applications

Niccolò Frascarelli, Nicasio Canino, Pierpaolo Dini, Daniele Rossi, Sergio Saponara
Department of Information Engineering, University of Pisa, Pisa, Italy

Università di Pisa

Dipartimento di Ingegneria dell'Informazione

ABSTRACT

Safety-critical applications require robust mechanisms **to ensure dependability**, thus guaranteeing safe and secure operations. **Automotive and space systems operate under extreme conditions**, where failure can lead to catastrophic outcomes.

This study focuses on the automotive domain, aligning with the **EPI-SGA2 project**'s focus on **RISC-V-based embedded platforms**. We propose an **Anomaly Detection System** (ADS) that monitors CAN bus traffic to distinguish between nominal and anomalous behaviour.

TOPIC DISCUSSION

Problem

Safety-critical applications, such as those in automotive and space systems, must:

- **Ensure dependability** for their lifetime, and
- Be able to **operate under harsh conditions**

Because **failures could result in catastrophic consequences** [1]

Case Study

In the **automotive domain**, to improve dependability against:

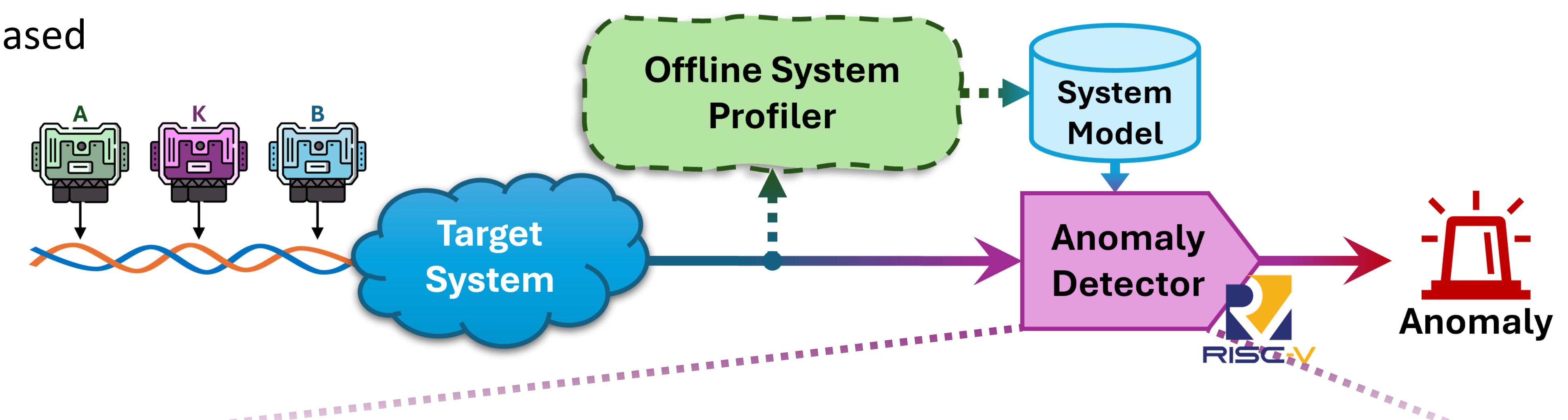
- **Hardware faults**, and
- **Cyberattacks**

We developed an **Anomaly Detection Systems (ADS)** to monitor **CAN-bus** traffic, **looking for anomalies**

METHODOLOGY

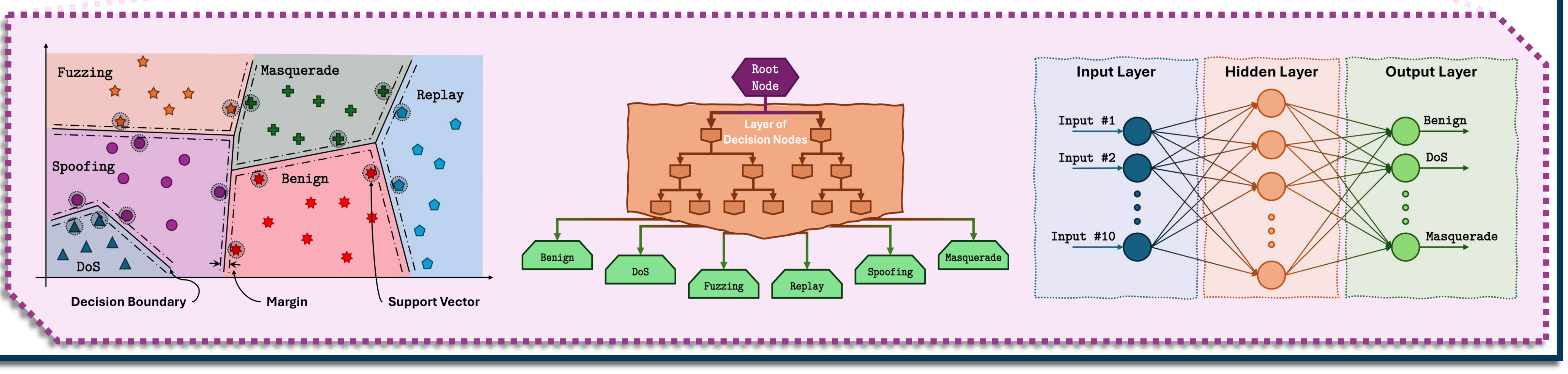
We designed a **lightweight ADS to be integrated** into a RISC-V-based platform, emphasizing:

- **memory efficiency**, and
- **real-time performance**



Main building blocks of **Anomaly Detection System (ADS):**

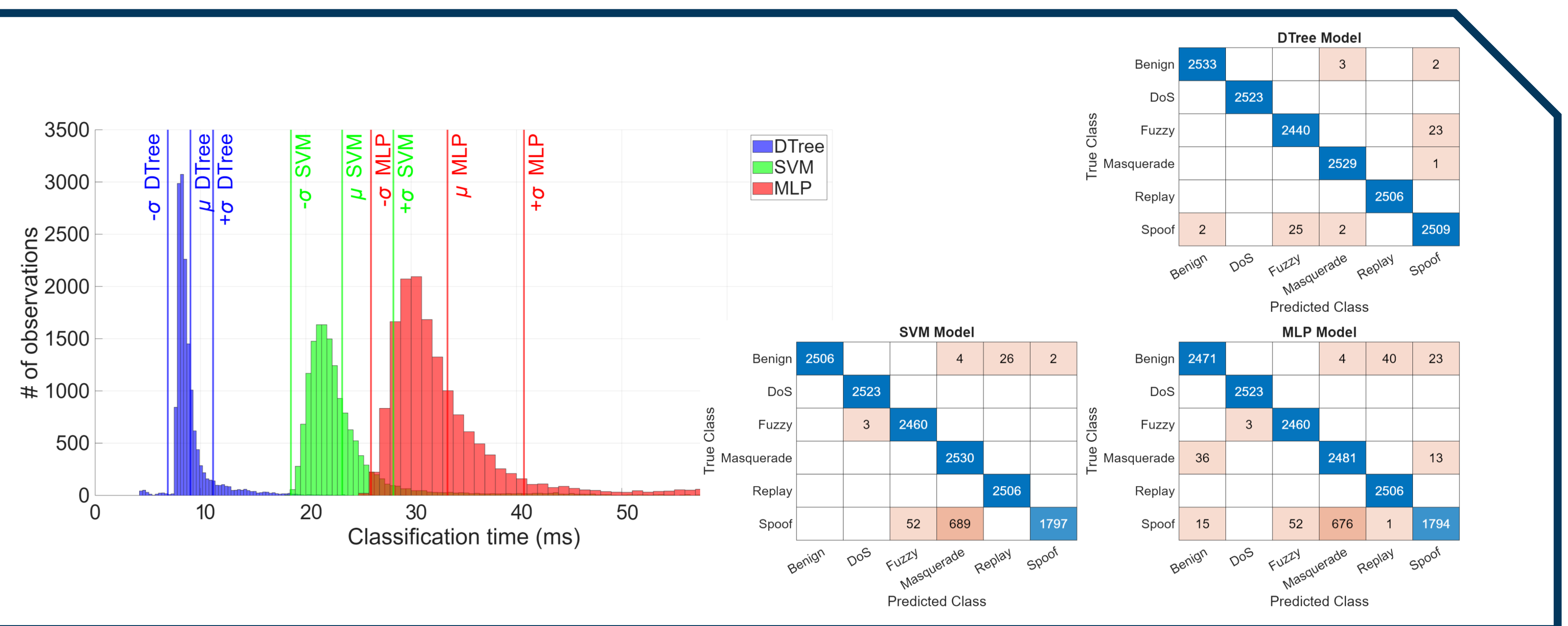
- **Target System:** CAN-bus inside the vehicle.
- **Offline System Profiler:** dataset of nominal and anomalous system behavior.
- **System Model:** parameters determined offline to classify the behavior of *Target System*.
- **Anomaly Detector:** classifier based on ML algorithms.



ANOMALY DETECTION RESULTS

Train, Validation, and Test results for the three ML models with a CAN dataset containing 6 traffic classes, benign and attacks:

Classifier	Accuracy	Memory Footprint	Classification Time
DTree	0,9962	12 KB	9,05 ms
SVM	0,9486	240 KB	25,45 ms
MLP	0,9428	10 KB	33,45 ms



DTree Model

	Benign	DoS	Fuzzy	Masquerade	Replay	Spoof
Benign	2533			3		2
DoS		2523				
Fuzzy			2440			23
Masquerade				2529		1
Replay					2506	
Spoof	2		25	2		2509

SVM Model

	Benign	DoS	Fuzzy	Masquerade	Replay	Spoof
Benign	2506			4	26	2
DoS		2523				
Fuzzy		3	2460			
Masquerade				2530		
Replay					2506	
Spoof			52	689		1797

MLP Model

	Benign	DoS	Fuzzy	Masquerade	Replay	Spoof
Benign	2471			4	40	23
DoS		2523				
Fuzzy		3	2460			
Masquerade	36			2481		13
Replay					2506	
Spoof	15		52	676	1	1794

CONCLUSIONS

&

From our results, some **key findings** to implement effective **Anomaly Detection Systems**:

- **DTree classifier achieves 99.62% accuracy**, making it the most efficient choice for embedded systems.
- **Lightweight ADS can effectively monitor CAN bus** traffic under tight resource constraints.
- An **ADS can improve dependability** on platforms working in **safety-critical and harsh environments**.

FUTURE WORK

Future work will migrate towards **space domain**, adapting the ADS to **address challenges specific** to the space domain:

- **Optimize ML classifiers to handle space-related anomalies**, such as radiation-induced faults or signal interference.
- Tailor the ADS requirements for **minimal memory and energy consumption** during long-term operations.
- **Test and validate ADS in simulated space environments** for robustness assessment.

REFERENCES

[1] R. K. Kaur et al., "Dependability analysis of safety critical systems: Issues and challenges," Annals of Nuclear Energy, vol. 120, pp. 127–154, 2018.

European Processor Initiative
epi
dare