CANDoSA: A Hardware Performance Counter-Based Intrusion Detection System for DoS Attacks on Automotive CAN bus

Franco Oberti[2], Stefano Di Carlo[1], Alessandro Savino[1]

[1]Politecnico di Torino, [2]Dumarey Softronix

Politecnico di Torino
Department of Control and Computer Engineering

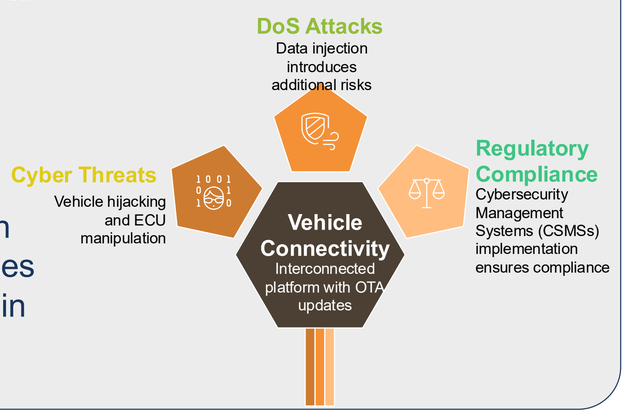
INTRODUCTION

In automotive cybersecurity, integrating advanced technologies has led to the development of sophisticated Intrusion Detection Systems (IDS) that are crucial for safeguarding connected vehicles. This research focuses on a novel IDS designed to enhance attack detection on Controller Area Network (CAN) systems by leveraging Hardware Performance Counters (HPC). The motivation behind this study stems from the increasing complexity of vehicle architectures and the corresponding rise in cyber threats, necessitating robust security measures.

MOTIVATION

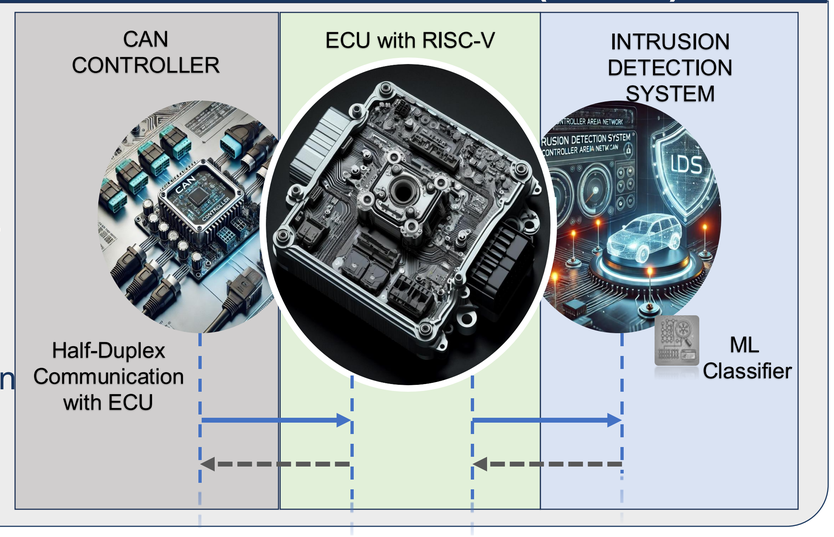
Addressing Cybersecurity Challenges: Vehicles are increasingly interconnected, making them vulnerable to cyber threats like hijacking and data manipulation. Effective cybersecurity measures are crucial for the safety and integrity of automotive systems.

Enhancing Detection Capabilities: Traditional IDS often fails to keep up with dynamic cyber attacks. This research uses HPC data to perform anomaly detection in application execution and enhance automotive security.



PERFORMANCE MONITORING UNITS (PMCs)

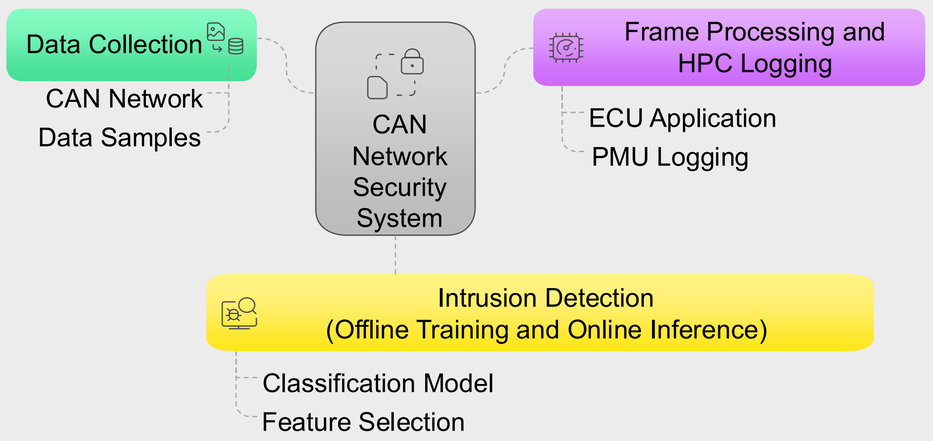
Modern Electronic Control Units (ECUs) offer monitoring features that trace execution deviations. They enhance vehicle security by detecting anomalies early, addressing vulnerabilities in interconnected systems.



CONTRIBUTION

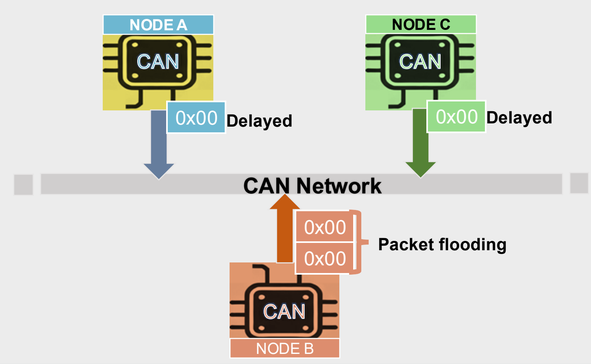
HARDWARE-BASED INTRUSION DETECTION FRAMEWORK

- Based on Three Phases:
  1. **Data Collection**
     - CAN frames are sent, received, and managed by the OS/application
  2. **Hardware Performance Counters (HPCs) logging**
     - HPCs are monitored and connected
  3. **Intrusion Detection**
     - Based on a Binary Classification Model
     - **Offline** Training
     - **Online** Inference



DATASET

- **OBD-II** port of a KIA SOUL car with regular CAN data (attack-free) and several attacks, including DoS attacks
  - H. Lee, S. H. Jeong, and H. K. Kim, "Otids: A novel intrusion detection system for in-vehicle network by using remote frame," in 2017 15th Annual Conference on Privacy, Security and Trust (PST), 2017

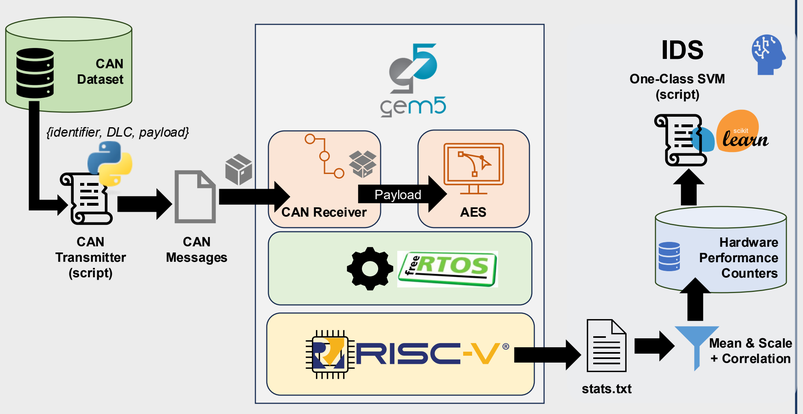


EXPERIMENTAL RESULTS

EXPERIMENTAL SET-UP

- FreeRTOS environment with a CAN Controller Receiver Task
- gem5 RISC-V full system simulation with logs as HPCs
- One-Class SVM classifier with Radial Basis Function (RBF) Kernel
- Training data ranging from 20% to 95%, with 5% as test

gem5 Based Simulation Environment



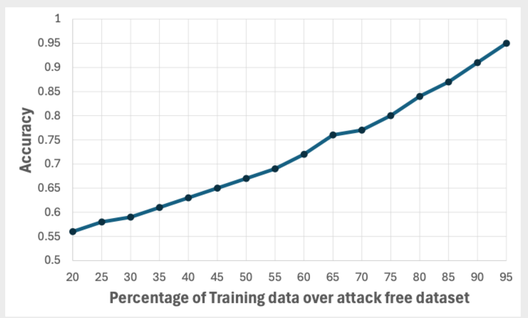
Considered Performance Counters

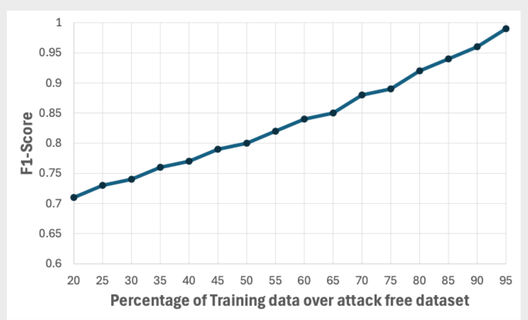
Event	Meaning	RISC-V HPC Similarity
cpu.commitStats0.numInsts	Committed instructions	minstret (Retired instruction counter)
cpu.fetchStats0.numBranches	Fetched branch instructions	Branch instructions event (PULP)
cpu.dcache.demandHits::cpu.data	Data cache Demand hits	L1 D-Cache hit event (PULP)
cpu.dcache.demandMisses::cpu.data	Data Cache Demand misses	L1 D-Cache miss event (PULP)
cpu.dcache.ReadReq.hits::cpu.data	Data Cache Read request hits	Load access event (CVA6)
cpu.dcache.ReadReq.misses::cpu.data	Data Cache Read request misses	Load access event (CVA6)
cpu.dcache.WriteReq.hits::cpu.data	Data Cache Write request hits	Store access event (CVA6)
cpu.dcache.WriteReq.misses::cpu.data	Data Cache Write request misses	Store access event (CVA6)
cpu.icache.demandHits::cpu.inst	Instruction cache Demand hits	L1 I-Cache hit event (PULP)
cpu.icache.demandMisses::cpu.inst	Instruction cache Demand misses	L1 I-Cache miss event (PULP)
cpu.icache.ReadReq.hits::cpu.inst	Instruction cache Read request hits	Instruction fetch event (CVA6)
cpu.icache.ReadReq.misses::cpu.inst	Instruction cache Read request misses	Instruction fetch event (CVA6)
l2.demandHits::cpu.data	Demand hits in the L2 cache	L2 cache hit event*
l2.demandMisses::cpu.inst	Demand misses in the L2 cache (instructions)	L2 cache miss event*
l2.demandMisses::cpu.data	Demand misses in the L2 cache (data)	L2 cache miss event*
l2.demandMisses::total	Total demand misses in the L2 cache	Total L2 cache miss event*

* (if implemented in PULP/CVA6)

Attack Detection Results

Results are with ν = 0.2, and γ = auto.





CONCLUSION

The research presents a promising approach to enhancing cybersecurity in automotive systems by integrating HPC data in IDS frameworks. While initial findings demonstrate the feasibility of detecting attacks, further experiments are necessary to **refine** the model and explore its application in safety-critical real-time embedded systems. Future work will focus on developing a comprehensive IDS that combines CAN bus anomaly detection with host-based intrusion detection, paving the way for more resilient automotive cybersecurity solutions.

This work was supported by Project SERICS through the MUR National Recovery and Resilience Plan, funded by the European Union NextGenerationEU under Grant PE00000014, project COLTRANE-V funded by the Ministero dell'Universit` a e della Ricerca within the PRIN 2022 program (D.D.104 - 02/02/2022), and Project Vitamin-V funded by the European Union: Project 101093062.

franco.oberti@dumarey.com
stefano.dicarlo@polito.it
alessandro.savino@polito.it