SYNOPSIS

Title: Securing Connected and Autonomous Vehicles through AI-based Threat Detection and Incident Response

1. Introduction & Background

A key component of the next generation of Intelligent Transportation Systems (ITS) are Connected and Autonomous Vehicles (CAVs), which provide substantial gains in mobility, traffic efficiency, road safety, and environmental sustainability. CAVs facilitate real-time coordination between cars, infrastructure, and traffic management systems by utilising enhanced sensor fusion, artificial intelligence (AI), and Vehicle-to-Everything (V2X) connectivity.

However, CAVs' growing software-drivenness and connectivity greatly increase their cyber-attack surface. Vehicle safety, operational dependability, and public trust are seriously threatened by cyber-physical dangers such spoofing, denial-of-service (DoS), false data injection, remote hijacking, and sensor manipulation. Even short detection delays or inadequate mitigation might have disastrous consequences in safety-critical settings where choices must be taken in milliseconds.

The majority of solutions are still restricted to passive detection, even though current Intrusion Detection Systems (IDS) for automotive contexts have shown promising detection capabilities utilising Machine Learning (ML) and Deep Learning (DL). Their real-world deployability is limited by their reliance on isolated or unrealistic simulation settings, lack of automated, real-time reaction mechanisms, inadequate adaptation to zero-day assaults, and dataset imbalance.

2. Research problem Statement

Even though AI-based IDS for CAVs has advanced significantly, existing systems have the following serious drawbacks:

- Detection without response: In safety-critical automotive contexts, automatic incident mitigation is crucial, yet most IDS systems just generate alerts.
- Limitations of the dataset: Current models are frequently trained on tiny, unbalanced, or artificial datasets that do not accurately represent the diversity of attacks and traffic in the actual world.
- Simulation-only validation: A lot of research uses single-domain simulations, which don't account for how traffic behavior, communication networks, and vehicle dynamics interact.
- Scalability limitations: Few methods assess IDS performance in situations with heavy network traffic, limited onboard processing power, and dense traffic.
- Limited resistance to evolving and zero-day attacks: Due to their heavy reliance on labelled data, supervised ML/DL models have trouble fending off adaptive adversaries.

These drawbacks underscore the necessity of an IDS framework that is lightweight, flexible, and transportable and that combines automated incident response with real-time detection, verified in realistic multi-domain scenarios.

3. Aim and scope of this research

Designing, implementing, and experimentally validating a lightweight AI-based intrusion detection system with integrated automated incident response for connected and autonomous vehicles that can offer real-time resilience against changing cyber-physical threats is the main goal of this research.

Scope

The research encompasses:

- AI-based detection of V2X, network-level, and in-vehicle cyberattacks.
- Using a detect-decide-act cycle to integrate automated response systems.

- The creation of a synchronised co-simulation testbed with CARLA, SUMO, and NS-3.
- Assessment of the system's performance in terms of scalability, resilience against zero-day attacks, response latency, false positives, and detection accuracy.

4. Research Objectives

The research's particular goals are as follows:

- To create reliable ML and DL models that can reliably identify various cyber-physical assaults on CAVs with few false alarms.
- To create an automatic incident response system that can control and lessen risks on its own without endangering car safety.
- To include the detection-response framework for practical evaluation into a synchronized co-simulation environment (NS-3, SUMO, CARLA).
- To assess system performance empirically using criteria including scalability, response latency, false positive rate, and detection accuracy.
- To evaluate the suggested system's resistance to adaptive and zero-day assaults in dynamic traffic settings.

5. Research Methodology

The following stages make up the experimental and simulation-based technique used in this study:

1) Co-Simulation Environment Setup:-

By combining NS-3 for in-car and V2X communication modelling, SUMO for traffic and mobility simulation, and CARLA for high-fidelity vehicle dynamics and sensor simulation, a synchronised simulation testbed is created.

2) Data Collection and Preprocessing:-

To enhance model generalisation, both publicly available datasets and traffic data produced by simulations are gathered, cleaned, normalised, and balanced.

3) **ML/DL Model Development:-**

For threat identification across several attack vectors, many ML and DL models (such as Random Forest, XGBoost, CNN, and LSTM) are created and trained.

4) **Automated Incident Response Design:-**

To allow real-time mitigation measures like isolation, alarm propagation, and traffic management adaption, a detect-decide-act architecture is used to construct a lightweight response module.

5) **Experimental Evaluation and Validation:-**

The accuracy, latency, scalability, and resilience of the suggested framework are assessed under various traffic densities, attack intensities, and network loads.

6. Key Contributions of the Research

The following noteworthy contributions are made by this thesis:

- Goes beyond conventional detection-only methods by proposing a comprehensive AI-based intrusion detection and automatic response framework for CAVs.
- Creates a realistic multi-domain co-simulation test bed that integrates vehicle, traffic and network dynamics for through security assessment.
- Exhibits scalable and low-latency threat mitigation appropriate for vehicle situations with limited resources.
- Enhances resilience against zero-day and adaptive attacks through robust model design and response automation.
- Provides a deployable cybersecurity architecture that bridges the gap between academic IDS research and real-world CAV deployment.

7. Significance of the study

The results of this study enable real-time, autonomous threat mitigation, which advances cybersecurity in connected and autonomous vehicles. The suggested paradigm facilitates the safer use of CAV technology and offers a starting point for further investigation into robust, AI-powered car security systems.

8. Conclusion

By combining AI-based intrusion detection with automated incident response and verifying the method in a realistic co-simulation scenario, this study fills a significant gap in CAV cybersecurity. The suggested system offers a workable and future-ready approach for safeguarding next-generation digital transportation systems by improving operational safety, scalability, and resilience.