**Purpose of Project Work outline/ abstract**

The Project Work outline (abstract) should give an overview of the work they intend to pursue for Project Work and present a time schedule of their planned tasks or milestone events.

The proposal submitted by the student will be evaluated by the institute. The evaluation would typically include the following issues.

1. Problem definition, clarity of the proposed work by the student and the proposed outcome of the work

2. Quality of work to qualify as Project Work

2. Justification for **16 weeks of work,** which is the assigned duration for Project Work

3. Proposed action plan for carrying out the work.

Once prepared and submitted it serves as the specification document for carrying out the work. If the outline is prepared with care and in detail with sufficient inputs, it will become a plan document and will aid the student to complete the tasks effectively within the stipulated duration.

The students are requested to prepare the outline keeping this in mind and submit it in the format prescribed in the “guidelines for Project Work outline”, which is presented below in this document.

Once the outline is prepared the students may start working on the Project Work, without waiting for any approval by the institute. Modifications, if any, are required to be made. The Project Work feedback will be provided by the Institute within a period of two weeks.

**Intrusion Detection and Prevention of CAN Bus Attacks Using Deep Learning and Reinforcement Learning in Software-Defined Vehicles (SDVs).**

DISSERTATION

Submitted in partial fulfillment of the requirements of the

**M.Tech in Artificial intelligence and Machine Learning**

By

**Nicky Kattukaran**

**2022AC05445**

Under the supervision of

**Abhilash SK**

Associate Technical Architect

At KPIT Technologies, Bangalore.

BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE

Pilani (Rajasthan) INDIA

December, 2024

**II. The following format for Dissertation Outline (Abstract) should be used**

**BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI**

**FIRST SEMESTER 2024-25**

DSECLZG628T **/ AIMLCZG628T DISSERTATION**

Dissertation Title:Intrusion Detection and Prevention of CAN Bus Attacks Using Deep Learning and Reinforcement Learning in Software-Defined Vehicles (SDVs).

Name of Supervisor : Abhilash SK

Name of Student : Nicky Kattukaran

ID No. of Student : 2022AC05445

Courses Relevant for the Project & Corresponding Semester:

1. Machine Learning (1st Semester)
2. AI and ML Techniques for Cyber Security (2nd Semester)
3. Deep Neural Network (2nd Semester)
4. Reinforcement Learning (2nd Semester)
5. Advanced Deep Learning (3rd Semester)

## Abstract

Software-Defined Vehicles (SDVs) represent a transformative shift in the automotive industry, where key vehicle functionalities are governed by software, enabling advanced features such as remote diagnostics, vehicle-to-vehicle (V2V) communication, and over-the-air updates. These capabilities position SDVs as ideal platforms for autonomous driving technologies and advanced driver assistance systems (ADAS). However, the reliance on software and connectivity introduces significant cybersecurity challenges, particularly in the Controller Area Network (CAN), a critical in-vehicle communication protocol. CAN attacks, such as Denial of Service (DoS), Flooding, and Fuzzy attacks, pose severe threats by disrupting communication, impairing functionality, and compromising passenger safety.

This project proposes a novel framework to detect and mitigate CAN-based cyberattacks in SDVs by integrating advanced AI techniques. A **hybrid model** combining a CAN Transformer and a Convolutional Neural Network (CNN) is utilized for feature extraction and anomaly detection. The extracted features are fused and fed into a Multi-Layer Perceptron (MLP) classifier, which generates anomaly scores and classifies the type of CAN attack. The hybrid model leverages the CAN Transformer’s attention mechanisms to model sequential dependencies in CAN traffic while utilizing CNNs to extract spatial patterns from message data. The model is trained and validated using the OTIDS CAN dataset, ensuring its robustness in detecting complex attack patterns across real-world scenarios.

Once an anomaly is detected, the **Proximal Policy Optimization (PPO)** algorithm is employed for intrusion prevention. The PPO agent dynamically decides the optimal preventive actions to ensure vehicle safety and operational continuity. Preventive measures include dropping malicious CAN packets, reconfiguring communication priorities, and activating failsafe mechanisms such as transitioning to a degraded operational state or safely halting the vehicle. The PPO agent is trained in a simulation environment to handle various attack scenarios, optimizing its responses through reinforcement learning.

The proposed framework is evaluated on key metrics such as detection accuracy, precision, recall, and response latency to ensure real-time performance. By combining the hybrid model’s ability to detect anomalies with the PPO agent’s capacity for intelligent prevention, this project provides a scalable and adaptive solution to address the critical challenge of CAN cyberattacks in SDVs. The framework enhances the cybersecurity of in-vehicle networks, contributing to the safe and reliable operation of next-generation automotive systems.

**Key Words:** Software-Defined Vehicles (SDVs), Controller Area Network (CAN), CAN Bus Security, Cybersecurity, CAN Attacks, Denial of Service (DoS), Flooding Attacks, Fuzzy Attacks, Hybrid Model, CAN Transformer, Convolutional Neural Network (CNN), Multi-Layer Perceptron (MLP), Anomaly Detection, Proximal Policy Optimization (PPO), Intrusion Detection and Prevention.

**References:**

**Related Papers and journals:**

* <https://ieeexplore.ieee.org/document/8476919>
* <https://ieeexplore.ieee.org/document/10192485>
* <https://ieeexplore.ieee.org/document/10233123>
* <https://www.aloul.net/Papers/faloul_acs2021.pdf?utm_source=chatgpt.com>
* <https://arxiv.org/pdf/1905.11587>
* <https://cybersecurity.springeropen.com/articles/10.1186/s42400-023-00195-4>

**Software Defined Vehicles:**

* <https://www.ptc.com/en/blogs/alm/what-is-a-software-defined-vehicle>
* <https://www.valeo.com/en/everything-you-need-to-know-about-the-software-defined-vehicle-sdv/>
* <https://www.sonatus.com/blog/what-is-a-software-defined-vehicle/>
* <https://blackberry.qnx.com/en/ultimate-guides/software-defined-vehicle>
* <https://www.bosch-mobility.com/en/mobility-topics/software-defined-vehicle/>
* <https://www.keysight.com/us/en/cmp/topics/what-is-a-software-defined-vehicle.html>
* <https://www.pwc.com/jp/en/knowledge/column/definition-of-sdv.html>
* <https://www.md-elektronik.com/en/software-defined-vehicle-swdv-and-the-impacts-on-the-onboard-network/>

**CAN Protocol**

* <https://www.javatpoint.com/can-protocol>
* <https://www.csselectronics.com/pages/can-bus-simple-intro-tutorial>
* <https://kvaser.com/can-protocol-tutorial/>
* <https://en.wikipedia.org/wiki/CAN_bus>
* <https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/controller-area-network--can--overview.html?srsltid=AfmBOorKYvDYxzjOmo7puNGsKa_3Iy4c4DWLyPdRviPTHjCGgGByM_EO>
* <https://www.tutorialspoint.com/can-protocol>

**Dataset**

* <https://ocslab.hksecurity.net/Dataset/CAN-intrusion-dataset>

**Simulation**

* **Canoe**
* <https://www.vector.com/at/en/products/products-a-z/software/canoe/simulation/#c201134>
* <https://www.researchgate.net/publication/339547929_Integrating_Adversary_Models_and_Intrusion_Detection_Systems_for_In-vehicle_Networks_in_CANoe>
* <https://personales.upv.es/thinkmind/dl/conferences/vehicular/vehicular_2022/vehicular_2022_1_30_30014.pdf>
* <https://pure.coventry.ac.uk/ws/portalfiles/portal/25799443/Binder4.pdf>
* <https://pure.coventry.ac.uk/ws/portalfiles/portal/51847901/AI_CyberSec_2021_An_automotive_security_testbed_Camera_ready_.pdf>
* <https://www.researchgate.net/figure/System-implementation-based-on-CANoe_fig1_266643434>
* <https://publications.lib.chalmers.se/records/fulltext/251871/251871.pdf>
* **Carla**
* <https://ceur-ws.org/Vol-3125/paper5.pdf>
* <https://carla.readthedocs.io/en/latest/start_introduction/>
* <https://www.cs.ox.ac.uk/files/10140/Towards_a_Simulation-based_Framework_for_the_Security_Testing_of_Autonomous_Vehicles_Eduard_dos_Santos_Escar_USA_2018.pdf>
* <https://tum-esi.github.io/publications-list/PDF/2023-VTC-Simutack.pdf>
* <https://carla.org/>

**BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI**

**I SEMESTER 24-25**

DSECLZG628T **/ AIMLCZG628T DISSERTATION**

**Dissertation Outline (Abstract)**

**BITS ID No.** 2022AC05445 **Name of Student:** Nicky Kattukaran

**Name of Supervisor:** Abhilash SK

**Designation of Supervisor**: Associate Technical Architect, KPIT Technologies, Bangalore.

**Qualification and Experience:** B.Tech (ECE) and M.E. (ECE) with 10 years of Experience in Machine Learning and Deep Learning.

**Official E- mail ID of Supervisor:** abhilash.sk@kpit.com

**Topic of Dissertation**: Intrusion Detection and Prevention of CAN Bus Attacks Using Deep Learning and Reinforcement Learning in Software-Defined Vehicles (SDVs).

Nicky Kattukaran Abhilash SK

(Signature of Student) (Signature of Supervisor)

Date: 20-12-2024 Date: 20-12-2024

The following pages give basic guidelines regarding the Project Work requirement and the outline (abstract) preparation.

**Guidelines for Project Work outline (abstract) document preparation**

The student should prepare a detailed **outline** of the Project Work in consultation with his/her Supervisor. Current literature (journals, books etc.) may be reviewed to support your work.

**Project Work Title**

Title should reflect the work that is to be carried out and should not be a very general in nature.

**Discussion on the chosen topic**

This section should include:

1. The purpose of the work and expected outcome of the work

2. Literature review done in connection with the work, if applicable

3. Brief discussion on the existing process and its limitations

4. Justification for selecting a particular methodology for completing the tasks

5. Brief discussion on the Project Work methodology

6. Benefits derivable from the work

7. Any other details in support of the work

**Detailed plan of work**

In this section you are required to break down the Project Work into identifiable activities and give duration for each of these sub tasks, thus justifying for 16 weeks of work.

**Format for the outline (abstract) document to be submitted is presented in the following pages that has to be strictly followed.**

**Please note that: Outline document has to be uploaded on the viva portal.**

1. **Broad Area of Work**

The research focuses on enhancing cybersecurity in Software-Defined Vehicles (SDVs) by addressing vulnerabilities in the Controller Area Network (CAN), a critical in-vehicle communication protocol. With the increasing reliance on software for vehicle functionality, including autonomous driving and advanced driver assistance systems (ADAS), CAN networks face heightened risks from cyberattacks such as Denial of Service (DoS) and spoofing. The work integrates advanced artificial intelligence techniques, such as hybrid deep learning models and reinforcement learning algorithms, to detect and mitigate these attacks. This multidisciplinary approach combines cybersecurity, machine learning, and vehicular technology to ensure safe and reliable operation in next-generation automotive systems.

1. **Objectives**

The objectives of my project are as follows:

 **Enhance Cybersecurity in SDVs**: Develop a robust framework to detect and mitigate cyberattacks on the Controller Area Network (CAN) in Software-Defined Vehicles (SDVs).

 **Anomaly Detection**: Design a hybrid deep learning model combining CAN Transformer and Convolutional Neural Networks (CNNs) to detect anomalies and classify attack types based on sequential and spatial patterns in CAN traffic.

 **Intrusion Prevention**: Utilize Proximal Policy Optimization (PPO), a reinforcement learning algorithm, to dynamically determine and execute optimal preventive measures against CAN cyberattacks.

 **Simulation and Validation**: Create a simulated environment to train and evaluate the framework using real-world CAN datasets like OTIDS, ensuring high accuracy, precision, and real-time response.

 **Scalability and Adaptability**: Ensure the proposed framework is scalable and adaptive to various cyberattack scenarios, enhancing the safety and reliability of next-generation vehicular systems.

# 3. **Scope of Work**

Scope of this dissertation is to design and develop –

This research focuses on developing a cybersecurity framework to detect and mitigate CAN-based cyberattacks in Software-Defined Vehicles (SDVs). The framework integrates a hybrid deep learning model, combining a CAN Transformer for temporal analysis and Convolutional Neural Networks (CNNs) for spatial pattern recognition, to detect anomalies and classify attack types. Proximal Policy Optimization (PPO) is employed to dynamically decide and implement preventive actions against identified threats. The framework is trained and validated using the OTIDS CAN dataset and tested in simulated attack scenarios. Emphasis is placed on real-time performance, scalability, and adaptability to ensure robust protection for next-generation vehicular systems.

**4. Detailed Plan of Work (Sample)** (for 16 weeks)

The plan of work should have tangible weekly or fortnightly milestones and deliverables, which can be measured to assess the adherence to the plan and therefore the rate of progress in the work. The plan of work can be specified in the table given below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Serial Number of Task/Phases** | **Tasks or subtasks to be done (be precise and specific)** | **Start Date-End Date** | **Planned duration in weeks** | **Specific Deliverable in terms of the project** |
| 1. | Literature Review: Study existing CAN attack detection frameworks, hybrid deep learning models, and RL algorithms | Week 1 - Week 2 | 2 weeks | Comprehensive literature review report |
| 2. | Dataset Preprocessing: Analyze OTIDS dataset, clean data, normalize fields, and prepare sequences for training | Week 3 | 1 week | Preprocessed dataset ready for model training |
| 3. | CAN Transformer Design: Implement CAN Transformer architecture for sequential dependency modeling | Week 4 - Week 5 | 2 weeks | CAN Transformer model implementation and initial testing |
| 4. | CNN Model Design: Implement CNN architecture for extracting spatial features from CAN data | Week 6 | 1 week | CNN model implementation and initial testing |
| 5. | Hybrid Model Integration: Fuse CAN Transformer and CNN outputs into an MLP classifier for anomaly detection | Week 7 - Week 8 | 2 weeks | Integrated hybrid anomaly detection model |
| 6. | Hybrid Model Training and Validation: Train and validate the hybrid model using OTIDS dataset | Week 9 - Week 10 | 2 weeks | Trained hybrid model with evaluation metrics (accuracy, precision, recall, F1-score) |
| 7. | PPO Algorithm Design: Implement PPO agent for intrusion prevention | Week 11 | 1 week | PPO algorithm implementation |
| 8. | Simulation Environment Setup: Develop simulation environment with various CAN attack scenarios (DoS, flooding, spoofing) | Week 12 | 1 week | Simulated environment for testing and training PPO agent |
| 9. | PPO Training: Train the PPO agent in simulated attack scenarios | Week 13 - Week 14 | 2 weeks | Trained PPO agent with optimal preventive strategies |
| 10. | End-to-End Framework Integration: Combine hybrid detection model and PPO agent into a complete pipeline | Week 15 | 1 week | Integrated end-to-end cybersecurity framework |
| 11. | Final Evaluation and Refinement: Test the framework, refine hyperparameters, and optimize for real-time performance | Week 16 | 1 week | Finalized and optimized framework with performance metrics |

# **Literature References**

The following are referred journals from the preliminary literature review.

*[1] Agrawal K, Alladi T, Agrawal A, Chamola V, Benslimane A. 2022. NovelADS: a novel anomaly detection system for intra-vehicular networks. IEEE Transactions on*

*Intelligent Transportation Systems 23:22596\_22606 DOI 10.1109/TITS.2022.3146024.*

*[2] Cuzzocrea A, Mercaldo F, Martinelli F. 2020. A deep-learning-based framework for*

*supporting analysis and detection of attacks on CAN buses. Procedia Computer*

*Science 176:2999\_3008 DOI 10.1016/j.procs.2020.09.203.*

*[3] Jeong W, Han S, Choi E, Lee S, Choi JW. 2020. CNN-based adaptive source node*

*identifier for controller area network (CAN). IEEE Transactions on Vehicular*

*Technology 69:13916\_13920 DOI 10.1109/TVT.2020.3016352.*

*[4] Khandelwal S, Wadhwa E, Shreejith S. 2022. Deep learning-based embedded intrusion detection system for automotive CAN. In: 2022 IEEE 33rd international conference on application-specific systems, architectures and processors (ASAP). Piscataway: IEEE, 88\_92 DOI 10.1109/ASAP54787.2022.00023.*

*[5] Lokman SF, Othman AT, Musa S, Abu Bakar MH. 2019. Deep contractive autoencoderbased anomaly detection for in-vehicle controller area network (CAN). In: Abu Bakar MH, Mohamad Sidik MS, Öchsner A, eds. Progress in engineering technology: automotive, energy generation, quality control and efficiency, Cham: Springer International Publishing, 195\_205 DOI 10.1007/978-3-030-28505-0\_16.*

**Supervisor’s Rating of the Technical Quality of this Dissertation Outline**

EXCELLENT / GOOD / FAIR/ POOR (Please specify): GOOD

**Supervisor’s suggestions and remarks about the outline (if applicable).**

Date: 20-12-2024 Abhilash SK (Signature of Supervisor)

Name of the supervisor: Abhilash SK

Email Id of Supervisor: abhilash.sk@kpit.com

Mob # of supervisor: 9900809827