World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

# Real Time Anomaly Detection and Intrusion Detection for Safeguarding Intra-Vehicle Communication Powered by AI

Chitoor Venkat Rao Ajay Kumar [1], Parnam Venkatagirish [2], Sai Srinivas Patibandla [2,*] and Kapil Rathod [2]

[1] *Assistant Professor of Department of CSE(AI&ML).*
[2] *Students of Department CSE (AI&ML) of ACE Engineering College.*

World Journal of Advanced Research and Reviews, 2025, 25(01), 1992–2000

Publication history: Received on 17 December 2024; revised on 25 January 2025; accepted on 21 January 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.1.0283

## Abstract

This study addresses cyber-attacks in Electric Vehicles (EVs) and proposes an intelligent, secure framework to protect both in-vehicle and vehicle-to-vehicle communication systems. The proposed model uses an improved support vector machine (SVM) for anomaly and intrusion detection based on the Controller Area Network (CAN) protocol a critical component in vehicle communication. To further enhance detection speed and accuracy a new optimization algorithm the Social Spider Optimization (SSO) is introduced for reinforcing the offline training process. Simulation results on real-world datasets demonstrate the model's high performance, reliability and ability to defend against denial-of-service (DoS) attacks in EVs.

**Keywords:** Cyber-Attacks; Electric Vehicles (Evs); Intelligent Framework; Controller Area Network (CAN); Anomaly Detection; Intrusion Detection; Support Vector Machine (SVM); Social Spider Optimization (SSO); Offline Training, Simulation Results; Denial-Of-Service (Dos) Attacks

## 1. Introduction

The integration of advanced communication protocols such as CAN and LIN in electric vehicles has improved their functionality but exposed them to cybersecurity vulnerabilities. Cyber-attacks targeting intra-vehicle communication can disrupt critical systems like braking and navigation posing significant safety risks. This paper aims to address these challenges by exploring AI-based approaches for anomaly detection focusing on improving accuracy, efficiency and real-time threat mitigation. To address these challenges this study presents an intelligent, secure framework for real-time anomaly and intrusion detection in electric vehicles communication systems. The framework leverages an improved Support Vector Machine (SVM) model optimized with the Social Spider Optimization (SSO) algorithm. By enhancing the training process offline and incorporating real-time monitoring the system aims to provide robust protection against threats like denial-of-service (DoS) attacks. The results from simulations using real-world CAN bus datasets highlight the model's high performance, reliability and adaptability making it a promising solution for safeguarding EV communications.

### 1.1. Historical Background of Intra-Vehicle Communication

Intra-vehicle communication systems have evolved significantly, with the CAN protocol emerging as a standard due to its efficiency and scalability. Initially developed for automotive applications in the 1980s, CAN has since been widely adopted in various industries including medical devices and industrial automation. Despite its technical advantages the protocol's original design did not prioritize cybersecurity as vehicles at the time operated in isolation without external connectivity.

* Corresponding author: Sai Srinivas Patibandla.

The increasing integration of smart technologies and IoT devices in modern vehicles has transformed them into connected entities making them attractive targets for cybercriminals. The rise of connected EVs has brought to light the critical need for advanced cybersecurity measures to protect both intra-vehicle and inter-vehicle communication systems. Consequently, ensuring robust security has become a pivotal factor in development of intelligent vehicle systems. This study builds upon these historical advancements to propose a model tailored to the unique challenges of modern vehicular networks.

### 1.2. Benefits of Safeguarding Intra-Vehicle Communication

- **Enhanced Passenger Safety**: Prevents unauthorized access to critical vehicle systems like brakes, steering and airbags ensuring passenger safety.
- **Protection Against Cyber-Attacks**: Detects and mitigates threats such as Denial-of-Service (DoS) attacks and data spoofing reducing the risk of malicious activities.
- **Improved Vehicle Reliability**: Ensures consistent and accurate communication between vehicle components leading to better performance and reduced operational disruptions.
- **Data Integrity and Privacy**: Safeguards sensitive data such as driver behavior and navigation information from unauthorized access and misuse.
- **Compliance with Industry Standards**: Meets automotive cybersecurity standards (e.g., ISO/SAE 21434) and regulatory requirements ensuring the vehicle's communication systems adhere to safety and security protocols.
- **Real-Time Anomaly Detection**: Provides real-time monitoring to detect and respond to anomalies or irregularities promptly minimizing potential risks.
- **Adaptability to Emerging Threats**: Incorporates AI and machine learning algorithms to evolve with new types of cyber threats ensuring long-term protection.
- **Trust and Brand Reputation**: Builds consumer confidence in the safety and reliability of vehicles enhancing the manufacturer’s reputation.
- **Minimized Downtime and Maintenance Costs**: Reduces the likelihood of system failures caused by cyber-attacks leading to lower maintenance and repair costs.
- **Support for Advanced Features**: Enables the secure implementation of advanced driver-assistance systems (ADAS) and autonomous driving technologies by protecting communication network
- **Prevention of Financial Losses:** Safeguarding intra-vehicle communication helps to prevent financial losses associated with cyber-attacks including vehicle recalls, legal liabilities and reputational damage to manufacturers

## 2. Literature Review

Due to the increasing need for secure and reliable intra-vehicle communication research into anomaly detection methods has gained significant traction. Various studies have explored different algorithms, techniques and frameworks for ensuring the safety and security of vehicular networks.

- Kumar and Sharma (2021) proposed a Support Vector Machine (SVM)-based model for anomaly detection in CAN bus communication. Their approach achieved an accuracy of 89% in detecting cyber threats such as denial-of-service (DoS) attacks. However, their study emphasized the need for optimizing hyperparameters to reduce false positives and enhance performance.
- Lee et al. (2020) investigated the application of Long Short-Term Memory (LSTM) networks for cybersecurity in vehicular networks. Their method effectively modeled temporal dependencies in CAN bus data achieving a

detection rate of 93%. Despite its accuracy the study highlighted challenges related to high computational costs limiting real-time implementation.

- Zhang and Gupta (2022) introduced a hybrid anomaly detection framework combining Decision Trees (DT) and Random Forest (RF). This ensemble approach demonstrated improved detection capabilities achieving an accuracy of 91%. The study suggested lightweight alternatives for resource-constrained vehicular systems.

- Wang et al. (2021) explored unsupervised learning methods including clustering and autoencoders to identify previously unseen attack patterns. While effective in detecting novel anomalies their model required extensive tuning to balance sensitivity and specificity.

- Loukas et al. (2019) conducted a comprehensive survey of intrusion detection approaches for vehicular networks. They categorized techniques into signature-based, anomaly-based and hybrid methods emphasizing the need for adaptive models capable of evolving with emerging threats.

- Park et al. (2023) applied deep reinforcement learning (Deep RL) to detect and prevent cyber-attacks in automotive networks. Their model utilized dynamic data from multiple sensors achieving real-time detection with high precision. However, their approach faced scalability challenges in resource-constrained environments.

- Nguyen and Tran (2023) explored federated learning approaches for anomaly detection in connected vehicles. By training models across decentralized datasets, they improved privacy while maintaining detection accuracy. The study highlighted the potential of federated learning in enhancing cybersecurity without compromising data confidentiality.

These studies collectively underscore the importance of integrating machine learning and optimization techniques to enhance the security and reliability of vehicular communication systems.

### 2.1. Existing System

Existing Anomaly detection systems for intra-vehicle communication primarily rely on traditional techniques such as signature-based and rule-based methods. These systems work by identifying known attack patterns or predefined rules within the Controller Area Network (CAN) bus data. For instance, many employ algorithms to monitor CAN messages frequency and signal inconsistencies.

#### *2.1.1. Key Features*

- Signature Based Detection: These systems maintain a database of known attack signatures and match incoming data against these signatures to identify threats.

- Rule-Based Systems: Predefined rules are used to

- detect abnormalities in communication patterns such as deviations in message intervals or invalid data.

- Machine Learning Models: Basic models including Decision Trees and Support Vector Machines have been utilized for anomaly detection but often lack optimization for real-time applications.

### 2.2. Disadvantages of Existing System

#### *2.2.1. Limited Detection of Unknown Attacks*

Signature-based systems can only detect known threats, making them ineffective against zero-day attacks or novel anomalies.

#### *2.2.2. High False Positives*

Rule-based methods often flag normal variations as threats, leading to disruptions and unnecessary interventions.

#### *2.2.3. Lack of Real-Time Capabilities*

Many systems struggle to process large volumes of CAN bus data in real-time delaying threat detection.

#### *2.2.4. Scalability Issues*

Existing methods are not designed to scale efficiently with the increasing complexity and connectivity of modern vehicles.

#### *2.2.5. Resource-Intensive*

Machine learning models without optimization require significant computational power limiting their deployment in resource constrained environments like vehicles.

#### *2.2.6. Static Nature*

Existing systems often lack adaptability and cannot dynamically learn or evolve with new and emerging cyber-attack patterns reducing their effectiveness.

#### *2.2.7. Complex Implementation*

Attribute-based access control though flexible can be difficult to implement and manage especially when dealing with a large number of diverse users

### 2.3. Proposed System

The proposed framework incorporates the following components

#### *2.3.1. Data Collection and Preprocessing*

CAN bus communication data is collected and preprocessed to remove noise and standardize formats.

#### *2.3.2. Anomaly Detection Model*

A Support Vector Machine (SVM) forms the core of the anomaly detection system. It establishes normal communication patterns and flags deviations as potential threats.

#### *2.3.3. Optimization via SSO*

The SVM model is optimized using the Social Spider Optimization algorithm. This technique enhances detection accuracy by refining hyperparameters and improving the feature selection process.

#### *2.3.4. Real-Time Monitoring*

The system continuously monitors CAN bus data to identify anomalies in real-time. Alerts are triggered when suspicious activities are detected.

#### *2.3.5. Validation and Feedback*

The model is validated using real-world datasets and performance metrics are analyzed to refine the detection process.

### 2.4. Advantages of Proposed System

#### *2.4.1. High Accuracy*

The integration of SSO with SVM reduces false positives and enhances anomaly detection precision.

#### *2.4.2. 2Real-Time Threat Mitigation*

Continuous monitoring ensures prompt detection and response to cyber threats.

#### *2.4.3. Adaptability*

The model evolves with new attack patterns

ensuring long-term effectiveness.

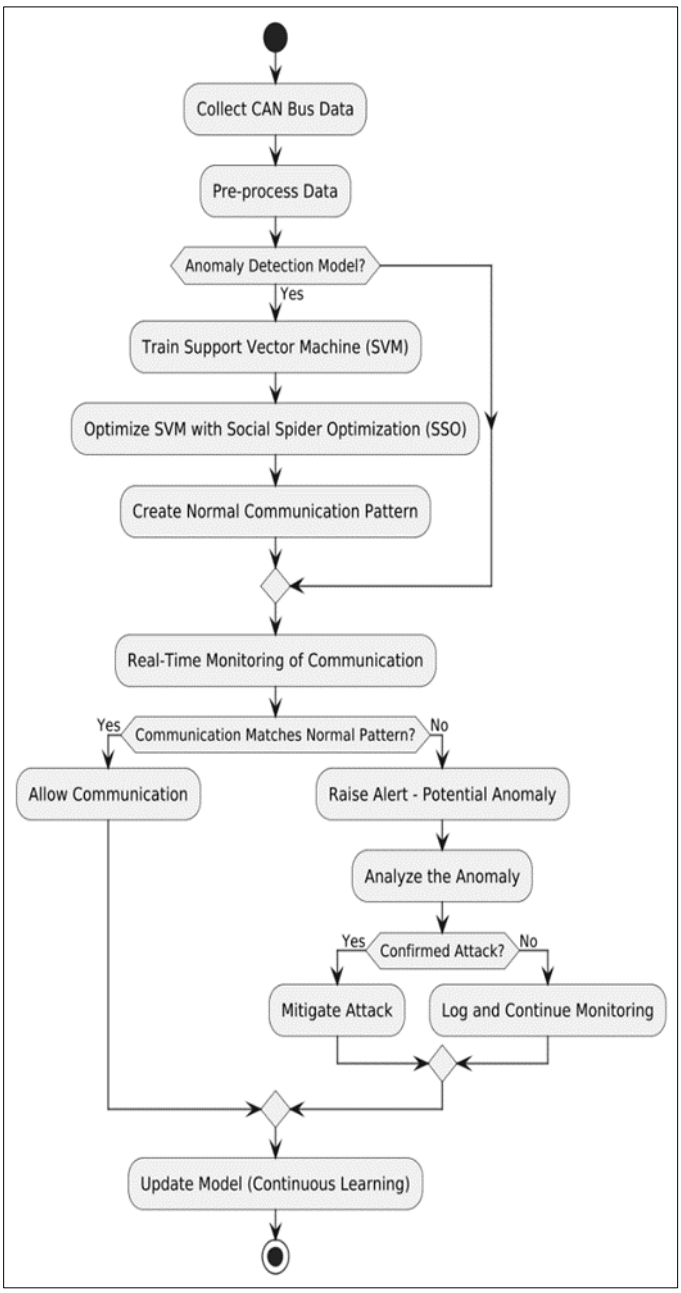
*2.4.4. Efficiency*

Optimized feature selection reduces computational overhead making the system suitable for deployment in real-time vehicular environments.

*2.4.5. Enhanced Vehicle Security*

By identifying malicious activities such as DoS attacks, the system enhances the security of intra-vehicle communication preventing dangerous situations like sudden brake activations or engine shutdown.

**2.5. Architecture**




This architecture represents a comprehensive system for anomaly detection and mitigation in Controller Area Network (CAN) bus communications a critical component in automotive and industrial systems. The process begins with the collection and pre-processing of CAN bus data to clean and normalize it for analysis. The system then trains a Support Vector Machine (SVM) a supervised learning model to recognize normal communication patterns. To enhance the SVM's

performance it is fine-tuned using the Social Spider Optimization (SSO) algorithm a metaheuristic inspired by the cooperative behavior of spiders ensuring the model is well-optimized for detecting anomalies accurately.

Once the SVM is optimized it creates a baseline for normal communication behavior which is then used for real-time monitoring of the CAN bus. As communication occurs the system compares it to the established normal pattern. If the communication matches the baseline it is allowed to proceed. However, if an anomaly is detected an alert is raised and the system analyzes the deviation to determine if it constitutes a confirmed attack. For confirmed attacks countermeasures are deployed to mitigate the threat. If the anomaly is not identified as malicious it is logged for further evaluation while monitoring continues.

A key feature of this architecture is its continuous learning capability. The model is updated with new data to adapt to evolving communication patterns and improve accuracy over time. This feedback loop ensures that the system remains proactive and resilient against new and sophisticated attack vectors, providing robust security for CAN bus communication systems. By combining machine learning, optimization techniques and real-time monitoring this architecture effectively safeguards against potential threats while allowing safe communication to proceed uninterrupted.

## 2.6. Algorithms

### *2.6.1. Support Vector Machine (SVM)*

A supervised learning algorithm used for anomaly

detection by classifying normal and abnormal communication patterns in the CAN bus data. It works by finding an optimal hyperplane that separates the data into different categories with maximum margin. SVM is effective in handling high-dimensional data and identifying complex patterns.

### *2.6.2. Social Spider Optimization (SSO)*

A metaheuristic optimization algorithm inspired by the cooperative behavior of social spiders in nature. It is used to optimize the hyperparameters of the SVM model to enhance its accuracy and efficiency. SSO improves feature selection and parameter tuning by simulating social interactions among spiders in a web.

### *2.6.3. 3. K-Means Clustering*

An unsupervised machine learning algorithm used for clustering CAN bus data into groups based on similarities. It helps identify patterns and detect anomalies by grouping normal and abnormal data points based on distance measures. K-Means enhances the detection process by reducing data complexity and improving feature representation.

### *2.6.4. 4. Data Preprocessing Algorithms*

Includes normalization and feature extraction techniques to clean and transform raw CAN bus data into a structured format suitable for model training. Common techniques include Min-Max scaling, feature encoding, and noise reduction.

### *2.6.5. 5. Anomaly Detection Techniques*

Rule-based detection is used alongside machine learning models to identify abnormal patterns in vehicle communication. These techniques help in filtering out false positives and refining the detection process.

### *2.6.6. 6. Principal Component Analysis (PCA)*

A dimensionality reduction method used to transform high-dimensional CAN bus data into lower-dimensional space while preserving essential features. PCA helps in improving model efficiency by eliminating redundant features.

### 2.7. OUTPUT

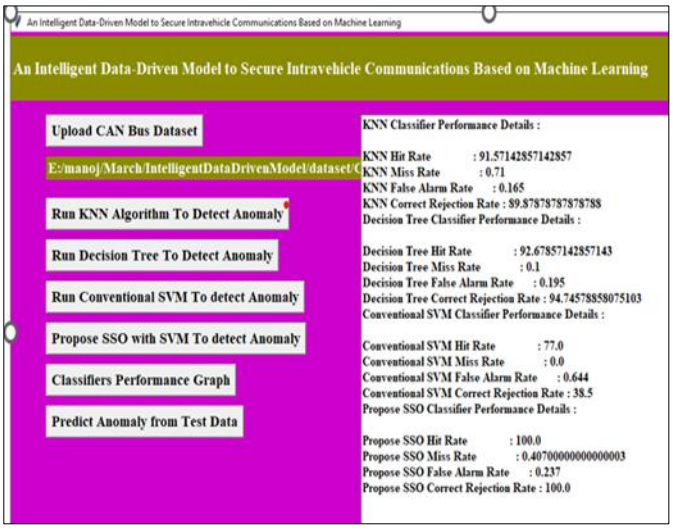



**Figure 1** Evaluating Model Performance

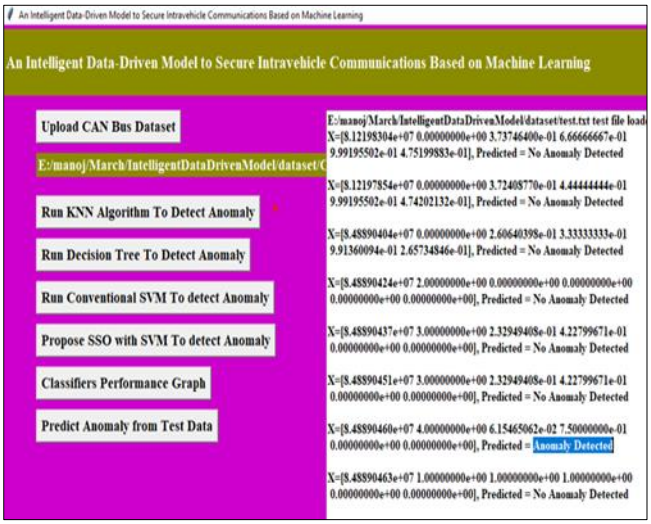



**Figure 2** Final Output

## 3. Results

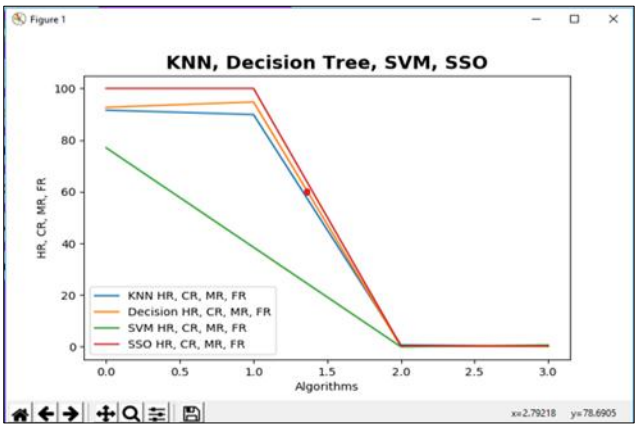



**Figure 3** KNN, Decision tree, SVM and SSO

### 3.1. Future Scope

#### *3.1.1. Integration with Autonomous Driving Systems*

Advanced anomaly detection models will be seamlessly integrated into autonomous vehicles to ensure secure and reliable communication between subsystems improving overall safety.

#### *3.1.2. Adoption of Federated Learning*

Federated learning will enable vehicles to collaboratively train anomaly detection models without sharing raw data enhancing privacy while maintaining system robustness.

#### *3.1.3. Real-Time Over-the-Air Updates*

The system will leverage over-the-air (OTA) updates to continually enhance the anomaly detection model ensuring it remains effective against emerging cyber threats.

#### *3.1.4. Utilization of Edge Computing*

Edge devices within vehicles will process anomaly detection tasks locally reducing latency and improving the real-time responsiveness of the system.

#### *3.1.5. Integration of Blockchain Technology*

Blockchain can be employed to create a tamper-proof log of vehicle communication ensure transparency and enhancing the anomaly detection system's ability to trace and verify malicious activities.

#### *3.1.6. 6. Standardization of Vehicle Communication Protocols*

Industry-wide adoption of standardized, secure communication protocols will work hand-in-hand with anomaly detection models to create a unified framework for safeguarding vehicular networks.

#### *3.1.7. Deployment on Embedded Systems:*

Optimize the solution for low-power embedded systems to support deployment in real-world automotive environments.

## 4. Conclusion

Intra-vehicle communication is a critical aspect of modern connected and autonomous vehicles making it essential to safeguard against anomalies and cyber threats. This project leverages an AI-powered machine learning model for real-time anomaly detection ensuring the integrity and reliability of vehicular networks. By identifying abnormal communication patterns and mitigating potential risks the system enhances the overall security and performance of intra-vehicle communication contributing to safer transportation solutions. The combination of robust machine learning techniques and real-time processing addresses the growing need for proactive measures in the automotive industry.

Looking ahead, this project lays the foundation for future advancements in intelligent vehicle security systems. With the integration of cutting-edge technologies such as edge computing, blockchain, and federated learning, the solution can evolve to meet emerging challenges and complexities. As the automotive sector moves towards greater connectivity and autonomy, this work underscores the importance of continuous innovation and collaboration to create secure and resilient vehicular networks, ensuring the safety of passengers and the integrity of data.

## Compliance with ethical standards

### *Disclosure of conflict of interest*

All authors declared that they do not have conflict of interest.

## References


[1] A. Monot; N. Navet; B. Bavoux; F. Simonot-Lion, "Multisource Software on Multicore Automotive ECUs—Combining Runnable Sequencing with Task Scheduling", IEEE Trans. Industrial Electronics, vol. 59, no. 10. Pp. 3934-3942, 2012.

[2] T.Y. Moon; S.H. Seo; J.H. Kim; S.H. Hwang; J. Wook Jeon, "Gateway system with diagnostic function for LIN, CAN and FlexRay", 2007 International Conference on Control, Automation and Systems, pp. 2844 – 2849, 2007.

[3] [3] B. Groza; S. Murvay, "Efficient Protocols for Secure Broadcast in Controller Area Networks", IEEE Trans. Industrial Informatics, vol. 9, no. 4, pp. 2034-2042, 2013.

[4] B. Mohandes, R. Al Hammadi, W. Sanusi, T. Mezher, S. El Khatib, "Advancing cyber physical sustainability through integrated analysis of smart power systems: A case study on electric vehicles", International Journal of Critical Infrastructure Protection, vol. 23, pp. 33 48, 2018.

[5] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, T. Vuong, A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles, Ad Hoc Networks, vol. 84, pp. 124-147, 2019.

[6] Hoppe T, Kiltz S, Dittmann J. Security threats to automotive can networks. practical examples and selected short-term countermeasures. Reliab Eng Syst Saf vol. 96, no. 1, pp. 11–25, 2011.

[7] Schulze S, Pukall M, Saake G, Hoppe T, Dittmann J. On the need of data management in automotive systems. In: BTW, vol. 144; pp. 217–26, 2009.

[8] Ling C, Feng D. An algorithm for detection of malicious messages on can buses. 2012 national conference on information technology and computer science. Atlantis Press; 2012.

[9] Oguma H, Yoshioka X, Nishikawa M, Shigetomi R, Otsuka A, Imai H. New attestation-based security architecture for in-vehicle communication. In: Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE. IEEE; pp. 1–6, 2008.

[10] L. Pan, X. Zheng, H. X. Chen, T. Luan, L. Batten, "Cyber security attacks to modern vehicular systems", Journal of Information Security and Applications, vol. 36, pp. 90-100, October 2017.

[11] Kang, M. J., & Kang, J. W., "Intrusion detection system using deep neural network for in-vehicle network security", PloS one, vol. 11, no. 6, e0155781, 2016.