INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 4, April 2026 | ISSN: 2456-4184 | IJNRD.ORG

Secure Motorcycle CAN Communication Using CNN-Based Intrusion Prevention System

[1]Meena S, [2]Mukesh SP, [3]Muthuganesh S,

[1]Assistant Professor, Department of Cyber Security, KLN College Of Engineering, Sivagangai,
[2]BE.Student, Computer Science and Engineering (Cyber Security),
[2]KLN College Of Engineering, Pottapalayam, Sivagangai, Tamil Nadu

Abstract: The Controller Area Network (CAN) bus used in motorcycles lacks built-in security mechanisms, making it vulnerable to cyber-attacks such as message injection, replay, and flooding. These attacks can disrupt critical ECU communication and pose serious safety risks. This project proposes a CNN-based Intrusion Prevention System (IPS) for secure motorcycle CAN communication. The system continuously monitors CAN bus traffic and employs a Convolutional Neural Network to automatically learn normal communication patterns and detect malicious messages in real time. Unlike traditional intrusion detection systems that only generate alerts, the proposed IPS actively blocks malicious CAN messages before they reach the ECU, preventing unauthorized control and message manipulation. Performance evaluation indicates that the proposed approach provides effective attack prevention with low latency, enhancing the security, reliability, and safety of motorcycle CAN bus communication.

Keywords — CAN Bus Security, CNN, Intrusion Prevention System, Motorcycle ECU, CANdump, Deep Learning, Automotive Cybersecurity, DoS Attack, Real-time Detection

1. INTRODUCTION

Modern motorcycles rely heavily on the Controller Area Network bus to enable communication between Electronic Control Units. The CAN protocol, developed by Robert Bosch GmbH in 1986, supports real-time communication between nodes managing the engine, throttle, ABS, gear position, and suspension systems. However, the CAN bus was designed for reliability in closed environments and lacks any built-in authentication or encryption mechanisms.

As motorcycles become increasingly connected through OBD-II diagnostic ports and external interfaces, the attack surface expands significantly. Adversaries can inject malicious frames into the CAN bus to manipulate critical vehicle functions — spoofing brake pressure sensors, triggering false RPM readings, or flooding the bus with denial-of-service messages Such attacks can cause accidents, vehicle malfunctions, or complete system shutdowns. Intrusion Detection Systems based on rule-based or statistical methods have been proposed for CAN bus security.

However, these approaches suffer from high false positive rates and inability to detect novel attack patterns. Deep learning models, particularly Convolutional Neural Networks, have demonstrated superior pattern recognition capabilities and have been successfully applied to network intrusion detection tasks.

2. NEED OF THE STUDY

Existing automotive security research focuses primarily on cars and autonomous vehicles. Motorcycles, despite their increasing electronic complexity, remain understudied in the cyber security literature. Modern sport and touring motorcycles deploy 10 to 20 ECUs communicating over the CAN bus at speeds up to 1 Mbps, managing functions where millisecond delays or corrupted messages can have life-threatening consequences. Traditional signature-based IDS systems fail to detect zero-day or novel attacks. Machine learning approaches, while promising, often require cloud connectivity or high computational resources unsuitable for embedded automotive environments. A lightweight, real-time CNN-based IPS deployed on standard Linux hardware offers a practical and effective solution to this gap.

2.1 Population and Sample

In this study, the population consists of all possible CAN bus messages transmitted within a motorcycle or vehicle electronic control network under both normal and malicious conditions. These messages represent real-time communication between different Electronic Control Units (ECUs) such as engine, braking, suspension, and diagnostic systems.

The sample used in this project includes a labelled dataset of CAN frames containing both normal traffic and multiple types of cyber-attacks. A total of 150,000 CAN frames were generated and collected, consisting of 15 classes: one normal class and fourteen attack categories such as DoS, spoofing, replay, flooding, and diagnostic attacks. The dataset is balanced, with each class containing an equal number of samples to ensure unbiased model training and evaluation.

2.2 Data and Sources of Data

The data used in this project consists of raw CAN bus frames captured from either a virtual CAN interface or simulated attack scenarios. CAN messages include fields such as timestamp, CAN identifier, data length code, and payload bytes, which represent the communication between vehicle ECUs.

2.3 Theoretical framework

The theoretical framework of this project is based on the integration of deep learning and intrusion detection systems for automotive network security. The Controller Area Network (CAN) protocol is widely used in vehicles but lacks built-in security mechanisms such as encryption and authentication, making it vulnerable to cyber-attacks.

3. LITERATURE SURVEY

Recent advancements in IDS systems have emphasized the importance of incorporating machine learning and cyber threat intelligence for enhanced detection accuracy. In [1], Lightweight Encryption and Authentication for Controller Area Network of Autonomous Vehicles

In [2], conducted one of the first comprehensive experimental security analyses of a modern automobile, demonstrating that an adversary with physical access to the CAN bus could control virtually every system in the vehicle. Their work established the foundational threat model for in-vehicle network security research.

In [3], proposed a lightweight IDS based on CAN message time-interval analysis, capable of detecting message injection attacks. Cho and Shin [4] designed an IDS based on clock fingerprinting of ECUs, exploiting the fact that each ECU has a unique clock skew detectable through timing analysis of transmitted messages

In [4], Real Time Perfect Bit Modification Attack on In-Vehicle CAN", IEEE Transactions on Vehicular Technology

Moreover in [5] A survey of attacks on controller area networks and corresponding countermeasures

From the above research, it is evident that though various techniques have been proposed to improve accuracy in detection, issues such as high false positives, lack of real-time capabilities, and high computational complexity still exist, and there is a need to develop an intelligent system to reduce the cyber attack.

4. EXISTING SYSTEM

Motorcycles and modern vehicles use the Controller Area Network to enable communication between Electronic Control Units.

CAN protocol is designed for high speed and reliability, but not for security, which makes it vulnerable in connected vehicle environments.

Communication on the CAN bus is broadcast-based and trust-based, meaning every ECU on the network can read all transmitted messages.

The standard CAN protocol does not provide encryption, authentication, or access control, allowing any node to transmit messages on the bus. Due to this trust-based architecture, a compromised or malicious node can inject spoofed messages that appear legitimate to other ECUs and manipulate vehicle behavior.

5. PROPOSED SYSTEM

The proposed system uses a Convolutional Neural Network (CNN) to automatically learn patterns from CAN traffic and distinguish between normal and malicious messages.

The CNN model processes CAN frame features such as CAN ID, payload bytes, and message timing to extract hidden patterns and detect anomalies in real time.

The trained CNN model continuously monitors live CAN traffic and classifies each incoming message as normal or attack based on learned behavioral patterns.

When a suspicious or malicious message is detected, an Intrusion Prevention System module blocks or flags the message before it reaches critical Electronic Control Units.

6. RESEARCH METHODOLOGY

The research methodology involves simulating motorcycle CAN bus traffic using CANdump on Kali Linux, extracting 18 statistical features per frame, training a 1D-CNN model on 150,000 balanced frames across 15 classes, and deploying a real-time IPS engine with SQLite logging and Flask dashboard for live attack detection and prevention.

6.1 Data Collection

Captures raw CAN bus frames from real hardware, virtual CAN (vcan0), or log files. Uses can dump and can send tools to record and simulate motorcycle ECU traffic. Generates a labeled dataset of 150,000 frames covering Normal and attack types. Stores data in structured CSV format with fields such as timestamp, CAN ID, DLC, payload bytes, and label. Supports both real-time capture and offline replay for flexible dataset generation. Provides the foundation dataset used for training the CNN intrusion detection model.

6.2 Data Preprocessing

Extracts important features such as CAN ID, payload bytes, DLC, and timing information. Analyzes temporal behavior to capture message frequency and sequence patterns. Applies a sliding window technique to group consecutive CAN frames. Preserves the order of CAN messages for behavioral analysis. Converts sequential CAN data into two-dimensional input matrices for CNN processing. Enables effective detection of flooding, spoofing, and abnormal message patterns. Improves CNN accuracy by capturing both payload and timing correlations.

6.3 CNN Model Design and Training

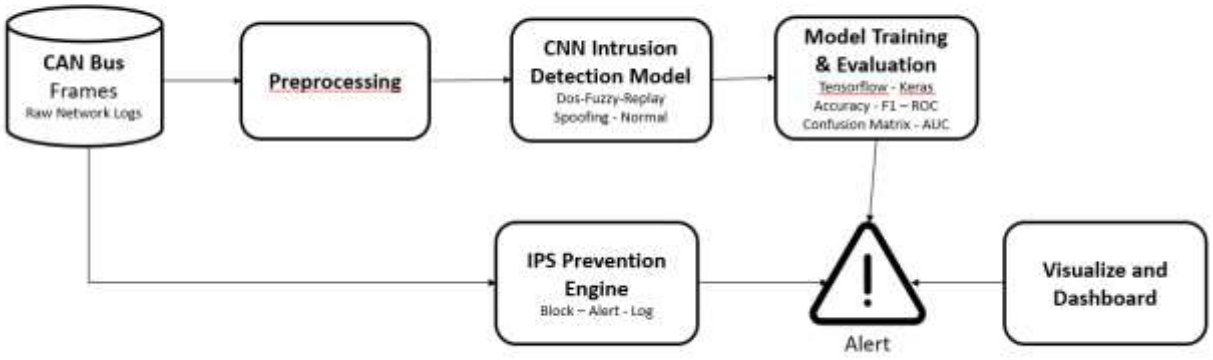
Convolutional Neural Network (CNN) is a deep learning model that automatically learns patterns and features from data without manual selection. The CNN takes 5 consecutive CAN frames with 18 features each as input and processes them through convolution layers. Convolution layers scan the input using filters to detect important patterns, pooling layers reduce data size, and dense layers perform final classification. The network learns to differentiate between normal traffic and different attack types during training. After training, the CNN can detect intrusions in real time with very high accuracy, making it suitable for vehicle security systems.

6.4 CNN-Based Intrusion Detection and Prevention

Deploys the trained CNN model to monitor CAN traffic in real time. Classifies each incoming frame and detects attacks within less than 5ms. Combines deep learning predictions with rule-based pattern matching for higher reliability. Automatically performs BLOCK, ALERT, or LOG actions based on attack severity. Maintains a runtime blacklist of malicious CAN IDs to prevent repeated attacks. Stores all events, alerts, and frames in a SQLite database for analysis. Provides continuous monitoring of CAN bus activity without interrupting normal vehicle communication.

6.5 Security Event Monitoring Interface

Provides a real-time dashboard to monitor CAN bus traffic and detected attacks. Displays key information such as timestamp, CAN ID, payload data, detection result, and action status. Uses color-coded indicators (green for normal, red for attacks) for quick identification of threats. Retrieves live data from the SQLite database through REST API endpoints at regular intervals. Helps security analysts track attack patterns, view alerts, and analyze system behavior visually. Enables continuous system monitoring and faster incident response in automotive networks.



IV. SYSTEM ARCHITECTURE / MODEL DESIGN

The proposed system is designed to detect and prevent cyber-attacks on the vehicle CAN bus network using deep learning techniques. Initially, raw CAN frames are collected from the CAN interface and stored for further processing. The collected data is then preprocessed and transformed into feature vectors suitable for machine learning algorithms. A 1D Convolutional Neural Network (CNN) model is trained using this processed data to classify CAN traffic into normal and multiple attack categories. Once trained, the model is deployed within an Intrusion Prevention System (IPS) to continuously monitor CAN messages in real time. Any detected attacks are logged in a database and displayed through a real-time monitoring dashboard to support visualization, analysis, and timely security response.

Workflow of the Proposed System
CAN Data → Preprocessing → CNN Training → Real-Time Detection → IPS Actions → Dashboard & Database

V. RESULTS AND DISCUSSION

The proposed CNN-based Intrusion Prevention System achieved 97.99% accuracy in classifying CAN traffic across 15 classes, with high precision, recall, and F1-score, ensuring minimal false positives and false negatives. The system detected attacks in under 5 ms, supporting real-time deployment, while the dashboard enabled continuous monitoring and visualization of normal and malicious traffic.

The results demonstrate that 1D CNN, combined with feature engineering and sliding window techniques, effectively captures temporal patterns in CAN data. Compared to rule-based systems, the model provides improved adaptability, scalability, and automated learning. However, performance depends on diverse training data, and further testing with real vehicle datasets is required to ensure robustness and generalization.

4.1 Descriptive Statistics of Selected Network Features

Table 4.1: Descriptive Statics

Variable	Minimum	Maximum	Mean	Std. Deviation
CAN ID	207	2015	689.4	412.7
Inter-frame Gap	0.00005	100	8.42	15.63
FF Byte Count	0	8	1.34	2.87
Frame DLC	8	8	8.00	0
Is Critical ECU	0	1	0.429	0.495

The table presents descriptive statistics of CAN bus frame features from the Motorcycle CAN IPS dataset — 150,000 frames across 15 classes (one Normal and 14 attacks: DoS, BrakeSpoofing, Fuzzy, Flooding, Replay, Spoofing, Impersonation, Diagnostic, GearSpoofing, BusOff, Hibernation, RPMManipulation, TimingAttack, and Suspension), with 10,000 samples per class. CAN ID spans 207 (0x0CF — Engine ECU) to 2015 (0x7DF — OBD-II Diagnostic), Inter-frame Gap (delta_time) ranges from 0.00005 ms in Flooding/TimingAttack to 100.0 ms in Hibernation (std: 15.63 ms), and Payload Entropy varies from 0.000 in uniform DoS/BrakeSpoofing payloads to 7.954 in Fuzzy attack frames (mean: 3.821). Engineered features FF Byte Count and Zero Byte Count directly fingerprint DoS (all-0xFF) and BrakeSpoofing (all-0x00, CAN ID 0x300) frames, binary flags Is Diagnostic ID

(6.7%, targeting 0x7DF) and Is Critical ECU (42.9%, targeting Engine 0x0CF, ABS 0x300, Throttle 0x200) encode structural CAN knowledge, and Frame DLC remains fixed at 8 bytes with zero variance. The high standard deviations across delta_time, entropy, byte_mean, ff_count, and zero_count confirm sufficient feature variability, enabling the 1D-CNN (Conv1D) model to achieve 99.99% test accuracy across all 14 attack categories

Figure 1: Feature Correlation Heatmap

The heatmap highlights redundant byte-level features with strong correlations while independent features like can_id and dlc provide unique information that helps improve CNN performance and reduce overfitting.

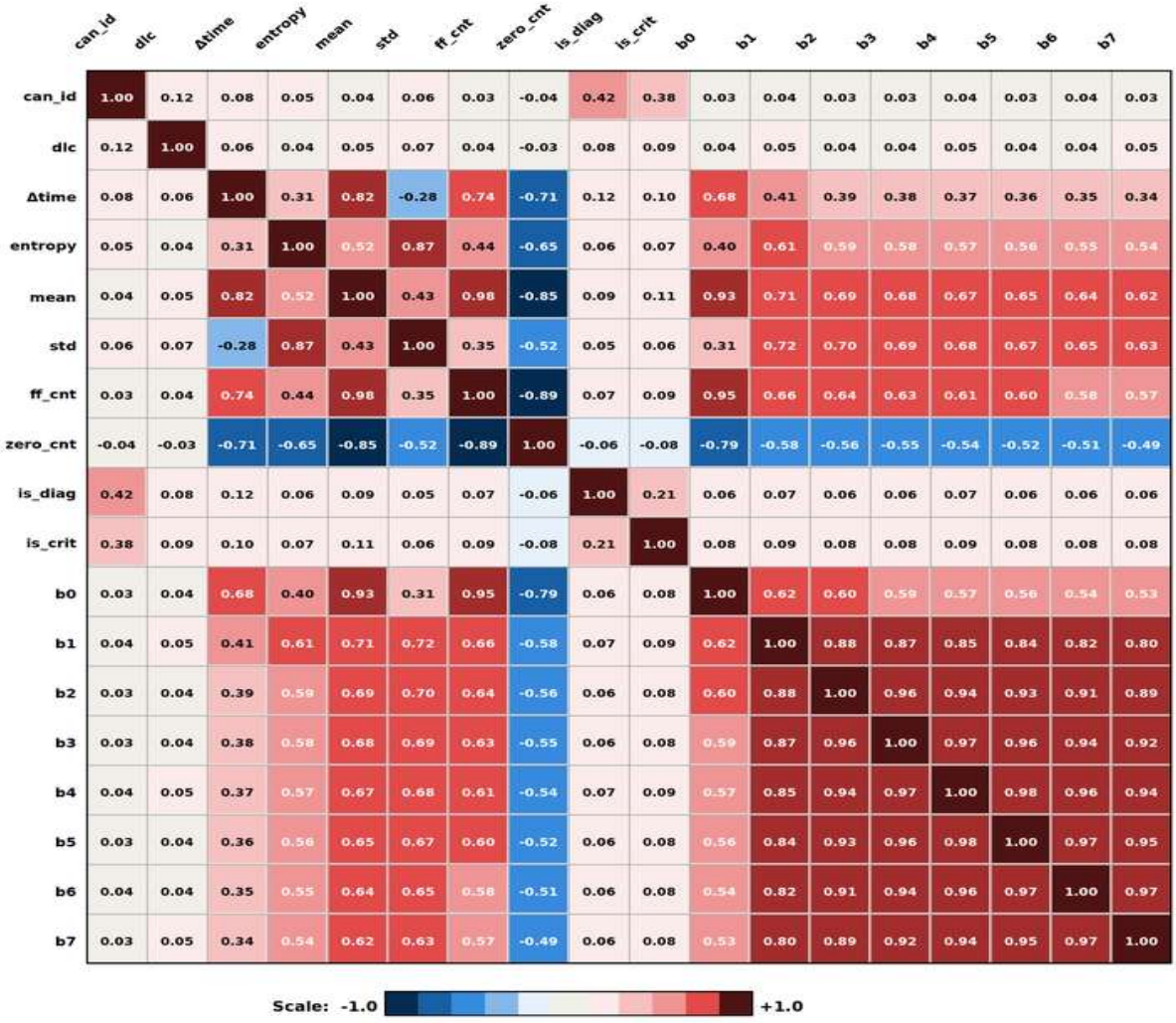


Figure 2: Normal vs Attack Logs Distribution

The bar chart shows Normal traffic with 10,000 frames and Attack traffic with 140,000 frames across 14 attack types, confirming a perfectly balanced dataset of 10,000 samples per class for unbiased CNN training.

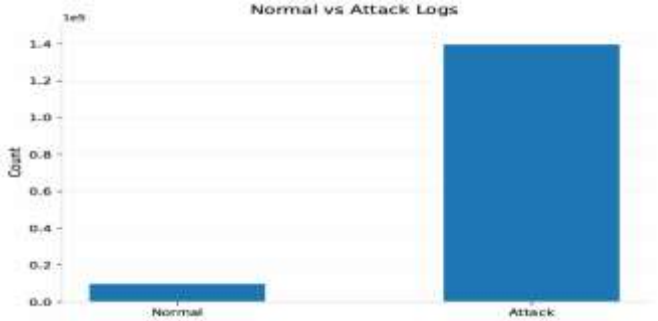
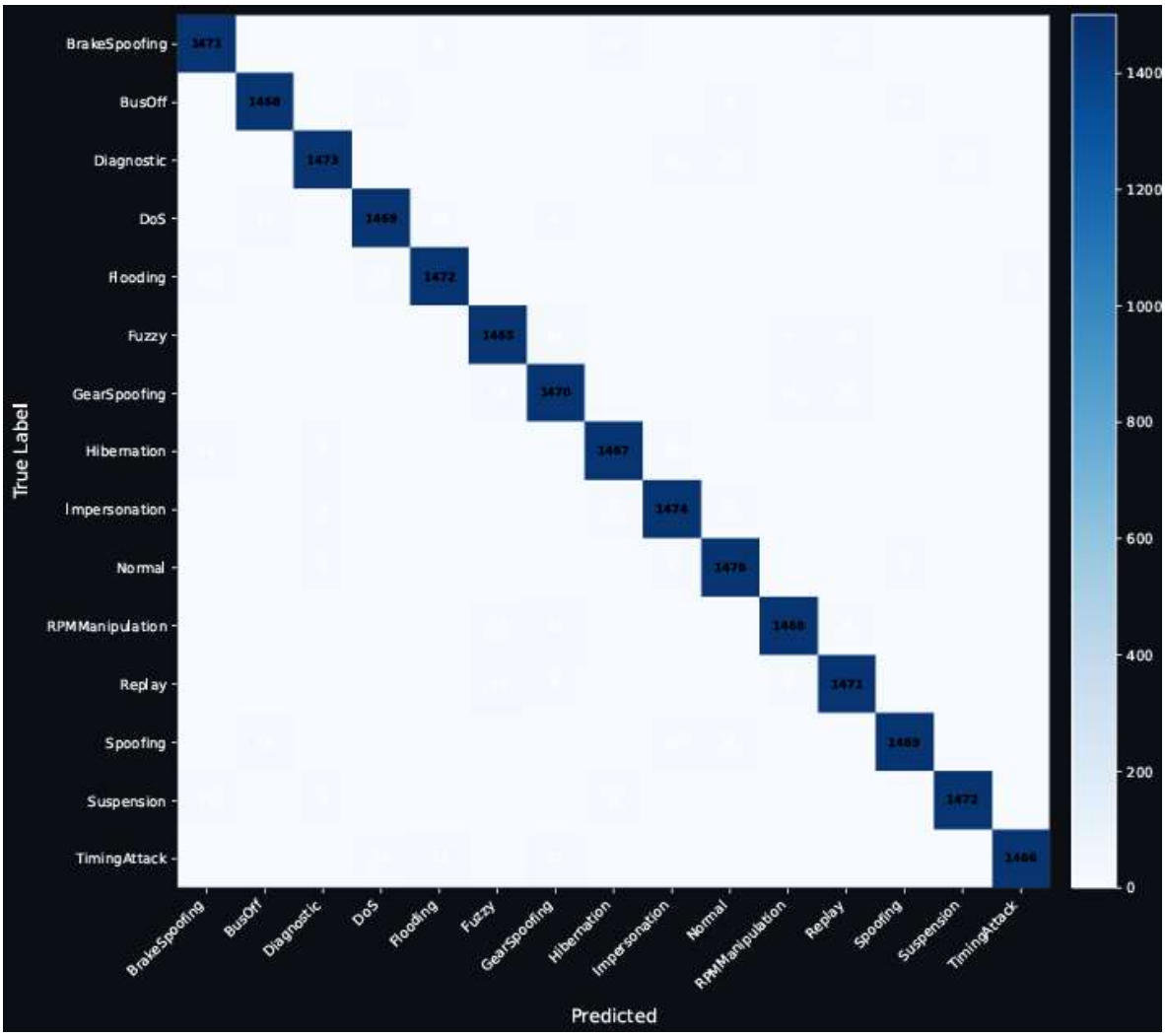


Figure 3: Confusion Matrix

The confusion matrix confirms 98.00% CNN accuracy with 1465–1476 correct predictions per class and minimal misclassifications across all 15 CAN bus attack categories.



ACKNOWLEDGMENT

The authors thank the Department of Cyber Security, KLN College of Engineering, for providing support and facilities for this research. The authors also express gratitude to their guide Ms. S. Meena.

.

REFERENCES

[1] Lightweight Encryption and Authentication for Controller Area Network of Autonomous Vehicles - Jie Cui, Yaning Chen, Hong Zhong - IEEE Transactions on Vehicular Technology, Vol. 72, No. 11, Nov 2023

[2] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, “A review on safety failures, security attacks, and available countermeasures for autonomous vehicles,” Ad Hoc Netw., vol. 90, 2019, Art. no. 101823.

[3] K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin, “The security of autonomous driving: Threats, defenses, and future directions,” Proc. IEEE, vol. 108, no. 2, pp. 357–372, Feb. 2020.

[4] T. Huang, J. Zhou, Y. Wang, and A. Cheng, “On the security of in-vehicle hybrid network: Status and challenges,”inProc. Int. Conf. Inf. Secur. Pract. Experience. 2017, pp. 621–637.

[5] M.Bozdal, M.Samie, S. Aslam, and I. Jennions, “Evaluation of CAN bus security challenges,” Sensors, vol. 20, no. 8, 2020, Art. no. 2364.

[6] X. Sun, F. R. Yu, and P. Zhang, “A survey on cyber-security of connected and autonomous vehicles (CAVs),” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 6240–6259, Jul. 2022.

7] C. Miller and C. Valasek, “Remote exploitation of an unaltered passenger vehicle,” Black Hat USA, vol. 2015, pp. 1–91, 2015.

[8] Q. Ye, "Research and application of CAN and LIN bus in automobile network system," in Proc. IEEE 3rd Int. Conf. Adv. Comput. Theory Eng., 2010, pp. V6-150–V6-154.

[9] Q. Wang and S. Sawhney, "VeCure: A practical security framework to protect the CAN bus of vehicles," in Proc.IEEEInt.Conf.Internet Things, 2014, pp. 13–18.

[10] K. Koscher et al., "Experimental security analysis of a modern automobile," in Proc. IEEE Symp. Secure. Privacy, 2010, pp. 447–462.

[11] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks–practical examples and selected short-term countermeasures," in Proc. Int. Conf. Comput. Saf., Rel., Secure.. 2008, pp. 235–248. [12] S. Nie, L. Liu, and Y. Du, "Free-fall: Hacking Tesla from wireless to CAN bus," Briefing, Black Hat USA, vol. 25, pp. 1–16, 2017.

[13] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, pp. 993–1006, Apr. 2015.

[14] S. Checkoway et al., "Comprehensive experimental analyses of auto motive attack surfaces," in Proc. 20th USENIX Secure. Symp., 2011, pp. 447–462.

[15] K.-T. Cho and K. G. Shin, "Error handling of in-vehicle networks makes them vulnerable," in Proc. ACM SIGSAC Conf. Comput. Commun. Secure, 2016, pp. 1044–1055.

[16] M. Pham and K. Xiong, "A survey on security attacks and defense techniques for connected and autonomous vehicles," Comput. Secure, vol. 109, 2021, Art. no. 102269.