Proceedings of Engineering & Technology PET -Vol 98, pp.35-41 **Advances in Control Systems and Information Technology**

Evaluating the Stochastic Robustness of Ensemble Learning Architecture for Multiclass Intrusion Detection in CAN-Based IoV Systems

Tamara Zhukabayeva[#1], Lazzat Zholshiyeva[*2], Nurdaulet Karabayev [#3], Yerik Mardenov [#4], Dilaram Baumuratova [#5]

[#] *L.N. Gumilyov Eurasian National University*
Astana International University
Astana, Kazakhstan
[1]zhukabayeva_tk@enu.kz, [3]020419501012@enu.kz, [4]emardenov@gmail.com, [5]baumaratova.d@gmail.com

[*] *Astana International University*
Astana, Kazakhstan
[2]lazzatzholshy@gmail.com

***Abstract*— The paper investigates the problem of multi-class intrusion detection in CAN-oriented vehicle networks for intelligent transport systems (ITS). The growing interconnectedness of such networks makes them vulnerable to cyberattacks, which requires the development of efficient and productive detection systems. The CIC IoV 2024 dataset is used, which contains CAN-bus traffic in both normal operation mode and various attack scenarios. The classification task includes the following classes: normal traffic, DoS attacks, as well as parameter change attacks for gas (GAS), engine speed (RPM), car speed (SPEED) and steering wheel control (STEERING_WHEEL). Data preprocessing involves scaling traits and applying the Principal Component (PCA) method to reduce dimension and eliminate correlations between traits. Detection system implemented using Decision Tree, Random Forest and AdaBoost algorithms. Performance assessment is based on the macro-averaged metrics Accuracy, Precision, Recall and F1-score. To assess the model's resilience under real cyber-physical attack conditions, a stochastic sensitivity test is offered in which stochastic perturbations are added to incoming CAN traffic. This allows simulating real-world disturbances, as opposed to optimizing Stochastic Sensitivity Tests. The comparison of clean and noisy data is done using error matrices and degradation analysis of quality indicators. Experimental results show that emsemble methods are effective in increasing the stability of intrusion detection systems in CAN-routed networks.**

Keywords*— IDS, IoV, CAN Bus Security, Stochastic Robustness, CIC IoV 2024

I. INTRODUCTION

The Internet of Vehicles (IoV) is a domain of IoT that enables intelligent transportation and traffic management through the integration of sensors, AI, and cloud technologies. [1]. Modern intelligent vehicle systems (IoV) are being actively implemented in the automotive industry [2], [3]. Modern vehicle ECUs communicate through the CAN protocol, which enables real-time data exchange but lacks built-in security mechanisms, making networks vulnerable to cyberattacks. [5], [6]. One of the key threats to CAN networks is message penetration attacks, such as Denial of Service (DoS) and spoofing attacks, aimed at falsifying critical car parameters [7]. In particular, spoofing attacks on throttle values, engine speeds, speed and steering can lead to incorrect vehicle behaviour and pose a serious risk to the safety of drivers and passengers [8]. In recent years, ML methods have been widely used for attack detection in automotive networks. Classical algorithms such as DT and ensemble methods effectively identify anomalies and malicious CAN traffic.

This paper investigates the effectiveness of classical machine learning models for multiclass attack classification in automotive CAN networks using the CIC IoV 2024 dataset. Decision Tree, Random Forest, and AdaBoost models were evaluated under Gaussian attack conditions using Accuracy, Precision, and F1-score metrics [9-14].

An The resistance of ML models to adversarial impacts in the classification of attacks in CAN car networks is a critical task due to the increasing complexity of cyber threats aimed at intelligent vehicles.

ISSN: 1737-9334

Proceedings of Engineering & Technology PET -Vol 98, pp.35-41 **Advances in Control Systems and Information Technology**

Existing studies have investigated ML and ensemble approaches for CAN intrusion detection. However, most of them focus on classification accuracy and pay limited attention to robustness against adversarial perturbations and stochastic disturbances [15-22].

II. METHODOLOGY

Modern vehicles rely on CAN networks for communication between electronic control units, but protocol vulnerabilities expose them to attacks such as DoS and parameter manipulation. This study proposes a machine learning approach with dimensionality reduction and stochastic sensitivity testing for attack detection and robustness evaluation.

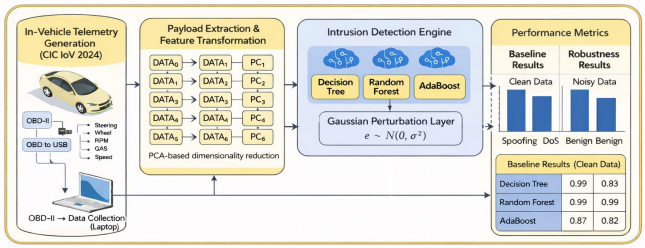

Fig. 1 Architecture of the proposed system

A. *Description and classes of dataset traffic*

The CIC IoV 2024 dataset provided by the Canadian Institute of Cybersecurity (CIC) is used to study CAN attacks on automotive networks. This dataset is intended for IoV safety analysis and comprises real and simulated CAN messages recorded during normal vehicle operation and under various cyberattacks.

B. *Data structure and characteristics*

The dataset contains 1,408,219 CAN messages with DATA_0–DATA_7 features and six traffic classes, enabling machine learning models to detect attacks based on message content variations rather than static characteristics.

C. *Data Research Analysis (EDA)*

Correlation analysis revealed moderate and high correlations among CAN bytes. PCA was utilized to compress the latent feature space and simulate the computational constraints of real-time Electronic Control Units (ECUs) while preserving 95% of the total signal variance.

D. *Data Preprocessing*

Data preprocessing included feature selection, data cleaning, and dataset preparation. CAN message bytes (DATA_0–DATA_7) were used as input features, while the CAN ID was excluded to avoid overfitting. The data were standardized using StandardScaler and split into training and testing sets (80/20) using stratified sampling.

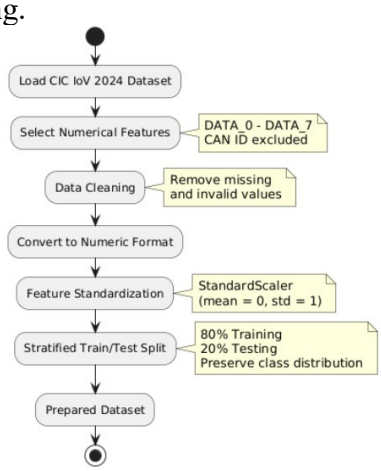

Fig. 2 Preprocessing algorithm

ISSN: 1737-9334

E. Feature standardization and data reduction (PCA)

Before the reduction of dimension methods and the training of classifiers, the feature space was standardized using StandardScaler. This operation brought all the signs to a single scale with an average value of zero and a standard deviation of one. The mathematical transformation is described by the following formula:

$$X_{scaled} = \frac{x-\mu}{\sigma} \quad (1)$$

F. Data Reduction (PCA)

CAN message payload bytes (DATA_0–DATA_7) may contain redundant and correlated information, which can reduce model robustness and generalization capability. Therefore, PCA was applied to reduce feature dimensionality, suppress noise, and eliminate redundancy. The original eight features were transformed into six principal components preserving at least 95% of the total variance. The data transformation was performed using the following formula:

$$X_{PCA}=X_{SCALED}\,W \quad (2)$$

Where W is the eigenvector matrix of the covariance matrix that defines the directions of the principal components. PCA reduced eight features into six principal components preserving 95% variance.

G. Simulation of Stochastic Sensitivity Tests

To evaluate the robustness of ML models against adversarial conditions, a Gaussian noise-based attack simulation was applied. This approach models real-world disturbances such as transmission errors, electromagnetic interference, and intentional modifications of CAN message payloads. Gaussian noise with intensity ε = 0.15 was added after PCA transformation to preserve the overall data structure while introducing perturbations. The generated attack data were then used to evaluate model performance under distorted conditions:

$$X_{adv} = X + \varepsilon, \quad \varepsilon \in \mathcal{N}(0.\sigma) \quad (3)$$

H. ML Models

Three classical machine learning models—Decision Tree (DT), Random Forest (RF), and AdaBoost—were selected for multiclass attack classification in automotive CAN networks. All models were trained and tested using the same standardized dataset processed with PCA to ensure fair comparison. DT provides simple learning, RF improves robustness through ensemble voting, and AdaBoost enhances performance by combining weak classifiers. Results showed that Random Forest achieved the highest accuracy, while AdaBoost demonstrated better stability under adversarial noise conditions.

III. RESULTS AND DISCUSSION

This section presents the results of a comprehensive analysis of the CIC IoV Dataset 2024, including statistical analysis of traffic class distribution, study of correlative dependencies between CAN-messages features, application of PCA for dimension reduction, as well as a comparative evaluation of the effectiveness of ML algorithms in the detection of anomalies in automotive networks. Special attention is given to the interpretation of the quality metrics of classification under conditions of normal operation of the network and under the influence of ambient noise data. The evaluation of model quality was carried out both on pure data and under the influence of the Stochastic Sensitivity Test, which allowed us to analyze not only the accuracy of classification, but also the resistance of models to distortions of input data. The experiments examined three models of ML: DT, RF and AdaBoost. To ensure a correct comparison, all models were trained and tested on the same samples of data that had passed the steps of standardization and dimensionality reduction using PCA.

I. Comparison of accuracy before and after the Noise Perturbation Analysis

To evaluate the impact of the Stochastic Sensitivity Tests on the accuracy of the models, a column chart was constructed showing the Accuracy values for pure data and for data distorted by the attack. This

ISSN: 1737-9334

Proceedings of Engineering & Technology PET -Vol 98, pp.35-41 **Advances in Control Systems and Information Technology**

visualization allows for a direct comparison of the behavior of models in two conditions. Analysis of the graph shows that all models under consideration show a decrease in accuracy after application of the Gaussian Attack. The Decision Tree model has the most pronounced drop, which confirms its high sensitivity to noise. The AdaBoost model also shows significant quality degradation. At the same time, Random Forest maintains a higher accuracy than other models, indicating its greater resistance to input distortions. Table 1 and Figure 4 compare the accuracy of ML models before and after the attack.

TABLE I
COMPARISON OF ACCURACY BEFORE AND AFTER NOISE PERTURBATION ANALYSIS

Model	Accuracy		Precision		Recall		F1-score	
	clean	attack	clean	attack	clean	attack	clean	attack
DT	0.996	0.831	0.985	0.556	0.965	0.434	0.973	0.455
RF	0.996	0.887	0.985	0.846	0.965	0.327	0.973	0.401
Ada Boost	0.872	0.820	0.300	0.301	0.182	0.179	0.184	0.173

Comparison of accuracy before and after Noise Perturbation Analysis.

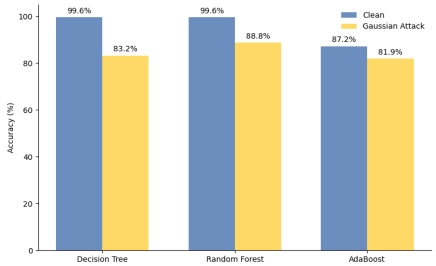

Fig. 3 Accuracy before and after the Noise Perturbation Analysis

J. Confusion Matrix

For a more detailed analysis of classification quality, confusion matrices were constructed for each model, both on the data and under the influence of the Noise Perturbation Analysis. Confusion matrices allow you to evaluate the distribution of true and false predictions for each class and identify the most problematic classes. Analysis shows that the models are classified for both normal traffic and most attacking classes. However, after using Noise Perturbation Analysis, there is an increase in errors, especially between spoofing classes such as GAS, RPM, SPEED and STEERING_WHEEL. This indicates the similarity of these attacks' characteristics and the increased complexity of differentiating them under noise conditions. The Decision Tree model shows an increase in errors, whereas Random Forest shows a more stable distribution of predictions and a lower number of errors even under attack (Figure 5).

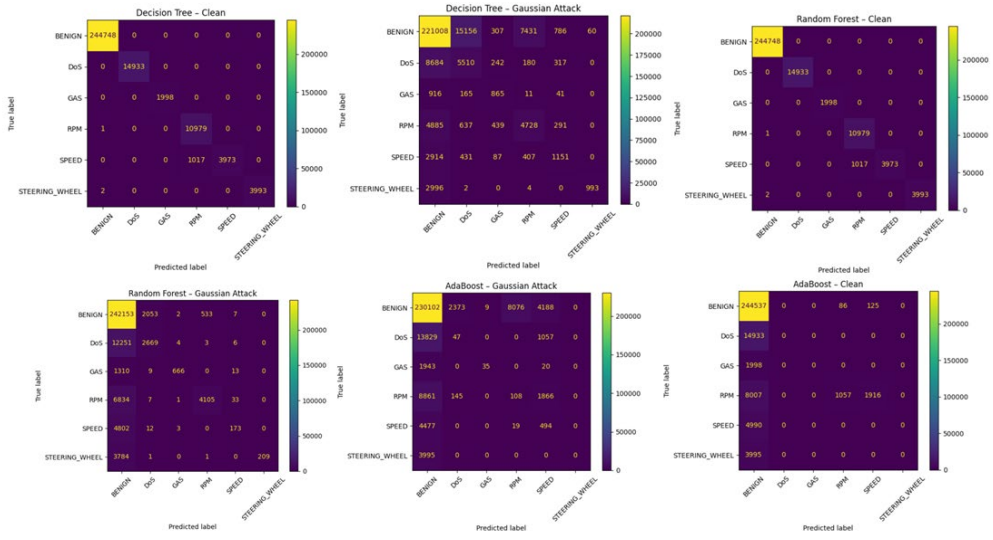

Fig. 4 Confusion matrix before (left) and after attack (right).

ISSN: 1737-9334

K. Confusion Matrix

To assess the models' resistance to a stochastic test for sensitivity, an accuracy loss graph was constructed showing the difference between the accuracy of clean data and the accuracy of noise analysis (Figure 6). This graph shows the degree of classification quality loss for each model. The solution tree model shows the greatest loss of accuracy, confirming its vulnerability to input data displacement. The AdaBoost model shows a moderate decrease in accuracy, while Random Forest shows the lowest Accuracy Drop value, indicating its best stability among the models under consideration. The use of visualizations in this work allowed not only to quantify the quality of classification, but also to obtain a qualitative understanding of the behavior of models under conditions of adversarial action, which is an important aspect in the development of attack detection systems in CAN car networks.

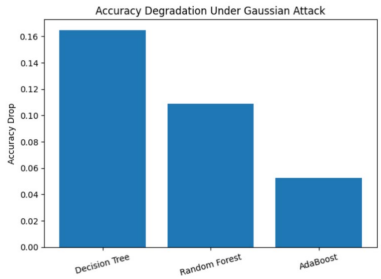

Fig. 5 Accuracy Degradation under Noise Perturbation Analysis.

The proposed architecture demonstrated stable performance degradation under stochastic perturbations. The Stability Delta (Δ) metric was used to measure model robustness, where smaller values indicate better resistance to disturbances. Random Forest achieved the highest overall classification accuracy under both clean and noisy conditions, while AdaBoost showed the lowest Stability Delta for some safety-critical classes, indicating better robustness. In contrast, the single Decision Tree model was more sensitive to input perturbations and noise..

IV. CONCLUSIONS

This paper investigated the detection of multiclass attacks in CAN-based automotive networks using machine learning algorithms and evaluated their robustness under stochastic conditions. The proposed approach considered practical cyber-physical disturbances such as noise, electromagnetic interference, and sensor degradation. The Stability Delta (Δ) metric enabled quantitative evaluation of performance degradation under noisy conditions. Experimental results showed that Random Forest achieved the highest classification accuracy, while AdaBoost demonstrated competitive robustness. Future work will focus on integrating advanced adversarial attacks and extending analysis across different vehicle environments..

ACKNOWLEDGMENT

This research has been funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No AP23489127).

REFERENCES

[1] C. He, W. Wang, W. Jiang, Z. He, J. Wang, and X. Xie, “Security for the Internet of Vehicles with Integration of Sensing, Communication, Computing, and Intelligence: A Comprehensive Survey,” *Sensors*, vol. 25, no. 16, p. 5119, Aug. 2025, doi: 10.3390/s25165119.

[2] P. Mishra and G. Singh, “Internet of Vehicles for Sustainable Smart Cities: Opportunities, Issues, and Challenges,” *Smart Cities*, vol. 8, no. 3, p. 93, May 2025, doi: 10.3390/smartcities8030093.

[3] P. Rani and R. Sharma, “Intelligent Transportation System Performance Analysis of Indoor and Outdoor Internet of Vehicle (IoV) Applications Towards 5G,” *Tsinghua Science and Technology*, vol. 29, no. 6, pp. 1785–1795, Dec. 2024, doi: 10.26599/tst.2023.9010119.

[4] Y. Liu et al., “Vehicular Intrusion Detection System for Controller Area Network: A Comprehensive Survey and Evaluation,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 7, pp. 10979–11009, Jul. 2025, doi: 10.1109/tits.2025.3567940.

ISSN: 1737-9334

[5] M. M. Rana, "EVTwinCyb: Evaluating Resilient State Estimation Techniques and Mitigation Strategies for Electric Vehicle Digital Twin Systems Against FDI and DoS Cyber Threats," *2025 27th International Conference on Advanced Communications Technology (ICACT)*, pp. 1–5, Feb. 2025, doi: 10.23919/icact63878.2025.10936788.

[6] S. Popic, B. Ramic, and S. Bojanic, "Security Challenges and Mitigation Strategies for CAN-Based Protocols: A Comprehensive Survey," *2025 24th International Symposium INFOTEH-JAHORINA (INFOTEH),* pp. 1–6, Mar. 2025, doi: 10.1109/infoteh64129.2025.10959305.

[7] Z. Pethő, T. M. Kazár, Z. Szalay, and Á. Török, "Quantifying Cyber Risks: The Impact of DoS Attacks on Vehicle Safety in V2X Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 11, pp. 18591–18600, Nov. 2024, doi: 10.1109/tits.2024.3436840.

[8] P. Kashikar, "Exploring Cyber Threats Associated With Autonomous And Connected Vehicles," *Educational Administration: Theory and Practice*, pp. 12823–12830, Mar. 2024, doi: 10.53555/kuey.v30i5.5418.

[9] I. Chiscop, A. Gazdag, J. Bosman, and G. Biczók, "Detecting Message Modification Attacks on the CAN Bus with Temporal Convolutional Networks," *Proceedings of the 7th International Conference on Vehicle Technology and Intelligent Transport Systems*, pp. 488–496, 2021, doi: 10.5220/0010445504880496.

[10] R. U. D. Refat, A. A. Elkhail, A. Hafeez, and H. Malik, "Detecting CAN Bus Intrusion by Applying Machine Learning Method to Graph Based Features," *Intelligent Systems and Applications*, pp. 730–748, Aug. 2021, doi: 10.1007/978-3-030-82199-9_49.

[11] B. S. Bari, K. Yelamarthi, and S. Ghafoor, "Intrusion Detection in Vehicle Controller Area Network (CAN) Bus Using Machine Learning: A Comparative Performance Study," *Sensors*, vol. 23, no. 7, p. 3610, Mar. 2023, doi: 10.3390/s23073610.

[12] A. D. M. Ibrahum, M. Hussain, and J.-E. Hong, "Deep learning adversarial attacks and defenses in autonomous vehicles: a systematic literature review from a safety perspective," *Artificial Intelligence Review*, vol. 58, no. 1, Nov. 2024, doi: 10.1007/s10462-024-11014-8.

[13] F. Aloraini, A. Javed, and O. Rana, "Adversarial Attacks on Intrusion Detection Systems in In-Vehicle Networks of Connected and Autonomous Vehicles," *Sensors*, vol. 24, no. 12, p. 3848, Jun. 2024, doi: 10.3390/s24123848.

[14] H. M. R. U. Rehman et al., "A systematic literature study of machine learning techniques based intrusion detection: datasets, models, challenges, and future directions," *Journal of Big Data*, vol. 12, no. 1, Nov. 2025, doi: 10.1186/s40537-025-01323-2.

[15] B. Xu, F. Cao, X. Li, S. Tian, W. Deng, and S. Yue, "BEPCD: an ensemble learning-based intrusion detection framework for in-vehicle CAN bus," *PeerJ Computer Science,* vol. 11, p. e3108, Aug. 2025, doi: 10.7717/peerj-cs.3108.

[16] E. Alalwany, I. Mahgoub, B. Alsharif, and A. Alfahaid, "An Intelligent Ensemble-Based Detection of In-Vehicle Network Intrusion," *Applied Sciences*, vol. 15, no. 12, p. 6869, Jun. 2025, doi: 10.3390/app15126869.

[17] B. Gül and F. Ertam, "Performance comparison of machine learning models on a novel in-vehicle controller area network dataset," *International Advanced Researches and Engineering Journal*, vol. 9, no. 2, pp. 78–88, Aug. 2025, doi: 10.35860/iarej.1607108.

[18] R. Rai and J. Grover, "CAN Bus Anomaly Detection Through Statistical Analysis and Machine Learning," *2025 IEEE Region 10 Symposium (TENSYMP)*, pp. 1–6, Jul. 2025, doi: 10.1109/tensymp63728.2025.11144974.

[19] Deekshith G. R., S. R. Sheetal, Divya G. S., Darshan B. M., and Balakrishna V, "Intrusion Detection System in CAN-BUS Vehicle Networks Using Machine Learning," *International Research Journal on Advanced Engineering Hub (IRJAEH)*, vol. 3, no. 09, pp. 3819–3825, Sep. 2025, doi: 10.47392/irjaeh.2025.0555.

[20] K. G, P. M, N. K, and M. Kumar, "Real-Time Intrusion Detection System for Automotive CAN Bus Using Machine Learning and Virtual Simulation," *2025 International Conference on Sensors and Related Networks (SENNET) Special Focus on Digital Healthcare(64220),* pp. 1–6, Jul. 2025, doi: 10.1109/sennet64220.2025.11135991.

[21] W.-C. Lu and B.-C. Cheng, "GNN-Based in-Vehicle Network Intrusion Detection System," *2025 7th International Conference on Computer Communication and the Internet (ICCCI)*, pp. 66–71, Jun. 2025, doi: 10.1109/iccci65070.2025.11158677.

[22] J. P. A. Bonomo, J. V. Volpato, R. S. De Carvalho, and G. Gracioli, "Machine Learning-Based Intrusion Detection for Automotive CAN Networks on Embedded Platforms," *2024 XIV Brazilian Symposium on Computing Systems Engineering (SBESC)*, pp. 1–6, Nov. 2024, doi: 10.1109/sbesc65055.2024.10771926.

[23] D. Drake, V. Cobilean, H. S. Mavikumbure, M. Stuart, S. Das, and M. Manic, "GAP-CAN: Gradient-Based Adversarial Attack on Transformers for CAN Bus Anomaly Detection," *2025 IEEE 8th International Conference on Industrial Cyber-Physical Systems (ICPS)*, pp. 1–7, May 2025, doi: 10.1109/icps65515.2025.11087840.

[24] E. Seo, J. Kim, W. Lee, and J. Seok, "Adversarial Attack of ML-based Intrusion Detection System on In-vehicle System using GAN," *2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN),* pp. 700–703, Jul. 2023, doi: 10.1109/icufn57995.2023.10200297.

ISSN: 1737-9334