

---

# MACHINE LEARNING-BASED DETECTION OF DDoS ATTACKS IN VANETS FOR EMERGENCY VEHICLE COMMUNICATION

---

A PREPRINT

 **Bappa Muktar\***

Department of Computer Science  
University of Quebec in Outaouais (UQO)  
Gatineau, QC J8X 3X7  
mukb06@uqo.ca

 **Vincent. Fono**

Department of Computer Science  
University of Quebec in Outaouais (UQO)  
Gatineau, QC J8X 3X7

 **Adama Nouboukpo**

Department of Computer Science  
University of Quebec in Outaouais (UQO)  
Gatineau, QC J8X 3X7

June 11, 2025

## ABSTRACT

Vehicular Ad Hoc Networks (VANETs) play a key role in Intelligent Transportation Systems (ITS), particularly in enabling real-time communication for emergency vehicles. However, Distributed Denial of Service (DDoS) attacks, which interfere with safety-critical communication channels, can severely impair their reliability. This study introduces a robust and scalable framework to detect DDoS attacks in highway-based VANET environments. A synthetic dataset was constructed using Network Simulator 3 (NS-3) in conjunction with the Simulation of Urban Mobility (SUMO) and further enriched with real-world mobility traces from Germany's A81 highway, extracted via OpenStreetMap (OSM). Three traffic categories were simulated: DDoS, VoIP, and TCP-based video streaming (VideoTCP). The data preprocessing pipeline included normalization, signal-to-noise ratio (SNR) feature engineering, missing value imputation, and class balancing using the Synthetic Minority Over-sampling Technique (SMOTE). Feature importance was assessed using SHapley Additive exPlanations (SHAP). Eleven classifiers were benchmarked, among them XGBoost (XGB), CatBoost (CB), AdaBoost (AB), GradientBoosting (GB), and an Artificial Neural Network (ANN). XGB and CB achieved the best performance, each attaining an F1-score of 96%. These results highlight the robustness of the proposed framework and its potential for real-time deployment in VANETs to secure critical emergency communications.

**Keywords** VANET, DDoS attacks, Emergency vehicles, Machine learning, Intrusion detection, NS-3, SUMO, Traffic classification, Supervised learning, Artificial Neural Network

## 1 Introduction

VANETs have emerged as a cornerstone of ITS, enabling real-time communication between vehicles and infrastructure to improve traffic efficiency and road safety [1, 2]. These systems are particularly vital for emergency response units, which rely on uninterrupted connectivity to minimize response time and save lives. However, their open communication channels, decentralized architecture, and dynamic topology expose them to a wide range of cybersecurity threats [3]. Among the most critical of these threats are DDoS attacks, which aim to overwhelm network resources and degrade the

---

\*Use footnote for providing further information about author (webpage, alternative address)—*not* for acknowledging funding agencies.

performance of safety-critical services. Such disruptions can cause severe consequences, including delayed emergency interventions, increased traffic congestion, and potential loss of life [4, 5].

Despite increasing academic interest in intrusion detection systems for VANETs, many existing studies present notable limitations, such as exclusive reliance on synthetic datasets, lack of reproducibility, and a predominant focus on dense urban environments [3, 6]. In particular, realistic highway scenarios—where uninterrupted communication for emergency vehicles is equally critical—remain significantly underexplored. Moreover, most prior research depends on a single machine learning classifier, which limits the robustness and generalization capacity of the proposed models.

To bridge these gaps, this paper proposes a comprehensive machine learning-based framework for detecting DDoS attacks in VANETs operating in highway environments.

The main contributions of this work are as follows:

- We design and simulate realistic VANET traffic using the NS-3 and SUMO simulators, incorporating real-world vehicle mobility traces from Germany’s A81 highway extracted via OSM.
- We evaluate a wide range of supervised learning algorithms, including XGB, CB, AB, Extra Trees (ET), Random Forest (RF), GB, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Logistic Regression (LR), Decision Tree (DT), and ANN.
- We apply SHAP to assess feature importance, thereby enhancing the interpretability and reliability of the models. The proposed framework achieves excellent predictive performance, with F1-scores reaching up to 96% for XGB and CB classifiers.

The remainder of this paper is organized as follows: Section 2 presents a comprehensive literature review of machine learning-based intrusion detection in VANETs. Section 3 details the methodology, including dataset generation and preprocessing. Section 4 describes the classifiers used and the predictive modeling approach. Section 5 reports and discusses the experimental results. Finally, Section 6 concludes the paper and outlines future research directions.

## 2 Literature Review

Securing VANETs against DDoS attacks has emerged as a critical research area due to the potential disruptions in vital communication channels, especially those involving emergency vehicles. Recent advances have emphasized developing robust, accurate, real-time intrusion detection mechanisms utilizing machine learning (ML) and deep learning (DL) approaches.

Several researchers have investigated innovative machine learning models tailored explicitly to the unique constraints of VANET environments. For instance, Setia et al. proposed a framework employing machine learning combined with fuzzification methods within cloud-based VANET systems, achieving a remarkable accuracy of 99.59% in proactively detecting DDoS threats [7]. Similarly, Polat, O. et al. introduced a hybrid model blending a one-dimensional Convolutional Neural Network (1D-CNN) with decision trees for real-time detection in Software-Defined Vehicular Ad-Hoc Networks (SD-VANETs), attaining an accuracy close to 90% [8]. Further expanding this direction, Polat, H. et al. presented an advanced deep learning architecture using stacked sparse autoencoders combined with a softmax classifier, significantly improving accuracy to approximately 96.9% in SDN-based VANET scenarios [9].

Addressing not only attack detection but also network congestion, Gopi et al. developed a two-phase Intelligent DoS Attack Detection with Congestion Control (IDoS-CC) system. Their methodology combined Teaching and Learning-Based Optimization (TLBO) with a Gated Recurrent Unit (GRU) deep learning model, demonstrating substantial reductions in network congestion and improved detection accuracy [10]. Kadam et al. also contributed notably by proposing a hybrid classification approach (KSVM) integrating K-Nearest Neighbors (KNN) and Support Vector Machines (SVM), exhibiting superior sensitivity, recall, and precision compared to traditional classifiers [11].

Data realism and reproducibility represent essential challenges often overlooked in the literature. In response, Alkadiri et al. generated a contemporary dataset leveraging OMNeT++, Veins, and SUMO simulations, optimized via SMOTE and classified using the XGBoost algorithm, achieving an F1-score of approximately 99% [12]. Similarly, Rashid et al. adopted OMNeT++ and SUMO for a realistic VANET simulation, presenting a real-time adaptive framework with various ML classifiers, yielding accuracies of up to 99% [13]. Anyanwu et al. further optimized detection by integrating Radial Basis Function SVM (RBF-SVM) with Grid Search Cross-Validation, showing detection rates of 99.22% on realistic SDN-based VANET datasets [14].

Hybrid optimization and multi-stage detection systems have also been extensively explored. Marwah et al. combined modified SVM enhanced by Harris Hawks Optimization (HHO) and Whale-Dragonfly optimization for efficient routing and bandwidth allocation, significantly improving throughput and reducing communication overhead under DDoS

conditions [15]. Adhikary et al. developed a hybrid model merging AnovaDot and RBFDot SVM kernels into a chained detection mechanism, achieving improved robustness and detection accuracy compared to single-kernel models [16]. Moreover, Tariq et al. proposed a comprehensive detection framework integrating Autoencoders, LSTM, clustering methods, fog computing, and blockchain technology, offering a low-latency, scalable, and robust solution with a detection rate of approximately 94% [17].

Deep learning-based anomaly detection approaches have recently gained momentum due to their scalability and superior pattern recognition capabilities. Lekshmi et al. leveraged convolutional autoencoders coupled with LSTM networks and self-attention mechanisms, achieving an F1-score of 98.20% in detecting DDoS attacks on realistic VANET data [18]. Similarly, Haydari et al. introduced a semi-supervised, non-parametric intrusion detection system using roadside units (RSUs), capable of detecting novel attack patterns without prior knowledge, significantly enhancing real-time responsiveness and detection accuracy [19].

While extensive progress has been made, gaps remain in terms of evaluating these methodologies in realistic highway scenarios. Most existing works predominantly target dense urban environments or lack reproducible real-world mobility data, limiting the generalizability of results. Additionally, comprehensive comparisons of various machine learning classifiers within a unified, realistic highway scenario remain scarce.

Our study aims to address these critical gaps by evaluating multiple prominent ML classifiers—including XGB, CB, AB, ET, RF, GB, SVM, KNN, LR, DT, and ANN—in a realistic VANET highway scenario. Leveraging NS-3 and SUMO simulators enriched with real mobility data from the A81 highway in Germany, our approach not only ensures realism but also enables reproducibility. Furthermore, data balancing through SMOTE and rigorous performance evaluation metrics (accuracy, precision, recall, and F1-score) strengthen our methodological framework, providing a robust and comprehensive assessment of classifier effectiveness.

Table 1 below summarizes and positions our work compared to existing state-of-the-art approaches based on several critical criteria.

Table 1: Comparative summary of DDoS detection in VANETs (continued on next page)

Reference	Model Type	Simulation Environment	Attack Type	Detection Approach	Data Balancing	Best Reported Metric
[7]	ML + Fuzzification	NS-2 (VANET cloud sim.)	DDoS	Fuzzy logic aided ML classifier	None	Accuracy: 99.59%
[8]	1D-CNN + Decision Tree	SD-VANET (Mininet+SUMO)	DDoS	Hybrid CNN+DT classification	None	~90% accuracy
[9]	Stacked Autoencoder (SSAE)	SDN-based VANET (sim.)	DDoS	Deep learning (SSAE + Softmax)	None	Accuracy: 96.9%
[10]	TLBO + GRU (two-stage)	VANET traffic simulation	DoS	Optimization (TLBO) + RNN classifier	None	Not specified
[11]	KNN + SVM (Hybrid KSVM)	Simulated VANET (not spec.)	DDoS	Combined KNN/SVM classifier	None	Accuracy: 92.46%
[12]	XGBoost	OMNeT++/Veins + SUMO	DDoS	Supervised ML (tree-based)	SMOTE	F1-score $\approx$ 99%
[13]	Multi-ML ensemble	OMNeT++/Veins + SUMO	DDoS	Distributed multi-layer IDS	None	Accuracy up to 99%
[14]	RBF-SVM (optimized)	SDN-VANET (realistic data)	DDoS	SVM + grid-search tuning	None	Detection Rate: 99.22%
[15]	SVM + HHO + WDO	Simulated VANET (Hwy)	DDoS	Optimized SVM (HHO, Whale-Dragonfly)	None	F1-score: 96%
[16]	Dual-kernel SVM	Simulated VANET (RSUs)	DDoS	Chained AnovaDot+RBF SVM	None	Accuracy $\sim$ 96–98%

Continued on next page

Table 1 Continued from previous page

Reference	Model Type	Simulation Environment	Attack Type	Detection Approach	Data Balancing	Best Reported Metric
[17]	Autoenc. + LSTM + BC (fog)	Simulated SD-VANET (fog)	DDoS	Hybrid IDS + blockchain	None	Detection Rate $\approx 94\%$
[18]	ConvAE + LSTM	Simulated VANET data	DDoS	Deep anomaly detection	None	F1-score: 98.20%
[19]	Statistical (non-param.)	SUMO + real traffic traces	DDoS	RSU-based anomaly detection	None	Detection $\sim 94\%$
<b>Ours</b>	ML & DL (XGB, CB, ANN...)	NS-3, SUMO, Real traces (A81 Hwy)	DDoS	ML/DL classifiers (with SMOTE)	SMOTE	F1-score $\sim 96\%$

This comparative analysis underscores the novelty and relevance of our research, emphasizing both methodological rigor and practical applicability, thus effectively filling the identified gaps in the current state of VANET cybersecurity research.

### 3 Methodology

This section outlines the methodological framework for developing a robust classification model for DDoS attacks in a VANET environment, simulating a realistic highway scenario.

#### 3.1 Experimental Architecture

This section outlines the architecture and methodology used to simulate a realistic highway-based VANET under coordinated DDoS attacks. It details the scenario design, simulator integration, and incorporation of real mobility traces to ensure data realism and model applicability.

##### 3.1.1 Scenario Description

The data collection scenario is structured to simulate a VANET highway environment with 13 vehicles (from  $V_0$  to  $V_{12}$ ) moving at a constant speed.  $V_0$  to  $V_2$  act as legitimate nodes, while  $V_3$  to  $V_{12}$  act as malicious nodes. Vehicle  $V_0$ , which symbolizes an emergency vehicle (for instance, a police car), will generate TCP traffic to vehicle  $V_2$ , which simulates a real-time video streaming application. At the same time, vehicle  $V_1$  is transmitting VoIP messages over UDP to the same destination. On the other hand, malicious nodes ( $V_3$  to  $V_{12}$ ) initiated a DDoS attack by overwhelming  $V_2$  with high UDP traffic flows to disrupt its communication capabilities. This scenario demonstrates the critical security threat in a VANET highway environment, where a coordinated cyberattack threatens the emergency vehicle’s operational integrity. Table 2 presents the NS-3 simulation parameters used in the VANET DDoS scenario.

##### 3.1.2 NS-3 and SUMO Integration

The experiment uses NS-3 [20] and SUMO [21] simulators to simulate communication protocols and vehicle dynamics. NS-3 handles network stack, protocol behavior, and traffic generation, while SUMO provides the precise mobility dynamics of the vehicle for realistic traffic scenarios.

##### 3.1.3 Incorporation of Real Mobility Traces

To further enhance the realism of the simulation, real-world mobility traces from the A81 highway in Germany were integrated into the SUMO simulation and imported into NS-3 using the Ns2MobilityHelper module. This integration ensures that the generated dataset reflects authentic vehicular behavior and spatial-temporal patterns, thus increasing the applicability and reliability of the intrusion detection model trained on this data. Figure 1 illustrates the A81 highway in OSM and its corresponding import within the SUMO environment.

Table 2: Simulation parameters used for the VANET DDoS scenario

Parameter	Value / Description
Simulation Time	30 seconds
Number of Nodes	13 vehicles total (3 legitimate, 10 malicious)
Legitimate Vehicles	$V_0$ : TCP (Video), $V_1$ : UDP (VoIP), $V_2$ : Sink
Malicious Vehicles	$V_3$ to $V_{12}$ (UDP DDoS)
WiFi Standard	IEEE 802.11 (10 MHz channel bandwidth)
WiFi Range	250 meters
Routing Protocol	OLSR (Optimized Link State Routing)
Propagation Model	Two-Ray Ground Propagation Loss Model
Mobility Model	Ns2MobilityHelper (A81 highway traces)
Packet Size (VoIP)	160 bytes
VoIP Rate	64 Kbps
Packet Size (DDoS)	1024 bytes
DDoS Rate per Bot	1 Mbps
Traffic Classification	TCP (Video), UDP (VoIP/DDoS), based on source address
Monitoring Tools	FlowMonitor (with SNR via MonitorSniffRx)
Output Files	vanet-ddos-data.csv, vanet-ddos-flowmon.xml



(a) A81 highway segment extracted from OpenStreetMap.



(b) Imported road segment visualized in SUMO.

Figure 1: Visualization of the A81 highway segment used in the simulation. (a) Map segment from OSM. (b) Simulation rendering in SUMO.

### 3.2 Data Generation and Labeling

The simulated dataset utilized in this study comprises three distinct classes of network traffic: (*DDoS*), *Voice over IP (VoIP)*, and *VideoTCP*. Each traffic category was generated using appropriate application models within the NS-3 simulation environment. Specifically, *VideoTCP* traffic, emulating a real-time video streaming application, was produced using the `BulkSendHelper` application over a TCP connection directed toward the target vehicle. Concurrently, *VoIP* traffic was simulated using the `OnOffHelper` application, configured at a constant data rate of 64 kbps and a fixed packet size of 160 bytes, thereby adhering to the widely used G.711 standard in VoIP communications. In contrast, *DDoS* traffic was generated using the same `OnOffHelper` application, but set to a significantly higher data rate of 1 Mbps per flow, explicitly modeling malicious traffic intended to saturate network resources.

To characterize the behavior and performance of each network flow, several relevant metrics were collected using the `FlowMonitor` module in NS-3. Key metrics extracted include the average throughput, measured in kilobits per second (kbps), computed according to the following equation:

$$\text{Throughput} = \frac{8 \times \text{RxBytes}}{\text{FlowDuration} \times 10^3}$$

Where  $RxBytes$  denotes the total number of bytes received and  $FlowDuration$  represents the effective duration of the flow in seconds. The mean delay was calculated using:

$$\text{MeanDelay} = \frac{\sum_{i=1}^{N_{rx}} \text{Delay}_i}{N_{rx}}$$

Where  $\text{Delay}_i$  is the delay experienced by each successfully received packet and  $N_{rx}$  corresponds to the total number of received packets. Additionally, the packet loss rate ( $LostPackets$ ) was determined by calculating the difference between transmitted ( $N_{tx}$ ) and received ( $N_{rx}$ ) packets:

$$\text{LostPackets} = N_{tx} - N_{rx}$$

Lastly, each network flow was explicitly labeled according to its traffic class (*DDoS*, *VoIP*, or *VideoTCP*) based on the originating IP address and the employed network protocol. Consequently, TCP-based flows were systematically classified as *VideoTCP*, UDP-based flows originating from legitimate nodes (IP addresses  $\leq 10.0.0.3$ ) were labeled as *VoIP*, whereas UDP flows initiated by malicious bot nodes were categorized as *DDoS*. This meticulous labeling procedure enhances the reliability and accuracy of the dataset, facilitating the development of robust and effective intrusion detection models. Figure 2 shows the first five rows of the dataset sample extracted from the NS-3 simulation.

FlowID	Src	Dest	Protocol	SrcPort	DestPort	TrafficLabel	TxPackets	RxPackets	LostPackets	ThroughputKbps	DelaySum	MeanDelay	TimeFirstTx	TimeLastRx	FlowDuration	AvgSignal_dBm	AvgNoise_dBm	Samples	
0	1	10.0.0.2	10.0.0.3	UDP	49163	9001	VoIP	914	4	910	0.220070	11.34730	2.83683	2.49	29.8367	27.3367	-17.4723	-96.852	397263
1	2	10.0.0.2	10.0.0.3	UDP	49183	9001	VoIP	914	31	883	1.705200	151.69700	4.89347	2.49	29.8323	27.3423	-17.4723	-96.852	397263
2	3	10.0.0.2	10.0.0.3	UDP	49203	9001	VoIP	914	4	910	0.223552	7.60270	1.90068	2.49	29.4009	26.9109	-17.4723	-96.852	397263
3	4	10.0.0.2	10.0.0.3	UDP	49223	9001	VoIP	914	3	911	0.167651	7.61703	2.53901	2.49	29.4031	26.9131	-17.4723	-96.852	397263
4	5	10.0.0.2	10.0.0.3	UDP	49243	9001	VoIP	914	3	911	0.167605	7.63322	2.54441	2.49	29.4104	26.9204	-17.4723	-96.852	397263

Figure 2: Dataset sample

### 3.3 Data Preprocessing

The preprocessing stage is a fundamental step in building an effective intrusion detection model. This process was structured into three main phases: data cleaning and normalization, creation of a derived SNR variable, and class rebalancing through oversampling techniques.

#### 3.3.1 Cleaning and Normalization

The raw dataset initially consisted of 6882 network flows described by 19 features, including identifiers, traffic characteristics, performance metrics, and physical measurements such as average signal and noise power. Several cleaning operations were applied:

- Removal of non-informative or highly correlated features: Columns such as `FlowID`, `Src`, `Dest`, `SrcPort`, `DestPort`, and `Samples` were discarded due to their low predictive value. Similarly, the temporal features `TimeFirstTx` and `TimeLastRx` were removed in favor of the derived feature `FlowDuration`, and `DelaySum` was excluded in favor of `MeanDelay`.
- Categorical feature encoding: The categorical variables `Protocol` and `TrafficLabel` were converted to numerical representations using `LabelEncoder`, where `DDoS`, `VoIP`, and `VideoTCP` were encoded as 0, 2, and 1, respectively.
- Duplicate removal: Approximately 7.5% of the data were identified as duplicates and subsequently removed to reduce model bias.
- Normalization: All numerical features were normalized using `StandardScaler` to enforce zero mean and unit variance—an essential condition for many machine learning algorithms.

#### 3.3.2 SNR Feature Engineering

Although the dataset initially contained the fields `AvgSignal_dBm` and `AvgNoise_dBm`, a new variable representing the average Signal-to-Noise Ratio (SNR) was computed as follows:

$$\overline{\text{SNR}} = \overline{S} - \overline{N}$$

where  $\overline{S}$  and  $\overline{N}$  denote the mean received signal and noise power respectively, measured in dBm. However, SHAP (SHapley Additive exPlanations) analysis revealed that these features had negligible predictive value in the highway VANET scenario, and they were therefore excluded from the final dataset used for training.

### 3.3.3 Class Rebalancing Using SMOTE

The Figure 3 below highlights a significant class imbalance: 3489 DDoS flows, 1996 VoIP flows, and only 882 VideoTCP flows. To address this, we applied the SMOTE [22] to the training data. SMOTE generates synthetic samples for the minority classes, resulting in a balanced training set with 2617 flows per class.

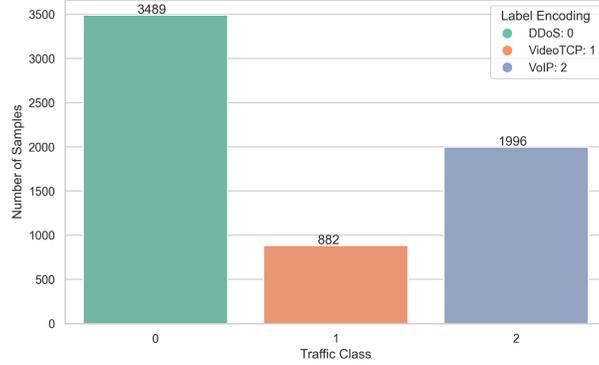


Figure 3: Traffic label distribution before SMOTE

This rebalancing significantly improved model generalization and reduced bias toward the majority class during training.

### 3.4 Feature Selection

Feature selection plays a pivotal role in the development of any predictive model, particularly in the context of VANETs, where the dataset may include redundant or highly correlated variables. To identify the most relevant attributes for classifying network traffic (*DDoS*, *VoIP*, and *VideoTCP*), we adopted an interpretability-based approach using SHAP values (see Fig. 4). This method quantifies the marginal contribution of each feature to the model's output while accounting for complex interdependencies among features.

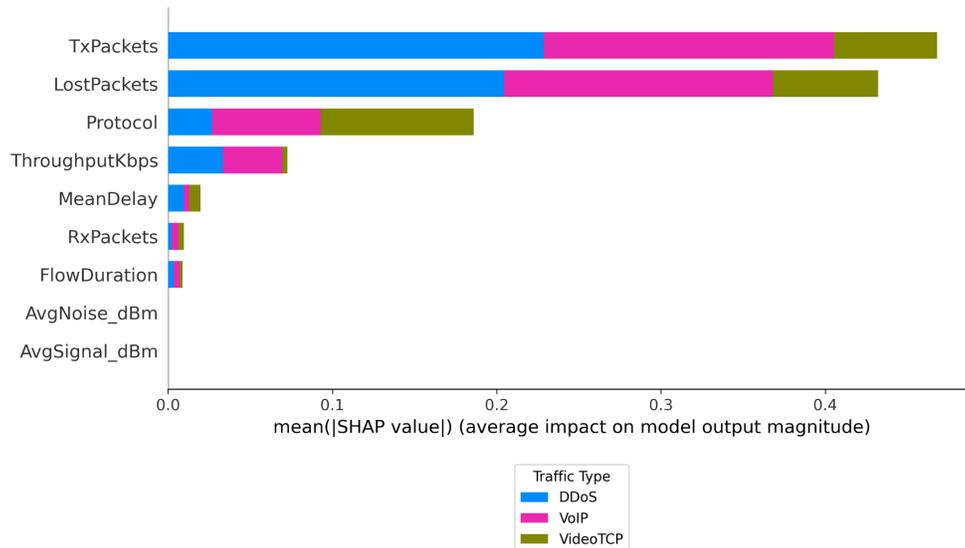


Figure 4: Feature importance based on SHAP values

As illustrated in Fig. 4, the SHAP analysis highlighted TxPackets, LostPackets, and Protocol as the most influential features in predicting the traffic class. Although these features exhibit some degree of correlation, they

offer complementary insights into traffic intensity and anomalous behavior, such as packet losses resulting from DDoS attacks.

Nonetheless, `TxPackets` and `LostPackets`, despite their high SHAP scores and strong correlation with the target variable, were deliberately excluded from the final feature set to mitigate multicollinearity effects. These variables directly influence several other performance metrics (e.g., `ThroughputKbps` and `MeanDelay`), and including them could introduce bias by over-representing certain aspects of the traffic.

The final selection includes the following features:

- `Protocol`: distinguishes UDP flows (VoIP) from TCP flows (VideoTCP), and supports the identification of traffic patterns typical of DDoS attacks.
- `ThroughputKbps`: reflects traffic intensity and helps discriminate between high-volume flows such as those generated by *VideoTCP* and *DDoS*.
- `MeanDelay`: captures average packet latency, which is critical for detecting delays caused by attacks or real-time services like VoIP.
- `RxPackets`: although moderately ranked in SHAP importance, this feature complements flow-level analysis without the redundancy of `TxPackets`.
- `FlowDuration`: captures the temporal dynamics of each flow and effectively substitutes highly correlated variables such as `TimeFirstTx` and `TimeLastRx`.

This refined feature set was selected based on its discriminative power while minimizing redundancy. It ensures improved robustness and interpretability of the classification model, which is essential for reliable intrusion detection in VANET environments.

## 4 Modeling and Classification

This section presents the modeling approach to classify network traffic in a VANET scenario under DDoS conditions.

### 4.1 Tested Machine Learning Models

To assess the ability to classify network traffic in a VANET environment, several machine learning algorithms were tested, encompassing both traditional methods and more advanced ensemble and boosting techniques.

The traditional models evaluated include:

- `Random Forest`: An ensemble method based on building multiple decision trees and averaging their predictions to improve generalization.
- `Extra Trees`: Similar to `Random Forest`, but introducing greater randomness in the selection of splitting thresholds to enhance diversity.
- `Decision Tree`: A simple hierarchical model based on attribute-based decision rules.
- `Logistic Regression`: A linear model adapted for multiclass classification through the softmax activation function.
- `Support Vector Machine`: Using an optimized linear kernel to separate network traffic classes effectively.
- `K-Nearest Neighbors`: A non-parametric method that classifies each observation based on the majority vote among its  $k$  nearest neighbors.

Advanced boosting and ensemble methods were also evaluated:

- `XGBoost`: A gradient boosting framework optimized for multiclass classification tasks using the `multi:softmax` objective function.
- `CatBoost`: Designed to efficiently handle categorical variables and exhibit robustness against class imbalance.
- `AdaBoost`: An iterative ensemble technique that sequentially improves weak classifiers.
- `Gradient Boosting`: Builds models sequentially to correct errors made by prior models.

Finally, an Artificial Neural Network was designed and implemented using Keras. The architecture consists of:

- An input layer receiving 5 features (Protocol, ThroughputKbps, MeanDelay, RxPackets, FlowDuration).
- A first dense hidden layer with 32 neurons and a ReLU activation function.
- A second dense hidden layer with 16 neurons, also activated by ReLU.
- A Dropout layer with a rate of 30% applied after the second hidden layer to mitigate overfitting.
- A third dense hidden layer with 8 neurons and a ReLU activation function.
- An output dense layer with 3 neurons using the Softmax activation function to classify among three classes: DDoS, VoIP, and VideoTCP.

Figure 5 illustrates the architecture of the designed ANN.

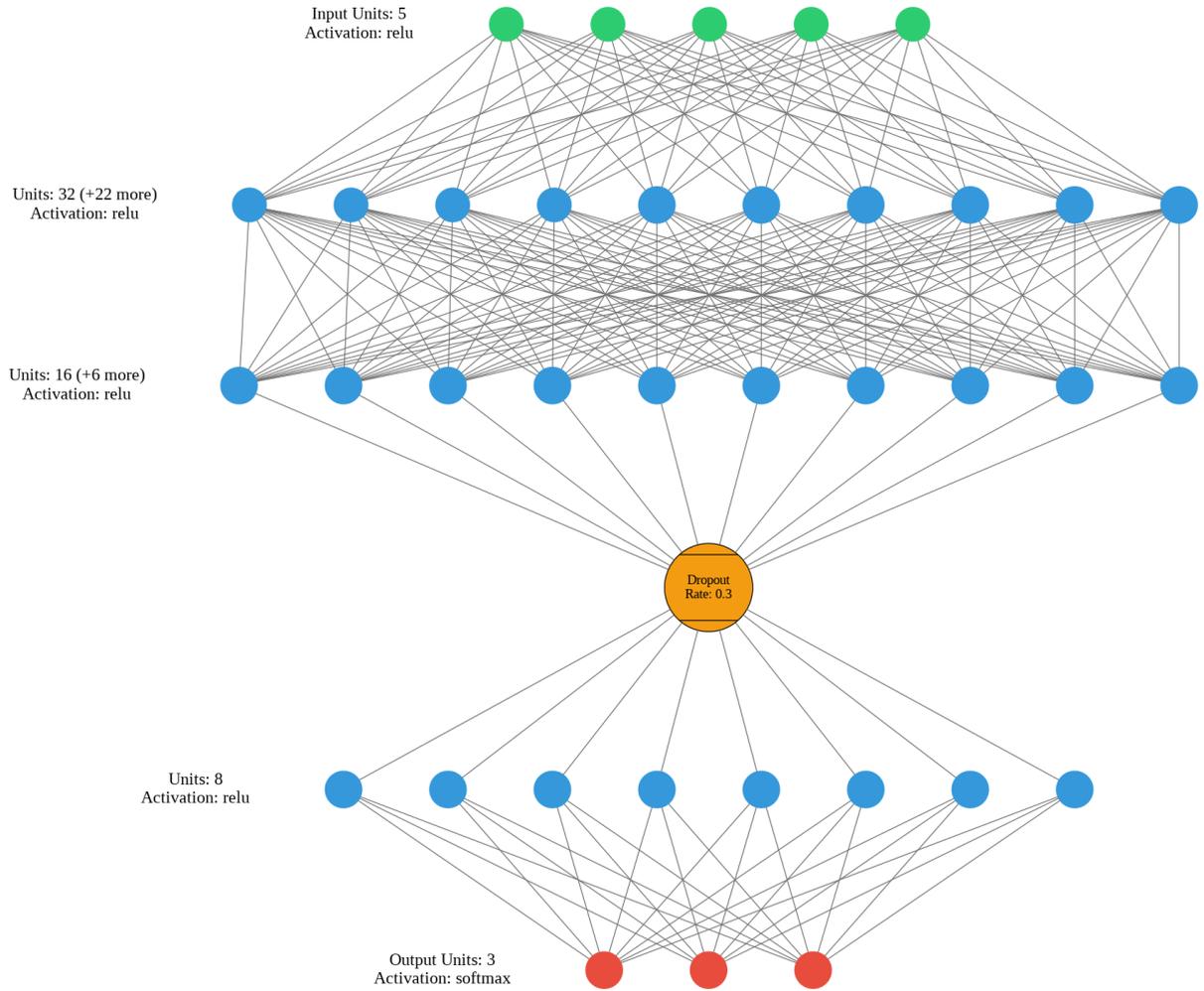


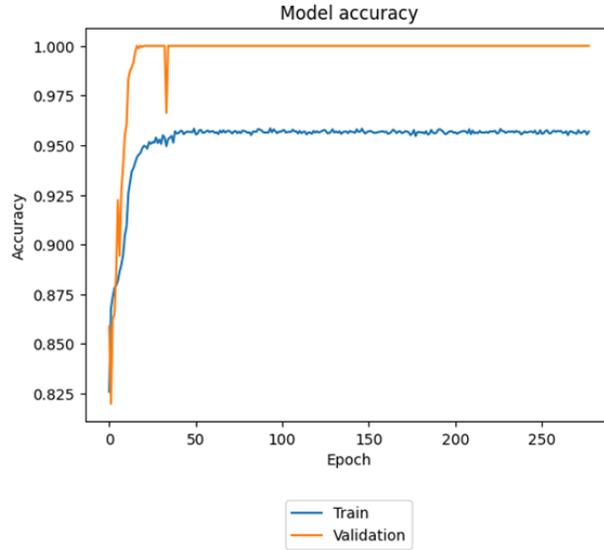
Figure 5: Architecture of the designed ANN

## 4.2 Training and Validation

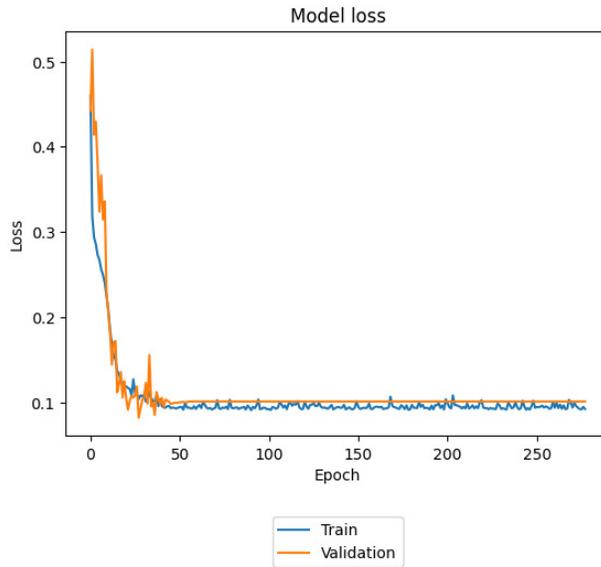
The dataset was split into a training set (75%) and a test set (25%) while maintaining class proportions through a *stratified split*. To address the class imbalance—particularly the under-representation of *VideoTCP* traffic—the SMOTE (refer to subsection 3.3.3) was applied to the training set, ensuring a balanced number of samples across classes.

For the scikit-learn models, training was performed after standardizing the variables using a `StandardScaler`. No explicit `class_weight` parameter was specified since SMOTE effectively mitigated the initial class imbalance.

For the ANN, class labels were converted into one-hot encoding before training. Validation was conducted through an internal split (20% of the training set) combined with an EarlyStopping strategy, monitoring the minimization of the validation loss. Figure 6 illustrates the evolution of the model’s performance during training, showing (a) the model accuracy and (b) the model loss.



(a) Evolution of model accuracy during training.



(b) Evolution of model loss during training.

Figure 6: Training history of the ANN: (a) model accuracy and (b) model loss.

### 4.3 Model Evaluation

The performance of each classification algorithm was assessed using standard evaluation metrics derived from the confusion matrix (CM), namely Accuracy, Precision, Recall, and F1-score. These metrics quantify the models’ ability to correctly classify the network traffic into the three categories: *DDoS*, *VoIP*, and *VideoTCP*. The definitions and formulas are as follows:

- **Accuracy (AC):** Represents the ratio of correctly predicted instances over the total number of samples. It is computed using:

$$Accuracy(AC) = \frac{TP + TN}{TP + TN + FP + FN}$$

- **Recall (R):** Measures the proportion of true positives detected among all actual positive cases. The formula is:

$$Recall(R) = \frac{TP}{TP + FN}$$

- **Precision (P):** Indicates the ratio of correctly predicted positive observations to the total predicted positives:

$$Precision(P) = \frac{TP}{TP + FP}$$

- **F1-score:** Combines precision and recall into a single metric by calculating their harmonic mean:

$$F1\ Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

To compute these metrics for each algorithm, the confusion matrices were extracted after testing on the evaluation set. These matrices contain the number of true positive (TP), false positive (FP), true negative (TN), and false negative (FN) predictions for each class. The values were used to assess how each model performed in distinguishing between normal traffic (VoIP, VideoTCP) and malicious traffic (DDoS).

Figure 7 illustrates an example confusion matrix for the best-performing model (XGBoost), showing a high rate of correct predictions across all classes. This model achieved an F1-score of 0.96, with a balanced performance across the three traffic types.

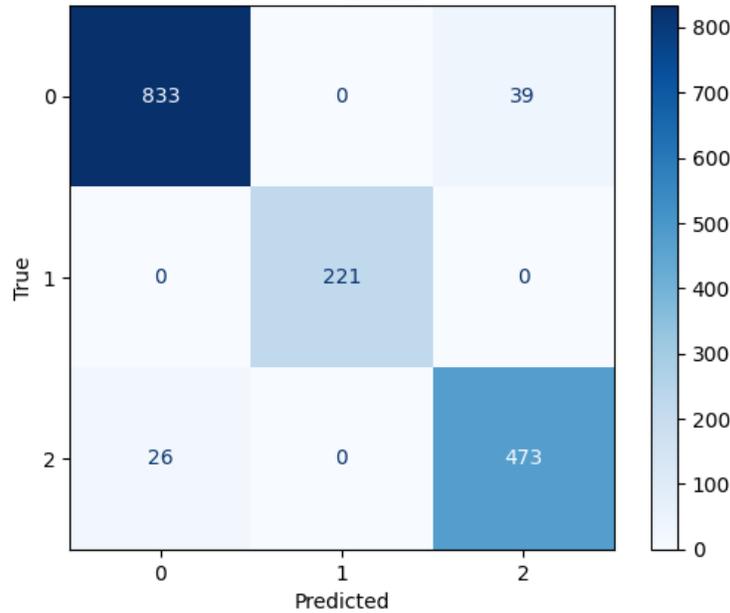


Figure 7: Confusion matrix of the XGBoost model. Class labels 0, 1, and 2 correspond to DDoS, VideoTCP, and VoIP, respectively.

## 5 Results and Discussion

This section outlines the performance outcomes of the machine learning models used in this study and provides a corresponding analysis and interpretation of these findings.

## 5.1 Results

The classification report summary (Table 3), together with the comparative analysis of F1-scores across various algorithms (Figure 8), offers a thorough evaluation of the predictive capabilities of each model.

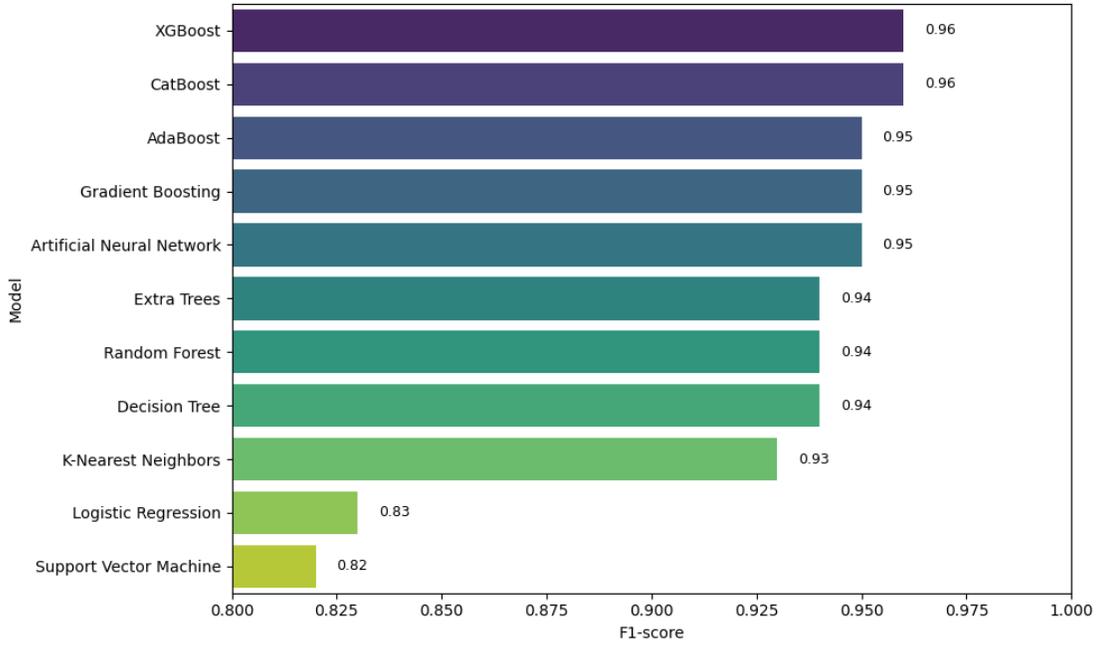


Figure 8: F1-score comparison across models.

Table 3: Summary of classification results across different models.

Class	Precision	Recall	F1-score	Accuracy	Support
<b>XGBoost</b>					
DDoS	0.97	0.96	0.96	-	872
VoIP	1.00	1.00	1.00	-	221
VideoTCP	0.92	0.95	0.94	-	499
<b>Overall</b>	<b>0.96</b>	<b>0.96</b>	<b>0.96</b>	<b>0.96</b>	<b>1592</b>
<b>AdaBoost</b>					
DDoS	1.00	0.92	0.95	-	872
VoIP	1.00	1.00	1.00	-	221
VideoTCP	0.87	1.00	0.93	-	499
<b>Overall</b>	<b>0.96</b>	<b>0.95</b>	<b>0.95</b>	<b>0.95</b>	<b>1592</b>
<b>CatBoost</b>					
DDoS	0.98	0.94	0.96	-	872
VoIP	1.00	1.00	1.00	-	221
VideoTCP	0.91	0.96	0.93	-	499
<b>Overall</b>	<b>0.96</b>	<b>0.96</b>	<b>0.96</b>	<b>0.96</b>	<b>1592</b>
<b>Extra Trees</b>					
DDoS	0.95	0.94	0.95	-	872
VoIP	1.00	1.00	1.00	-	221
VideoTCP	0.90	0.92	0.91	-	499

Continued on next page

Table 3 – continued from previous page

Class	Precision	Recall	F1-score	Accuracy	Support
<b>Overall</b>	<b>0.94</b>	<b>0.94</b>	<b>0.94</b>	<b>0.94</b>	<b>1592</b>
<b>Random Forest</b>					
DDoS	0.95	0.94	0.95	-	872
VoIP	1.00	1.00	1.00	-	221
VideoTCP	0.90	0.92	0.91	-	499
<b>Overall</b>	<b>0.94</b>	<b>0.94</b>	<b>0.94</b>	<b>0.94</b>	<b>1592</b>
<b>Gradient Boosting</b>					
DDoS	0.96	0.94	0.95	-	872
VoIP	1.00	1.00	1.00	-	221
VideoTCP	0.90	0.93	0.92	-	499
<b>Overall</b>	<b>0.95</b>	<b>0.95</b>	<b>0.95</b>	<b>0.95</b>	<b>1592</b>
<b>Logistic Regression</b>					
DDoS	0.85	0.84	0.84	-	872
VoIP	1.00	1.00	1.00	-	221
VideoTCP	0.72	0.74	0.73	-	499
<b>Overall</b>	<b>0.83</b>	<b>0.83</b>	<b>0.83</b>	<b>0.83</b>	<b>1592</b>
<b>Decision Tree</b>					
DDoS	0.95	0.94	0.95	-	872
VoIP	1.00	1.00	1.00	-	221
VideoTCP	0.90	0.92	0.91	-	499
<b>Overall</b>	<b>0.94</b>	<b>0.94</b>	<b>0.94</b>	<b>0.94</b>	<b>1592</b>
<b>K-Nearest Neighbors</b>					
DDoS	0.95	0.92	0.93	-	872
VoIP	1.00	1.00	1.00	-	221
VideoTCP	0.87	0.91	0.89	-	499
<b>Overall</b>	<b>0.93</b>	<b>0.93</b>	<b>0.93</b>	<b>0.93</b>	<b>1592</b>
<b>Support Vector Machine</b>					
DDoS	0.84	0.82	0.83	-	872
VoIP	1.00	1.00	1.00	-	221
VideoTCP	0.70	0.72	0.71	-	499
<b>Overall</b>	<b>0.82</b>	<b>0.82</b>	<b>0.82</b>	<b>0.82</b>	<b>1592</b>
<b>Artificial Neural Network</b>					
DDoS	1.00	0.91	0.95	-	872
VoIP	1.00	1.00	1.00	-	221
VideoTCP	0.86	1.00	0.93	-	499
<b>Overall</b>	<b>0.96</b>	<b>0.95</b>	<b>0.95</b>	<b>0.95</b>	<b>1592</b>

## 5.2 Results Analysis

This section analyzes the classification results obtained from various models, focusing on overall performance, robustness to class imbalance, and sources of misclassification. Key insights are drawn from evaluation metrics and confusion matrices to highlight model strengths and areas for improvement.

### 5.2.1 Performance Interpretation

The classification results obtained from the tested models are summarized in Table 3 and illustrated in Figure 8. Overall, algorithms leveraging boosting methods (XGBoost, CatBoost, AdaBoost, and Gradient Boosting) along with ANN exhibited remarkable performance, achieving global F1-scores ranging between 0.95 and 0.96. Particularly, the

XGBoost and CatBoost models demonstrated superior performance, each attaining an F1-score of 0.96, underscoring their effectiveness in capturing the characteristic patterns of network traffic within DDoS, VoIP, and VideoTCP scenarios.

Decision tree-based models (Random Forest, Extra Trees, and Decision Tree) also yielded robust results, each reaching an F1-score of 0.94. In contrast, simpler approaches such as Logistic Regression and Support Vector Machines exhibited relatively lower performances, achieving global F1-scores of 0.83 and 0.82, respectively. These findings confirm their limitations in effectively capturing complex interactions inherent to network traffic flows.

### 5.2.2 Robustness to Class Imbalance

The unequal distribution of data across the DDoS, VoIP, and VideoTCP classes represents a significant challenge to model robustness. Nevertheless, detailed results shown in Table 3 indicate that most tested models successfully maintained high precision and recall rates for the minority class (VoIP), often achieving scores close to 1.00. This outcome highlights the effectiveness of the adopted data rebalancing strategy via SMOTE, combined with the inherent robustness of the tested algorithms, in mitigating negative impacts caused by initial class imbalance. However, despite being less imbalanced than VoIP, the VideoTCP class consistently displayed slightly lower precision and recall scores. This observation suggests the persistent sensitivity of models to subtle intrinsic variations of VideoTCP flows, indicating a potential need for supplementary augmentation or specific data generation strategies targeting this particular class.

### 5.2.3 Misclassification Analysis

Confusion matrix analysis (cf. Table 3) reveals that most classification errors predominantly occur between DDoS and VideoTCP classes, while the VoIP class is almost perfectly distinguished by all models. This finding indicates that flows associated with DDoS attacks and VideoTCP transmissions exhibit very similar characteristics regarding throughput and duration, complicating their clear differentiation by classification algorithms. Models such as XGBoost and CatBoost managed to significantly reduce these errors compared to other algorithms. However, the observed persistent confusion highlights the importance of better differentiating features used during training and suggests exploring hybrid approaches or advanced deep learning methods capable of capturing subtle distinctions between these two traffic types more effectively.

## 6 Conclusion and Future Work

This paper presented a comprehensive evaluation of multiple machine learning techniques for detecting DDoS attacks in VANETs, specifically targeting emergency vehicle communication scenarios on highways. Leveraging a realistic simulation setup, which integrates the NS-3 network simulator with the SUMO mobility simulator and real-world vehicular mobility traces from Germany’s A81 highway, we generated a robust and reproducible dataset for rigorous evaluation.

The experimental results demonstrated the high effectiveness of several machine learning algorithms, notably XGB, CB, AB, GB, and ANN, all achieving exceptional classification performance with F1-scores up to 96%. Our findings confirmed the efficacy of SMOTE to handle imbalanced datasets, significantly enhancing the model’s ability to accurately classify minority classes, particularly the VoIP traffic class.

This study offers significant scientific contributions, including the introduction of a reproducible and realistic methodology combining NS-3 and SUMO simulators with authentic mobility data, and a systematic comparison of widely recognized machine learning classifiers in the context of highway VANET scenarios. Furthermore, the detailed SHAP-based feature selection analysis provided valuable insights into the key predictors necessary for accurate intrusion detection.

Despite these contributions, the study has several limitations. Primarily, the results remain constrained by the synthetic nature of the dataset, albeit enhanced by real-world mobility patterns. Moreover, the simulations did not encompass the full complexity of real-world communication scenarios, such as varying signal propagation conditions, diverse network topologies, and real-time network adaptations.

Future research should focus on extending the present approach through the following perspectives:

- Conducting experiments in real-world settings by utilizing actual connected vehicles and infrastructure, which would validate and potentially refine the proposed classification models.
- Investigating the feasibility and effectiveness of deploying these detection systems onboard vehicles, thus enabling practical intrusion detection solutions in real-time scenarios.

- Expanding the methodology to detect other prominent cybersecurity threats in VANETs, including spoofing, Sybil, and blackhole attacks, thereby broadening the scope and practical applicability of the developed intrusion detection framework.

## **Acknowledgements**

None.

## **Funding**

The authors received no specific funding for this study.

## **Author Contributions**

Conceptualization, B.M.; Methodology, B.M. and V.F.; Software, B.M.; Investigation, B.M.; Writing—original draft, Bappa Muktar; Writing—review & editing, V.F and N.A. All authors reviewed the results and approved the final version of the manuscript.

## **Availability of Data and Materials**

The data that support the findings of this study are available from the Corresponding Author, B.M., upon reasonable request.

## **Ethics Approval**

Not applicable.

## **Conflicts of Interest**

The authors declare no conflicts of interest to report regarding the present study.

## Abbreviations

The following abbreviations are used in this manuscript:

1D-CNN	One-Dimensional Convolutional Neural Network
AB	AdaBoost
ANN	Artificial Neural Network
CB	CatBoost
DL	Deep Learning
DDoS	Distributed Denial of Service
DT	Decision Tree
FDI	False Data Injection
GB	Gradient Boosting
GRU	Gated Recurrent Unit
IDoS-CC	Intelligent DoS Attack Detection with Congestion Control
IoV	Internet of Vehicles
KNN	K-Nearest Neighbors
LR	Logistic Regression
LSTM	Long Short-Term Memory
ML	Machine Learning
NS-3	Network Simulator 3
OMNeT++	Objective Modular Network Testbed in C++
OSM	OpenStreetMap
RF	Random Forest
RSU	Roadside Unit
SD-VANET	Software-Defined Vehicular Ad Hoc Network
SDN	Software Defined Networking
SHAP	SHapley Additive exPlanations
SMOTE	Synthetic Minority Over-sampling Technique
SNR	Signal-to-Noise Ratio
SVM	Support Vector Machine
SUMO	Simulation of Urban MObility
TLBO	Teaching and Learning-Based Optimization
UDP	User Datagram Protocol
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VANET	Vehicular Ad Hoc Network
VoIP	Voice over IP
XGB	XGBoost

## References

- [1] Dutta, Arijit and Samaniego Campoverde, Luis Miguel and Tropea, Mauro and De Rango, Floriano. A comprehensive review of recent developments in vanet for traffic, safety & remote monitoring applications. *Journal of Network and Systems Management*. 2024;32(4):73. [CrossRef]
- [2] Pawar, Vaishali and Zade, Nilima and Vora, Deepali and Khairnar, Vaishali and Oliveira, Aurenice and Kotecha, Ketan and Kulkarni, Ambarish. Intelligent Transportation System With 5G Vehicle-to-Everything (V2X): Architectures, Vehicular Use Cases, Emergency Vehicles, Current Challenges, and Future Directions. *IEEE Access*. 2024;12:183937–183960. [CrossRef]
- [3] Al-Mohtaseb, Abeer and Hanoon, Ali Qasim and Samara, Ghassan and Al Daoud, Essam and Alidmat, Omar and Batyha, Radwan and Aljaidi, Mohammad and Alazaidah, Raed and Elrashidi, Ali. A Comprehensive Review of VANET Attacks: Predictive Models, Vulnerability Management, and Defense Selection. *25th International Arab Conference on Information Technology (ACIT)*; 2024 Dec 10–12; Zarqa, Jordan. Piscataway, NJ, USA: IEEE; 2024. p. 1–9
- [4] Polat, Onur and Oyucu, Saadin and Türkoğlu, Muammer and Polat, Hüseyin and Aksoz, Ahmet and Yardımcı, Fahri. Hybrid AI-Powered Real-Time Distributed Denial of Service Detection and Traffic Monitoring for Software-Defined-Based Vehicular Ad Hoc Networks: A New Paradigm for Securing Intelligent Transportation Networks. *Applied Sciences*. 2024;14(22):10501. [CrossRef]

- 
- [5] Ababsa, Mohamed and Ribouh, Soheyb and Malki, Abdelhamid and Khoukhi, Lyes. Deep Multimodal Learning for Real-Time DDoS Attacks Detection in Internet of Vehicles. arXiv preprint. 2025. [CrossRef]
- [6] Vamshi Krishna, K and Ganesh Reddy, K. Classification of distributed denial of service attacks in VANET: a survey. *Wireless Personal Communications*. 2023;132(2):933–964. [CrossRef]
- [7] Himanshu Setia, Amit Chhabra, Sunil K. Singh, Sudhakar Kumar, Sarita Sharma, Varsha Arya, Brij B. Gupta, Jinsong Wu. Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments. *Cyber Security and Applications*. 2024;2:100037. [CrossRef]
- [8] Polat, Onur and Oyucu, Saadin and Türkoğlu, Muammer and Polat, Hüseyin and Aksoz, Ahmet and Yardımcı, Fahri. Hybrid AI-Powered Real-Time Distributed Denial of Service Detection and Traffic Monitoring for Software-Defined-Based Vehicular Ad Hoc Networks: A New Paradigm for Securing Intelligent Transportation Networks. *Applied Sciences*. 2024;14(22):10501. [CrossRef]
- [9] Polat, Huseyin and Turkoglu, Muammer and Polat, Onur. Deep network approach with stacked sparse autoencoders in detection of DDoS attacks on SDN-based VANET. *IET Communications*. 2020;14(22):4089–4100. [CrossRef]
- [10] Gopi, R and Mathapati, Mahantesh and Prasad, B and Ahmad, Sultan and Al-Wesabi, Fahd N and Alohalı, Manal Abdullah and Hilal, Anwer Mustafa. Intelligent DoS Attack Detection with Congestion Control Technique for VANETs. *Computers, Materials & Continua*. 2022;72(1):141–156. [CrossRef]
- [11] Kadam, Nivedita and Krovi, Raja Sekhar. Machine Learning Approach of Hybrid KSVN Algorithm to Detect DDoS Attack in VANET. *International Journal of Advanced Computer Science and Applications*. 2021;12(7). [CrossRef]
- [12] Alkadiri, Naam and Ilyas, Muhammad. Machine Learning-Based Architecture for DDoS Detection in VANETs System. 2022 International Conference on Artificial Intelligence of Things (ICAIoT); 2022 Dec 29–30; Istanbul, Turkey. Piscataway, NJ, USA: IEEE; 2022. p. 1–7
- [13] Rashid, Kanwal and Saeed, Yousaf and Ali, Abid and Jamil, Faisal and Alkanhel, Reem and Muthanna, Ammar. An adaptive real-time malicious node detection framework using machine learning in vehicular ad-hoc networks (VANETs). *Sensors*. 2023;23(5):2594. [CrossRef]
- [14] Anyanwu, Goodness Oluchi and Nwakanma, Cosmas Ifeanyi and Lee, Jae-Min and Kim, Dong-Seong. Optimization of RBF-SVM kernel using grid search algorithm for DDoS attack detection in SDN-based VANET. *IEEE Internet of Things Journal*. 2022;10(10):8477–8490. [CrossRef]
- [15] Marwah, Gagan Preet Kour and Jain, Anuj and Malik, Praveen Kumar and Singh, Manwinder and Tanwar, Sudeep and Safirescu, Calin Ovidiu and Mihaltan, Traian Candin and Sharma, Ravi and Alkhayyat, Ahmed. An improved machine learning model with hybrid technique in VANET for robust communication. *mathematics*. 2022;10(21):4030. [CrossRef]
- [16] Adhikary, Kaushik and Bhushan, Shashi and Kumar, Sunil and Dutta, Kamlesh. Hybrid algorithm to detect DDoS attacks in VANETs. *Wireless Personal Communications*. 2020;114(4):3613–3634. [CrossRef]
- [17] Tariq, Usman. Optimized Feature Selection for DDoS Attack Recognition and Mitigation in SD-VANETs. *World Electric Vehicle Journal*. 2024;15(9):395. [CrossRef]
- [18] Lekshmi V, R. Suji Pramila and Tibbie Pon Symon V A. Defense Mechanisms for Vehicular Networks: Deep Learning Approaches for Detecting DDoS Attacks. *International Journal of Advanced Computer Science & Applications*. 2024;15(7). [CrossRef]
- [19] Haydari, Ammar and Yilmaz, Yasin. RSU-based online intrusion detection and mitigation for VANET. *Sensors*. 2022;22(19):7612. [CrossRef]
- [20] Riley GF, Henderson TR. The ns-3 network simulator. In: Wehrle K, Güneş M, Gross J, editors. *Modeling and tools for network simulation*. Berlin, Heidelberg: Springer Berlin Heidelberg; 2010. p. 15–34.
- [21] Behrisch, Michael and Bieker, Laura and Erdmann, Jakob and Krajzewicz, Daniel. SUMO—simulation of urban mobility: an overview. In *Proceedings of the SIMUL 2011, The Third International Conference on Advances in System Simulation*; 2011 Oct 23–28; Barcelona, Spain. Red Hook, NY, USA: ThinkMind; 2011.
- [22] Chawla, Nitesh V and Bowyer, Kevin W and Hall, Lawrence O and Kegelmeyer, W Philip. SMOTE: synthetic minority over-sampling technique. *Journal of artificial intelligence research*. 2002;16:321–357. [CrossRef]