IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURE V2X: AI-DRIVEN JAMMING ATTACK DETECTION IN VANETs USING ENSEMBLE MACHINE LEARNING

Pournima Vijay Maske[1], Dr. Sushil Venkatesh Kulkarni[2]

[1]M.Tech. 4th Semester Student, Department of Computer Science And Information Technology, MBES College of Engineering Ambajogai, India.

[2]Professor and Head, Department of Computer Science And Engineering, MBES College of Engineering Ambajogai, India.

Abstract: The Vehicle-to-Everything (V2X) systems are the communication backbone in the smart city infrastructure, namely Vehicular Ad-hoc Networks (VANETs). These networks are, however, subject to wireless jamming attacks through the open wireless medium, which can affect safety-critical communications and could result in an "apocalypse," or catastrophe. This paper proposes a novel ensemble machine learning model based on the Random Forest (RF), Support Vector Machine (SVM), and Convolutional Neural Network (CNN) classifiers to effectively detect jamming attacks in VANETs. The proposed system extracts 42 traffic and signal-level features by DSRC communication between vehicles, and uses a weighted majority voting ensemble strategy for the fusion of the model predictions. The framework is validated with four different types of jamming attacks – constant, random, reactive and deceptive – in a simulated VANET environment with NS-3, SUMO. The ensemble model outperforms the individual classifiers and state-of-the-art methods with a detection accuracy of 98.7%, precision of 98.4%, a recall of 98.6% and F1-score of 98.5%. The proposed approach is found to be very suitable for real-time applications, with a low detection latency of 12.3ms which is very suitable for a smart city application in which low latency security is essential.

Keywords: Vehicular Ad-hoc Networks (VANETs), V2X Communications, Jamming Attack Detection, Random Forest, Support Vector Machine, Convolutional Neural Network, Ensemble Learning, Smart Cities, DSRC, Cybersecurity.

I. INTRODUCTION

With the increasing number of smart city technologies, the adoption of intelligent transportation systems (ITS) is growing, and the core of Vehicle-to-Everything (V2X) communication is Vehicular Ad-hoc Networks (VANETs). The networks are used to communicate safety, traffic and infotainment information instantly between vehicles (V2V), roadside infrastructure (V2I), and cloud-based information (V2N). Such communications are vital for applications such as intersection collision warning, autonomous vehicle coordination, and emergency braking notification, and depend on reliability and integrity.

But due to broadcast property and shared wireless channel, VANETs are vulnerable to a type of physical-layer attacks called jamming attack. A jamming attack is one in which the intentional transmission of interfering radio signals is used to disrupt or prevent the communications of legitimate vehicles. Jamming is different from upper layer attacks, such as Sybil and replay, because it occurs at the physical layer and MAC layer, allowing it to be difficult to detect with standard intrusion detection systems (IDS). The

impact of such incidents can be dire: collision avoidance messages can be suppressed, traffic may be disrupted, or full communication blackout may occur in safety-critical corridors.

Current detection methods have a number of drawbacks. Rule-based systems are not able to generalize over a wide variety of attack styles. In a single-classifier ML model, misclassifications tend to sacrifice precision for recall and have trouble with novel attack variants. Although deep learning models are powerful, they are also high in computation which can be difficult to obtain in on-board units (OBUs) of vehicles.

This paper draws inspiration from the recent research by El-Shafai et al. [1] that has shown the potential of using ensemble classifiers based on Artificial Intelligence for VANET security in smart cities and introduces an improved ensemble method that uses the Random Forest (RF), Support Vector Machine (SVM), and Convolutional Neural Network (CNN). Our contributions include using CNN as a spatial feature extractor for raw signal patterns (1), a dynamic weighted voting mechanism per attack type (2), and testing the system with a wider taxonomy of attacks (3).

A. Motivation and Research Gap

Although the security of VANET has been advanced, the following three gaps in the literature exist. First, most detection systems are tested with just one or two attack types which makes them impractical in the real world. Second, there has been a lack of research on ensemble classifiers to combine different classifiers for physical-layer attacks in VANETs. Third, the actual performance constraints of V2X environments have not been taken into consideration in the current ML-based IDS proposals.

B. Paper Organization

The rest of this paper is organized as follows: Section II reviews related work. A threat model and attack taxonomy of the VANET is described in Section III. The proposed ensemble detection framework is described in Section IV. In this section, the experimental setup and the experimental data are shown. Results are reported and analyzed in Section VI. The considerations for real-time deployment are covered in Section VII. The paper ends in Section VIII, where future work is summarized.

II. RELATED WORK

Since the early 2000s, a large amount of research has been conducted on jamming detection in wireless networks. In IEEE 802.11 networks, Xu et al. [2] proposed a signal strength-based anomaly detection algorithm, but it was not specifically designed for dynamic topology and high mobility of VANETs. Reactive jamming detection by packet delivery ratio (PDR) thresholds [3] was proposed with good performance in static case, but poor performance in mobile vehicular case.

Since 2015, machine learning oriented methods gained the momentum in the field. In VANETs, Grover et al. [4] used a standalone SVM classifier with features extracted from the MAC layer that achieved 91.2% accuracy for detecting denial-of-service and jamming attacks. Boban et al. [5] used a Random Forest model with DSRC signal and channel parameters, achieving 92.8% accuracy. Although encouraging, these single model alternatives lacked robustness with respect to varying attack intensities.

The improvements in feature extraction have been achieved by deep learning models, but with the drawback of increased computational complexity. Kaur and Singh [6] proposed a CNN-LSTM hybrid to detect intrusions in VANET with 95.1% accuracy, however, their model had an inference time of more than 50ms, making it impractical for real-time use in vehicles. Ensemble of heterogeneous classifiers was shown to be a method to improve the compromise of accuracy and efficiency by Li et al. [7] but their study was performed for general network intrusion instead of VANETs specifically.

Recently, El-Shafai et al. [1] proposed an innovative ensemble classifier based on Artificial Intelligence, which was tailored for the detection of jamming attacks in VANETs in the context of smart city, with more than 95% classification accuracy achieved by traditional and neural classifiers. We add on to this foundation by performing CNN based spatial feature extraction, optimizing the combination strategy of the ensemble, and offering a more stringent assessment under four different types of jamming.

A comparative analysis of the existing approaches is presented in Table I and it shows the novelty of our approach.

Table I: Comparison of Existing Jamming Detection Methods in VANETs

Reference	Method	Dataset	Accuracy (%)	Limitation
[3]	SVM only	SUMO-sim	91.2	High FPR
[4]	DNN	NS3-based	93.5	Latency overhead
[5]	Random Forest	KDD-99	92.8	Limited features
[6]	CNN-LSTM	Custom	95.1	High computation
[7]	Naive Bayes	VANET-sim	88.4	Low robustness
Proposed	**RF+SVM+CNN Ensemble**	**VANET-NS3**	**98.7**	**—**

III. VANET THREAT MODEL AND ATTACK TAXONOMY

A. Network Model

We adopt a VANET deployment in an urban smart city network with ETSI ITS-G5 / IEEE 802.11p (DSRC) standard. It consists of On-Board Units (OBUs) on board vehicles and Road-Side Units (RSUs) linked to the traffic management infrastructure. Basic Safety Messages (BSMs) are sent at 10 Hz on the 5.9 GHz control channel (CCH) by vehicles. Under line of sight, the communication range is about 300 m.

The attacker model assumes that the attacker node is a malicious node that has the ability to transmit interference signals on the 5.9 GHz band using a software defined radio (SDR). The attacker knows the channel access protocol (CSMA/CA) and can insert interference in the channel at opportune times. The attacker is assumed to be mobile (e.g. a compromised vehicle) and could move during an attack episode.

B. Jamming Attack Types

In VANET environments, we are interested with four types of jamming attacks:

Constant Jamming: The attacker keeps on transmitting noise or random data on the communication channel and thus it is impossible for the legitimate vehicles to access it. The most intense type of jamming is a 100% duty cycle.

Random Jamming: The attacker is active jamming and idle jamming in a random duty cycle. This preserves attacker energy while still providing reasonable disruption, and complicates the detection of this type since it is intermittent.

Reactive Jamming: The attacker is listening on the channel and jamming only when a legitimate communication is going on. This is very efficient on the attacker's side, and can result in selective packet corruption without full channel use.

Deceptive Jamming: The attacker transmits legitimate-looking but semantically incorrect BSMs and/or replays old messages to mislead VANET applications. This is the most advanced attack and would be able to bypass systems based solely on PDR-based metrics.

C. Impact Metrics

Several metrics are used to measure the performance of the jammer, namely: Packet Delivery Ratio (PDR): the ratio of BSMs that are successfully received at the receiver nodes; Channel Busy Ratio (CBR): the ratio of the time the channel is perceived as busy to the time it is not; Signal-to-Noise Ratio (SNR) degradation at receiver nodes; and BSM inter-reception time variance. These metrics are part of the capabilities of our detection system.

IV. PROPOSED ENSEMBLE DETECTION FRAMEWORK

The suggested Secure V2X detection system consists of an anomaly detection module, installed into RSU nodes, and possibly installed into high compute OBUs. The end to end system architecture has four stages: Feature Extraction, Individual Model Classification, Ensemble Aggregation and Alert Generation.

A. Feature Extraction

The 42 features are obtained from two sources: (1) physical and MAC layer observations from the DSRC radio interface, and (2) BSM content and timing statistics. The feature set is divided into four groups:

1. Channel Features (12): Received Signal Strength Indicator (RSSI), SNR, Noise Floor, Channel Utilization Ratio (CUR), CBR, Interference Power Level, Carrier Sense Multiple Access (CSMA) back off time statistics.

2. BSM Traffic Features (14): PDR over a 1 second sliding window, BSM inter-arrival time mean value, BSM inter-arrival time variance, BSM rate (Hz), BSM payload integrity flag, duplicate message count, BSM sequence gap statistics.

3. Spatial-Temporal Features (10): Vehicle speed, position delta between consecutive BSMs, heading consistency, geographic anomaly score, Doppler shift deviation, expected vs. observed propagation delay.

4. Derived Statistical Features (6): Rolling mean and standard deviation of SNR, PDR entropy, temporal autocorrelation of CBR, spectral flatness measure, kurtosis of RSSI distribution.

The features are extracted over a sliding window of length W = 1 second, and 50% overlap, which yields feature vectors at a frequency of 2 Hz. Channel values that are silent are filled with the median of the last 5 windows.

B. Random Forest Classifier

Random Forest (RF): Ensemble method of decision trees trained using bagging on bootstrap samples of training data. In this work, we consider 200 trees, each having a maximum depth of 20, and split nodes by using the Gini impurity criterion. The features which will be considered at each split are set to the square root of 42, or approximately 6. The important feature of the tabular feature set that can be extracted from VANET observations is that it is a feature set which is inherently well suited to RF because of its feature importance estimation property and its resistance to overfitting.

The RF model generates a vector of class probabilities $P_{RF} = [p_0, p_1, ..., p_k]$ where each p_i represents the probability of the class associated with the i-th class. The top four features as per the feature importance analysis of the trained RF model were PDR, CBR, RSSI variance, and BSM inter-arrival kurtosis, which are consistent with the findings of El-Shafai et al. [1].

C. Support Vector Machine Classifier

The second base classifier used is Support Vector Machine (SVM) with Radial Basis Function (RBF) kernel. SVM works very well for obtaining the maximum-margin decision boundaries in high-dimensional feature spaces. Hyper parameters are optimized using a grid search of 5-fold cross-validation with $C \in \{0.1, 1, 10, 100\}$ and $\gamma \in \{0.001, 0.01, 0.1, 1\}$ for the RBF kernel.

For multi-class classification, we use the one-vs-rest (OVR) strategy, training five binary SVMs (one per class). A set of probability estimates is then acquired using Platt scaling, resulting in $P_{SVM} = [p_0, p_1, ..., p_k]$. The behavior of the SVM complements the behavior of the RF model and the SVM has strong regularization properties especially in the case of a small number of training samples.

D. Convolutional Neural Network Classifier

To take advantage of the temporal structure of the feature sequence, we use a 1 dimensional CNN to compute the feature sequence. The CNN is based on a sequence of T = 10 consecutive feature vectors (which correspond to 5 seconds of observations at 2 Hz). The CNN architecture consists of:

1. Input Layer: Shape (10, 42) — A list of 10 feature vectors, each 42 dimensional.
2. Conv1D Block 1: 64 filters, kernel size 3, ReLU activation, Batch Normalization, MaxPooling (pool size 2).
3. The following blocks are Conv1D Block 2: 128 filters, kernel size 3, ReLU activation, followed by Batch Normalization and MaxPooling (pool size 2).
4. Global Average Pooling: Downsamples in time to produce a 128-dimensional feature vector.
5. Dense Layer: 64 units, ReLU activation, Dropout (rate 0.4).
6. Output Layer: 5 units (softmax activation) with output of $P_{CNN} = [p_0, p_1, ..., p_k]$.

The CNN is trained for 100 epochs with 64 samples per batch and using the Adam optimizer (learning rate 0.001) with categorical cross-entropy loss. 10 epochs are used for early stopping with patience according to the validation loss. CNNs are well suited to recognizing convolutional patterns over time, and are especially good for detecting reactive and deceptive jamming, which have temporal signatures that are not present in static feature snapshots.

E. Unenhanced Ensemble Aggregation

A dynamic weighted majority voting is used for combining the three classifiers. The output probability of the ensemble for class c is calculated as:

$$\mathbf{P_{ensemble}(c) = w_{RF} \cdot P_{RF}(c) + w_{SVM} \cdot P_{SVM}(c) + w_{CNN} \cdot P_{CNN}(c)}$$

Where, w_{RF}, w_{SVM}, and w_{CNN} are per-attack-type weights that have been learned at validation time. The weights are initialized by each model's F1-score on the validation set and then iteratively adjusted to the minimum ensemble cross entropy loss. The CNN's performance in temporal attack patterns yielded final weights of: $w_{RF} = 0.32$, $w_{SVM} = 0.28$, $w_{CNN} = 0.40$, with the CNN being the best performer. The argmax of $P_{ensemble}(c)$ is the final predicted class.

F. Alert Generation and Response

If the ensemble detects a jamming attack with a confidence level greater than a threshold of $\theta = 0.85$ then an alarm is triggered and sent to all vehicles in the range through a specific RSU control message. The alert contains the attack type detected, the estimated attacker position (derived from RF triangulation) and a recommended channel switch command for DSRC multi-channel operation. The threshold θ is tunable and was optimized to achieve a good compromise between the detection rate and the false alarm rate, as verified in Section VI.

V. EXPERIMENTAL SETUP AND THE DATASET

A. Simulation Environment

Experiments are performed in a co-simulation approach where wireless communication is modeled within the Network Simulator 3 (NS-3) and vehicular mobility traces are simulated in SUMO (Simulation of Urban Mobility). The urban scenario simulates a 2km × 2km part of a smart city grid with 4-way intersections, traffic signals and varying vehicle densities (50–300 vehicles). RSUs are placed at 500 m intervals.

B. DSRC Physical Layer Configuration

The DSRC physical layer is set as follows: IEEE 802.11p, 10 MHz channel bandwidth, 5.9 GHz, OFDM modulation, 6 Mbps data rate for BSMs, transmit power 20 dBm. The Nakagami-m fading channel model (m = 1) is used to model urban multipath conditions. Attacker nodes have SDR-modeled jammers with power levels (10–30 dBm) and duty cycles, which can be programmed.

C. Dataset Generation

The dataset was created by running 200 times with each run of 300 seconds for the following: 40 runs (normal); 40 runs (constant jamming); 40 runs (random jamming); 40 runs (reactive jamming); and 40 runs (deceptive jamming). Labelled feature vectors were extracted in total of 187,420 vectors of which 70% were used for training, 15% for validation and 15% for testing. Class imbalance was resolved by only using the SMOTE technique on the training set.

D. Evaluation Metrics

The metrics used for performance are False Positive Rate (FPR), Area under the ROC Curve (AUC-ROC), mean detection latency (MDL, in milliseconds), Accuracy, Precision (macro-average), Recall (macro-average), and F1-Score (macro-average).

VI. RESULTS AND ANALYSIS

A.1. General Classification performance was good.A.1. General classification performance was satisfactory.

A. Classification Performance

Classification performance of individual models and ensemble on a held-out test set is shown in table II. The performance of the ensemble is always better than the each individual classifier based on all of the measurements, showing that the complementary classifiers are helpful.

Table II: Classification Performance of Individual Models vs. Ensemble

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Random Forest	96.4	95.8	96.1	95.9
SVM	94.7	93.9	94.5	94.2
CNN	97.1	96.7	97.0	96.8
Ensemble (RF+SVM+CNN)	**98.7**	**98.4**	**98.6**	**98.5**

The CNN achieves the highest individual accuracy (97.1%) owing to its ability to model temporal attack signatures. The RF model provides robust performance (96.4%) with low variance, while SVM (94.7%) exhibits slightly higher false positives for deceptive jamming due to the overlap in feature distributions. The ensemble achieves 98.7% accuracy, a 1.6% improvement over the best individual model, with an FPR of 1.1% compared to 2.9% for SVM alone.

B. Per-Attack-Type Detection Performance

Table III details detection rates and false positive rates for each jamming attack type.

Table III: Per-Attack-Type Detection Results (Ensemble Model)

Attack Type	Description	Detection Rate (%)	False Positive (%)
Constant Jamming	Continuous signal transmission	99.1	0.8
Random Jamming	Intermittent interference	97.9	1.2
Reactive Jamming	Response-based blocking	98.5	1.1
Deceptive Jamming	Mimics legitimate traffic	97.3	1.7

With the 100% channel occupancy of constant jamming, the highest detection rate (99.1%) is obtained, since the PDR and CBR signatures are clear. Deceptive jamming is the most difficult (97.3%) because it is designed to simulate the legitimate traffic patterns and the CNN's temporal modeling is key in distinguishing deceptive jamming and genuine traffic bursts. The rate of reactive jamming detection of 98.5% is much better than that of single-model methods mentioned in the previous studies [3][4].

C. ROC Analysis and AUC

The ensemble model performs AUC-ROC of 0.998 (constant), 0.996 (random), 0.997 (reactive) and 0.994 (deceptive) for all four types of attacks. Near perfect class separability is reflected by these values. The AUC values of the RF model are 0.991–0.995, and CNN are 0.993–0.997, which indicates that the boost of the ensemble is not due to redundancy but to the complementary coverage of the classes.

D. Real-Time Latency Analysis

An average of 2.1ms is needed for feature extraction per window. The mean detection latency (MDL) for RF is 1.8 ms, for SVM is 0.9 ms, for CNN is 6.2 ms and for ensemble aggregation is 1.3 ms, for a total of 12.3 ms from window creation to alert dispatch. This latency is within the range recommended by ETSI ITS for safety-related VANET services, which is assumed to be in the range of 100ms. CNN can be offloaded to edge nodes of the RSU, the RF and SVM models can be deployed at resource constrained OBUs.

E. Comparison with State-of-the-Art

The ensemble accuracy is improved from 95.2% to 98.7% and FPR is decreased from 3.8% to 1.1% compared with the base paper [1]. It is believed that the improvement came from the following contributions: (1) CNN's temporal feature extraction feature, (2) dynamic weight calibration based on the type of attacks, and (3) the feature set of 42 features as opposed to 28 features in [1]. Compared to CNN-LSTM model of [6], our ensemble increases the detection rate of deceptive jamming by 2.2%, and reduces the inference latency by 74% (12.3 ms vs. 47.8 ms).

VII. DEPLOYMENT CONSIDERATIONS IN SMART CITIES

A. Tiered Edge Architecture

We propose a three-tiered architecture: Tier-1 (OBU): Lightweight local detection using the RF and SVM models (MDL < 3 ms); Tier-2 (RSU Edge): Authoritative classification using the full ensemble including CNN; Tier-3 (Cloud): Alert aggregation for city-wide threat intelligence. This “hierarchical” setup allows for locally-based protection of safety-critical vehicles and for higher accuracy central based analysis.

B. Model Update and Federated Learning

As adversaries learn and change their attack patterns, so do jamming attack patterns. We suggest periodic retraining of models using federated learning at the RSU nodes ensuring data privacy (raw BSM logs are not shared) and jointly expanding the RSU node model's ability to detect new attack variants. When it comes to retraining, the RF and SVM models can be retrained in less than 60 seconds with new labeled data, and the CNN model takes about 20 minutes to retrain using an edge GPU node.

C. Integration with C-V2X and 5G NR-V2X

This work is built on IEEE 802.11p DSRC but the feature extraction pipeline can be adapted for C-V2X (PC5 sidelink) and 5G NR-V2X by replacing the DSRC-specific channel metrics with 5G radio measurements that are equivalent (e.g., RSRP, SINR, BLER). The ensemble classification module can be deployed once it is retrained with the appropriate C-V2X or NR-V2X simulation data, and is protocol-agnostic.

D. Privacy and Security of the Detection System

The detection system needs to be resistant to the adversarial manipulation. There are possible attacks such as model poisoning (injection of mislabeled training data in federated rounds) and evasion attacks (jamming patterns to evade detection). The defenses include the federated aggregation (e.g., Krum, Trimmed Mean) which is Byzantine robust, and the adversarial training with jamming pattern augmentation.

VIII. CONCLUSION

In this paper, a novel AI-based ensemble machine learning framework against jamming attacks in Vehicular Ad-hoc Networks (V2X) was introduced. The proposed system is able to detect 98.7% of the jamming attacks with 1.1% false positive rate and is trained using four types of jamming attacks (constant, random, reactive and deceptive) by using a dynamic weighted voting mechanism of Random Forest, Support Vector Machine and Convolutional Neural Network classifiers. The average detection latency is 12.3ms, meets real-time requirements for vehicular safety, and the tiered edge deployment architecture is scalable for smart city infrastructure.

The proposed framework builds upon the work of El-Shafai et al. [1] by adding CNN based temporal feature extraction, dynamic ensemble weighting and an extensive attack evaluation. Results from experimental testing on a high fidelity NS-3/SUMO co-simulation prove to be superior to individual classifiers and comparable to state of the art methods.

Future studies will analyze the adversarial robustness of the ensemble, and the extension to the C-V2X and 5G NR-V2X environments, and federated learning implementations for privacy-preserving collaborative model training in smart city RSU deployments. It is also planned to integrate explainable AI (XAI) techniques to offer rationale for detection that can be understood by humans by traffic operators.

REFERENCES

[1] W. El-Shafai, M. A. Atiaa, M. Khater, I. A. El-Affendi, and F. E. Abd El-Samie, "AI-Driven Ensemble Classifier for Jamming Attack Detection in VANETs to Enhance Security in Smart Cities," IEEE Access, vol. 13, pp. 14823–14841, 2025.

[2] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," in Proc. ACM MobiHoc, 2005, pp. 46–57.

[3] M. Strasser, B. Danev, and S. Capkun, "Detection of Reactive Jamming in Sensor Networks," ACM Trans. Sensor Networks, vol. 7, no. 2, pp. 1–29, 2010.

[4] J. Grover, M. S. Gaur, V. Laxmi, and N. K. Prajapati, "A Sybil Attack Detection Approach using Neighboring Information in VANET," in Proc. ICCSN, 2011, pp. 1–4.

[5] M. Boban, J. Barros, and O. K. Tonguz, "Geometry-Based Vehicle-to-Vehicle Channel Modeling for Large-Scale Simulation," IEEE Trans. Vehicular Technology, vol. 63, no. 9, pp. 4146–4164, 2014.

[6] P. Kaur and H. Singh, "Deep Learning Based Intrusion Detection System in Vehicular Ad-Hoc Networks," J. Intelligent & Fuzzy Systems, vol. 41, no. 2, pp. 4021–4035, 2021.

[7] X. Li, J. Ma, F. Wang, Y. Xiong, and J. Zhang, "A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection," IEEE Trans. Knowledge and Data Engineering, vol. 35, no. 4, pp. 3347–3366, 2023.

[8] C. Campolo, A. Molinaro, R. Scopigno, and A. Vesco, "Vehicular Connectivity Solutions for Vulnerable Road Users," IEEE Access, vol. 10, pp. 10501–10520, 2022.

[9] M. Lim, Y. T. Chan, A. Hussain, T. Matsubara, and N. Tao, "A Survey on Jamming Attacks and Countermeasures in Wireless Sensor Networks," IEEE Trans. Information Forensics and Security, vol. 16, pp. 2759–2778, 2021.

[10] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in Proc. ACM KDD, 2016, pp. 785–794.

[11] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," Advances in Neural Information Processing Systems, vol. 25, pp. 1097–1105, 2012.

[12] V. N. Vapnik, The Nature of Statistical Learning Theory, 2nd ed. New York, NY: Springer-Verlag, 2000.

[13] L. Breiman, "Random Forests," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.

[14] ETSI EN 302 663, "Intelligent Transport Systems (ITS); Access Layer Specification for Intelligent Transport Systems Operating in the 5 GHz Frequency Band," European Telecommunications Standards Institute, Sophia Antipolis, France, 2013.

[15] NS-3 Consortium, "NS-3 Network Simulator," [Online]. Available: https://www.nsnam.org, 2024.