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 – A Comprehensive Survey

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 -Vehicular Ad Hoc Networks (VANETs) are the communication backbone of modern Intelligent Transportation Systems (ITS) and Vehicle-to-Everything (V2X), enabling real-time communication among vehicles, roadside infrastructure, pedestrians, and cloud services. VANETs can improve traffic efficiency, autonomous driving, and road safety, but their wireless communication channels are highly susceptible to attacks, including jamming that can disrupt the network and affect availability. Traditional security solutions, such as cryptographic and rule-based intrusion detection systems, are unable to detect complex and adaptive jamming techniques in highly dynamic vehicular environments. In recent years, Artificial Intelligence (AI) and Machine Learning (ML) techniques have emerged, enabling intelligent attack identification and mitigation. Ensemble machine learning techniques have shown better performance by fusing multiple learning models to enhance detection accuracy, robustness, and generalization. This survey provides a thorough overview of the state of the art in AI-based jamming attack detection for VANETs, with a focus on ensemble learning. It analyzes various jamming attack models, machine learning algorithms, deep learning frameworks, and hybrid ensemble techniques for securing V2X communications. It also covers public datasets, evaluation criteria, implementation issues, and new research fields such as Explainable Artificial Intelligence (XAI), federated learning, edge intelligence, and V2X security in the context of 6G. Finally, the survey reveals gaps in current research and points to opportunities for future research and development of scalable, intelligent, and robust Secure-V2X systems to counter emerging jamming attacks in future vehicular networks.

Keywords--Secure-V2X, Vehicular Ad Hoc Networks (VANETs), Vehicle-to-Everything (V2X), Jamming Attacks, Cybersecurity, Intrusion Detection System (IDS), Artificial Intelligence (AI), Machine Learning (ML).

1. INTRODUCTION

Intelligent Transportation Systems (ITS) are rapidly evolving, transforming traditional transportation into highly connected, intelligent networks. Vehicular Ad Hoc Networks (VANETs) [1],[22] are a specialized type of Mobile Ad Hoc Network (MANET) that enable communication among vehicles and other entities, including Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), and Vehicle-to-Network (V2N) communications. These approaches are collectively known as vehicle-to-everything (V2X) and have a wide range of applications, including collision avoidance, traffic management, autonomous driving, emergency services, and infotainment.

As V2X technologies continue to grow, ensuring secure and reliable communication is critical. VANETs must operate in highly dynamic environments characterized by high node mobility, frequent topology changes, wireless channel interference, and strict latency requirements [9], [22]. These features render VANETs highly vulnerable to cyberattacks that can degrade communication performance and endanger road safety [3]. Jamming is one of the most serious security threats to network availability [4], [12]. Jamming attacks occur when a malicious actor deliberately transmits radio-frequency signals to disrupt normal communications, causing packet loss, increased latency, reduced throughput, and communication failures [8]. Traditional defense strategies against jamming attacks mainly include cryptographic, signal processing, and channel-hopping techniques, as well as rule-based intrusion detection systems [7].

These methods can provide some degree of protection, but they are difficult to implement in real-time driving conditions where intelligent and adaptive jamming is present. As attackers become more sophisticated, security solutions must also become more complex and adaptive, learning complex attack patterns and reacting dynamically to emerging threats [6]. Artificial Intelligence (AI) and Machine Learning (ML) have recently been proposed to improve the security of VANETs [7], [11].

Machine learning-powered intrusion detection systems (IDSs) can monitor network traffic, radio signal characteristics, and communication patterns to identify normal and malicious traffic [15], [16]. Many algorithms have been studied for detecting attacks in vehicular networks, including Decision Trees, Support Vector Machines (SVMs), Random Forests, K-Nearest Neighbors (KNNs), and Neural Networks [7], [24]. Recently, Deep Learning (DL) models, such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and Long Short-Term Memory (LSTM) networks, have shown improved performance in learning complex features from high-dimensional data [18], [20].

Ensemble machine learning has gained attention because it combines multiple classifiers, leveraging the strengths of each and their complementary nature [1], [17]. Ensemble methods, such as Random Forest, Gradient Boosting, AdaBoost, XGBoost, Voting Classifiers, and Stacking frameworks, are usually more accurate in detection, have fewer false alarms, and are more robust than individual models [23], [25]. These properties make ensemble learning well-suited to detecting more complex jamming attacks, especially in highly dynamic VANET environments [1], [5].

This survey aims to provide:

1) Analysis of existing artificial intelligence-based techniques for detecting jamming attacks in VANETs, with a specific focus on ensemble machine learning methods.
2) It presents a literature survey on VANET security, jamming attack classification, machine learning-based intrusion detection systems (IDSs), deep learning models, and ensemble frameworks.
3) Reviews typical datasets, performance assessment metrics, implementation issues, and research avenues.
4) The main goal is to provide researchers and practitioners with a unified vision of the latest progress and future potential of Secure-V2X systems, enabling them to create intelligent, adaptive, and resilient security solutions for next-generation vehicular networks.

2. LITERATURE SURVEY

2.1 AI-Driven Ensemble Classifier for Jamming Attack Based Detection

El-Shafai et al. [3] proposed one of the most comprehensive AI-based frameworks for detecting jamming attacks in VANETs. The study evaluated numerous machine learning and deep learning algorithms, including Random Forest (RF), Extra Trees (ET), CNN, LSTM, and hybrid architectures. The authors ultimately developed an ensemble model combining RF, ET, and CNN to leverage both statistical learning and deep feature extraction. Experimental results demonstrated exceptional detection accuracy exceeding 99%, outperforming individual classifiers. The paper emphasized that VANET communication is highly dynamic, making traditional threshold-based intrusion detection methods ineffective. By integrating ensemble learning with deep neural networks, the proposed model improved resilience against constant, random, and sweep jamming attacks. A major strength of this work is its comprehensive comparison among classical ML, DL, and ensemble approaches. However, the model was evaluated primarily in simulation environments, leaving questions about scalability and real-time deployment in large-scale V2X ecosystems. Nevertheless, this work represents a foundational reference for ensemble-based jamming detection research.

2.2 Optimal Attack or Malicious Activity Based Detection in VANET

Kawale et al. [4] investigated the use of ensemble machine learning techniques to detect malicious behavior in VANETs. The research focused on identifying abnormal node activity that degrades routing performance and communication reliability. The proposed framework combined multiple classifiers to improve attack detection accuracy while reducing computational overhead. The authors demonstrated that ensemble learning can effectively handle heterogeneous traffic patterns generated by highly mobile vehicular nodes. Unlike single-model approaches, the ensemble architecture provided greater robustness against false positives and false negatives. Although the paper addressed malicious activity broadly rather than jamming attacks specifically, its methodology highlights the advantages of combining multiple classifiers for security applications. The work establishes an important precedent for extending ensemble learning frameworks toward specialized jamming attack detection systems in Secure-V2X environments.

2.3 Traffic Coordination by Reducing Jamming Attackers in VANET

Santhi et al. [5] The study introduced a probabilistic Manhattan Grid Topology model to enhance communication reliability and traffic coordination in urban VANET scenarios. The authors analyzed how jamming attacks degrade packetdelivery ratio, throughput, and network stability. Their proposed approach improved routing efficiency and reduced communication disruption caused by malicious interference. A key contribution of this work is the demonstration that mobility-aware routing strategies can complement security mechanisms. However, the approach lacks intelligent attack classification and adaptive learning capabilities. Future Secure-V2X frameworks could integrate machine learning-based detection systems with such topology-aware mitigation mechanisms to achieve comprehensive defense against jamming attacks.

2.3 Machine Learning-Based Misbehavior Detection Systems

Boualouache and Engel [6]. This survey provides a comprehensive overview of machine learning applications in vehicular misbehavior detection systems for modern V2X networks. The authors classify existing solutions according to supervised, unsupervised, and reinforcement learning paradigms while examining their effectiveness against diverse attacks. The survey highlights that traditional cryptographic defenses alone cannot address sophisticated network-layer attacks and emphasizes the growing importance of intelligent detection mechanisms. The authors identify challenges such as dataset imbalance, concept drift, real-time processing requirements, and explain ability of AI models. Although jamming attacks are only one category within the broader threat landscape, the survey offers valuable insights into designing ML-based intrusion detection systems for future V2X architectures. The

recommendations regarding feature engineering and model validation are particularly relevant for ensemble learning-based jamming detection frameworks.

2.4 Machine Learning for Security in Vehicular Networks: A Comprehensive Survey

Talpur and Gurusamy [7] presented one of the earliest comprehensive reviews of machine learning techniques applied to vehicular network security. The survey categorized security threats into availability, confidentiality, integrity, and authentication attacks, highlighting jamming attacks as a significant threat to communication availability. The authors analyzed how machine learning algorithms such as SVM, Random Forest, Decision Trees, and Neural Networks can enhance attack detection capabilities. A notable contribution of the survey is its identification of research gaps related to feature selection, distributed learning, privacy preservation, and real-time implementation. The paper concludes that hybrid and ensemble models offer superior detection performance due to their ability to capture complex attack patterns. These findings strongly support the development of AI-driven ensemble frameworks for Secure-V2X environments.

2.5 A Taxonomical Analysis of Attacks and Solutions

Verma et al. [3] The paper systematically classified attacks into network-layer, application-layer, and physical-layer threats, identifying jamming as one of the most disruptive availability attacks. The authors reviewed existing cryptographic, trust-based, and machine learning-based countermeasures while discussing their limitations in highly dynamic vehicular environments. The survey emphasizes that future intelligent transportation systems require adaptive security solutions capable of learning evolving attack behaviors. Although the work does not specifically focus on ensemble learning, its taxonomy provides an essential conceptual framework for understanding where AI-driven jamming detection systems fit within the broader VANET security ecosystem.

2.6 A Survey on Jamming in VANET

Malebary and Xu [10] provided one of the earliest dedicated surveys focusing exclusively on jamming attacks in VANETs. The authors examined different categories of jammers, including constant, deceptive, random, and reactive jammers. They analyzed the impact of these attacks on communication performance metrics such as throughput, packet delivery ratio, and latency. Furthermore, the paper reviewed detection and mitigation strategies based on signal analysis, channel monitoring, and protocol-level defenses. While the surveyed techniques were largely non-AI-based, the work established the fundamental understanding of jamming behavior that later enabled machine learning researchers to develop intelligent detection systems. This survey remains an important historical reference for understanding the evolution from rule-based detection methods to modern AI-driven ensemble approaches.

3 ARCHITECTURE OF AI- DRIVEN JAMMING ATTACK DETECTION

3.1 V2X Communication Layer

Vehicles communicate with neighboring vehicles (V2V), roadside units (V2I), pedestrians (V2P), and cloud servers (V2N) using DSRC, IEEE 802.11p, C-V2X, or 5G technologies [2], [22]. These communications are vulnerable to jamming attacks that can disrupt safety-critical message delivery [8], [12].

3.2 Data Collection and Monitoring

Network monitoring agents continuously collect communication parameters such as:

1. Received Signal Strength Indicator (RSSI)
2. Signal-to-Noise Ratio (SNR)
3. Packet Delivery Ratio (PDR)
4. Packet Loss Rate
5. Throughput
6. End-to-End Delay
7. Channel Busy Ratio (CBR)

These metrics help identify abnormal wireless channel behavior.

3.3 Feature Extraction

The collected raw network data undergoes preprocessing to remove noise and redundancy. Relevant features are extracted and normalized to improve the performance of AI models.

3.4 AI-Based Detection Engine

Machine learning and deep learning algorithms analyze the extracted features to identify patterns associated with jamming attacks.

The AI engine learns:

1. Normal VANET communication behavior
2. Abnormal channel occupancy
3. Signal interference patterns
4. Packet dropping behavior
5. Intelligent adversarial jamming activities

3.5 Attack Classification

Once an anomaly is detected, the system classifies the type of jamming attack:

1. Constant Jamming
2. Random Jamming
3. Reactive Jamming
4. Deceptive Jamming
5. AI-Driven Adaptive Jamming

3.6 Security Decision Engine

The threat severity is evaluated using confidence scores generated by the AI model. Based on the detected attack type, appropriate countermeasures are selected.

3.7 Mitigation Layer

The system responds by:

1. Switching communication channels
2. Applying frequency hopping techniques
3. Re-routing packets through alternate paths
4. Adjusting transmission power
5. Issuing warnings to nearby vehicles and RSUs

3.8 Block chain-Based Trust Layer (Optional)

A block chain framework can be integrated to:

1. Authenticate participating vehicles
2. Prevent malicious node impersonation
3. Store attack logs securely
4. Maintain trust scores among vehicles

4 DEEP LEARNING IN JAMMING ATTACK DETECTION

The increasing deployment of Vehicular Ad Hoc Networks (VANETs) and Vehicle-to-Everything (V2X) communications has introduced significant security challenges, particularly jamming attacks that disrupt wireless communication channels [9], [10]. Traditional detection techniques often fail to identify intelligent and adaptive jammers due to the dynamic nature of vehicular environments [6]. Deep Learning (DL) has emerged as a promising solution because of its ability to automatically learn complex communication patterns from large-scale network data [11], [18]. Deep learning models can process high-dimensional VANET datasets and accurately distinguish between normal communication behavior and malicious jamming activities [1], [20].

4.1 CNN Based Jamming Attack detection

CNN is one of the most widely used deep learning architectures for wireless network security [21], [30]. It automatically extracts spatial features from communication data without requiring manual feature engineering [1].

Working Principle

1. Input VANET traffic features are transformed into matrices.
2. Convolution layers extract hidden attack patterns.
3. Pooling layers reduce dimensionality.
4. Fully connected layers perform classification.

Applications

1. Constant Jamming Detection
2. Random Jamming Detection
3. Deceptive Jamming Detection

Advantages

1. Automatic feature extraction
2. High classification accuracy
3. Reduced preprocessing requirements

Limitations

1. Limited capability for temporal sequence analysis
2. High computational cost for large datasets

4.2 Long Short-Term Memory (LSTM) Based Attack Detection

LSTM is a recurrent neural network architecture specifically designed to process sequential data [18]. VANET communications generate time-dependent traffic patterns, making LSTM highly effective for jamming attack detection [1], [20].

Working Principle

1. Captures long-term dependencies in communication data.
2. Maintains memory cells for historical information.
3. Learns normal and abnormal communication behavior over time.

Applications

1. Reactive Jamming Detection
2. Intelligent Jamming Detection
3. Adaptive Jamming Detection

Advantages

1. Excellent temporal learning capability
2. High detection accuracy for dynamic attacks
3. Effective in high-mobility environments

Limitations

1. Long training time
2. Computationally intensive

4.3 Gated Recurrent Unit (GRU) Based Detection

GRU is a simplified version of LSTM that uses fewer parameters while maintaining similar performance [18].

Working Principle

1. Utilizes update and reset gates.
2. Captures temporal communication dependencies.
3. Processes VANET traffic sequences efficiently.

Applications

1. Real-Time Jamming Detection
2. Adaptive Attack Classification

Advantages

1. Faster training than LSTM
2. Lower computational complexity
3. Suitable for edge devices

Limitations

1. Slightly lower learning capability for very complex patterns

4.4 Auto encoder (AE) Based Detection

Auto encoders are unsupervised deep learning models used for anomaly detection [11].

Working Principle

1. Learn normal communication behavior.
2. Compress input data into latent representations.
3. Reconstruct original inputs.
4. High reconstruction error indicates anomalies.

Applications

1. Unknown Attack Detection
2. Zero-Day Jamming Detection

Advantages

1. No labeled data required
2. Effective for anomaly detection

Limitations

1. Sensitive to noise
2. Reconstruction threshold selection is challenging

4.5 Deep Auto encoder (DAE) Based Detection

Deep Auto encoders contain multiple hidden layers and can learn more complex representations than standard auto encoders.

Applications

1. Intelligent Jamming Detection.
2. Advanced Threat Identification.

Advantages

1. Better feature learning.
2. Improved anomaly detection capability.

Limitations

1. Higher training complexity.

5 SIMILARITY MATCHING TECHNIQUES IN AI-DRIVEN JAMMING ATTACK DETECTION

Similarity matching detection is the fundamental operation that determines whether a given keyword representation compare current network behavior with normal or attack patterns. These techniques help machine learning and deep learning models identify anomalies caused by jamming attacks.

5.1 Euclidean Distance Similarity matching

Euclidean distance is a distance function that calculates the distance between two vectors of features using the nearest straight line.

$$d(x,y) = \sqrt{\sum_{i=1}^{n}(xi - yi)} \quad \textbf{(5.1)}$$

Application in VANETs

Normal traffic patterns are used for comparison with the current RSSI, SINR, PDR and throughput.

A larger distance means that there is abnormal behavior, which can be related to jamming.

Advantages

1. Implementation is simple.
2. Efficiently computational.

Limitations

1. Responsive to the scaling of features
2. A drop in performance for high dimensional data

5.2 Cosine Similarity matching

Calculate the angle between two feature vectors.

$$\cos(x,y) = \frac{x \cdot y}{||x|| \times ||y||} \quad \textbf{(5.2)}$$

Application

1. Used to compare network traffic signatures.
2. Identifies similarities in patterns irrespective of differences in the size.

Advantages

1. It works best for high-dimensional datasets. It is useful for datasets with high dimensions.
2. More tolerant of the data size

Limitations

1. Fails to consider absolute feature values.
2. Does not pay attention to absolute feature values.

5.3 Jaccard Similarity matching

Jaccard similarity calculates overlaps between two sets.

$$(A, B) = \frac{(A \cap B)}{(A \cup B)} \quad \textbf{(5.3)}$$

Application

1. Compare the pattern of packet transmissions.
2. Useful for network features with two values.

Advantages

1. Applies to categorical data.
2. Interpretation is easy.

Limitations

1. Not suitable for continuous valued VANET metrics

5.4 Pearson Correlation Similarity matching

Calculate linear relationship between network parameter.

$$r = \frac{\sum(xi-\bar{x})(yi-\bar{y})}{\sqrt{\sum(xi-\bar{x})^2 \sum(yi-\bar{y})^2}} \quad \textbf{(5.4)}$$

Application

1. Discuss the correlation between RSSI and PDR.
2. Detect jamming or deviation resulting from it.

Advantages

1. Captures statistical dependency.

Limitations

1. Only deals with linear relations.

5.5 Dynamic Time Warping (DTW)

Compares time sequences, showing differing time shifts.

Application

1. Examine movement of vehicles.
2. Make comparisons between the communication styles of different time periods.

Advantages

1. For time-series VANET data Effective from 1995 onwards.
2. Handles sequence misalignment.

Limitations

1. Higher computational complexity.

5.6 K-Nearest Neighbor (KNN) Similarity

Applies distance similarity to sort observations.

Application

1. Correlate unknown traffic samples to known attack samples.
2. Identify and detect constant, deceptive, random and reactive jamming attacks.

Advantages

1. Interpretable and simple.

Limitations

1. Not efficient when dealing with a large set of data.

5.7 Comparative Summary of Similarity Matching Techniques

Table 1 shows the comparative summary of similarity matching techniques

Table 1 SIMILARITY MATCHING TECHNIQUES

Matching Type	Data type	AI integration	Accuracy	Complexity
Euclidean Distance	Numerical	ML	Medium	Low
Cosine Similarity	High-dimensional	ML/DL	High	Low
Jaccard Similarity	Binary	ML	Medium	Low
Pearson Correlation	Statistical	ML	Medium	Low
DTW	Time-Series	Ml/DL	High	High
KNN Similarity	Numerical	ML	High	Medium

6 CHALLENGES AND OPEN RESEARCH PROBLEMS IN AI-DRIVEN JAMMING ATTACK DETECTION IN VANETS

These networks facilitate communications between cars, roadside units (RSUs), people and cloud-based systems for safety purposes. VANETs are, however, very susceptible to jamming attacks whose goal is to interfere with wireless communication channels in order to disrupt data transmission. In recent times, Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) techniques have been integrated with the efforts to detect and counteract such attacks. While these studies have shown promising results, there are still several technical challenges and unsolved research issues that hinder the implementation of accurate jamming detection methods in real-world VANET scenarios.

6.1 Dynamic and highly mobile network topology

VANETs are distinguished by rapidly changing topologies of vehicles' mobility as opposed to conventional wireless networks [9], [10]. Constantly entering and exiting in communication ranges leads to frequent change of connection states and communication patterns [5].

Impact on AI Models

Generally, AI models are trained with data that is assumed to have a similar distribution to the data they will be tested on. However, in VANETs:

1. The density of traffic varies over time.
2. There is a wide range of vehicle speeds.
3. Communication links are short-lived.

4. There is a difference between urban and highway conditions.

In this way, models that are well trained for one context can suffer from significant drop in performance when they are applied to other contexts.

6.2 Mobile deep learning architectures

The lack of standardized real-world data sets is another issue is the lack of standardized real-world data sets [6], [19].

The majority of research on AI jamming detection systems have been conducted using simulation software including [26], [27]:

1. SUMO
2. NS-3
3. OMNeT++
4. Veins

While simulations offer flexibility, these are not necessarily representative of real world channel characteristics and attacker behavior.

1. Impact
2. Limited model generalization.
3. Struggles with comparing and contrasting research methods.
4. Overestimated performance results.

6.3 Intelligent and Adaptive AI-Powered Jammers

Traditional jammers broadcast either continuously or at intervals [8], [12]. Attacks by emerging attackers can take advantage of AI and RL to learn the best attack strategy [6].

Such jammers can:

1. Observe network behavior.
2. Forecast channel access patterns.
3. Adjust transmission power to change.Adapt transmission power dynamically.
4. Avoid detection mechanisms.

Impact

Static AI classifiers are ineffective against an adaptive attacker.

6.4 The detection of Zero-Day Jamming Attacks is not feasible.

For supervised ML/ DL, attack samples must be labeled during the training phase [7], [11].

However, future attackers may generate previously unseen attack patterns.

Impact

It is because the traditional classifiers cannot recognize attacks not included in the training data.

6.5 Unsupervised anomaly detection

The high False Positive and False Negative rate.Several network congestion effects such as fading, shadowing and interference may have similar symptoms to jamming [4], [5].

1. Examples include:
2. Increased packet loss.
3. Reduced throughput.
4. Low SINR values.

The term attack is used for normal communication conditions.

False Negatives Real attacks cannot be detected. These cases are serious enough to have a significant impact on road safety.

6.6 Resource Constraints in Vehicular Devices

The area of limited availability is onboard Units (OBUs):

1. CPU power.
2. Memory.
3. Energy resources.

Deep learning models can be computationally intensive.

It is hard to implement in practice.

7 OPEN RESEARCH PROBLEMS IS JAMMING ATTACK DETECTION

Based on current literature [1], [2], [9], [11], the major open research problem includes:

7.1 Generalization of different traffic environment

Many AI models can be very accurate on the exact data set or simulator they were trained on.

Why it is difficult?

The conditions of VANET vary drastically over urban roads, highways, rural areas, weather conditions, vehicle densities and radio environments. Models trained in one environment often fail in another because the statistical distribution of the data changes (domain shift).

Open research question

How to enable AI models to achieve high detection performance in heterogeneous and unseen environments?

Possible directions:

1. Transfer learning and domain adaptation.
2. Meta-Learning for Fast Adaptation.
3. Constantly-Learning online.
4. Benchmarks for multi-environment training.

7.2 Zero-Day and Unknown Jammer Attack Detection

Most of the existing methods are based on supervised learning with labeled attack classes.

Why it is difficult?

Future attackers may exhibit new jamming behaviors that are dissimilar to any training example.

Open research question

How can a system discover new jamming attacks without having seen labeled examples before?

Possible directions:

1. Anomaly detection, unsupervised.
2. Auto encoders and variant-based Auto-Encoders.
3. Self-supervised representation learning.
4. Open set recognition architectures.

7.3 AI-Enabled Adaptive Jammer Detection

Emerging attackers can use reinforcement learning to evolve their strategy over time.

Why it is difficult?

The attacker dynamically changes the transmission power, timing, and channel usage. Static signatures are no longer effective.

Open problem in research

And if the adversaries also learn and adapt, how do AI defenses keep up?

Possible directions

1. Adversarial RL.
2. Game-Theoretic AI Security Models
3. Co-evolutionary attacker-defender training.
4. Learning policies and adaptive holding.

7.4 Real-Time Detection with Tight Latency Constraints

Accurate, but also computationally expensive, are standard models for deep learning.

Why it is difficult?

Decisions for safety critical V2X applications may be needed in milliseconds. Large models have higher inference latency.

Open problem in research

Trade-off between the detection accuracy and ultra-low latency requirements

Possible directions:

1. Small Neural Networks and Tiny ML.
2. Model pruning & quantization.
3. Edge AI Deployment Neural Architecture Search with Hardware Awareness.

7.5 Adversarial Machine Learning Attack Resistance

Features such as RSSI, SINR, or traffic patterns can be manipulated by attackers to deceive AI models.

Why it is difficult?

Even a small perturbation can cause misclassification.

Open problem in research

How can AI-based jamming detectors stay robust when the AI model is under attack?

Possible directions:

1. Adversarial Training
2. Proven robust methods.
3. Secure future extraction.

7.6 Explainable and Trustworthy AI for VANET Security

The problem with AI models Deep learning models often act like boxes that we cannot understand.

The need for transparency Network operators want to know why an alert was triggered, in systems where safety is crucial.

One of the challenges is:

How can AI explain its decisions when it comes to detecting jamming in a way that makes sense to humans?

Some possible ways to tackle this include:

1. Using SHAP and LIME analysis to understand AI decisions.
2. Creating AI models that can explain themselves using attention mechanisms.
3. Applying inference to improve network security.
4. Involving humans in security systems to ensure they are trustworthy.

7.7 Lack of Real-World Datasets

Most research studies use simulated data from tools like NS-3, OMNeT++, SUMO or Veins.

Life vehicular radio channels are affected by many factors like fading, shadowing, interference and hardware issues that are hard to replicate accurately in simulations.

The question remains:

How can we create and share datasets that everyone can use as a benchmark?

Some potential solutions are:

1. Conducting large-scale measurements in the field.
2. Collecting data from cities and countries.
3. Agreeing on protocols for labeling data.

8 APPLICATIONS OF AI-DRIVEN JAMMING ATTACK DETECTION

8.1 Road Safety and Collision Avoidance Systems

VANETs allow vehicles to send important safety messages such as:

1. Emergency braking alerts
2. Collision warnings
3. Lane change notifications
4. Blind spot alerts

Jamming attacks can block or delay these messages.

Role of AI Detection

AI continuously checks communication parameters like RSSI, SINR, packet loss, and transmission delays to spot interference.

Benefits

1. Prevents loss of safety messages.
2. Reduces accident risks.
3. Improves driver and passenger safety.

8.2 Autonomous and Connected Vehicles

Autonomous Vehicle

Self-driving vehicles depend on V2V and V2I communication for:

1. Navigation
2. Cooperative driving
3. Traffic awareness
4. Obstacle detection

Role of AI Detection

Detect harmful jamming attack attempts that could disrupt sensor sharing and communication.

Benefits

1. Increases reliability of autonomous driving.
2. Aids safe decision-making.
3. Protects vehicle coordination.

8.3 Vehicle-to-Vehicle (V2V) Communication Security

V2V communication allows vehicles to exchange information directly with nearby vehicles.

Examples include:

1. Speed information
2. Traffic updates
3. Hazard notifications

Role of AI Detection

Identifies unusual communication patterns and separates jamming attacks from normal interference.

Benefits

1. Secure vehicle cooperation.
2. Reliable information sharing.
3. Better traffic management.

8.4 Vehicle-to-Infrastructure (V2I) Communication Protection

Vehicles communicate with roadside units (RSUs), traffic signals, and transportation infrastructure.

Role of AI Detection

Monitor infrastructure communication channels to find malicious interference that targets RSUs.

Benefits

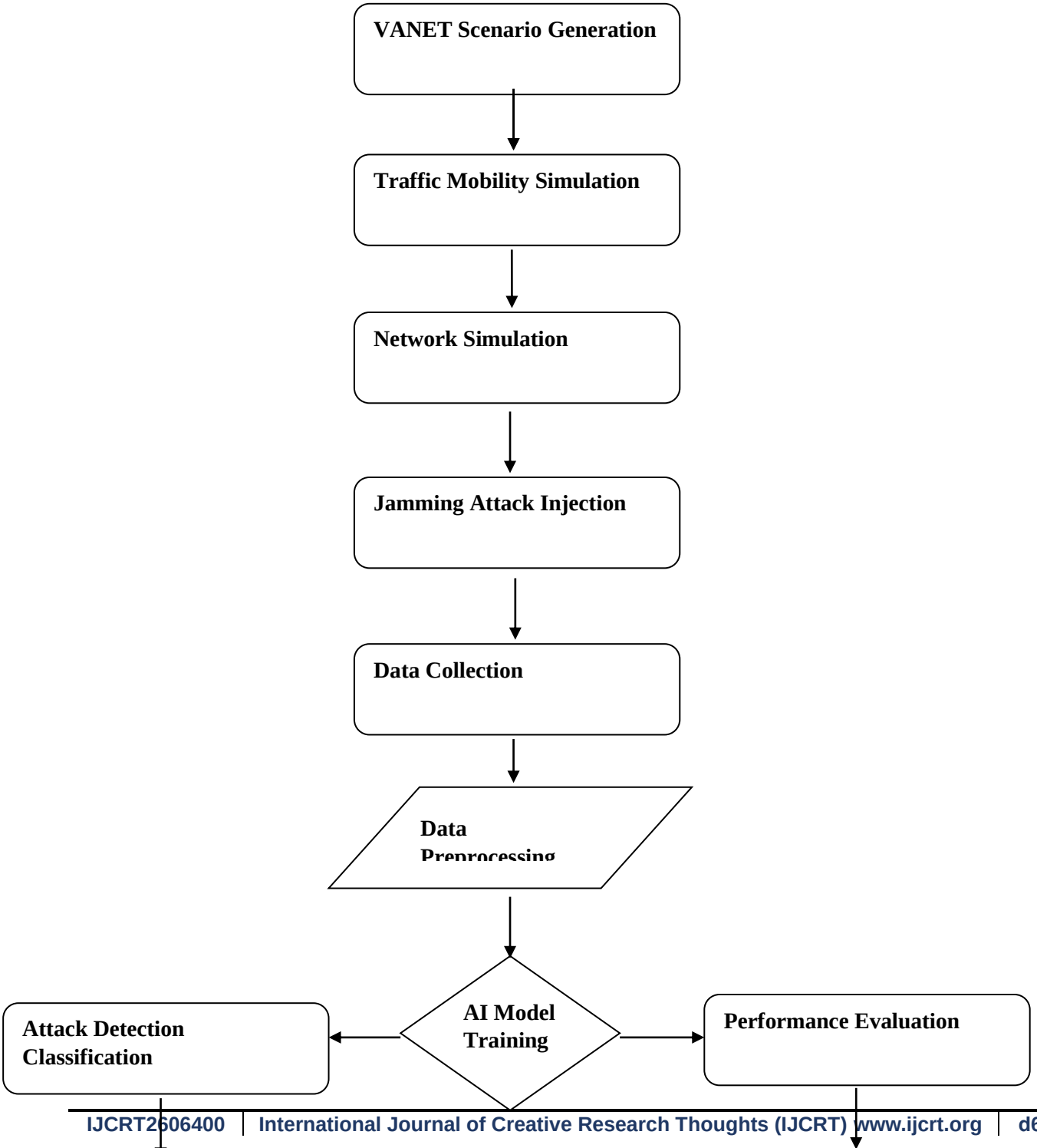
1. Reliable traffic signal coordination.
2. Improved infrastructure availability.
3. Better transportation efficiency.

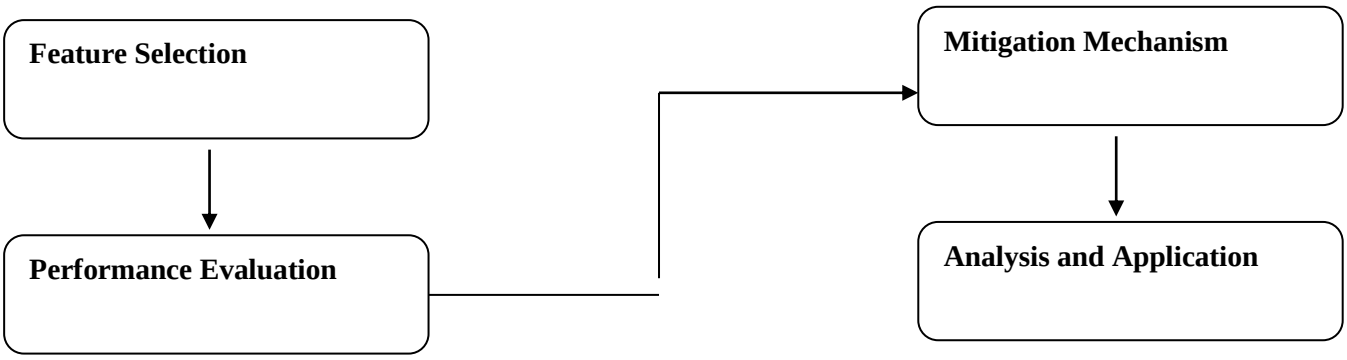
9 FULL IMPLEMENTATION METHODOLOFY USING VANETS IN AI-DRIVEN JAMMING ATTACK DETECTION

The proposed method seeks to create an AI-driven framework for spotting and classifying jamming attacks in Vehicular Ad Hoc Networks (VANETs). The framework combines vehicular mobility simulation, network simulation, data generation, feature engineering, machine learning, and deep learning for detection and attack prevention.

9.1 Methodology Framework

The full processing chain is illustrated below:





9.2 Tools and Software used

Table 2 provides the tools used to implement project.

Table 2 TOOLS USED TO IMPLEMENT PROJECT

Tool	**Purpose**
SUMO	Vehicle mobility generation
NS-3	VANET network simulation
OMNeT++	Communication simulation
Veins	Integration of SUMO and OMNeT++
Python	Data processing and AI implementation
Tensor Flow	Deep learning model development
Scikit-learn	Machine learning algorithms
Jupyter Notebook	Experiment execution
Pandas	Dataset handling
NumPy	Mathematical operations
Matplotlib	Graph generation
Seaborn	Performance visualization

9.3 Dataset Description: VANETs

The VANET (Vehicular Ad Hoc Network) dataset captures how vehicles and roadside infrastructure communicate in Intelligent Transportation Systems (ITS). It includes network, mobility, and physical-layer features collected from Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications under normal and attack conditions [9]. Researchers use this dataset to train and evaluate Machine Learning (ML) and Deep Learning (DL) models that detect jamming attacks, intrusion attempts, and communication issues in VANET settings [1], [24]. Typically, the dataset is generated using vehicular mobility simulators like SUMO and network simulators such as NS-3 or OMNeT++ [26], [27]. These tools mimic realistic traffic conditions, wireless communication, vehicle movement patterns, and attack scenarios. Each instance of the dataset represents a communication event and includes various network parameters that describe the state of the vehicular network at a specific moment.

9.3.1 Dataset Characteristics

Table 3 provides the Dataset Characteristics used in project.

Table 3 DATASET CHARACTERISTICS

Attribute	**Description**
Dataset Type	Supervised Classification Dataset
Domain	Vehicular Ad Hoc Networks (VANETs)
Communication Type	V2V and V2I
Network Standard	IEEE 802.11p / DSRC
Frequency Band	5.9 GHz
Traffic Scenarios	Urban, Highway, Rural
Vehicle Density	20-300 Vehicles
Attack Classes	Normal, Constant, Random, Reactive, Deceptive, Intelligent Jammer
Data Format	CSV
Learning Type	Multi-class classification

10 FUTURE SCOPES

10.1 Introducing Federated Learning for Privacy-Preserving Detection

AI jamming detection systems need centralized datasets that enlist the communication data of all vehicles. This system is inefficient due to the overhead of communication data and the violation of data privacy [11]. Future VANET security systems can integrate Federated Learning (FL) to allow the distributed training of AI models at the vehicle level, unlike the centralized model that requires the distribution of data [6]. In this case, only the model parameters are communicated, which increases detection accuracy while preserving data privacy. Broad-based participation of vehicles that span large geographical spaces and a wide network of jamming detection systems may be possible with the integration of Federated Learning, which also introduces the benefit of real-time response to changing jamming attacks [1].

10.2 Integration of XAI for Security Decision Frameworks

Deep learning models for detecting jamming attacks are largely black-box systems [6], [11]. As a result, there is little understanding of communication events that are classified as attacks. Future systems should integrate Explainable AI (XAI) approaches that promote frameworks for clear understanding and justification of decisions [6]. Other approaches in XAI may be helpful in evaluating the contribution of different features and in building confidence in AI-enabled security systems. XAI will be especially critical for the systems of autonomous vehicles [1].

10.3 Detection of Unknown and Zero-Day Jamming Attacks

Current supervised learning frameworks can only classify known attack patterns that were included in training [7], [24]. Future attackers that are more sophisticated may easily evade detection systems by employing jamming attacks that are unknown and unseen [11]. Research in this area should focus on the detection of Zero-Day attacks and unknown jamming attacks using unsupervised learning and self-supervised learning frameworks [6]. An approach that integrates Auto encoders, a Variation Auto encoder (VAE), Generative Adversarial Networks (GANs), or anomaly detection may be useful [1].

10.4 Graph Neural Networks for Topology-Aware Security

Most AI models at present analyze communication logs in isolation and attempt no consideration of the dynamic network topology of the VANETs [1], [6]. Since vehicular networks intuitively form a graph of vehicles and roadside units and their communication links, Graph Neural Networks (GNNs) and Graph Attention Networks (GATs) may be used in the future to analyze complex relationships in the space-time continuum [11]. GNN-based methods may improve the accuracy of the detection of jamming attacks by learning the communication interdependencies and detecting abnormal changes in the network topology.

10.5 Deep Reinforcement Learning-Based Adaptive Defense Mechanisms

Most of the existing solutions focus on the detection of the attack, while the mitigation of the attack is, for the most part, static. A significant portion of the future security frameworks for VANETs may be based on Deep Reinforcement Learning (DRL), whereby the DRL agents may learn defense mechanisms. Examples of such mechanisms may include strategies such as defense on the fly in the form of hopping, adaptive power control, route changes, and cooperative communication, all of which may constitute intelligent defense.

10.6 Edge AI and Mobile Edge Computing Integration

Jamming detection systems based on the cloud may be provided with communication lags due to bandwidth constraints [11]. Future architectures for VANETs may integrate Edge AI and Mobile Edge Computing (MEC) [1]. AI models may be implemented on roadside units and edge servers. Detection that is performed on the edge may reduce latency, facilitate the real-time security of the detection system, improve the resource system, and enable the AI models for use in crowded and complex vehicular environments. As a result, research in the area may focus on the development of efficient and lightweight AI models [6].

11 CONCLUSION

Advanced ITs, VANETs, and V2X technologies are proving invaluable in making transport systems safer and more efficient [9], [22]. The advancements being made in automation and self-driving vehicles can also be attributed to these technologies [2]. The wireless communication channels used by VANETs are open and therefore susceptible to unauthorized intrusion, manipulation, and interference [7], [14]. The absence of security measures to protect against these ‘jamming attacks’ can result in the safety of autonomous transport systems being compromised [8], [12]. For these reasons, the challenge of detecting jamming attacks is one of the most pressing issues concerning the safety of systems that integrate connected and autonomous vehicles [1], [4].

Artificial Intelligence and its application in detecting jamming attacks in VANETs were the main focus of the survey. The survey traced the history of jamming attacks and their intelligence. The survey examined various attack models, and how Artificial Intelligence can provide security to vehicular communications. The survey also examined machine learning and deep learning technologies and their advancements, and improvements over traditional, rule-based, and signature-based security solutions. Techniques that incorporate decision trees, random forests, support vector machines, k-nearest neighbors, and xgboost were examined, as well as various forms of convolutional neural networks(CNN), long short-term memory networks, gated recurrent units, auto encoders, and transformers. The importance of employing multi-layer features to enhance the detection of complex jamming attacks is also identified and discussed in the survey.

The survey also focused on standard VANET datasets, simulation environments, benchmarking frameworks, evaluation metrics, and implementation techniques. AI-based detection techniques were evaluated with metrics including Accuracy, Precision, Recall, F1 score, ROC-AUC, Matthews Correlation Coefficient (MCC), Packet Delivery Ratio (PDR), Throughput, End-to-End Delay, Packet Loss Ratio (PLR), and Signal-to-Interference-plus-Noise Ratio (SINR). It was found that even though most AI models achieve high detection rates in simulation; their performance is poor in highly dynamic vehicular environments, novel attack patterns, and real-world situations.

The survey highlighted several challenges and open research issues that restrict the widespread use of AI-driven jamming detection systems. These challenges include real-world benchmark datasets, detection of zero-day and adaptive AI jammers, computational complexity, jamming attacks and adversarial machine learning attacks, the black-box nature of deep learning, privacy issues related to federated learning, and the ability to meet real-time requirements in highly mobile environments. Moreover, the continuing evolution of 5G and 6G V2X networks will introduce new security requirements that detection systems will be unable to meet.

12 REFERENCES

1] W. El-Shafai et al., "AI-Driven Ensemble Classifier for Jamming Attack Detection in VANETs to Enhance Security in Smart Cities," IEEE Access, vol. 13, 2025.

[2] IEEE Computer Society, "IEEE Standard for Information technology--Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," IEEE 802.11p Standard Documentation, 2024.

[3] A. Alalhesn et al., "A review of security attacks and intrusion detection in the vehicular ad hoc network," Computers & Security, vol. 118, 2023.

[4] S. M. A. Oteafy et al., "Jamming attack detection in a pair of RF communicating vehicles using received signal anomalies," IEEE Transactions on Vehicular Technology, 2022.

[5] K. Grover et al., "Machine Learning-Based Jamming Detection for Safety Applications in Vehicular Networks: Individual Detection," IEEE Internet of Things Journal, 2021.

[6] M. M. N. Toor et al., "RF Jamming Classification using Relative Speed and Signal Processing in VANETs," IEEE Transactions on Intelligent Transportation Systems, 2022.

[7] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[8] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc), pp. 46-57, 2005.

[9] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANET security challenges and solutions: A survey," Vehicular Communications, vol. 7, pp. 7-20, 2017.

[10] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," Telecommunication Systems, vol. 50, no. 4, pp. 217-241, 2012.

[11] M. A. Al-Garadi et al., "A survey of machine and deep learning methods for internet of things (IoT) security," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, 2020.

[12] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," IEEE Communications Surveys & Tutorials, vol. 13, no. 2, pp. 245-257, 2010.

[13] A. Boualouache, S. M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 770-790, 2017.

[14] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," Vehicular Communications, vol. 16, pp. 45-61, 2019.

[15] T. O. Olasupo, "Intrusion detection systems for vehicular ad hoc networks (VANETs): A review," Journal of Network and Computer Applications, vol. 144, pp. 106-125, 2019.

[16] Y. Maleh, "Machine learning techniques for intrusion detection in VANETs," Security and Privacy in Smart Sensor Networks, pp. 150-175, 2018.

[17] S. A. H. Baza et al., "Detecting jamming attacks in autonomous vehicles utilizing ensemble learning," IEEE International Conference on Communications (ICC), pp. 1-6, 2021.

[18] M. H. Ali et al., "An intelligent intrusion detection system for vehicular ad hoc networks using deep learning," IEEE Access, vol. 8, pp. 122851-122864, 2020.

[19] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 184-208, 2015.

[20] B. Liang, J. Zheng, X. Chen, and M. Zeng, "Deep learning-based jamming detection for 5G-V2X communications," IEEE Transactions on Vehicular Technology, vol. 69, no. 9, pp. 9508-9521, 2020.

[21] L. Li, J. Wu, L. Chen, and C. Liu, "A Convolutional Neural Network-based approach for RF jamming detection in V2I communications," IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5183-5194, 2019.

[22] F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A security and privacy review of VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985-2996, 2015.

[23] Y. Zhou, Y. Wang, Y. Liu, and S. Li, "An ensemble learning approach for anomaly detection in vehicular networks," Computer Networks, vol. 178, 107335, 2020.

[24] A. K. Singh and R. S. Singh, "Machine learning-based intrusion detection systems for VANETs: A comprehensive review," Wireless Personal Communications, vol. 115, no. 2, pp. 1321-1348, 2020.

[25] Z. MacHardy, A. Vasan, and M. R. Lyu, "Evaluating the performance of SVM and Random Forest for jamming classification," Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6, 2018.

[26] SUMO Documentation, "Simulation of Urban MObility (SUMO)," Eclipse Foundation, Accessed: Jun. 2025. [Online]. Available: https://sumo.dlr.de/

[27] NS-3 Network Simulator, "NS-3 Documentation and Tutorials," NS-3 Consortium, 2025. [Online]. Available: https://www.nsnam.org/

[28] A. S. Rostami et al., "A novel anomaly-based intrusion detection system for VANETs using Support Vector Machines," Vehicular Communications, vol. 22, 100207, 2020.

[29] T. R. Gopal and S. K. Singh, "Analysis of Random Forest algorithm for detecting DoS attacks in VANET," International Journal of Computer Applications, vol. 181, no. 43, pp. 33-38, 2019.

[30] R. Sharma and B. Singh, "Spectrogram-based feature extraction for RF jamming detection using Convolutional Neural Networks," IEEE Sensors Journal, vol. 21, no. 14, pp. 16212-16220, 2021.