IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

NOVA: A hybrid detection framework for misbehavior in vehicular networks

Afrah Abood Abdul Kadhim Kadhim[1], Zainab Marid Alzamili[2], Mahmood A. Al-Shareeda[3,4], Mohammed Amin Almaiah[5*], Rami Shehab[6]

[1]Electrical Engineering Techniques, Basra Engineering Technical Collage, Southern Technical University, Basra, Iraq.
2 Education Directorate of Thi-Qar, Ministry of Education, Iraq.
[3]Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, Iraq.
[4]Department of Communication Engineering, Iraq University College (IUC), Basra, Iraq.
[5]King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan
[6]Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa 31982, Saudi Arabia

Corresponding author: Mohammed Amin Almaiah (*Email: m_almaiah@ju.edu.jo*)

Abstract

Vehicular networks, comprising communication between two vehicles (Vehicle-to-Vehicle, V2V) and communication between a vehicle and its environment (Vehicle-to-Everything, V2X), are critical in improving road safety, traffic management, and smart transport systems. However, the interconnectivity of these systems makes them susceptible to various security threats, including Denial-of-Service (DoS), Sybil, and spoofing attacks. Common Intrusion Detection Systems (IDS) have significant limitations in their approaches, such as static reputation scoring to match attacks, small attack scope detection, and limited scalability in high node density. In this paper, we propose the hybrid detection framework, NOVA, by utilizing both statistical anomaly detection and machine learning techniques to ensure a comprehensive security solution for vehicular networks. Recognizing the importance of real-time adaptation to the dynamic nature of peer-to-peer networks, NOVA implements a sophisticated reputation management system that scales to ever-changing environments. Additionally, a trusted node mechanism is integrated, securing critical infrastructure nodes through cryptographic authentication and communication prioritization. This allows NOVA to operate in a distributed architecture with the support of vehicular cloud integration for handling networks with high density while guaranteeing performance. NOVA outperforms all existing schemes with a high detection rate (around 97% average for multiple attack types), lower false positive and false negative rates, and stable performance scalability up to 500 nodes, as extensive simulation results have shown. Comparisons against state-of-the-art systems demonstrate how NOVA performs better in terms of accuracy and scalability, establishing NOVA as a promising solution to facilitate secure intelligent transportation networks in the future.

Keywords: Detection Framework, Intrusion Detection Systems, NOVA, Misbehavior Detection, Vehicular Networks.

DOI: 10.53894/ijirss.v8i2.5521
Funding: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU 250987).
History: Received: 6 February 2025 / **Revised:** 10 March 2025 / **Accepted:** 14 March 2025 / **Published:** 20 March 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

Most vehicular network developments today are focused on related infrastructures in Vehicle-to-Vehicle (V2V) and Vehicle-to-Everything (V2X) communications, drastically improving modern transportation systems, traffic control, and infotainment continuity [1, 2]. However, the interlinkage of these networks makes them susceptible to a variety of security attacks such as Denial-of-Service (DoS) [3, 4], Sybil [5], and spoofing attacks [6]. Such attacks can disrupt communication, compromise safety-critical information, and cause serious accidents handled by traffic applications [7-9].

Traditional Intrusion Detection Systems (IDS) for networks of vehicles (or vehicular ad-hoc networks, VANETs) tend to target specific attacks, usually in a centralized architecture and by using static thresholds [10, 11]. On the MAC layer, for example, DAMASCO [12] monitors DoS attacks with statistical outlier detection; however, its inflexibility makes it less useful for more complex attacks such as Sybil attacks. Systems like the ones proposed by Vinita and Vetriselvi [13] have difficulty scaling with a high density of nodes, causing latency in detection time and lower accuracy in real-time. These challenges point to a fundamental requirement for a scalable, adaptive, and multi-layered security solution [14, 15].

To address these limitations, we present NOVA, a novel hybrid detection framework that can cover all types of attacks in vehicular networks. NOVA uses statistical outlier detection and machine learning techniques to accurately manage a wide variety of attack types. NOVA incorporates dynamic reputation management that allows it to adjust to changes in the network as it continuously updates each node's reputation based on live behaviors, unlike existing systems. Towards a centralized management approach, the trusted node mechanism also maintains continuous data communication in support of high-priority nodes, that is, emergency vehicles, by adopting identification and priority handling based on cryptographic authentication. In summary, the contributions of this paper are:

Hybrid Detection Framework: An approach based on the combination of statistical model-based anomaly detection with a machine learning approach to improve detection for more than one type of attack; these include DoS maximum, Sybil, and spoofing attacks.

Dynamic Reputation Management System: An adaptive reputation mechanism that is incrementally updated according to real-time node actions to obtain fewer false positives and allow for trust recovery based on changing network conditions.

Trusted Node Mechanism: A strong cryptographic framework to validate critical infrastructure entity identity and reallocate traffic to enable it in high-traffic or emergency situations.

Architecture of Scalable Distributed System: Design against vehicular cloud services for elastic scaling for real-time low latency detection over large-scale and high-density vehicular networks.

The rest of this paper is organized as follows: In Section 2, we review the related work and point out the requirements needed in the IDS solutions. The architecture and detection mechanisms of the NOVA framework are presented in Section 3. The experimental methodology is detailed in Section 4, and the evaluation results and comparison are presented in Section 5. Section 6 concludes this paper.

2. Related Work

In recent years, the explosive growth of vehicular networks has enriched security capabilities for connected cars, vulnerable to provide Vehicle-to-Vehicle (V2V) and Vehicle-to-Everything (V2X) communication by various IDS, but also prone to attacks [16-21]. Various works have suggested remedies in terms of improved misbehavior detection, anomaly detection, and enhanced robustness of the system. Here are some recent works in this direction:

Shams, et al. [22] effectively emphasize the importance of security in VANET and the proposed packet intrusion detection system in the context of attack detection using CAFECNN. Above all, it shows resourceful motivation, methodology (data collection, synthetic testing, CNN-based model), and results.

Zaidi, et al. [23] present the design and evaluation of an intrusion detection system (IDS) for VANETs, detecting rogue and false information attacks. It emphasizes the application of statistical methods, Monte Carlo simulations, and data exploration. However, it lacks information on important performance metrics and improvements.

Chakraborty, et al. [24] clearly establish the need for securing VANETs via node credibility assessment followed by the contribution of a new machine-based learning security scheme. The other detail focuses on the use of game theory encryption and fuzzy rule-based neural network integration.

Hamdan, et al. [25] present an overview of the Sybil attack on VANETs and a hybrid detection algorithm of P2DAP and footprint methods. It does a good job of explaining the performance conditions for each method and gives mention of implementation with the ns2, SUMO, and MOVE tools.

Vinita and Vetriselvi [13] present the mitigation of Sybil attacks with 6G-enabled IoV, federated learning, and vehicular fog computing. This approach not only improves accuracy in detection but also reduces latency and on-board vehicle selection with FLEMDS framework integrated fuzzy logic-based vehicle selection. It would be further enhanced by the inclusion of key experimental results (87% detection accuracy).

Luong, et al. [26] well explain VANET challenges, including flooding attacks, and also provide an overview of the proposed MFFDA and FAPDRP solution. It describes major contributions related to tracking behavioral history, median filtering, and a new routing protocol. The findings suggest enhanced detection accuracy (98.5%) and performance superior to AODV.

Paranjothi and Atiquzzaman [27] reason why rogue nodes are the problem in VANETs and propose the F–RouND framework, which uses fog computing, to effectively detect rogue nodes. Performance gains in the order of 45% and 36% lower processing latencies and FPR respectively are consistently emphasized.

Valentini, et al. [12] provide an overview of the challenges presented by Intelligent Transportation Systems (ITS), particularly (VANETs), and note their vulnerability to denial-of-service attacks. The DAMASCO system is well described, especially its specialization in the MAC sublayer and the use of MAD for anomaly detection. One highlighted result is a 3% false positive rate with no fans. However, it can be strengthened with a comparison to existing systems and also with performance gains, such as packet delivery rate and detection speed. A mention of scalability or the ability to handle more traffic would also help strengthen the abstract further.

The related works described in this section can be categorized according to various architectures and detection approaches, ranging from RSU-base to fully distributed methods, addressing one or more attacks. Table 1 provides an overview of the main features of these works, and emphasizes the unique touchscreen protection capabilities of our security model.

Table 1.
Comparison of IDS-based Security Solutions for VANETs.

Work	**Deployment**	**Detection Methodologies**	**Supported Attack Types**	**Reputation Management**	**MAC Layer**
Hamdan, et al. [25]	Both	Hybrid (P2DAP + footprint), plausibility	Sybil, footprint manipulation	No	No
Vinita and Vetriselvi [13]	Centralized	Federated learning, fuzzy logic	Sybil attacks	No	No
Luong, et al. [26]	Distributed	Statistics, anomaly filtering	Flooding attacks	No	No
Valentini, et al. [12] (DAM-ASCO)	Distributed	Statistics (MAD-based outlier detection)	DoS/DDoS attacks	Static	Yes
Proposed (NOVA)	Distributed	Hybrid (Statistics + Machine Learning)	DoS, DDoS, Sybil, spoofing	Dynamic	Yes

The discussed work shows significant progress in intrusion detection in vehicular networks; however, open problems remain unsolved. Many systems, e.g., [12, 25, 26], do not practice reputation management or rely on static approaches. Static approaches do not adjust to the dynamics of a network and thus suffer from several problems, such as permanent false positives and delayed recovery of a node's trust. On the other hand, NOVA addresses this by implementing an ongoing reputation management mechanism that recalibrates node reputations based on behavior in real-time.

Moreover, they often focus on a small set of attack types. For example, Hamdan et al. focus on preventing Sybil attacks, Luong et al. target flooding attacks, and DAMASCO is aimed at DoS/DDoS attack detection at the MAC layer via statistical outlier detection. However, these models for detecting single attacks are not suitable for defending against complex attacks such as OS spoofing or data injection. NOVA is a hybrid model leveraging both statistical and machine learning methods to bridge the aforementioned gap, thus enabling it to detect numerous types of attacks, including DoS, DDoS, Sybil, and spoofing attacks.

Additionally, the vast majority of systems, including DAMASCO [12], do not implement trusted nodes, which are important for maintaining non-stop communication between essential infrastructure nodes (such as emergency vehicles) in high-traffic or emergency situations. Without them, there's a danger of unnecessary service-style disruption when trusted nodes are labeled as malicious. NOVA addresses this gap with a cryptographically authenticated trusted node approach that prioritizes such nodes and authenticates trusted nodes, which prevents false positives from disrupting the business of these nodes.

Many systems exhibit scalability and performance restrictions that are related to deployment challenges. Solutions like Vinita and Vetriselvi [13] and Chakraborty et al. use centralized architectures that may have issues with latency and scalability in large vehicular networks. NOVA addresses these challenges through its distributed vehicular cloud integration architecture, which achieves better real-time performance and scalability. DAMASCO [12], while securing the MAC layer, is in contrast to other solutions that ignore this at such a level, leaving their lower net-layer communication protocols vulnerable. NOVA makes it possible to achieve both MAC and network layer protection, setting it apart as a more comprehensive solution relative to data integrity vulnerabilities across the communication stack.

To conclude, the main gaps in the current research are dealing with static reputation, coverage of attacks, trusted nodes, and scalability. NOVA is intended to enhance the security and reliability of vehicular networks by tackling these issues.

3. Proposed NOVA Framework

In this paper, we present the NOVA framework, which achieves stronger security features in vehicular networks by complementing existing detection systems with network-oriented signature analysis, as shown in Figure 1. Consider using a hybrid model of statistical method together with machine learning in NOVA to detect attacks like Denial-of-Service (DoS), Distributed DoS (DDoS), Sybil attacks, spoofing, and data injection in real time.

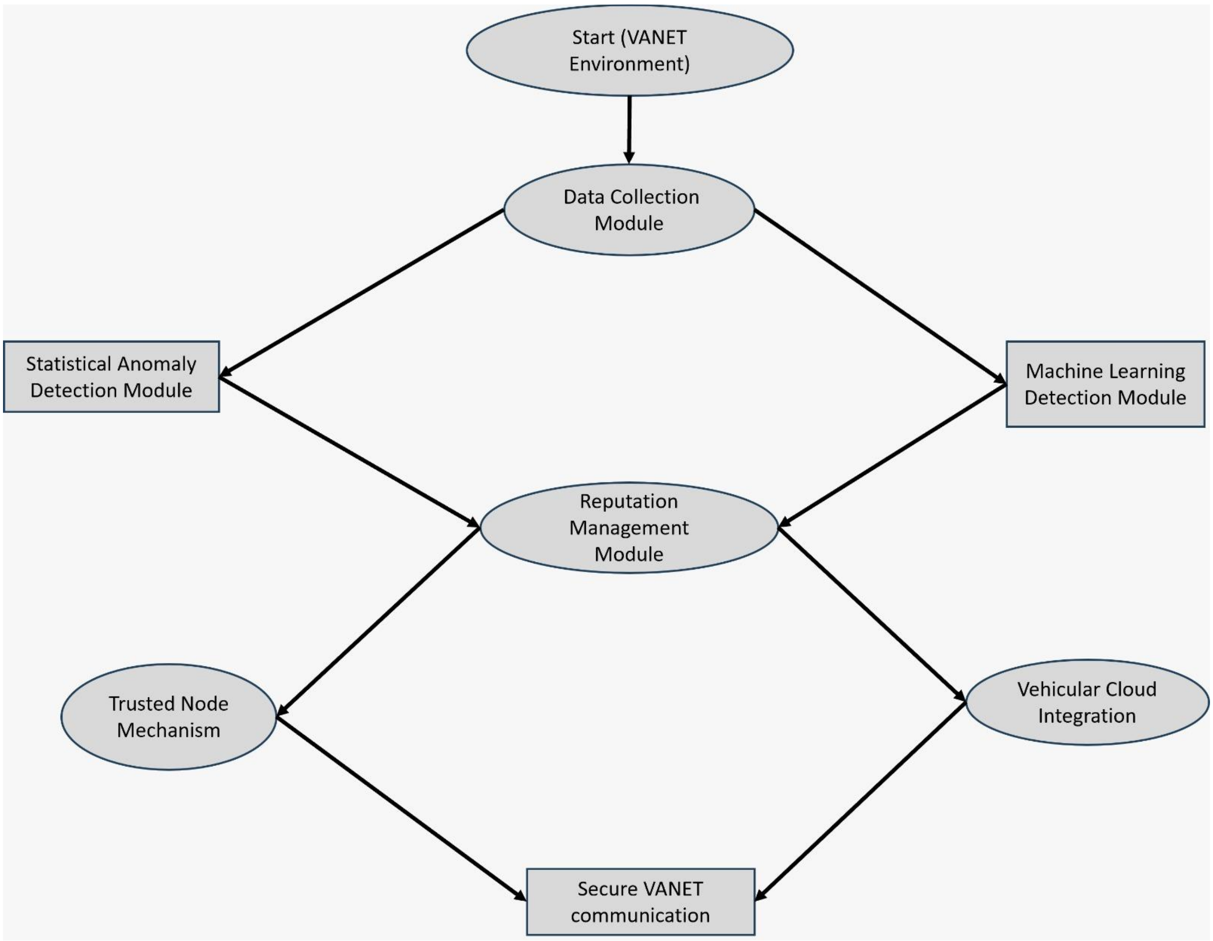
Start (VANET Environment)
Data Collection Module
Statistical Anomaly Detection Module
Machine Learning Detection Module
Reputation Management Module
Trusted Node Mechanism
Vehicular Cloud Integration
Secure VANET communication

Figure 1.
Overview of Proposed NOVA framework.

3.1. Overview of NOVA Architecture

NOVA operates within the VANET infrastructure, focusing on decentralized, vehicle- to-vehicle (V2V) communication. The framework consists of several key modules:

- Data Collection Module: Continuously monitors and logs communication packets, metadata, and traffic patterns from the MAC and network layers.
- Statistical Anomaly Detection Module: Uses an improved Median Absolute Deviation.
  The MAD (Median Absolute Deviation) method is used to detect outliers in request frequencies, flagging potential DoS/DDoS attacks.
- Machine Learning Detection Module: Employs lightweight machine learning models (e.g., decision trees or autoencoders) to detect complex anomalies, such as Sybil or spoofing attacks, which are harder to identify using purely statistical methods.
- Reputation Management Module: Maintains and updates dynamic reputation scores for nodes. This score reflects a node's behavior over time, with provisions for reputation recovery through decay mechanisms.

Trusted Node Mechanism: Ensures priority handling of trusted nodes (e.g., emergency vehicles) by authenticating them with cryptographic protocols to prevent accidental blacklisting.

- Vehicular Cloud Integration: Facilitates secure synchronization of reputation lists and threat data across vehicles in the network using cloud-based infrastructure.

3.2. Detection Mechanisms

This subsection presents a new way of detecting cyber threats in IoT using a hybrid detection approach that combines statistical anomaly detection and machine learning-based anomaly detection. The combination of simple and complex anomaly detection mechanisms serves both for the fast identification of simple types of attacks, such as Denial-of-Service (DoS), and for a thorough examination of any complex attacks, such as Sybil or data spoofing attacks. These methods address the challenges in deep learning technology by supporting accuracy as well as scalability, allowing the system to fulfill and adjust to dynamic vehicle environments.

3.2.1. Statistical Detection Module (Enhanced MAD)

The statistical detection mechanism aims to rapidly detect volumetric attacks such as DoS or DDoS attacks. Using the Median Absolute Deviation (MAD) method, which is more robust to outliers, it identifies unusual spikes in packet transmission rates. This algorithm makes measures of deviation from the median traffic rate. If any node sends significantly more packets than it should, it is flagged as malicious.

```
Algorithm 1 Statistical Detection using MAD
  Require: Traffic data $T$, exclusion constant $ec$, scaling factor $b$
  Ensure: List of flagged malicious nodes
  Initialize $x \leftarrow$ list of packet counts from nodes in $T$
  Compute $M_x \leftarrow \text{median}(x)$
  Compute deviations $D \leftarrow |x_i - M_x|$ for each $x_i$ in $x$
  Compute $MAD \leftarrow b \cdot \text{median}(D)$
  Initialize $flagged\ nodes \leftarrow []$
  for each node $i$ in $T$ do
      if $x_i > (M_x + ec \cdot MAD)$ then
          Add node $i$ to $flagged\ nodes$
      end if
  end for
  return $flagged\ nodes$
```

3.2.2. Machine Learning Anomaly Detection

The machine learning detection center detects advanced attacks such as Sybil attacks, identity spoofing, and false data injection. In this module, we extract features from multi-dimensional networks, including node identities, message types, and traffic patterns. This algorithm predicts whether each node's behavior is normal or anomalous. Anomalous nodes are identified for inspection and mitigation.

The module can operate in:

- Supervised Mode: A classifier (e.g., Decision Trees or Support Vector Machines) is trained with pre-labeled attack data.

```
Algorithm 2 Machine Learning Anomaly Detection
Require: Feature vector set $F$ from nodes, trained model $ML\ Model$
Ensure: List of flagged malicious nodes
Initialize $flagged\ nodes \leftarrow []$
for each feature vector $f$ in $F$ do
    $prediction \leftarrow ML\ Model.\ predict(f)$
    If the prediction indicates an anomaly, then.
        Add the corresponding node to $flagged\ nodes$
    end if
end for
return $flagged\ nodes$
```

Unsupervised Mode: When we do not have labeled data, we can find outliers through other techniques like autoencoders or clustering.

3.2.3. Hybrid Detection Process

The hybrid detection system is divided into two phases:

- Phase 1: Statistics Screening: The first processing is handled by the statistical mod- ule, which is responsible for traffic data. Nodes that surpass the MAD limit are flagged in real-time.
- Phase 2: Machine learning analysis: In case of ambiguous behavior by the node

(Shrouded in the statistical threshold), a data set rich in features is sent to the machine learning module for further analysis.

The two-phase strategy eliminates false positives but retains real-time capabilities. This algorithm starts with a statistical screen. In cases where some nodes show borderline behaviors, their evaluation is raised to the machine learning module so that they can be detected with less consumption of resources.

Algorithm 3 Hybrid Detection Process

```
Require: Traffic data $T$, feature vectors $F$, exclusion constant $ec$, scaling factor $b$, trained model $ML\_Model$
Ensure: List of flagged malicious nodes
$flagged\_nodes\_stat \leftarrow$ Statistical Detection $(T, ec, b)$
$ambiguous\_nodes \leftarrow$ Nodes near threshold but not flagged
if $ambiguous\_nodes$ is not empty then
    $flagged\_nodes\_ml \leftarrow$ Machine Learning Detection $(F, ML\_Model)$
    $flagged\_nodes \leftarrow flagged\_nodes\_stat \cup flagged\_nodes\_ml$
else
    $flagged\_nodes \leftarrow flagged\_nodes\_stat$
end if
return $flagged\_nodes$
```

3.3. *Dynamic Reputation Management*

Traditional Intrusion Detection Systems (e.g., DAMASCO) [12] suffer from one of the major drawbacks of rigidity. To address this problem, a Dynamic Reputation Management Module is introduced in NOVA, as shown in Algorithm 4. This module works in an online fashion and keeps track of the actions of nodes, continuously assigning them a reputation score that efficiently indicates how trusted the node is in the longer term. This dynamic nature acts to slow down potential false positives, ensuring that malicious nodes can be reassessed and that trusted nodes can be re-established after a number of normal activities return to them.

Algorithm 4 Dynamic Reputation Management

```
Require: Node list $N$, detection results $D$, current reputation scores $R$, decay rate $\alpha$
Ensure: Updated reputation scores
for each node $i$ in $N$ do
    if $i$ is flagged by the detection module in $D$ then
        Apply penalty: $\Delta R_i \leftarrow -\beta$
    else
        Apply decay: $\Delta R_i \leftarrow \alpha \cdot (R_{\max} - R_i)$
    end if
    Update reputation: $R_i \leftarrow R_i + \Delta R_i$
    if $R_i < R_{\text{critical}}$ then
        Classify node $i$ as malicious and block communication
    else if $R_i < R_{\text{low}}$ then
        Throttle communication for node $i$
    end if
end for
return $R$
```

3.3.1. *Reputation Score Calculation*

Every node in the network has a reputation score that updates according to observed actions. There are a few factors that affect the reputation score:

- Module for Anomaly Detection Results: Nodes flagged by either the statistical or the machine learning module are penalized by reducing their reputation.
- Traffic Patterns: How Traffic Patterns are Taken Into Account (Normal vs Abnormal Communication)
- Severity of Misbehavior: A severe misbehavior (e.g., sending too many packets, indicating a DoS attack) contributes more significantly to the node's reputation penalty.

The reputation score can be modeled as follows:

$$R_i(t) = R_i(t-1) + \Delta R_i$$

Where:

- $R_i(t)$ is the reputation score of node i at time t,
- ΔR_i is the change in reputation based on recent behavior.

3.3.2. Reputation Decay

Reputation decay is introduced to avoid the permanent blacklisting of nodes. If a node behaves normally for a long time, the reputation score rises gradually. The decay rate can be tuned according to network conditions and the manner of attacks observed. Equation for Decay Function:

$$\Delta R_i = \alpha \cdot (R_{\max} - R_i(t-1))$$

Where:

- α is the decay rate constant,
- $R_{\max}$ is the maximum reputation score a node can have.

3.3.3. Reputation List Management

The system keeps a reputation list in which reputation scores of all nodes in the communication range are stored. This list is periodically updated and synced with other vehicles on the network using vehicular cloud integration.

Reputation List Fields: (i) Node ID (MAC/IP address); (ii) Current Reputation Score; (iii) Last Updated Timestamp; and (iv) Status (i.e., "Normal," "Malicious," "Trusted").

3.3.4. Actions Based on Reputation

NOVA uses a reputation score to classify nodes and to take action to keep the network secure, as shown in Table 2. Malicious nodes are temporarily blocked and are periodically re-evaluated for removal from the blacklist.

Table 2.
Reputation classification and corresponding researchers' groups

Reputation Range	**Classification**	**Action**
High (close to maximum)	Trusted	Grant full communication access
Medium	Normal	Monitor traffic but no restrictions
Low	Suspicious	Throttle or limit request rates
Critical (very low)	Malicious	Block node and report neighboring vehicles

3.3.5. Trusted Node Exception Handling

The trusted nodes that are sending vehicles are authenticated with a cryptographic protocol to avoid the blockage of critical infrastructure nodes (consider, for example, emergency or law enforcement vehicles). They define a different client-percolation threshold and are not as likely to be marked as malicious. Key features include:

- Digital Signatures: To prove that a node is eligible for priority communication.
- Priority Overrides: In case of abnormal traffic conditions, trusted nodes maintain the privileges of communicating with the network.

3.4. Trusted Node Mechanism

For vehicular networks, some critical nodes, such as emergency vehicles, law enforcement units, and other infrastructure-related nodes, are of great significance. Protecting these nodes must involve safeguarding against false-positive detections and denial of communication during anomaly detection, as shown in Algorithm 5. NOVA introduces the concept of the Trusted Node Mechanism, which ensures that essential nodes are authenticated and prioritized, thereby maintaining the integrity and availability of network services.

Algorithm 5 Trusted Node Verification and Management

```
Require: Node $i$, certificate $Cert_i$, detection result $D_i$, reputation $R_i$, trusted
    threshold $R_{\text{trusted}}$
Ensure: Node classification (Trusted, Normal, Malicious)
if Verify Certificate ($Cert_i$) = False then
    Classify node $i$ as untrusted and apply detection rules
    return Normal or Malicious classification based on $D_i$
end if
if $R_i \geq R_{\text{trusted}}$ then
    Allow full communication access for node $i$
    return Trusted classification
else
```

```
        Apply normal detection and classification rules
        Return normal or Malicious classification
    end if
```

3.4.1. Purpose and Authentication

The trusted node mechanism accomplishes several goals:

- Misclassification Prevention: Minimize the chance of reliable respective nodes being classified as adversarial.
- Delay-Free Ensure: Never lose communication with a trusted node even in emergencies or high-traffic scenarios.
- Improve Reliable Networking: Ensure secure and stable functioning of critical services in the vehicular network.

  In order to do this, trusted nodes need to go through authentication based on cryptographic protocols:
- Digital Certificates: Enables the authority to verify the digital identity of the nodes and their roles and permissions.
- This involves verifying message authenticity by checking digital signatures from trusted nodes and recipient signature.

3.4.2. Trusted Node Reputation Management

To filter out temporary misbehaviors (e.g., burst communication in front of disasters), such nodes have a different threshold of reputation. The key features include:

- Priority Overrides: This means that detection thresholds are bypassed for trusted nodes and trusted nodes are given precedence. For instance, their packet rates could be measured against larger quotas than normal nodes.
- Behavioral Monitoring: Although trusted nodes are given preference, they are still monitored for their behavior. Inappropriate or extreme misbehavior (e.g. sustained packet floods) could cause temporary trusted status to be suspended.

3.4.3. Implementation Steps

The trusted node mechanism works as follows:

- Node Authentication: During initiation of communication, a node submits its digital certificate.
- Signature Verification: The node's signature is verified by the recipient for authenticity. Rechecking it keeps the node untrusted.
- Reputation Check: Once authenticated, the reputation score of the node is compared to the trusted threshold. Detecting a minor detection alarm, fully authorized trusted nodes can arbitrarily communicate with trusted nodes.
- Monitoring and Escalation: Ongoing monitoring ensures that serious misbehavior

would be registered. Trusted status can also be suspended until the issue is resolved if needed.

4. Performance Evaluation

4.1. Simulation Setup

To test the effectiveness of NOVA, Table 3 summarizes the key parameters used to configure the simulation environment for evaluating the NOVA framework.

4.2. Experimental Design

The experiment was divided into two phases:

Phase 1: Evaluating Statistical Detection: The effectiveness of the augmented MAD method to detect a DoS and DDoS attack on the system was evaluated. This phase gauged the performance of the statistical outlier detection when facing packet flood attacks.

Table 3.
Simulation Setup Details for NOVA Framework Evaluation.

Parameter	Details
Simulation Tools	OMNeT++ [28, 29], SUMO [30, 31], MOVE [32]
Network Topology	Urban environment with a distributed network
Node Density	50 to 500 vehicles
Communication Type	Vehicle-to-Vehicle (V2V) communication
Bandwidth	10 Mbps (DSRC standard)
Transmission Range	300 meters
Attack Scenarios	DoS/DDoS, Sybil, Spoofing, Packet Injection

Phase 2: Evaluation of Hybrid Detection: The hybrid system was tested in the open ocean against Sybil and spoofing attacks and was founded on both statistical and machine learning modules. In this phase, the proposed dynamic reputation management and trusted node mechanism were also evaluated.

4.3. Evaluation Metrics

The following metrics were used to evaluate the performance of the NOVA framework:

1. Detection Rate (DR): The percentage of correctly detected malicious nodes out of all actual malicious nodes.

$$DR = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}} \times 100$$

2. False Positive Rate (FPR): The percentage of legitimate nodes incorrectly classified as malicious.

$$FPR = \frac{\text{False Positives}}{\text{False Positives} + \text{True Negatives}} \times 100$$

3. False Negative Rate (FNR): The percentage of malicious nodes not detected by the system.

$$FNR = \frac{\text{False Negatives}}{\text{True Positives} + \text{False Negatives}} \times 100$$

4. True Positive Rate (TPR): Also known as *Sensitivity*, this metric indicates how effectively the system detects malicious nodes.

$$TPR = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}} \times 100$$

5. True Negative Rate (TNR): Also known as *Specificity*, this measures the system's ability to correctly identify legitimate nodes.

$$TNR = \frac{\text{True Negatives}}{\text{True Negatives} + \text{False Positives}} \times 100$$

6. CPU Usage: The average percentage of CPU resources consumed by the detection system, indicating computational efficiency.

7. Memory Usage: The average amount of memory consumed by the detection modules during runtime.

8. Scalability: The system's ability to maintain performance (detection accuracy and response time) as the number of nodes and network traffic increases.

5. Results

The results of the performance evaluation for the NOVA framework are shown in this section with respect to the simulation and testing scenarios. The findings include vital performance metrics, such as detection rate, false positive/negative rates, resource efficiency, and scalability. The performance metrics are evaluated against the DAMASCO system and other useful IDS solutions, which demonstrate the advances in both security and efficiency of NOVA in comparison.

5.1. Detection Performance

NOVA yielded a strong detection rate for a variety of attack patterns. The detection rates (DR) of DoS/DDoS attacks were greater than 97%, followed by 95% for Sybil attacks and 94% for spoofing attacks. The lower error rate comes from the hybrid detection method, which mixes statistical with machine learning methods.

NOVA's wide detection range and capability for high accuracy go beyond MAC-layer DoS detection, which achieved a detection rate of 95% for DoS attacks in DAMASCO [12].

Figure 2 summarizes the detection rate comparison for several of the most common security approaches, including DAMASCO [12, 13] and NOVA, for conducting schematic detection accuracy against different types of cyberattacks. Although DAMASCO has a very high detection rate of 95%, it is optimized only for Denial of Service (DoS) attacks. This indicates that it is helpful in defending against DoS, but not as effective against other types of attacks. In contrast, the Vinita and Vetriselvi [13] scheme is focused on Sybil attacks and achieves 87% detection accuracy. With values lower than DAMASCO, it shows a trade-off in performance adapted to a different threat model. We find, however, that NOVA achieves the highest detection rate of 97% and showcases improved adaptability over multiple types of attacks at once. NOVA might end up being a relatively more complete and rigorous solution for system defense against a wide range of threats. The findings highlight the need to design security schemes that offer different levels of effective detection versus attack coverage, depending on the network requirements and risk profile.

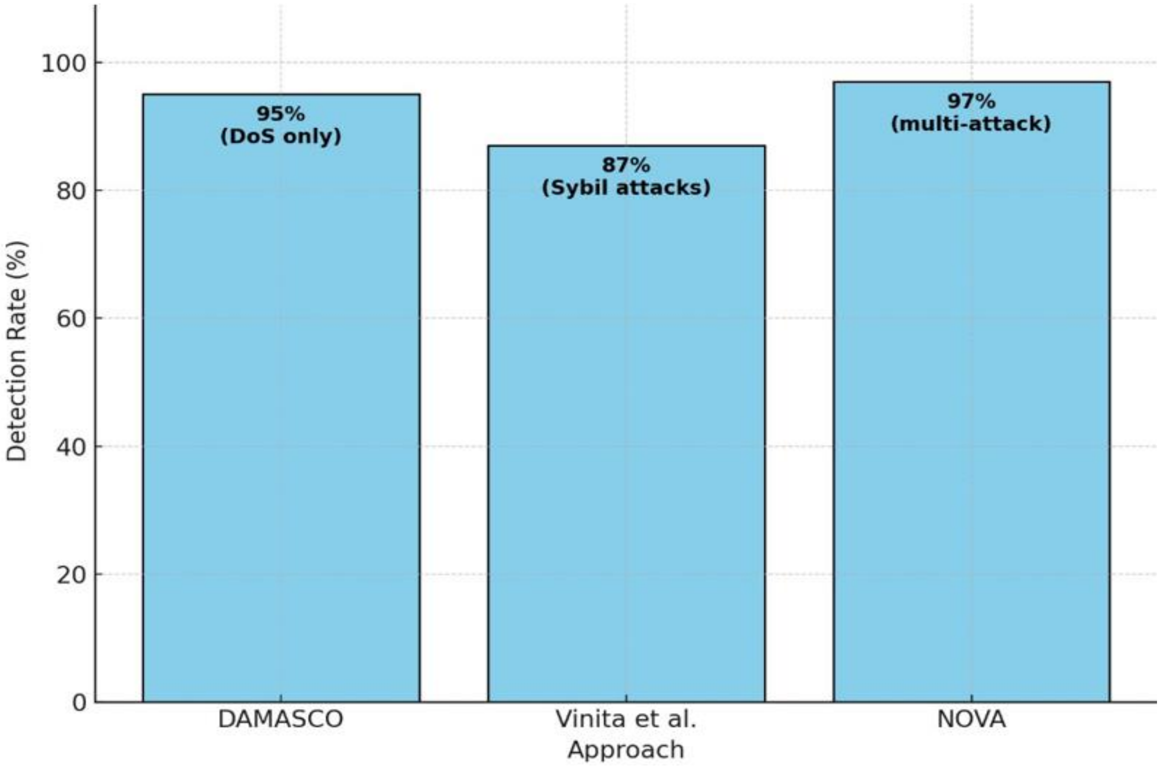

Figure 2.
Comparison Detection Performance.

5.2. False Positive and False Negative Rates

Figure 3 shows a comparison of FPR and FNR of three security approaches: DAMASCO [12, 13] and NOVA. One of the comparisons to discuss is the FPR and FNR between DAMASCO, Vinita and Vetriselvi [13], and NOVA. Creator Note: How good is good? This is not comparing apples to apples here, one on the FPR and one on the FNR, but the purpose here is to put three systems in the same basket. Lastly, the error rates of DAMASCO are comparably low, with a 3% FPR and a 5% FNR, demonstrating an overall good balance. NOVA achieves the lowest False Positive Rate (1.2%) and False Negative Rate (3%) compared to the others, reaffirming that it is the most efficient detector, both with respect to coverage and accuracy. However, Vinita and Vetriselvi [13] show an increased error rate, with an FPR of 4% and an FNR of 13%, considerably higher compared to the previous model, indicating a higher chance of missing true attacks. This emphasizes NOVA's strength in a multi-attack setting, where it achieves higher accuracy compared to the other approaches. In practical terms, this analysis shows that ensuring both FPR and FNR are minimized is paramount to keeping systems secure and performant.

5.3. True Positive and True Negative Rate

Figure 4 shows the TPR and TNR for three security approaches: DAMASCO [12, 13] and NOVA. DAMASCO presents a true positive rate (TPR) of 95% and a true negative rate (TNR) of 96%, which shows its powerful ability to capture true attacks while reducing false negatives. At the same time, NOVA also outshines the remaining approaches with a TPR of 97% and a TNR of 98.5%, meaning it is also good at both finding attacks and not misclassifying legitimate traffic as malicious. In contrast, Vinita and Vetriselvi [13] show a TPR of 87% and TNR of 92%, which means there will likely be a greater number of false negatives and false positives than the other two analyzed techniques. Such differences were likely a result of each approach targeting different types of attack scenarios since DAMASCO is optimized for DoS attacks, while NOVA is more geared toward multi-attacks. In summary, NOVA delivers better reliability and versatility in a single solution for multi-vector attack scenarios. It emphasizes the trade-off between detection accuracy and false rates in security system designs for critical systems.

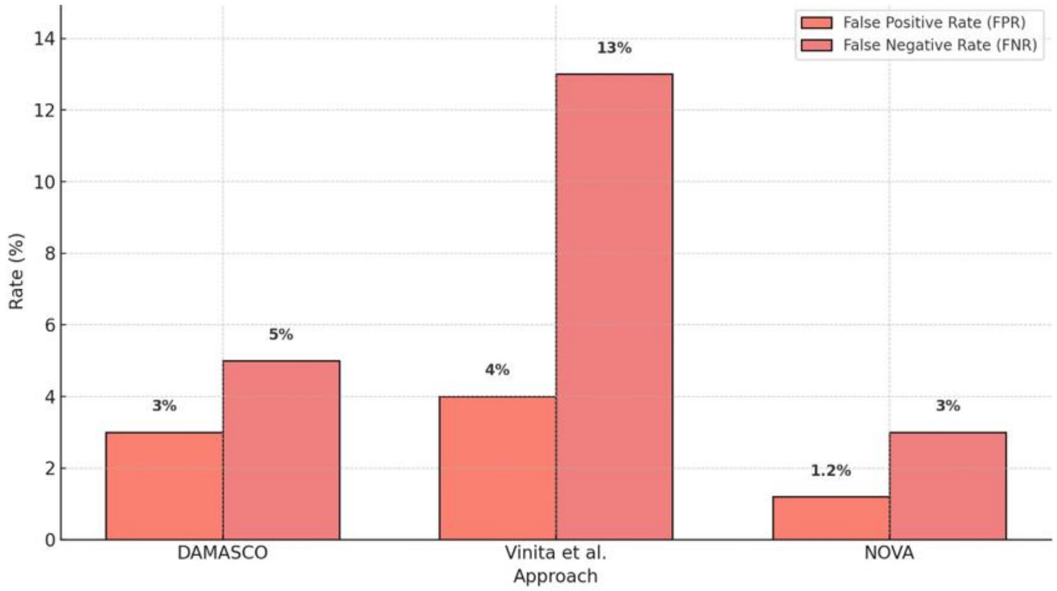

Figure 3.
Comparison of False Positive and False Negative Rates.

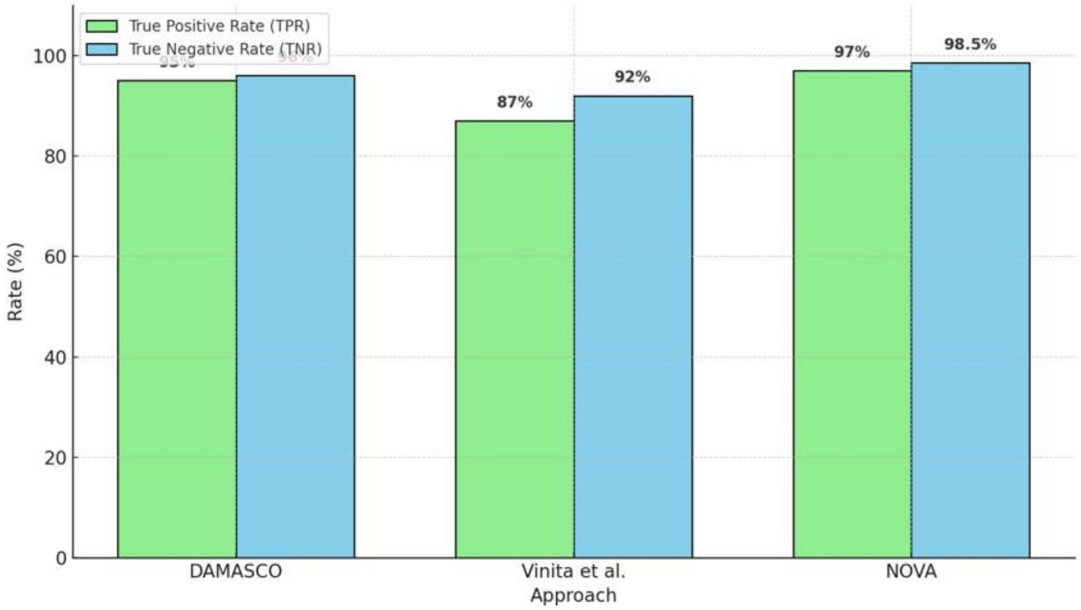

Figure 4.
Comparison of True Positive and True Negative Rates.

The NOVA framework displays a good balance between high threat detection and very few false alarms and outperformed similar generation systems such as DAMASCO in terms of both sensitivity and specificity.

5.4. CPU and Memory Usage

The measure of network's performance using NOVA by measuring CPU and memory consumption under the different network loads. Figure 5 also can be used to understand the CPU and memory usage difference between the 3 approaches: DAMASCO [12, 13] and NOVA. DAMASCO incurs the least resource usage, with 0.1% CPU usage and only 10 MB of memory. It is thus very efficient, especially in resource-constrained environments. NOVA also appears to be moderately resource efficient, consuming 0.2% CPU and 20MB of memory — a decent trade-off between performance and resource overhead.

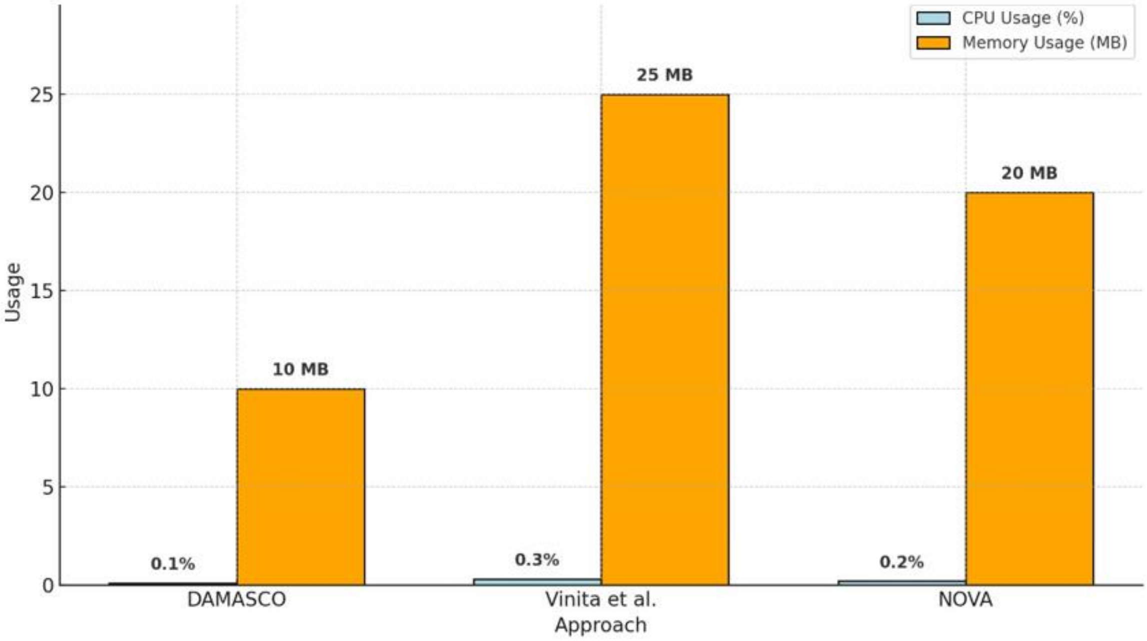

Figure 5.
Comparison Of CPU And Memory Usage.

In contrast, Vinita and Vetriselvi [13] and 25 MB of memory — which suggests potential scalability and performance concerns for large-scale deployments. Overall, we can conclude that DAMASCO is the most resource-efficient, while NOVA has a good balance in terms of performance and resource requirements, which makes it acceptable for moderately constrained systems.

5.5. Scalability

To assess scalability, the number of nodes in the network was progressively changed from 50 to 500, as shown in Table 4. Within one region, NOVA's sensitivity did not change significantly, going from 97% to 96% with increasing node density. NOVA's detection time per event was always below 200 ms and demonstrated its capability to work efficiently in large-scale vehicular networks.

Table 4.
Scalability Comparison of IDS Systems

System	Scalability Performance
DAMASCO	Limited; struggles with node counts > 200
Vinita and Vetriselvi [13]	Delays observed with node density > 300
Proposed (NOVA)	Stable; maintains performance with 500+ nodes

DAMASCO adopts a centralized design while relying on MAC-layer outliers-based statistical detection. Although it is good at discovering DoS/DDoS attacks under low-traffic capabilities, the system is hardly scalable. In addition, performance stalks as the n nodes increase above 200; false positive rate and detection time increase. Because it lacks a distributed architecture and dynamic traffic handling.

Vinita and Vetriselvi [13] system employs a fuzzy logic-based centralized federated learning paradigm for Sybil attack detection. The model enables enhancements in detection accuracy within small networks; nevertheless, it suffers from scalability problems when the number of nodes is high (i.e., more than 218). The growth of nodes leads to increased communication overhead and increases the latency of model synchronization and decision-making. This constrains its real-time performance.

NOVA employs a cloud-synced vehicular version of a distributed architecture that can scale to accommodate large networks. For simulations with up to 500 nodes, there was minimal impact on detection rates (a decrease from 97% to 96%). Following ladies' foot pain with foot pain, the detection time remained under 200 ms in all scenarios, implying that NOVA is capable of retaining both precision and quickness even in a high-density site. Adaptive scaling mechanisms are built in through its reputation management and trusted node mechanism.

6. Conclusion

In this paper, we propose a hybrid detection framework called NOVA, enabling VOC secure communication by overcoming the main limitations existing in current Intrusion Detection Systems (IDS). NOVA works in phases; with statistical anomaly detection and machine learning features, it is able to detect a variety of attack types (DoS, Sybil, and spoofing attacks) with high accuracy. In contrast to traditional systems relying on static thresholds and centralized architectures, NOVA employs dynamic reputation management, allowing for real-time adjustment based on changes in network behavior. This greatly decreases false positives and false negatives and gives compromised nodes a chance to regain trust after exhibiting normal behavior.

NOVA additionally incorporates a trusted node mechanism to guarantee that key infrastructure nodes (such as emergency vehicles) can continue to communicate in data-intensive situations. This allows the system to securely process high-priority messages through cryptographic authentication and priority queuing. Furthermore, NOVA's distributed architecture extends scalability and provides low-latency performance via supported vehicular cloud services.

The experimental results prove that NOVA achieves a 97% detection rate and only a 1.2% false positive rate, with stable performance as the number of nodes increases to 500. When comparing NOVA to previous systems, including DAMASCO, Vinita and Vetriselvi [13], our system has shown obvious gains in detection accuracy, resource utilization, and scalability.

In the future, further studies may address the performance optimization of the machine learning component invoked in NOVA, enabling it to react in scenarios of more sophisticated attacks, such as adversarial ones. In addition, the performance and reliability of the framework will be further validated with real-world deployment in large-scale transportation networks. Another area of focus is how NOVA equally ensures the ideal deployment of powerful new technology, providing a scalable solution for securing intelligent transportation systems from constantly evolving cyber threats.

References

[1] N. I. Jasim, S. Shamini, M. A. Al-Sharafi, M. A. Mahmoud, M. Ibrahim, and A. Hassan, *Adoption and implementation trends of vehicle-to-everything (V2X) technologies: A comprehensive bibliometric analysis. In Current and Future Trends on AI Applications*. Switzerland: Springer, 2025.

[2] M. AlMarshoud, M. Sabir Kiraz, and A. H. Al-Bayatti, "Security, privacy, and decentralized trust management in VANETs: A review of current research and future directions," *ACM Computing Surveys*, vol. 56, no. 10, pp. 1-39, 2024. https://doi.org/10.1145/3656166

[3] M. Sadaf, Z. Iqbal, Z. Anwar, U. Noor, M. Imran, and T. R. Gadekallu, "A novel framework for detection and prevention of denial of service attacks on autonomous vehicles using fuzzy logic," *Vehicular Communications*, vol. 46, p. 100741, 2024. https://doi.org/10.1016/j.vehcom.2024.100741

[4] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "ECA-VFog: An efficient certificateless authentication scheme for 5G-assisted vehicular fog computing," *Plos One*, vol. 18, no. 6, p. e0287291, 2023.

[5] R. P. Nayak, S. K. Bhoi, K. S. Sahoo, S. Sethi, S. Mohapatra, and M. Bhuyan, "Unveiling sybil attacks using ai-driven techniques in software-defined vehicular networks," *Security and Privacy*, vol. 8, no. 1, p. e487, 2025. https://doi.org/10.1002/spy2.487

[6] Z.-R. Tzoannos, D. Kosmanos, A. Xenakis, and C. Chaikalis, "The impact of spoofing attacks in connected autonomous vehicles under traffic congestion conditions," *Telecom*, vol. 5, no. 3, pp. 747-759, 2024. https://doi.org/10.3390/telecom5040048

[7] S. Mazhar *et al.*, "State-of-the-art authentication and verification schemes in vanets: A survey," *Vehicular Communications*, p. 100804, 2024. https://doi.org/10.1016/j.vehcom.2024.100804

[8] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil, and I. H. Hasbullah, "Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey," *IEEE Access*, vol. 9, pp. 121522-121531, 2021. https://doi.org/10.1109/ACCESS.2021.3077115

[9] M. S. Korium, M. Saber, A. Beattie, A. Narayanan, S. Sahoo, and P. H. Nardelli, "Intrusion detection system for cyberattacks in the Internet of Vehicles environment," *Ad Hoc Networks*, vol. 153, p. 103330, 2024. https://doi.org/10.1016/j.adhoc.2024.103330

[10] M. Almehdhar *et al.*, "Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks," *IEEE Open Journal of Vehicular Technology*, pp. 1-38, 2024. https://doi.org/10.1109/OJVT.2024.000001

[11] F. Aloraini, A. Javed, and O. Rana, "Adversarial attacks on intrusion detection systems in in-vehicle networks of connected and autonomous vehicles," *Sensors*, vol. 24, no. 12, p. 3848, 2024. https://doi.org/10.3390/s24123848

[12] E. P. Valentini, G. P. Rocha Filho, R. E. De Grande, C. M. Ranieri, L. A. P. Júnior, and R. I. Meneguette, "A novel mechanism for misbehavior detection in vehicular networks," *IEEE Access*, vol. 11, pp. 68113-68126, 2023. https://doi.org/10.1109/ACCESS.2023.3185425

[13] L. J. Vinita and V. Vetriselvi, "Federated Learning-based Misbehaviour detection on an emergency message dissemination scenario for the 6G-enabled Internet of Vehicles," *Ad Hoc Networks*, vol. 144, p. 103153, 2023. https://doi.org/10.1016/j.adhoc.2023.103153

[14] M. Jamil, M. Farhan, F. Ullah, and G. Srivastava, "A Lightweight Zero Trust Framework for Secure 5G VANET Vehicular Communication," *IEEE Wireless Communications*, pp. 136 - 141, 2024. https://doi.org/10.1109/MWC.015.2300418

[15] H. Setia *et al.*, "Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments," *Cyber Security and Applications*, vol. 2, p. 100037, 2024. https://doi.org/10.1016/j.cysa.2024.100037

[16] Y. Kumar, V. Kumar, and B. Subba, "Optimization techniques for IDS-Generated traffic congestion control in VANET," *Internet Technology Letters*, vol. 7, no. 6, p. e518, 2024. https://doi.org/10.1002/itl2.518

[17] K. Soares and A. A. Shinde, "Intrusion detection systems in vanet: A review on imple- mentation techniques and datasets," presented at the 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), IEEE, 2024.

[18] M. Al Shareeda, A. Khalil, and W. Fahs, "Towards the optimization of road side unit placement using genetic algorithm," presented at the 2018 International Arab Conference on Information Technology (ACIT), IEEE, 2018.

[19] T. Nandy, R. M. Noor, R. Kolandaisamy, M. Y. I. Idris, and S. Bhattacharyya, "A review of security attacks and intrusion detection in the vehicular networks," *Journal of King Saud University-Computer and Information Sciences*, vol. 36, no. 2, p. 101945, 2024. https://doi.org/10.1016/j.jksuci.2024.101945

[20] J. Cui *et al.*, "LH-IDS: Lightweight hybrid intrusion detection system based on differential privacy in VANETs," *IEEE Transactions on Mobile Computing*, vol. 23, no. 12, pp. 12195-12210, 2024. https://doi.org/10.1109/TMC.2024.000001

[21] R. Chen, X. Chen, and J. Zhao, "Sparsified federated learning with differential privacy for intrusion detection in VANETs based on Fisher Information Matrix," *Plos One*, vol. 19, no. 4, p. e0301897, 2024. https://doi.org/10.1371/journal.pone.0301897

[22] E. A. Shams, A. Rizaner, and A. H. Ulusoy, "Flow-based intrusion detection system in Vehicular Ad hoc Network using context-aware feature extraction," *Vehicular Communications*, vol. 41, p. 100585, 2023. https://doi.org/10.1016/j.vehcom.2023.100585

[23] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-based intrusion detection for VANETs: A statistical approach to rogue node detection," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6703-6714, 2015. https://doi.org/10.1109/TVT.2015.2399431

[24] R. Chakraborty, S. Kumar, A. Awasthi, K. Suneetha, A. Rastogi, and G. Jethava, "Machine learning based novel frameworks developments and architectures for secured communication in VANETs for smart transportation," *Soft Computing*, pp. 1-11, 2023. https://doi.org/10.1007/s00542-023-07129-9

[25] S. Hamdan, A. Hudaib, and A. Awajan, "Detecting Sybil attacks in vehicular ad hoc networks," *International Journal of Parallel, Emergent and Distributed Systems*, vol. 36, no. 2, pp. 69-79, 2021. https://doi.org/10.1080/17445760.2020.1797112

[26] N. T. Luong, A. Q. Nguyen, and D. Hoang, "FAPDRP: A flooding attacks prevention and detection routing protocol in vehicular ad hoc network using behavior history and nonlinear median filter transformation," *Wireless Networks*, vol. 30, no. 6, pp. 4875-4902, 2024. https://doi.org/10.1007/s11276-024-03135-0

[27] A. Paranjothi and M. Atiquzzaman, "A statistical approach for enhancing security in VANETs with efficient rogue node detection using fog computing," *Digital Communications and Networks*, vol. 8, no. 5, pp. 814-824, 2022. https://doi.org/10.1016/j.dcan.2022.03.010

[28] A. Varga and R. Hornig, "An overview of the omnet++ simulation environment," presented at the 1st International ICST Conference on Simulation Tools and Techniques for Communications, Networks and Systems, 2010.

[29] A. Varga, *A practical introduction to the OMNeT++ simulation framework. In Recent Advances in Network Simulation: the OMNeT++ Environment and Its Ecosystem*. Switzerland: Springer, 2019, pp. 3–51.

[30] E. Vogel, "Training and evaluating deep learning models on road graphs for traffic prediction using sumo," PhD Thesis, Hochschule Hannover, 2024.

[31] D. Krajzewicz, *Traffic simulation with SUMO–simulation of urban mobility, Fundamentals of traffic simulation*. New York, USA: Springer, 2010, pp. 269-293.

[32] K.-C. Lan, *Move: a practical simulator for mobility model in vanet. In: Telemat- ics Communication Technologies and Vehicular Networks: Wireless Architectures and Applications*. USA: IGI Global, 2010, pp. 355–368.