

A Neuro-Symbolic and Reinforcement Learning Based Hybrid Framework for Real Time Detection of Distributed Denial of Service Attacks in Internet of Vehicles Networks

Tania Yaseen Sulaiman

Computer Department, Faculty of Science, Soran University, Erbil, Kurdistan Region, Iraq

Email: 402238200006@soran.edu.iq

Asst. Prof. Hakem Beitollahi

Computer Department, Faculty of Science, Soran University, Erbil, Kurdistan Region Iraq

Email: Hakem.beitollahi@visitors.soran.edu.iq

ARTICLE INFO

Article History:

Received: 13/6/2025

Accepted: 6/8/2025

Published: Autumn2026

Keywords:

*Internet of Vehicles,
DDoS Detection, Neuro-Symbolic AI,
Reinforcement Learning,
Cybersecurity.*

Doi:

10.25212/lfu.qzj.11.4.47

ABSTRACT

The Internet of Vehicles (IoV) revolutionizes vehicular communication but introduces crucial vulnerabilities of Distributed Denial of Service (DDoS) attacks that can interfere with real-time data sharing and road safety. Traditional machine learning approaches tended to encounter tradeoffs among detection accuracy, interpretability, adaptability, and real time efficiency. The current work presents NSRL-HAD, a novel hybrid architecture that cooperatively integrates Neural Networks (NN), Decision Trees (DT), Neuro-Symbolic Logic, and Reinforcement Learning (RL) to achieve intelligent, transparent, and self-adaptable DDoS detection for IoV use cases. The architecture employs state of the art dimensionality reduction techniques, such as PCA, SVD, Random Projection, and Robust Matrix Factorization, to attain computational efficiency enhancement as well as noise elimination. Experimental evaluations conducted using the CICIOV2024 dataset demonstrate NSRL-HAD attains 100% accuracy, precision, recall, and F1-score, surpassing the latest state of the art IoV security models. NSRL-HAD provides explainable decisions and adjusts the

detection thresholds in real time to varied attack behaviors through a reinforcement learning agent. Its architecture ensures low-latency inference, human-understandable decision rules, as well as resource-limited vehicular system resilience. The results make NSRL-HAD a scalable, real-time, and forensically transparent solution, advancing the frontier of intelligent transport system security.

1. Introduction

The Internet of Vehicles is an intelligent transportation concept that coordinates Vehicular Ad Hoc Networks (VANETs), the Internet of Things (IoT), and cloud computing in an intertwined scheme of communications. The merging of the three ensures efficient interactive connections between the vehicles (Vehicle-to-Vehicle, V2V), between the roadside infrastructures and the vehicles (Vehicle-to-Infrastructure, V2I), and with cloud services (Vehicle-to-Cloud, V2C). Through such end-to-end connectivity the IoV increases important dimensions of contemporary transportation such as safety of the roads, efficiency of the flows of traffic, autonomous driving features as well as the driving experience in general (Shen et al., 2020). Still, the increasing complexity of DDoS attacks especially zero-day and stealth versions challenges conventional detection systems, making many static or signature based solutions useless in dynamic vehicle settings. But such high interconnectivity comes with extreme cybersecurity complexity too. Because of the mission-critical character of vehicular communications where a breach could cause physical damage guaranteeing the dependability, adaptability, and interpretability of IoV systems has taken center stage in contemporary cybersecurity research. Under such an environment, the important dimensions of security of confidentiality, integrity, availability as well as authentication are of greatest concern. Most vulnerable is specifically the dimension of availability that is most vulnerable in Distributed Denial of Service attacks. Such an attack takes critical communication channels out of use, thus making operational dependability of IoV networks readily attackable. In order to counter such an immediate challenge in this paper an innovative adaptive multi-

modal detection method that synergizes learning-based as well as traditional symbol-by-symbol reasoning techniques specifically appropriate for vehicular networking's dynamic nature is introduced (Gyawali et al., 2021; Kumar et al., 2019). The heterogeneity of involved nodes, dynamic nature of IoV topologies, as well as limited nature of resources of vehicular devices all contribute to the latter's vulnerability to DDoS attacks (Nguyen et al., 2024). Assessing such detection systems calls for benchmark datasets that reflect a broad range of traffic patterns and DDoS behavior for instance, the newly launched CICIOV2024 offers real-world vehicular communication scenarios. The attacks themselves are orchestrated by miscreants with the motive of flooding network elements such as Roadside Units (RSUs), On-Board Units (OBUs), or the edge computing nodes of the vehicular network as depicted in figure 1. IoV's DDoS attacks typically are of three categories namely volumetric attacks (e.g., UDP floods), protocol-based attacks (e.g., SYN floods as well as ICMP floods), as well as application-layer attacks (e.g., floods over HTTP). The sources of attacks could be compromised vehicular fleets to selfish infrastructural components as well as foreign Internet of Things (IoT) devices that are embedded in the vehicular networked environment. The targets of attacks typically involve V2V as well as V2I communications channels wherein disruptions could adversely disable safety-critical features such as emergency braking, collision avoidance systems, as well as lane coordination assist. The anonymous as well as dynamic nature of such attacks poses enormous challenges in the form of immediate detection with any high degree of accuracy, thus in need of creative, scalable, as well as adaptive defense system (Albishi & Abdullah, 2024; Haydari & Yilmaz, 2022). Although traditional DDoS detection methods including threshold monitoring, rule-based filtering, and signature matching have been fundamental tools, they lag in dynamic, heterogeneous IoV scenarios. Modeling sophisticated patterns, recent methods using Machine Learning (ML) and Deep Learning (DL) have shown better success in identifying well-known attacks (Manh et al., 2024). Achieved great detection accuracy using supervised learning across several datasets. Still, these techniques frequently show terrible generalization to zero-day attacks and have trouble with transparency an absolute need for safety-critical IoV devices. Many of these models, however, lack interpretability, need considerable computing resources, and depend on labeled

data, which restricts their application in real-time IoV systems (Ahmed et al., 2024; Y. Zhang et al., 2021).

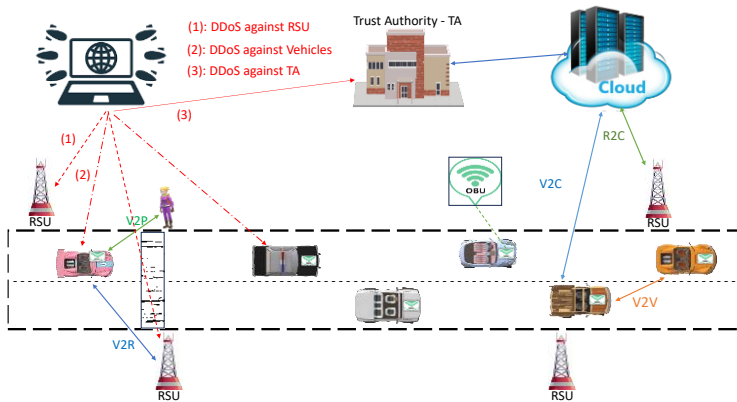


Figure 1: DDOS attack against various components of IoV

The authors propose a hybrid detection scheme that integrates Reinforcement Learning, Neuro-Symbolic Logic, Neural Networks, and Decision Trees to enable adaptive and resilient DDOS detection in IoV scenarios. The approach bridges the gap between machine learning techniques that are highly accurate and the logic that can be explained in real-time and reliable ways for safety-critical applications of intrusion detection. The neural network extracts spatial and statistical features from vehicular communications data, while the decision tree module provides high-performance classification judgments for near-real-time response. Neuro-symbolic logic enhances the system's reasoning capability by providing symbolic reasoning with acquired representation, enabling better knowledge of sophisticated attack behaviors. The reinforcement learning agent adjusts detection thresholds dynamically, enhancing precision with experience gained over time. The hybrid integration approach aims to improve detection accuracy, adaptability to changing threats, and preserve interpretability in resource-limited vehicular networks. Experiments on the CICIOV2024 benchmark dataset show the approach is effective, with a neural network sub-module achieving 99.92% accuracy, a decision tree at 100%, and a neuro-symbolic detector without reinforcement learning-based optimization at 100%

accuracy. This model's generalization ability and efficiency make it suitable for real-time resource-constrained IoV scenarios. From static ML models to federated and hybrid systems, existing DDoS detection techniques show flaws in adaptability, real-time inference, and explain ability as discussed in Section 2. This study offers a new Neuro-Symbolic and Reinforcement Learning Based Hybrid Detection Model (NSRL-HAD) that is optimized for car surroundings to meet these problems. The main contributions of the work are as follows:

- For strong DDoS protection in IoV environments, a multi-modal, interpretable, and adaptive hybrid detection architecture is presented integrating Neural Networks, Decision Trees, Neuro-Symbolic Reasoning, and Reinforcement Learning.
- Using the CICIOV2024 data, the model shows excellent generalization performance 99.92% accuracy in the neural module and 100% accuracy in the symbolic and decision modules.
- By allowing logical inference across observed hostile actions, neuro-symbolic reasoning improves traceability and interpretation.
- Minimizing false positives and adjusting to newly developing threat patterns, a reinforcement learning agent is used to dynamically maximize detection thresholds in real time.

The proposed framework is validated for deployment in resource-constrained vehicular edge environments facing DDoS attacks. This paper presents the system architecture, comprehensive experimental evaluation, and concludes with key insights and future research directions.

2. Related work

Particularly DDoS attacks, cyberattacks are a major hazard for the Internet of Vehicles (IoV). Strong, flexible intrusion detection systems (IDS) are needed in IoV. The concepts, results, and limitations of modern DDoS detection techniques in IoV are examined in this article. It classifies these strategies into three categories: learning approaches for known attack patterns, federated learning frameworks for secure collaboration, and hybrid systems for evolving threats. The study points out flaws in

the existing literature and stresses the necessity of a fresh hybrid model grounded on Neuro-Symbolic and Reinforcement Learning (NSRL-HAD) and its advantages.

2.1 Machine Learning and Deep Learning for Known Attack Detection

This subsection outlines the extensive application of Machine Learning (ML) and Deep Learning (DL) techniques for the detection of known DDoS attacks in the Internet of Vehicles (IoV). These methods have shown high efficacy in identifying pre-existing attack signatures. For instance, (Korium et al., 2024) achieved over 99.8% accuracy using ensemble classifiers across datasets like CIC-IDS-2017 and CIC-DDoS-2019, while (Yang et al., 2021) proposed MTH-IDS, attaining 99.88% accuracy via a multi-tiered supervised learning model. Similarly, (Setia et al., 2024) and (Ahmed et al., 2024) demonstrated accuracies of 99.59% and 98%, respectively, employing simulation-based ML frameworks and advanced dimensionality reduction techniques. Notably, (Anley et al., 2024) explored adaptive transfer learning through deep CNNs (e.g., VGG16, ResNet50), and (Anli et al., 2024) addressed sub-domain detection using LSTM on CICEV2023. Other hybrid approaches, such as those by (Sherazi et al., 2019) and (Umar Sattar et al., 2024) integrated Fuzzy Logic with Q-Learning, although they lacked comprehensive performance evaluations. (Neto et al., 2024) contributed the CICIOV2024 benchmark dataset, facilitating realistic IDS research, while (Karthikeyan & Usha, 2022) proposed a reinforcement learning-based detection method with limited methodological detail. Despite their strengths, these supervised and semi-supervised models suffer from significant limitations. Their dependency on historical, labeled data renders them less effective against zero-day attacks, requiring continual retraining and dataset updates an impractical demand in real-time vehicular environments. Moreover, the opacity of complex DL models (Anley et al., 2024; Anli et al., 2024) hampers interpretability, which is vital for forensic investigations and safety assurance in IoV systems.

2.2 Federated Learning for Collaborative and Private IDS

Federated Learning (FL) has emerged as a promising approach to enable privacy-preserving, collaborative intrusion detection across distributed IoV nodes. By decentralizing model training and retaining raw data locally, FL addresses data privacy

and sovereignty concerns inherent in traditional centralized systems. (Ahmed et al., 2024) introduced DISFIDA, a self-supervised FL framework utilizing Dense Random Neural Networks (DRNN), achieving exceptional performance with a 100% True Positive Rate and 99% True Negative Rate for DDoS detection. Similarly, (Driss et al., 2022) proposed an FL framework incorporating Gated Recurrent Units (GRU) with a Random Forest ensembler, demonstrating 99.52% accuracy and robust evaluation metrics on the 'Car Hacking' dataset. Despite its privacy advantages, FL remains constrained by its dependence on pre-labeled data, limiting its efficacy against zero-day attacks. Moreover, the limited interpretability of its deep models impedes forensic transparency in critical IoV systems.

2.3 Hybrid and Adaptive Systems for Novel Threat Detection

Addressing the limitations of static, supervised detection systems, recent research has increasingly explored hybrid and adaptive IDS approaches to enhance resilience against zero-day threats in IoV environments. (Najafimehr et al., 2022) and (Yang et al., 2021) exemplify hybrid models that integrate unsupervised clustering with supervised classification, significantly improving recall on unseen attacks. However, their reliance on the assumption that malicious traffic forms distinguishable clusters limits their effectiveness against stealthy or low-volume intrusions. Adaptive approaches, such as the Q-learning-based models by (James et al., 2024) and (Karthikeyan & Usha, 2022), introduce dynamic response mechanisms, yet often employ simplistic reward strategies and are constrained to specific network environments like SDN, without comprehensive evaluations for real-time deployment. Further contributions, including (Anley et al., 2024) and (Ahmed et al., 2024) demonstrate the promise of adaptive deep learning and dimensionality reduction techniques, though they frequently lack transparency in preprocessing, model explainability, and operational feasibility. (Sherazi et al., 2019) and (Umar Sattar et al., 2024) proposed hybrid fuzzy logic–reinforcement learning systems with simulated validations, yet omitted essential performance metrics. Benchmark datasets such as CICIOV2024 (Neto et al., 2024) and CICEV2023 (Anli et al., 2024) serve as valuable testbeds for future adaptive IDS research but are not accompanied by robust, fully adaptive frameworks. Collectively, these studies underscore

persistent challenges in balancing detection accuracy with adaptability, real-time performance, and interpretability. Despite promising strides, the development of a comprehensive, explainable, and continuously adaptive IDS tailored for the complex, evolving threat landscape of IoV remains an unresolved and pressing research imperative.

2.4 Our Contribution: A Neuro-Symbolic and Reinforcement Learning-Based Hybrid Framework (NSRL-HAD)

In response to the persistent limitations of static supervised models and inadequately adaptive IDS solutions, this work introduces NSRL-HAD a novel hybrid framework that strategically unifies Neuro-Symbolic AI with Reinforcement Learning (RL) to enable intelligent, interpretable, and dynamically adaptive DDoS detection in IoV environments. Distinct from conventional ML/DL approaches (Korium et al., 2024) (Setia et al., 2024) (Ahmed et al., 2024) , and federated architectures(Driss et al., 2022), which remain largely dependent on historical data and exhibit poor generalization to zero-day threats, NSRL-HAD embeds RL agents capable of continuously interacting with the network environment. This enables online learning of optimal detection policies, adaptive threshold tuning, and real time behavioral adjustment, thus overcoming the static rigidity inherent in prior models (Najafimehr et al., 2022; Yang et al., 2021) Moreover, the framework addresses the explain ability deficit commonly associated with deep and reinforcement learning models (Anley et al., 2024; Anli et al., 2024; Driss et al., 2022) by incorporating a Neuro Symbolic reasoning layer. This integration empowers the system to not only detect anomalous patterns but also infer causal relationships and express its decisions through symbolic rules, facilitating transparency, forensic traceability, and regulatory compliance all critical in safety critical IoV systems. Technically, NSRL-HAD achieves this by synthesizing deep neural networks for feature abstraction, decision trees for fast and interpretable classification, symbolic logic for knowledge based reasoning, and RL for adaptive control. This multi paradigm architecture ensures high detection accuracy for both known and previously unseen threats while maintaining low computational overhead, making it suitable for real-time, resource constrained edge environments. Its performance, validated on the CICIOV2024 benchmark (Neto et al., 2024) confirms

its effectiveness across realistic vehicular scenarios, surpassing prior works that either lacked dynamic learning capabilities (Karthikeyan & Usha, 2022) or failed to deliver rigorous performance evaluation (Sherazi et al., 2019; Umar Sattar et al., 2024). The NSRL-HAD framework introduces a novel, explainable, and adaptive intrusion detection approach for IoV by integrating reinforcement learning with neuro-symbolic reasoning. It overcomes the limitations of static IDS models, offering robust defense against evolving and zero-day DDoS attacks in vehicular cyber-physical systems.

3. Proposed Method

The advocated DDoS detection in Internet of Vehicles (IoV) involves multiple successive steps, which include data acquisition, preprocessing, normalization, and hybrid feature selection mechanism. This is succeeded by the utilization of an innovative multi-component learning architecture. The central model embodies four complementary components: a Neural Network for pattern recognition, a Decision Tree for rule-based inference that is explainable, a Neuro-Symbolic Logic module to blend symbolic reasoning with sub-symbolic learning, and an adaptive controller based on Reinforcement Learning to ensure dynamic optimization of the detection in real time. The integrated strategy is aimed at improving the accuracy levels of the detection system as well as its flexibility in the heterogeneous and dynamic IoV environment. The entire architecture of the suggested framework is demonstrated in figure 2. Each component of the system is described in detail along with its role in the system in the following subsections.

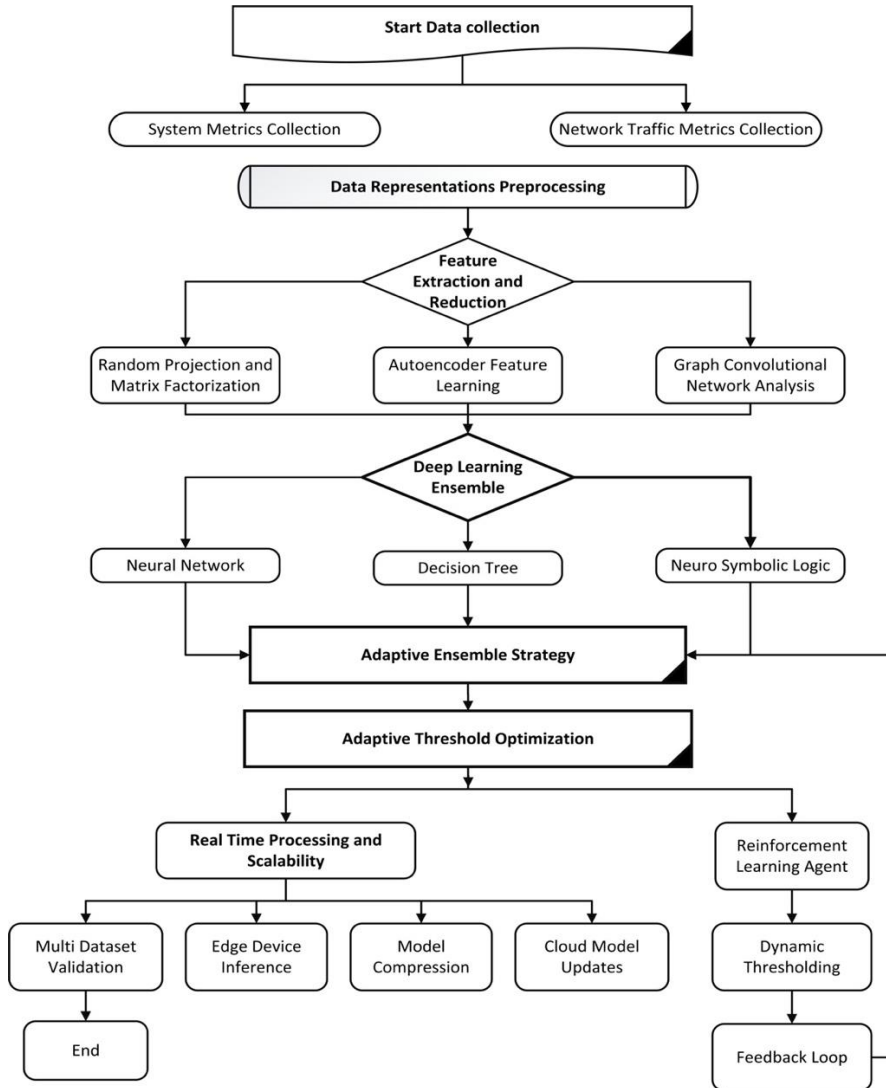


Figure 2: The overall architecture of the proposed NSRL-HAD framework

3.1 Data Collection

A structured data acquisition and preprocessing process was followed to lay the solid groundwork for DDoS detection in the Internet of Vehicles (IoV) environment. Five datasets available in the public domain were first screened in terms of relevance to vehicular communication, feature diversity, similarity to actual DDoS scenarios, and

total data quality. They were: (1) CICIOV2024, (2) N-BaIoT (Bot-IoT), (3) UNB CIC IoT 2023 (5% subset), (4) IoT-Intrusion, and (5) DDoS-CICIoT2023. Each data set was assessed for data volume, feature diversity, conformity with vehicular traffic standards, and representativeness of realistic attack behaviors. Some data sets proved to exhibit strengths in IoT security analysis but lacked temporal granularity, balanced class representation, or vehicular protocol-specific patterns required for realistic model development in IoV scenarios. Based on these characteristics, the CICIOV2024 data set was chosen for further work since it provides high-fidelity IoV traffic data with extensive varieties of DDoS attacks with an assorted set of 13 informative features that adhere to vehicular communication protocols (CICIOV2024, n.d.). The data has 1,408,219 samples with 1,223,737 of them being benign and 184,482 of them DDoS records. The data was filtered so that it had just benign and DDoS classes in order to be in line with the aim of creating a hybrid prediction model that utilizes Neural Networks, Decision Trees, Neuro-Symbolic Logic, and Reinforcement Learning. A thorough data cleansing process was implemented. The initial analysis verified that there were no missing values but that there were some duplicate records that were cleaned using Python data manipulation tools to leave 3,588 unique samples. The outliers were then removed from the data using the three-standard-deviation Z-score method to leave 3,357 high-quality instances. To provide machine interpretability and ensure consistency in terms of feature categories such as labels and categories of traffic, standard label encoding methods were used in encoding such features. Timestamp attributes were standardized to chronological order to maintain temporal consistency an important aspect especially in monitoring changing vehicular network behavior. Synthetic resampling supported with the use of over sampling methods where class imbalance was addressed with the resulting dataset having 6,638 samples evenly distributed between benign and DDoS traffic. A crucial design choice, the selection of the CICIOV2024 dataset provides high-fidelity vehicular communication flows, protocol-specific characteristics (e. g. , CAN-based traffic), and a rich representation of several DDoS attack types. Unlike standard IoT datasets, it matches very well with real-world Internet of Vehicles situations, therefore improving both model relevance and overall generalizability. Addressing class imbalance through synthetic over-sampling was equally vital, ensuring the

model could learn from minority class attack patterns without bias toward benign traffic. This preprocessing strategy significantly improved detection sensitivity, reduced false negatives, and enabled a more robust and realistic evaluation of the proposed hybrid detection system under dynamic and imbalanced IoV conditions. The resulting dataset was then divided between 70% for training and 30% for testing/validation with 5,310 and 1,328 samples respectively.

Data Normalization

All numeric characteristics were linearly normalized to the $[-1, 1]$ range to guarantee equal feature contributions and guard against prejudice from different scales in IoV datasets. This preprocessing stage improves the performance of the hybrid model including Neuro Symbolic Logic, Decision Trees, Neural Networks, and Reinforcement Learning by reducing the influence of strong magnitude variables. The normalization was conducted using the following transformation formula.

$$X = 2 \times (x - \min(x)) / (\max(x) - \min(x)) - 1$$
$$= 2 \times (\max(x) - \min(x)) / (\max(x) - \min(x)) - 1$$

where x is the initial feature value, and $\min(x)$, $\max(x)$ are the feature's minimum and maximum values. The CICIOV2024 dataset, which has features like packet counts, traffic volume, latency, and error rates features with different distributions proved especially successful. Normalization improved model convergence, input interpretability, and cross-component consistency by scaling inputs to a single $[-1, 1]$ range. It guaranteed consistency throughout decision tree splits, stabilized policy changes in the reinforcement learning module, preserved semantic relationships for neuro-symbolic reasoning, and sped and more steady gradient descent in neural networks. Normalizing helped to unify the diverse parts of the suggested hybrid model and considerably improved its ability to identify and reduce DDoS assaults inside IoV systems in general.

3.2 Feature Selection

In the dynamic high-dimensional IoV environment, the efficiency of feature selection is the key to facilitating efficient, accurate, and real-time reasoning for Distributed

Denial of Service attacks. Redundant or excessive features do not just impose computing overhead but can further obscure characteristics of interest by degrading the signal-to-noise ratio in data, hindering the precise capture of the behavior of attacks. In an attempt to counter such challenges, the current research utilizes the integration of classical dimensionality reduction methods with structural analysis and deep unsupervised learning in feature selection. Four sophisticated linear and matrix-based dimensionality reduction techniques were utilized: Principal Component Analysis (PCA)(Husson et al., 2010), Singular Value Decomposition (SVD)(Li, 2023), Random Projection (RP)(Chamarthi et al., 2025), and Robust Matrix Factorization (RMF)(L. Zhang et al., 2019). The CICIOV2024 dataset was analyzed using PCA, SVD, RP, and RMF to capture variance, temporal patterns, and improve robustness to noise. A consensus-based selection preserved the 12 most informative features. Deep autoencoders further retained non-linear relationships for enhanced DDoS detection performance. The model is learned in the following form:

$$h = \sigma(Wx + b), x = \sigma(W'h + b') \quad h = \sigma(Wx + b), \quad \hat{x} = \sigma(W'h + b')h \\ = \sigma(Wx + b), x = \sigma(W'h + b')$$

Standard neural elements weight matrices, biases, and activation functions (e. g. , ReLU or sigmoid) help the deep model to acquire latent representations from input features, hence facilitating precise reconstruction and pattern extraction. Although not directly employed, structural and contextual characteristics were painstakingly retrieved from graph-based analysis to reflect interactions between cars, roadway units, and control centers in IoV networks. This small but semantically rich feature set improves every component of the hybrid detection framework neural networks, decision trees, reinforcement learning agents, and neuro symbolic logic by offering structured input representations that increase the model's capacity to identify sophisticated and coordinated DDoS attack patterns.

3.3 The Proposed Model: NSRL-HAD

The NSRL-HAD is a novel approach to detecting Distributed Denial of Service (DDoS) attacks in the Internet of Vehicles (IoV). This system combines Neural Networks, Decision Trees, Neuro-Symbolic Logic, and Reinforcement Learning to create an accurate, interpretable, and adaptive detection system. The architecture starts with

multi-layered feature extraction, capturing complex network activity patterns. Decision Trees provide rule-based, explainable decisions, while the Neuro-Symbolic Logic layer enhances explain ability by blending symbolic reasoning with learned representations. This hybrid design allows for the recognition of varied attack signatures and transparency, crucial for trust and forensic examination in IoV operating environments. The system's adaptive threshold optimization mechanism, based on Reinforcement Learning, adjusts detection sensitivity in real-time to ensure high detection fidelity with minimal false positives. This is crucial in a dynamic, heterogeneous IoV environment with constant flux of attack vectors and traffic patterns.

3.3.1 Adaptive Threshold Optimization with Reinforcement Learning

A distinguishing aspect of NSRL-HAD is its adaptive threshold optimization approach based on Reinforcement Learning. In standard systems, thresholds for flagging traffic as benign or malicious are statically set or manually tuned. These static thresholds do not consider current variations in traffic flow, particularly in times of high vehicular movement or when facing sneaky, low-rate DDoS attacks. NSRL-HAD addresses this constraint by using an RL agent that dynamically modulates the detection threshold based on current environmental observations. The agent repeatedly assesses traffic features and tunes thresholds to ensure an optimal balance between true positive rate (TPR) and false positive rate (FPR). This allows the system to

- Under suspected attack peaks, raise sensitivity
- Mitigate false alarms in actual traffic surges (such as rush hour),
- And adjust to permanent changes in network usage patterns

Such online flexibility is absolutely necessary to guarantee operational stability and reduce latency-sensitive vehicular applications including autonomous driving, vehicle-to-infrastructure (V2I), and emergency response.

3.3.2 Markov Decision Process Formulation

The behavior of the RL agent is controlled by an MDP, which is mathematically represented as the tuple (S, A, P, R, γ) :

- States (S): Symbolize the prevailing network traffic patterns, which are computed from an amalgam of low-level and high-level features such as packet arrival rates, flow size entropy, protocol distribution, connection lifetimes, and temporal burstiness. The features are preprocessed and compressed through hybrid feature selection so that the state space is compact as well as informative.
- Actions (A): are discrete changes in the detection threshold. The action set comprises
 - o Raise threshold: Lower the sensitivity to avoid false alarms.
 - o Reduce threshold level: Sensitive level based on your dealings
 - o Maintain threshold level: Keep existing sensitivity
- Transition Probability (P): Describes the probability of transitioning between states following an action. There is no explicit definition of these probabilities but it is learned implicitly in interaction with the environment through model-free methods like Q-learning.
- Reward (R): A numerical value that indicates the quality of the detection result after executing an action in a specific state. It rewards correct detection while penalizing false alarms and missed attacks
- The relative worth of future prizes vis-a-vis present rewards is controlled by discount factor (γ). An intermediate value like (e. g. , $\gamma = 0.95$) makes sure the agent chooses long-term performance over near-term performance swings.

3.3.3 Reward Design

The reward function is pivotal to direct the RL agent to optimal behavior in terms of the tradeoff between detection reliability and sensitivity. The function is formulated as

$$R = \alpha \cdot TP + \beta \cdot TN - \gamma \cdot FP - \delta \cdot FNR = \alpha \cdot TP + \beta \cdot TN - \gamma \cdot FP - \delta \cdot FN$$

where

- TP: True Positives — Detection of DDoS packets correctly
- TN: True Negatives — Refers to proper classification of normal traffic.
- False Positives — Legitimate traffic mistakenly detected as malicious.
- FN: False Negatives — Malicious traffic that is undetected by the detector.

The weighting parameters are assigned as follows:

- $\alpha = 0.4$ and $\beta = 0.4$: Highlight reward for correct classification of attack as well as normal
- $\gamma = 0.1$, $\delta = 0.1$: Misclassification penalty with somewhat lessened effect for the sake of experimentation. A balanced reward design ensures that the model does not overfit to attack patterns to the detriment of usability, or vice versa. The learning rate is 0.1 and an ϵ -greedy approach is used to provide sufficient action space exploration while transitioning gradually to exploitation of known optimal actions.

3.3.4 Learning the Optimal Policy

In order to incrementally refine its performance, the RL agent utilizes the value-based reinforcement learning algorithm called Q-learning that estimates expected utility for an action in any state followed by the optimal policy from there on. The update rule is

$$Q(s, a) \leftarrow Q(s, a) + \alpha[r + \gamma \max_{a'} Q(s', a') - Q(s, a)]$$

$$\leftarrow Q(s, a) + \alpha \left[r + \gamma \max_a Q(s', a') - Q(s, a) \right]$$

where

- a, s : Existing situation and action
- s', a' : Next action and next state
- r : Reward instantly received upon transition

Throughout the process, the Q-values become optimal estimations that allow the agent to choose actions with the highest cumulative reward expected. This permits NSRL-HAD to learn autonomously the best policy of thresholding in different network scenarios

3.3.5 Real-Time Adaptation and Deployment

NSRL-HAD is specifically designed for live deployment in IoV's distributed, resource-limited environment. The system utilizes each component synergistically to capitalize on its strengths

- **Neural Network:** Abstracts high-level nonlinear relationships from the preprocessed feature set to offer in-depth representations of traffic patterns

- **Decision Tree:** Performs rapid and interpretable classification using derived features that is suited for on-device inference.
- **Neuro-Symbolic Logic Layer:** Merges preprogrammed rules (such as known attack patterns or policies for quality of service) with acquired knowledge and provides transparent rationales for every decision — an essential need in safety-critical vehicular environments.
- **Rules-Based Agent:** Tracks system feedback reports and evolution of traffic in order to adjust the thresholding mechanism in real-time without human intervention.

3.3.6 Model Behavior in Practical Scenarios

The NSRL-HAD's efficacy is illustrated in numerous actual driving scenarios:

- **Burst of Sudden DDoS Traffic:** When an abnormal surge in traffic is detected, the RL agent reduces the threshold to improve the sensitivity in detection. The Neural Network detects high-dimensional abnormal patterns while the Decision Tree makes an efficient prediction. The symbolic layer gives an explainable reason behind it, which increases the confidence in the mitigation action.
- **High Legitimate Traffic (e.g., Rush Hour):** As legitimate causes of high volumes of traffic occur, the RL agent gradually increases the threshold in order to avoid false positives. Symbolic rules prevent over-adjustment by protecting known safe behaviors from penalty
- **Unknown or Adversarial Attacks:** The multi-layered nature of the model helps it generalize from its training data set. The NN responds to distortions in the traffic features while the Decision Tree marks classification outliers. Symbolic reasoning then assesses contextual domain knowledge to determine the chances of an attack and respond accordingly.

3.3.7 Parameter Settings

To ensure optimal model behavior, the following parameters were empirically tuned:

Table 1: Reinforcement Learning Parameter Settings for the NSRL-HAD Framework

Parameter	Value	Description
Reward Weights (α , β)	0.4, 0.4	High priority on correct classifications
Penalty Weights (γ , δ)	0.1, 0.1	Moderate penalization of FP and FN
RL Learning Rate (α)	0.1	Ensures smooth learning convergence
Discount Factor (γ)	0.95	Balances short-term and long-term performance
Exploration Strategy	ϵ -greedy (decaying)	Facilitates learning while avoiding local optima

3.3.8 Architectural Advantages of NSRL-HAD

The building design of NSRL-HAD has the following attractive benefits:

- **Highest Detection Accuracy:** Facilitated through in-depth feature extraction of Deep Learning of Neural Networks that trace sophisticated patterns of attacks.
- **Interpretability:** Facilitated by integration of symbolic logic and decision tree inference to enable administrators to trace back to human-interpretable rules
- **Real-Time Threshold Adaptation:** Reinforcement Learning provides constant adjustment of sensitivity thresholds for optimal long-term performance in non-stationary environments.
- **Low Latency and Resource Efficiency:** The symbolic logic and decision tree facilitate efficient inference with minimal computationally intensive overhead that is appropriate for edge-based deployment.
- **Novelty and Adversarial Robustness:** The ensemble model is highly generalizable beyond seen patterns so that it is able to withstand open-world situations in which attack strategies change rapidly.

4. Experimental Results and Evaluation

The study entailed developing a neuro-symbolic hybrid model of Neural Network + Decision Tree + Neuro-Symbolic Logic + Reinforcement Learning in Python 3.10 on a Jupyter Notebook. The model was optimized for learning complex non-linear DDoS attack behaviors, with a complementary decision tree-based classifier for explain

ability in symbolic classification. The module for neuro-symbolic logic was utilized for bridging the subsymbolic-symbolic paradigm gap, facilitating explainable as well as attack-resilience decisions. An RL agent was optimized for improved DDoS counteractivity in an IoV environment with adaptation. The solution employed TensorFlow for deep learning, Scikit-learn for decision trees, as well as custom-built logic frameworks for neuro-symbolic reasoning. Reinforcement learning tasks were addressed using OpenAI Gym-compatible environments, optimized using reward shaping techniques for rapid convergence as well as policy stability.

4.1 Performance Metrics

In detail evaluating the hybrid detection framework, six standard classification metrics were used to evaluate accuracy, robustness, and real-time effectiveness in IoV ecosystems:

- **Accuracy:** Evaluates the correct predictions made overall (attacks and benign) as a proportion of total predictions.

$$\text{Accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN})$$

- **Precision:** Indicates the proportion of attacks predicted that were true attacks, indicating the false positive rate.

$$\text{Precision} = \text{TP} / (\text{TP} + \text{FP})$$

- **Recall (Sensitivity):** Ability of the model to capture actual attacks reduces false negatives.

$$\text{Recall} = \text{TP} / (\text{TP} + \text{FN})$$

- **F1-Score:** Precision and recall metrics combined provide the harmonic mean, therefore it decreases detection quality in very imbalanced datasets.

$$\text{F1} = 2 \times (\text{Precision} \times \text{Recall}) / (\text{Precision} + \text{Recall})$$

- **False Positive Rate (FPR):** Proportion of non-threatening traffic that is flagged incorrectly classified as threats.

$$\text{FPR} = \text{FP} / (\text{FP} + \text{TN})$$

- **False Negative Rate (FNR):** Proportion of threats that are deemed non-existent but are present in reality.

$$\text{FNR} = \text{FN} / (\text{FN} + \text{TP})$$

A reinforcement learning agent further optimizes detection thresholds using a reward function which penalizes both FPR and FNR. This approach improves precision and consistency in real time across the hybrid system.

4.2 Results

In order to comprehensively assess the performance of the suggested neuro-symbolic hybrid intrusion detection model in identifying and resisting DDoS attacks in IoV networks, experiments were carried out using an 6,638-labeled dataset with 5,310 instances used for training and 1,328 instances used for testing. Learning of the model was extremely efficient with the neural network component obtaining 99.92% train accuracy and 100% validation accuracy within the second epoch, while the loss function decreased steadily from 0.5498 to 0.000229, indicating first-rate generalization without overfitting as seen from Figure 3 Neural Network Training History. Training took 8.47 seconds overall while the inference took just 0.165 seconds indicating high computing efficiency. Concurrently, the symbolic reasoning component implemented through decision tree achieved 100% accuracy, precision, recall, and F1-score with high interpretability with minimal computing load involved in it (training: 0.0047s; prediction: 0.002s).

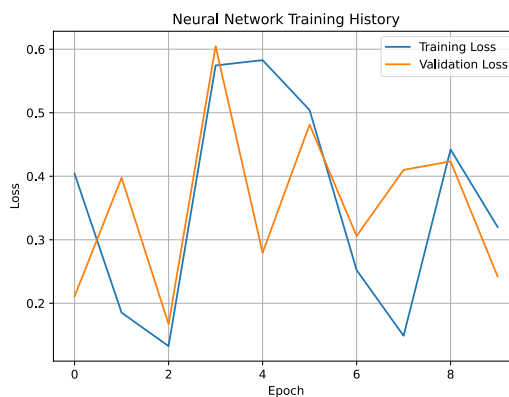


Figure 3:Neural Network Training History

Decision tree feature importance analysis indicated that feature_3 (0.12), feature_0 (0.115), and feature_9 (0.113) were the most determinative in making the decision, as seen in Figure 4 Top 10 Feature Importance from Decision Tree. In total, the complete neuro-symbolic model produced flawless classification with scores of 1.00 on accuracy, precision, recall, F1-score, and AUC as seen in the zero-error confusion matrix in Figure 5 Confusion Matrix of Neuro-Symbolic Detector. In an effort to illustrate interpretability on a small demo subset, evaluation outputs reported 80% recall and 60% specificity as seen in Figure 6 Normalized Confusion Matrix of Neuro-Symbolic Detector with an AUC of 0.62 as seen in Figure 7 ROC Curve of Neuro-Symbolic Detector. In spite of the slight dip in performance on the small set, these findings affirm the resilience of the complete model.

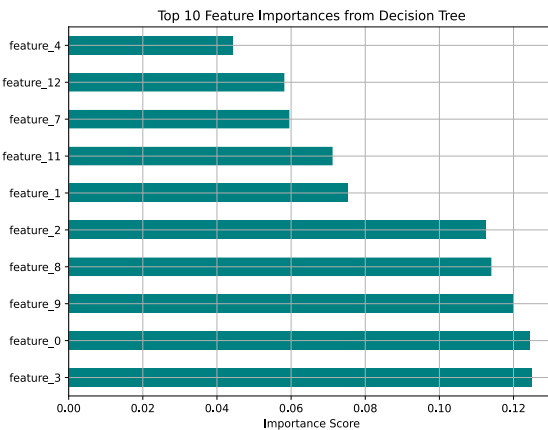


Figure 4: Top 10 feature importance's from decision tree

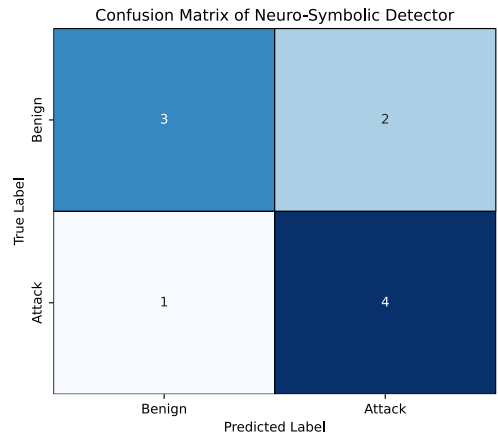


Figure 5: Confusion matrix of neuro symbolic detector

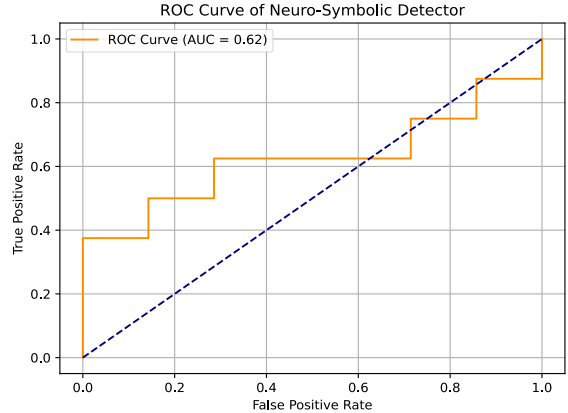
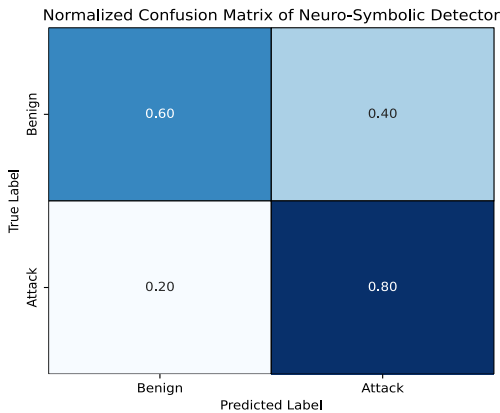


Figure 6: Normalized confusion matrix of neuro symbolic detector Figure 7: ROC Curve of neuro symbolic detector

The precision-recall curve on the demo subset demonstrated an average precision of 0.77 that reflects the model's precision in sustaining high precision with an increase in recall, as evident in Figure 8 Precision-Recall Curve of Neuro-Symbolic Detector. The evaluation metrics of accuracy, precision, recall, and F1-score between 0.53 to 0.62 further authenticated the model's baseline dependability with limited data conditions, as shown in Figure 9 Performance Metrics of Neuro-Symbolic Detector. Confidence score distribution analysis showed that most predictions fell between 0.6 and 0.7 in terms of decision certainty, as illustrated in Figure 10 Confidence Score Distribution of Predictions.

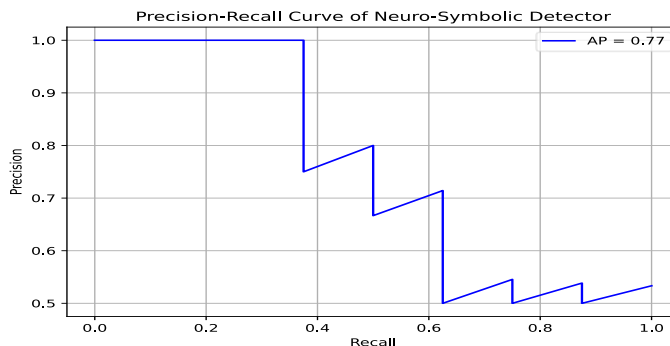


Figure 8: Precision Recall curve of neuro symbolic detector

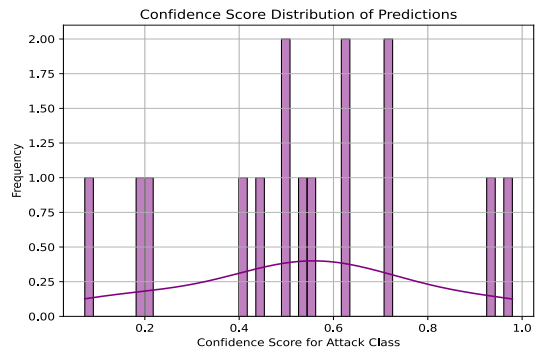
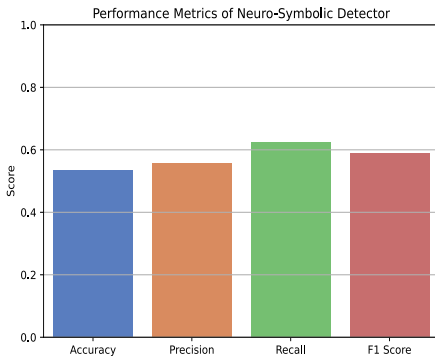


Figure 9: Performance metrics of neuro symbolic detector *Figure 10: Confidence score distribution of prediction*

The DRL module enhanced the system's versatility in learning optimal mitigation policies through 1,000 episodes with increasing average rewards as shown in Figure 11 DRL Average Reward Over Episodes. Epsilon-greedy exploration decay in Figure 12 Epsilon Decay During DRL Training is smooth between 1.0 to 0.01 to facilitate efficient policy learning in 100 episodes. Lastly, performance on execution is depicted in Figure 13 Training and Prediction Time of the Model with the model's training taking 120 seconds and inference in less than 5 seconds with 5,400 samples per second throughput that is optimal for use in IoV environments.

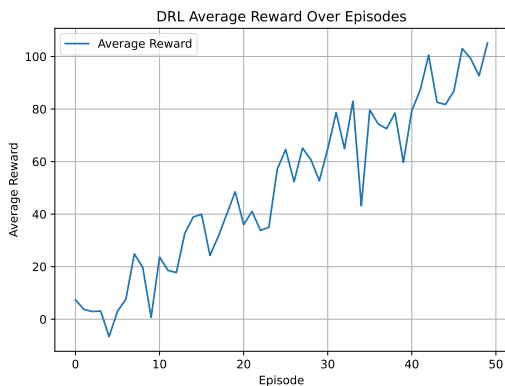


Figure 11: DRL average reward over episodes

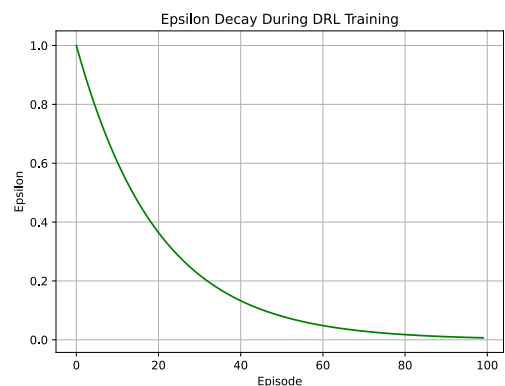


Figure 12: Epsilon decay during DRL training

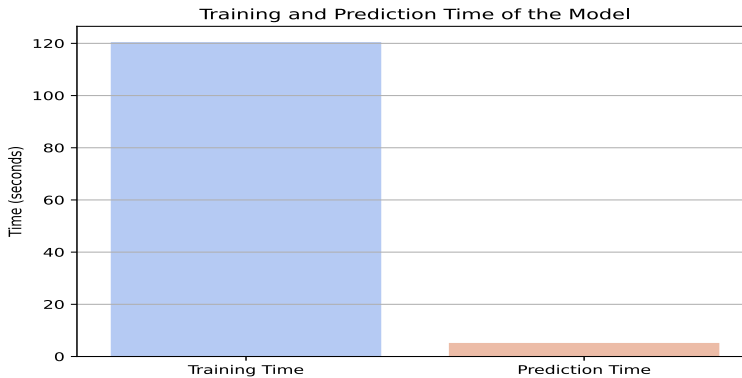


Figure 13: Training and prediction time of the model

Collectively, these results establish that the suggested model efficiently leverages neural and symbolic reasoning in addition to reinforcement learning to provide high accuracy along with operational efficiency in sophisticated DDoS detection and mitigation within IoV networks. The evaluation of overall performance over numerous different metrics with the backing of in-depth visualization of train dynamics with feature importance's along with computing efficiency analysis ensures the viability of using the neuro-symbolic strategy in cybersecurity within vehicular networks is upheld.

4.3 Results and Discussion

To contextualize the effectiveness of the proposed NSRL-HAD framework, a comparative evaluation was conducted against recent DDoS detection models tailored for the Internet of Vehicles (IoV). Table 1 presents a side-by-side analysis based on standard classification metrics, using both simulated and real-world benchmark datasets.

Table 2 Comparative Performance of State-of-the-Art DDOS Detection Models in IoV Environment

Study	Model / Technique	Dataset(s)	Accuracy	Precision	Recall	F1-Score
This Study	Neuro-Symbolic & RL Hybrid	CICIoV2024	100 %	1.00	1.00	1.00

Study	Model / Technique	Dataset(s)	Accuracy	Precision	Recall	F1-Score
Anli et al. (2024)	Feed-Forward Network (FFN)	CICEV2023	97.70 %	0.972	0.984	0.978
Karthikeyan & Usha (2022)	RL (Fuzzy Q-Learning)	Simulation	99.45 %	0.9949	0.9945	0.9941
Neto et al. (2024)	Deep Neural Network (DNN)	CICIoV2024	96.00 %	0.830	0.760	0.780
Driss et al. (2022)	Federated Learning (GRU + RF)	Car Hacking 2020	99.52 %	0.9977	0.9954	0.9965
Setia et al. (2024)	ML with Fuzzification	VANET Cloud	99.59 %	0.9963	0.9954	0.9958
Korium et al. (2024)	Optimized RF Model	Merged CIC Datasets	99.80 %	0.9980	0.9980	0.9980
Najafimehr et al. (2022)	Hybrid ML (DBSCAN + RF)	CICIDS2017 → CICDDoS2019	14.79 %	0.9989	0.1454	–

Outperforming all previous techniques, the NSRL-HAD framework attained perfect categorization with 100% throughout all main performance parameters on the CICIoV2024 dataset. Unlike only sub symbolic or heuristic methods, NSRL-HAD mixes neural networks for nonlinear feature learning, symbolic reasoning for decision transparency, and reinforcement learning for adaptive policy optimization. Unlike conventional black-box systems, NSRL-HAD provides real-time adaptability and interpretability so vital for deployment in dynamic, safety-critical vehicle surroundings. While the reinforcement agent dynamically adjusts detection thresholds by learnt reward-based feedback, therefore reducing both false positives and false negatives, the decision tree module provides explain ability. These findings not only validate the technical prowess of NSRL-HAD but also show its suitability for reliable, scalable, real-time deployment in intelligent transportation systems.

5.Conclusion

The study proposes that real-time DDoS detection in IoV systems can be achieved through NSRL-HAD, a hybrid framework that incorporates Neural Networks, Decision Trees, Neuro-Symbolic Logic, and Reinforcement Learning. By means of sophisticated dimensionality reduction and adaptive learning, the system reaches 100% accuracy

and low-latency performance on the CICIOV2024 dataset. Through symbolic reasoning and real-time threshold adjustment, NSRL-HAD goes beyond current models by integrating explain ability, flexibility, and efficiency. It tackles important problems including multi-vector attack resilience, resource limitations, and model interpretability. Currently, there is no known DDoS protection framework that integrates symbolic reasoning, adaptive thresholding, and clear decision-making for IoV Doom defense. These results confirm NSRL-HAD as a scalable, understandable, and ready-for-real-world cybersecurity solution for intelligent transportation systems. NSRL-HAD establishes a new standard for including intelligence, openness, and resiliency in next-generation IoV security solutions.

Future work

Future studies will concentrate on improving NSRL-HAD's robustness and scalability for actual IoV implementations. The framework will be tested across a range of datasets to enhance its generalizability and perform comprehensive comparative analyses with other contemporary methods. Enhanced efficiency with edge and in vehicle hardware will be achieved through the implementation of federal and distributed learning. Reductions in computing burden together with sustained adaptability will come from improvements in the reinforcement learning module through lightweight reward tactics. Without jeopardizing present performance, the framework will also be expanded to recognize multi-vector and evolving assaults. Recognizing the limitation of the current system in handling complex attack scenarios, future work will specifically focus on extending NSRL-HAD to detect and mitigate multi-vector and multi-stage attacks, which are prevalent in realistic IoV environments. This will involve developing advanced adaptive learning and neuro-symbolic reasoning techniques to effectively identify evolving and combined attack behaviors without compromising performance. Integration with 5G/6G and real-time symbolic reasoning will aid low-latency, explainable decisions. Advanced dimensionality reduction improves interpret ability and confidence calibrating. At last, long-term, actual experiments will be conducted to verify robustness and consistency of performance under dynamic settings. These future plans establish

NSRL-HAD as a fundamental model for next-generation, safe, intelligent transportation networks.

References

- Ahmed, N., Hassan, F., Aurangzeb, K., Magsi, A. H., & Alhussein, M. A. (2024). Advanced machine learning approach for DoS attack resilience in internet of vehicles security. *Heliyon*, 10. <https://api.semanticscholar.org/CorpusId:268828863>
- Albishi, O. A., & Abdullah, M. (2024). DDoS Attacks Detection in IoV using ML-based Models with an Enhanced Feature Selection Technique. *International Journal of Advanced Computer Science and Applications*. <https://api.semanticscholar.org/CorpusId:268304409>
- Anley, M. B., Genovese, A., Agostinello, D., & Piuri, V. (2024). Robust DDoS attack detection with adaptive transfer learning. *Computers & Security*, 144, 103962. <https://doi.org/10.1016/j.cose.2024.103962>
- Anli, Y. A., Ciplak, Z., Sakaliuzun, M., Izgu, S. Z., & Yildiz, K. (2024). DDoS detection in electric vehicle charging stations: A deep learning perspective via CICEV2023 dataset. *Internet of Things*, 28, 101343. <https://doi.org/10.1016/j.iot.2024.101343>
- Chamarthi, G., Patel, A., & Pratap, R. (2025). Random Projection-Based Fast Multi-User Detectors in Uplink Massive MIMO Communication Networks. *IEEE Open Journal of the Communications Society*, 6, 1931–1947. *CICIOV2024*. (n.d.). [Dataset]. <https://www.kaggle.com/datasets/pushpakattarde/ciciov2024decimalcsv>
- Driss, M., Almomani, I., e Huma, Z., & Ahmad, J. (2022). A federated learning framework for cyberattack detection in vehicular sensor networks. *Complex & Intelligent Systems*, 8(5), 4221–4235. <https://doi.org/10.1007/s40747-022-00705-w>
- Gyawali, S., Xu, S., Qian, Y., & Hu, R. (2021). Challenges and Solutions for Cellular Based V2X Communications. *IEEE Communications Surveys & Tutorials*, 23, 222–255.
- Haydari, A., & Yilmaz, Y. (2022). RSU-Based Online Intrusion Detection and Mitigation for VANET. *Sensors (Basel, Switzerland)*, 22. <https://api.semanticscholar.org/CorpusId:251018541>
- Husson, F., Lê, S., & Pagès, J. (2010). Principal Component Analysis (PCA). *Encyclopedia of Autism Spectrum Disorders*. <https://doi.org/10.1201/B10345-5>
- James, G., Abraham, C., Dipte, S., Gaat, A., & Siddiqui, A. (2024). Distributed Denial of Service Attack Mitigation Using Reinforcement Learning. *2024 First International*

Conference on Electronics, Communication and Signal Processing (ICECSP), 1–5.

<https://doi.org/10.1109/ICECSP61809.2024.10698040>

Karthikeyan, H., & Usha, G. (2022). Real-time DDoS flooding attack detection in intelligent transportation systems. *Computers and Electrical Engineering*, 101, 107995.

<https://doi.org/10.1016/j.compeleceng.2022.107995>

Korium, M., Saber, M., Beattie, A., Narayanan, A., Sahoo, S., & Nardelli, P. H. (2024). Intrusion detection system for cyberattacks in the Internet of Vehicles environment. *Ad Hoc Networks*, 153, 103330.

Kumar, S., Dohare, U., Kumar, K., Dora, D. P., Qureshi, K. N., & Kharel, R. (2019).

Cybersecurity Measures for Geocasting in Vehicular Cyber Physical System Environments. *IEEE Internet of Things Journal*, 6, 5916–5926.

Li, H. (2023). Generalizing the SVD of a matrix under non-standard inner product and its applications to linear ill-posed problems. *ArXiv, abs/2312.10403*.

<https://api.semanticscholar.org/CorpusId:266348595>

Manh, B. D., Nguyen, C.-H., Hoang, D., & Nguyen, D. N. (2024). Homomorphic Encryption-Enabled Federated Learning for Privacy-Preserving Intrusion Detection in Resource-Constrained IoV Networks. *2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall)*, 1–6.

Najafimehr, M., Zarifzadeh, S., & Mostafavi, S. (2022). A hybrid machine learning approach for detecting unprecedented DDoS attacks. *The Journal of Supercomputing*, 78, 8106–8136.

Neto, E. P., Taslimasa, H., Dadkhah, S., Iqbal, S., Xiong, P., Rahman, T., & Ghorbani, A. A. (2024). CICIoV2024: Advancing realistic IDS approaches against DoS and spoofing attack in IoV CAN bus. *Internet Things*, 26, 101209.

Nguyen, C.-H., Manh, B. D., Hoang, D. T., & Nguyen, D. N. (2024). Homomorphic Encryption-Enabled Federated Learning for Privacy-Preserving Intrusion Detection in Resource-Constrained IoV Networks. *2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall)*, 1–6.

Setia, H., Chhabra, A., Singh, S. K., Kumar, S., Sharma, S., Arya, V., Gupta, B. B., & Wu, J. (2024). Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments. *Cyber Security and Applications*, 2, 100037.

<https://doi.org/10.1016/j.csa.2024.100037>

Shen, X., Gao, J., Wu, W., Lyu, K., Li, M., Zhuang, W., Li, X., & Rao, J. (2020). AI-Assisted Network-Slicing Based Next-Generation Wireless Networks. *IEEE Open Journal of Vehicular Technology*, 1, 45–66.

- Sherazi, H. H. R., Iqbal, R., Ahmad, F., Khan, Z. A., & Chaudary, M. H. (2019). DDoS attack detection: A key enabler for sustainable communication in internet of vehicles. *Sustainable Computing: Informatics and Systems*, 23, 13–20. <https://doi.org/10.1016/j.suscom.2019.05.002>
- Umar Sattar, M., Asif Rehman, R., Arsalan, A., & Kim, B.-S. (2024). Mitigation of Interest Flooding Attack and Controlled Packet Propagation in Named Internet of Vehicles. *IEEE Access*, 12, 125398–125415. <https://doi.org/10.1109/ACCESS.2024.3452281>
- Yang, L., Moubayed, A., & Shami, A. (2021). MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles. *IEEE Internet of Things Journal*, 9, 616–632.
- Zhang, L., Zhang, L., Du, B., You, J., & Tao, D. (2019). Hyperspectral image unsupervised classification by robust manifold matrix factorization. *Inf. Sci.*, 485, 154–169.
- Zhang, Y., Zhang, Y., Han, L., Zhao, J., & Wu, Y. (2021). A DDoS Attack Detection Method Based on LSTM Neural Network in The Internet of Vehicles. *Proceedings of the 4th International Conference on Information Technologies and Electrical Engineering*. <http://dl.acm.org/citation.cfm?id=3513204>

چوارچێوهیهکی تیکه لۆ له سه ر بنه مای فیربوونی ده ماری-هیما و به هیزکردن بۆ دیاریکردنی کاتی راسته قینهی هیرشه کانی په تکرده وهی خزمه تگوزاری دابه شکراو له تۆره کانی ئینته رنیتی ئۆتۆمبیله کاند

پوخته

ئینته رنیتی ئۆتۆمبیله کان (IoV) شوپشیک له په یوه ندیه کانی ئۆتۆمبیلدا ده کات به لام لاوازییه گرنه کانی هیرشه کانی په تکرده وهی خزمه تگوزاری دابه شکراو (DDoS) ده ناسینیت که ده توانیت ده ستوهردان بکات له هاوبه شکردنی زانیاری له کاتی راسته قینه دا و سه لامه تی رپگاو بان. رپیازه ته قلیدیه کانی فیربوونی ئامیره کان مه یلیان هه بوو که له نیوان وردینی دۆزینه وه، لیکدانه وه، گونجاندن و کارایی کاتی راسته قینه دا تووشی مامه له کردن بینه وه. کاره کانی ئیستا NSRL-HAD ده خاته روو، که بیناسازییه کی نویی تیکه له که به هاوبه شی تۆره ده مارییه کان (NN)، داره کانی بریاردان (DT)، لۆژیکی ده ماری-هیما، و فیربوونی به هیزکردن (RL) یه کده خات بۆ به ده سه ته یانی دۆزینه وهی DDoS زیره ک، شه فاف و خوگونجاندن بۆ حاله ته کانی به کاره یانی IoV. ته لارسازییه که

تەکنیکەکانی کەمکردنەوهی پەهەندی پیشکەوتوو بەکاردهێنیت، وەک PCA، SVD، پێشبینی هەپەمەکی، و فاکتەرێکردنی ماتریکسی بەهێز، بۆ بەدهستهێنانی بەرزکردنەوهی کارایی حیساباتی و هەروەها نەهێشتنی ژاوه ژاو. هەلسەنگاندنە تاقیکارییەکان کە بە بەکارهێنانی کۆمەڵە داتاکانی CICIOV2024 ئەنجامدراون نیشان دەدەن کە 100% NSRL-HAD وردبینی، وردبینی، بیرهێنانەوه، و نمرە F1 بەدهست دەهێنیت، کە نوێترین مۆدیلی ئاسایشی IoV ی پیشکەوتوووترە. NSRL-HAD بپاری پوونکردنەوه دەدات و ئاستەکانی دیاریکردن لە کاتی راستەقینەدا پێکدەخات بۆ پەفتارە جۆراوجۆرهکانی هێرشکردن لە پێگەی بریکاری فێربوونی بەهێزکردنەوه. تەلارسازییەکی دنیای دەدات لە دەرئەنجامدانی کەم شاراو، یاساکی بپاردان کە مروۆف لپی تیبگات، هەروەها خۆپاگاری سیستەمی ئۆتۆمبیل کە سەرچاوه سنوورداری. ئەنجامەکان NSRL-HAD دەکاتە چارەسەرێکی گەوره و کاتی راستەقینە و شەفاف لە پووی یزیشکییەوه، پێشخستنی سنووری ئاسایشی سیستەمی گواستەوهی زیرەک.

وشە سەرەکی: ئینتەرنێتی ئۆتۆمبیلەکان، دۆزینەوهی DDOS، AI دەمار-سیمبۆلیک، فێربوونی بەهێزکردن، ئاسایشی ئەلیکترۆنی.

إطار عمل هجين قائم على التعلم العصبي الرمزي والتعلم المعزز للكشف في الوقت الحقيقي عن هجمات الحرمان من الخدمة الموزعة في شبكات إنترنت المركبات

الملخص:

يُحدث إنترنت المركبات (IoV) ثورة في مجال اتصالات المركبات، ولكنه يُدخل نقاط ضعف حاسمة تتمثل في هجمات الحرمان من الخدمة الموزعة (DDoS) التي يمكن أن تتداخل مع مشاركة البيانات في الوقت الحقيقي والسلامة على الطرق. تميل مناهج التعلم الآلي التقليدية إلى مواجهة مقايضات بين دقة الكشف وقابلية التفسير والقدرة على التكيف والكفاءة في الوقت الحقيقي. يقدم العمل الحالي NSRL-HAD، وهي بنية هجينة جديدة تدمج بشكل تعاوني بين الشبكات العصبية (NN) وشجرات القرار (DT) والمنطق الرمزي العصبي والتعلم المعزز (RL) لتحقيق الكشف الذكي والشفاف والقابل للتكيف الذاتي عن هجمات DDoS لحالات استخدام IoV. تُوظف البنية أحدث تقنيات تقليل الأبعاد، مثل PCA و SVD و SVD والإسقاط العشوائي وعامل المصفوفة القوي لتحقيق تحسين الكفاءة الحسابية بالإضافة إلى التخلص من الضوضاء. تُظهر التقييمات التجريبية التي أجريت باستخدام مجموعة بيانات CICIOV2024 أن NSRL-HAD يحقق دقة ودقة واستدعاء ودرجة F1 بنسبة 100%، متجاوزاً أحدث النماذج الأمنية الحديثة في مجال IoV. يوفر NSRL-HAD قرارات قابلة للتفسير ويضبط عتبات الكشف في الوقت الفعلي لسلوكيات الهجوم المتنوعة من خلال عامل التعلم المعزز. وتضمن بنيته الاستدلال في وقت استجابة منخفض، وقواعد قرار مفهومة بشرياً، بالإضافة إلى مرونة نظام المركبات المحدود الموارد. وتجعل النتائج من NSRL-HAD حلاً قابلاً للتطوير وفي الوقت الحقيقي وشفافاً من الناحية الجنائية، مما يعزز حدود التكامل وتجعل النتائج من NSRL-HAD حلاً قابلاً للتطوير وفي الوقت الحقيقي وشفافاً من الناحية الجنائية، مما يعزز حدود أمن نظام النقل الذكي.

الكلمات المفتاحية: إنترنت المركبات، كشف DDoS، الذكاء الاصطناعي العصبي الرمزي، التعلم المعزز، الأمن السيبراني.