NSS

Neutrosophic Sets and Systems, Vol. 87, 2025

University of New Mexico

Neutrosophic Set and Machine Learning Models for Detection of DoS Attack Resilience

Ahmad M. Nagm[1,2], Mamdouh Gomaa[3], Rabih Sbera[4], Darin shafek[5], Ahmed A El-Douh[6,7], Ahmed Abdelhafeez[7,8], Ahmed E Fakhry[3,8]

[1]Department of Computer Engineering and Electronics, Cairo Higher Institute for Engineering, Computer Science and Management, Cairo 11477, Egypt

[2]Computer Science Department, Future Academy-Higher Future Institute for Specialized Technological Studies, Cairo, 3044, Egypt

[3]Department of Computer Science, Faculty of Information Technology, Amman Arab University, 11953, Amman, Jordan

[4]Computer Engineering Techniques Department, College of Engineering Technology, Ashur University, Baghdad, Iraq

[5]Computer Engineering Techniques Department, Alma'moon University College, Baghdad, Iraq

[6]Information Systems Department, Faculty of Information Systems and Computer Science, October 6 University, Giza, 12585, Egypt

[7]Applied Science Research Center. Applied Science Private University, Amman, Jordan

[8]Computer Science Department, Faculty of Information Systems and Computer Science, October 6 University, Giza, 12585, Egypt

Abstract: Security has been a major problem in in-vehicle networks (VNs) in recent years, assaults that broadcast a deluge of packets, including Denial of Service (DoS) and Distributed Denial of Service (DDoS) assaults, might put the network at risk. Consequently, malicious traffic is clogging the network's resources. In this regard, the literature currently in publication has offered several strategies for dealing with DoS and DDoS attacks. In contrast to the conventional methods, this work uses machine learning (ML) to suggest an intelligent intrusion detection system (IDS). To mitigate DDoS assaults, the suggested IDS makes use of an application layer dataset that is openly accessible. Then we use the neutrosophic set model to select the best ML model under different evaluation matrices. The MABAC method is used to select the best model. A neutrosophic set is used to overcome uncertainty information.

Our method's experimental validation involves a thorough assessment of various machine learning models, including naïve Bayes (NB), decision trees (DT), and random forests (RF). Surprisingly, the average system accuracy of 0.99 obtained from the combined accuracy of these models outperforms current techniques. In contrast to traditional methods, our proposed IDS is highly effective and performs well in identifying DoS and DDoS attacks in VN.

Keywords: Neutrosophic Set; Uncertainty; Vehicle Networks; Machine Learning; Denial of Service (DoS); Distributed Denial of Service (DDoS).

1. Introduction

Unquestionably, wireless communication has improved recently because of the rapid improvements in technology, particularly in Vehicular Ad hoc Networks (VNs). By 2023 and beyond, 66% of people worldwide will have internet connectivity, according to a recent prediction by Cisco.[1]. This translates to 5.3 billion Internet users worldwide. The average number of networked devices per person is also expected to expand, according to the research, from 2.4 devices per capita in 2018 to 3.6 devices per capita by 2023 and beyond. Vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) connections exist between cars, much like they do with cell phones, household appliances, and televisions.[2], [3].

Through a wireless network, VN links the Transport Authority (TA), Internet, V2V, and V2I, facilitating smooth communication for improved road safety, data sharing, and real-time traffic monitoring. Strong processing, communication, and storage capacity are features of VN-enabled cars. These cars can exchange a variety of data, including entertainment services, traffic, and weather updates.[4], [5]. Roadside Units (RSUs) and other permanent infrastructures let the VN create vehicle connections in addition to cars.

The strong security of cars in the face of changing cyber threats and vulnerabilities remains a big concern, despite the enormous characteristics of VN, such as improved vehicle communication, decreased traffic congestion, and increased road safety.[6], [7]. The current VN is extremely susceptible to several security risks, including Distributed DoS (DDoS) and Denial of Service (DoS) attacks.

The suggested study lessens VN DoS threats. DoS attacks are used to stop or crash network performance by spreading a torrent of malicious or repetitive data. An excessive number of packets from attacker nodes are introduced by this storm of malicious data, which causes anomalous traffic. DoS attacks are primarily motivated by the desire to undermine the availability of network resources, which results in service disruptions.[8]. VN service delays are made worse by redundant packets sent by an attacker node. DDoS assaults, on the other hand, comprise several coordinated requests intended at degrading the network's efficiency of the network.

However, there is already literature that mentions a DDoS attack detection system that is based on Machine Learning (ML)[9], [10]. This study makes use of an ML-based DOS/DDoS attack detection system at the application layer in VN, in contrast to conventional and insufficient alternatives. ML models are applied in different fields.[11].

Since uncertainty frequently entails complications beyond membership and non-membership functions, a type-2 fuzzy set by itself might not be sufficient to manage all forms of doubt. In certain situations, considering the degree of indeterminacy is necessary when dealing with extremely complicated uncertainty. Some criteria may be appropriate while others may not be when choosing the best ML model[12], [13]. Furthermore, ML model selection is made uncertain by elements. We tackle this by combining the ideas of neutrosophic sets and type-2 fuzzy sets. T2NN was not included in the prior combinations of these sets by researchers. A neutrosophic set

is used to deal with uncertainty information[14], [15]. Neutrosophic set is applied in different application to solve vague problems[16], [17], [18].

To tackle the issue in this study, we use T2NN, which offers a more thorough handling of uncertainty by considering levels of indeterminacy, reluctance, and neglect. In comparison to a type-1 fuzzy set or a regular neutrosophic set, T2NN is also more capable of managing ambiguity in a variety of situations.[19].

2. Neutrosophic and Machine Learning Model

This section shows the steps of the neutrosophic and Machine Learning Models to rank models and select the best one. We show definitions of type-2 neutrosophic set (T2NS) in this part[12], [19]. We show the operations of two type-2 neutrosophic numbers such as:

$$H_1 = \left(\left(T_{T_{H_1}}(R), T_{I_{H_1}}(R), T_{F_{H_1}}(R)\right), \left(I_{T_{H_1}}(R), I_{I_{H_1}}(R), I_{F_{H_1}}(R)\right), \left(F_{T_{H_1}}(R), F_{I_{H_1}}(R), F_{F_{H_1}}(R)\right)\right) \quad H_2 = \left(\left(T_{T_{H_2}}(R), T_{I_{H_2}}(R), T_{F_{H_2}}(R)\right), \left(I_{T_{H_2}}(R), I_{I_{H_2}}(R), I_{F_{H_2}}(R)\right), \left(F_{T_{H_2}}(R), F_{I_{H_2}}(R), F_{F_{H_2}}(R)\right)\right)$$

$$H_1 \oplus H_2 = \begin{pmatrix} \begin{pmatrix} T_{T_{H_1}}(R) + T_{T_{H_2}}(R) - T_{T_{H_1}}(R)T_{T_{H_2}}(R), \\ T_{I_{H_1}}(R) + T_{I_{H_2}}(R) - T_{I_{H_1}}(R)T_{I_{H_2}}(R), \\ T_{F_{H_1}}(R) + T_{F_{H_2}}(R) - T_{F_{H_1}}(R)T_{F_{H_2}}(R) \end{pmatrix}, \\ \left(I_{T_{H_1}}(R)I_{T_{H_2}}(R), I_{I_{H_1}}(R)I_{I_{H_2}}(R), I_{F_{H_1}}(R)I_{F_{H_2}}(R)\right), \\ \left(F_{T_{H_1}}(R)F_{T_{H_2}}(R), F_{I_{H_1}}(R)F_{I_{H_2}}(R), F_{F_{H_1}}(R)F_{F_{H_2}}(R)\right) \end{pmatrix} \tag{1}$$

$$H_1 \otimes H_2 = \begin{pmatrix} \left(T_{T_{H_1}}(R)T_{T_{H_2}}(R), T_{I_{H_1}}(R)T_{I_{H_2}}(R), T_{F_{H_1}}(R)T_{F_{H_2}}(R)\right), \\ \begin{pmatrix} I_{T_{H_1}}(R) + I_{T_{H_2}}(R) - I_{T_{H_1}}(R)I_{T_{H_2}}(R), \\ I_{I_{H_1}}(R) + I_{I_{H_2}}(R) - I_{I_{H_1}}(R)I_{I_{H_2}}(R), \\ I_{F_{H_1}}(R) + I_{F_{H_2}}(R) - I_{F_{H_1}}(R)I_{F_{H_2}}(R) \end{pmatrix}, \\ \begin{pmatrix} F_{T_{H_1}}(R) + F_{T_{H_2}}(R) - F_{T_{H_1}}(R)F_{T_{H_2}}(R), \\ F_{I_{H_1}}(R) + F_{I_{H_2}}(R) - F_{I_{H_1}}(R)F_{I_{H_2}}(R), \\ F_{F_{H_1}}(R) + F_{F_{H_2}}(R) - F_{F_{H_1}}(R)F_{F_{H_2}}(R) \end{pmatrix} \end{pmatrix} \tag{2}$$

$$\curlywedge H_1 = \begin{pmatrix} \begin{pmatrix} \left(1 - \left(1 - T_{T_{H_1}}(R)\right)^{\curlywedge}\right), \\ \left(1 - \left(1 - T_{I_{H_1}}(R)\right)^{\curlywedge}\right), \\ \left(1 - \left(1 - T_{F_{H_1}}(R)\right)^{\curlywedge}\right) \end{pmatrix}, \\ \left(\left(I_{T_{H_1}}(R)\right)^{\curlywedge}, \left(I_{I_{H_1}}(R)\right)^{\curlywedge}, \left(I_{F_{H_1}}(R)\right)^{\curlywedge}\right), \\ \left(\left(F_{T_{H_1}}(R)\right)^{\curlywedge}, \left(F_{I_{H_1}}(R)\right)^{\curlywedge}, \left(F_{F_{H_1}}(R)\right)^{\curlywedge}\right) \end{pmatrix} \tag{3}$$

$$H_1^{\wedge} = \begin{pmatrix} \left(\left(T_{T_{H_1}}(R)\right)^{\wedge}, \left(T_{I_{H_1}}(R)\right)^{\wedge}, \left(T_{F_{H_1}}(R)\right)^{\wedge}\right), \\ \left(\begin{pmatrix} \left(1-\left(1-I_{T_{H_1}}(R)\right)^{\wedge}\right), \\ \left(1-\left(1-I_{I_{H_1}}(R)\right)^{\wedge}\right), \\ \left(1-\left(1-I_{F_{H_1}}(R)\right)^{\wedge}\right) \end{pmatrix}, \\ \begin{pmatrix} \left(1-\left(1-F_{T_{H_1}}(R)\right)^{\wedge}\right), \\ \left(1-\left(1-F_{I_{H_1}}(R)\right)^{\wedge}\right), \\ \left(1-\left(1-F_{F_{H_1}}(R)\right)^{\wedge}\right) \end{pmatrix} \end{pmatrix} \quad (4)$$

We show the steps of the MABAC method to rank the alternatives. Experts use T2NNs to evaluate criteria and alternatives and compute the criteria weights using the average method.

Normalize the decision matrix.

$$y_{ij} = \frac{x_{ij} - \min x_i}{\max x_i - \min x_i} \quad (5)$$

$$y_{ij} = \frac{x_{ij} - \max x_i}{\min x_i - \max x_i} \quad (6)$$

obtain the weighted decision matrix.

$$q_{ij} = w_j + w_j y_{ij} \quad (7)$$

Obtain the border approximation area.

$$T_j = \left(\prod_{i=1}^{m} q_{ij}\right)^{\frac{1}{m}} \quad (8)$$

Obtain the distance.

$$D_{ij} = q_{ij} - T_i \quad (9)$$

Obtain the total distance.

$$U_i = \sum_{j=1}^{n} D_{ij} \quad (10)$$

We have selected the " DoS attack dataset," which looks at DoS assaults at the application layer that were gathered from Kaggle. There were 809,361 entries and seventy-eight characteristics in the collection. Based on network analysis, the data was separated into three groups: DDOS Hulk assaults, DOS slow Loris attacks, and benign traffic, which is legal traffic. To develop effective defenses, the study sought to recognize and understand the characteristics of these attacks. Figure 1 shows the distribution of the dataset.

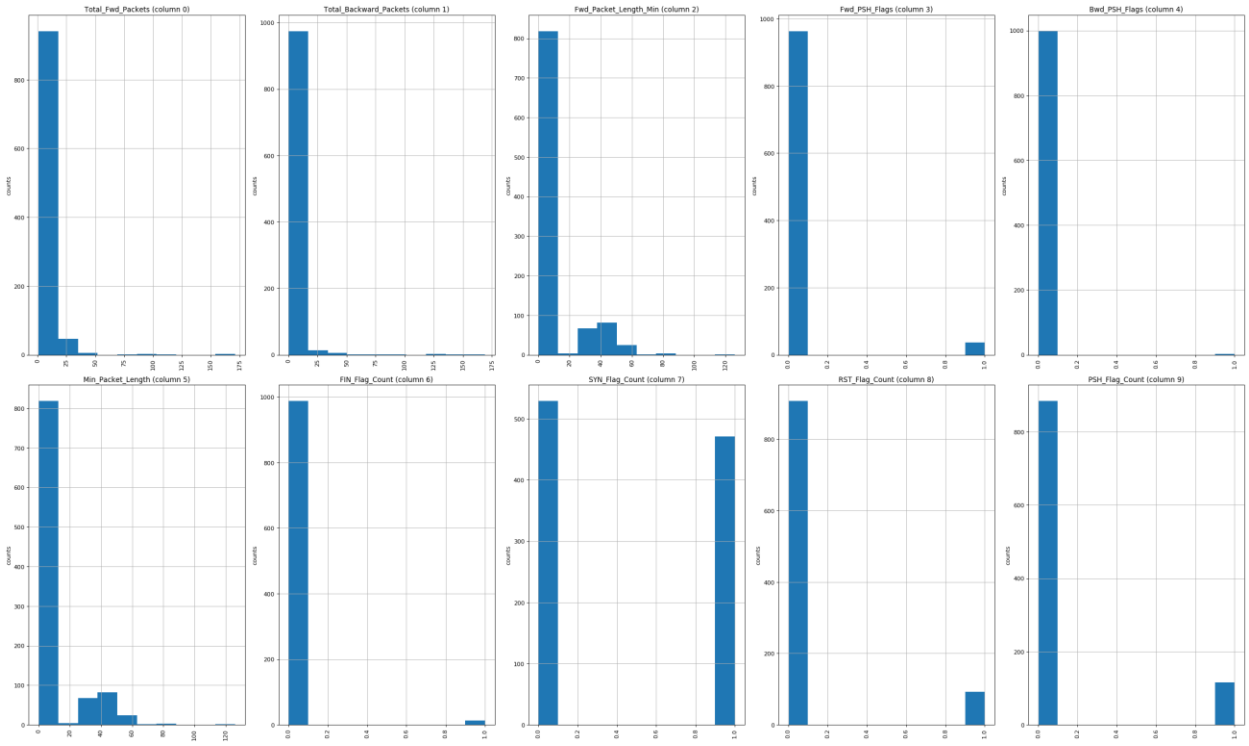

Figure 1. Distribution of criteria of the dataset.

A key component of machine learning is data preparation, which entails locating important characteristics in the dataset for the ML model's training. ML models can enhance performance by choosing pertinent characteristics. The dataset for the ML-based model has been selected, and we have now prepared it with feature extraction. The dataset has been split into training (70%) and testing (30%). To improve the learning process and teach the machine to get the best accuracy after deciding, this study makes use of feature selection. The many ML-based classifiers, including naïve Bayes, decision trees, and random forest, utilize the following feature selection.

3. Results

In this work, we assessed an IDS's ability to identify DoS and DoS assaults on VNs using an ML model. To distinguish between benign and harmful outcomes, we used three machine learning models: naïve Bayes (NB), decision tree with different max depths such as 3,5,7,9,11, and 13 (DT), and random forest (RF).

A concise summary of the expected results based on the specified model is given by the confusion matrices and tables for each classifier. We assessed the classifiers' performance using accuracy, precision, recall, and f1-score. The outcomes showed that the classifiers' accuracy was increased. Table 1 shows the performance of each classifier.

Table 1. Performance of different classifiers.

	Accuracy	Precision	Recall	F1-Score

NB	0.948188	0.948188	0.948188	0.948188
DT with max depth =3	0.99682	0.99682	0.99682	0.99682
DT with max depth =5	0.99975	0.99975	0.99975	0.99975
DT with max depth =7	0.99996	0.99996	0.99996	0.99996
DT with max depth =9	0.99997	0.99997	0.99997	0.99997
DT with max depth =11	0.99996	0.99996	0.99996	0.99996
DT with max depth =13	0.99995	0.99995	0.99995	0.99995
RF	0.99997	0.99997	0.99997	0.99997

Then, we show the results of the neutrosophic model to show the best ML model. Three experts evaluate the criteria (performance matrices) and alternatives (different ML models) as shown in Table 2. Then we compute the criteria weights using the average method as: 0.251489674, 0.242510815, 0.244796343, and 0.261203167.

Table 2. Decision matrix.

	$DoSC_1$	$DoSC_2$	$DoSC_3$	$DoSC_4$
$DoSA_1$	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.35,0.35,0.10), (0.50,0.75,0.80), (0.50,0.75,0.65))	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))
$DoSA_2$	((0.70,0.75,0.80), (0.15,0.20,0.25), (0.10,0.15,0.20))	((0.95,0.90,0.95), (0.10,0.10,0.05), (0.05,0.05,0.05))	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.60,0.45,0.50), (0.20,0.15,0.25), (0.10,0.25,0.15))
$DoSA_3$	((0.60,0.45,0.50), (0.20,0.15,0.25), (0.10,0.25,0.15))	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))	((0.35,0.35,0.10), (0.50,0.75,0.80), (0.50,0.75,0.65))	((0.70,0.75,0.80), (0.15,0.20,0.25), (0.10,0.15,0.20))
$DoSA_4$	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))	((0.95,0.90,0.95), (0.10,0.10,0.05), (0.05,0.05,0.05))
$DoSA_5$	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))	((0.35,0.35,0.10), (0.50,0.75,0.80), (0.50,0.75,0.65))	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))
$DoSA_6$	((0.35,0.35,0.10), (0.50,0.75,0.80), (0.50,0.75,0.65))	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.60,0.45,0.50), (0.20,0.15,0.25), (0.10,0.25,0.15))	((0.35,0.35,0.10), (0.50,0.75,0.80), (0.50,0.75,0.65))
$DoSA_7$	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.95,0.90,0.95), (0.10,0.10,0.05), (0.05,0.05,0.05))	((0.70,0.75,0.80), (0.15,0.20,0.25), (0.10,0.15,0.20))	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))
$DoSA_8$	((0.95,0.90,0.95), (0.10,0.10,0.05), (0.05,0.05,0.05))	((0.70,0.75,0.80), (0.15,0.20,0.25), (0.10,0.15,0.20))	((0.60,0.45,0.50), (0.20,0.15,0.25), (0.10,0.25,0.15))	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))
	$DoSC_1$	$DoSC_2$	$DoSC_3$	$DoSC_4$
$DoSA_1$	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.35,0.35,0.10), (0.50,0.75,0.80), (0.50,0.75,0.65))	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))
$DoSA_2$	((0.70,0.75,0.80), (0.15,0.20,0.25), (0.10,0.15,0.20))	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.60,0.45,0.50), (0.20,0.15,0.25), (0.10,0.25,0.15))
$DoSA_3$	((0.60,0.45,0.50), (0.20,0.15,0.25), (0.10,0.25,0.15))	((0.70,0.75,0.80), (0.15,0.20,0.25), (0.10,0.15,0.20))	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.70,0.75,0.80), (0.15,0.20,0.25), (0.10,0.15,0.20))
$DoSA_4$	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))	((0.60,0.45,0.50), (0.20,0.15,0.25), (0.10,0.25,0.15))	((0.70,0.75,0.80), (0.15,0.20,0.25), (0.10,0.15,0.20))	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))
$DoSA_5$	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.70,0.75,0.80), (0.15,0.20,0.25), (0.10,0.15,0.20))
$DoSA_6$	((0.70,0.75,0.80), (0.15,0.20,0.25), (0.10,0.15,0.20))	((0.70,0.75,0.80), (0.15,0.20,0.25), (0.10,0.15,0.20))	((0.70,0.75,0.80), (0.15,0.20,0.25), (0.10,0.15,0.20))	((0.60,0.45,0.50), (0.20,0.15,0.25), (0.10,0.25,0.15))
$DoSA_7$	((0.60,0.45,0.50), (0.20,0.15,0.25), (0.10,0.25,0.15))	((0.60,0.45,0.50), (0.20,0.15,0.25), (0.10,0.25,0.15))	((0.60,0.45,0.50), (0.20,0.15,0.25), (0.10,0.25,0.15))	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))
$DoSA_8$	((0.95,0.90,0.95), (0.10,0.10,0.05), (0.05,0.05,0.05))	((0.70,0.75,0.80), (0.15,0.20,0.25), (0.10,0.15,0.20))	((0.60,0.45,0.50), (0.20,0.15,0.25), (0.10,0.25,0.15))	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))

	$DoSC_1$	$DoSC_2$	$DoSC_3$	$DoSC_4$
$DoSA_1$	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))
$DoSA_2$	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))	((0.60,0.45,0.50), (0.20,0.15,0.25), (0.10,0.25,0.15))
$DoSA_3$	((0.35,0.35,0.10), (0.50,0.75,0.80), (0.50,0.75,0.65))	((0.35,0.35,0.10), (0.50,0.75,0.80), (0.50,0.75,0.65))	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))
$DoSA_4$	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))
$DoSA_5$	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))
$DoSA_6$	((0.35,0.35,0.10), (0.50,0.75,0.80), (0.50,0.75,0.65))	((0.50,0.30,0.50), (0.50,0.35,0.45), (0.45,0.30,0.60))	((0.35,0.35,0.10), (0.50,0.75,0.80), (0.50,0.75,0.65))	((0.35,0.35,0.10), (0.50,0.75,0.80), (0.50,0.75,0.65))
$DoSA_7$	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.35,0.35,0.10), (0.50,0.75,0.80), (0.50,0.75,0.65))	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))
$DoSA_8$	((0.95,0.90,0.95), (0.10,0.10,0.05), (0.05,0.05,0.05))	((0.20,0.20,0.10), (0.65,0.80,0.85), (0.45,0.80,0.70))	((0.60,0.45,0.50), (0.20,0.15,0.25), (0.10,0.25,0.15))	((0.40,0.45,0.50), (0.40,0.45,0.50), (0.35,0.40,0.45))

Normalize the decision matrix using equations. (5 and 6) as shown in Table 3.

Obtain the weighted decision matrix using the equation. (7) as shown in Table 4.

Obtain the border approximation area using the equation. (8).

Obtain the distance using the equation. (9).

Obtain the total distance using eq. (10) as shown in Figure 2. The results show the DT with max depth = 9 is the best model by the neutrosophic model.

Table 3. Normalized decision matrix.

	$DoSC_1$	$DoSC_2$	$DoSC_3$	$DoSC_4$
$DoSA_1$	0	0.081731	0.507463	0.369458
$DoSA_2$	0.627635	0.706731	0	0.990148
$DoSA_3$	0.40281	0.649038	0.05597	1
$DoSA_4$	0.166276	0.451923	0.761194	0.487685
$DoSA_5$	0.156909	0	0.257463	0.325123
$DoSA_6$	0.229508	0.557692	0.723881	0.044335
$DoSA_7$	0.098361	1	0.660448	0
$DoSA_8$	1	0.875	1	0.369458

Tale 4. Weighted decision matrix.

	$DoSC_1$	$DoSC_2$	$DoSC_3$	$DoSC_4$
$DoSA_1$	0.25149	0.262331	0.369021	0.357707
$DoSA_2$	0.409333	0.413901	0.244796	0.519833
$DoSA_3$	0.352792	0.39991	0.258498	0.522406
$DoSA_4$	0.293306	0.352107	0.431134	0.388588
$DoSA_5$	0.290951	0.242511	0.307822	0.346126
$DoSA_6$	0.309209	0.377757	0.422	0.272784
$DoSA_7$	0.276226	0.485022	0.406472	0.261203

$DoSA_8$	0.502979	0.454708	0.489593	0.357707

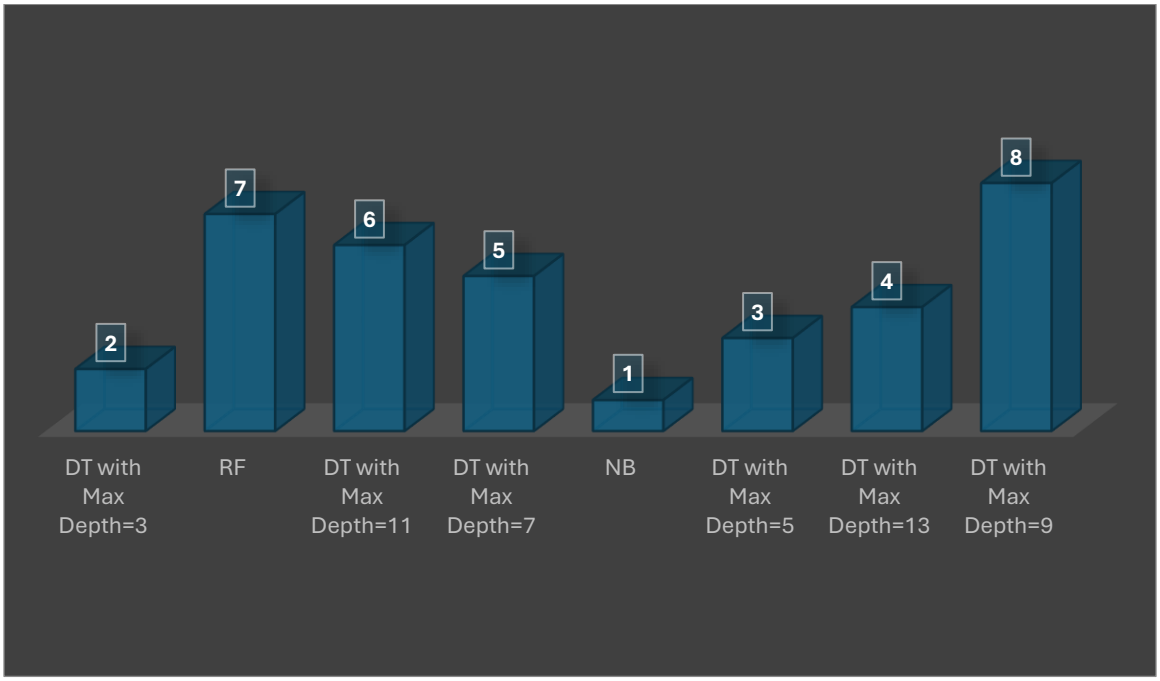

Figure 2. Rank of machine learning models.

4. Conclusions

This study presents an ML-based framework for the application layer of DoS and DDoS attack detection in VNs, given that DoS and DDoS assaults are susceptible to VNs. To increase the precision of identifying these assaults in our tests using the classifiers NB, DT, and RF. Using the combined characteristics, the classifier DT with max depth =9 produced the best results. These outcomes show how well the suggested system works to strengthen VN security against DoS and DDoS assaults.

This study used the type-2 neutrosophic set model to select the best ML model. The neutrosophic set is used to overcome the uncertainty. Three experts evaluate performance matrices and eight ML models. We used the MABAC method to select the best model. The results show the DT with max depth = 9 is the best.

Since Deep Learning (DL) classifiers may be assessed for further research, we can select the dataset that should be created based on the road network simulation results in subsequent work and examine the effects of various datasets with more classifiers. Additionally, the scope of this study is restricted to DOS/DDOS attack detection; future research might evaluate this further in terms of computing complexity and energy usage.

References

[1] N. Ahmed, F. Hassan, K. Aurangzeb, A. H. Magsi, and M. Alhussein, "Advanced machine learning approach for DoS attack resilience in internet of vehicles security," *Heliyon*, vol. 10, no. 8, 2024.

[2] P. S. Tadepalli, D. Pullaguram, and M. N. Alam, "Cyber-Resilient Strategy for DC Microgrids Against Concurrent FDI and DoS Attacks," *IEEE Trans. Ind. Informatics*, 2025.

[3] J. Dai, Y. Xu, Y. Wang, T.-L. Nguyen, and S. Dasgupta, "A cyber-resilience enhancement method for network controlled microgrid against denial of service attack," in *IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society*, IEEE, 2020, pp. 3511–3516.

[4] Z. Ju, H. Zhang, X. Li, X. Chen, J. Han, and M. Yang, "A survey on attack detection and resilience for connected and automated vehicles: From vehicle dynamics and control perspective," *IEEE Trans. Intell. Veh.*, vol. 7, no. 4, pp. 815–837, 2022.

[5] S. Hu, P. Yuan, D. Yue, C. Dou, Z. Cheng, and Y. Zhang, "Attack-resilient event-triggered controller design of DC microgrids under DoS attacks," *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 67, no. 2, pp. 699–710, 2019.

[6] H. Mokari, E. Firouzmand, I. Sharifi, and A. Doustmohammadi, "DoS attack detection and resilient control in platoon of smart vehicles," in *2021 9th RSI International Conference on Robotics and Mechatronics (ICRoM)*, IEEE, 2021, pp. 144–150.

[7] W. Yao, Y. Wang, Y. Xu, and C. Deng, "Cyber-resilient control of an islanded microgrid under latency attacks and random DoS attacks," *IEEE Trans. Ind. Informatics*, vol. 19, no. 4, pp. 5858–5869, 2022.

[8] H. Mokari, E. Firouzmand, I. Sharifi, and A. Doustmohammadi, "Resilient control strategy and attack detection on platooning of smart vehicles under DoS attack," *ISA Trans.*, vol. 144, pp. 51–60, 2024.

[9] R. Sihwail, K. Omar, K. A. Zainol Ariffin, and S. Al Afghani, "Malware detection approach based on artifacts in memory image and dynamic analysis," *Appl. Sci.*, vol. 9, no. 18, p. 3680, 2019.

[10] M. Shehab *et al.*, "Machine learning in medical applications: A review of state-of-the-art methods," *Comput. Biol. Med.*, vol. 145, p. 105458, 2022.

[11] R. Karim and M. I. Asjad, "Improving Equity in Healthcare: Machine Learning-Based Thyroid Disease Classification," *SciNexuses*, vol. 1, pp. 139–147, 2024.

[12] P. Singh, "A type-2 neutrosophic-entropy-fusion based multiple thresholding method for the brain tumor tissue structures segmentation," *Appl. Soft Comput.*, vol. 103, p. 107119, 2021.

[13] M. Abdel-Basset, N. N. Mostafa, K. M. Sallam, I. Elgendi, and K. Munasinghe, "Enhanced

COVID-19 X-ray image preprocessing schema using type-2 neutrosophic set," *Appl. Soft Comput.*, vol. 123, p. 108948, 2022.

[14] T. Fujita and F. Smarandache, "Pythagorean, Fermatean, and Complex Turiyam Neutrosophic Graphs," *SciNexuses*, vol. 2, pp. 39–63, 2025.

[15] V. Christianto and F. Smarandache, "Neutrosophic Logic Guide to Risk Management Especially Given Stable Pareto Distribution," *SciNexuses*, vol. 2, pp. 27–32, 2025.

[16] A. Hazaymeh, Y. Al-Qudah, F. Al-Sharqi, and A. Bataihah, "A novel Q-neutrosophic soft under interval matrix setting and its applications.," *Int. J. Neutrosophic Sci.*, vol. 25, no. 4, 2025.

[17] A. Bataihah, A. A Hazaymeh, Y. Al-Qudah, and F. Al-Sharqi, "Some fixed point theorems in complete neutrosophic metric spaces for neutrosophic ψ-quasi contractions," *Neutrosophic Sets Syst.*, vol. 82, no. 1, p. 1, 2025.

[18] E. Hussein *et al.*, "Matrices and Correlation Coefficient for possibility interval-valued neutrosophic hypersoft sets and their applications in real-life.," *Int. J. Neutrosophic Sci.*, vol. 26, no. 1, 2025.

[19] L. Shaw, S. K. Das, S. K. Roy, L. Sakalauskas, G.-W. Weber, and H. Dan, "Redistribution of humanitarian items in disaster management multi-period location–allocation problem under type-2 neutrosophic environment," *Appl. Soft Comput.*, p. 113217, 2025.

Received: March 1, 2025. Accepted: June 13, 2025