SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I8P102

Volume 12 Issue 8, 11-21, August 2025
© 2025 Seventh Sense Research Group®

Original Article

Adaptive Ship Rescue Optimization Enabled Deep Learning for Sybil Attack Detection with Secure Transmission in Urban VANET

Nitha C Velayudhan[1], Arun Pradeep[2], Mukesh Madanan[3]

[1]*Department of Computer Science & Engineering, Christ College Of Engineering, Kerala, India.*
[2]*Department of Electronics & Communication Engineering, Saveetha Engineering College, Tamil Nadu, India.*
[3]*Department of Computer Science, Dhofar University, Salalah, Oman.*

[2]*Corresponding Author : arunpradeep@msn.com*

Received: 01 June 2025 Revised: 03 July 2025 Accepted: 02 August 2025 Published: 30 August 2025

Abstract *- Future Road transportation is primarily reliant on connected vehicles. Moreover, the Intelligent Transportation Systems support road users through the utilization of Vehicular Ad hoc Networks (VANETs). The rogue node, termed a sybil node, transmits bogus signals to interrupt the system, impacting its security. However, the detection of a Sybil attack is complicated due to the dynamic nature of nodes and stability issues. Adaptive Ship Rescue Optimization-based Deep Kronecker Network (ASRO_DKN)-based Sybil attack detection is proposed to solve such an issue. The VANET simulation is initially carried out, and the Fractional Glowworm Swarm Optimization for Traffic Aware Routing (FGWSO-TAR) is performed. The Sybil attack is detected at the Base Station (BS), where the input data packet is applied to feature extraction, and the attack is detected by the Deep Kronecker Network (DKN). The hyperparameters of the DKN are tuned using the ASRO. The Precision, recall, and F-measure metrics are utilized to validate the ASRO_DKN-based Sybil attack detection in VANET, and the optimum values of 90.84%, 90.48%, and 90.13% are achieved.*

Keywords *- Vehicular Adhoc Networks, Sybil attack, Fractional Glowworm Swarm Optimization, Deep Kronecker Network, Ship Rescue Optimization.*

1. Introduction

Intelligent vehicles are revolutionizing modern transportation systems, offering increased safety, efficiency, and automation. These advancements rely heavily on real-time data exchange between vehicles and infrastructure, enabled by Vehicular Ad Hoc Networks (VANETs). VANETs are a crucial component of Intelligent Transportation Systems (ITS), supporting key applications such as dynamic route planning, information dissemination, safety alerts, and telemetry data sharing.

VANETs enable vehicles to communicate with one another and with Road Side Units (RSUs), enhancing road safety and traffic efficiency by broadcasting relevant contextual information. This interconnectivity contributes significantly to reducing traffic accidents and congestion. However, evaluating the performance of VANET routing and security protocols in real-world environments is often prohibitively expensive. As a result, most research depends on simulation-based evaluations to assess protocol effectiveness under various traffic and attack scenarios.

Despite their benefits, VANETs remain vulnerable to numerous security threats. The Sybil attack poses a serious risk, where a malicious vehicle generates multiple fake identities to mislead other vehicles or infrastructure systems. Such attacks can compromise safety-critical applications by creating false congestion reports, blocking traffic flow, or disrupting routing decisions.

Several conventional Machine Learning (ML) methods have been applied for Sybil attack detection. However, these approaches often fall short in handling high-dimensional and non-linear data patterns, which are common in real-time vehicular communication systems. Recent advances in Deep Learning (DL) show promise in overcoming these limitations, offering superior pattern recognition capabilities and improved detection accuracy. Specifically, models like Convolutional Neural Networks (CNNs) are well-suited for identifying complex patterns associated with security threats in VANETs.

Despite this, existing deep learning-based methods lack adaptive mechanisms to optimize model parameters efficiently, often resulting in sub-optimal performance or requiring significant manual tuning. Therefore, there is a pressing need for an intelligent, adaptive, and optimized deep learning method for Sybil attack detection in VANETs.

The research gap mentioned above is addressed in this study with a novel ASRO_DKN-based framework for Sybil attack detection, which integrates: Dynamic Kernel-based Network (DKN) for high-accuracy detection, and Adaptive Ship Rescue Optimization (ASRO) to fine-tune the DKN's hyperparameters for optimal performance. The key contributions of this paper are:

1.1. Development of ASRO_DKN Framework

A novel approach that combines Adaptive Ship Rescue Optimization (ASRO) with Dynamic Kernel-based Network (DKN) to detect Sybil attacks in VANETs.

1.2. Simulation and Validation

The VANET environment is simulated, and the proposed FGWSO-TAR method is used for traffic-aware routing, followed by ASRO_DKN-based attack detection.

1.3. Performance Improvement

The proposed method aims to enhance detection accuracy, reduce false positives, and achieve efficient parameter tuning in dynamic vehicular environments.

The remaining section of the paper is organized as follows: Sections 2 and 3 discuss the motivation and review existing works on attack detection in VANETs. Section 4 provides the design and implementation part of the ASRO_DKN model. Section 5 presents the experimental-based results and performance metrics, and the paper is concluded in Section 6 with future directions.

2. Motivation

Sybil attacks create more security threats in VANETs, in which malicious nodes create multiple identities to manipulate the performance of the network and disrupt communication. Thus, the detection of Sybil attacks is needed to provide VANETs with reliability.

3. Literature Survey

Rakhi, S. and Shobha, K.R., [1] devised the Longest Common Subsequence (LCS)-based Sybil attack detection in VANET. This model significantly improved the detection rate for variable vehicle counts. However, this model failed to integrate a mean-based change point finding to validate any rapid variations occurring in the Received Signal Strength Indicator (RSSI). Zhang, Z., et al. [2] developed the Basic Security Message (BSM) packets for detecting the Sybil attack. This model attained high detection accuracy and minimized the deployment cost. Still, it failed to include simpler and more effective detection approaches for attaining more precise outcomes. Azam, S., et al. [3] devised the Ensemble-based Majority Voting technique for the Sybil attack detection in VANET. It enabled multiple vehicles to share information and learning from each other. Still, the communication overhead leads to network congestion. Zhu, Y., et al. [4] developed the Beacon Packet-based Traceability mechanism for detecting the Sybil attack in VANET. It enhanced trust among vehicles and led to better coordination.

Nevertheless, the detection and traceability were resource-intensive and complex. Recent studies have taken varied approaches to enhance the security of VANETs, focusing on intelligent clustering, deep learning models, and trust-based mechanisms. Dalal et al. [16] proposed an integrated framework that combines the Self-Improved Kookaburra Optimization Algorithm with an enhanced LSTM model for intrusion detection, alongside Blowfish encryption to secure data transmission. Ajin et al. [17] developed a method using Adaptive Bald Eagle Search Optimization in conjunction with a multi-agent Deep Q Network, applying BIRCH clustering and an efficient cluster head selection strategy to improve detection of Sybil attacks. Kirubakaran et al. [18] introduced a secure communication model that incorporates Spatial Bayesian Neural Networks, optimized using a Fractional Order Water Flow algorithm, and protected by advanced encryption methods. Aledhari et al. [19] offered a comprehensive review of communication security in connected autonomous vehicles, outlining key attack types and proposing practical countermeasures. In a related effort, Balakumar et al. [20] designed a Multi-Dimensional Trust-based Data Dissemination mechanism aimed at addressing blackhole attacks by assessing multiple trust metrics within a DSR routing context. Collectively, these works reflect a growing shift toward adaptive, multi-layered security frameworks, aligning with the direction and contribution of the ASRO_DKN approach presented in this study.

3.1. Challenges

The challenges of existing techniques for Sybil attack detection in VANET are described below:

- The LCSS-based Sybil attack detection in [1] was computationally intensive, particularly in real-time utilization. Moreover, the execution of LCSS may lead to delays in detection.
- In [4], the Beacon Packet-based Traceability mechanism was complex because the mechanism failed as the count of connected vehicles was increased.
- VANETs are considered a dynamic topology with high mobility. Vehicles often move quickly in and out of communication ranges; hence, creating stable connections over time was difficult.

4. Proposed Adaptive Ship Rescue Optimization-based Deep Kronecker Network for Attack Detection in VANET

VANETs are considered a significant part of ITSs, increasing road safety and transport efficiency. VANETs facilitate rapid communication and information sharing. This capability is helpful for making roads safer for passengers. Still, vehicle communication is susceptible to many threats, which require robust safety measures for deploying the VANETs in ITS. The major threat to VANET is the Sybil attack. The Sybil attacks in VANETs reduce the trustworthiness of communications and disturb the traffic management systems. To tackle such complexity, an ASRO_DKN-based Sybil attack detection is developed. The VANET simulation is performed, and the FGWSO-TAR protocol [11] is employed for routing. The attack detection is done in the BS, where the required features are extracted. Sybil attack detection is implemented using the DKN [12], and its hyperparameters are trained using the ASRO. Figure 1 shows the block diagram of the proposed model.

4.1. Simulation in VANET

The simulation model [9] for VANET is shown in Figure 2. The entities, such as vehicles, Roadside Units (RSUs), and servers, are presented in the model. The primary component of the VANET is vehicles, which are linked to an Onboard Unit (OBU) to transmit and receive data by wireless links. Vehicle-to-Infrastructure (V2I) and Vehicle-To-Vehicle (V2V) are the major ways of communication. The RSU is connected alongside the roadside and is utilized as a medium between the vehicles and servers.

The server controls the movements of vehicles, and the environmental details are gathered from the vehicles. Afterwards, the vehicle details are transmitted to the application server to distribute a specific operation to the vehicles. Moreover, the OBU is used to capture the latitude and longitude of the Global Position Sensor (GPS). Lastly, the service providers are used to aggregate the data and control the driving instructions.

4.2. Routing Based on FGWSO-TAR

Routing is utilized to find the way data packets are transmitted across the V2V and V2I. In VANETs, the network topology varies quickly; hence, the data transmission is complex. Therefore, routing protocols are designed to adjust to the dynamic environment and effectively deliver the data. Here, the FGWSO-TAR system effectively carried out the routing.

4.2.1. Algorithmic steps for FGWSO

Step 1: Initialization

The parameters such as population member U, initial luciferin, radial range of search agents, the iteration Q, and the present iteration q, are initialized.

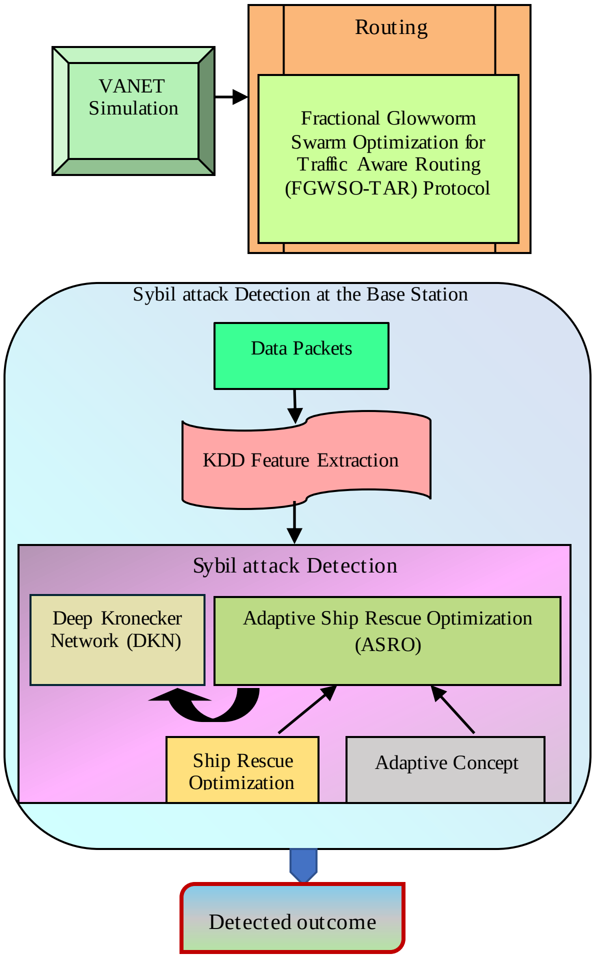

VANET Simulation
Routing
Fractional Glowworm Swarm Optimization for Traffic Aware Routing (FGWSO-TAR) Protocol
Sybil attack Detection at the Base Station
Data Packets
KDD Feature Extraction
Sybil attack Detection
Deep Kronecker Network (DKN)
Adaptive Ship Rescue Optimization (ASRO)
Ship Rescue Optimization
Adaptive Concept
Detected outcome

Fig. 1 Block diagram of ASRO_DKN for sybil attack detection in VANET

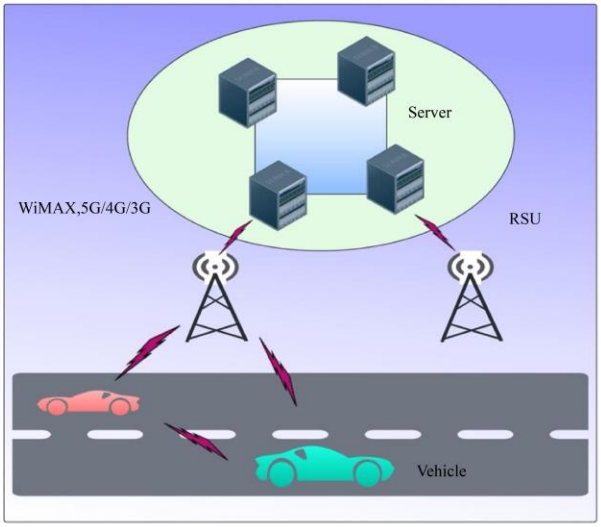


Fig. 2 Simulation model for VANET

Hence, the solution vector is given as,

$$U = \{u_1, u_2, \dots . u_a, \dots . . u_B\} \quad (1)$$

The overall solution is specified as $u_B$and a^{th} The solution is indicated as, u_a.

Step 2: Fitness Estimation

The fitness for each agent with the dimension of population B is computed. Moreover, it is estimated by the distance traveled and the delay of the vehicle. Hence, the fitness function is computed as follows,

$$Fitness = \left[\sum_{\substack{r=1\\w=1}}^{CV_r} \frac{Le^r}{PA_w^r(S_p)} + HD\right] * \frac{1}{N_f} \tag{2}$$

Where the road segment ID is indicated as r, and N_f Specifies the normalizing factor. The count of vehicles is denoted as CV_r. Moreover, the predicted average speed during the period w is denoted as PA_w^r, and the hop distance is specified as HD. The term Le^r shows the road segment length and S_pIndicates the vehicle's speed.

Step 3: Fractional Movement Stage

The search agent is moved to the adjacent glowworm based on the probabilistic approach for the fractional movement. Hence, the upgraded expression $t_d(q+1)$ for FGWSO is given as,

$$t_d(q+1) = nt_d(q) + \frac{1}{2}t_d(q-1) + B\left[\frac{t_\lambda(q)-t_d(q)}{\|t_\lambda(q)-t_d(q)\|}\right] \tag{3}$$

Where B is indicated as the step size, n specifies a constant, $t_\lambda(q)$ denotes the λ^{th} glowworm on the iteration q , and the Euclidean norm operation is indicated as $\| \|$.

Step 4: Re-Computation of Fitness

This step is followed until the maximum count of iterations is reached.

Step 5: Termination

The algorithm reaches the termination stage when the optimal solution is obtained, and the highest count of iterations is performed.

4.3. Detection of Sybil Attack at the Base Station

In the BS for attack detection, steps like data acquisition and feature extraction are performed, and the DKN detects the Sybil attack in VANET.

4.3.1. Data Acquisition

The input data is collected from the KDD Cup 1999 Dataset [14]. The competition process is formed with network intrusion detection, and a predictive model distinguishes the ``good" connections as normal, and ``bad" connections as attacks or intrusions. The data is given as,

$$C = \{C_1, C_2, \dots . C_b, \dots . . C_y\} \tag{4}$$

The term C specifies the dataset in which the whole data is symbolized by y, and the b^{th}Data is denoted by C_b.

4.3.2. Feature Extraction

After collecting the data from the dataset, the essential features are extracted to detect the Sybil attack. Moreover, the extracted features are specified as C_b.

4.3.3. ASRO_DKN-based Sybil Attack Detection

Attack detection is needed to identify the presence of attacks in the VANET. Here, the DKN is used to find the attack, and its hyperparameters are trained by the proposed ASRO.

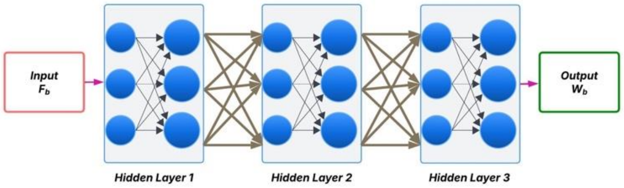


Fig. 3 Structure of DKN

Structure of DKN

The networking functionality of DKN [12] depends on the Kronecker product. Figure 3 portrays the structure of DKN, where the input, hidden, and output layers are presented in DKN. The feature F_b It is fed to DKN, and the resulting matrix is reshaped and flattened after the creation of the Kronecker product. The DKN resolves the complex interaction of features without any additional parameters. The output of the DKN is indicated by the term. W_b.

$$\mathrm{W_b} = \psi(\sigma_b)\mathrm{Exp}\{\sigma_b\langle \mathrm{F_b}, \mathrm{A}\rangle - \xi(\langle \mathrm{F_b}, \mathrm{A}\rangle)\} \tag{5}$$

Here, $\psi(.)$and $\xi(.)$ symbolizes the known univariate. The following expression indicates a certain known link function

$$\vartheta(\mathrm{D}(\sigma_b)) = \langle \mathrm{F_b}, \mathrm{A}\rangle \tag{6}$$

Furthermore, the decomposition for the Kronecker $\mathrm{L}(\geq 2)$ with the rank L, and the coefficient A is given as

$$\mathrm{A} = \sum_{l=1}^{L} \mathrm{T_H^1} \otimes \mathrm{T_{H-1}^1} \otimes \dots \otimes \mathrm{T_1^1} \tag{7}$$

Where, $\mathrm{h} = 1, \dots, \mathrm{H}$ and $1 = 1, \dots, \mathrm{L}$ denotes the component of Kronecker product, in which

$\upsilon = \Pi_{h=1}^{H}\upsilon_h$ and $g = \Pi_{h=1}^{H} g_h$; hence, it is simplified by,

$$\mathrm{T_{h'}} \otimes \mathrm{T_{h'-1}} \otimes \dots \otimes \mathrm{T_{h''}} = \otimes_{h=h'}^{h"} \mathrm{T_0} \tag{8}$$

The decomposition for each matrix is specified as $\mathrm{A}=\sum_{l=1}^{L} \otimes_{h=H}^{1} \mathrm{T_h^1}$.

Training of DKN by ASRO

ASRO is formed by merging SRO [13] with an adaptive concept. SRO is based on the ship's manoeuvring motion and the rescue approach. SRO is employed to resolve the complex optimization issues. The ship rescue is split up into two classes: wide area rescue (delayed rescue) and small rescue (immediate rescue), which are based on the searched individual. Furthermore, these two rescue behaviors are correlated with exploration and exploitation. To diminish the complexity of computation, the adaptive concept has been added to ASRO.

Step 1: Initialization

The count of ships is considered as a population member, and the location of the ship is expressed as,

$$\mathrm{A_k(h+1)} = \mathrm{A_{min}} + \mathrm{c} \times (A_{max} - A_{min}) \tag{9}$$

The current iteration is specified as h, and c represents the random number between 0 and 1. At the iteration h, the location of ship k is denoted as $\mathrm{A_k(h)}$. The terms A_{max} and A_{min} Indicate the bounds.

Step 2: Computation of Fitness

The fitness function indicates the way of attaining the ideal solution, and is expressed as,

$$Fitness = \frac{1}{y}\sum_{b=1}^{y}[W_b^* - W_b]^2 \tag{10}$$

Where, W_b indicates the outcome of DKN, and W_b^* Portrays the expected output.

Grouping of Ships

Isolating every ship into I groups, in which the count of ships in every group is denoted as $J/_I$. Moreover, the location of every ship is specified as $A_b^i, i \in \{1, \dots, I\}, k \in \{1, \dots J/_I\}$

Step 3: Compute the Ideal Value in Every Group and the Global Ideal Overall Ships

The ideal ship location of every cluster is termed as A_{best}^i, and globally, the best location of the ship is stated as A_{best} .

Step 4: Upgrade the Manoeuvring Function of the Ship

For ship manoeuvring purposes, the coefficient H indicates the highest count of iterations. Moreover, the maximum count of iterations is denoted as H_{max}.

$$x_k^i(h+1) = Z_k^i(h).e^{-\frac{h}{Max\_Iter}} + l.\alpha_k^i(h) \tag{11}$$

Here, the present iteration is indicated as h, the regular constant is specified as l, and Max_Iter implies the maximum count of iterations. Furthermore, $Z_k^i(h)$ implies the constant for the i^{th} group of ships k, and the rudder angle for i^{th} group at the h^{th} iteration is symbolized as $\alpha_k^i(h)$. The term $x_k^i(h)$ denotes the rotational angle for l group of ships at the iteration h. The expression for the rude and rotational angle is derived as follows,

$$Z_k^i(h+1) = \frac{v_k^i(h) - l.\alpha_k^i(h)}{e^{\frac{-h}{Max\_Iter}}} \tag{12}$$

$$\alpha_k^i(h+1) = rnd.dc.angle_k^i(h) \tag{13}$$

Where, rnd specifies the random value within (−2, 2). Moreover, the coefficient of direction dc controls the rudder angle and is set as 1 or−1. The rotation angular velocity at the iteration h is indicated as. At the iteration i, the angle between two ships is denoted as $angle_k^i(h)$.

$$angle_k^i(h) = arc\ cos\frac{A_k^i(h).A_{best}^i}{\|A_k^i(h)\|\|A_{best}^i\|} \tag{14}$$

Step 5: Exploration Phase

In exploration, the ideal value does not vary in 10 iterations when upgrading the ship location. The updated formula is given as,

$$A_k^i(h+1) = A_{best}^i(h) + z_1.\lambda_k^i(h).\cos\left(G_k^i(h)\right) - z_2.(A_{best}^i(h) - A_k^i(h)) \tag{15}$$

Where, z_1 and z_2 are the coefficients, in which z_1 lies between (0,1), and z_2 lies between (-1,1). The terms $G_k^i(h)$ specifies the direction of movement for i^{th} A group of ships at the h^{th} iteration, and the value ranges between $(-\pi, \pi)$. The specific computation is expressed as,

$$G_k^i(h+1) = G_k^i(h) + \alpha_k^i(h) \tag{16}$$

The movement speed of the ship at the h^{th} iteration is specified as $\beta_k^i(h)$. Initially, the value is set as 0.

$$\beta_k^i(h+1) = \beta_k^i(h) + \chi_k^i(h) \tag{17}$$

The acceleration is indicated as χ_k^i.

Step 6: Exploitation Phase

In exploitation, if any one of the generations varies within 10 successive iterations at the upgrading of the ship location. The trajectory of the ship is classified into three forms: spiral, sector, and inward-joining circle-based search approaches.

Case 1: If the population is $\left[1, \frac{1}{2}N\right] Then$, the spiral search approach is used.

$$A_k^i(h+1) = A_k^i(h) + (M_1(h) + M_2(h) \tag{18}$$

$$M_1(h) = p.j(h)\cos\left(\left(A_k^i(h)\right)\right).dist_\chi(h) \quad (19)$$

$$M_2(h) = p.j(h)\sin\left(\left(A_k^i(h)\right)\right).dist_\delta(h) \quad (20)$$

$$dist_\chi(h) = A_{best}^i(h) - A_k^i(h) \quad (21)$$

$$dist_\delta(h) = A_{best}(h) - A_k^i(h) \quad (22)$$

$$j(h) = \frac{-1}{2\pi.Max\_Iter} \quad (23)$$

Where $M_1(h)$ and $M_2(h)$ specifies the group as well as the global optimal curves. The present distances are indicated as $dist_\chi(h)$ and $dist_\delta(h)$. The random value p lies between -1 and 1.

Case 2: If the count of the population is $\left[\frac{1}{2}\mathrm{N}, \frac{9}{10}\mathrm{N}\right]$ Then, the sector search approach is utilized. Hence, the upgraded expression is given as,

$$A_k^i(h+1) = A_k^i(h) + \frac{\pi}{3}.p.dist_\delta(h).D \quad (24)$$

The step size D attains the Levy flight motion as per the following expression,

$$D(Dim) = 0.01\frac{\varepsilon\times\mu}{|\lambda|^{\frac{1}{\eta}}} \quad (25)$$

$$\mu = \left[\frac{\Gamma(1+\eta)\times sin\left[\frac{\pi\eta}{2}\right]}{\Gamma\frac{(1+\eta)}{2}\times\eta\times 2^{\frac{\eta-1}{2}}}\right]^{\frac{1}{\eta}} \quad (26)$$

The terms ε and μ specify that the random number lies in (0, 1), and η is set as 1.5.

Case 3: If the count of the population is $\left[\frac{9}{10}\mathrm{N}, \mathrm{N}\right]$ Then, the circle search approach is used. Therefore, the upgraded expression is given as,

$$A_k^i(h+1) = p.O(h) + cos(A_k^i(h)) + dist_\delta(h).cos(P(h)) \quad (27)$$

The expression for $O(h)$ and $P(h)$ are specified as,

$$O(h) = dist_\chi(h) - dist_\delta(h) \quad (28)$$

$$P(h) = O(h).A_k^i(h) \quad (29)$$

Step 7: Ship Squad Communication

In each 20 iterations, the ships are interconnected to each other and upgrade the worst 3 ship locations of every group as follows,

$$A_k^i(h+1) = A_k^i(h) + z_1(A_{best}^i(h) - A_k^i(h)) + z_2(A_{best}^i(h) - A_k^i(h)) \quad (30)$$

Where the coefficients z_1 lies between (0,2), and z_2 lies between (0,2). Moreover, the terms z_1, and z_2 are considered adaptive, and it is expressed as,

$$z_1, z_2 = 3 - \left[\frac{\eta\times h\times J}{\frac{-1}{e^{Max\_Iter}}}\right] \quad (31)$$

Where η is set as 1.5, J specifies the population size and the maximum count of iteration is represented as Max_iter.

Step 8: Re-Estimation of Fitness

The fitness function is re-estimated after upgrading the food source.

Step 9: Termination

The aforesaid steps are repeated until the optimum solution is attained.

5. Result and Discussion

The experimental outcome of ASRO_DKN-based Sybil attack detection in VANET is illustrated. The measuring parameters, dataset, implementation tools, and comparative analysis are explained.

5.1. Experimental Setup

The ASRO_DKN-based Sybil attack detection in VANET is implemented in the PYTHON tool.

5.2. Dataset Description

The data are collected for the KDD Cup 1999 Dataset [14]. Here, the predictive model is used to distinguish the ``bad" connections as attacks or intrusions, and the ``good" connections as normal.

5.3. Performance Metrics

The Precision, recall, and F1-measure metrics are employed to validate the ASRO_DKN-based Sybil attack detection in VANET.

5.3.1. Precision

The quantity of true positives to the total positive is defined as Precision [15]. The mathematical form of Precision is given by,

$$Precision = \frac{R^{pos}}{R^{pos} + S^{pos}} \quad (32)$$

Where, R^{pos} shows the true positive, and S^{pos} Implies a false positive.

5.3.2. Recall

The percentage of true positives to the precise positive is termed as recall [15]. Furthermore, the recall is given as,

$$Recall = \frac{R^{pos}}{R^{pos} + S^{neg}} \quad (33)$$

Where the false negative is symbolized as S^{neg}.

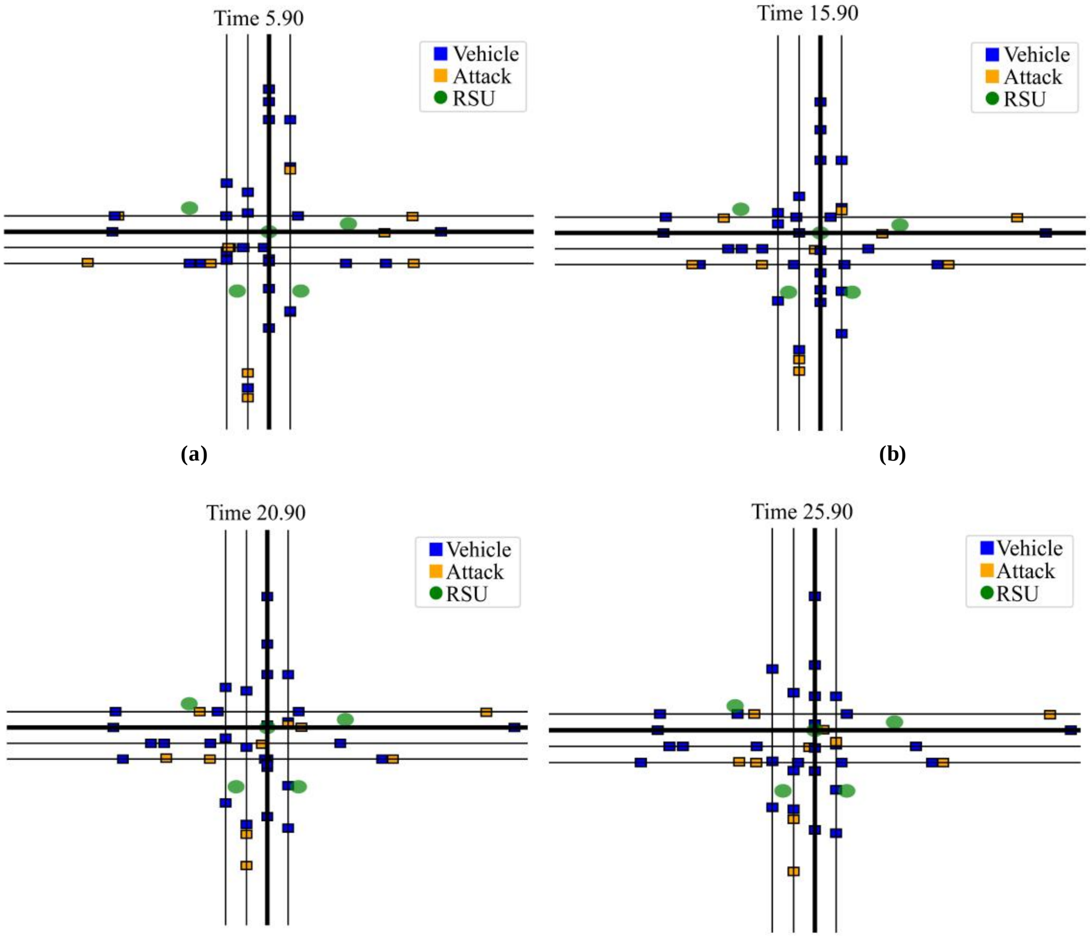
5.3.3. *F1-Measure*

The F1-score [15] is a weighted portion of Precision and recall. The F1-score [20] is given as,

$$F1\ Score = 2 \times \left[\frac{Recall\ \times Precision}{Recall\ \times Precision}\right] \tag{34}$$

5.4. Simulation Results

Figure 4 shows the simulation outcome for ASRO_DKN-based Sybil attack detection in VANET, where Figures 4 (a), (b), (c), and (d) show the simulated result at the intervals 5.9 Sec, 15.9 Sec, 20.9 Sec, and 25.9 Sec. Here, the blue square represents the vehicle, the yellow square represents the attack, and the green circle indicates the RSU.



(a)

(b)

(c)

(d)

Fig. 4 Simulation results for the interval, (a) 5.9 sec, (b) 15.9 sec, (c) 20.9 sec, and (d) 25.9 sec.

5.5. Comparative Methods

Methods like LCSS [1], BSM [2], Ensemble Majority Voting [3], Beacon Packet-based Traceability mechanism [4], and CDEO-Based Deep Residual Network are considered as the comparative approaches to compute the effectiveness of ASRO_DKN-based Sybil attack detection in VANET.

5.5.1. Assessment using Training Data

Figure 5 deliberates the evaluation of ASRO_DKN-based Sybil attack detection in VANET. Figure 5 (a) exhibits the Assessment regarding Precision. The Precision attained by the ASRO_DKN is 82.77%, in which the existing models like LCSS, BSM, Ensemble Majority Voting, Beacon Packet-based Traceability mechanism, and CDEO-Based Deep Residual Network attained the Precision of 75.08%, 77.13%, 77.17%, 79.13%, and 80.20% for the training data=50%. The Assessment regarding recall is exhibited in Figure 5 (b). For the training data of 50%, the recall achieved by the ASRO_DKN is 81.79%, whereas the LCSS, BSM, Ensemble Majority Voting, Beacon Packet-based Traceability mechanism, and CDEO-Based Deep Residual Network achieved the recall of 74.36%, 765.38%, 79.28%, 79.73%, and 79.83%. Moreover, the analysis concerning the F-measure is depicted in Figure 5(c). The existing approaches attain the F-measure of 74.72%, 76.25%, 78.21%, 79.43%, 80.01%, and 80.09%, and the ASRO_DKN under 60% of training data.

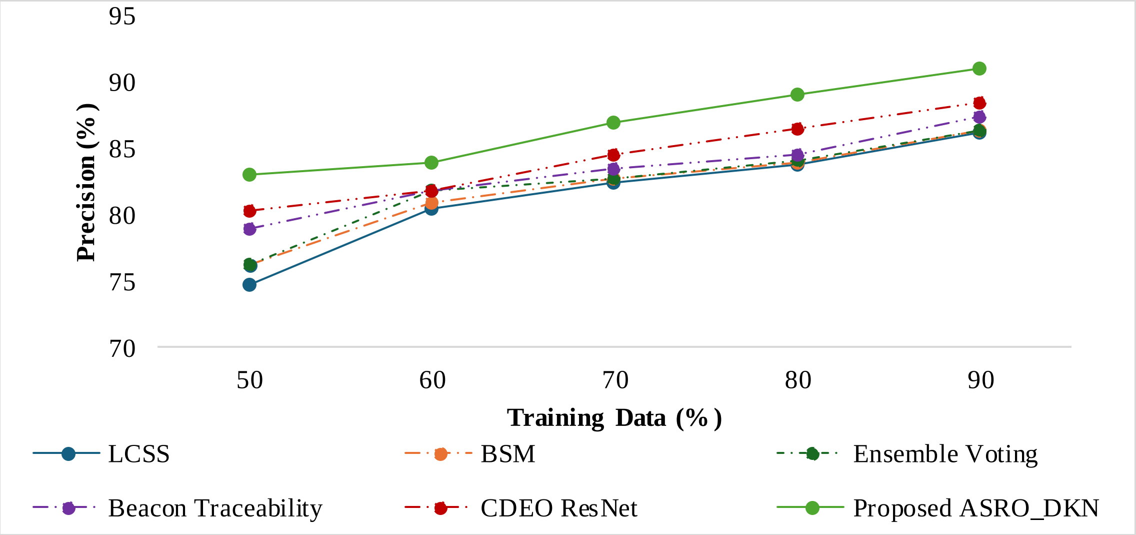


Fig. 5(a) Comparative assessment in terms of training data vs Precision

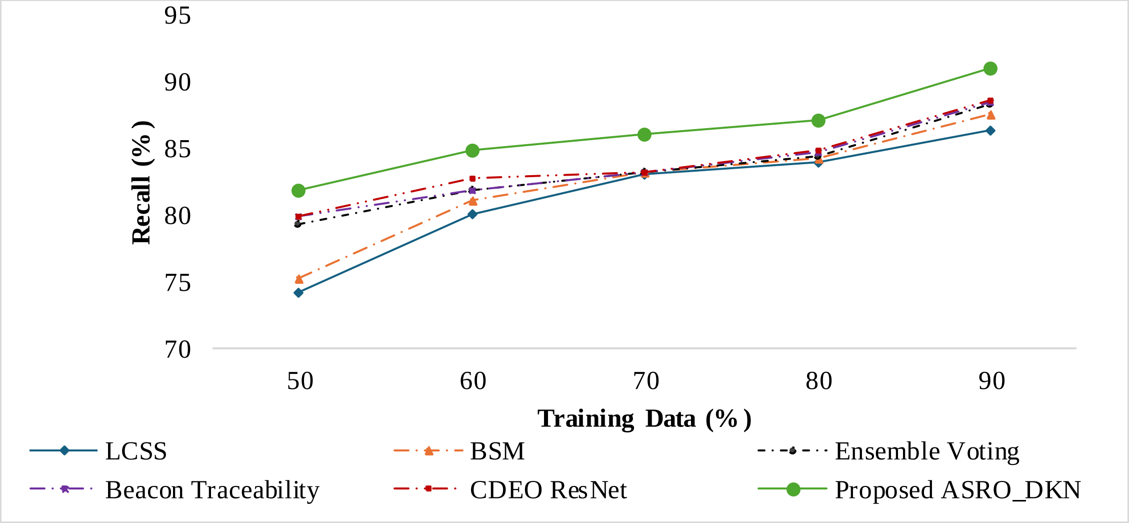


Fig. 5(b) Comparative assessment in terms of training data vs Recall

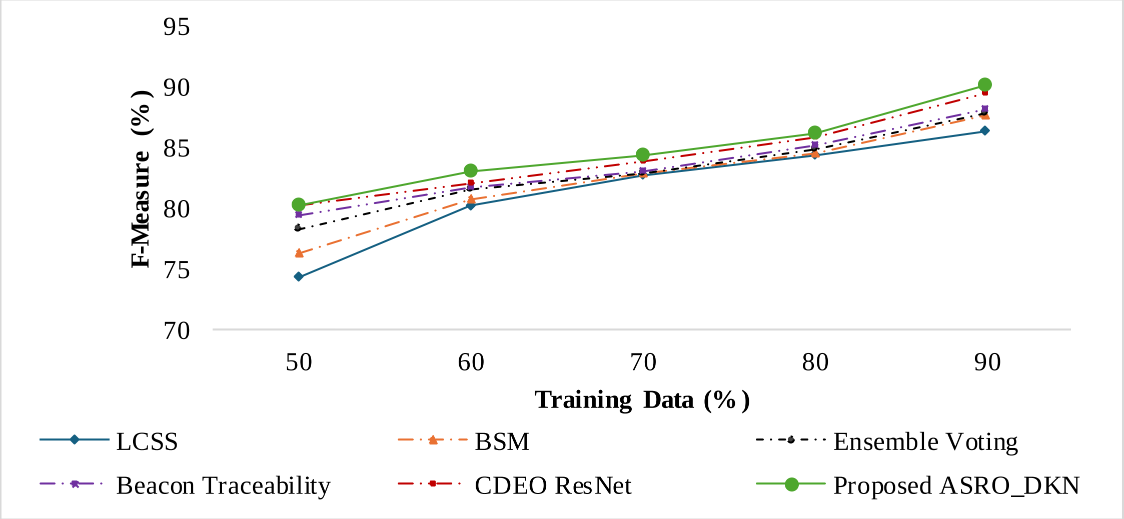


Fig. 5(c) Comparative assessment in terms of training data vs F-Measure

5.5.2. Assessment based on K-Value

Figure 6 displays the Assessment of ASRO_DKN-based Sybil attack detection in VANET with respect to K-Value. The evaluation with respect to Precision is exhibited in Figure 6(a). With the K-Value =5, the Precision achieved by the ASRO_DKN is 82.74%. In contrast, the Precision of 77.88%, 78.40%, 79.81%, 80.02%, and 80.14% is attained by the LCSS, BSM, Ensemble Majority Voting, Beacon Packet-based Traceability mechanism, and CDEO-Based Deep Residual Network. Figure 6(b) exhibits the analysis regarding Precision. For the K-Value=6, the Precision of ASRO_DKN is 82.79%, in which the Precisions of 76.21%, 76.46%, 76.87%, 79.34%, and 79.573% are achieved by the LCSS, BSM, Ensemble Majority Voting, Beacon Packet-based Traceability mechanism, and CDEO-Based Deep Residual Network. The Assessment related to F-measure is shown in Figure 6(c). Here, the existing methods, and the ASRO_DKN attained the F-measure of 74.72%, 76.25%, 78.21%, 79.43%, 80.01%, and 82.28% for the K-Value of 5.

5.6. Comparative Discussion

A comparative discussion of ASRO_DKN-based Sybil attack detection in VANET is described. Here, the ASRO_DKN attains the ideal values in training data-based analysis. The ASRO_DKN achieved the finest Precision of 90.84%. In contrast, the Precision of the existing models, such as LCSS, BSM, Ensemble Majority Voting, Beacon Packet-based Traceability mechanism, and CDEO-Based Deep Residual Network, are 86.78%, 86.83%, 86.99%,87.88%, and 88.90%. The optimal recall attained by the ASRO_DKN is 90.48%, in which the LCSS, BSM, Ensemble Majority Voting, Beacon Packet-based Traceability mechanism, and CDEO-Based Deep Residual Network achieved the recall of 86.44%,87.52%,88.05%,88.36%, and 88.39%. The better F-measure of 90.13% is achieved by the ASRO_DKN, whereas the F-measure obtained by the existing approaches is 86.71%,87.68%,88.35%,88.70%, and 89.69%. In addition, the superior values of 90.38%, 90.65%, and 90.66% are achieved in K-value-based analysis.

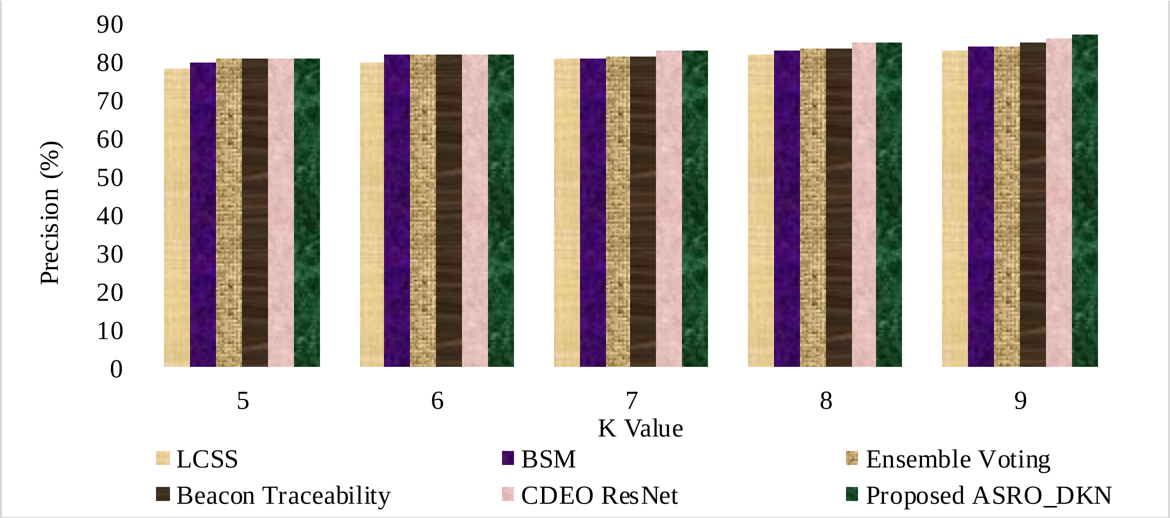


Fig. 6(a) Comparative assessment in terms of K-Value vs Precision

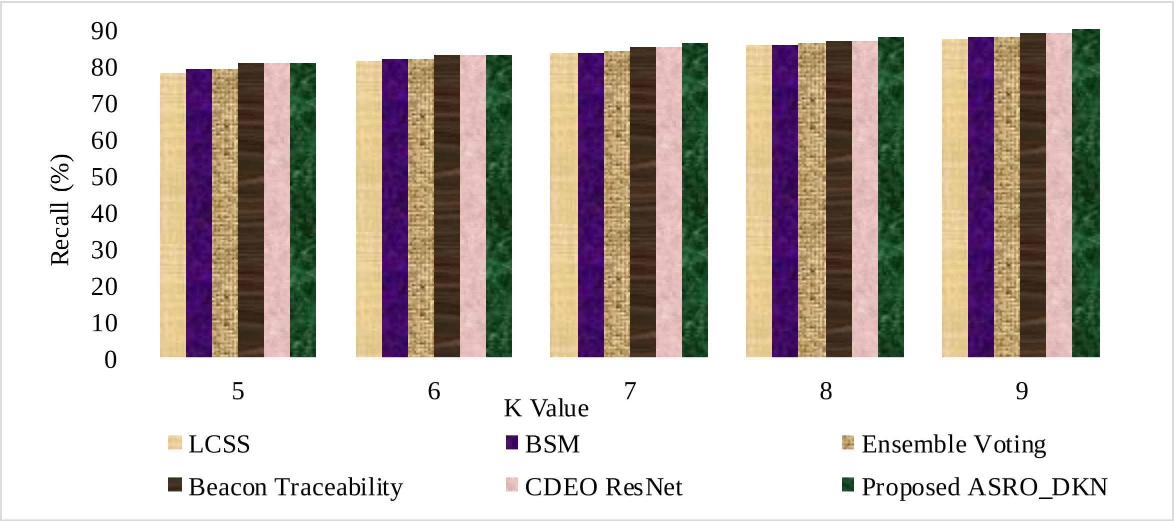


Fig. 6(b) Comparative assessment in terms of K-Value vs Recall

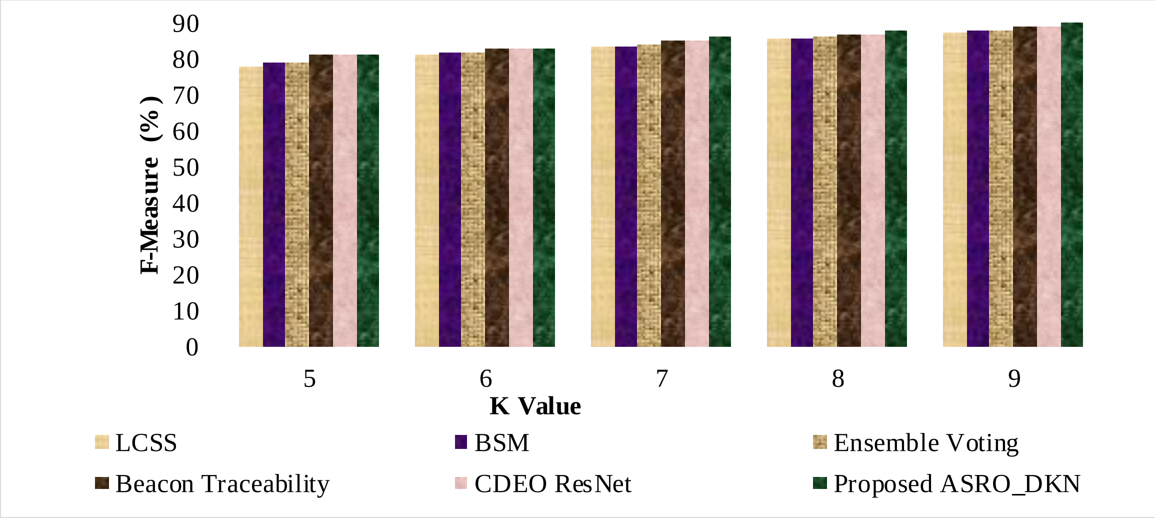


Fig. 6(c) Comparative assessment in terms of K-Value vs F-measure

Table 1. Comparative discussion of ASRO_DKN-based sybil attack detection in VANET

Variations	Metrics/ Methods	LCSS	BSM	Ensemble majority voting	Beacon Packet-based Traceability mechanism	CDEO-based Deep Residual network	Proposed ASRO_ DKN
Training data=90%	Precision (%)	86.78	86.83	86.99	87.88	88.90	90.84
	Recall (%)	86.44	87.52	88.05	88.36	88.39	90.48
	F-measure (%)	86.71	87.68	88.35	88.70	89.69	90.13
K-Value=9	Precision (%)	85.86	86.74	86.84	87.34	88.33	90.38
	Recall (%)	85.94	87.82	88.03	88.29	88.79	90.65
	F-measure (%)	86.71	87.15	87.60	87.97	88.63	90.66

6. Conclusion

VANETs are employed to exchange information and detect and mitigate critical circumstances in transportation. Still, VANETs are susceptible to numerous security hazards. Sybil attack is one of the severe attacks, wherein a malicious node creates a massive number of fake identities to interrupt the function of VANET. Moreover, it generates a significant threat to the protection of vehicle movement. However, it is very complex to identify the Sybil attack due to the real scenario, such as attacker density and traffic flow. Hence, this work proposes the ASRO_DKN-based Sybil attack detection in VANET. The VANET simulation is the initial step, and the FGWSO-TAR Protocol is used to perform the routing. The Sybil attack is detected at the BS, where the essential features are extracted from the data. The DKN is used for Sybil attack detection, and the ASRO trains the hyperparameters of DKKN. Moreover, metrics like Precision, recall, and F-measure are used to validate the efficiency of the model, and the optimal values of 90.84%, 90.48%, and 90.13% are achieved. In the future, the hybrid network will be designed to attain more precise outcomes. In conclusion, this study presents a novel and comprehensive approach to Sybil attack detection in VANETs by combining Adaptive Ship Rescue Optimization (ASRO) with a Deep Kronecker Network (DKN). Unlike prior methods such as LCSS, basic security message analysis, and ensemble-based detection, which are often limited by static configurations, high complexity, or scalability issues, the proposed framework introduces adaptability and efficiency through ASRO-based hyperparameter tuning. By incorporating FGWSO-TAR for realistic traffic-aware routing and leveraging the DKN's capability to model complex feature interactions, the system effectively addresses communication dynamics and security threats. The comparative evaluation confirms that the proposed ASRO_DKN method achieves superior detection performance across all key metrics, establishing its potential for enhancing the reliability and security of vehicular networks.

References

[1] S. Rakhi, and K.R. Shobha, “LCSS Based Sybil Attack Detection and Avoidance in Clustered Vehicular Networks,” *IEEE Access*, vol. 11, pp. 75179-75190, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Zhaoyi Zhang et al., “Detection Method to Eliminate Sybil Attacks in Vehicular Ad-Hoc Networks,” *Ad Hoc Networks*, vol. 141, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Sofia Azam et al., “Collaborative Learning Based Sybil Attack Detection in Vehicular AD-HOC Networks (VANETS),” *Sensors*, vol. 22, no. 18, pp. 1-17, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Yaling Zhu et al., “Sybil Attacks Detection and Traceability Mechanism Based on Beacon Packets in Connected Automobile Vehicles,” *Sensors*, vol. 24, no. 7, pp. 1-26, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Julia Silva Weber, Miguel Neves, and Tiago Ferreto, “VANET Simulators: An Updated Review,” *Journal of the Brazilian Computer Society*, vol. 27, pp. 1-31, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Nabeel Akhtar, Sinem Coleri Ergen, and Oznur Ozkasap, “Vehicle Mobility and Communication Channel Models for Realistic and Efficient Highway VANET Simulation,” *IEEE Transactions on Vehicular Technology*, vol. 64, no. 1, pp. 248-262, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[7] Mushtak Y. Gadkari, and Nitin B. Sambre, “VANET: Routing Protocols, Security Issues and Simulation Tools,” *IOSR Journal of Computer Engineering*, vol. 3, no. 3, pp. 28-38, 2012. [Google Scholar] [Publisher Link]

[8] Dhia Eddine Laouiti et al., “Sybil Attack Detection in VANETs using an AdaBoost Classifier,” *2022 International Wireless Communications and Mobile Computing*, Dubrovnik, Croatia, pp. 217-222, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Jin Wang et al., “ClusterRep: A Cluster-Based Reputation Framework for Balancing Privacy and Trust in Vehicular Participatory Sensing,” *International Journal of Distributed Sensor Networks*, vol. 14, no. 9, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[10] Yi-Ying Zhang et al., “A Self-Learning Detection Method of Sybil Attack Based on LSTM for Electric Vehicles,” *Energies*, vo. 13, no. 6, pp. 1-15, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] Deepak Rewadkar, and Dharmpal Doye, “FGWSO-TAR: Fractional Glowworm Swarm Optimization for Traffic Aware Routing in Urban VANET,” *International Journal of Communication Systems*, vol. 31, no, 1, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[12] Long Feng, and Guang Yang, “Deep Kronecker Network,” *Arxiv Preprint*, pp. 1-40, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Shu-Chuan Chu et al., “Ship Rescue Optimization: A New Metaheuristic Algorithm for Solving Engineering Problems,” *Journal of Internet Technology*, vol. 25, no. 1, pp. 61-78, 2024. [Google Scholar] [Publisher Link]

[14] KDD Cup 1999 Data, 1999. [Online]. Available: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[15] Mahır Kaya, and Yasemın Çetın-Kaya, “A Novel Deep Learning Architecture Optimization for Multiclass Classification of Alzheimer’s Disease Level,” *IEEE Access*, vol. 12, pp. 46562-46581, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Kusum Dalal, “Ensuring Secure Transmission in VANET: Optimal Clustering and Improved LSTM-Based Intrusion Detection,” *International Journal of Communication Systems*, vol. 38, no. 4, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] M. Ajin, and R.S. Shaji, “Enhancing Security in Vanets: Adaptive Bald Eagle Search Optimization Based Multi-Agent Deep Q Neural Network for Sybil Attack Detection,” *Vehicular Communications*, vol. 54, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] M.K. Kirubakaran et al., “Enhanced VANET Communication: Fractional Order Water Flow Optimization and Secure Communication via Spatial Bayesian Neural Network,” *International Journal of Communication Systems*, vol. 38, no. 12, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[19] Mohammed Aledhari et al., “Safeguarding Connected Autonomous Vehicle Communication: Protocols, Intra- and Inter-Vehicular Attacks and Defenses,” *Computers & Security*, vol. 151, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[20] C. Balakumar, and S. Vydehi, “Multi-Dimensional Trust Based Data Dissemination Mechanism (MDTD) for Ensuring Authentication by Eliminating Blackhole Attack in VANET,” *Journal of Intelligent Systems and Internet of Things*, vol. 16, no. 1, pp. 102-117, 2025. [CrossRef] [Google Scholar] [Publisher Link]