

EFLO_QDCNN: Exponential Frilled Lizard Optimization_Quantum Dilated Convolutional Neural Network for Sybil attack detection in VANET

Vinay Kumar S B

*Department of Electronics and Communication Engineering
JAIN (Deemed to be University), Bangalore -562112, India
sb.vinaykumar@jainuniversity.ac.in*

Abstract: In Vehicular Ad Hoc Networks (VANETs), detecting Sybil attacks is crucial for maintaining the integrity, reliability, and security of VANETs. These attacks can lead to severe consequences like traffic congestion, false accident reports, or even life-threatening situations due to misleading data. Specifically, detecting Sybil attacks where a single node masquerades as multiple identities poses a significant problem, as it directly conflicts with privacy preservation objectives. Existing solutions typically fall short of addressing these concerns effectively. To address these challenges, this research introduces the Exponential Frilled Lizard Optimization_Quantum Dilated Convolutional Neural Network (EFLO_QDCNN) framework for effective Sybil attack detection. Firstly, a VANET simulation is conducted, and secure communication is done through routing. Furthermore, Sybil attack detection is performed at the Base Station (BS). Initially, input data is subjected to feature selection, and it is performed based on the Histogram Intersection metric. Subsequently, QDCNN is employed for detecting Sybil attacks. Here, the QDCNN is trained using EFLO. The EFLO algorithm mimics the adaptive survival behavior of frilled lizards to balance exploration and exploitation in optimization tasks. Moreover, EFLO_QDCNN gained Energy, F-measure, and precision of 0.054J, 90.714%, and 89.742%. This demonstrates that the model provides not only accurate detection results but also low energy consumption, which is essential for resource-constrained VANET environments.

Keywords: Vehicular Ad Hoc Networks, Deep Learning, Quantum Dilated Convolutional Neural Network, Exponential Weighted Moving Average, Frilled Lizard Optimization.

Nomenclature

Abbreviations	Description
VANET	Vehicular Ad Hoc Network
EFLO	Exponential Frilled Lizard Optimization
QDCNN	Quantum Dilated Convolutional Neural Network
BS	Base Station
OBU	On Board Unit
RSU	Roadside Unit
EWMA	Exponential Weighted Moving Average
FLO	Frilled Lizard Optimization
BSM	Basic Security Message
CA	Central Authority
DSRC	Dedicated Short-Range Communication

1. Introduction

Vehicular communications have garnered significant interest from both academic researchers and industry professionals. This enables communication between vehicles and potentially with roadside units, meaning that at least one of the transmitting or receiving entities is a vehicle, which may also serve as a routing node. A VANET is a specialized branch of Mobile Ad hoc Networks (MANETs) developed to enable communication between nearby vehicles and roadside substructures. In such networks, vehicles act as communication nodes capable of forming a self-organizing network without the need for preceding configuration or knowledge of the presence of supplementary nodes. The network nodes are categorized into two types, such as On-Board Units (OBUs) and Road Side Units (RSUs) [1]. In VANETs, moving vehicles can communicate with each other through inter-vehicle communications and with nearby RSUs through RSU-to-vehicle links. This connectivity has directed the development of a wider range of

applications, which are considered promising solutions for enabling innovative and ubiquitous traffic management setups. The fundamental concept behind these applications is to allow vehicles to secure data sharing and feedback with the control system, thereby enabling the creation of a spatiotemporal view of traffic conditions and facilitating the extraction of critical traffic congestion statistics.

The application of VANET can make roads safe and efficient by supporting a variety of functions, like traffic flow management, improved route guidance, and navigation. However, these applications rely on the information provided by participating vehicles. Consequently, it is essential to protect drivers' privacy while ensuring the verification of their identities in an anonymous manner [2]. In addition, a malicious vehicle could exploit this privacy protection to carry out a Sybil attack. In a Sybil attack, a malicious entity integrates multiple pseudonyms to masquerade as numerous different nodes within the network. For instance, a malicious vehicle might simulate traffic congestion by creating false reports. Therefore, detecting and preventing Sybil attacks in VANETs is of critical importance to maintain the integrity and safety of the network [3]. Traditional methods for detecting Sybil attacks often face challenges related to scalability and adaptability in VANET environments, where vehicles frequently change positions and network topologies are in a constant state of flux. In recent years, Deep Learning (DL) techniques have emerged as a promising scheme for identifying and mitigating Sybil attacks. Additionally, DL models improve the accuracy and efficiency of Sybil attack detection in VANETs, offering more robust security against adversarial manipulation [4]. Despite their advantages, many existing DL-based approaches require substantial computational resources, limiting their real-time applicability in dynamic vehicular scenarios.

The main aim of this article is to introduce an EFLO_QDCNN for detecting Sybil attacks. At first, a VANET simulation is performed, and routing is done to ensure secure communication. At BS, input data is used for feature selection, and it is carried out using the Histogram Intersection metric. Subsequently, the QDCNN model is utilized for detecting Sybil attacks. The hyperparameters of QDCNN are optimized using EFLO. EFLO integrates Exponential Weighted Moving Average (EWMA) for adaptive memory-based learning with Frilled Lizard Optimization (FLO), a metaheuristic inspired by the agility and exploration behavior of frilled lizards. This hybridization ensures enhanced convergence and optimal hyperparameter tuning.

The major contribution of this work is elucidated as,

- **Proposed EFLO_QDCNN for Sybil attack detection:** This research introduces a robust Sybil attack detection model tailored for VANET environments. The proposed framework, named EFLO_QDCNN, offers a comprehensive solution for accurately identifying Sybil attacks. Here, the QDCNN hyperparameters are tuned using EFLO, which combines the strengths of Exponential Weighted Moving Average (EWMA) and Frilled Lizard Optimization (FLO).

This article is organized as follows: Section 2 presents traditional methods based on Sybil attack detection. Section 3 introduces EFLO_QDCNN with its detailed architecture and mathematical modeling. Section 4 presents the results and discussion of the devised method. Section 5 provides a conclusion and insights for future development. This results in a lightweight yet highly accurate detection system, suitable for real-time VANET applications.

2. Motivation

The recent advancements in VANETs for intelligent transportation systems underscore the critical requirement of robust security mechanisms for ensuring safe and trustworthy communication among vehicles. Detecting Sybil attacks is particularly important, as these malicious activities can disrupt network operations, compromise data integrity, and lead to serious safety hazards. This part explains the main complications faced by classical Sybil attack detection models. This motivates the design of a more effective, privacy-preserving detection framework capable of addressing the shortcomings of existing approaches. A major challenge lies in balancing detection accuracy with computational efficiency, especially in highly dynamic vehicular networks where real-time responsiveness is essential.

2.1 Literature Survey

The literature review of classical models related to Sybil attack detection is explained below.

N. C Velayudhan *et al.* [5] designed an Emperor Penguin Optimization-based Routing protocol (EPORP) for Sybil attack detection. This model gained low delay and improved security and performance for Sybil attack detection. However, this scheme failed to apply to detecting diverse VANET attacks.

S. Azam *et al.* [6] employed an Ensemble Majority Voting approach for Sybil attack detection. The developed scheme mainly focused on detecting security disruptions and fake information distribution. Moreover, this model neglected to consider more ensemble techniques, such as stacking, for evaluating its performance.

Z. Zhang *et al.* [7] introduced Basic Security Message (BSM) packets to mitigate the influence of Sybil attacks. Moreover, this scheme failed to optimize the performance of the developed model for detecting various attacks.

S. Rakhi *et al.* [8] designed the Longest Common Subsequence-based Sybil Detection in Clustering Network (LSDCN). This algorithm attained low computational complexity. Nevertheless, this scheme failed to process large data by using effective pre-processing techniques.

In summary, while these works offer valuable contributions, they generally suffer from limitations in model adaptability, computational scalability, and handling of real-time detection in rapidly changing vehicular environments.

2.2 Main Challenges

The main complexities of conventional sybil attack detection models are,

- The presented module in [5] enabled efficient exploration and exploitation and accurately identified the malicious nodes attempting to impersonate multiple identities. Nevertheless, this scheme required an effective hyperparameter tuning technique for improving detection accuracy.
- The Ensemble Majority Voting approach designed in [6] accomplished high robustness and improved the decision-making process. Furthermore, the effectiveness of the ensemble heavily depends on the diversity and individual performance of classifiers.
- In [7], the BSM was devised for detecting various attacks in VANET. This model was less complex and required low implementation costs. However, it had increased network overhead and consumed bandwidth and energy.
- The high dynamic topology of vehicles in VANET results in frequent network partitions and fluctuating communication links, making it challenging to distinguish between legitimate vehicles and Sybil nodes effectively. Additionally, timely detection is significant for optimizing computational and communication resources, often constrained in VANET environments. Thus, an effective hybrid DL structure is essential for detecting various attacks in VANET. This necessitates the development of intelligent, lightweight detection mechanisms that can adaptively respond to evolving attack patterns with minimal resource consumption.
- Furthermore, existing models often lack integration of efficient feature selection strategies, leading to redundant or irrelevant input features that can degrade model performance.

3. Proposed Exponential Frilled Lizard Optimization_ Quantum dilated Neural Network for detection of Sybil attacks in VANET

VANET is a promising technology for automated driving that offers significant advantages in terms of user convenience by enhancing road safety and driving comfort. However, the swift advancements in this field also bring about a rise in digital threats. Among various attacks, the Sybil attack has been identified as one of the most critical risks in VANETs. Diverse classical sybil attack detection models faced complications due to high computational complexity, poor scalability with large networks, and limited adaptability to evolving attack strategies.

To conquer these complications, this research introduces an EFLO_QDCNN for conducting sybil attack detection. Firstly, a VANET simulation is conducted, and routing is performed for secure communication. At BS, the input data is acquired from a specific dataset illustrated in [9]. Then, feature selection is done based on the Histogram intersection metric. After that, Sybil attack detection is conducted by utilizing QDCNN [10]. Moreover, QDCNN is trained by EFLO. Here, the EFLO is devised by incorporating EWMA [11] and FLO [12]. EWMA contributes by adaptively smoothing temporal data to enhance stability in learning, while FLO enhances exploration and exploitation in parameter tuning. The hybrid nature of EFLO helps in optimizing QDCNN's performance by avoiding local minima and accelerating convergence.

The resulting EFLO_QDCNN model is designed to handle high-speed vehicular mobility, dynamic topology, and resource constraints effectively, making it well-suited for real-time Sybil attack detection in VANETs.

The block diagram of EFLO_QDCNN is shown in Fig. 1.

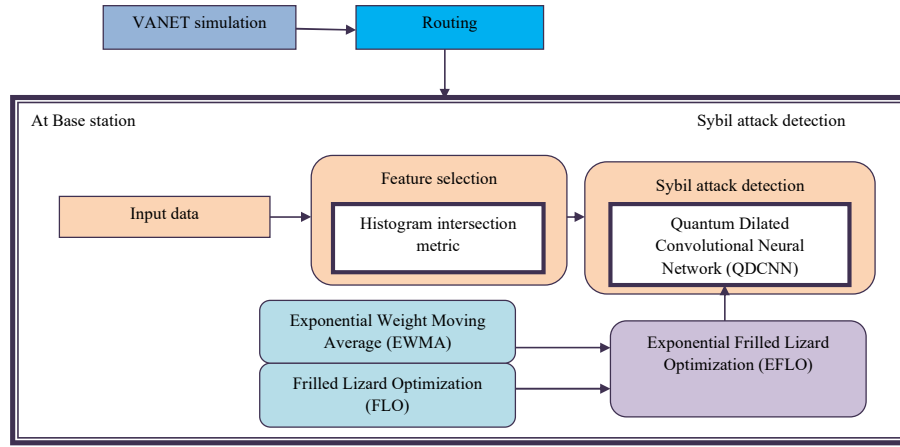


Fig. 1. Block diagram of EFLO_QDCNN for Sybil attack detection

3.1 VANET Simulation

A **VANET** [13] is a type of decentralized, self-organizing wireless network specifically designed for communication between vehicles and roadside infrastructure. It consists of RSU, OBU, and the central authority (CA). The system design of VANET is depicted in Fig. 2. The simulation models realistic urban or highway traffic conditions where vehicles exchange safety-critical messages, allowing for the evaluation of network behavior under various mobility patterns and attack scenarios.

3.1.1 OBU

An OBU is a tamper-proof device (TPD) capable of executing cryptographic operations and securely storing sensitive information [7]. By utilizing the OBU, vehicles can communicate with each other through the Dedicated Short-Range Communications (DSRC) protocol. The OBU supports essential functions such as message authentication, encryption, and pseudonym generation to preserve user privacy while enabling secure data exchange.

3.1.2 RSU

RSUs are installed along the roadside that facilitate communication between vehicles and central management systems. These RSUs transmit data to vehicles to enhance traffic safety and improve traffic management. They also act as intermediaries in the detection framework, aggregating vehicle data and forwarding it to the Base Station (BS) or Central Authority for further analysis.

3.1.3 CA

This serves as the central management entity for VANETs. During registration, the CA issues them an anonymous identity and a private key, while their true identities are kept confidential and known only to the CA. The CA is also responsible for certificate revocation and system-wide coordination in case of detected anomalies or misbehaving nodes.

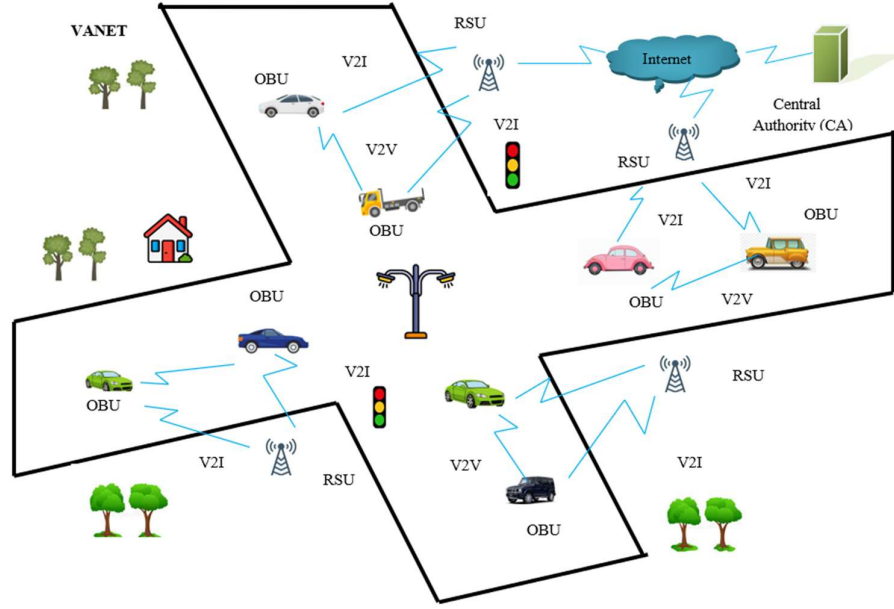


Fig. 2. System model of VANET

3.2 Routing

Routing [14] is the process of establishing and maintaining efficient communication paths between vehicles to facilitate the exchange of information such as safety alerts, traffic updates, and infotainment services. It involves selecting optimal routes for transmitting information, taking into account the highly dynamic topology, and varying communication needs of vehicles on the move. Effective routing ensures reliable, timely delivery of messages, which is essential for safety applications, traffic management, and infotainment services within intelligent transportation systems.

In the proposed framework, routing not only supports data transmission but also plays a crucial role in preserving message integrity and preventing message drops or delays caused by malicious behavior.

3.3 Sybil attack detection at BS

A Sybil attack is a security threat in which a malicious entity disrupts normal operations in VANET. Detecting such attacks is crucial because they compromise the integrity and security of the network. Effective detection mechanisms help prevent malicious activities, enable accurate data aggregation, and maintain the overall robustness of VANET. In this model, Sybil attack detection is done at BS, and it is explained in the subsequent part.

The BS acts as the central processing unit, collecting information from RSUs and vehicles for global analysis and decision-making. It facilitates the implementation of a resource-intensive detection model like EFLO_QDCNN, which requires substantial computational power.

3.3.1 Input data

The KDD Cup 1999 dataset [9] remains a foundational resource for developing and testing intrusion detection algorithms, although it is generated using simulated network traffic in a military environment. The number of input data presented in the specific dataset is illustrated as follows,

$$N = \{N_1, N_2, \dots, N_s, \dots, N_z\} \quad (1)$$

where N represents the input database, z implies the total samples and N_s data with the size $[U \times V]$ is utilized as an input for Sybil attack detection.

Although the dataset is not inherently designed for VANETs, its comprehensive labeling and variety of attack types make it suitable for transfer learning and benchmarking detection performance.

3.3.2 Feature selection using histogram intersection matrix

Feature selection is used to find and select the most relevant attributes from the input N_s with the size $[U \times V]$ that contributes to attack detection. This process strengthens the ability of the model to distinguish legitimate and malicious nodes and improves detection accuracy. In this scheme, feature selection is conducted based on a histogram intersection matrix. The Histogram Intersection Matrix compares the

distribution of features between different nodes or data samples by calculating the overlap between their respective histograms. The histogram intersection matrix is expressed as,

$$M_s = 1 - \frac{\sum_x \min(p_x q_x)}{\min\left(\sum_x p_x, \sum_x q_x\right)} \quad (2)$$

where p_x implies candidate feature and q_x represents target feature. The result attained from the feature selection model is specified M_s with size $[U \times X]$, such that $V > X$.

This approach effectively reduces dimensionality, enhances generalization capability, and minimizes noise or irrelevant information, thereby accelerating the convergence of deep learning models.

3.3.3 Sybil attack detection using EFLO_QDCNN

A detection model of Sybil attack identifies and mitigates malicious activities in a network where a single adversary creates multiple fake identities to disrupt normal operations. Effective Sybil attack detection is critical for preserving network integrity, ensuring fair resource distribution, and maintaining trust among participating entities. In this model, QDCNN is used for Sybil attack detection by using selected features M_s with size $[U \times X]$. By effectively identifying Sybil attacks, the detection systems aim to maintain the integrity, trustworthiness, and security of the network.

a) Structure of QDCNN

The QDCNN [10] structure combines quantum-inspired mechanisms to enhance sybil attack detection. Initially, the input layer receives the selected feature M_s , which is then processed through multiple dilated convolutional layers. These layers utilized filters with increasing dilation rates, allowing the network to capture wide-ranging spatial and temporal dependencies. The advantage of using dilated convolutions is their ability to extract multi-scale contextual features without increasing computational complexity. The dilated convolutions are integrated to reduce dimensionality and highlight key features. In the quantum-inspired component, simulated quantum layers or parameterized quantum circuits are introduced, and the quantum gates are used to represent complex feature interactions and enable parallel computation. This hybrid mechanism combines classical deep learning with quantum characteristics, improving the model's ability to distinguish between subtle feature variations caused by Sybil nodes. Finally, the network includes one or more fully connected layers and a softmax or sigmoid output layer for classification. The result obtained from the QDCNN is given as,

$$Q_s = \left[\langle M_s, \Phi | H^{\otimes Y} | M_s, \Phi \rangle \right] \quad (3)$$

Where $H^{\otimes Y}$ implies expectation value, M_s indicates selected feature, and the Q_s specified QDCNN outcome. Fig. 3 illustrates sturcture of QDCNN. This layered design ensures the detection model can achieve high accuracy while maintaining low latency, making it suitable for real-time VANET environments.

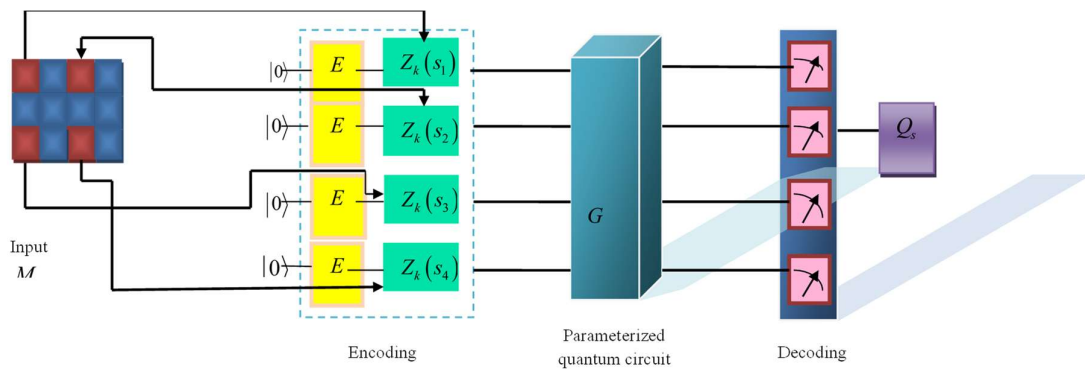


Fig. 3. Architecture of QDCNN

b) Training of QDCNN using EFLO

The training procedure aims to enable the module to accurately distinguish between legitimate nodes and Sybil nodes. As training progresses, the model adjusts its internal weights to improve its ability to correctly classify nodes, and this process improves the generalization of the network to learn patterns from

unseen data for effective attack detection. Here, the hyperparameters of QDCNN are tuned with EFLO. The FLO [12] is a nature-inspired metaheuristic algorithm developed by mimicking the unique defensive behavior of the frilled lizard. The algorithm uses the lizard's sudden frill expansion and escape response as metaphors for escaping local optima and exploring new regions in the searching space. On the other hand, EWMA [11], is used to smooth time series data by giving more weight to recent observations while not entirely discarding older ones. It is particularly useful for solving complex, non-linear, and multi-modal optimization problems.

By combining FLO's exploratory behavior with EWMA's stability in gradient smoothing, EFLO provides a hybrid mechanism that enhances convergence speed and avoids premature stagnation in local optima. The development of EFLO is explained below.

i) Solution encoding

Solution encoding is employed to obtain better outcomes for a given optimization issue in a specified search space χ , such that $\chi \in [1 \times \kappa]$ where κ denotes learning parameters of QDCNN. Each encoded solution corresponds to a unique configuration of QDCNN hyperparameters such as learning rate, kernel size, number of filters, and dilation factors.

ii) Fitness function

The computation of fitness is done by making a comparison among obtained solutions to the target for achieving effective training. The expression of QDCNN is given as,

$$\rho_{fit} = \frac{1}{z} \sum_{s=1}^z [D - Q_s]^2 \quad (4)$$

where ρ_{fit} implies fitness function, z denotes total samples, D represents a target, and Q_s denotes QDCNN outcome. The fitness function minimizes classification loss (e.g., cross-entropy), enabling better convergence of hyperparameter tuning.

iii) Algorithm EFLO

The algorithm of EFLO is explained in the subsequent section.

Step 1-Initialization: The FLO utilizes a group of frilled lizards as its member in a specified search space. Each frilled lizard assigns values to the decision variables based on its specific position in the search space. The total members in the FLO are mathematically modeled as,

$$V = \{V_1, V_2, \dots, V_f, \dots, V_l\} \quad (5)$$

where V implies population matrix, V_f denotes f^{th} lizard in the population, and V_l indicates total lizard in a search space.

Step 2- Fitness function: The fitness function is computed by comparing the obtained solution to the target for attaining effectual hyperparameter tuning of QDCNN. The Fitness value is computed by Eq. (4). This determines how well each lizard's solution performs in training QDCNN.

Step 3-Exploration stage: The hunting strategy is the most distinctive natural behavior of a frilled lizard. The frilled lizard is a sit-and-wait predator and simulates the movement of the frilled lizard toward its prey resulting in significant variations in the positions of the population members. In FLO, the location of a lizard with optimal fitness function is considered a potential prey location. Accordingly, the set of prey locations for each frilled lizard is computed as follows,

$$P_g = \{V_h : Y_h < Y_f \text{ and } h \neq f\} \quad (6)$$

where P_g implies set of candidate prey, V_h denotes member in the population with objective function higher than i^{th} lizard with objective value Y_f .

Let us consider, each frilled lizard randomly selects the candidate prey. Due to the movement of the lizard's, a new location of each member is computed by,

$$v_{f,t}^l = v_{f,t} + j \cdot (YR_{f,t} - B \cdot v_{f,t}), \quad f = 1, 2, \dots, F \text{ and } t = 1, 2, \dots, T \quad (7)$$

Let us consider the following assumptions,

$$v_{f,t}^l = v_{f,t}(d+1) \quad (8)$$

$$v_{f,t} = v_{f,t}(d) \quad (9)$$

$$YR_{f,t} = YR_{f,t}(d) \quad (10)$$

By applying the above considerations, the expression $v_{f,t}^l$ is rewritten as,

$$v_{f,t}(d+1) = v_{f,t}(d)[1 - B \cdot j] + j \cdot YR_{f,t}(d) \quad (11)$$

The standard expression of EWMA is given as,

$$v_{f,t}^A(d) = \mu v_{f,t}(d) + (1 - \mu) v_{f,t}^A(d-1) \quad (12)$$

$$v_{f,t}(d) = \frac{1}{\mu} \left[v_{f,t}^A(d) - (1-\mu)v_{f,t}^A(d-1) \right] \quad (13)$$

By applying Eq. (13) in Eq. (11), the updated solution of EFLO is given as,

$$v_{f,t}(d+1) = \frac{1}{\mu} \left[v_{f,t}^A(d) - (1-\mu)v_{f,t}^A(d-1) \right] + \frac{1}{\mu} j \cdot \mu \cdot YR_{f,t}(d) \quad (14)$$

where j represents random value, $YR_{f,t}(d)$ implies selected prey with dimension t , μ denotes the random value with range $\{1,2\}$. Moreover, if the accomplished fitness function of the new position is better the location of each lizard is updated as,

$$V_f = \begin{cases} V_f^{l1}, & Y_f^{l1} < V_f \\ V_f, & \text{else} \end{cases} \quad (15)$$

where V_f^{l1} implies the latest location of f^{th} the frilled lizard, and its objective function is termed as Y_f^{l1} .

Step 4-Exploitation stage: In this phase, the location of individuals in the population is updated through the retreating strategy of lizards. The new location for each member in the search space is computed as,

$$v_{f,t}^{l2} = v_{f,t} + (1-2j) \cdot \frac{(ub_t - lb_t)}{w}, \quad w = 1, 2, \dots, W \text{ and } t = 1, 2, \dots, T \quad (16)$$

If this latest position has improved fitness value, the location of members is updated as,

$$V_f = \begin{cases} V_f^{l2}, & Y_f^{l2} < V_f \\ V_f, & \text{else} \end{cases} \quad (17)$$

where V_f^{l2} implies a current position of f^{th} the frilled lizard, and Y_f^{l2} denotes objective function.

Step 5-Revaluation of fitness function: The fitness of accomplished result is re-evaluated to achieve a better result for the training process of QDCNN and it is done by Eq. (4).

Step 6-Termination: The above steps are iterated till achieving effectual result for effective training of QDCNN.

4. Result and Discussion

This part evaluates the performance of EFLO_QDCNN designed for detecting Sybil attacks. The effectiveness of the proposed module is compared with its classical systems to expose its efficacy.

4.1 Experimental Setup

The developed Sybil attack detection model, named EFLO_QDCNN is implemented and evaluated using Python on a PC with Windows 10 OS. The essential simulation parameters are explained in Table 1.

Table 1. Simulation parameters

Parameter	Range
road_width	4
lane_count	1
road_length	50
vehicles_per_lane	10
time_steps	100
vehicle_speed	0.5
vehicle_size	2
rsu_radius	1.5
initial energy	100J
Acceleration/Deceleration	$\pm 2.5 \text{ m/s}^2$
Communication Range	250 meters
Channel Bandwidth	10 MHz
Transmission Power	20 dBm
Packet Interval	0.1 s
Tx Energy per Bit	50 nJ/bit
Rx Energy per Bit	30 nJ/bit

4.2 Dataset Description

The KDD Cup 1999 dataset [9] is a widely used benchmark dataset for evaluating intrusion detection systems. It was created for the Third International Knowledge Discovery and Data Mining Tools Competition to distinguish between legitimate and malicious network connections. It contains 5 million connection records, each represented by 41 features covering basic TCP/IP attributes

4.3 Simulation Results

Fig. 4 displays the simulation results of EFLO_QDCNN. Fig. 4 a) shows simulation outcomes by considering time=11.60sec. Here, the green square represents the vehicle, and RSU is shown in blue circles. Moreover, the attack is displayed in Red-squares. Fig. 4 b) illustrates simulation outcomes by considering time=59.40sec.

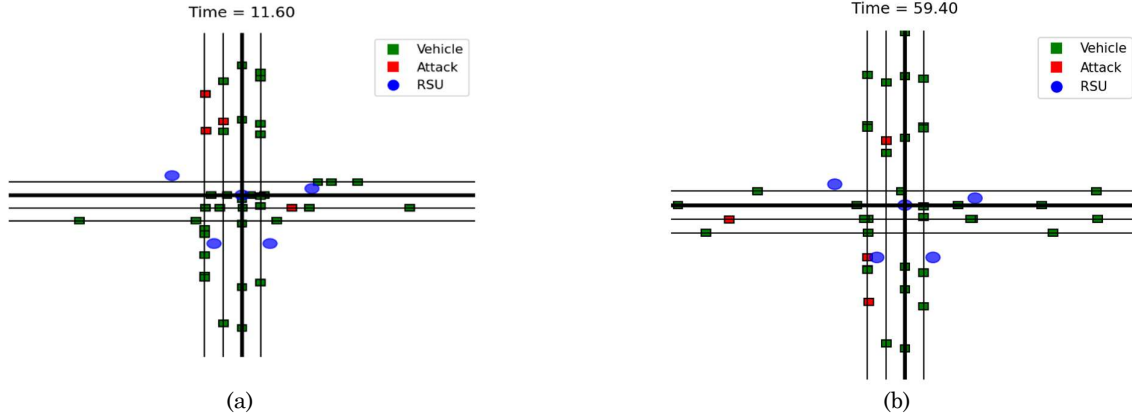


Fig. 4. Simulation results of EFLO_QDCNN, a) considering time=11.60sec, b) considering time=59.40sec

4.4 Evaluation Parameters

The key parameters used to assess the performance of EFLO_QDCNN are described in the following section.

4.4.1 Energy

Energy [15] refers to the computational and resource consumption associated with the detection process of Sybil attacks.

4.4.2 F1-measure

F1-measure [16] is a harmonic mean of precision and recall, providing a balanced assessment of the detection system's accuracy. It combines the capability of the algorithm for identifying true Sybil nodes with its accuracy in avoiding false positives. The F1- measure is determined as,

$$\Gamma_1 = \frac{2C_p}{2C_p + D_p + D_n} \quad (18)$$

where C_p implies true positive, and D_p, D_n denotes false positive and negative.

4.4.3 Precision

The ratio of correctly identified Sybil nodes to the total number of nodes that the detection system classifies as Sybil is termed Precision [16]. The precision is derived as,

$$\Gamma_2 = \frac{C_p}{C_p + D_p} \quad (19)$$

4.5 Comparative Techniques

This part evaluates EFLO_QDCNN by comparing it with existing models to demonstrate the effectiveness of the proposed module. The classical approaches such as EPORP [5], Ensemble Majority Voting approach [6], BSM [7], and LSDCN [8] are considered for evaluation.

4.6 Comparative Evaluation

This part shows a comparative evaluation of EFLO_QDCNN, assessing its efficiency by assuming a node range of 50 to 100.

4.6.1 Evaluation by Considering 50 Nodes

Fig. 5 shows an analysis of EFLO_QDCNN by using 50 nodes. Fig. 5 a) illustrates the assessment using Energy. When rounds=1101, the EFLO_QDCNN achieved an energy of 0.001J, and its existing models, like EPORP, Ensemble Majority Voting approach, BSM, and LSDCN, gained energy as 0.008J, 0.003J, 0.002J, and 0.046J. Fig. 5 b) presents the evaluation of the developed module based on F-measure, the developed scheme and its classical modules gained F-measure as 90.44%, 78.548%, 81.144%, 84.265%, and 85.858% by considering 90% of the training data. The devised approach accomplished enhanced efficiency

of 13.149%, 10.279%, 6.828%, and 5.066% than its previous modules. In Fig. 5c, the analysis of EFLO_QDCNN based on precision is depicted. When training data = 90%, the EFLO_QDCNN accomplished a precision of 90.764%, and its classical approaches gained a precision of 81.454%, 82.45%, 84.53%, and 86.309%. The designed scheme achieved improved effectiveness by 10.257%, 9.160%, 6.868%, and 4.908% than its classical modules.

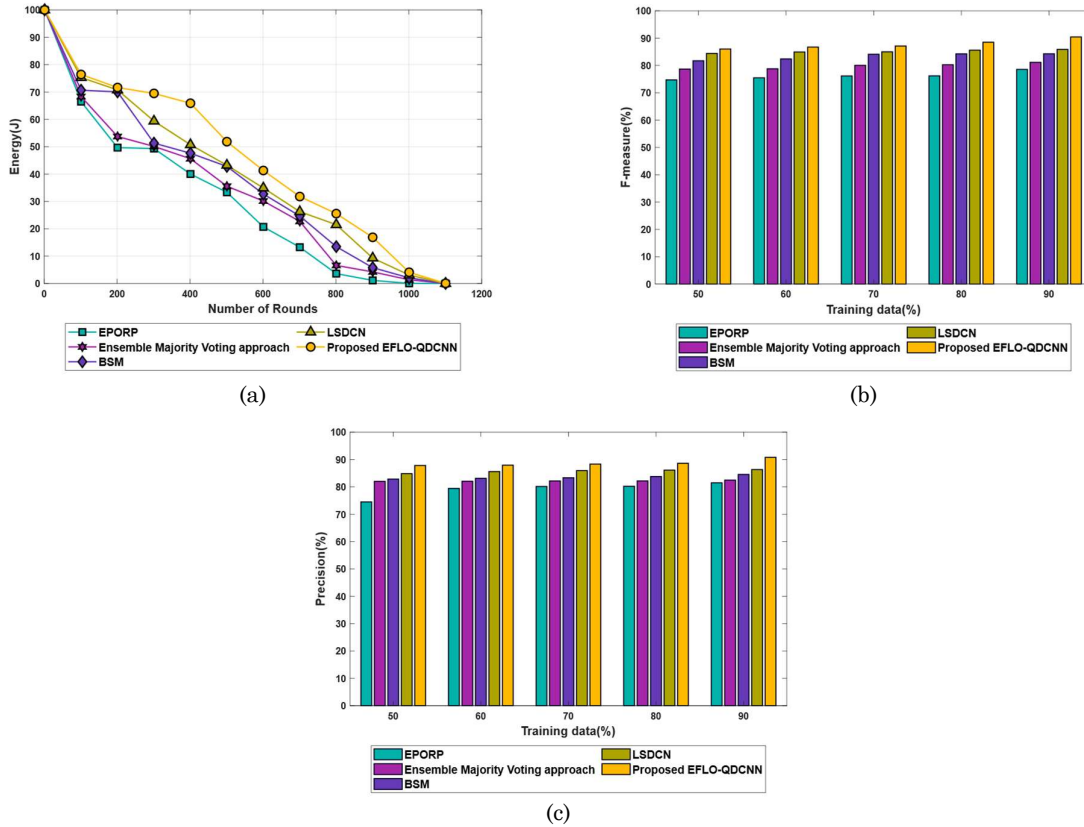


Fig. 5. Assessment of EFLO_QDCNN by assuming 50 nodes, a) Energy, b) F-measure, c) Precision

4.6.2 Evaluation by Using 100 Nodes

Fig. 6 shows the evaluation of EFLO_QDCNN by assuming 100 nodes. Fig. 6 a) displays the evaluation of EFLO_QDCNN using Energy. The EFLO_QDCNN and its conventional modules gained energy of 0.054J, 0.001J, 0.009J, 0.004J, and 0.008J for 1101 rounds. Fig. 6 b) displays the evaluation of the designed scheme using F-measure. The designed approach attained an F-measure of 90.714%, and its classical models, like EPORP, Ensemble Majority Voting approach, BSM, and LSDCN, obtained an F-measure of 80.612%, 82.234%, 83.944%, and 88.211%. The performance improvement accomplished by the presented scheme is 11.136%, 9.348%, 7.463%, and 2.759%, which is higher than conventional approaches. The assessment of EFLO_QDCNN with precision is shown in Fig. 6c. When training data = 90%, EFLO_QDCNN attained a precision of 89.742%, and its conventional approaches gained a precision of 80.211%, 81.908%, 83.167%, and 84.552%. The EFLO_QDCNN achieved enhanced performance of 10.620%, 8.729%, 7.327%, and 5.783% than its classical approaches.

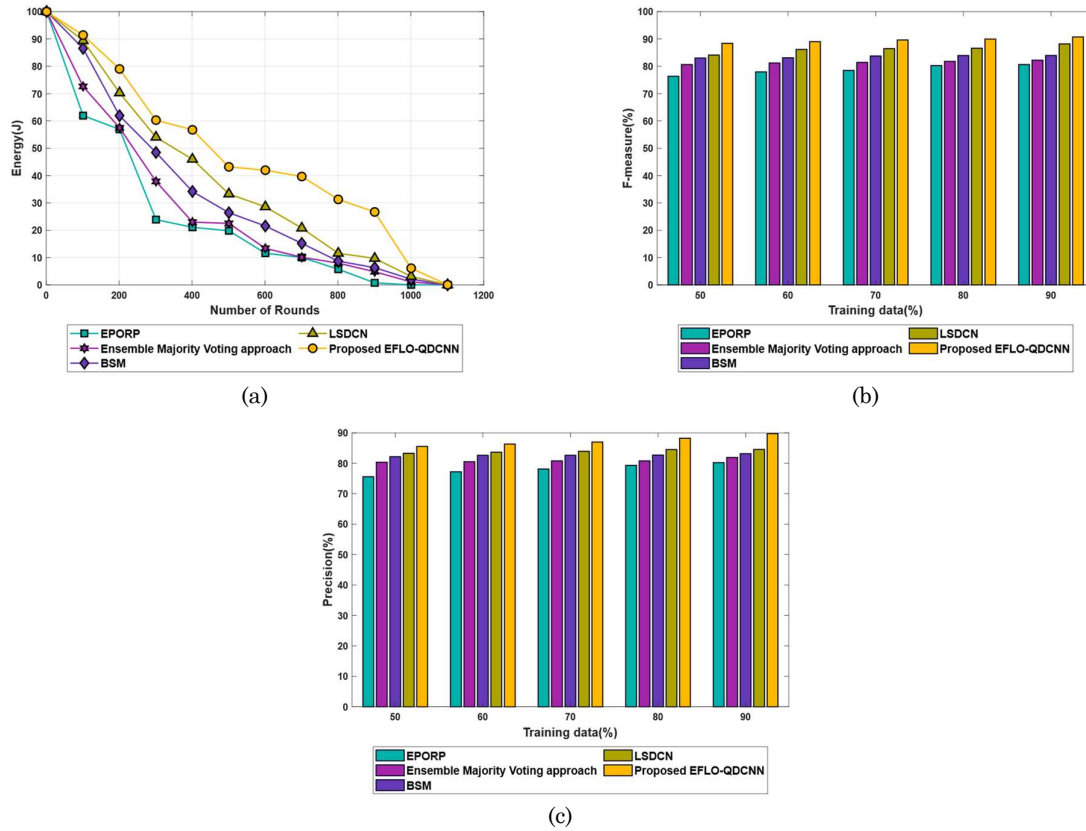


Fig. 6. Analysis of EFLO_QDCNN by considering 100 nodes, a) Energy, b) F-measure, c) Precision

4.7 Comparative Discussion

The comparative discussion of EFLO_QDCNN is detailed in Table 2. The EFLO_QDCNN and its classical approaches attained energy as 0.054J, 0.001J, 0.009J, 0.004J, and 0.008J by assessing 1101 rounds. High energy efficiency ensures that the detection system can operate continuously without significantly impacting vehicle performance or requiring frequent maintenance. The designed approach attained an F-measure of 90.714%, and its classical schemes, like EPORP, Ensemble Majority Voting approach, BSM, and LSDCN, attained an F-measure of 80.612%, 82.234%, 83.944%, and 88.211%. A high F-measure signifies that the detection mechanism is more effective for identifying malicious nodes and is efficient in avoiding the misclassification of legitimate vehicles. The EFLO_QDCNN accomplished a precision of 89.742%, and its conventional approaches gained a precision of 80.211%, 81.908%, 83.167%, and 84.552%. High precision enhances the ability of the network to identify and isolate malicious nodes. Moreover, the EFLO_QDCNN has gained Energy, F-measure, and precision as 0.054J, 90.714%, and 89.742% by assessing with 100 nodes.

Table 2. Comparative discussion

Data	Techniques /Metrics	EPORP	Ensemble Majority Voting approach	BSM	LSDCN	Proposed EFLO_QDCNN
Nodes=50	Energy (J)	0.001	0.008	0.003	0.002	0.046
	F-measure (%)	78.548	81.144	84.265	85.858	90.440
	Precision (%)	81.454	82.450	84.530	86.309	90.764
Nodes=100	Energy (J)	0.001	0.009	0.004	0.008	0.054
	F-measure (%)	80.612	82.234	83.944	88.211	90.714
	Precision (%)	80.211	81.908	83.167	84.552	89.742

5. Conclusion

Detecting Sybil attacks is essential for preserving the trustworthiness and efficiency of VANETs, and it is crucial for maintaining secure and reliable communication between vehicles. In a Sybil attack, a single malicious vehicle produces multiple fake characteristics to mislead other vehicles or infrastructure, leading to issues such as false traffic congestion reports, disruption in routing protocols, and manipulation of

location-based services. Classical detection models often fail to address the dynamic and high-mobility nature of VANETs. To address these challenges, this research proposes the EFLO_QDCNN framework for the effective detection of Sybil attacks. The process begins with a VANET simulation and secure routing communication. Subsequently, the detection of the Sybil attack is carried out at BS. Initially, input data undergoes feature selection based on the Histogram Intersection metric. The selected features are then subjected to QDCNN for Sybil attack detection. Moreover, the hyperparameters of QDCNN are tuned using EWMA-FLO. Moreover, EFLO_QDCNN gained Energy, precision, F1-measure as 0.054J, 90.714%, and 89.742%. In future expansion, the presented approach will be incorporated with an attention module to consider the most appropriate characteristics within highly dynamic network environments for improving robustness against sophisticated attack strategies.

Compliance With Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

- [1] R. Gilles Engoulou, M. Bellache, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, no. 1-13, 2014.
- [2] . F. Qu, Z. Wu, . F.-Y. Wang and W. Cho, "A security and privacy review of VANETs. *IEEE Transactions on Intelligent Transportation Systems*," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985-2996, 2015.
- [3] M. Baza, M. Nabil, N. Bewermeier, K. Fidan, . M. Mahmoud and M. Abdallah, "Detecting sybil attacks using proofs of work and location in VANETS," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 39-53, 2020.
- [4] B. Karthiga, D. Durairaj, N. Nawaz, T. Kesavan Venkatasamy, G. Ramasamy and A. Hariharasudan, "Intelligent intrusion detection system for VANET using machine learning and deep learning approaches," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 5069104, 2022.
- [5] N. C Velayudhan, Dr. A. Anitha and M. Madanan, "Sybil attack with RSU detection and location privacy in urban VANETs: An efficient EPORP technique," *Wireless Personal Communications*, no. 1-29, 2022.
- [6] S. Azam, M. Bibi, R. Riaz, S. Shahla Rizvi, and S. Jin Kwon, "Collaborative learning based Sybil attack detection in vehicular ad-hoc networks (VANETS)," *Sensors*, vol. 22, no. 18, p. 6934, 2022.
- [7] Z. Zhang, Y. Lai, Y. Chen, J. Wei, and Y. Wang, "Detection method to eliminate Sybil attacks in Vehicular Ad-hoc Networks. *Ad Hoc Networks*," vol. 141, p. 103092, 2023.
- [8] 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.
- [9] "KDD Cup 1999 Dataset," [Online]. Available: "<https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>",. [Accessed March 2025].
- [10] Y. Chen, "QDCNN: quantum dilated convolutional neural network," 2021.
- [11] W. Febrina and W. Fitriana, "Exponential weight moving average (EWMA) control chart for quality control of crude palm oil product," *International Journal of Management and Business Applied*, vol. 1, no. 1, pp. 19-27, 2022.
- [12] I. Abu Falahah, O. Al-Baik, I. Leonova, S. Alomari, G. Bektemyssova, O. Parkash Malik, F. Werner, M. Dehghani, and S. Gochhait, "Frilled lizard optimization: A novel nature-inspired metaheuristic algorithm for solving optimization problems," *Preprints*, p. 2024030898, 2024.
- [13] Y. Genc, C. Korkuc, N. Aytas, E. Afacan, . M. H. Sazli and E. Yazgan, "A novel identity-based privacy-preserving anonymous authentication scheme for vehicle-to-vehicle communication," vol. 29, no. 2, 2023.
- [14] R. Muthaiyan, S. Senthilkumar, C. Vijesh Joe, and M. Kavitha, "Reliability based multi-objective optimized routing protocol for VANETs using a pelican optimization algorithm," *Discover Applied Sciences*, vol. 7, no. 4, p. 228, 2025.
- [15] A. R. Abdellah, A. Muthanna, and A. Koucheryavy, "Energy estimation for VANET performance based robust neural networks learning," *Springer International Publishing*, pp. 127-138, 2019.
- [16] H. Kumar Bhuyan and V. Ravi, "An integrated framework with deep learning for segmentation and classification of cancer disease," *International Journal on Artificial Intelligence Tools*, vol. 32, no. 02, p. 2340002, 2023.