International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V73I11P124

Volume 73 Issue 11, 336-348, November 2025

Review Article

MANET Intrusion Detection Model Based on Dynamic Lyrebird Optimization with Hybrid Convolutional Neural Network and Long Short-Term Memory

Divya Boya[1], Syed Shabbeer Ahmad[2]

[1]*Department of CSE, UCE, Osmania University, Hyderabad, Telangana, India.*
[2]*Department of CSE, MJCET, Hyderabad, Telangana, India.*

[1]*Corresponding Author : divyaboya1291@gmail.com*

Received: 17 September 2025 Revised: 12 November 2025 Accepted: 15 November 2025 Published: 25 November 2025

Abstract - *Wireless portable nodes with a decentralized and distributed network form a Mobile Ad hoc Network (MANET) that directly links without any fixed centralized administration or communication base station. Continuously moving the MANET nodes in arbitrary and random directions leads to difficulties, such as security threats in networks. Node energy and mobility are constantly changing due to node movements and the resulting changes in topology and direction. The topmost challenges in MANET are energy consumption and security. Compared to the previous routing protocols, the Optimization methods are more efficient for Cluster Head (CH) selection because they provide optimal solutions to address the issues. Due to the mobility of nodes in MANET, several issues have been raised, including sudden changes, reliability, security, power consumption, and path maintenance. To overcome these challenges, this work presents a novel, optimized deep learning model. The clusters are formed using Spectral Clustering (SC), followed by the CH selected using Dynamic Lyrebird Optimization (DLO) for optimal routing and energy consumption in MANET. Different intrusions are detected by using Sailfish Optimization (SO) with a Hybrid Convolutional Neural Network and Long Short-Term Memory (CNN-LSTM) model. The varying network densities and different parameters, along with the NS-3 Tools, are used to conduct extensive simulations. The proposed work demonstrates improvements. In intrusion detection, it extends network lifespan and balances energy consumption when compared to existing state-of-the-art models.*

Keywords - *Spectral clustering, MANET, Dynamic lyrebird optimization, Sailfish optimization, and Hybrid CNN-LSTM.*

1. Introduction

Mobile Ad-hoc Networks (MANETs) are self-configuring wireless systems in which nodes communicate with each other without centralized control or fixed infrastructure [1]. MANETs have high levels of flexibility, as they can link to other networks or devices when an external communication channel is accessible. The MANETs have become an important part of modern wireless technology because of their low cost, ease of installation, and ability to provide mobility and communication in any place [2]. A MANET is composed of mobile nodes that are free to move and can form themselves within the transmission range. These dynamically changing positions of these nodes cause a constant change in the network topology, making the connecting links of the communication dynamic and of a transient nature [3]. There has been an explosion of wireless devices and mobile computing, and MANETs are today being used in many different environments, such as in military missions, disaster recovery, and emergency communications. These networks have numerous security, performance, and stability issues despite their portability and flexibility. The vulnerability of MANETs to routing problems, energy loss, and other security risks is higher because they are not permanently structured and centrally regulated. Moreover, the frequent disconnection of the linkage and limited bandwidth reduce the network performance in general [4, 5]. Since the old systems do not have relevant firewall systems and secure route policies, they often fail in safeguarding the information being sent about them. Due to this, MANETs can easily be affected by malicious or self-centered nodes that disrupt network operations. An Intrusion Detection System (IDS) [6] is one of the most appropriate tools to detect such malicious activities in MANETs. To detect anomalous behavior that could indicate security threats, Intrusion Detection Systems (IDS) observe the network traffic or activities of nodes. There are Network-Based (NIDS) and Host-Based (HIDS), and this is determined by the way these components are implemented [7]. Typically, they use some means, such as reputation-based, anomaly-based, or signature-based detection. However, existing models of IDS often possess such limitations as false

alarms are very high, resource usage is also very high, and they are not very flexible in dynamic and encrypted network settings [8]. The current methods of intrusion detection that are considered to be used in MANETs are based on single optimization or fixed routing protocols, which are not suitable in networks with high dynamic activity and energy limitations.

Such methods often cannot be effective in selecting cluster heads that can be used in stable routing, and also often lose their high detection rates as the node mobility increases. Furthermore, many of the currently existing systems that are based on optimization cannot effectively balance the power consumption and adapt to the network changes in real time. This in turn puts a gaping research gap to develop one model capable of achieving both high-accuracy intrusion detection as well as energy-efficient routing in dynamic MANET settings. This research paper proposes a new MANET. The proposed model employs a hybrid Convolutional Neural Network-Long Short-Term Memory (CNN-LSTM) architecture tuned by Sailfish Optimization (SFO) to detect intrusions accurately, Dynamic Lyrebird Optimization (DLO) to select stable and energy-aware cluster heads, and Spectral Clustering (SC) to form efficient clusters. By optimizing energy consumption, increasing packet delivery, and accurately identifying attacks like blackhole and Denial of Service (DoS) even under varying mobility and node density conditions, this hybrid framework, in contrast to earlier methods, improves network performance and security. The remaining sections of this paper are arranged as follows: Section 2 presents the literature review on MANET intrusion detection methods.

Section 3 gives the proposed methodology and the algorithm design. Section 4 describes the simulation setup and experimental outcomes, while Section 5 presents the conclusion and outlines possible future research directions of the paper. Since MANETs are finding more applications in mission-critical systems such as emergency response, tactical military communication, and intelligent transport systems, where continuous and secure transmission of data is essential, the issue of intrusion Detection and routing optimization in MANETs should be considered. Any delay, loss of data, or Malicious Intrusion can cause serious operational failure. Due to the fact that the traditional routing and intrusion detection systems were often designed to suit a static or semi-dynamic network, these systems cannot be used in MANETs where mobility of nodes, topology change, and energy limitations are taking place simultaneously. Section 3 elaborates on the proposed methodology and design of the algorithm. Section 4 presents the simulation configuration and experiment findings, while Section 5 provides the conclusion and research directions of the paper.

Since MANETs are also finding their way into operations that are of the mission-critical type, such as emergency response, tactical military communication, and intelligent transport systems, where continuity and uninterrupted data delivery are of paramount importance, Intrusion detection and routing optimization in MANETs should be addressed. Any form of delay, Loss of data, or malicious Intrusion can lead to serious operational failures since the traditional Routing and Intrusion detection system is often designed to support a static or semi-dynamic network. It is inadequate for MANETs, which are networks characterized by topology changes, node mobility, and limited energy supplies.

Unlike previous models, the study will develop a tiered system, which connects intrusion detection and routing. The framework incorporates energy consumption, stability, and security under one design and not as isolated processes. The Spectral Clustering and Dynamic Lyrebird Optimization (DLO) algorithm ensures that routing decisions consider connectivity and energy balance in addition to routing and security as two different problems. Moreover, the Sailfish-optimised CNN-LSTM (SFO-CNN-LSTM) also presents deep temporal and spatial learning to detect the pattern of an attack in real-time. In comparison with the existing models of IDS optimised by means of deep learning or other optimization methods, the presented hybrid approach can not only enhance the detection accuracy but also increase the network lifetime and ensure the maintenance of the same operation in dynamic MANET conditions.

2. Related Works

Due to the fast development of wireless communication systems, Mobile Ad-hoc Networks (MANETs) have become a viable service of decentralized communication and dynamic data transfer. Nevertheless, the openness of wireless media and the lack of a fixed infrastructure expose MANETs to a wide variety of vulnerabilities and security and intrusion-detection research issues that remain. The design of a safe and energy-efficient Intrusion Detection System (IDS) in the MANETs is still a very important activity. The authors Prasad et al. [9] developed the Secure Energy Routing (SER) protocol to address security threats during routing in MANETs. The model incorporated efficient routing with intrusion monitoring, which detected and countered attacks. Despite SER enhancing the reliability of packet forwarding, it remained prone to overhead and slower convergence in high-mobility settings.

In intrusion detection, Singh et al. [10] proposed a Principal Component Analysis-based Fuzzy Extreme Learning Machine (PCA-FELM) model to enhance classification accuracy. This hybrid learning approach achieved 99.08% reliability; however, it was limited by its dependence on fixed input features, making it unsuitable for dynamically changing MANET environments. Prasad et al. [11] proposed a learning-based intrusion detection system that analyzed node behavior using data extracted from network packets. Their algorithm demonstrated good detection accuracy under static conditions but was inefficient in random broadband or rapidly changing topologies, which reduced its

scalability. Reka et al. [12] presented a Centrality Coati Optimization Algorithm based on the Cluster Gradient method to detect multiple attacks in MANETs. Their approach utilized clustering inspired by network centrality and applied a multi-head self-attention gated graph Convolutional Network (MSA-GCNN) to detect Denial-of-Service (DoS) and zero-day attacks. While this method reduced IDS traffic and memory consumption, its computational cost remained high, and it became more vulnerable to complex coordinated attacks. To improve trust and data security in MANETs using 5G-enabled environments, Alghamdi et al. [13] developed a Trust-Aware Intrusion Detection and Prevention System (TA-IDPS). This approach employed lightweight cryptographic techniques and a deep belief network to classify data as normal or malicious. Although it enhanced intra-cluster routing security, the system was difficult to scale and required careful parameter tuning to remain efficient. Srilakshmi et al. [14] introduced a Genetic Algorithm with Hill Climbing (GAHC) for optimal multipath routing.

Cluster heads were selected using an improved fuzzy C-means approach to resist packet-dropping attacks. The model achieved a detection rate of 91% but suffered from unpredictable performance due to high energy consumption and unbalanced node workloads. Intrusion detection systems based on deep learning have also attracted attention in recent research.

The hybrid algorithm, namely, Rider Optimization and Spotted Hyena Optimizer (S-ROA), was proposed by Karthik et al. [15] to optimize a Residual Network-based Feature Extraction (RNBFE) model. Their model enhanced the extraction of features, which are used to classify attacks through a fuzzy neural classifier at the cost of producing a heavy model, which was not as applicable in distributed MANETs. Meddeb et al. [16] came up with Intrusion Detection System (Stacked AE-IDS), a Stacked Autoencoder-based system that applied deep neural networks in modelling DoS attacks in MANETs. This method enhanced the accuracy of detection and minimized redundant features, yet it was not able to generalize to a variety of attack types and used labelled data. Based on the literature review, it can be noted that notable advancements have occurred in the application of optimization and deep learning to MANET intrusion detection.

Nevertheless, the majority of the existing approaches consider routing efficiency or intrusion accuracy but not both at the same time. Most of the models can work well in a controlled environment, but do not remain stable in high mobility and large-scale deployment. Therefore, it is still necessary to use a hybrid and flexible framework that unites clustering, optimization, and deep learning to find a middle ground with regard to energy consumption, a high level of intrusion detection, and routing stability. This encourages the design of the proposed model based on Dynamic Lyrebird Optimization (DLO) with Spectral Clustering and Hybrid CNN-LSTM architecture driven by Sailfish Optimization (SFO), as shown in the next section.

3. Proposed Framework

This framework should be designed to realise energy-efficient routing and correct intrusion detection in MANETs by incorporating Spectral Clustering (SC) to form clusters, Dynamic Lyrebird Optimization (DLO) to select the Cluster Head (CH), and a Hybrid CNN-LSTM model that has been trained on Sailfish Optimization (SFO).

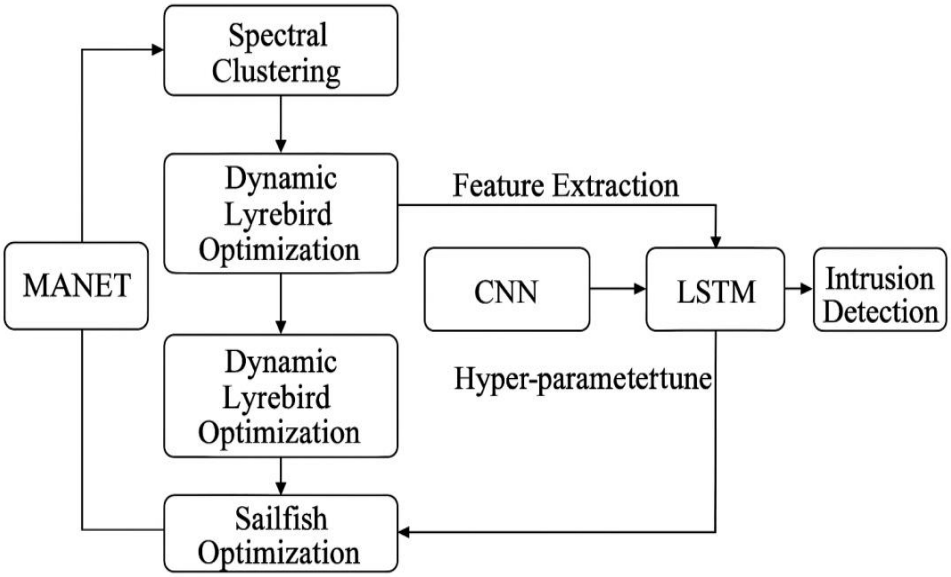

Fig. 1 Proposed SC-DLO-SFO-CNN-LSTM framework for MANET intrusion detection

3.1. Cluster Formation

In MANET, information is disseminated among multiple mobile nodes without the help of any centralised infrastructure. Clustering increases the scalability, minimises the overhead communication, and increases network lifetime because MANETs are self-organising and dynamic. To form clusters in the suggested system, the Spectral Clustering (SC) model is employed [17]. Spectral clustering groups mobile nodes based on the similarity of their energy status, distances, and connectivity characteristics. The SC process is decentralised, and it does not need a control node. It is done through the calculation of the eigenvectors of the Laplacian matrix, which is based on the node similarity graph. The similarity matrix between two nodes $i$and $j$is calculated as:

$$S(i,j) = e^{-\frac{\|x_i - x_j\|^2}{2\sigma^2}} \quad (1)$$

Where $x_i$and x_jThe position vectors of the two nodes, and $\sigma$is the scaling factor. The inverse graph representation and eigenvector-based feature mapping facilitate the identification of clusters with high internal connectivity and low inter-cluster dependency. Consequently, nodes are grouped efficiently, minimizing routing load and extending network lifetime.

By applying SC, the MANET achieves better scalability, lower overhead, and more stable communication paths due to balanced cluster formation.

3.2. Cluster Head Selection

After clusters are formed, Dynamic Lyrebird Optimization (DLO) is employed to select optimal Cluster Heads (CHs). Inspired by the lyrebird's behavior of scanning, escaping, and hiding from predators, DLO mimics a balance between global search (exploration) and local refinement (exploitation) for optimization.

3.2.1. Solution Initialization

While constituting the population of lyrebirds, the metaheuristic population-based optimization called the DLO algorithm is used to choose CH [18]. For problem-solving space, the members of the search power are provided with suitable solutions through DLO. The decision variables are represented by a vector in each element, modeling each lyrebird. The position with decision variable values is determined via the DLO algorithm. The following equations initialize the population and problem-solving space.

$$W = \begin{bmatrix} W_1 \\ \vdots \\ W_j \\ \vdots \\ W_M \end{bmatrix}_{M\times n} = \begin{bmatrix} w_{1,1} \cdots w_{1,D} \cdots w_{1,n} \\ \cdots \ddots \vdots \cdots \\ w_{j,1} \cdots w_{j,D} \cdots w_{j,n} \\ \cdots \vdots \ddots \vdots \\ w_{M,1} \cdots w_{M,D} \cdots w_{M,n} \end{bmatrix}_{M\times n} \quad (2)$$

$$w_{j,D} = B_{low_D} + Rnd \cdot \left(B_{up_D} - B_{low_D}\right) \quad (3)$$

Here, the DLO member clusters are with the matrix population. The decision variables and the number of lyrebirds (clusters) are$n$and$N$. At d^{th} variable, the upper and lower bounds becomeB_{up}andB_{low}. Evaluate the objective function and the objective function present in the random variable.Rnd To the interval [0, 1].

$$of = \begin{bmatrix} of_1 \\ \vdots \\ of_j \\ \vdots \\ of_M \end{bmatrix}_{M\times n} = \begin{bmatrix} of(W_1) \\ \vdots \\ of(W_j) \\ \vdots \\ of(W_M) \end{bmatrix}_{M\times 1} \quad (4)$$

The cluster-based objective function vector is of, and the j^{th} objective function is of_j.

3.2.2. Escaping Mechanism

Based on the search space, update the population member positions of clusters and account for a wide variation in their positions due to the safe area movement of the lyrebird. For the problem-solving space, scanning of various areas, such as global search for exploration. The safe area is considered an excellent objective function along with the population member's position.

$$sa_j = \left\{W_k, of_k < of_j and k \in \{1,2,..,M\}\right\} \quad (5)$$

The safe area set of the lyrebird is$sa_j$with the k^{th} row of the lyrebird matrix W_k.

$$W_j = \begin{Bmatrix} W_j^{p_1}, of_j^{p1} \le of_j \\ W_j, otherwise \end{Bmatrix} \quad (6)$$

The calculated new position is$W_j^{p_1}$with the j^{th} dimension based on the objective function of_j^{p1}.

3.2.3. Hiding Mechanism

Due to the search space, update the position of each population member. To achieve the suitable area, the small steps involving movement and the surrounding environment were scanned [19]. Based on local search, the DLO-based exploitation ability is indicated. The following formula enhances the objective function values.

$$W_j^{p_2} = w_{j,k} + \left(1 - 2Rnd_{j,k}\right) \cdot \frac{B_{up} - B_{low}}{t} \quad (7)$$

$$W_j = \begin{Bmatrix} W_j^{p_2}, of_j^{p_2} \le of_j \\ W_j, otherwise \end{Bmatrix} \quad (8)$$

The calculated new cluster's position is $W_j^{p_2}$ with the j^{th} The dimension-based objective function is $of_j^{p_2}$. An iteration counter is *T*.

3.2.4. Repetition Process

Complete the DLO iteration to update each lyrebird position. Perform the final iteration. Save and update the optimal candidate solution at the end of every iteration. The problem solution output is to store the best solution for determining optimal cluster heads and enhancing energy consumption. Algorithm 1 represents the pseudocode for DLO to select CH.

3.3. Intrusion Detection

The MANET intrusion and non-intrusion data were detected using Sailfish optimization with CNN-LSTM, as well as the proposed intrusion detection model, which is further described in the following section.

Algorithm 1: DLO pseudocode to select CH

Start
Initialize the constraints, objective function, clusters, and variables
Set the iteration T and the size of the population M
Equation (2) randomly initializes the node population matrix
Compute the fitness function (CH)
Find the optimal candidate solution
for $T = 1 to T$
for $j = 1 to M$
Equation (3) determines the defense mechanism against attacking predators

If $Rnd_P \leq 0.5$

Equation (4) defines a safe area-based candidate solution
Equation (5) defines a safe area-based candidate solution

Update $W_j = \begin{Bmatrix} W_j^{p_1}, of_j^{p1} \leq of_j \\ W_j, otherwise \end{Bmatrix}$

Else
Equation (7) calculates the new node position

Update $W_j = \begin{Bmatrix} W_j^{p_2}, of_j^{p_2} \leq of_j \\ W_j, otherwise \end{Bmatrix}$

End If
End for
End for
Store the optimal CH
End

3.3.1. Convolutional Neural Network

CNN is used to extract spatial features, and it has two key components: convolution and pooling. With the application of mathematical operations, the filters are applied in the convolutional layer. The input matrix is used for the filter application in generating the feature map [20]. Over the input matrix, the kernel is slid in the vertical and horizontal directions while starting the process. The estimation of the kernel and the input matrix is performed using the dot product, where the components of multiplication are summed with single scalar values. Repeat the process until there is no way to slide. Based on the output matrix, the feature map is determined. The neuron value is estimated with the threshold-based activation function and the estimated feature map. The ReLU is used for the activation function and can be estimated as $ReLU(Z_j) = Max(0, Z_j)$. After applying the activation function, it can be evaluated as follows,

$$Z = f\left(\sum_j^{m \times n} W_j I_j + c\right) \quad (9)$$

The activation function is implied as with the weight of And its respective input value is I. The bias value of the matrix is c. The sizes of the input matrix data are m and n. The subsampling layer is affected by the convolution of the information. The overfitting is mitigated by improved learning based on subsampling. It will mitigate the sample size without impacting the weights of the CNN architecture. The architecture used for the spatial feature extraction and respective intrusion detection is shown in Figure 2.

3.3.2. Long and Short-Term Memory (LSTM)

An extension of a neural feedback network is a Recurrent Neural Network (RNN) that propagates gradients. To alleviate the issues, Long Short-Term Memory (LSTM) can be employed. The design of LSTM is made up of a single cell memory and three gates. The dependencies are captured via LSTM [21]. Figure 3 represents the basic LSTM structure.

$$Z = \begin{bmatrix} H_{t-1} \\ y_t \end{bmatrix} \quad (10)$$

$$F_t = \beta(M_F \cdot Y) + F_b \quad (11)$$

Where Z represents the input layer, and the forget layer has F_b the bias based on the forget gate? The sigmoid function updates the input gate layers.

The cell state adds the new vector, and the forget gate decides the information, and then the new vector values are updated.

$$j_t = \delta\left(M_j \cdot Z\right) + B_j \quad (12)$$

$$OP_t = (M_{OP} \cdot Z) + B_j \quad (13)$$

The sigmoid function is used to decide the output layer.

The Tanh layer passes the results to the LSTM output.

$$D_t = F_j \oplus D_{t-1} + j_t \oplus tanh(M_d \cdot W + B_D) \quad (14)$$

$$g_t = OP_t \oplus tanh(D_t) \quad (15)$$

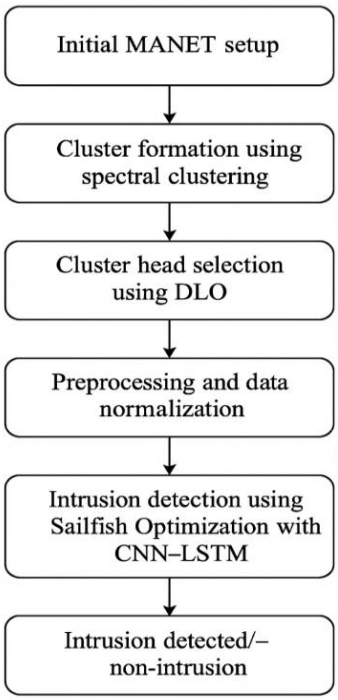

Fig. 2 Intrusion detection in MANET is performed based on the CNN, and its architecture is represented with the feature map

3.3.3. Sail Fish Optimization Algorithm

For better tuning of the hybrid CNN-LSTM parameters, the proposed SFO is utilized. The sailfish and its respective behavior are taken for the SFO algorithm. The individual and the population are initialized at the initial stage, and it can be used for fine-tuning. The overall population of the SFO is described as,

$$SF(t) = \{SF_1, SF_2, .., SF_b\} \quad (16)$$

The specific intrusion detection based on the current population is determined for $SF(t)$ each mobile node, and the respective solutions are describedSF.

The Fitness value to analyze the optimal solution is formulated using the following equation.

$$SF_{fit} = \begin{bmatrix} SF_{fit_1} \\ SF_{fit_2} \\ \vdots \\ SF_{fit_n} \end{bmatrix} \quad (17)$$

The sailfish value at the k[th] dimension is $SF_{fit_{j,k}}$for several nodes. a. With the sardines, the sailfish's rostrum got injured. The locations are saved for each iteration. The Sailfish elite location is Z^j_{Elite}, and the injured sardine is Z^k_{Injur} at the j[th] iteration. The sailfish attack the prey school, and the hunting success rate is promoted with the new location updated with the following equation,

$$Z^j_{New} = Z^j_{Elite} - \rho_j \times \left(Rdn(0,1) \times \left(\frac{Z^j_{Elite} - Z^j_{Injur}}{2} \right) - Z^j_{Old} \right) \quad (18)$$

The location of the elite and the injured is described as $Z^j_{Elite}$and $Z^j_{Injur}$with the random limits of 0 and 1. The coefficient $\rho_j$can be described as,

$$\rho_j = 2 \times Rdn(0,1) \times MP - MP \quad (19)$$

The number of prey is denoted as MP, and every iteration, the location is updated with the parameters such as Botox optimization, and can be enhanced with the following equation.

$$MP = 1 - \left(\frac{B_{SF}}{B_{SF} + B_{botox}} \right) + SB_j \quad (20)$$

The decision variables of the proposed optimization to enhance the fine-tuning of the parameters are implied as $SB$with the sailfish and Botox members $B_{SF}$and B_{botox}. The group hunting is initiated with the slaughter of sardines, and in each iteration, the upgradation of sailfish and power attack are mimicked in this process using the current locations. At the jth iteration, the new location is described with the $Z^j_{New,SF}$as,

$$Z^j_{New,SF} = Rnd \times \left(Z^j_{Elite} - Z^j_{Old} + RA \right) \quad (21)$$

The location of the current sardine and the elite are described as $Z^j_{New,SF}$and Z^j_{Elite}. The optimal solution for finding solution for intrusion detection is RA.

$$RA = R \times \left(1 - (2 \times iteration \times \vartheta) \right) \quad (22)$$

The power attack is reduced linearly from R to 0 with the coefficients R and ϑ. The locations and number of variables can be estimated with the $\eta$and κ.

$$\mu = D_j \times RA \quad (23)$$

$$\kappa = SF_A \times RA \quad (24)$$

The number of sardines and the variables are formulated as SF_AandD_j. The parameters, such as the bias factor and the weight coefficient, are updated with the location of the sailfish and the injured sardine.

The best values are obtained through the repeated process. The number of population and the flowchart for the proposed algorithm are framed in Figure 4.

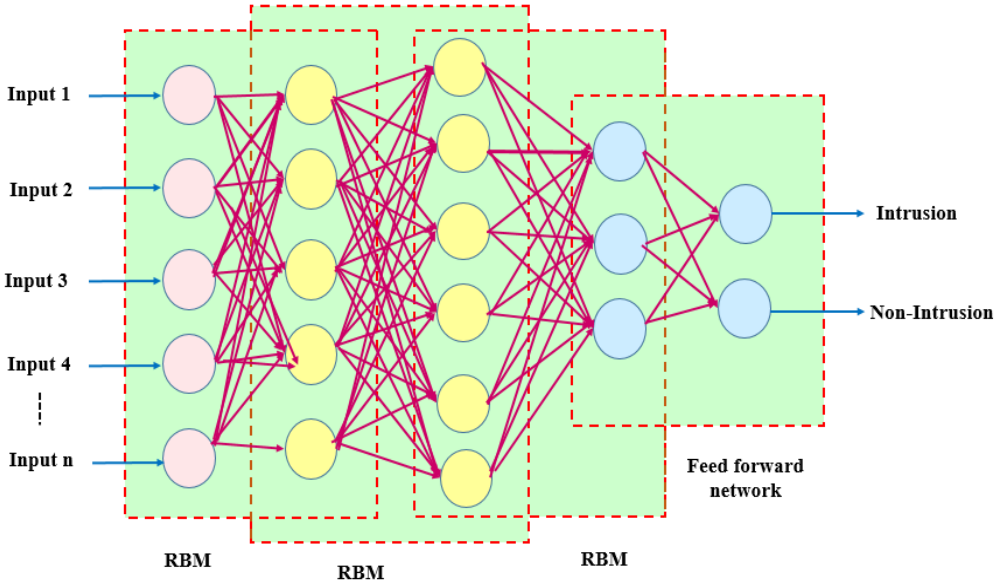

Fig. 3 The basic LSTM structure

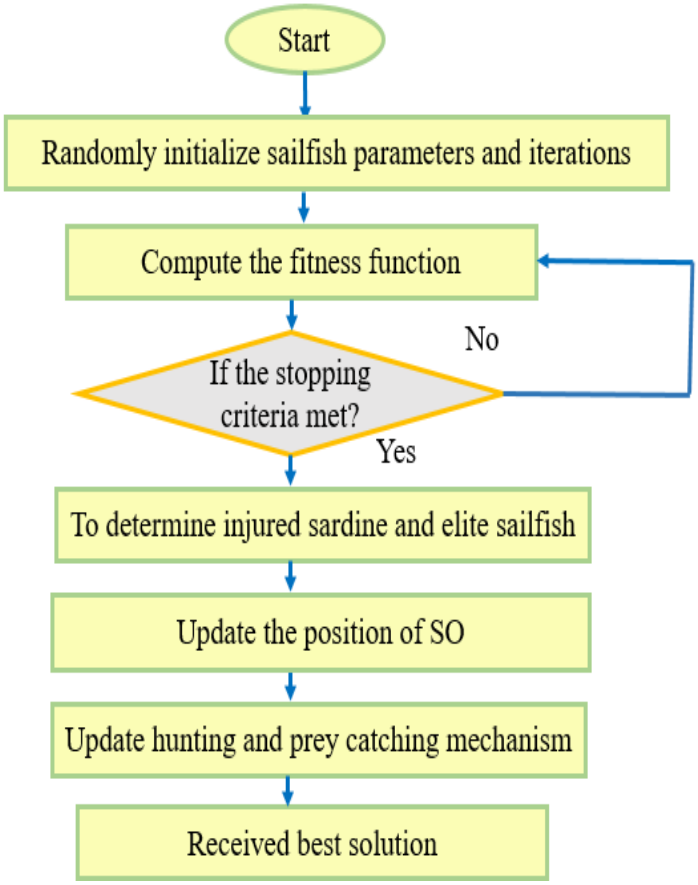

Fig. 4 Flowchart based on the SO algorithm

3.3.4. SO with CNN-LSTM for Intrusion Detection

The Intrusion in MANET is detected by using SO with CNN-LSTM, thereby improving the accuracy and security. From the data, the hierarchical spatial features were extracted by applying pooling and convolutional layers. This CNN-LSTM network receives spatial features-the sequential patterns in the data captured via LSTM, which are critical for black-hole and flooding attacks. To avoid the issues in long-term dependencies, the SO algorithm tunes the weights of the LSTM.

The CNN-LSTM model-based hyperparameters, such as dropout rates, number of LSTM units, learning rate, kernel size, and the number of CNN layers, were optimized via the SO algorithm. Normal traffic, including DoS and black hole attack classes, is represented in each node. The fully connected layer passes the output from the LSTM. Each class probability is determined by applying the softmax function. The computational overhead and false positives are minimized, resulting in enhanced classification performance.

3.3.5. Comparative Analysis with Existing Models

To evaluate the effectiveness of the proposed framework, its performance was compared with four existing state-of-the-art models: Secure Energy Routing (SER) [9], PCA-FELM [10], MSA-GCNN [12], and GAHC [14]. These models represent various generations of MANET intrusion detection systems, including both traditional optimization-based designs and the latest deep learning approaches. The SER protocol emphasized secure energy routing but lacked flexibility for mobility, resulting in increased end-to-end delays. PCA-FELM was unable to maintain performance in dynamic MANET topologies because it also requires predefined feature sets, which are not accurate in dynamic datasets. MSA-GCNN employed a graph convolutional architecture, which excelled at capturing the relationship between nodes; however, this approach came at the cost of excessive computation, making it impractical for energy-constrained networks.

Evolutionary optimization based on multipath routing (GAHC) delivered good packet delivery and had high energy consumption, but low accuracy in detecting attacks. However, unlike it, the suggested SC-DLO-SFO- CNN-LSTM model combines clustering, metaheuristic optimization, and deep learning in a single framework. The Spectral Clustering (SC) algorithm minimizes communication overhead by creating stable and efficient clusters. The Dynamic Lyrebird Optimization (DLO) is a dynamic algorithm that utilizes energy-sensitive cluster heads, adapting to live network conditions. The Sailfish Optimization (SFO) is a fine-tuning of CNN-LSTM hyperparameters, which improves its ability to learn temporal and spatial characteristics of MANET traffic. This combination has been designed to guarantee energy-efficient routing, as well as high-precision intrusion detection. As the experimental results indicate, the proposed model outperforms all baseline methods in terms of packet delivery ratio, throughput, energy consumption, and detection accuracy. In particular, the model achieved 97.2% detection accuracy, 9.3 Mbps throughput, and an average energy consumption of 3 J, which was up to 25% better in network performance than the old methods. Additionally, the proposed model minimized false positives and achieved a high precision (97%), which exemplifies its strength in various mobility and density scenarios. Compared to previous designs that only optimize one layer of MANET performance, the presented hybrid architecture considers several network dimensions simultaneously, such as stability in clustering, routing efficiency, energy balance, and security detection, which is why it is more suitable for the actual implementation of MANET. From the reviewed literature, it is evident that most MANET intrusion detection systems focus on either routing or security, but not both. Many existing methods fail to adapt under high mobility or energy constraints. Therefore, this study proposes a unified optimization-deep learning framework to achieve efficient routing, low energy consumption, and accurate intrusion detection in MANETs.

4. Result and Discussion

The proposed work aims to provide robust routing that incorporates intrusion detection. The effectiveness of the work can be analysed with the simulation, which is elaborated on in the following section.

4.1. Simulation Setup and Selection of Parameters

The input for each simulation is the application of the exact scenario of packets for every node's motion. The simulation is executed simultaneously and analyzes the motion of packets generated by the nodes. For the simulation, an NS-3 simulator is used. The parameters used to execute the process are listed in Table 1.

Table 1. Parameters

Parameter	Value
Simulation Tool	NS-3
Simulation Area	1000 m × 1000 m
Number of Nodes	100
Mobility Model	Random Waypoint
Node Speed	0–20 m/s
Routing Protocol	AODV
MAC Protocol	IEEE 802.11b
Traffic Type	CBR over UDP
Packet Size	512 bytes
Simulation Time	250 s
Number of Connections	2–10

The simulation uses 100 nodes within a 1000 m × 1000 m space area, and execution is conducted for 250 seconds. The mobility model used is a random waypoint with a maximum speed of 0 to 20 m/s. IEEE 802.11b is used as the MAC layer, and the trace files are used for analyzing the beneficial data

and statistics. To evaluate the effectiveness of the proposed SC–DLO–SFO-CNN-LSTM framework, extensive simulations were conducted using the NS-3 simulator. The experiments were conducted in a Linux-based environment using a 64-bit system with an Intel Core i7 processor and 16 GB of RAM. The MANET environment was configured to emulate realistic node mobility, transmission, and routing conditions. A total of 100 mobile nodes were deployed randomly within a 1000 × 1000 m² area using the Random Waypoint Mobility Model, with node speeds varying between 0 m/s and 20 m/s.

The Ad-hoc On-demand Distance Vector (AODV) protocol was used as the base routing mechanism, and communication was established through the IEEE 802.11b MAC layer. Constant Bit Rate (CBR) traffic was transmitted over UDP connections, with packet sizes fixed at 512 bytes. A 250-second simulation was run on each of the simulations, and 2 to 10 data connections were active at a given time. In the intrusion detection part, a standard NSL-KDD dataset was taken to train and test the hybrid CNN-LSTM model. This spectrum has both normal and attack traffic, which includes cases of Denial of Service (DoS), probe, Remote-to-Local (R2L), and User-to-Root (U2R) attacks. To achieve robustness, 30% of the data were used for testing and 70% for training. Min-max normalization was used to scale the features, ensuring an equal distribution of data. The CNN structure consisted of two convolutional layers (kernel size = 3, stride = 1) with ReLU activation, and a max-pooling layer (pool size = 2). The LSTM model consisted of 64 hidden units and a dropout rate of 0.3 to avoid overfitting. The hyperparameters of the hybrid network were optimized by applying the Sailfish Optimization (SFO) algorithm that maximized the learning rate, epochs, and batch size.

The optimal parameters identified were:

Learning rate	:	0.001
Batch size	:	64
Epochs	:	100
Optimizer	:	Adam

The simulation parameters used for routing evaluation are summarized in Table 1. These settings were chosen to balance computational cost and represent realistic MANET deployment conditions. Each experiment was repeated five times, and the average results were recorded to minimize statistical bias.

4.2. Performance Evaluation

The performance evaluation is the key step in evaluating the proposed work and comparing it with existing works. For the evaluation, the existing works such as SER [9], PCA-FELM [10], MSA-GCNN [12], and GAHC [14] were considered. For the MANET, the work analysed the parameters such as Overhead delay, Packet drop ratio, Packet delivery ratio, energy consumption, and throughput for the routing step.

The visual effect of the Overhead delay is shown in Figure 5. This analysis examines the delays of various works, including SER [9], PCA-FELM [10], MSA-GCNN [12], and GAHC [14], as well as the proposed work.

The delay of the proposed work is lower, at 17ms or less, for a total of 120 nodes, while others are delayed by more than 22 seconds. This demonstrates the robustness and efficiency of the proposed work when conducting routing using the proposed algorithm.

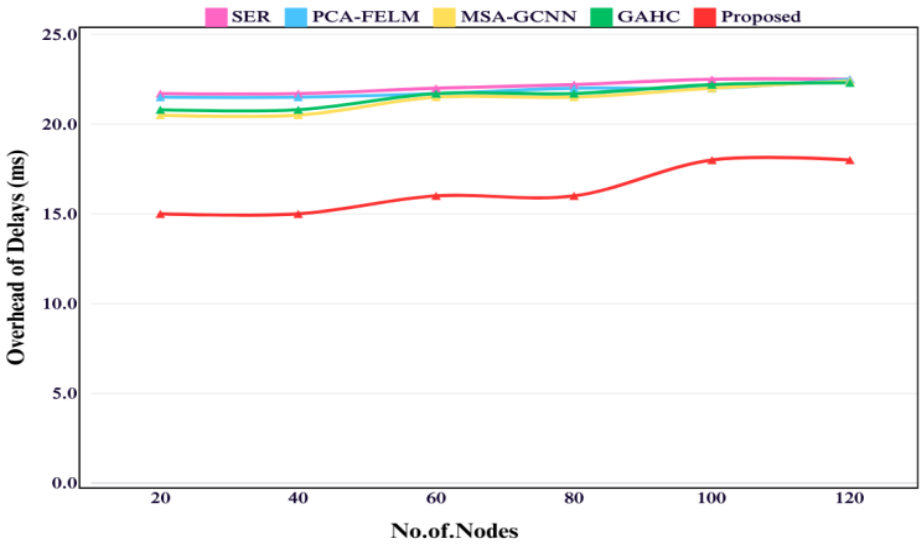

Fig. 5 Performance evaluation based on the OVERHEAD of delays

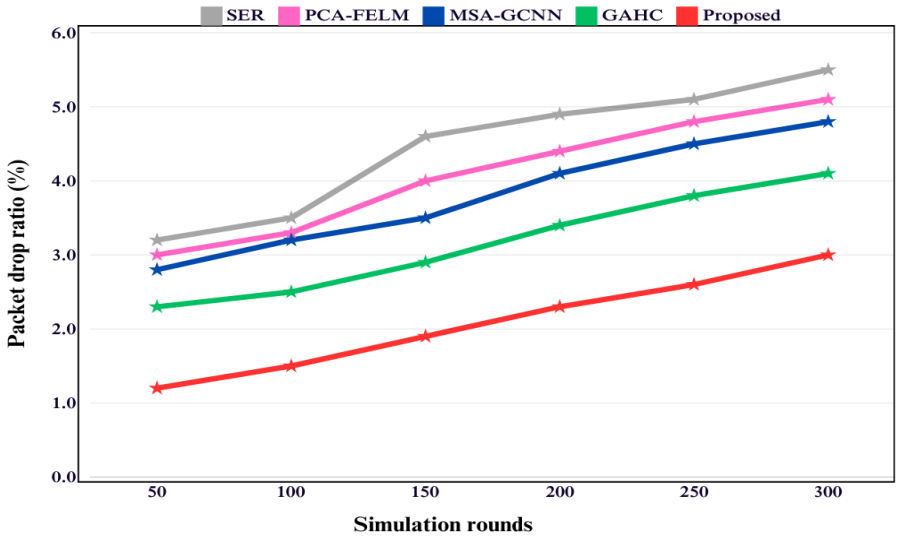

Fig. 6 Performance evaluation based on packet drop ratio

The packet drop ratio is analyzed and graphically illustrated in Figure 6 for the proposed work and state-of-the-art approaches, including SER [9], PCA-FELM [10], MSA-GCNN [12], and GAHC [14]. The proposed work is analyzed to verify its routing system during communication in a MANET. The packet drop ratio is lower for the proposed work, as shown in Figure 3 at the simulation rounds of 300. While other techniques such as SER [9], PCA-FELM [10], MSA-GCNN [12], and GAHC [14] show higher Packet drop ratios of around 5.5%, 5.1%, 4.8%, and 4.1% respectively, at the simulation rounds of 300. Energy consumption shows the robustness of the proposed routing system. If it is low, then the system has better routing and vice versa. Here, the average energy consumption of the network is analyzed with the number of simulation rounds and depicted in Figure 7. The proposed work is compared with the existing works, such as SER [9], PCA-FELM [10], MSA-GCNN [12], and GAHC [14]. The energy consumed by the proposed work is lower, with 3 J at the 300th simulation. Meanwhile, other works showed higher consumption of around 4J, 4.2J, 4J, and 4.5J, respectively, for the methods SER [9], PCA-FELM [10], MSA-GCNN [12], and GAHC [14].

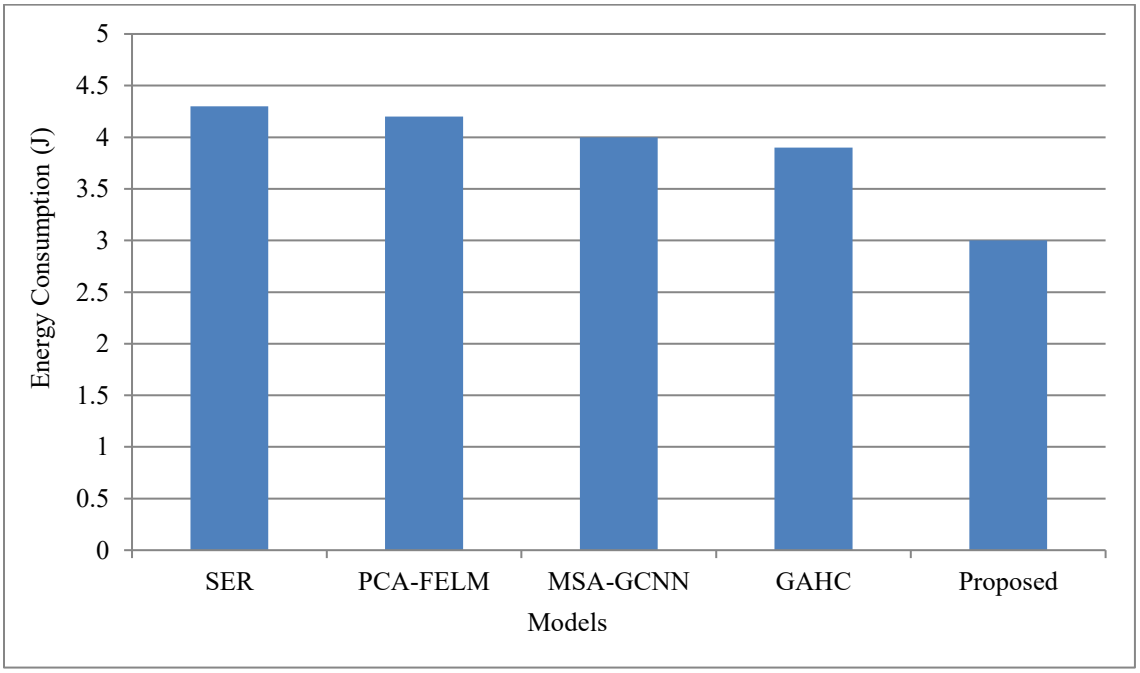

Fig. 7 Performance evaluation based on energy consumption

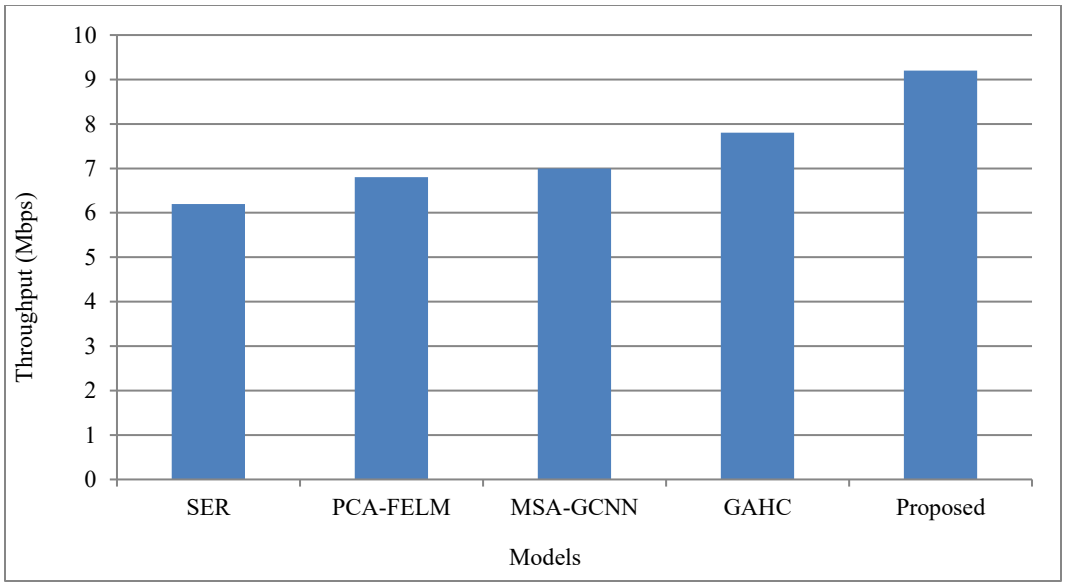

Fig. 8 Performance evaluation based on throughput

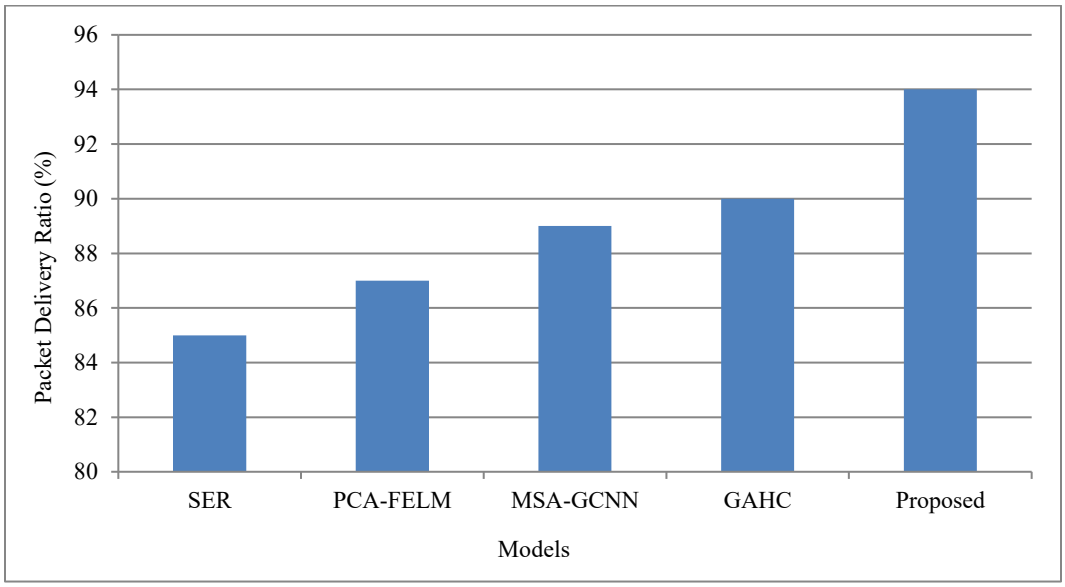

Fig. 9 Performance evaluation based on Packet delivery ratio

Throughput refers to the estimation of how packets are traveling from the source to the destination. For the proposed work and existing works SER [9], PCA-FELM [10], MSA-GCNN [12], and GAHC [14], it is analyzed and visualized in Figure 8. The throughput of the proposed work is higher, at 9 Mbps, for a node count of 100, as shown in the figure. At the 100th node, the throughput of other works SER [9], PCA-FELM [10], MSA-GCNN [12], and GAHC [14] showed 5.8 Mbps, 6.4 Mbps, 6 Mbps, and 7Mbps, respectively. The packet delivery ratio is the opposite of the packet drop ratio. The former determines the packets that arrive at the destination safely without being dropped, and the latter determines the dropped packet ratio. The packet delivery ratio of the proposed work and the other works SER [9], PCA-FELM [10], MSA-GCNN [12], and GAHC [14] is shown in Figure 9. As discussed earlier, the packet delivery ratio is higher when the routing system is utilized correctly, at 9%, with 100 nodes, as shown in the figure. The other tactics SER [9], PCA-FELM [10], MSA-GCNN [12], and GAHC [14] showed packet delivery ratios for the number of nodes equal to 100 are 6.7%, 7%, 7.8%, and 8.2% respectively.

4.3. Intrusion Detection Analysis

Intrusion detection is another key point to analyze the performance of the proposed work. For this purpose, state-of-the-art works such as SER [9], PCA-FELM [10], MSA-GCNN [12], and GAHC [14] are examined and analyzed for parameters including detection accuracy and precision. The

detection accuracy of the proposed and other techniques is shown in Figure 10. For that, accuracy is analysed based on the number of simulations and the simulation rounds of 250 on MANET. The detection accuracy of the proposed work at the 250th round is 96%, and other works have shown lower accuracy than the proposed work.

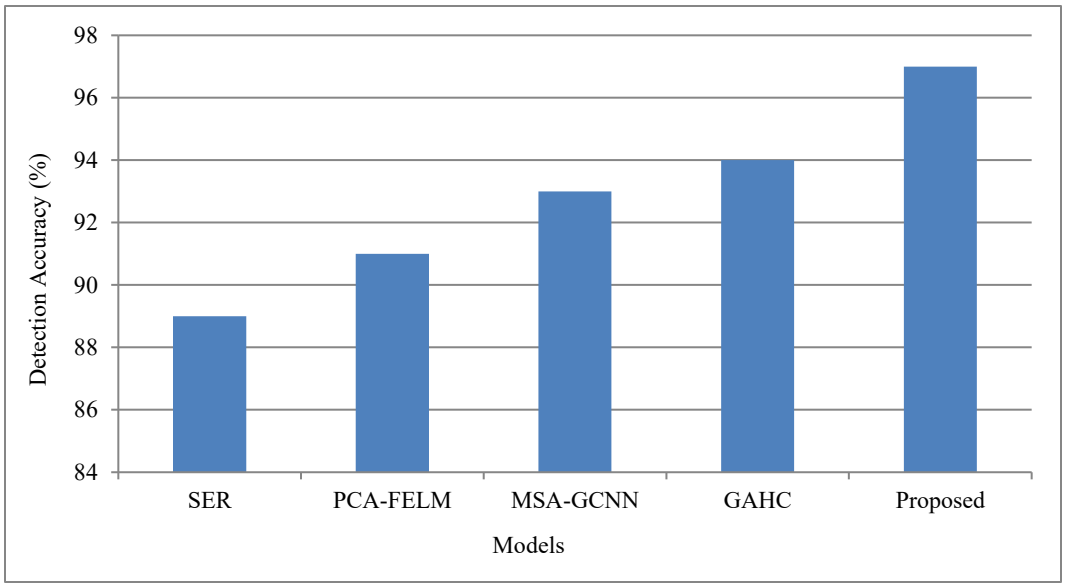

Fig. 10 Performance evaluation based on intrusion

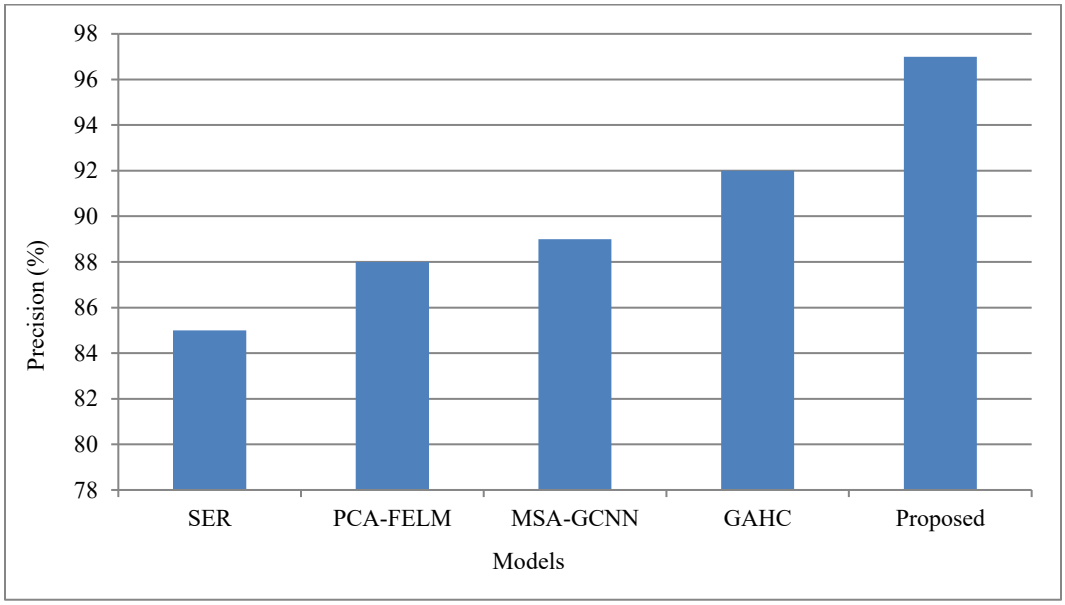

Fig. 11 Performance evaluation based on intrusion detection precision

Based on the precision, the intrusion detection is analysed for the proposed and other state-of-the-art works, such as SER [9], PCA-FELM [10], MSA-GCNN [12], and GAHC [14], and plotted in Figure 11. The precision of the proposed work is higher at 97%, whereas other tactics, including SER [9], PCA-FELM [10], MSA-GCNN [12], and GAHC [14], showed precisions of 85%, 88%, 89%, and 92%, respectively, as shown in the figure. This is because the intrusion detection of the proposed work is higher with the balanced usage of deep learning and optimization algorithms.

5. Conclusion

This work proposes a novel dynamic lyrebird optimization approach using a hybrid convolutional neural network and long short-term memory for the detection of Intrusions in MANET. The spectral clustering and DLO perform cluster formation and CH selection. The Intrusion and non-intrusion data were predicted using SO with CNN-LSTM. The detection accuracy of the proposed work at the 250th round is 96%, and other works have shown lower accuracy than the proposed work.

The simulation is executed simultaneously and analyzes the motion of packets generated by the nodes. The energy consumed by the proposed work is lower, with 3 J at the 300th simulation. The delay of the proposed work is lower, at 17ms or less, for a total of 120 nodes, while others are delayed by more than 22 seconds. The packet drop ratio is lower for the proposed work3 at the simulation rounds of 300. The throughput of the proposed work is higher, at 9 Mbps, for a number of nodes equal to 100. The proposed work aims to improve intrusion detection results, achieving superior performance compared to existing state-of-the-art models, such as SER, PCA-FELM, MSA-GCNN, and GAHC. Future work will explore lightweight federated intrusion detection and blockchain-based trust management to further enhance node authenticity and data integrity in large-scale MANET deployments.

References

[1] Zhao Niu et al., "Identification of Critical Nodes for Enhanced Network Defense in Manet-IoT Networks," *IEEE Access*, vol. 8, pp. 183571-183582, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Cheng-Xiang Wang et al., "Artificial Intelligence Enabled Wireless Networking for 5G and Beyond: Recent Advances and Future Challenges," *IEEE Wireless Communications*, vol. 27, no. 1, pp. 16-23, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Bin Liao et al., "Security Analysis of IoT Devices by using Mobile Computing: A Systematic Literature Review," *IEEE Access*, vol. 8, pp. 120331-120350, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Amin Shahraki et al., "A Survey and Future Directions on Clustering: from WSNs to IoT and Modern Networking Paradigms," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 2242-2274, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Daniele Bringhenti et al., "Automated Firewall Configuration in Virtual Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 1559-1576, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Inadyuti Dutt, Samarjeet Borah, and Indra Kanta Maitra, "Immune System Based Intrusion Detection System (IS-IDS): A Proposed Model," *IEEE Access*, vol. 8, pp. 34929-34941, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Ziadoon Kamil Maseer et al., "Benchmarking of Machine Learning for Anomaly based Intrusion Detection Systems in the CICIDS2017 Dataset," *IEEE access*, vol. 9, pp. 22351-22370, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Abebe Diro et al., "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," *IEEE Access*, vol. 8, pp. 60539-60551, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] P. Rajendra Prasad, and Shiva shankar, "Secure Intrusion Detection System Routing Protocol for Mobile Ad-Hoc Network," *Global Transitions Proceedings*, vol. 3, no. 2, pp. 399-411, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] C. Edwin Singh, and S. Maria Celestin Vigila, "Fuzzy based Intrusion Detection System in Manet," *Measurement: Sensors*, vol. 26, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Mahendra Prasad, Sachin Tripathi, and Keshav Dahal, "An Enhanced Detection System Against Routing Attacks in Mobile Ad-Hoc Network," *Wireless Networks*, vol. 28, no. 4, pp. 1411-1428, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] R. Reka et al., "Multi Head Self-Attention Gated Graph Convolutional Network based Multi-Attack Intrusion Detection in MANET," *Computers & Security*, vol. 136, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Saleh A. Alghamdi, "Novel Trust-Aware Intrusion Detection and Prevention System for 5G MANET-Cloud," *International Journal of Information Security*, vol. 21, no. 3, pp. 469-488, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Uppalapati Srilakshmi et al., "An Improved Hybrid Secure Multipath Routing Protocol for MANET," *IEEE Access*, vol. 9, pp. 163043-163053, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] M. Ganesh Karthik et al., "An Intrusion Detection Model Based on Hybridization of S-ROA in Deep Learning Model for MANET," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 48, no. 2, pp. 719-730, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Rahma Meddeb et al., "A Deep Learning-Based Intrusion Detection Approach for Mobile Ad-Hoc Network," *Soft Computing*, vol. 27, no. 14, pp. 9425-9439, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Jiang Xie et al., "An Efficient Spectral Clustering Algorithm based on Granular-Ball," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 9, pp. 9743-9753, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Mohammad Dehghani et al., "Lyrebird Optimization Algorithm: A New Bio-Inspired Metaheuristic Algorithm for Solving Optimization Problems," *Biomimetics*, vol. 8, no. 6, pp. 1-62, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Mandli Rami Reddy et al., "Energy-Efficient Cluster Head Selection in Wireless Sensor Networks using an Improved Grey Wolf Optimization Algorithm," *Computers*, vol. 12, no. 2, pp. 1-17, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Shahnawaz Ahmad, Shabana Mehfuz, and Javed Beg, "An Efficient and Secure Key Management with the Extended Convolutional Neural Network for Intrusion Detection in Cloud Storage," *Concurrency and Computation: Practice and Experience*, vol. 35, no. 23, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Vanlalruata Hnamte et al., "A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE," *IEEE Access*, vol. 11, pp. 37131-37148, 2023. [CrossRef] [Google Scholar] [Publisher Link]