SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I7P116

Volume 12 Issue 7, 208-219, July 2025

Original Article

Improved Network Security in MANET using Dingo Optimizer with Attention Convolutional Neural Network-based Intrusion Detection and Classification Model

M.N.S. Gangadhar[1], T. Suresh[2*], D. Sujatha[3]

[1,2]*Department of CSE, Annamalai University, Chidambaram, Tamil Nadu, India.*
[3]*Department of CSE, Malla Reddy College of Engineering & Technology, Hyderabad, Telangana, India.*

**Corresponding Author : sureshaucse@gmail.com*

Received: 09 May 2025 Revised: 10 June 2025 Accepted: 11 July 2025 Published: 31 July 2025

Abstract *- The fast popularization and growth of Mobile Ad-Hoc Networks (MANET) raise numerous security concerns. An Intrusion Detection System (IDS) is an effective defense tool to identify malicious data in intricate network landscapes and ensure computer system security. Conversely, conventional IDS, based on classical ML models, lacks accuracy and reliability. Rather than using classical Machine Learning (ML) as in preceding research, Deep Learning (DL) can perform better in extracting features from large datasets and massive cyber traffic in the current context. In general, MANET has inferior physical security for mobile devices due to effects like a deficiency of centralized management, node mobility, and restricted bandwidth. To challenge these safety concerns, classical cryptography systems do not protect MANETs from new attacks and vulnerabilities, so employing DL models in IDS efficiently alters the potent environments of MANETs. It permits the method to decide on intrusion while continuing to study their mobile landscape. This study proposes an Improved Network Security using the Dingo Optimizer Algorithm-based Intrusion Detection and Classification (INSDOA-IDC) model in MANET. The main aim of the INSDOA-IDC technique is the effective detection and classification of intrusions in MANET. Initially, the INSDOA-IDC technique applies the Z-score normalization method for pre-processing the input data. Attention with a convolutional Neural Network-Bidirectional Long Short-Term Memory (A-CNN-BiLSTM) method is used for intrusion recognition and classification. Finally, the Dingo Optimizer Algorithm (DOA) is implemented to ensure the optimum selection of the hyperparameters connected to the A-CNN-BiLSTM model. Extensive simulations of the INSDOA-IDC method are accomplished under the NSLKDD and UNSW-NB15 datasets. The comparison study of the INSDOA-IDC model portrayed superior accuracy values of 99.53% and 99.55% under dual datasets over existing models.*

Keywords *- MANET, Intrusion Detection System, Dingo optimizer, Long Short-Term Memory, Convolutional Neural Network.*

1. Introduction

MANET is a brand-new wireless communication design that operates in a very challenging and unpredictable environment [1]. Owing to their fast deployment and the increasing fame of mobile appliances, this network has recently become critical and common to wireless communications. MANETs have some benefits across a network without a stable design, such as the capacity to construct an ad hoc network somewhere by mobile appliances, the capability to supplement extra nodes toward the system, and management costs that may be inexpensive [2]. MANET is usually applied in science, the military, and rescue operations. The inherent susceptibility of MANET presents a new security problem that mainly deals with network and data linking at the protocol stack level [3]. Malicious routing assaults might focus on the maintenance process or routing detection by dying following the routing protocol specifications [4]. Compared with fixed networks, MANET securities are considered from different ideas: privacy, encryption, availability, authentication, reliability, usage control, and access control [5]. Novel threats like attacks from Byzantine, internally mischievous nodes, and wormhole attacks are complex to secure. An IDS is efficient for identifying attacks after an attack arises in a MANET [6].

The IDS observes the system activity and analyzes the activity to decide which activity is breaking the rules of security [7]. When an IDS establishes a rare activity or an activity identified as an attack, it later makes an alarm to warn the security administrator [8]. Additionally, IDS initiates

accurate responses for malicious activities. IDSs help in the determination, detection, and classification of data deletion, copying, and content modification, all breaking samples of illegal behaviour of a system [9]. This is vital for wireless ad-hoc networks to defend against malevolent behaviour in securing the MANET routing and handling within the limits of cryptographic structures. IDSs that are effectively utilized for detecting attacks in MANET can present a proper defence to detect misbehaving nodes and malicious traffic in wireless environments [10]. The dynamic and infrastructure-less characteristic of MANETs facilitates security threats. Conventional methods face difficulty in detecting growing attacks, motivating the need for intelligent, adaptive intrusion detection using DL and optimization techniques for improved protection.

This study proposes an Improved Network Security using the Dingo Optimizer Algorithm-based Intrusion Detection and Classification (INSDOA-IDC) model in MANET. The main aim of the INSDOA-IDC technique is the effective detection and classification of intrusions in MANET. Initially, the INSDOA-IDC technique applies the Z-score normalization method for pre-processing the input data.

Attention with a Convolutional Neural Network-Bidirectional Long Short-Term Memory (A-CNN-BiLSTM) method is used for intrusion recognition and classification. Finally, the Dingo Optimizer Algorithm (DOA) is implemented to ensure the optimum selection of the hyperparameters connected to the A-CNN-BiLSTM model. Extensive simulations of the INSDOA-IDC method are accomplished under the NSLKDD and UNSW-NB15 datasets. The key contribution of the INSDOA-IDC method is listed below.

- The INSDOA-IDC model applies Z-score normalization for standardizing inputs, improving training efficiency while contributing to more stable and accurate intrusion detection outcomes.
- The integration of Attention with CNN-BiLSTM enables advanced feature extraction and temporal sequence learning, enhancing detection precision and improving the overall classification performance of the INSDOA-IDC method.
- The INSDOA-IDC technique implements the DOA approach to effectively fine-tune the model parameters, improving detection accuracy and minimizing false positives for more reliable intrusion classification.
- The novelty of the INSDOA-IDC methodology is in its synergistic integration of Attention-based CNN-BiLSTM with DOA, enabling dynamic tuning of DL parameters. This hybrid model delivers robust intrusion detection by effectively capturing spatial-temporal features. Its adaptability ensures improved security in decentralized and rapidly changing MANET environments.

2. Related Works

The authors in [11] presented WOA-DNN to classify and detect intrusion. They utilized it to enhance the pre-processed data to create a network for predicting and identifying unexpected cyberattacks, which are either efficient or effective. Reka et al. [12] concentrated on the difficulties of node energy and mobility to advance a clustering method for selecting a cluster head, which two system criticalities encourage. The COA performs dense cluster creation. The MSA-GCNN with a hybrid IDS form identifies numerous attacks, including Zero-Day and DoS attacks. This model is applied in the NS-2 simulator. The presented performance method is studied with a few parameters to identify the intruder. Sathiya and Yuvaraj [13] proposed a BSOD-MMPEL node behaviour-based IDS for detecting intrusion. BSOD Evolution-based FS safeguards significant and robust balances among exploitation and exploration with a higher chance of union to local sub-optima Gudermannian Activation. Later, with the chosen features, an initial intrusion detection utilizing MMPEL Node behavior-based IDS is created. Rajan et al. [14] proposed a Two-Pronged IDS (TP-IDS) intended for MANET, concentrating on hello flooding, UDP flooding, and blackhole attacks. These attacks utilize the self-organising and dynamic MANETs features, causing the network to perform poorly. The author used SMOTE to overcome the class imbalance. Hyperparameter Optimization is executed by utilizing Optuna across Decision Tree (DT) and Bayesian Optimization, XGBoost, Random Forest (RF), and Naïve Bayes (NB) classifiers, displaying weaknesses and strengths for optimum selection. Sheela et al. [15] introduced a smart IDS framework for significantly improving the MANET security using the DL method. Currently, the min-max normalization technique is utilized to pre-process the provided cyberattack datasets. Next, AOMA is executed to select the optimum features for enhancing the speed and intrusion recognition. In addition, the DSLC method is also used to categorize and predict the intrusion based on appropriate training and learning processes.

Sasikumar and Rohini [16] focused on evaluating and developing an effective IDS presented for MANETs named Robust Dragonfly-Optimized enhanced NB (RDO-ENB). It functions by combining the efficiency and simplicity of the ENB approach with the adaptable abilities of RDO. It improves precision and decreases false positives, making it capable of mitigating and identifying intrusions in the ever-evolving and complex MANETs atmosphere. Sugumaran and Rajaram [17] concentrated on attaining higher-level security by integrating BC-based IDS. Therefore, the security level achieved by the previous research cannot deal with the growing attacks. To solve this problem, this research proposes LB-IDS that mutually detects and prevents the attacks endured by mobile networks. At first, the network nodes are verified by an LB-based LBMFA model. This process prevents the entry of malicious nodes into the system. Later, the data packets are communicated using the optimum route chosen by

the MOSO method. Saminathan et al. [18] developed a model by integrating Simple Contrastive Graph Clustering (SCGC), Deep Operator Neural Network (DONN), and Artificial Rabbits' Optimization (ARO) technique for energy-aware and secure data transmission, namely Multipath Routing With Contrastive Partitioning And Deep Neural Intrusion Detection for MANET using the DONN (MRCP-DNID-MANET-DONN) method. Sardar et al. [19] suggested a Graph Neural Network-based IDS (GNN-IDS) for MANETs to improve detection accuracy and network resilience by analyzing node behavior.

Hussain and Fathima [20] proposed a hybrid IDS for MANET, named HIDE-MAN, which utilizes a coati-optimised BiLSTM (CO-BiLSTM) model along with Federated Learning (FL) and Generative Adversarial Networks (GANs) models to effectively detect Distributed Denial Of Service (DDoS) and various attacks. Abdalhameed and Kadhim [21] aimed to improve security and data transmission efficiency in MANET by integrating Particle Swarm Optimization (PSO), Recurrent Neural Networks (RNN), and an improved randomization algorithm. AL-inizi et al. [22] introduced a model utilizing Artificial Intelligence (AI), specifically CNN, to improve the IDS in MANET by improving detection accuracy, reaction time, and packet delivery rates to better protect against DDoS attacks.

Krishna et al. [23] presented a Blockchain (BC)-based IDS that integrates Mantis Search Algorithm (MSA) for extraction, a lightweight BC consensus for secure trust management, and a Gated Recurrent Unit (GRU) classifier optimized by Giant Armadillo Optimization (GAO) to improve intrusion detection accuracy and network performance. Basani, Grandhi, and Abbas [24] proposed a model using Edward Prime Curve Cryptography (EPCC) and the Grey Wolf Optimization (GWO) model to enhance secure, efficient, and reliable data transmission in Internet of Things (IoT)-enabled MANETs. Li et al. [25] proposed a multi-scale CNN-bidirectional GRU-Single-Headed Attention (MSCNN-BiGRU-SHA), optimized by the Multi-Strategy Integrated Zebra Optimizer Approach (MI-ZOA) model.

Despite several advancements, many existing IDS models for MANET encounter challenges such as handling class imbalance, optimizing hyperparameters efficiently, and maintaining high detection accuracy under dynamic network conditions. Diverse approaches depend heavily on simulation environments, restricting real-world applicability.

Moreover, the integration of optimization algorithms often increases computational complexity, affecting scalability in resource-constrained MANETs. The research gap is in developing lightweight, adaptive IDS frameworks that balance detection performance, computational efficiency, and robustness while addressing diverse attack types in practical MANET scenarios.

3. Proposed Methodology

This study proposes the INSDOA-IDC technique in MANET. The technique aims to detect and classify intrusions effectively in MANET. It involves data pre-processing, A-CNN-BiLSTM using a detection process, and a DOA-based hyperparameter tuning method to accomplish that. Figure 1 depicts the overall process of the INSDOA-IDC model.

3.1. Data Pre-Processing

Initially, the INSDOA-IDC method uses the Z-score normalization method to change input data into a well-suited layout for pre-processing the input data. This is a vital pre-processing stage in IDS for MANETs [26]. It regulates the dataset by changing raw data values to a usual scale, where the standard deviation is one and the mean is zero.

This method aids in justifying the properties of outliers and changing data scales, which are general in MANET environments owing to dynamic network situations. By regularizing the data, the IDS effectively recognizes variations suggestive of potential intrusions. So, this enhances the consistency and accuracy of intrusion detection in MANETs.

3.2. Detection Process of the CNN-BiLSTM Method

Next, the proposed INSDOA-IDC technique applies the A-CNN-BiLSTM method for intrusion detection and classification. CNN is a kind of FFNN that mainly includes multilayer NN, and its neurons could respond to the incomplete covering of neighbouring elements, which has apparent benefits in local extraction [27]. The pooling and Convolutional Layers (CLs) constitute the most significant portion of CNN. The crucial building block of the CNN and CL exploits the convolution filter for extracting the spatial signal features from the input dataset for learning the features and convolving with the learning kernels.

$$X(i,j) = \sum_{m}\sum_{n} x\,(m+i, n+i)\omega(m,n) + b \qquad (1)$$

In Equation (1), $X(i,j)$ is the convolutional output, x refers to the input matrix, ω denotes the size $m \times n$ weight matrix, and b signifies bias.

The spatial feature extraction module consists of two 1-D CLs (Conv2 and Conv3) and three 2-D CLs (Convl, Conv4, and Conv5), which extract features for Bi-LSTM by abstracting input data and reducing noise at a high level. The I/Q multiplex signals are pre-processed and divided into I-channel and Q-channel data streams.

Later, they are processed individually by the Convl, Conv2, and Conv3 to capture single- and multi-channel features of I/Q signals. Conv2 and Conv3 use zero padding to maintain data integrity during modelling. Then, the output is integrated into a concatenation of two before being served to Conv5 for extracting spatial features.

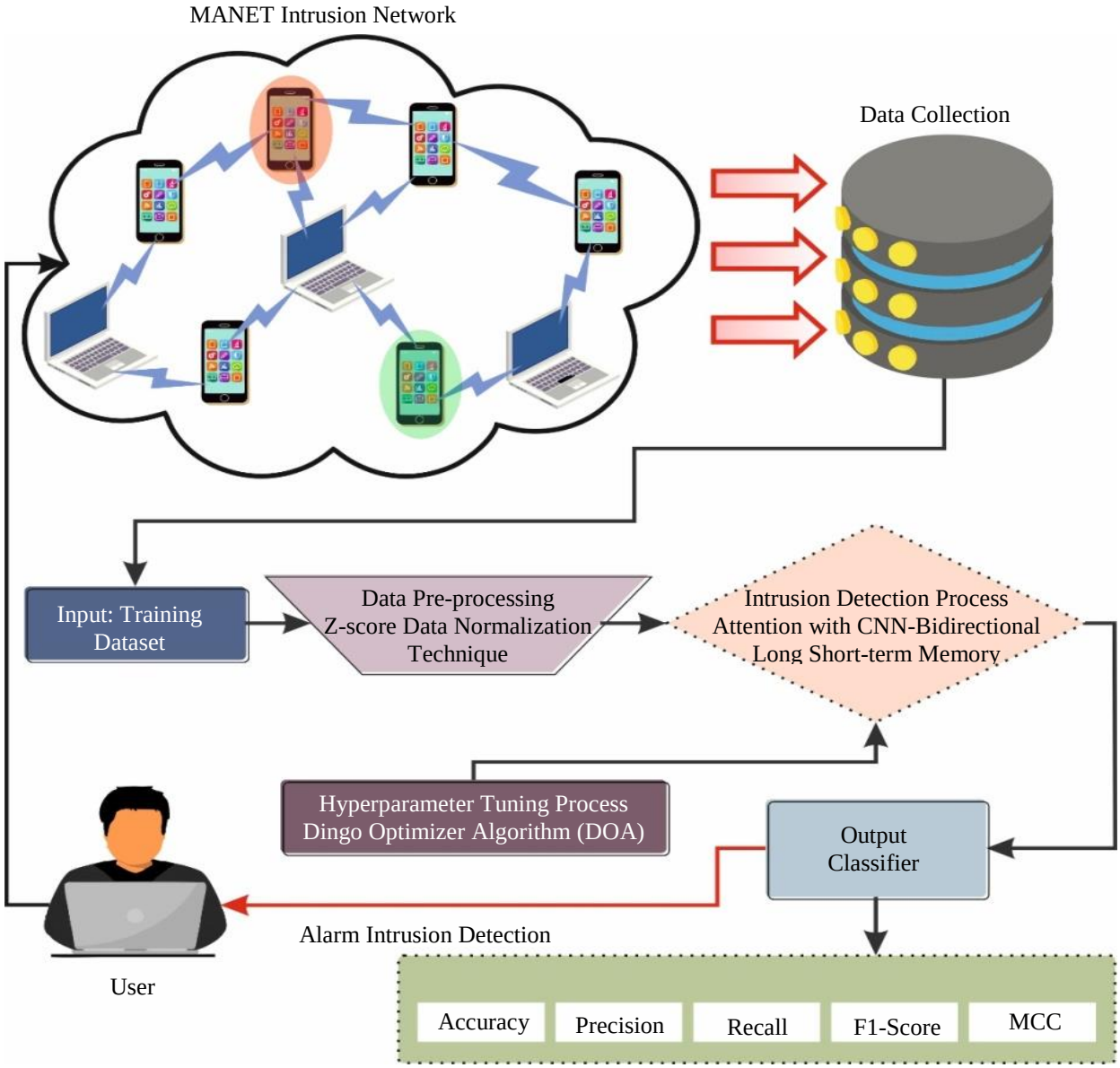

Fig. 1 Workflow of the INSDOA-IDC model

This multi-channel input framework efficiently takes representative features at dissimilar measures and increases the data usage from Q-channel, I-channel, and I/Q multi-channel datasets.

RNN has a particular dissimilarity called LSTMs, which contain output gates, input gates, forgetting gates, and memory units. These units cooperate to discard, store, and retrieve data in the system. The input and output gates control data storage in the memory and its flow to external resources, respectively. The forget gate regulates whether a particular data should be discarded or retained. The LSTM computational method is represented below:

$$F_t = \sigma\left(W_f \cdot [H_{t-1'} X_t] + b_f\right) \quad (2)$$

$$I_t = \sigma(W_i \cdot [H_{t-1'} X_t] + b_i) \quad (3)$$

$$\tilde{C}_t = \tanh(W_c \cdot [H_{t-1}, X_t] + b_c) \quad (4)$$

$$C_t = F_t \cdot C_t - 1 + I_t \cdot \tilde{C}_t \quad (5)$$

$$O_t = \sigma(W_o \cdot [H_{t-1'} X_t] + b_0) \quad (6)$$

$$H_t = O_t \cdot \tanh(C_t) \quad (7)$$

In these calculations, the input, output, and forget gates of particular outputs are represented by the characters F_t, I_t, and

O_t. $\tilde{C}_t$ and C_t Denote the state of a cell at the existing time step and the following time step, respectively. H_t Means the value of the final output. σ represents the sigmoid. W_f, W_i, W_c, and W_o are the gates of forget, input and output weight matrices and the existing state of the cell. b_f, b_j, b_c, and b_o Represent the gate bias terms.$[H_{t-1}, X_t]$ implies an output values vector composed from preceding and existing time steps.

The BiLSTM structure consists of two separate LSTMs. The input sequence is extracted by dual LSTMs, backwards and forward, correspondingly, and the extraction feature vectors emerge as concluding output features. The computation method is represented below:

$$\vec{C}_t = LSTM\left(X_t, \vec{H}_t, \vec{C}_{t-1}\right) \tag{8}$$

$$\overleftarrow{C}_t = LSTM\left(X_t, \overleftarrow{H}_{t-1}, \overleftarrow{C}_{t-1}\right) \tag{9}$$

$$C_t = W^T \vec{C}_t + W^V \overleftarrow{C}_t \tag{10}$$

$\vec{C}_t$ and $\overleftarrow{C}_t$ Signify the backwards and forward LSTM cell states at time-step t; W^V and W^T Indicate the backwards and forward LSTM weight coefficients.

However, a distinct CNN technique is proficient at capturing wireless signals' spatial workings and temporal nuances. Stimulated by the proposed structure, the combined sequences of the BiLSTM method after the CNN explore the bidirectional features of time series besides the sequential axis. This advanced strategy contains dual BiLSTM layers with 128 units, allowing effective handling of series data and time correlation extraction.

The time Attention Mechanism (AM) in DL is a technique for processing successive input. It enables the method to allocate attention or importance to the data by multiple time steps while handling sequence data. This method can efficiently recognize the significance and dependencies of different sequence parts and alter its attention as required. At first, this layer generates dual weight sets and is utilized for computing attention scores. The attention score is calculated in Equation (11):

$$e_{ij} = \tanh(Wx + b) \tag{11}$$

Whereas x signifies input. Weighted input index, Softmax and normalized the attention score to attain the weight. To highlight the input sequence components, these attention weights are used on an input. In conclusion, the sequence axis adds the weighted inputs to create the final output. Figure 2 depicts the architecture of the A-CNN-BiLSTM technique.

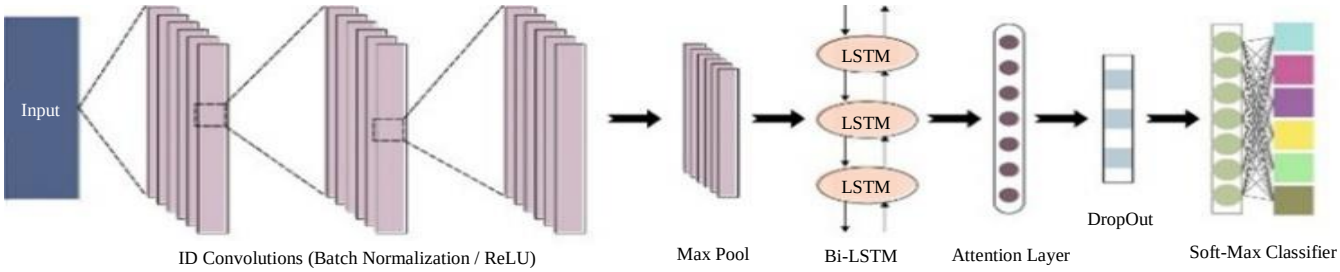

Fig. 2 Structure of the A-CNN-Bi-LSTM method

Using the method mentioned above, the sequential AM can dynamically change the weights based on the importance of different input sequence segments. This enables the technique to focus on the most relevant data at each phase, thus improving its handling efficacy and emphasizing the sequence data's outstanding features.

3.3. Hyperparameter Tuning using DOA

Furthermore, DOA is applied to ensure the optimum selection of hyperparameter tuning. The DOA contains four processes that create this process: encircling, searching, attacking, and hunting prey [28]. The below-mentioned method defines how this technique functions:

3.3.1. Encircling

Dingos have the intellect to discover their victims. If they follow their victim's location, the alpha and pack encircle the victim. Others are searching to study their plans in anticipation of this future method. Equation (12)-(16) demonstrate this behaviour stimulated by dingos.

$$\overrightarrow{Z_d} = \left|\vec{U} \cdot \vec{P}_p(x) - \vec{J}(i)\right| \tag{12}$$

$$\vec{J}(i+1) = \vec{J}_p(i) - \vec{U} \cdot \vec{Z}(d) \tag{13}$$

$$\vec{U} = 2. \tag{14}$$

$$\vec{V} = 2\vec{n} * \vec{m}_2 \tag{15}$$

$$\vec{n} = 3 \cdot \left(TS * \left(\frac{3}{I_{mx}}\right)\right) \tag{16}$$

The dingoes can arrive at any position among the facts established comprehensively by the randomly generated

numbers $m1$ and $m2$. They can travel near the victim at any position within the search region by Equations (12) and (13). Similar calculations are functional to attain a search space with sizes of N, where the Dingo will arrive in hyper-cubes near the finest result.

3.3.2. Hunting

In contrast, the method recommends that agents generally not add the best location of the victim in the search space. Let us consider that the beta, alpha, and other members were familiar with latent victim locations when the dingoes' hunting approach progressed. The mathematical formulations are mentioned below:

$$\vec{Z}_{\alpha} = \left|\vec{U}_1.\vec{J}_{\alpha} - \vec{J}\right| \quad (17)$$

$$\vec{Z}_{\beta} = \left|\vec{U}_2.\vec{J}_{\beta} - \vec{J}\right| \quad (18)$$

$$\vec{Z}_{o} = \left|\vec{U}_3.\vec{J} - \vec{J}\right| \quad (19)$$

$$\vec{J}_1 = \left|\vec{J}_{\alpha} - \vec{V}.\vec{Z}_{\alpha}\right| \quad (20)$$

$$\vec{J}_2 = \left|\vec{J}_{\beta} - \vec{V}.\vec{Z}_{\beta}\right| \quad (21)$$

$$\vec{J}_3 = \left|\vec{J}_{o} - \vec{V}.\vec{Z}_{o}\right| \quad (22)$$

The strength of every Dingo is formulated by:

$$\vec{G}_{\alpha} = \log\left(\frac{1}{Pit_{\alpha} - (1W - 100)} + 1\right) \quad (23)$$

$$\vec{G}_{\beta} = \log\left(\frac{1}{Fit_{\beta} - (1W - 100)} + 1\right) \quad (24)$$

$$\vec{G}_{o} = \log\left(\frac{1}{Fit_{0} - (1W - 100)} + 1\right) \quad (25)$$

"Fit" means the value of fitness, and "Fit_o" means the fitness value of another dingo.

3.3.3. Attacking Prey

The technique gradually reduces the n value. At a certain level, the encircling strategy shows exploration; however, DIOP wants additional operators to highlight the search. The DIOP helps its search agents alter their position depending on the location β and the targeted victim. With the help of operators, the DIOP can disable the local solution.

3.3.4. Searching

It is highly recommended for examining and evading adjacent goals. Based on a dingo's position, it will randomly decide on the victim's value and make it essential to encounter the Dingo severely. Purposely, $\vec{U}$ It is used to deliver stochastic exploration values. This model is effective in defending the outcome from local goals.

The DOA procedure is described in Algorithm 1.

Algorithm 1: Pseudocode of DOA

Input: Dingoes population
Output: Optimum Dingo
Early search agent Z_{in}
Set the value of $\vec{n}$ and $\vec{V}$.
If termination was not met, do
Evaluate every Dingo's fitness and intensity cost.
Z_{α} =Optimum search with Dingo
$Z_{\beta} = 2nd$ optimum search of Dingo
Z_0 = Search for Dingos
repeat
for
$i = 1: Z_{in}$ do
Newest Search
end for
Assess the intensity, cost, and fitness of dingos.
$R_{\alpha}, R_{\beta \rightarrow} R_{\delta}$ record
$\vec{n}, \vec{U}$ and $\vec{V}$ record
repeat = 1 +repeat
Repeat≥ Stopping conditions
output
end while

The DOA method defines a Fitness Function (FF) based on classifier error rate reduction, where a higher positive value indicates enhanced candidate performance, as illustrated in Equation (26).

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{no.of\ misclassified\ samples}{Total\ no.of\ samples} \times 100 \quad (26)$$

4. Result Analysis

The INSDOA-IDC technique's simulation valuation is examined under the NSLKDD dataset [29]. The dataset has 148517 samples and five classes, as shown in Table 1.

Table 1. Dataset description

NSLKDD Dataset	
Classes	**Sample Numbers**
Normal	77054
DoS	53385
Probe	14410
R2L	3416
U2R	252
Overall Samples	**148517**

Figure 3 presents the classifier outputs of the INSDOA-IDC method on the NSLKDD dataset. Figures 3(a)-3(b) depicts the confusion matrices under 70:30 TRAP/TESP. Figure 3(c) and 3(d) depict the PR and ROC curves over diverse classes.

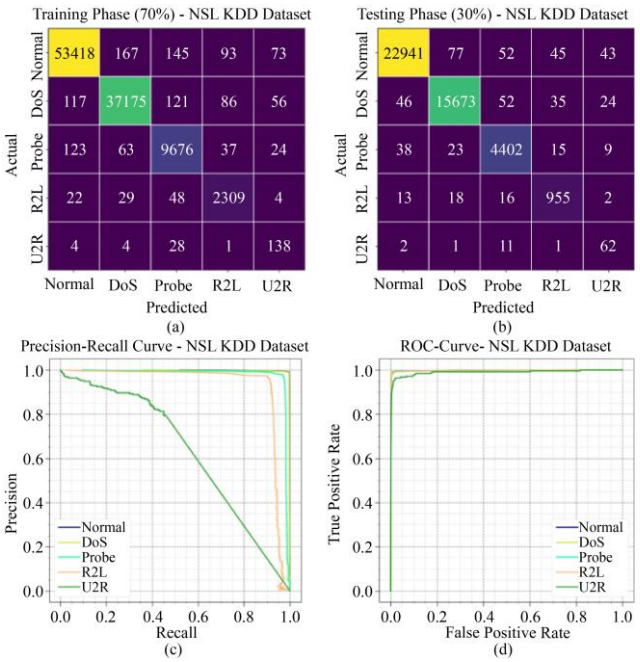

Fig. 3 NSLKDD dataset (a-b) confusion matrices, and (c-d) PR and ROC curves.

In Table 2 and Figure 4, the classifier result of the INSDOA-IDC approach is shown on the NSLKDD dataset. On 70%TRAP, the INSDOA-IDC model presents an average $accu_y$ of 99.52%, $prec_n$ of 86.72%, $reca_l$ of 94.04%, $F1_{score}$ of 89.55%, and MCC of 89.60%. Besides, on 30%TESP, the INSDOA-IDC model attains an average $accu_y$ of 99.53%, $prec_n$ of 86.2 2%, $reca_l$ of 94.36%, $F1_{score}$ of 89.23%, and MCC of 89.40%.

Table 2. Classifier outcome of the INSDOA-IDC method on the NSLKDD dataset

Classes	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{score}$	MCC
TRAP (70%)					
Normal	99.28	99.50	99.11	99.31	98.57
DoS	99.38	99.30	98.99	99.14	98.66
Probe	99.43	96.59	97.51	97.05	96.73
R2L	99.69	91.41	95.73	93.52	93.39
U2R	99.81	46.78	78.86	58.72	60.65
Average	**99.52**	**86.72**	**94.04**	**89.55**	**89.60**
TESP (30%)					
Normal	99.29	99.57	99.06	99.32	98.58
DoS	99.38	99.25	99.01	99.13	98.65
Probe	99.52	97.11	98.11	97.61	97.34
R2L	99.67	90.87	95.12	92.94	92.80
U2R	99.79	44.29	80.52	57.14	59.63
Average	**99.53**	**86.22**	**94.36**	**89.23**	**89.40**

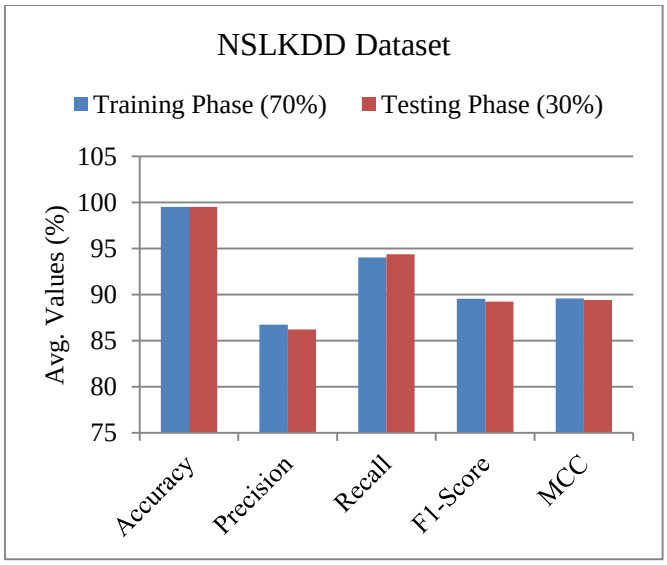

Fig. 4 Average of the INSDOA-IDC method under the NSLKDD dataset

In Figure 5, the TRAP/TESP accuracy results of the INSDOA-IDC technique on the NSLKDD dataset are indicated over 0-25 epochs. This figure shows that TRAP/TESP accuracy consistently improves with iterations, depicting the robust performance of the INSDOA-IDC approach. Their close alignment across epochs suggests minimal overfitting and reliable prediction on unseen samples.

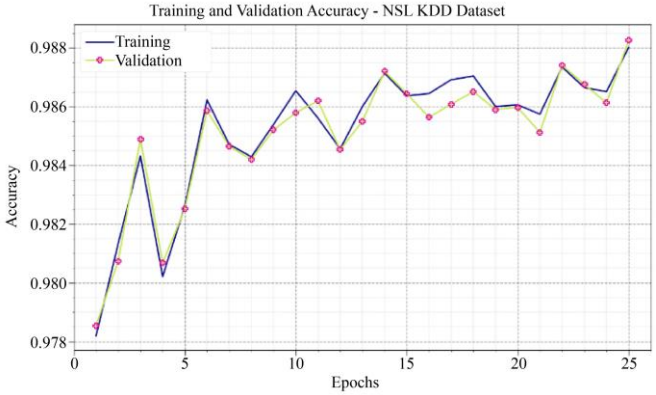

Fig. 5 $Accu_y$ curve of the INSDOA-IDC method under the NSLKDD dataset

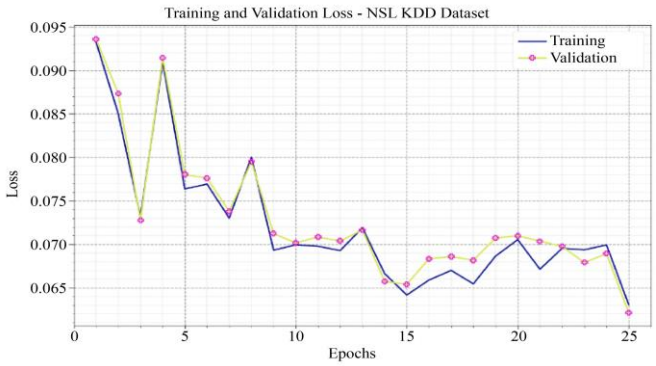

Fig. 6 Loss curve of the INSDOA-IDC technique under the NSLKDD dataset

Figure 6 illustrates the TRAP/TESP loss of the INSDOA-IDC method on the NSLKDD dataset over 0-25 epochs. The decreasing trend indicates the efficiency of the INSDOA-IDC technique in balancing generalization and data fitting. This consistent mitigation confirms improved performance and timely tuning of prediction outcomes.

Table 3 and Figure 7 depict the comparison outputs of the INSDOA-IDC method on the NSLKDD dataset with the existing methods [11, 31]. The outputs underlined that the NB, RF, DT, Bi-LSTM, and EM grouping techniques exhibited poor performance. Furthermore, WOA-DNN and HCSTS-DNN techniques attained closer outcomes. Additionally, the INSDOA-IDC approach illustrates superior performance with the highest $prec_n$, $reca_l$, $accu_y$, and $F1_{score}$ of 86.22%, 94.36%, 99.53%, and 89.23%, respectively.

Table 3. Comparative evaluation of the INSDOA-IDC method under the NSLKDD dataset [11, 31]

Classifiers	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{score}$
NB	96.41	79.84	92.04	87.64
RF	95.26	78.60	90.70	73.00
DT	96.57	76.24	93.29	74.99
Bi-LSTM	96.42	79.03	90.87	73.93
EM Clustering	96.69	77.36	92.31	78.64
WOA-DNN	98.41	73.17	92.29	85.48
HCSTS-DNN	99.37	81.49	93.50	87.08
INSDOA-IDC	99.53	86.22	94.36	89.23

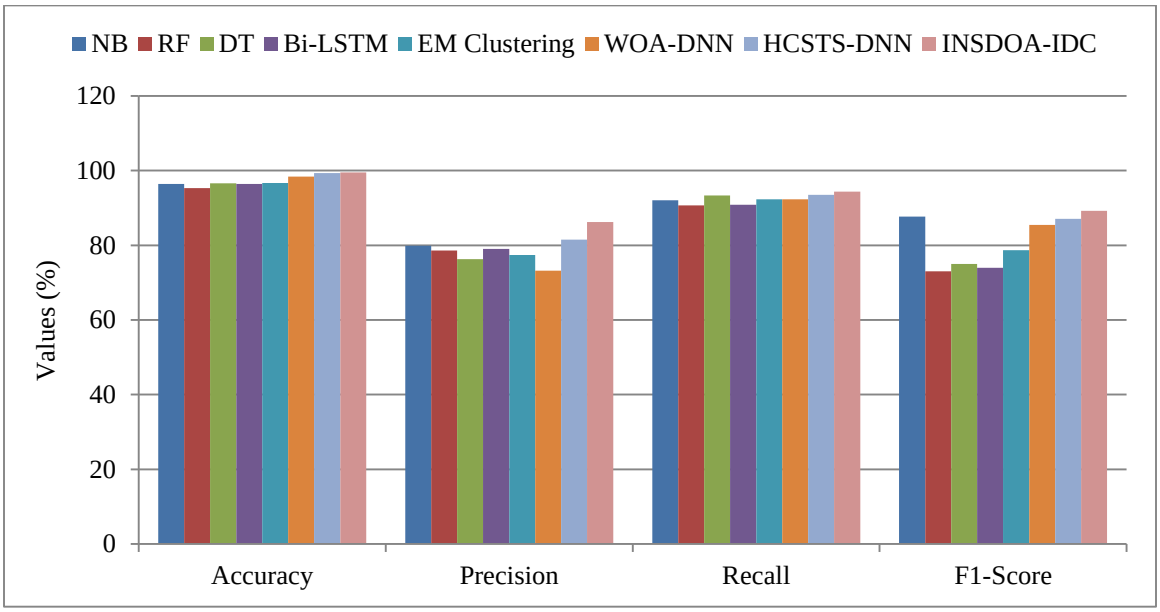

Fig. 7 Comparative evaluation of the INSDOA-IDC method under the NSLKDD dataset

The performance assessment of the INSDOA-IDC model is inspected under the UNSW-NB15 dataset [30]. Table 4 specifies the dataset.

Table 4. Dataset specification

UNSW-NB15 Dataset	
Classes	**Before Sampling**
Normal	2500
Generic	2500
Exploits	2500
Fuzzers	2500
Backdoors	1746
Shellcode	1133
Worms	130
Overall Samples	**13009**

Figure 8 depicts the classifier outputs of the INSDOA-IDC approach under the UNSW-NB15 dataset. Figures 8(a)-8(b) illustrates the confusion matrix of overall classes on 70:30 TRAP/TESP. Figure 8(c) and 8(d) depict the PR and ROC study, showing greater performance of the model over diverse classes.

In Table 5 and Figure 9, the classifier result of the INSDOA-IDC technique under the UNSW-NB15 dataset. The outputs stated that the INSDOA-IDC approach properly classified and detected the samples. On 70%TRAP, the INSDOA-IDC approach attained an average $accu_y$ of 99.48%, $prec_n$ of 92.84%, $reca_l$ of 97.90%, $F1_{score}$ of 94.66%, and MCC of 94.72%. Moreover, on 30%TESP, the INSDOA-IDC approach attained an average $accu_y$ of 99.55%, $prec_n$ of 93.62%, $reca_l$ of 98.17%, $F1_{score}$ of 95.38%, and MCC of 95.38%.

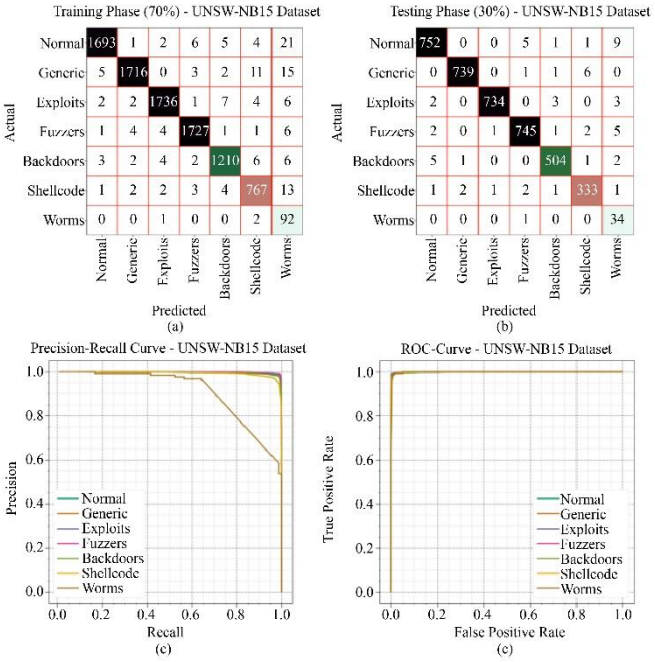

Fig. 8 UNSW-NB15 dataset (a-b) confusion matrices, and (c-d) PR and ROC curves.

Table 5. Classifier output of the INSDOA-IDC technique under the UNSW-NB15 dataset

Classes	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{score}$	MCC
TRAP (70%)					
Normal	99.44	99.30	97.75	98.52	98.18
Generic	99.48	99.36	97.95	98.65	98.33
Exploits	99.62	99.26	98.75	99.00	98.76
Fuzzers	99.65	99.14	99.03	99.08	98.86
Backdoors	99.54	98.45	98.13	98.29	98.03
Shellcode	99.42	96.48	96.84	96.66	96.34
Worms	99.23	57.86	96.84	72.44	74.55
Average	**99.48**	**92.84**	**97.90**	**94.66**	**94.72**
TESP (30%)					
Normal	99.33	98.69	97.92	98.30	97.89
Generic	99.69	99.60	98.80	99.19	99.01
Exploits	99.72	99.59	98.92	99.26	99.08
Fuzzers	99.49	98.81	98.54	98.68	98.36
Backdoors	99.59	98.63	98.25	98.44	98.20
Shellcode	99.54	97.08	97.65	97.37	97.12
Worms	99.46	62.96	97.14	76.40	77.98
Average	**99.55**	**93.62**	**98.17**	**95.38**	**95.38**

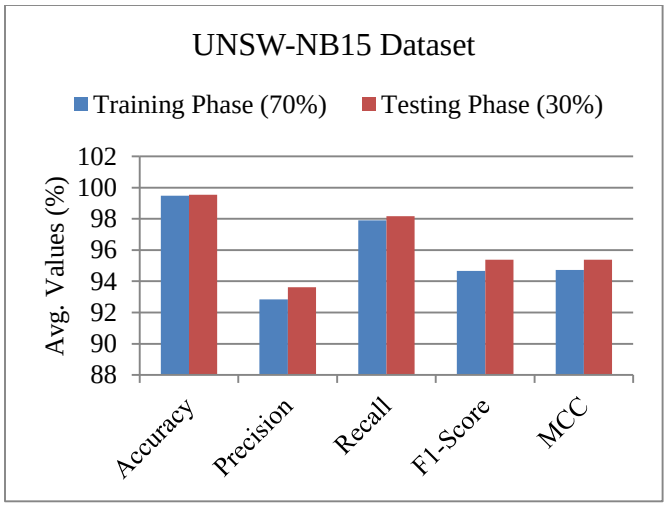

Fig. 9 Average of the INSDOA-IDC technique under the UNSW-NB15 dataset

Figure 10 depicts the TRAP/TESP accuracy of the INSDOA-IDC method over 0-25 epochs. The figure highlights a steady increase, demonstrating the robust performance of the INSDOA-IDC approach across iterations. The close alignment of both curves indicates minimal overfitting and reliable prediction on unseen data.

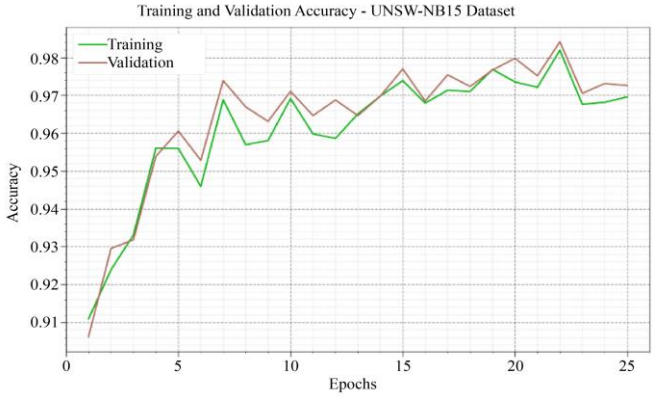

Fig. 10 $Accu_y$ curve of the INSDOA-IDC technique under the UNSW-NB15 dataset

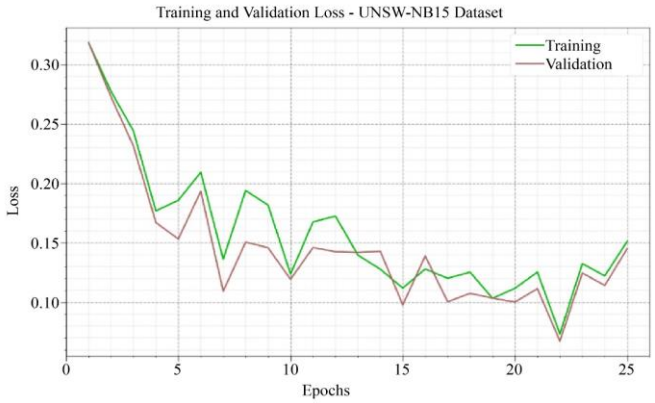

Fig. 11 Loss curve of the INSDOA-IDC technique under the UNSW-NB15 dataset

Figure 11 shows the TRAP/TESP loss of the INSDOA-IDC technique over 0-25 epochs. The figure demonstrated a decrease in the loss values, indicating the efficiency of the approach in balancing generalization and data fitting, while consistently improving prediction accuracy.

Table 6 and Figure 12 analyze the comparison outcomes of the INSDOA-IDC method under the UNSW-NB15 dataset with the existing techniques [15, 32]. The outputs illustrated that the NB, RF, DT, Bi-LSTM, and EM grouping models have described poorer performance. At the same time, WOA-DNN and HCSTS-DNN models have gained adjacent outcomes. Moreover, the INSDOA-IDC technique exhibited enhanced performance with maximal $prec_n$, $reca_l$, $accu_y$, and $F1_{score}$ of 93.62%, 98.17%, 99.55%, and 95.38%, respectively.

Table 6. Comparative assessment of the INSDOA-IDC approach under the UNSW-NB15 dataset [15, 32]

Classifiers	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{score}$
NB	98.56	82.99	94.85	90.81
RF	93.02	85.37	96.79	93.24
DT	94.82	82.18	92.24	93.91
Bi-LSTM	95.75	90.55	93.40	90.12
EM Clustering	93.86	87.27	95.31	94.92
WOA-DNN	96.08	82.46	96.61	86.13
HCSTS-DNN	98.72	92.51	94.60	94.62
INSDOA-IDC	99.55	93.62	98.17	95.38

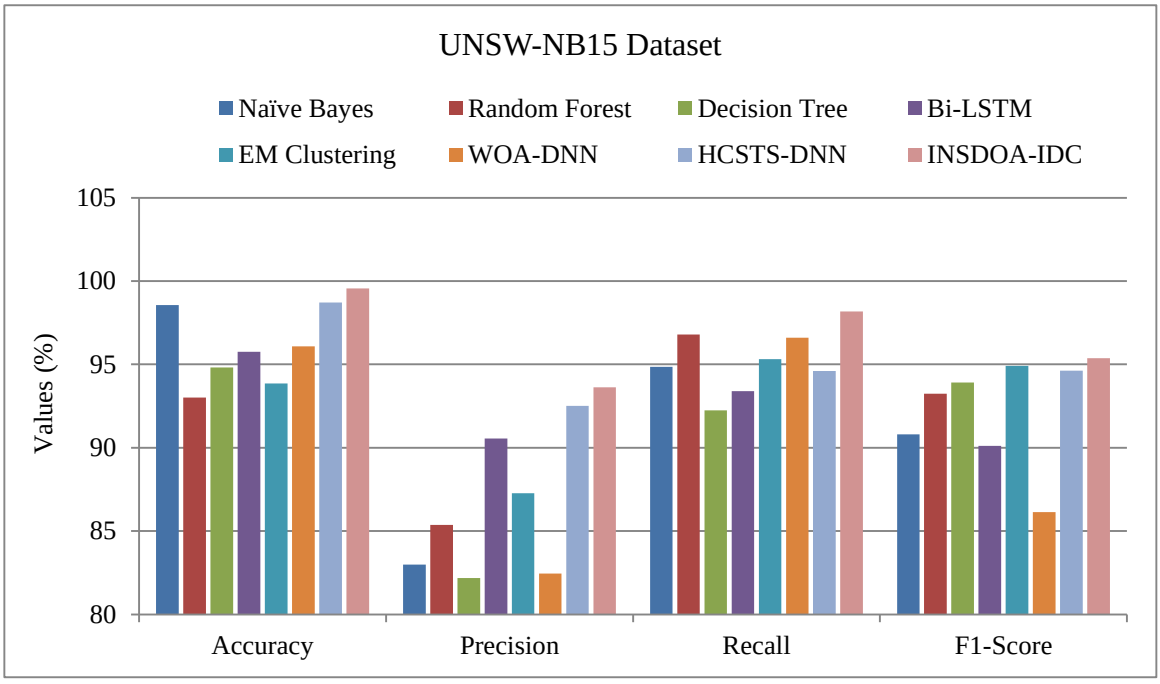

Fig. 12 Comparative assessment of the INSDOA-IDC approach under the UNSW-NB15 dataset

5. Conclusion

In this research, the INSDOA-IDC technique in MANET is proposed. The main goal of the presented INSDOA-IDC model is to detect and classify intrusions in MANET effectively. To accomplish that, the INSDOA-IDC technique involves data pre-processing, a detection process using A-CNN-BiLSTM, and a DOA-based hyperparameter tuning method. Initially, the INSDOA-IDC method applies the Z-score normalization. Furthermore, the A-CNN-BiLSTM method is employed for intrusion classification and detection. Finally, the DOA is used for the optimum selection of the hyperparameters connected to the A-CNN-BiLSTM model. Extensive simulations of the INSDOA-IDC method are accomplished under the NSLKDD and UNSW-NB15 datasets. The comparison study of the INSDOA-IDC model portrayed superior accuracy values of 99.53% and 99.55% under dual datasets over existing models.

References

[1] Saurabh Singh et al., "A Cryptographic Approach to Prevent Network Incursion for Enhancement of QoS in Sustainable Smart City Using MANET," *Sustainable Cities and Society*, vol. 79, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Surjeet Dalal et al., "An Adaptive Traffic Routing Approach Toward Load Balancing and Congestion Control in Cloud–MANET Ad Hoc Networks," *Soft Computing*, vol. 26, pp. 5377-5388, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Shivani Uyyala, and Dinesh Naik, "Anomaly Based Intrusion Detection of Packet Dropping Attacks in Mobile Ad-Hoc Networks," *2014 International Conference on Control, Instrumentation, Communication and Computational Technologies*, Kanyakumari, India, pp. 1137-1140, 2014. [CrossRef] [Publisher Link]

[4] Po-Jen Chuang, and Si-Han Li, "Network Intrusion Detection Using Hybrid Machine Learning," *2019 International Conference on Fuzzy Theory and Its Applications (iFUZZY)*, New Taipei, Taiwan, pp. 1-5, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[5] Mahendra Prasad, Sachin Tripathi, and Keshav Dahal, "A Probability Estimation-Based Feature Reduction and Bayesian Rough Set Approach for Intrusion Detection in Mobile Ad-Hoc Network," *Applied Intelligence*, vol. 53, pp. 7169-7185, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] 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]

[7] Malek Al-Zewairi, Sufyan Almajali, and Arafat Awajan, "Experimental Evaluation of a Multi-Layer Feed-Forward Artificial Neural Network Classifier for Network Intrusion Detection System," *2017 International Conference on New Trends in Computing Sciences (ICTCS)*, Amman, Jordan, pp. 167-172, 2017. [CrossRef] [Publisher Link]

[8] Nour Moustafa, Gideon Creech, and Jill Slay, "Anomaly Detection System Using Beta Mixture Models and Outlier Detection," *Progress in Computing, Analytics and Networking*, pp. 125-135, 2018. [CrossRef] [Publisher Link]

[9] Hossam Mahmoud Ahmad Fahmy, *Wireless Sensor Networks Essentials*, Wireless Sensor Networks, Springer, Cham, pp. 3-39, 2020. [CrossRef] [Publisher Link]

[10] S. Shinly Swarna Sugi, and S. Raja Ratna, "Investigation of Machine Learning Techniques in Intrusion Detection System for IoT Network," *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, Thoothukudi, India, pp. 1164-1167, 2020. [CrossRef] [Publisher Link]

[11] C. Edwin Singh, and S. Maria Celestin Vigila, "WOA-DNN for Intelligent Intrusion Detection and Classification in MANET Services," *Intelligent Automation & Soft Computing*, vol. 35, no. 2, pp. 1737-1751, 2023. [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] R. Sathiya, and N. Yuvaraj, "Swarm Optimized Differential Evolution and Probabilistic Extreme Learning Based Intrusion Detection in MANET," *Computers & Security*, vol. 144, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Nandana Rajan et al., "Two-Pronged Intrusion Detection System for MANET," *2024 International Conference on Emerging Technologies in Computer Science for Interdisciplinary Applications (ICETCS)*, Bengaluru, India, pp. 1-6, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] M. Sahaya Sheela et al., "Adaptive Marine Predator Optimization Algorithm (AOMA)-Deep Supervised Learning Classification (DSLC) Based IDS Framework for MANET Security," *Intelligent and Converged Networks*, vol. 5, no. 1, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] M. Sasikumar, and K. Rohini, "Expedient Intrusion Detection System in MANET Using Robust Dragonfly-Optimized Enhanced Naive Bayes (RDO-ENB)," *International Journal of Computer Networks and Applications*, vol. 11, no. 1, pp. 46-60, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] V.R. Sugumaran, and A. Rajaram, "Lightweight Blockchain-Assisted Intrusion Detection System in Energy Efficient MANETs," *Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology*, vol. 45, no. 3, pp. 4261-4276, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Karunakaran Saminathan et al., "Multicast On-Route Cluster Propagation to Detect Network Intrusion Detection Systems on MANET Using Deep Operator Neural Networks," *Expert Systems with Applications*, vol. 271, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[19] Tanvir H Sardar et al., "Enhancing Security in MANETs with Deep Learning-Based Intrusion Detection," *Procedia Computer Science*, vol. 259, pp. 120-129, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[20] S. Faizal Mukthar Hussain, and S.M.H. Sithi Shameem Fathima, "Federated Learning-Assisted Coati Deep Learning-Based Model for Intrusion Detection in MANET," *International Journal of Computational Intelligence Systems*, vol. 17, no. 1, pp. 1-15, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] Ahmed Ayad Abdalhameed, and Ammar Ismael Kadhim, "Molecular Swarm Optimization Analysis of Data Transmission and Recurrent Neural Networks (RNNs) for Attack Prevention in Mobile Ad Hoc Networks (MANETs)," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 19, no. 3, pp. 973-986, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[22] Mahdi Salah Mahdi AL-Inizi et al., "Improvement Networks Intrusion Detection System Using Artificial Neural Networks (ANN)," *Innovative Computing and Communications*, pp. 571-587, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] ES Phalguna Krishna et al., "Enhancing Intrusion Detection in MANETs with Blockchain-Based Trust Management and Enhanced GRU Model," *Peer-to-Peer Networking and Applications*, vol. 18, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[24] Dinesh Kumar Reddy Basani, Sri Harsha Grandhi, and Qamar Abbas, "A Centralized Infrastructure-Aware Reliable Data Transaction Model in IoT-Enabled MANET and Cloud Using GWO and Attention Mechanism with LSTM," *International Journal of Advanced Research in Information Technology and Management Science*, vol. 1, no. 1, pp. 110-134, 2024. [Google Scholar] [Publisher Link]

[25] Chunhui Li et al., "DDoS Attack Autonomous Detection Model Based on Multi-Strategy Integrate Zebra Optimization Algorithm," *Computers, Materials and Continua*, vol. 82, no. 1, pp. 645-674, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[26] Nanyi Fei et al., "Z-Score Normalization, Hubness, and Few-Shot Learning," *2021 IEEE/CVF International Conference on Computer Vision*, Montreal, QC, Canada, pp. 142-151, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[27] Xueqin Zhang, Zhongqiang Luo, and Wenshi Xiao, "CNN-BiLSTM-DNN-Based Modulation Recognition Algorithm at Low SNR," *Applied Sciences*, vol. 14, no. 13, pp. 1-14, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[28] K. Kishore Kumar, and G. Sreenivasulu, "An Efficient Routing Algorithm for Implementing Internet-of-Things-Based Wireless Sensor Networks Using Dingo Optimizer," *Engineering Proceedings*, vol. 59, no. 1, pp. 1-8, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[29] M Hassan Zaib, NSL-KDD, Kaggle. [Online]. Available: https://www.kaggle.com/datasets/hassan06/nslkdd

[30] Wells David, UNSW_NB15, Kaggle. [Online]. Available: https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15/data

[31] 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]

[32] Ketan Kotecha et al., "Enhanced Network Intrusion Detection System," *Sensors*, vol. 21, no. 23, pp. 1-15, 2021. [CrossRef] [Google Scholar] [Publisher Link]