Intelligent and Converged Networks ISSN 2708-6240
2024, 5(1): 1−18 DOI: 10.23919/ICN.2024.0001

Adaptive Marine Predator Optimization Algorithm (AOMA)–Deep Supervised Learning Classification (DSLC) based IDS framework for MANET security

M. Sahaya Sheela, A. Gnana Soundari, Aditya Mudigonda, C. Kalpana, K. Suresh, K. Somasundaram, and Yousef Farhaoui*

Abstract: Due to the dynamic nature and node mobility, assuring the security of Mobile Ad-hoc Networks (MANET) is one of the difficult and challenging tasks today. In MANET, the Intrusion Detection System (IDS) is crucial because it aids in the identification and detection of malicious attacks that impair the network's regular operation. Different machine learning and deep learning methodologies are used for this purpose in the conventional works to ensure increased security of MANET. However, it still has significant flaws, including increased algorithmic complexity, lower system performance, and a higher rate of misclassification. Therefore, the goal of this paper is to create an intelligent IDS framework for significantly enhancing MANET security through the use of deep learning models. Here, the min-max normalization model is applied to preprocess the given cyber-attack datasets for normalizing the attributes or fields, which increases the overall intrusion detection performance of classifier. Then, a novel Adaptive Marine Predator Optimization Algorithm (AOMA) is implemented to choose the optimal features for improving the speed and intrusion detection performance of classifier. Moreover, the Deep Supervise Learning Classification (DSLC) mechanism is utilized to predict and categorize the type of intrusion based on proper learning and training operations. During evaluation, the performance and results of the proposed AOMA-DSLC based IDS methodology is validated and compared using various performance measures and benchmarking datasets.

Key words: Intrusion Detection System (IDS); Security; Mobile Ad-hoc Network (MANET); min-max normalization; Adaptive Marine Predator Optimization Algorithm (AOMA); Deep Supervise Learning Classification (DSLC)

1 Introduction

Mobile Ad-hoc Network (MANET) is a brand-new form of wireless communication that functions in a highly unpredictable and challenging environment[1, 2].

Due to their ease of deployment and the rising popularity of mobile devices, these networks have recently become more and more common and crucial

• M. Sahaya Sheela is with Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Chennai 600069, India. E-mail: hisheelu@gmail.com.
• A. Gnana Soundari is with Department of Computer Science and Engineering, Saveetha School of Engineering, SIMATS, Chennai 602105, India. E-mail: soundarivenkat77@gmail.com.
• Aditya Mudigonda is with JNIAS School of Planning and Architecture, Hyderabad 500034, India. E-mail: adityaouce@outlook.com.
• C. Kalpana is with Department of Computer Science and Engineering, NPR College of Engineering and Technology, Natham Dindigul 624401, India. E-mail: kalpanasoundar13@gmail.com.
• K. Suresh is with Department of Computer Science and Engineering, PSNA College of Engineering and Technology, Poolangulathupatti 620009, India. E-mail: kokulavani1982@gmail.com.
• K. Somasundaram is with Department of Computer Science and Engineering, Sri Muthukumaran Institute of Technology, Chennai 600069, India. E-mail: soms72@yahoo.com.
• Yousef Farhaoui is with Department of Computer Science, Moulay Ismail University, Meknes 5003, Morocco. E-mail: y.farhaoui@fste.umi.ac.ma.
* To whom correspondence should be addressed.
Manuscript received: 2023-01-29; revised: 2023-07-03; accepted: 2023-08-20

to wireless communications.

Typically, MANET[3] is generally understood to be a network with a large number of independent or self-reliant nodes, frequently made up of mobile devices or other mobile nodes which can organize themselves in different ways and function without rigidly enforced top-down network management. There are numerous configurations that could be referred to as MANET, and this kind of network's potential continues to be researched[4]. The network and data link layers of the protocol stack are the main targets of new security issues caused by networks' inherent vulnerability. Each packet must move quickly through intermediate nodes in order to travel from its source to its final destination[5, 6]. By disregarding the routing protocol's requirements, malicious routing attacks can take aim at the detection or maintenance of routing. Attacks like snooping, impersonation attack, denial of service, and session hijacking are now more likely to occur. When compared to fixed networks, the security of mobile ad-hoc networks is considered from a number of angles, including accessibility, privacy, dependability, encryption, verification, and permissions. Security measures[7–9] used to protect fixed networks cannot be applied to MANETs because of their distinctive characteristics. The typical Intrusion detection system framework used in MANET is shown in Fig. 1. In order to quickly and automatically detect and categorize cyber-attacks at the host- and network-level, the IDS[10–12] frameworks are being developed using machine learning techniques. It is challenging to defend against new threats like active attacks, Byzantine attacks, and assassination attempts from malicious internal nodes. A method for keeping track of it and looking into activities taking place in a computer system is represented as IDS[13–15], which includes sophisticated techniques for analyzing and identifying abnormal behaviors. They look for evidence of malicious activity on the network to determine whether it exists. This is typically done by automatically gathering information from different networks and systems sources, then scanning the data for potential security flaws. However, the majority of systems based on these techniques struggle with high false negative and false positive detection rates as well as a lack of ongoing adaptation to malicious behaviors that change over time. Therefore, the Artificial Intelligence (AI) mechanisms[16–19] such as Machine Learning (ML) and Deep Learning (DL) techniques are developed, which makes it possible to quickly perform data analysis and visualization with the goal of enabling security professionals to find sensor

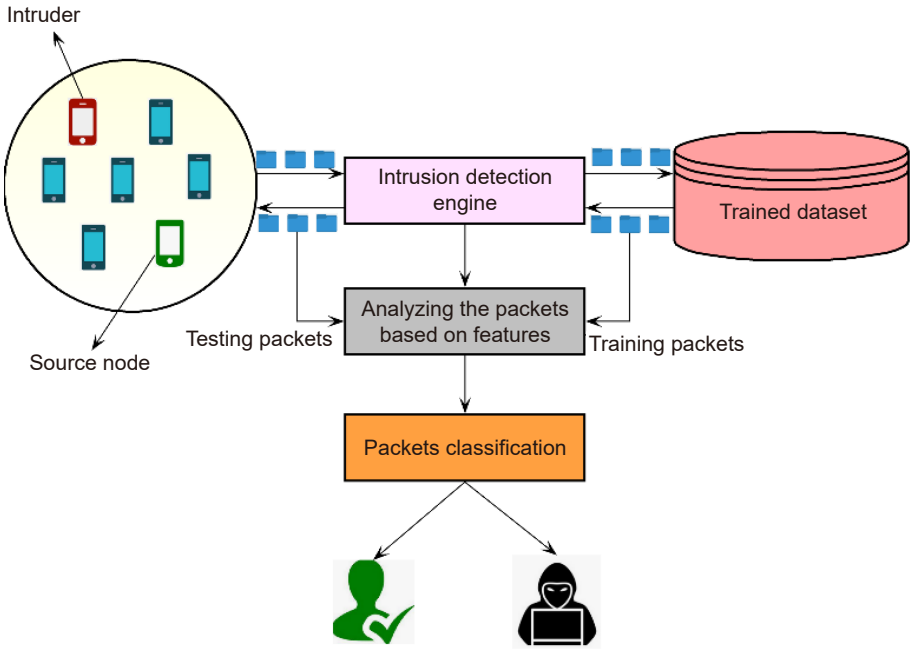

Fig. 1 IDS framework in MANET.

vulnerabilities and flaws.

However, the conventional AI-based IDS[20, 21] are unreliable and inaccurate. Hence, the proposed work intends to implement a new IDS framework for detecting network anomalies with improved performance outcomes. The key objectives of the proposed work are as follows:

To preprocess the given cyber-attack datasets for normalizing the attributes or fields, the min-max normalization model is used.

To choose the optimal features from the preprocessed dataset for improving the processing speed and detection accuracy of intrusion classification, an Adaptive Marine Predator Optimization Algorithm (AOMA) is developed.

To accurately predict and categorize the kind of intrusion based on learning and training, the Deep Supervised Learning Classification (DSLC) algorithm is implemented in Algorithm 1.

Algorithm 1 Deep supervised learning classification

```
Start
for itr in 1 to mx_itr do
  Divide the given data into k number of folds with the training and test samples;
  for each data fold do
    for each learner in the ensemble model do
      Train the learner with the foldable train set;
      Estimate the class probability value in each fold;
      Formulate the prediction matrix with class probability value;
    end for;
  end for;
  Estimate the weight value for minimizing the loss function according to the actual and predicted labels;
  Estimate the average probability value by multiplying the prediction value with the estimated weight values;
  Obtain the loss function with an estimated average probability and actual labels;
  if loss value < pre_itr then
    Add average probability in the data;
  else
    Note iteration;
  end if;
end for;
```

To validate and assess the performance of the proposed AMOA-DSLC mechanism, an extensive analysis is carried out using various parameters and benchmark datasets.

The remaining sections of this article are divided into the following groups: The comprehensive literature review of the models currently was used to create an effective IDS framework is presented in Section 2. It also evaluates each model's advantages and disadvantages in terms of intrusion detection effectiveness and results. The proposed DL-based IDS framework for MANET security is clearly explained in Section 3. Additionally, Section 4 validates and compares the outcomes of the proposed methodology using various datasets and parameters. In Section 5, the overall paper is summarized along with the conclusions, benefits, results, and future work.

2 Related work

This section investigates the different types of existing techniques used for developing an effective IDS framework to secure MANET. Moreover, it examines the advantages and disadvantages of each mechanism according to its detection operations and performance outcomes.

Laqtib et al.[22] presented a comprehensive literature review on various machine learning techniques used for developing an IDS in MANET. Here, the different types of architectures used to detect various intrusions in the network are developed, which generates the reports by analyzing the misbehavior and attacking activities. It includes the following types: standalone architecture, distributed & collaborative model, and hierarchical model. Moreover, the different types of DL architecture models are also investigated in this work for developing an IDS framework. Since deep architecture-based IDS can be much more representationally efficient than shallow ones, and it is necessary to develop an effective training algorithms for these systems. Also, it may be crucial for choosing the appropriate techniques based on the MANET situation. Ali Khan and Herrmann[23] presented a comprehensive analysis to study the recent advancements in IDS for IoT systems. Despite being a relatively new field of study, security of IoT networks can benefit from research done for networks like MANET and Cyber-Physical Systems (CPS). The IDS

is categorized into the following types: decision quality, responses on attacks, attacker type, detection technique, and implementation strategy. When other security measures like access control or encryption are unable to identify attacks, it is frequently considered a second line of defense solution. Moreover, the IDS implementation strategies are validated and assessed in terms of energy consumption, processor requirements, detection accuracy, and resource constrained nodes. One type is voting-based IDSs, which are already light enough to be used sparingly with resources. Regrettably, they still have below-average accuracy, and more studies are required to lower the number of false negatives. Moudni et al.[24] deployed a fuzzy-based IDS framework for identifying blackhole attacks in MANET. Here, the Adaptive Neuro-Fuzzy Inference System (ANFIS) is developed that detects the blackhole attacks in the network based on the membership functions, position and shape. Moreover, the Particle Swarm Optimization (PSO) algorithm is used to enhance the detection performance of ANFIS with reduced time and error rate. Here, two different parameters such as Forward Packet Ratio (FPR) and Average Destination Sequence Number (ADSN) have been used to assess the performance of IDS framework. Moreover, a new table, called as neighboring table, is formulated to record all activities of neighborhood nodes in the network. Ali Zardari et al.[25] deployed a new dual attack detection mechanism for detecting both the blackhole and grayhole attacks in the network. Also, the Connected Dominating Set (CDS) has been used to enhance the performance of IDS, which includes two different features such as energy and non-existence. Here, the energy level of nodes are validated to predict the malicious nodes in the network based on the trusted query. The primary advantage of the suggested framework are increased detection rate, delivery ratio, and low time consumption. Rachid et al.[26] deployed an M-best feature selection mechanism for identifying intrusions from MANET. Here, the Random Forest (RF) classification approach was used to detect and categorize the intrusions in the network with high accuracy and stability. Here, the final prediction rate is highly improved by properly training and testing the features of the given dataset. Ali Abbood et al.[27] presented a comprehensive survey to examine the different types of approaches used for developing an effective IDS framework. Here, various detection approaches such as Recurrent Neural Network (RNN), Naïve Bayes (NB), Extreme Learning Machine (ELM), Deep Belief Network (DBN), and Self-Organizing Map (SOM) have been investigated in this work. Typically, the IDS process in MANET is categorized into the following types: intrusion prevention, detection, and mitigation. Furthermore, even the most sophisticated and secure systems are vulnerable to insiders who abuse their access. When inspecting vulnerability visualizations, an alarming trend emerges: the overall number of reported vulnerabilities each year is increasing, and the vast majority of them are classified as medium or high severity.

Prasad et al.[28] implemented a clustering based unsupervised learning model for spotting intrusions in MANET. The suggested centroid initialization based clustering method outperforms basic clustering in terms of accuracy and takes fewer iterations to form final clusters. Moreover, the unsupervised feature selection model used in this work eliminates redundant and pointless features from the unlabeled dataset and chooses sequence features. These redundant features could lead to issues like increasing computations, deviating from actual clusters, supporting poor decisions, etc. Hadi et al.[29] developed a Zone Sampling-Based Traceback Algorithm (ZSBT) for identifying and categorizing the type of intrusions in MANET. The contribution of this paper was to accurately detect the DoS attacks in MANET, where the different types of parameters such as packet loss, packet sending rate, packet receiving rate, and energy consumption. Moreover, the discretization based preprocessing is applied to normalize the dataset for accurately spotting intrusions in the dataset. Meddeb et al.[30] deployed a Mobile Data Analysis (MDA) based security model for detecting intrusions in MANET. Here, the stacked auto-encoder model is utilized to enhance the performance of IDS with ensured flexibility, accuracy, and reduced time consumption.

Venkatasubramanian[31] implemented a multi-stage optimization based fuzzy mechanism for securing MANET from intrusions. In this framework, the z-score normalization mechanism is applied to preprocess the given dataset by converting the categorical values into the numerical attributes. Then, the SMOTE analysis is performed to enhance the training performance of classifier with reduced oversampling rate. Moreover, the Information Gain based Feature Selection (IGBFS) mechanism is applied to extract the most suitable features from the normalized dataset. The key benefits of this work are better system performance, easy to understand, and efficient problem handling.

Asharf et al.[32] presented a comprehensive review on various ML and DL approaches used for developing an IDS frameworks. The aim of this paper is to deploy a new security model for analyzing the different types of risk factors associated to the IoT networks. Here, some of the most vulnerabilities such as authorization attacks, integration attacks, confidentiality attacks, and vulnerability in visualization platform are considered for securing the distributed architecture. Based on this study, it is observed that the IDS design is highly depends on the followings: data source, detection methods, detection time, architecture, and environment. Venkateshwaran and Prabaharan[33] designed a neuro-deep learning algorithm for spotting intrusions from MANET. This framework includes the modules of data preprocessing, intrusion recognition, reporting, and response. This kind of hybrid IDS framework provides the benefits of increased delivery ratio and detection accuracy.

It is determined from the literature review that the existing IDS frameworks were created using different feature selection and learning models. However, it persists to have significant issues with the following:

- Ineffective handling of large dimensional datasets.
- Increased false prediction.
- High oversampling rate.
- Lack of reliability and detection accuracy.

Therefore, the proposed work aims to create a computationally proficient deep learning-based IDS framework for MANET security.

3 Proposed methodology

This section provides the clear explanation for the proposed AMOA-DSLC based IDS framework for securing MANET from intrusions. The novel contribution of this work is to implement an advanced soft-computing methodologies for creating an effective IDS framework[34]. In this framework, a computationally intelligent and effective mechanisms, such as Adaptive Marine Predator Optimization Algorithm (AMOA) and Deep Supervised Learning Classification (DSLC) are developed for creating an IDS framework. The overall workflow of the proposed system is shown in Fig. 2, which holds the following key operations:

- Dataset normalization.
- Feature optimization using AMOA.
- Intrusion classification using DSLC.
- Performance evaluation.

The min-max normalization model is used to preprocess the data after receiving the input cyber-threat datasets, helping to enhance classification performance. In this study, the popular datasets are obtained from the public repositories, which have some missing fields, attributes, and information. Hence, the performance of classifier may be degraded with high false predictions and error outputs. In order to solve this issue, the proposed work aims to apply a data preprocessing method to generate the balanced dataset for accurate attack classification. During this process, the irrelevant attributes removal, redundant field elimination, missing information replacement, and attribute balancing are performed to transform the imbalanced input dataset to balanced dataset. The aforementioned operations are performed with the use of min-max normalization mechanism. It helps to increase the overall performance of the proposed system with high accuracy, precision, and lower false predictions. The AMOA is then used to select the features from the normalized dataset that will best aid in training the classifier with data samples. The AMOA is one of the novel and intelligent optimization algorithms that offers the advantages of increased convergence rate, processing speed, and less time,

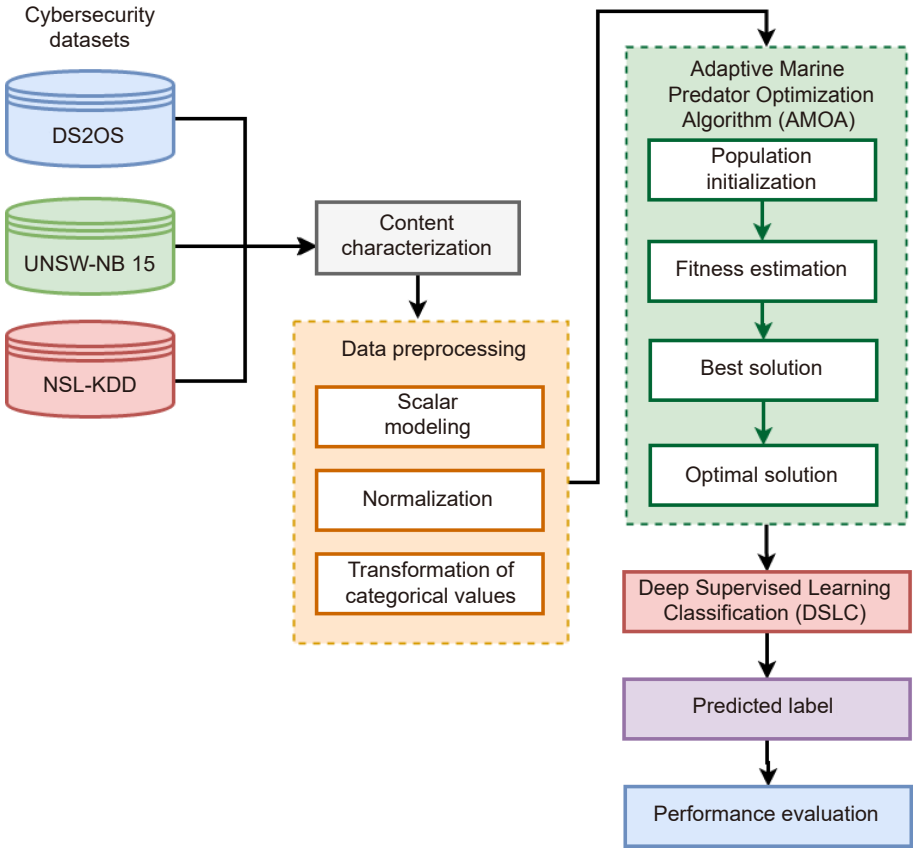

Fig. 2 Workflow of the proposed model.

among other optimization technique. We have used the Marine Predator Optimization (MOA)[35–37] algorithm to choose the pertinent and essential attributes from the cyber-security datasets based on its best optimal solution. In the previous studies, the MOA technique is used to resolve some of the complex engineering problems, due to its increased convergence rate and best optimal performance. Therefore, the proposed work intends to use this optimization technique for assuring better cyber-system performance. As a result, the DSLC algorithm is used to precisely predict the type of intrusion based on the chosen features. In the previous works, a different types of optimization based classification techniques are implemented for developing an IDS framework to secure MANET. According to the recent surveys, it is determined that the majority of existing works could use the reliable techniques for ensuring cyber-security, but they follows some complex models for obtaining an increased attack detection rate. So, the training & testing complexity of the existing classification models are high, which leads to high time consumption. Therefore, the proposed work aims to develop an accurate and simple IDS framework for securing MANET from cyber-threats. For this purpose, the recent as well as efficient optimization technique, named as AMOA, is used in this study for choosing the relevant and well-suited features from the given datasets. The obtained dimensionality reduced attributes or features are used to train the classifier, which supports to increase the processing speed and accuracy of classifier while detecting attacks from datasets. The novel contribution of this work uses the combination of AMOA and DSLC techniques for developing an IDS framework with high accuracy and lower false predictions. Moreover, the Marine predator optimization is not increasingly used in the MANET applications, hence we aims to apply this technique for simplifying the detection process of classifier.

3.1 Dataset normalization

One of the key stages in the attack detection and

classification systems is generally data normalization. Because the raw datasets are made up of network data packets with some values missing. In the proposed framework, data preprocessing is one of the most important and essential component, since it helps to generate the attribute balanced dataset for making an effective and accurate decision while predicting attacks. Typically, the original datasets obtained from the public repositories are not balanced, which may have some missing attributes and fields that affects the classifier's prediction performance. Normalization is a preprocessing step, a scaling tool, or a mapping approach. From an existing range, we are able to determine a new range. It can be quite beneficial for purposes of forecasting or prediction. Moreover, there are numerous ways to make predictions or estimates, but they can all differ significantly from one another. Therefore, the normalization technique is needed to make prediction closer while maintaining their wide range. Typically, the min-max normalization is a method that applies linear transformation to the initial set of data. The term min-max normalization refers to a method that preserves the associations between the original data. It is a straightforward technique that allows data to be precisely fitted inside a given boundary using a predetermined border. Therefore, it may result in more false positives that significantly reduces the classification performance. Therefore, the initial stage of preprocessing involves the replacement of missing values, and the conversion of categorical to numerical values. The network IDS datasets typically contains a wide range of values, so it is imperative to normalize the data using a common scale. Normalization is primarily carried out to speed up convergence and improve classification accuracy because without it, gradient descents may take longer to converge. In this model, the obtained original network dataset DS_N is considered as the input, where each and every element present in the data is validated for replacing the missing data elements as shown in below:

$$N_D = \prod_{n=1}^{N} \frac{DS_N(n,:) - \min(DS_N(n,:))}{\max(DS_N(n,:)) - \min(DS_N(n,:))} \quad (1)$$

where N_D represents the normalized dataset, DS_N is the obtained network dataset, and n indicates the number of elements exist in the data. The preprocessed data can then be used for additional processing, which helps to minimize false positives and results from misclassification.

In the proposed IDS framework, there are three different and popular intrusion datasets are used for system implementation and testing. After that, the content characterization is performed, where the basic and traffic based contents characteristics are estimated for an effective prediction. Consequently, the normalization and categorical transformation are performed to preprocess the given data. Here, the data values are initially transformed to optimize the information, which helps to reduce the complexity of classification. Moreover, the normalized data could speed up the training process with improved efficiency. In the proposed framework, the data scaling based normalization is applied, which is often known as min-max normalization that converts the data with the interval of [–1, 1] and [0, 1]. Then, an APOA based optimization technique is used to choose the optimal features from the normalized dataset for making an accurate decisions while predicting the intrusions. The APOA provides the optimal solution for selecting the best features that are used to improve the training speed of classifier. Furthermore, the DSLC technique is implemented to categorize the type of intrusion according to the chosen features. It is a kind of ensemble classification method, which incorporates the functions of five different base learners such as KNN, RF, XGB, LR, and randomized trees. During classification, the processes including cross validation, training of base learners, optimization of loss function, estimation of weighted average, and final prediction are carried out, which supports to accurately identify the type of intrusion from the given data. In the proposed framework, the AMOA is integrated with the DSLC algorithm for intrusion identification and classification, whereas the AMOA is used for feature optimization and DSLC is used for intrusion identification.

Adaptive Marine Predator Optimization Algorithm (AMOA): After normalization, an

Adaptive Marine Optimization Algorithm is deployed to optimally select the features from the preprocessed dataset. The marine predator algorithm is a new meta-heuristic algorithm that draws inspiration from nature and imitates the natural interactions between marine predators and prey. Additionally, it has been noted in the literature that this algorithm is capable of resolving a wide range of practical optimization issues, making it a new favorite among researchers. The marine predator algorithm still has some shortcomings, including the inability to generate a diverse initial population with high productivity, the lack of quick escape from the local optimization, and the lack of thorough and thorough exploration of the search space. An improved version of this algorithm is put forth in the current study and is based on the opposition-based learning method, chaos maps, population self-adaptation, and switching between exploration and exploitation phases. In each iteration, the self-adaptive population method automatically modifies the population size, which facilitates quickening convergence.

In the proposed work, an AMOA technique is mainly used for optimizing the features of the normalized dataset, since an increased dimensionality of features may affect the overall performance of the classifier. Hence, it is more essential to reduce the size of features before attack identification and classification. For this purpose, the most recent AMOA technique is implemented in this study. When compared to the other optimization algorithms, the AMOA has the key benefits of high convergence rate, increased searching speed, requires low time for reaching optimal solution in the searching area, and high efficiency. Due to these reasons, the proposed AMOA technique is incorporated in the proposed intrusion detection framework. Moreover, this technique provides the best optimal solution for the given problem with low complexity. The guiding principles for the best foraging, interactions, and learning in marine predators are outlined in the main points listed below:

The same proportions of Lévy and Brownian movement were seen throughout the lifetime of marine predators as they moved through various habitats.

Marine predators adopt the Lévy approach in environments with low concentrations of prey and the Brownian movement in environments with prevalent prey.

They alter their behavior in an effort to locate places with an altered distribution of prey due to ecological effects such as those generated by human activity or natural phenomena.

They make use of their sharp memories to keep track of one another and the best places to go foraging.

The MPA optimization process is broken down into three main phases that take different velocity ratios into account while simulating a predator and prey's entire life cycle:

• When there is a large velocity ratio or when the predator is outpacing the prey.

• When both the predator and the prey are moving at almost the same speed or in the unit velocity ratio.

• In a situation when the predator is travelling more quickly than the prey.

• A precise duration of iteration is designated and assigned for each phase that is determined.

These actions are described in accordance with the regulations governing predator and prey movement while imitating predator and prey movement in nature. These actions are described based on the regulations that govern how predators and prey move in nature, simulating such regulations.

In this algorithm, the optimization process's first, second, and third stages each have one-third of all the iterations. Intuitively, the order of these strategies will change as the total number of iterations varies. The same number of times, or one-third of the total number of iterations, should be chosen for the exploration and exploitation phase. However, increasing the total number of iterations for the same optimizations does not produce the same median results; instead, they are occasionally better and every once in a while worse. The exploration or operation phase of the optimization process is thus chosen by the MMPA algorithm using an adaptive strategy.

The operating phases involves

• Levy-motion for low-concentration prey environment.

• Brownian-motion for moderate prey environment.

• Good memory in recounting their partners as well as the position of effective hunting are the key components of MPA.

The phases are divided into categories according to time and velocity ratio.

Phase 1: Predator moves more slowly than its prey (Increased velocity ratio).

Phase 2: The speed of the prey and the predator is nearly equal (Unity velocity ratio).

Phase 3: The predator is pursuing the prey while moving more quickly (Decreased velocity ratio).

The following equation describes the Lévy flight, which is nothing more than a series of random numbers with step sizes determined by the Lévy distribution.

$$\text{Lévy}(\alpha) = 0.05 \times \frac{a}{|b|^{\frac{1}{\rho}}} \tag{2}$$

Standard Brownian motion is the probability function derived from a normal (Gaussian) distribution with mean (μ) 0, and variance (σ) is 1 with step length from a random process. The Probability Density Function (PDF) for this motion at point a is given by equation:

$$f(a;\mu,\sigma) = \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{a^2}{2}} \tag{3}$$

The first solution is uniformly dispersed over the search space as the initial trial in MPA, just like other meta-heuristics.

$$M_0 = M_{\min} + r(M_{\max} - M_{\min}) \tag{4}$$

where the lower and upper limits for the variables are $M_{\min}$ and $M_{\max}$, respectively, and r is the random number. According to the survival of the fittest theory, the marine predators (P) that are the fittest develop an Elite Matrix (EM). Certainly, the top predators (denoted by w) have an excellent hunting skills. Search agents are both predator and prey; both are searching for their food. If the topmost predator is replaced by a better predator, then the elite matrix is updated, and other matrix termed as prey is formulated as follows:

$$\text{EM} = \begin{bmatrix} w_{1,1} & \cdots & w_{1,n} \\ \vdots & \ddots & \vdots \\ w_{m,1} & \cdots & w_{m,n} \end{bmatrix}_{m \times n} \tag{5}$$

$$P = \begin{bmatrix} w_{1,1} & \cdots & w_{1,n} \\ \vdots & \ddots & \vdots \\ w_{m,1} & \cdots & w_{m,n} \end{bmatrix}_{m \times n} \tag{6}$$

It's crucial to remember that the MPA's elite and prey matrices are two crucial components on which the optimization technique tends to depend. The exploration phase, which corresponds to the period when the prey moves more quickly than the predator, occurs in this section of the MPA algorithm.

The MPA algorithm's exploration phase has the following mathematical model:

$$\overrightarrow{\text{SS}_x} = \overrightarrow{R_{\text{B}}} \times (\overrightarrow{\text{EM}_x} - \overrightarrow{R_{\text{B}}} \times \overrightarrow{P_x}); x = 1, \ldots, n \tag{7}$$

where $\overrightarrow{\text{SS}_{\text{a}}}$ represents the step size, $\overrightarrow{\text{EM}_{\text{x}}}$ indicates an elite matrix, and $\overrightarrow{P_x}$ denotes the prey, then these parameters as updated by using the following models:

$$\overrightarrow{P_x} = \overrightarrow{P_x} + P\overrightarrow{\text{R}} \times \overrightarrow{\text{SS}_x} \tag{8}$$

$$\overrightarrow{\text{SS}_x} = \overrightarrow{R_{\text{L}}} \times (\overrightarrow{\text{EM}_x} - \overrightarrow{R_{\text{L}}} \times \overrightarrow{P_x}); x = 1, 2, \ldots, \frac{n}{2} \tag{9}$$

$$\overrightarrow{P_x} = \overrightarrow{P_x} + P\overrightarrow{R} \times \overrightarrow{\text{SS}_x} \tag{10}$$

$$\overrightarrow{\text{SS}_x} = \overrightarrow{R_{\text{B}}} \times (\overrightarrow{R_{\text{B}}} \times \overrightarrow{\text{EM}_x} - \overrightarrow{P_x}); x = \frac{n}{2}, \frac{n+1}{2}, \ldots, n \tag{11}$$

$$\overrightarrow{P_x} = \overrightarrow{\text{EM}_x} + P\overrightarrow{\text{CF}} \times \overrightarrow{\text{SS}_x} \tag{12}$$

where $\overrightarrow{R_{\text{L}}}$ is the random vector generated using Levy distribution, $\overrightarrow{R_{\text{B}}}$ defines the dimensional vector that is uniformly distributed in the range of 0 to 1.

The exploration phase gradually transitions into the exploitation phase during the unit velocity estimation, which is the middle stage of the optimization process. When the predators outpace the prey and the exploitation phase of the algorithm is finished, the MPA is established, and the final step is the low velocity estimation.

$$\overrightarrow{P_x} = \begin{cases} \overrightarrow{P_x} + \text{CF}\left(\overrightarrow{M_{\min}} + \overrightarrow{R} \times \left(\overrightarrow{M_{\max}} - \overrightarrow{M_{\min}}\right) \times \overrightarrow{U}\right), \text{if } r \leqslant \text{FD}_{\text{s}}; \\ \overrightarrow{P_x} + (\text{FD}_{\text{s}} \times (1-r) + r)\left(\overrightarrow{P_{r1}} - \overrightarrow{P_{r2}}\right), \text{ if } r \leqslant \text{FD}_{\text{s}} \end{cases} \tag{13}$$

where FD represents the fish aggregating devices, and CF defines the step size controlling parameter. Finally, the optimal best solution is obtained as the output of this algorithm, which is used to choose the features from the dataset for training the samples of classifier.

3.2 Deep Super Learning Classification (DSLC)

Here, the Deep Super Learning Classification (DSLC) technique is used to precisely classify the intrusions

from the dataset after the features have been extracted. This classifier is developed based on the cascading hierarchical architecture model, which processing the features layer by layer and each layer feeding its processed to the one below it for more processing. Figure 3 shows the DSL technique's cascading structure, which is composed of processing features that are applied layer by layer. This technique allows information to be processed based on a layered architecture where *j* stands for classes, *k* for folds, *l* for features, *m* for base learners, and *n* for records in the training set. Additionally, it includes the following steps:

• Cross-validation.
• Feature development and training.
• Loss function and weight optimization.
• Retraining the set, prediction.

For the purpose of producing the out of sample predictions, cross validation is first conducted on the entire training dataset. The training set can then be divided into groups of equal size to serve as the validation sets. Following that, it was possible to build and train each fold in the model output class. As a result, the base learners are used to obtain the prediction for the entire set. In order to reduce the true values, the loss function can also be optimized for recognizing the linear combination. The best weight values are then calculated in relation to the weighted average of the predictions. With enough cross validation folds, each mode on the entire training dataset could be retrained. On top of the raw training data, which incorporates the vectors as additional features of the records, the overall prediction results are also added. Finally, these procedures can be repeated until the training data have undergone the most iterations. In the proposed DSLC, there are five different base learning algorithms have been used for an effective prediction, which includes eXtreme Gradient Boost, Random Forest, Logistic Regression, K-Nearest Neighbor, and Randomized tree. In this algorithm, each trained model is applied with weight values that have been optimized at each iteration to generate predictions on test data that has not yet been observed. If the models were successfully trained on

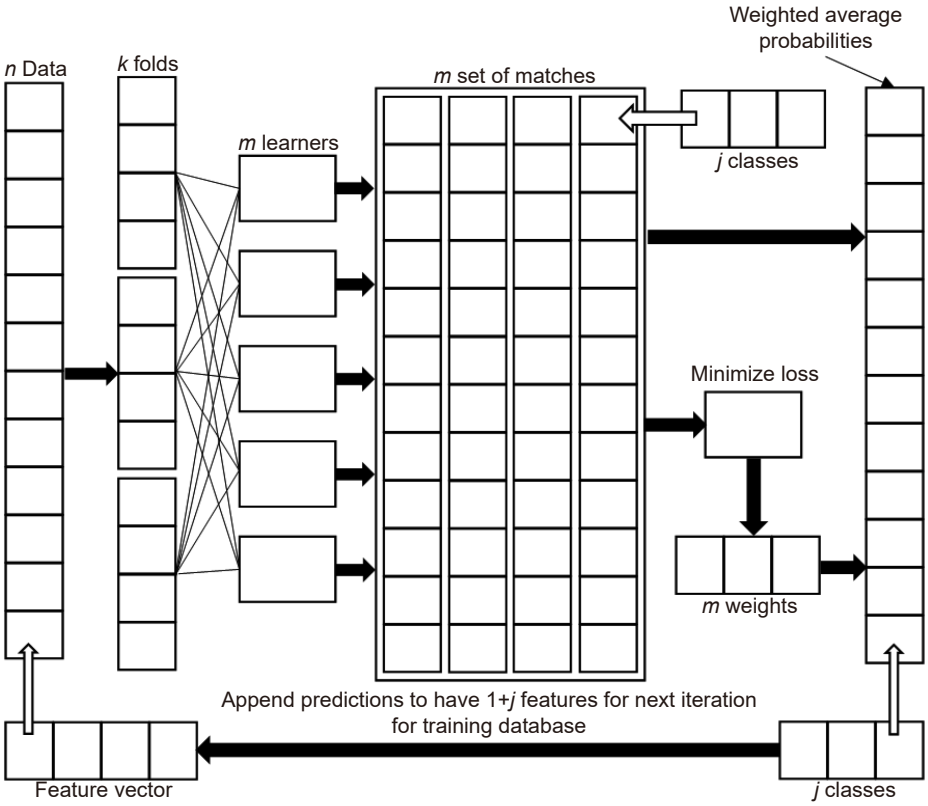

Fig. 3 Architecture of DSLC.

the whole training set, the m models are used for every iteration. Moreover, the linear combination of predictions are identified from all m learners in order to reduce the desired outcome and the true values for the training data by optimizing a loss function. After that, the optimized weights and the loss function value are retained. In this case, convex optimization will do because log loss is a convex function. Then, the weighted average is estimated to gain overall predictions for each record, which is performed by each learned according to the optimized weight value. The predictions are incorporated using the aforementioned procedures into the training data. This process is repeated until it is no longer decreasing the optimized loss value with each cycle and keep track of how many training iterations are completed.

4 Result and discussion

This section presents the results and discussion of the proposed AMOA-DSLC based IDS framework by using different parameters and evaluation indicators. The correctness of the dataset can be used to assess the performance of IDSs. As a result, three different datasets are used to evaluate the proposed NIDS in order to thoroughly examine the model's performance. Table 1 shows the list of datasets used in this work for validating the performance of AMOA-DSLC based IDS framework. These benchmarking datasets are the most popular and widely used in many cyber-security applications for validating the performance of IDS frameworks. In this study, the publicly available datasets including UNSW-NB 15, DS2OS, and NSL-KDD are used for system implementation and validation. These benchmarking datasets are publicly available and accessible from the Kaggle repository[38–43]. By using these, the performance of the proposed intrusion detection is evaluated and compared based on the parameters of detection rate, accuracy, precision, recall, efficiency, and F1-score[44]. During assessment, some of the recent literature models are compared with the proposed approach for determining its efficacy over other approaches[45–47].

Table 1 Different datasets used in this work.

Dataset	Description
Dataset 1	NSL-KDD
Dataset 2	DS2OS
Dataset 3	BoT-IoT

Moreover, various evaluation parameters used to assess the results of the proposed AMOA-DSLC are as calculated by using the following equations:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{14}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{15}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{16}$$

$$\text{F1-score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{17}$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}} \tag{18}$$

where TP–True Positive, TN–True Negative, FP–False Positive, and FN–False Negative. True Positives (TPs) are cases in which the prediction is correct and the actual value is correct. True Negatives (TNs) are cases in which the prediction is negative and the actual value is also negative. False Positive (FPs) are cases in which the prediction is positive but the actual value is negative. The term False Negatives (FNs) refers to situations in which the prediction is negative but the actual value is positive. Table 2 and Fig. 4 presents the comparative analysis of the existing ML, DL, and proposed DSL methodologies used for developing an IDS framework. According to the results, it is noted that the proposed AMOA-DSLC based IDS methodologies provides an improved result, when compared to the baseline approaches. Because, the best way to detect intrusion is by optimizing functionality. This is a crucial step in correctly classifying the various types of attacks. Without feature optimization, it would

Table 2 Performance evaluation using Dataset 1.

Method	Accuracy (%)	Precision (%)	F1-score (%)	Recall (%)
RF	99.66	99.85	99.84	99.83
CNN	85.99	90.90	85.76	81.17
Inc-CNN	89.03	85.08	85.33	85.58
Bi-LSTM	84.33	93.98	89.82	86.01
GRU	78.98	81.08	84.20	87.56
Proposed	98.89	99.21	98.99	99.10

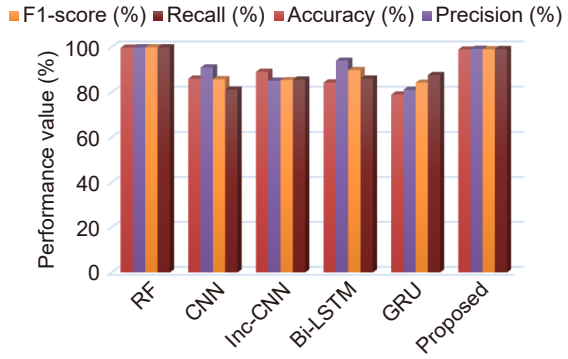

Fig. 4 Comparative analysis among the existing and proposed approaches using Dataset 1.

take a long time to develop a model and it might be possible to misclassify assaults. The methods for selecting functions greatly cut down on training and testing time and improved the rate of intrusion detection. Due to the inclusion of AMOA technique, the results of the proposed IDS framework is highly improved over the other models[48–51].

Consequently, the detection rate of the existing[28] and proposed AMOA-DSLC models are validated and compared using Dataset 1 as shown in Fig. 5 and Table 3. Typically, the detection rate is one of the most important parameter used to assess the overall performance of IDS. When the TP and TN are higher, the system performs better, but when the FP and FN are higher, the system performs worse. Moreover, FP is the incorrect classifier prediction in the context of the

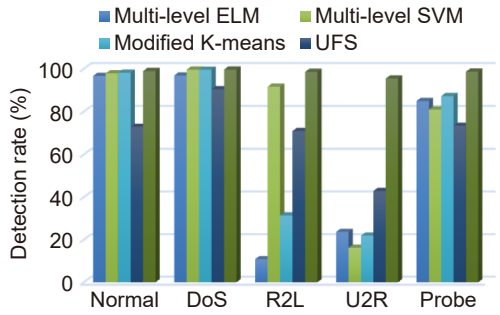

Fig. 5 Detection rate on Dataset 1.

Table 3 Detection rate analysis using Dataset 1. (%)

Attack type	Multi-level ELM	Multi-level SVM	Modified K-means	UFS	Proposed
Normal	96.64	97.83	98.13	72.87	98.89
DoS	96.83	99.57	99.54	90.39	99.60
R2L	10.84	91.60	31.39	70.94	98.50
U2R	23.68	16.23	21.93	42.86	95.40
Probe	84.93	80.94	87.22	73.36	98.60

normal category, which enables attack to enter the system. In contrast, FN also makes incorrect predictions when normal does, which raises the alert threshold. The obtained results indicate that the proposed AMOA-DSLC technique provides an improved performance outcomes over the other techniques, rate among the existing, and proposed approaches using Dataset 1.

Figure 6 and Table 4 presents the comparative analysis among the baseline[31], and proposed security frameworks based on different parameters. These results also depict that the proposed AMOA-DSLC provides an improved results, when compared to the baseline models.

Figures 7 and 8 compares the detection rate of the existing[41] and proposed security models using Datasets 2 and 3 with respect to different types of attacks correspondingly. Similarly, the accuracy is also compared among the existing and proposed models using Datasets 2 and 3 as shown in Figs. 9 and 10. The overall results indicate that the proposed AMOA-DSLC overwhelms the baseline security frameworks

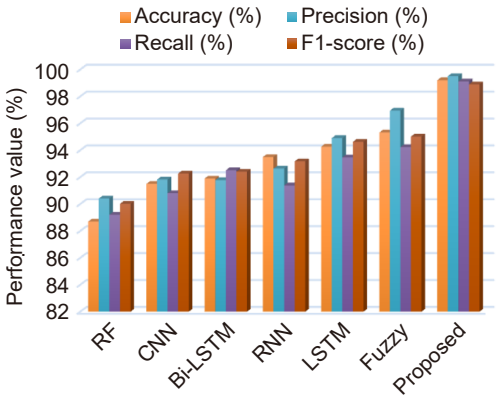

Fig. 6 Performance comparative analysis among the existing and proposed IDS frameworks using Dataset 1.

Table 4 Overall performance comparison using Dataset 1.

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
RF	88.70	90.41	89.21	90.02
CNN	91.50	91.82	90.81	92.27
Bi-LSTM	91.90	91.78	92.52	92.41
RNN	93.50	92.63	91.38	93.18
LSTM	94.27	94.91	93.47	94.63
Fuzzy	95.32	96.95	94.24	95.02
Proposed	99.21	99.51	99.12	98.90

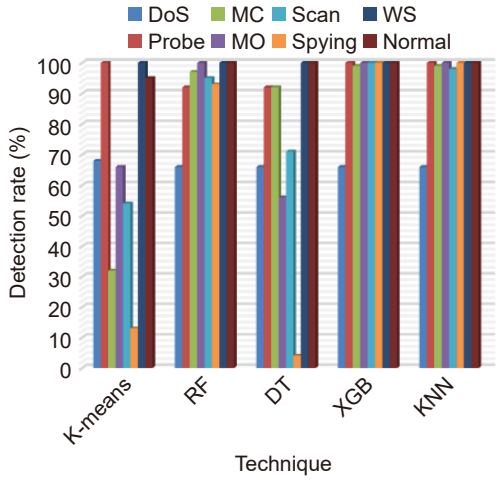

Fig. 7 Detection rate analysis using DS2OS dataset.

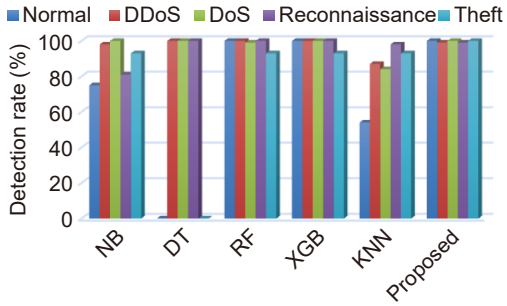

Fig. 8 Detection rate analysis using BoT-IoT dataset.

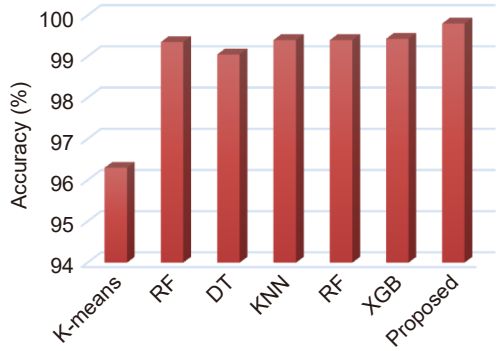

Fig. 9 Accuracy analysis using DS2OS dataset.

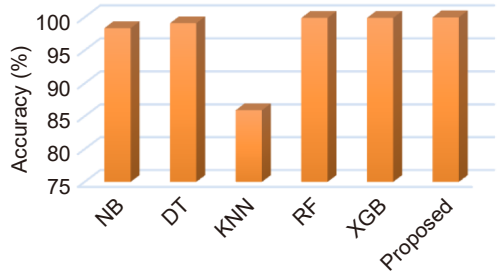

Fig. 10 Accuracy analysis using BoT-IoT dataset.

with increased accuracy and detection rate.

Here, the efficiency also known as prediction accuracy of the classifier is estimated with respect to the number of epochs. Efficiency is one of the most essential parameter used to test classifier's training and training performance. As shown in Fig. 11, the training efficiency and testing efficiency of the proposed classification system is validated and compared with respect to number of epochs. In order to validate the effectiveness of classifier by determining how it predict the desired results, the training and testing efficiencies are evaluated in this study. The improved level of efficiency indicates the improved performance of the classifier, and the results reveal that the training efficiency is increased to 99%, and the testing efficiency is increased to 98% by using the AMOA technique integrated with the DSLC algorithm. According to the estimations, it is analyzed that the proposed AMOA-DSLC outperforms the other classification techniques with increased training & testing efficiency values. Here, the optimized feature set is used to train the classifier, which helps to obtain an improved performance in the proposed system. Figure 12 validates the detection rate and validation accuracy of the proposed DSLC with and without

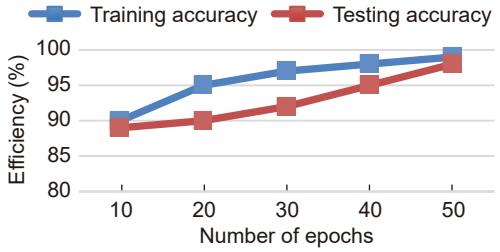

Fig. 11 Training efficiency and testing efficiency.

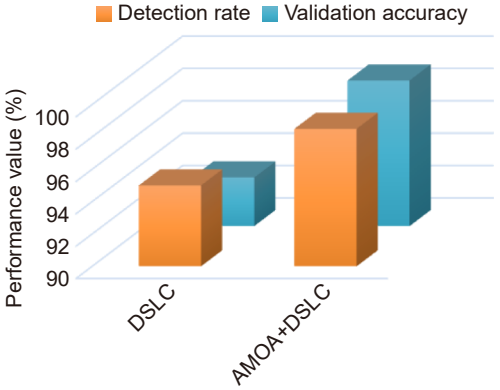

Fig. 12 Detection rate and validation accuracy of the proposed DSLC with and without AMOA technique.

AMOA technique. Based on the outcomes, it is determined that the proposed classification technique provides an increased detection rate and validation accuracy, when it incorporates with the AMOA technique. By using the optimized set of features, the AMOA+DSLC technique provides an improved performance outcomes. The parameters such as detection rate and validation accuracy are validated and compared with and without inclusion of optimization technique, i.e., AMOA. These parameters are mainly used to determine the overall performance of the classifier in intrusion detection. The findings indicate that the DSLC integrated with AMOA technique provides an increased detection rate and validation accuracy, when comparing to the DSLC technique. Since, the feature optimization using AMOA technique helps to speed up the processing speed of classifier with the reduced set of features. Hence, the false predictions are effectively reduced in the proposed model, which supports to obtain an increased accuracy and detection rate while predicting intrusions from the given dataset.

The findings reveal that the average accuracy for all datasets is increased up to 99% with the detection rate 98.5%, and the obtained results are superior to the existing models. Due to the integration of AMOA, the detection performance of the DSLC is greatly improved in the proposed model. Table 5 presents the statistical performance analysis of the proposed AMOA technique based on the parameters of *p*-value, *z*-value, mean, and standard deviation. It is used to analyze the exploitation and exploration capabilities of the optimization algorithm. The obtained results indicate that the AMOA reaches the global optimum with increased convergence speed and better exploration & exploitation capabilities.

5 Conclusion

This paper presents a new AMOA-DSLC based IDS framework for protecting MANET from intrusions. The original contribution of this work is to guarantee the security of MANET by creating a computationally effective IDS framework using an advanced soft-computing methodology. The proposed framework is composed with the stages of dataset normalization, feature selection, and intrusion classification. Here, the min-max normalization model is used to preprocess the provided cyber-attack datasets for normalizing the attributes or fields. The original contribution of this research work is to develop a new intrusion detection framework by integrating the AMOA and DSLC methodologies. Here, the AMOA is used for choosing the relevant features from the preprocessed dataset with the best optimal solution. Consequently, the DSLC algorithm is used to accurately predict and categorize the type of intrusion based on learning and training. During evaluation, various parameters and benchmark datasets are used in a thorough analysis to validate and rate the effectiveness of the proposed AMOA-DSLC mechanism. According to the results, it is observed that the proposed AMOA-DSLC methodology provides an improved result in terms of high detection rate, accuracy, and low false positive rates for all datasets. Then, the selected features are passed to the input layer of DSLC classifier, which obtains the input features and produces the predicted label as the output. Here, the layer by layer processing is performed with m learners, j classes, m weights and weighted average probabilities. The DSLC is a kind of ensemble learning model that integrates the functions of five base learners including KNN, RF, LR, XGB, and randomized trees. For validation, the different types of performance measures are used to evaluate the results of the proposed method, which includes accuracy, sensitivity, specificity, F1-score, and efficiency. The obtained results reveal that the combination of proposed AMOA-DSLC technique provides superior results in terms of average accuracy 99% for all datasets used in this study. Due to the inclusion of AOMA, the overall effectiveness and intrusion categorization performance of the proposed model is highly improved in this framework. In future, we intend to expand our research to find other attacks that have taken place in real time

Table 5 Statistical analysis of AMOA technique.

Parameter	Value
p-value	0.886 00
z-value	0.143 83
Mean	−10.536 40
Standard deviation	3.89×10^{-11}

MANET environment.

References

[1] M. Prasad, S. Tripathi, and K. Dahal, A probability estimation-based feature reduction and Bayesian rough set approach for intrusion detection in mobile ad-hoc network, *Appl. Intell.*, vol. 53, no. 6, pp. 7169–7185, 2023.

[2] C. Edwin Singh and S. M. Celestin Vigila, Fuzzy based intrusion detection system in MANET, *Meas. Sens.*, vol. 26, p. 100578, 2023.

[3] M. Prasad, S. Tripathi, and K. Dahal, An enhanced detection system against routing attacks in mobile ad-hoc network, *Wirel. Netw.*, vol. 28, no. 4, pp. 1411–1428, 2022.

[4] T. K. Jebuer, An IDS based on modified chaos Elman's neural network approaches for securing mobile ad hoc networks against DDoS attack, *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 8, pp. 2759–2764, 2022.

[5] S. Ajjaj, S. El Houssaini, M. Hain, and M. A. El Houssaini, A new multivariate approach for real time detection of routing security attacks in VANETs, *Information*, vol. 13, no. 6, p. 282, 2022.

[6] M. Prasad, S. Tripathi, and K. Dahal, An intelligent intrusion detection and performance reliability evaluation mechanism in mobile ad-hoc networks, *Eng. Appl. Artif. Intell.*, vol. 119, p. 105760, 2023.

[7] L. Legashev and L. Grishina, Development of an intrusion detection system prototype in mobile ad hoc networks based on machine learning methods, in *Proc. 2022 Int. Russian Automation Conf.* (*RusAutoCon*), Sochi, Russian, 2022, pp. 171–175.

[8] M. Mayuranathan, S. K. Saravanan, B. Muthusenthil, and A. Samydurai, An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique, *Adv. Eng. Softw.*, vol. 173, p. 103236, 2022.

[9] S. Venkatasubramanian, A. Suhasini, and N. Lakshmi Kanthan, A sparrow search algorithm for detecting the cross-layer packet drop attack in mobile ad hoc network (MANET) environment, in *Computer Networks, Big Data and IoT*, A. P. Pandian, X. Fernando, and H. X. Wang, eds. Singapore: Springer, 2022.

[10] M. M. Rathore, A. Ahmad, and A. Paul, Real time intrusion detection system for ultra-high-speed big data environments, *J. Supercomput.*, vol. 72, no. 9, pp. 3489–3510, 2016.

[11] X. Zhang, L. Jiao, A. Paul, Y. Yuan, Z. Wei, and Q. Song, Semisupervised particle swarm optimization for classification, *Math. Probl. Eng.*, vol. 2014, pp. 1–11, 2014.

[12] M. M. Rathore, A. Paul, A. Ahmad, S. Rho, M. Imran, and M. Guizani, Hadoop based real-time intrusion detection for high-speed networks, in *Proc. 2016 IEEE Global Communications Conf.* (*GLOBECOM*), Washington, DC, USA, 2016, pp. 1–6.

[13] P. M. Manohar and D. V. Divakara Rao, Performance enhancement of DYMO routing protocol in MANETs using machine learning technique, in *Smart Intelligent Computing and Applications, Volume 1*, V. Bhateja, S. C. Satapathy, C. M. Travieso-Gonzalez, and T. Adilakshmi, eds. Singapore: Springer, 2022, pp. 463–470.

[14] S. Gbetondji Michoagan, S. M. Mali, and S. Gore, Salient features selection techniques for instruction detection in mobile ad hoc networks, *Teh. Glas*, no. Online, pp. 40–46, 2022.

[15] R. Rai, K. G. Dhal, A. Das, and S. Ray, An inclusive survey on marine predators algorithm: Variants and applications, *Arch. Comput. Methods Eng.*, vol. 30, no. 5, pp. 3133–3172, 2023.

[16] K. N. Venkata Ratna Kumar, R. Mahaveerakannan, C. M. Rao, P. N. Rao, and K. S. Rao, Intrusive detection of wormhole attack using cluster - based classification model in MANET, in *Proc. 2022 8th Int. Conf. Advanced Computing and Communication Systems* (*ICACCS*), Coimbatore, India, 2022, pp. 1869–1874.

[17] A. Ramkissoon and W. Goodridge, An ensemble based computational social system for fake news detection in MANET messaging, https://assets.researchsquare.com/files/rs-1208481/v1_covered.pdf?c=1643135268, 2022.

[18] P. Satyanarayana, V. Nihani V G, A. Joshua Daniel G, A. Kumar Raju D V, and H. Sai Abhinaya C, Design and implementation of trust based routing algorithm to enhance QoS for MANETs, in *Proc. 2022 Int. Conf. Wireless Communications Signal Processing and Networking* (*WiSPNET*), Chennai, India, 2022, pp. 64–68.

[19] A. Mughaid, S. AlZu'bi, A. Alnajjar, E. AbuElsoud, S. El Salhi, B. Igried, and L. Abualigah, Improved dropping attacks detecting system in 5g networks using machine learning and deep learning approaches, *Multimed. Tools Appl.*, vol. 82, no. 9, pp. 13973–13995, 2023.

[20] E. Gyamfi and A. Jurcut, Intrusion detection in Internet of Things systems: A review on design approaches leveraging multi-access edge computing, machine learning, and datasets, *Sensors*, vol. 22, no. 10, p. 3744, 2022.

[21] S. A. Asra, Security issues of vehicular ad hoc networks (VANET): A systematic review, *TIERS Inf. Technol. J.*, vol. 3, no. 1, pp. 17–27, 2022.

[22] S. Laqtib, K. El Yassini, and M. L. Hasnaoui, A technical review and comparative analysis of machine learning

techniques for intrusion detection systems in MANET, *Int. J. Electr. Comput. Eng. IJECE*, vol. 10, no. 3, p. 2701, 2020.

[23] Z. Ali Khan and P. Herrmann, Recent advancements in intrusion detection systems for the Internet of Things, *Secur. Commun. Netw.*, vol. 2019, pp. 1–19, 2019.

[24] H. Moudni, M. Er-rouidi, H. Mouncif, and B. El Hadadi, Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET, *Procedia Comput. Sci.*, vol. 151, no. C, pp. 1176–1181, 2019.

[25] U. Ali Zardari, J. He, N. Zhu, K. H. Mohammadani, M. S. Pathan, M. I. Hussain, and M. Q. Memon, A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs, *Future Internet*, vol. 11, no. 3, pp. 1–17, 2019.

[26] K. Rachid, R. Mohammed, and S. Omar, Intrusion detection system based M-best features selection in Manet, *Models & Optim. Math. Anal. J.*, vol. 10, no. 1, pp. 20–25.

[27] Z. Ali Abbood, D. C. Atilla, C. Aydin, and M. S. Mahmoud, A survey on intrusion detection system in ad hoc networks based on machine learning, in *Proc. 2021 Int. Conf. Modern Trends in Information and Communication Technology Industry* (*MTICTI*), Sana'a, Yemen, 2021, pp. 1–8.

[28] M. Prasad, S. Tripathi, and K. Dahal, Unsupervised feature selection and cluster center initialization based arbitrary shaped clusters for intrusion detection, *Comput. Secur.*, vol. 99, p. 102062, 2020.

[29] R. M. Hadi, S. H. Abdullah, and W. M. S. Abedi, Proposed neural intrusion detection system to detect denial of service attacks in MANETs, *Period. Eng. Nat. Sci. PEN*, vol. 10, no. 3, p. 70, 2022.

[30] R. Meddeb, F. Jemili, B. Triki, and O. Korbaa, A deep learning-based intrusion detection approach for mobile Ad-hoc network, *Soft Comput. A Fusion Found. Methodol. Appl.*, vol. 27, no. 14, pp. 9425–9439, 2023.

[31] S. Venkatasubramanian, Multistage optimized fuzzy based intrusion detection protocol for NIDS in MANET, https://ijirt.org/master/publishedpaper/IJIRT153276_PAPER.pdf, 2021.

[32] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, A review of intrusion detection systems using machine and deep learning in Internet of Things: Challenges, solutions and future directions, *Electronics*, vol. 9, no. 7, p. 1177, 2020.

[33] N. Venkateswaran and S. Prabaharan, An efficient neuro deep learning intrusion detection system for mobile adhoc networks, *ICST Trans. Scalable Inf. Syst*., p. 173781, 2018.

[34] A. Paul, Graph based M2M optimization in an IoT environment, in *Proc. 2013 Research in Adaptive and Convergent Systems*, Montreal, Canada, 2013, pp. 45–46.

[35] M. Ramezani, D. Bahmanyar, and N. Razmjooy, A new improved model of marine predator algorithm for optimization problems, *Arab. J. Sci. Eng.*, vol. 46, no. 9, pp. 8803–8826, 2021.

[36] D. S. A. Elminaam, A. Nabil, S. A. Ibraheem, and E. H. Houssein, An efficient marine predators algorithm for feature selection, *IEEE Access*, vol. 9, pp. 60136–60153, 2021.

[37] A. Faramarzi, M. Heidarinejad, S. Mirjalili, and A. H. Gandomi, Marine predators algorithm: A nature-inspired metaheuristic, *Expert Syst. Appl.*, vol. 152, p. 113377, 2020.

[38] DS2OS traffic traces, https://www.kaggle.com/datasets/francoisxa/ds2ostraffictraces.

[39] NSL-KDDNetwork Security, Information Security, Cyber Security. Available: https://www.kaggle.com/datasets/hassan06/nslkdd.

[40] UNSW-NB15 Network Intrusion Detection, https://www.kaggle.com/datasets/dhoogla/unswnb15.

[41] P. Kumar, G. P. Gupta, and R. Tripathi, Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for IoT networks, *Arab. J. Sci. Eng.*, vol. 46, no. 4, pp. 3749–3778, 2021.

[42] Y. Farhaoui, Design and implementation of an intrusion prevention system, *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 675–683, 2017.

[43] Editorial, *Big Data Mining and Analytics*, vol. 6, no. 3, pp. i-ii, 2023,doi: 10.26599/BDMA.2022.9020045.

[44] Y. Farhaoui, Intrusion prevention system inspired immune systems, *Indones. J. Electr. Eng. Comput. Sci.*, vol. 2, no. 1, p. 168, 2016.

[45] Y. Farhaoui, Big data analytics applied for control systems, in *Lecture Notes in Networks and Systems*. Cham, Switzerland: Springer, 2017, pp. 408–415.

[46] Editorial, *Big Data Mining and Analytics*, vol. 5, no. 4, pp. i-ii, 2022,doi: 10.26599/BDMA.2022.9020004.

[47] S. S. Alaoui, Y. Farhaoui, and B. Aksasse, Hate speech detection using text mining and machine learning, *Int. J. Decis. Support. Syst. Technol.*, vol. 14, no. 1, pp. 1–20, 2022.

[48] S. S. Alaoui, Y. Farhaoui, and B. Aksasse, Data openness for efficient e-governance in the age of big data, *Int. J. Cloud Comput.*, vol. 10, no. 5/6, p. 522, 2021.

[49] A. El Mouatasim and Y. Farhaoui, Nesterov step reduced gradient algorithm for convex programming problems, in *Big Data and Networks Technologies*, Y. Farhaoui, ed. Cham, Switzerland: Springer, 2019, pp. 140–148.

[50] S. Sossi Alaoui, Y. Farhaoui, and B. Aksasse, A comparative study of the four well-known classification

algorithms in data mining, in *Lecture Notes in Networks and Systems*, J. Kacprzyk, ed. Cham, Switzerland: Springer, 2017, pp. 362–373.

M. Sahaya Sheela is working as an assistant professor in Department of Electronics and Communication Engineering for Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology. She received the BE degree in electronics and communication engineering from Sethu Institute of Technology, and the ME degree in communication systems from the Anna University, Tamilnadu, India, in 2002 and 2010, respectively. She completed the PhD degree in the field of wireless sensor networks at Anna University, Chennai, India. She has published and presented several research articles in the reputed journals and conferences, respectively. Her research interests include wireless sensor networks, digital signal processing, antenna design, and communication systems.

A. Gnana Soundari is presently working as a professor in Department of Computer Science and Engineering, Saveetha School of Engineering, SIMATS. She received the Undergraduate bachelor degree in information technology from SRM Valliammai Engineering College (2004), Madras University, Chennai, and master degree in information technology from Sathyabama University (2007), Chennai, India. She has been awarded PhD degree in the field of computer science and engineering by Sathyabama University, Chennai, during 2020. Her area of interests includes wireless sensor networks, big data analytics, machine learning, IoT, mobile computing, data structures and algorithms, programming languages such as C, C++, Java, Python, information management, and distributed systems. She has published more than 30 research papers in reputed journals and conference proceedings. She is presently teaching a wide variety of courses at undergraduate level and has 18 years of teaching experience. She has guided more than 40 undergraduate student projects till date. She has a Life Membership from Indian Society for Technical Education (ISTE) and IEEE.

K. Suresh is working as an assistant professor in Department of Computer Science and Engineering, PSNA College of Engineering and Technology, Tamil Nadu, India. He has completed master of engineering computer science and engineering in M. Kumarasamy College of Engineering, Anna University, Chennai and bachelor of engineering in electrical and electronics engineering in Annai Mathammal Sheela engineering College, Anna University, Chennai.

[51] Y. Farhaoui, Securing a local area network by IDPS open source, *Procedia Comput. Sci.*, vol. 110, pp. 416–421, 2017.

Aditya Mudigonda is a specialist in construction management and information technology applications, is currently employed as an assistant professor at JNIAS School of Planning and Architecture. He is currently working on submitting the PhD thesis to University College of Engineering (Autonomous), Osmania University, which will focus on sustainable supply chain management, and integrate data mining and machine learning. He received both the BE degree in civil engineering and the ME degree, with a specialization of construction engineering and management, from the same organization. His area of interests in research includes value engineering, construction management, machine learning, data mining, and sustainable development. He has about 12 peer-reviewed articles in national and international journals and conferences. Due to his knowledge of construction management, he was connected to numerous private and governmental organizations, including the National Academy of Construction and the Engineering Staff College of India.

C. Kalpana is currently working as an assistant professor in Department of Computer Science and Engineering at NPR College of Engineering and Technology, Tamil Nadu, India. She is pursuing the PhD degree in information and communication engineering, Anna University, Chennai. She received the master degree of engineering in computer science and engineering at SBM College of Engineering and Technology, Anna University, Chennai, and the bachelor degree of engineering in computer science and engineering at Odaiyappa College of Engineering and Technology, Anna University, Chennai. Her research interest includes machine learning, deep learning, and cloud computing. She has published publications in international journals and conferences.

Yousef Farhaoui is a professor at Moulay Ismail University, Morocco, chair of IDMS Team, and director of STI Laboratory. He obtained the PhD degree in computer security from Ibn Zohr University of Science. His research interests include learning, e-learning, computer security, big data analytics, and business intelligence. He has three books in computer science. He is a coordinator and member of the organizing committee, and also a member of the scientific committee of several international congresses, and is a member of various international associations. He has authored 7 book and many book chapters with reputed publishers such as Springer and IGI. He is served as a reviewer for IEEE, IET, Springer, Inder science, and Elsevier journals. He is also the guest editor of many journals with Wiley, Springer, Inder Science, etc. He has been the general chair, session chair, and panelist in several conferences. He is a senior member of IEEE, IET, ACM, and EAI Research Group.

K. Somasundaram has about 25 years of experience in industry and teaching. He serves in various positions in industry and teaching. He is currently serving as a professor in Computer Science and Engineering Department at Sri Muthukumaran Institute of Technology, Mangadu, Chennai India. He has published about 95 papers in international journals, and presented 32 papers in referred national and international conferences. He is a Life Member of IE (India), IETE, CSI, ISTE, and C.Eng (IEI). His area of interests includes data mining and data analytics, wireless sensor networks, grid/cloud computing, and application of Internet of Things.