Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.039111
Article

New Denial of Service Attacks Detection Approach Using Hybridized Deep Neural Networks and Balanced Datasets

Ouail Mjahed[1,*], Salah El Hadaj[1], El Mahdi El Guarmah[1,2] and Soukaina Mjahed[1]

[1]L2IS, Department of Computer Sciences, Faculty of Sciences and Technology, Cadi Ayyad University, Marrakech, 40000, Morocco
[2]Mathematics and Informatics Department, Royal Air School, Marrakech, 40000, Morocco
*Corresponding Author: Ouail Mjahed. Email: mjahed.ouail97@gmail.com
Received: 10 January 2023; Accepted: 20 March 2023; Published: 26 May 2023

Abstract: Denial of Service (DoS/DDoS) intrusions are damaging cyber-attacks, and their identification is of great interest to the Intrusion Detection System (IDS). Existing IDS are mainly based on Machine Learning (ML) methods including Deep Neural Networks (DNN), but which are rarely hybridized with other techniques. The intrusion data used are generally imbalanced and contain multiple features. Thus, the proposed approach aims to use a DNN-based method to detect DoS/DDoS attacks using CICIDS2017, CSE-CICIDS2018 and CICDDoS 2019 datasets, according to the following key points. a) Three imbalanced CICIDS2017-2018-2019 datasets, including Benign and DoS/DDoS attack classes, are used. b) A new technique based on K-means is developed to obtain semi-balanced datasets. c) As a feature selection method, LDA (Linear Discriminant Analysis) performance measure is chosen. d) Four metaheuristic algorithms, counting Artificial Immune System (AIS), Firefly Algorithm (FA), Invasive Weeds Optimization (IWO) and Cuckoo Search (CS) are used, for the first time together, to increase the performance of the suggested DNN-based DoS attacks detection. The experimental results, based on semi-balanced training and test datasets, indicated that AIS, FA, IWO and CS-based DNNs can achieve promising results, even when cross-validated. AIS-DNN yields a tested accuracy of 99.97%, 99.98% and 99.99%, for the three considered datasets, respectively, outperforming performance established in several related works.

Keywords: Classification; neural networks; metaheuristic algorithm; intrusion detection system; DoS/DDoS

1 Introduction

With the growing diversity of cyber-attacks, research on intrusion detection has received extensive attention. Attack detection is a complex task that is closely linked to other requirements, such as selecting the best features and training on relevant data. The existing datasets are diverse, generally imbalanced, and cover many features and several attack classes. Recently, a wide range of intrusion

detection methods based on machine learning (ML) has been developed, demonstrating that neural networks (NNs) and deep neural networks (DNNs) are among the most efficient techniques. DNNs, with several models, are widely used in various branches of science and technology, where several optimizing techniques have been explored, including the use of metaheuristic (MH) algorithms. Some MH algorithms are applied to optimize DNNs for intrusion detection. While some MHs such as genetic algorithms (GA) and particle swarm optimization (PSO) have been commonly used, others like Artificial Immune System (AIS), Cuckoo Search (CS), Invasive Weed Optimization (IWO), and Firefly Algorithm (FA) have received less attention. Additionally, feature selection and dataset balancing have made various progress, also involving ML techniques. Different methods have been proposed to select a subset of relevant features, including techniques such as principal component analysis, recursive feature elimination and GA. Imbalanced datasets have also been addressed using oversampling techniques such as SMOTE (Synthetic Minority Over-sampling Technique), undersampling techniques such as edited nearest neighbors, and hybrid approaches.

The literature review concerning intrusion detection shows that although DNN-based methodologies are the most effective, few or no studies are focused on their hybridization with MH algorithms like AIS, CS, IWO, or FA. However, recent ML-based feature selection and data balancing techniques have proven to be effective, and some conventional methods, such as linear discriminant analysis (LDA) and K-Means, remain rigorous and deserve further exploration.

The main contribution of this work and its novelty concern the improvement of DNN-based DoS/DDoS attacks detection by using MH algorithms, according to the following key points.

a) Denial of Service (DoS/DDoS) attack classes from the CICIDS2017, CSE-CICIDS2018, and CIC-DDoS2019 datasets are used. To semi-equilibrate these imbalanced data, a new technique based on the K-Means algorithm is explored.
b) As a feature selection method, LDA performance measure such as F_1-score is employed.
c) First a DBPNN (Back-Propagation based DNN) is used to identify DoS/DDoS attacks. This DNN is then enhanced by four MH algorithms, the first time used together, such as AIS, FA, IWO, and CS.

In an evaluation step, hybrid DNN-based approaches will be validated on considered imbalanced datasets and compared to recent state-of-the-art results.

In the remainder of the paper, the following abbreviations are used, DBPNN (for BP-based DNN), MH-DNN (for MH-based DNN), AIS-DNN, FA-DNN, IWO-DNN, and CS-DNN for DNNs based on the four MHs.

The paper is organised as follows. Section 2 provides a summary of related work in the field of attack detection. In Section 3, the methods adopted (DBPNN, the four MH algorithms), the datasets and the performance measures used are succinctly presented. Section 4 is focused on implementing the proposed approach, which involves balancing datasets using K-Means, selecting features using LDA, and implementing both DBPNN and MH-DNN. The results of the experiment are also detailed. Section 5 is devoted to a cross-validation and a comparison between the state-of-the-art works and the proposed DoS/DDoS attack detection. Moreover, the obtained results are thoroughly discussed. The main conclusions are summarized in Section 6.

2 Related Works

ML methods have been frequently adopted in IDS design, as detection or features selection tools. In [1], a Random Forest Regressor is employed to choose the best features, exploited by several ML techniques, such as K-Nearest Neighbor (KNN), Random Forest (RF), Multi-Layer Perceptron (MLP), and Adaptive Boosting. The best accuracy value, extracted from a CICIDS2017 dataset, reached 0.98 with RF. Deep Learning (DL) methods, such as DNN, recurrent neural network (RNN), and deep reinforcement learning, have been developed [2,3]. The information gain (IG) method is used to select appropriate and weighty features and ML algorithms as RF and Random Tree are applied in an investigation of CICIDS2017 dataset [4]. Specifically, RF reaches the highest accuracy value of 99.86%. In [5], a modular deep neural network is performed on CSE-CICID 2018 dataset, reaching an accuracy value of 100%. Filho et al. [6] developed several ML methods, to detect DoS/DDoS attacks using several datasets, including CICIDS2017 and CSE-CICIDS2018. The precision attained is close to 100%. Hua [7] used lightGBM (light Gradient-Boosting Machine) algorithms to address the imbalanced problems in CICIDS2018 and to detect intrusions. The obtained accuracy reached the value of 98.37%.

In [8], a support value-based graph is used to classify intrusions from CICDDoS2019 dataset. Kareem et al. [9] used several ML techniques, trained with on CICIDS2017 and validated using the CICDDoS2019 dataset, showing a DDoS attacks detection accuracy of above 99.77%. In [10], DNN proposed the recognition of DoS/DDoS attacks, by using CICIDS2017 dataset, which reaches an accuracy of 98.72%. Haider et al. [11] suggested a deep convolutional neural network (CNN) based solution to detect DDoS attacks, trained on CICIDS2017 data, which achieves an accuracy of 99.45%. Wang et al. [12] suggested an information entropy and CNN method to identify DDoS attacks in Software-Defined Networking environment. The accuracy of the CNN approach is 98.98%. The model proposed in [13], based on long short-term memory attains an accuracy of 99.19% in detecting DoS/DDoS attacks on the reflection-based CICDDoS2019 dataset. In [14], by exploiting negative selection (NSA), an AIS algorithm, the accuracy in CICIDS2017 dataset is improved to a value of 97%. In [15], the Fisher Score, Support Vector Machine (SVM), KNN, and Decision Tree (DT) algorithms are suggested for features selection and classification tasks, to design a DoS-based IDS. With KNN, DT and SVM, this IDS reached 99.7%, 57.76%, and 99% success rates, respectively. Kanimozhi et al. [16] conducted research on detecting the botnet intrusions in the CSE-CICIDS2018 dataset through NN, achieving an accuracy of 99.97%. Ferrag et al. [17] show that the DL models, based on Naïve Bayes, NN, SVM, and RF and applied to CSE-CICIDS2018 dataset, achieved a 95% of detection rate. In [18], SVM, KNN, and DT performances are compared by using multiple datasets, including CSE-CICIDS2018 dataset, showing that the IDS-based accuracy ranged from 95% to 100%. A Data Dimensionality Reduction method based IDS has been proposed [19], where SVM, XGBoost (Extreme Gradient Boosting), and Neural network classifiers using 36 selected features were evaluated. The highest accuracy achieved on CICIDS2017 dataset was 98.93% with XGboost. A fusion of regularization techniques is applied in [20], for increasing a DNN-based IDS performance, by using several datasets, including CICIDS2017.

Apart from IDS, many optimizations of DNNs, as optimization of weights, network architecture, training factors and algorithm, have been developed using MH algorithms, like PSO [21], GA [22], Differential Evolution [23], Ant Colony Optimization [24], Chimp Optimization Algorithm [25–27], Grey Wolf Optimization (GWO) [28], Artificial Bee Colony (ABC) [29], Whale Optimization Algorithm [30], FA [31]. On the other hand, in IDS framework, several MH algorithms have been used, such as PSO [32], FA [33], AIS [14] and GA [34]. A hybrid classification model based on ABC and artificial fish swarm algorithm is developed, attaining a detection accuracy of 99% [35]. In [36], a model

based on GA is proposed to address feature selection and attacks detection using the CICIDS2017 dataset, achieving an F_1-score of 91%. In [37], the GWO and Moth-Flame Optimizer algorithms are combined to improve attacks detection accuracy in CICIDS2017 to 99.2%. In [38], PSO, GWO, FA and GA are used to optimize the feature selection.

Based on this succinct state-of-the-art overview, it is evident that in the IDS framework, MH algorithms are certainly used, but rarely hybridized and exploited in a context of DNN optimization. Moreover, some MHs, such as AIS, CS, IWO or FA are little or not dealt with. Thus, the main contribution and novelty of this work can be specified as follows:

- improving detection of DoS/DDoS attacks using DNNs hybridized by four MHs (like AIS, FA, IWO, and CS), and
- balancing the considered datasets by a new K-means-based technique.

3 Datasets and Methods Used

This subsection provides an overview of the CICIDS2017, CSE-CICIDS2018, and CICDDoS2019 datasets used, as well as the methods and evaluation metrics employed in this work.

3.1 Datasets

CICIDS2017 was generated by the Canadian Institute for Cyber-security (CIC) [39]. This dataset consists of 15 imbalanced traffic classes (one normal class and 14 attack traffic categories), where classes are present with an abundant number of occurrences and classes have few instances. In the proposed research, only a reduced amount of the DoS/DDoS attacks in CICIDS2017 dataset is considered (Dataset 1), whose distribution after cleaning is depicted in Table 1.

Table 1: Characteristics of the used imbalanced datasets

		Dataset 1: CICIDS2017	Dataset 2: CSE-ICIDS2018	Dataset 3: CICDDoS2019
Class	Class label [39]	N_{Ci}	N_{Ci}	N_{Ci}
C_1	Benign	100000	100000	5200
C_2	DDoS	12800	12000	100000
C_3	DoS hulk	23000	13200	–
C_4	DoS goldenEye	1000	4015	–
C_5	DoS slowloris	570	980	–
C_6	DoS slowhttptest	530	4	–
All C_i		137900	130199	105200

CSE-CICIDS2018 dataset was produced through a collaboration between the Communications Security Establishment (CSE) and the CIC [40]. This dataset, identical to the CICIDS2017, includes 13 different attack scenarios. As the CSE-CICIDS2018 dataset is too large, only a small set is used, with class distribution (Dataset 2), after cleaning, given in Table 1.

CICDDoS2019 dataset is provided by the CIC and the University of New Brunswick [41]. This huge dataset comprises benign and some 12 different kinds of DDoS attacks. Simply a reduced lot of the cleaned instances from this dataset are considered for this work (Dataset 3), as presented in Table 1.

Notice that, Datasets 1-2 contain six attack classes (Benign, DDoS, DoS Hulk, DoS GoldenEye, DoS Slowloris, and DoS SlowHTTPtest), while Dataset 3 consists of two classes (Benign, DDoS). These three datasets contain imbalanced attack classes.

3.2 Methods

The objective of this work consists first in the use of a Deep Back-propagation based DNN (DBPNN), then a hybridization of DNN by four MH algorithms (CS, IWO, FA, AIS).

3.2.1 DBPNN

A DBPNN is a neural network whose architecture contains multiple hidden layers, one input layer, and one output layer. Each neuron i in a layer l produces a response $Y_i^{(l)}$, as given in Eq. (1).

$$Y_i^{(l)} = s\left(\sum_{j=1}^{N^{(l-1)}} W_{ij}^{(l)} Y_j^{(l-1)} - \theta_i^{(l)}\right) \tag{1}$$

where $\theta_i^{(l)}$ and $W_{ij}^{(l)}$ are the threshold of the neuron i in layer l and its connection weight with neurons j (in layer l-1), $N^{(l-1)}$ the number of neurons in the layer l-1 and s an activation function. Through a supervised training, using the BP algorithm, the quadratic error existing between the actual outputs o_i of the network and the desired outputs r_i is minimized Eq. (2) [42,43].

$$E = \sum_i (o_i - r_i)^2 \tag{2}$$

DNN hybridization concerns the optimization of the connection weights and the thresholds of the neurons, thanks to the four MHs proposed.

3.2.2 Metaheuristic Algorithms Used

AIS is a computational intelligence method that imitates the immune system to solve optimization problems. In AIS, potential solutions to a problem are treated as antigens, and the algorithm uses various mechanisms inspired by the immune system, such as clonal selection and immune memory, to select and evolve the best solutions, as explained in AIS Diagram (Fig. 1) [44].

FA is motivated by the behavior of fireflies. Three rules are used to build FA: fireflies are unisex; the intensity of a firefly is computed by a fitness function; attraction is relative to brilliance but falls with distance [45]. The main FA steps are summarized in FA Flowchart (Fig. 1).

IWO takes its principle from the natural behavior of invasive plants. IWO uses a set of rules inspired by the growth and reproduction of invasive plants to select and evolve the best solutions, where several aspects are considered like cloning, spatial scattering, and spatial exclusion [46].

The CS algorithm is stimulated by the life of a cuckoo bird and its specific reproduction and egg-laying. In CS, a population of solutions (i.e., cuckoo eggs) is generated, and a combination of local search and random walk methods is used to inspect the exploration space and find the best solutions. Details of this algorithm are described in [47]. The flowcharts of the IWO and CS algorithms are shown in Fig. 1.

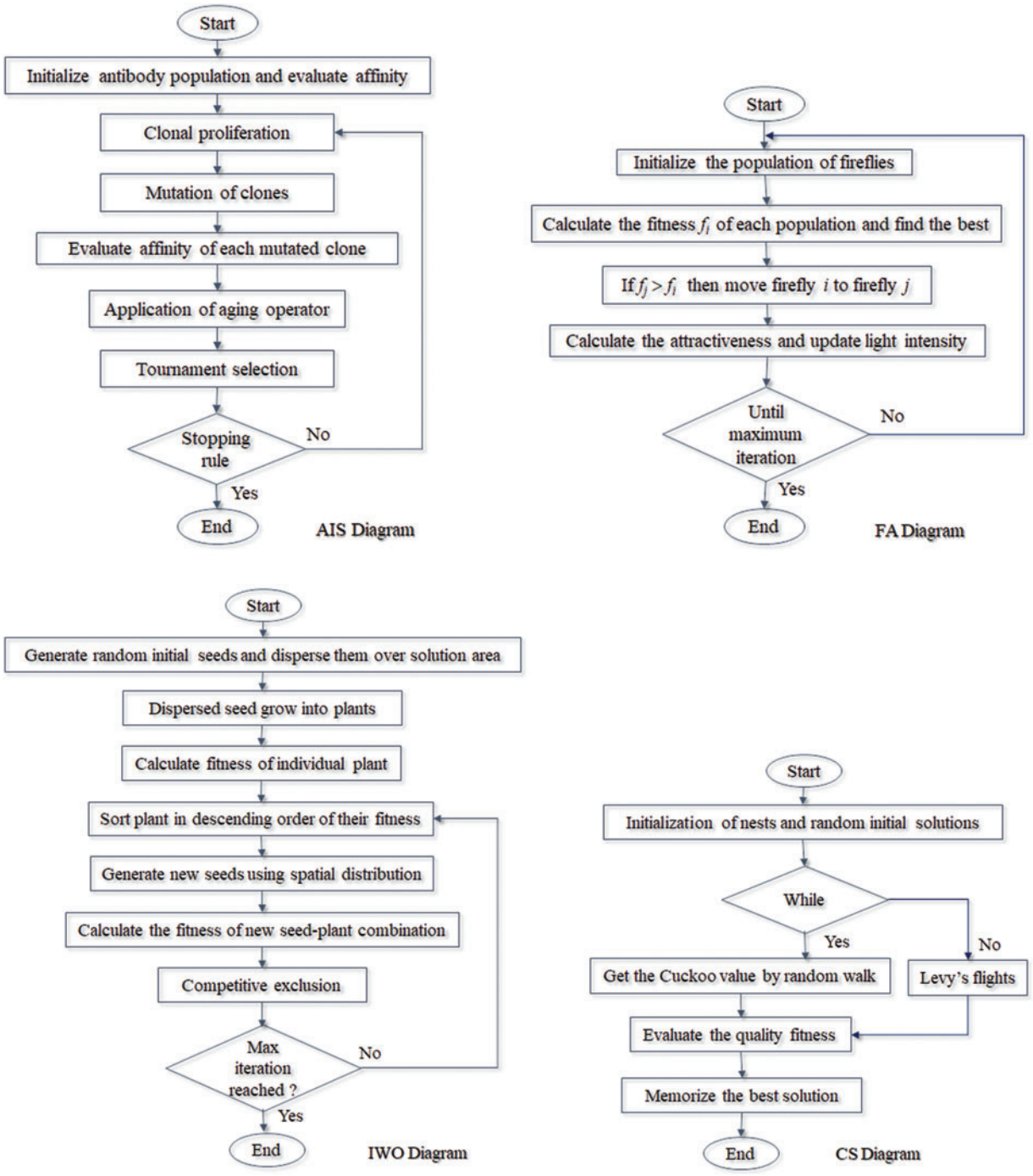

Figure 1: AIS, FA, IWO and CS flowcharts

3.3 Evaluation Metrics

To estimate the DNN-based DoS/DDoS attacks detection, precision rate β_i, sensitivity rate γ_i, and F_{1i} -score are computed, for each class C_i, according to Eq. (3).

$$\beta_i = \frac{A_{ii}}{N_i}, \quad \gamma_i = \frac{A_{ii}}{\sum_j A_{ji}}, \quad F_{1i} = \frac{2\beta_i\gamma_i}{\beta_i + \gamma_i} \tag{3}$$

where A_{ij} denotes the number of instances of *class* C_i categorized as *class* C_j and N_i is the size for class C_i. Thus, the global rates as accuracy β, the global sensitivity (γ), and the global F_1-score, become as specified in Eq. (4).

$$\beta = \frac{\sum_i N_i\beta_i}{\sum_i N_i}, \quad \gamma = \frac{\sum_i N_i\gamma_i}{\sum_i N_i}, \quad F_1 = \frac{\sum_i N_i F_{1i}}{\sum_i N_i} \tag{4}$$

4 Implementation of the Proposed Approach

As earlier presented, this work aims to improve the detection of DoS/DDoS attack families in CICIDS2017, CSE-CICIDS2018 and CICDDoS 2019 datasets, by using DNN and hybridized DNN. To achieve this, the work is carried out in three main steps.

i) Data extracted from CICIDS2017, CSE-CICIDS2018 and CICDDoS2019 are first considered with almost the same initial proportions. This dataset is then semi-balanced using the K-means technique.
ii) To select the best features, F_1-score extracted from LDA is adopted.
iii) For the detection of intrusions, DNN and four hybrid DNNs using AIS, FA, IWO and CS algorithms are performed.

The step-by-step process of the suggested approach will be elaborated on in the following subsections.

Notice that, the various analyses achieved in this work have been developed under the Matlab environment, R2017b, with an Intel Core i7 3.0 GHz processor, 16 GB of RAM.

4.1 Balancing Dataset with K-Means

In order to improve the performance of the suggested approach in detecting attacks with few records, the number of instances for the few attacks is balanced. There are several techniques for balancing data, such as SMOTE [48]. The approach adopted in this work, to semi-balance datasets, consists in randomly generating new instances for the less frequent classes (such as DoS/DDoS attack classes in CICIDS2017 and CSE-CICIDS2018 datasets and Benign class in CICDDoS2019 dataset). Validation of these generated instances uses the K-Means method as described in Algorithm 1.

In the K-means clustering algorithm, instances are assigned to the closest among the K clusters by updating the clusters centers iteratively. Thus, using Algorithm 1, less frequent classes were semi-balanced with the proportions given in Table 2. For example, DDoS attacks are enhanced from 12800 examples in Dataset 1 to 20000 in Dataset 4, DoS Slowloris intrusions are improved from 980 in Dataset 2 to 3000 instances in Dataset 4 and Benign cases increase from 5200 (Dataset 3) to 20000 (Dataset 6). In addition, the DDoS subclasses in Datasets 3 and 6 are present with almost the same proportions, without attempting to distinguish between them. Note that, the proposed approach is trained, tested on semi-balanced Datasets 4-6 and cross-validated on imbalanced Datasets 1-3.

Algorithm 1: New K-Means-based dataset balancing

Input: Training lot of Datasets 1, 2, and 3.
Output: Datasets 4, 5, and 6, respectively.
K = 6 for Datasets 1-2, K=2 for Dataset 3
1: For each training dataset, execution of the K-Means algorithm, where at the end each intrusion is assigned to the nearest cluster.
2: Generation of a new instance and assigning it to the nearest cluster. If the cluster is the correct class (DoS/DDoS for Datasets 1 and 2 and Benign for dataset 3), then the generated sample is accepted and added to the dataset.
3: Generation of new instances stops when the desired number of instances per class is reached.

Table 2: Characteristics of the used semi-balanced datasets

Class	Dataset 4: CICIDS2017			Dataset 5: CSE-CICIDS2018			Dataset 6: CICDDoS2019		
	N_{Ci}	Train	Test	N_{Ci}	Train	Test	N_{Ci}	Train	Test
C_1	100000	70000	30000	100000	70000	30000	20000	14000	6000
C_2	20000	14000	6000	20000	14000	6000	100000	70000	30000
C_3	25000	17500	7500	20000	14000	6000	–	–	–
C_4	5000	3500	1500	6000	4200	1800	–	–	–
C_5	2000	1400	600	3000	2100	900	–	–	–
C_6	2000	1400	600	1000	700	300	–	–	–
All C_i	154000	107800	46200	150000	105000	45000	120000	84000	36000

4.2 Features Selection

In this work, to select the best features, F_1-score extracted from Linear Discriminant Analysis (LDA) is explored. In LDA, the discriminant function (DF) h_1, in the simple 2-class case (C_i and C_j), is computed, using the training set, as given in Eq. (5) [42,49].

$$h_1 = \left(g_i - g_j\right)^t \; V^{-1} \tag{5}$$

where g_i and g_j are class centroids and V is the covariance matrix. An intrusion instance x_0 is classified as C_i or C_j, according to $h_1(x_0)$, as proposed in System (6).

$$\begin{cases} if\ h_1\left(x_0\right) \geq 0\ then\ x_0 \in C_i \\ else\ x_0 \in C_j \end{cases} \tag{6}$$

Datasets 4 and 5 have the same 79 features (including the class label), while Dataset 6 contains 80 features. For each training lot of the datasets, a univariate LDA was developed, allowing to calculation of the DFs by considering one variable x_i at a time and a pair of classes at a time as well. A confusion matrix for each DF (and for each feature) is established, allowing us to deduce of the F_1-score value (F_{1i}). Thus, considering all classes, each feature x_i has an average value F_{1mi}. By ordering in decreasing order these F_{1mi}, the best features are deduced. Accordingly, by using the semi-balanced CICIDS2017 dataset (Dataset 4), the 78 features are ranked by decreasing value of F_{1mi}. Table 3 lists the 24 best features of Dataset 4. The application of the same process for Datasets 5 and 6 (corresponding to semi-balanced CSE-CICIDS2018 and CICDDoS2019 datasets), provides the results illustrated in Table 3,

where 24 features are selected for each dataset. The relevance of the selected features will be addressed during the DNN optimization presented in the next section.

Table 3: The selected features for semi-balanced datasets

Semi-balanced CICIDS2017 dataset (Dataset 4)												
Rank	1	2	3	4	5	6	7	8	9	10	11	12
Feature ID [39]	41	13	65	66	63	42	40	12	18	39	67	52
Rank	13	14	15	16	17	18	19	20	21	22	23	24
Feature ID [39]	54	14	20	8	55	22	9	25	26	24	21	36
Semi-balanced CSE-CICIDS2018 dataset (Dataset 5)												
Rank	1	2	3	4	5	6	7	8	9	10	11	12
Feature ID [40]	63	12	65	41	66	13	18	52	40	42	39	67
Rank	13	14	15	16	17	18	19	20	21	22	23	24
Feature ID [40]	14	20	54	9	25	8	55	26	36	21	36	24
Semi-balanced CICDDoS2019 dataset (Dataset 6)												
Rank	1	2	3	4	5	6	7	8	9	10	11	12
Feature ID [41]	12	13	52	63	41	66	18	42	40	54	65	67
Rank	13	14	15	16	17	18	19	20	21	22	23	24
Feature ID [41]	39	8	14	20	36	21	22	9	25	55	24	26

4.3 DBPNN and MH-DNN Based DoS\DDos Attacks Detection

To identify DoS/DDoS intrusions belonging to six classes (Benign, DDoS, DoS Hulk, DoS GoldenEye, DoS Slowloris and DoS SlowHTTP Test) or two classes (Benign, DDoS), the three semi-balanced training datasets, grouped in Table 2 (Dataset 4-6) will be used to optimize DBPNN. Four MH-DNNs denoted AIS-DNN, FA-DNN, IWO-DNN and CS-DNN) are then designed, according to the procedure described in Algorithm 2, while respecting the tuning parameters summarised in Table 4. It is worth highlighting that DNN involves not only the use of multiple hidden layers but also a thorough exploration to achieve the best possible outcomes.

Algorithm 2: DBPNN and MH-DNN Implementation

Input: {Training Dataset 4-6 as appropriate, A DNN Architecture}.

Output: {Optimized DNN with weights and thresholds, Performances metrics}.

1: For the DBPNN case, update weights and thresholds using the BP algorithm, with the training dataset.
2: Return the DBPNN weights, threshold and DBPNN training and test performances (precision, sensitivity, F_1-score and accuracy).
3: For the MH-DNN (AIS-DNN, FA-DNN, IWO-DNN, or CS-DNN), improve thresholds and weights based on the corresponding MH procedure.
4: Return the MH-DNN weights and thresholds, training and test performances (precision, sensitivity, F_1-score and accuracy).

Table 4: Algorithms parameters tuning

Algorithm	*Parameters tuning*
All	Number of features = 24, Population size = 10–100, Number of runs = 50, Max number of iterations = 1000
AIS	Antibodies selected for cloning = 50, Multiplication factor = 3, Threshold = 10
FA	Attractiveness = 0.2, Step factor = 0.2, Light absorption coefficient = 1
IWO	Seeds = 0–20, Variance exponent = 5
CS	Abandon probability = 0.25, Lévy flights settings = 0.1 and 1.5

It should be noted that the DNN model consists of one input layer including 24 neurons, corresponding to 24 selected features in Table 3. The input layer is followed by several hidden layers, whose exact number and sizes are to be determined. The output layer consists of 6 neurons (for Datasets 4 and 5) or 2 neurons for Dataset 6, where each neuron is dedicated to a class C_i. During the DNN training phase, the desired response r_i of the i^{th} output neuron, for each instance x, is as defined in Eq. (7).

$$\begin{cases} r_i(x) = 1 \, for \, x \in C_i \\ r_i(x) = -1 \, for \, x \notin C_i \end{cases} \tag{7}$$

For every intrusion instance x_0, a decision rule is proposed, based on the output o_i of the ith neuron, as specified in System (8).

$$\begin{cases} if \; o_i(x_0) \geq 0 \; then \; x_0 \in C_i \\ else \; x_0 \notin C_i \end{cases} \tag{8}$$

In the search for the best DNN, all architectures with 1 to 6 hidden layers, enclosing between 10 and 100 neurons each, are considered. During DBPNN training, the NN weights and thresholds are computed using the BP principle. To optimize an MH-DNN (AIS-DNN, FA-DNN, IWO-DNN, and CS-DNN), the weights and thresholds are adjusted using the respective MH algorithm, to maximize the accuracy β, the sensitivity γ and F_1-score. This led to considering the fitness function f given in Eq. (9).

$$f = 1 - F_1 \tag{9}$$

Moreover, experiments were conducted with iteration counts ranging from 10 to 1000, and populations varying from 10 to 100 individuals. To find the best architecture for the DNN, various factors are taken into account, including the ideal number of features, the optimal quantity of hidden layers and neurons in each layer, and the most suitable neural parameters (neuron weights and thresholds). In the framework of hybridization by one of the chosen algorithms, the MH-DNN architecture also depends on the tuning parameters. The Accuracy-Number of Neurons reliance summary is displayed in Fig. 2, where accuracy rates are plotted as a function of the number of neurons per layer for DBPNN, AIS-DNN, FA-DNN, IWO-DNN, and CS-DNN.

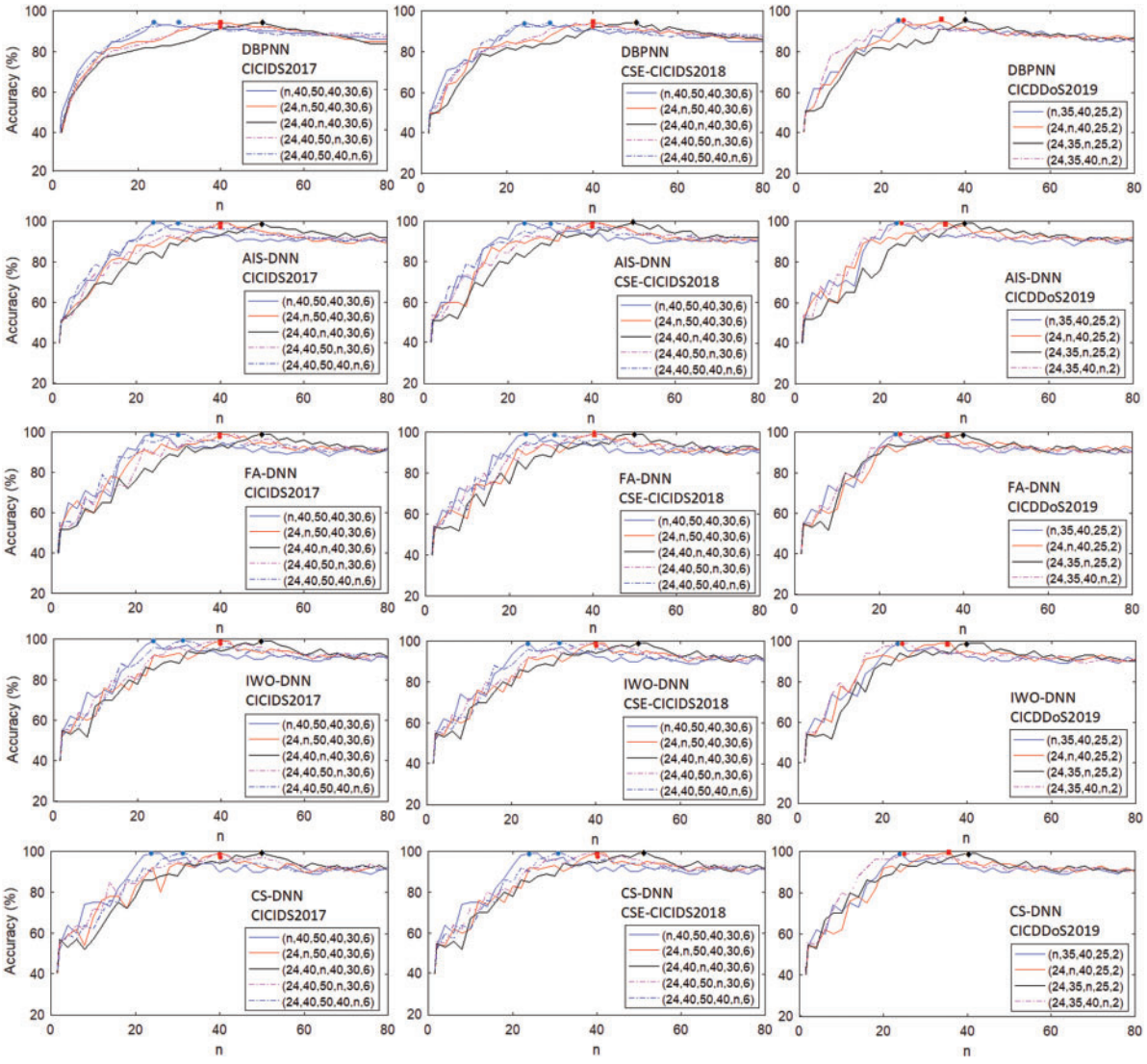

Figure 2: DoS/DDoS attack detection accuracy *vs*. the number of neurons n by layer ($4 \leq n \leq 80$)

The number of features needed for accurate detection of DoS/DDoS attacks is the first aspect to be considered. All the results shown in Fig. 2 demonstrate the relevance of the 24 features selected for the three datasets, regardless of the DNN used. The best results obtained, favor DNNs with four hidden layers (for Datasets 4 and 5) and three hidden layers (for Dataset 6). The best architectures are (24, 40, 50, 40, 30, 6) for Datasets 4-5 and (24, 35, 40, 25, 2) for Dataset 6.

Fig. 3 shows the maximum accuracies obtained for different values of population size for architectures (24, 40, 50, 40, 30, 6) and (24, 35, 40, 25, 2), adopted for the Datasets 4-5 and Dataset 6, respectively. On average, populations of 40 to 50 individuals provide the best results.

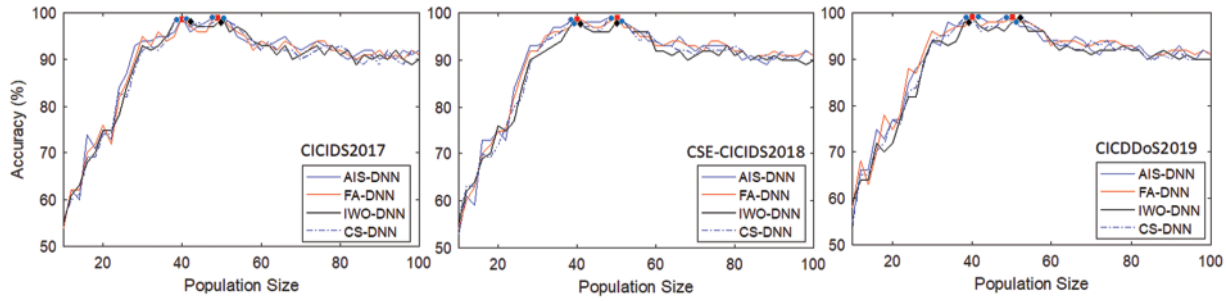

Figure 3: DoS/DDoS attack detection accuracy *vs*. population size for MH-DNN approaches

To prevent overfitting issues of each DNN architecture, the dropout regularization technique was applied. With dropout, the DNNs models are trained with a rate of 0.3 of randomly selected neurons "dropped out" during each iteration of training. The results demonstrated that adding dropout significantly improved the overall detection accuracy, reducing overfitting and increasing the model's generalization ability. The use of dropout in the DBPNN and MH-DNN approaches led to higher precision and sensitivity rates, compared to the non-dropout approaches. Specifically, the study reported an improvement of 2–3% in terms of detection accuracy using dropout.

On the other hand, to circumvent potential distortion caused by the random initialization of the MH algorithms, the hybrid DNNs are executed 50 times. The results obtained from the 50 runs, using the four MH-DNN for both training and testing semi-balanced Datasets 4-6, are shown in Table 5, where performance was evaluated using accuracy (β) and F_1-score. The best-tested accuracy (in %) obtained by DBPNN, AIS-DNN, FA-DNN, IWO-DNN and CS-DNN, can be summarized in the same respective order, as follows.

- Dataset 4: 96.65, 99.97, 99.60, 99.09, and 99.56. - Dataset 5: 96.63, 99.98, 99.63, 99.08, and 99.32.
- Dataset 6: 96.66, 99.99, 99.69, 99.11, and 99.43.

The best tested F_1 values are (in %), for DBPNN, AIS-DNN, FA-DNN, IWO-DNN and CS-DNN, as follows:

- Dataset 4: 96.18, 99.98, 99.60, 99.48, and 99.44. - Dataset 5: 96.73, 99.97, 99.63, 99.25, and 99.41.
- Dataset 6: 96.72, 99.99, 99.72, 99.51, and 99.58.

The above results prove that AIS-DNN is the best solution. The details on the distribution of AIS-DNN performance rates against the 6 (or 2) classes of DoS/DDoS attacks, given in Table 6, for the test datasets, show excellent performance. Precisions and F_1 values vary, for all classes, between 99.37% and 99.99%.

5 Validation of the Proposed Methodology

In this section, the results obtained thanks to semi-balanced Datasets 4-6 are cross-validated on imbalanced datasets (Datasets 1-3). In addition, comparisons regarding the suggested approaches and state-of-the-art works are exposed. Furthermore, the overall results are discussed.

Table 5: Training and test DoS/DDoS attacks detection performance based on semi-balanced datasets

Method	Training performance					
	CICIDS2017 Dataset 4		CICIDS2018 Dataset 5		CICDDoS2019 Dataset 6	
	Best DNN Architecture		Best DNN Architecture		Best DNN Architecture	
	(24, 40, 50, 40, 30, 6)		(24, 40, 50, 40, 30, 6)		(24, 35, 40, 25, 2)	
	β (%)	F_1 (%)	β (%)	F_1 (%)	β (%)	F_1 (%)
DBPNN	95.56 ± 1.11	95.21 ± 0.97	95.71 ± 0.99	95.73 ± 1.03	95.38 ± 0.98	95.43 ± 1.09
AIS-DNN	99.07 ± 0.89	99.04 ± 0.94	98.97 ± 1.01	98.97 ± 0.98	98.98 ± 1.02	99.02 ± 0.97
FA-DNN	98.53 ± 1.07	98.92 ± 1.01	98.71 ± 0.99	98.41 ± 1.03	98.61 ± 0.99	98.32 ± 1.07
IWO-DNN	98.25 ± 0.95	98.34 ± 0.97	98.13 ± 0.98	97.87 ± 1.04	98.03 ± 0.98	98.42 ± 1.09
CS-DNN	98.65 ± 1.09	98.61 ± 1.01	98.36 ± 0.99	98.41 ± 1.05	98.24 ± 0.99	98.51 ± 1.08
Method	Test performance					
	CICIDS2017 Dataset 4		CICIDS2018 Dataset 5		CICDDoS2019 Dataset 6	
	β (%)	F_1 (%)	β (%)	F_1 (%)	β (%)	F_1 (%)
DBPNN	95.61 ± 1.04	95.21 ± 0.97	95.65 ± 0.98	95.71 ± 1.02	95.65 ± 1.01	95.63 ± 1.09
AIS-DNN	99.04 ± 0.93	99.02 ± 0.96	98.95 ± 1.03	98.96 ± 1.01	98.96 ± 1.03	99.01 ± 0.98
FA-DNN	98.49 ± 1.11	98.59 ± 1.01	98.67 ± 0.96	98.61 ± 1.02	98.80 ± 0.89	98.71 ± 1.01
IWO-DNN	98.11 ± 0.98	98.52 ± 0.96	98.11 ± 0.97	98.31 ± 0.94	98.13 ± 0.98	98.45 ± 1.06
CS-DNN	98.53 ± 1.03	98.42 ± 1.02	98.31 ± 1.01	98.38 ± 1.03	98.44 ± 0.99	98.53 ± 1.05

Table 6: Test detection rates by attack class for semi-balanced datasets by using AIS-DNN

Attack class	CICIDS2017 Dataset 4		CICIDS2018 Dataset 5		CICDDoS2019 Dataset 6	
	β (%)	F_1 (%)	β (%)	F_1 (%)	β (%)	F_1 (%)
C_1	99.02 ± 0.95	99.10 ± 0.89	99.10 ± 0.89	99.10 ± 0.89	99.10 ± 0.89	99.10 ± 0.89
C_2	99.01 ± 0.96	99.04 ± 0.94	98.93 ± 1.01	98.99 ± 0.97	98.97 ± 1.02	99.01 ± 0.98
C_3	98.69 ± 1.07	98.74 ± 1.06	98.52 ± 0.99	98.35 ± 1.03	–	–
C_4	98.96 ± 1.01	99.06 ± 0.89	99.08 ± 0.89	99.10 ± 0.89	–	–
C_5	98.67 ± 0.91	98.54 ± 0.97	98.53 ± 0.98	98.63 ± 1.04	–	–
C_6	98.76 ± 1.09	98.42 ± 1.01	98.44 ± 0.99	98.35 ± 1.02	–	–

5.1 Cross-Validation

As suggested previously, MH-DNN approaches are evaluated by applying the obtained neural networks to the imbalanced data (Datasets 1-3). The best results are collected in Table 7, showing excellent detection rates for AIS-DNN, FA-DNN and CS-DNN.

Table 7: Best cross-validation performance achieved on imbalanced datasets

Method	CICIDS2017 Dataset 1			CICIDS2018 Dataset 2			CICDDoS2019 Dataset 3		
	β (%)	γ (%)	F_1 (%)	β (%)	γ (%)	F_1 (%)	β (%)	γ (%)	F_1 (%)
DBPNN	96.81	96.73	96.78	96.75	96.79	96.77	97.02	97.00	97.01
AIS-DNN	99.93	99.90	99.92	99.92	99.93	99.93	99.98	99.97	99.97
FA-DNN	99.79	99.67	99.73	99.69	99.71	99.70	99.74	99.78	99.76
IWO-DNN	99.13	99.21	99.25	99.11	99.23	99.16	99.41	99.30	99.35
CS-DNN	99.82	99.83	99.82	99.79	99.86	99.80	99.76	99.86	99.90

5.2 Comparison with State-of-the-art Works

The performances of the suggested approaches and some related published works are presented in Table 8. The proven results show that the three algorithms AIS-DNN, FA-DNN and CS-DNN are very effective in the task of detecting DoS/DDoS attack classes. Additionally, the AIS-DNN algorithm provides improved performance over state-of-the-art studies regarding accuracy (β) and F_1 -score.

Table 8: Comparison with state-of-the-art works on CICIDS2017-2018 and CICDDoS2019 Datasets

Dataset	Work	Method	β (%)	γ (%)	F_1 (%)
CICIDS2017	[14]	NSA	–	97.00	97.00
	[4]	IG + RF	99.79	99.90	99.90
	[50]	RF	99.92	99.92	99.91
	[51]	MLP	99.10	99.79	99.11
	Proposed approach	**AIS-DNN**	**99.97**	**99.99**	**99.98**
		FA-DNN	99.60	99.61	99.60
		CS-DNN	99.56	99.51	99.43
CSE-CICIDS2018	[52]	DL	95.00	–	–
	[53]	HCRNN	97.75	–	–
	[54]	CNN	98.31	–	–
	[50]	RF	99.04	99.04	98.83
	Proposed approach	**AIS-DNN**	**99.98**	**99.97**	**99.97**
		FA-DNN	99.63	99.63	99.63
		CS-DNN	99.34	99.37	99.41
CIC-DDoS2019	[55]	RNN-Encoder	99.00	–	99.00
	[56]	MLP	99.98	99.89	99.93
	[57]	DNN	94.21	94.03	94.12
	Proposed approach	**AIS-DNN**	**99.99**	**99.99**	**99.99**
		FA-DNN	99.69	99.76	99.72
		CS-DNN	99.43	99.72	99.58

5.3 Discussion

The performance of MH-DNN in detecting DoS/DDoS attacks, as presented in Tables 5 and 6, for the training and test used datasets, is significantly improved. This improvement is due to the optimal DNN design, through selecting the best features and optimizing the network architecture, as shown in Fig. 2. Further investigations regarding MH-DNN, including population size and the number of iterations, prove that, presumably, average populations of 40 to 50 individuals (Fig. 3) and a number of iterations around 1000 give the best results. AIS-DNN achieves tested accuracy of 99.97%, 99.98% and 99.99% and F_1 values of 99.98%, 99.97% and 99.99% for Datasets 4-6, respectively. Generally, the proposed approaches show better performance for Dataset 6, explained by the fact that this dataset is composed of only two classes (benign and DDoS attacks).

The evaluation of imbalanced datasets (Datasets 1-3), illustrated in Table 7, shows the effectiveness of MH-DNN approaches. The test accuracy of AIS-DNN approach is excellent, reaching a value of 99.93%, 99.92%, and 99.98% for the three imbalanced datasets, while test F_1 amounts to 99.92%, 99.93%, and 99.97%, respectively. In addition, the cross-validation of the proposed approaches on imbalanced datasets shows that there is no break between the imbalanced and semi-balanced results. This comforts the choice of K-means as a validating technique for the generated instances.

Regarding the comparison with the state-of-the-art works, Table 8 shows that the results obtained by the proposed approach, especially AIS-DNN, generally exceed those obtained in the recent works, and this for the datasets CICIDS2017 [4,14,49,50], CSE-CICIDS2018 [49,51–53] and CICDDoS2019 [54–56].

The training times, reached with MH-DNN using architecture (24, 40, 50, 40, 30, 6), with 1000 iterations, for Dataset 4, are collected in Table 9, showing with previous results that the AIS-DNN approach offers the best performance-computational cost. Training a DoS/DDoS attack detection algorithm requires a lot of computation time, because for a DNN optimization need, the number of iterations, the size of the DNN, and the parameters of the MHs, must be adapted to achieve the expected performance. For an architecture of (24, 40, 50, 40, 30, 6), and as illustrated in Table 9, AIS-DNN requires more than 551 s for its optimization, but its execution takes very little time and gives near real-time results. Detections by AIS-DNN, for example, are instant and do not need a powerful CPU or a large memory.

Table 9: Average training times in seconds for all DNNs approaches using architecture (24, 40, 50, 40, 30, 6) with 1000 iterations for Dataset 4

Method	DBPNN	AIS-DNN	FA-DNN	IWO-DNN	CS-DNN
CPU time (s)	254.14	551.15	532.75	579.77	541.19

Overall, considering their hybridization with DNNs, AIS, FA and CS algorithms are relatively simple to implement and have shown promising results when hybridized with DNNs. CS has the advantage of good convergence speed, while AIS and FA have the benefit of effectively handling multiple optima. IWO has potential and could be worth exploring further in other contexts.

6 Conclusion

The purpose of this paper is to improve DNN-based DoS/DDoS attacks detection on CICIDS 2017, 2018, CICDDoS2019 Datasets, by using four MH algorithms.

First, reduced datasets, extracted from the CICIDS2017-2018 and CICDDoS2019 datasets, were cleaned and balanced based on the K-means technique. The initial features are then reduced to 24 features only, as a ranking result of F_1 score extracted using a univariate LDA analysis.

New hybridizations of DNN are suggested and applied for the first time in the IDS research. MH-DNN has greatly improved the detection of DoS/DDoS attacks, in the three considered semi-balanced datasets. AIS-NN offered tested accuracy of 99.97%, 99.98%, 99.99%, and tested F_1 values of 99.98%, 99.97%, and 99.99% respectively for the three considered semi-balanced datasets.

The proposed MH-DNN are reassessed using imbalanced datasets. The results obtained further confirmed the correctness of the proposed approaches. The tested accuracy of AIS-DNN approach is excellent, reaching a value of 99.93%, 99.92%, and 99.98% for the three imbalanced datasets.

The new dataset balancing technique proposed, based on K-means, has shown its correctness, as there are no abnormal deviations in the cross-validation results.

The comparison of the proposed approaches with the state-of-the-art works proved that AIS-DNN outperforms some recently published results and this is for the three datasets considered. The improvement rate increases to 4.99% in some cases.

Future works should include the following key points.

- Data can be reduced by merging multiple datasets and using the same features. This could simplify the IDS design and would further increase the performance. Moreover, a dataset is best when it is described with a minimum of very relevant features. This can be completed by visiting new feature selection tools.
- Regarding imbalanced datasets, greater interest should be focused on the methods to be considered to balance the rare attack classes.
- Usually, each MH algorithm has advantages and disadvantages. It would be wise to carefully examine the hybridization of two or more MH methods to further improve the detection of cyber-attacks.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] I. Sharafaldin, A. H. Lashkari and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. ICISSP*, Funchal, Madeira, Portugal, pp. 108–116, 2018.

[2] C. Yin, Y. Zhu, J. Fei and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[3] C. Tang, N. Luktarhan and Y. Zhao, "SAAE-DNN: Deep learning method on intrusion detection," *Symmetry*, vol. 12, pp. 1965, 2020.

[4] K. Kurniabudi, D. Stiawan, D. Darmawijoyo, M. Y. Bin Idris, A. M. Bamhdi *et al.,* "CICIDS-2017 dataset feature analysis with information gain for anomaly detection," *IEEE Access*, vol. 8, pp. 132911–132921, 2020.

[5] R. Atefinia and M. Ahmadi, "Network intrusion detection using multi-architectural modular deep neural network," *Journal of Supercomputing*, vol. 77, no. 4, pp. 3571–3593, 2021.

[6] S. Filho, F. A. Silveira, J. A. De Medeiros Brito, G. Vargas-Solar and I. F. Silveira, "Smart detection: An online approach for dos/ddos attack detection using machine learning," *Security and Communication Networks*, 2019. https://doi.org/10.1155/2019/1574749

[7] Y. Hua, "An efficient traffic classification scheme using embedded feature selection and lightGBM," in *Proc. ICTC*, Nanjing, China, pp. 125–130, 2020.

[8] R. B. Adhao and V. K. Pachghare, "Support based graph framework for effective intrusion detection and classification," *Preprint, Version 1*, 2021. https://doi.org/10.21203/rs.3.rs-1035364/v1

[9] M. I. Kareem and M. N. Jasim, "DDOS attack detection using lightweight partial decision tree algorithm," in *Proc. CSASE*, Duhoq, Iraq, pp. 362–367, 2022.

[10] U. Sabeel, S. Heydari, H. Mohanka, Y. Bendhaou, K. Elgazzar *et al.,* "Evaluation of deep learning in detecting unknown network attacks," in *Proc. SmartNets*, Sharm El Sheikh, Egypt, pp. 1–6, 2019.

[11] S. Haider, A. Akhunzada, I. Mustafa, T. B. Patel, A. Fernandez *et al.,* "A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 53972–53983, 2020.

[12] L. Wang and Y. Liu, "A DDoS attack detection method based on information entropy and deep learning in SDN," in *Proc. ITNEC*, Chongqing, China, pp. 1084–1088, 2020.

[13] M. Shurman, R. Khrais and A. Yateem, "DoS and DDoS attack detection using deep learning and IDS," *International Arab Journal of Information Technology*, vol. 17, no. 4A, pp. 655–661, 2020.

[14] S. Hosseini and H. Seilani, "Anomaly process detection using negative selection algorithm and classification techniques," *Evolving Systems*, vol. 12, no. 3, pp. 769–778, 2021.

[15] D. Aksu, S. Üstebay, M. A. Aydin and T. Atmaca, "Intrusion detection with comparative analysis of supervised learning techniques and fisher score feature selection algorithm," in *Proc. ISCIS*, Poznan, Poland, pp. 141–149, 2018.

[16] V. Kanimozhi and T. P. Jacob, "Artificial intelligence based network intrusion detection with hyperparameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," in *Proc. ICCSP*, Chennai, India, pp. 33–36, 2019.

[17] M. A. Ferrag, L. Maglaras, S. Moschoyiannis and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, no. 1, pp. 102419, 2020.

[18] I. F. Kilincer, F. Ertam and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Computer Networks*, vol. 188, pp. 107840, 2021.

[19] A. Bansal, DDR scheme and LSTM RNN algorithm for building an efficient IDS, Master's Thesis. Thapar Institute of Engineering and Technology, Punjab, India, 2018.

[20] A. Thakkar and R. Lohiya, "Analyzing fusion of regularization techniques in the deep learning-based intrusion detection system," *International Journal of Intelligent Systems*, vol. 6, no. 12, pp. 7340–7388, 2021.

[21] H. Basak, R. Kundu, P. K. Singh, M. F. Ijaz, M. Wozniak *et al.,* "A union of deep learning and swarm-based optimization for 3D human action recognition," *Scientific Reports*, vol. 12, no. 1, pp. 1–17, 2022.

[22] S. Kilicarslan, M. Celik and S. Sahin, "Hybrid models based on genetic algorithm and deep learning algorithms for nutritional Anemia disease classification," *Biomedical Signal Processing and Control*, vol. 63, pp. 102231, 2021.

[23] J. W. Han, Q. X. Li, H. R. Wu, H. J. Zhu and Y. L. Song, "Prediction of cooling efficiency of forced-air precooling systems based on optimized differential evolution and improved BP neural network," *Applied Soft Computing*, vol. 84, pp. 105733, 2019.

[24] K. Socha and C. Blum, "An ant colony optimization algorithm for continuous optimization: Application to feed-forward neural network training," *Neural Computing &Applications*, vol. 16, no. 3, pp. 235–247, 2007.

[25] M. Khishe and M. R. Mosavi, "Classification of underwater acoustical dataset using neural network trained by chimp optimization algorithm," *Applied Acoustics*, vol. 157, pp. 107005, 2020.

[26] A. Saffari, M. Khishe and S. H. Zahiri, "Fuzzy-ChOA: An improved chimp optimization algorithm for marine mammal classification using artificial neural network," *Anal Integr Circuits Signal Process*, vol. 111, no. 3, pp. 403–417, 2022.

[27] F. Chen, C. Yang and M. Khishe, "Diagnose Parkinson's disease and cleft lip and palate using deep convolutional neural networks evolved by IP-based chimp optimization algorithm," *Biomedical Signal Processing and Control*, vol. 77, pp. 103688, 2022.

[28] H. Faris, S. Mirjalili and I. Aljarah, "Automatic selection of hidden neurons and weights in neural networks using grey wolf optimizer based on a hybrid encoding scheme," *International Journal of Machine Learning and Cybernetics*, vol. 10, no. 10, pp. 2901–2920, 2019.

[29] C. Kirankaya and L. G. Aykut, "Training of artificial neural networks with the multi-population based artifical bee colony algorithm," *Network Computation in Neural Systems*, vol. 33, no. 1, pp. 124–142, 2022.

[30] I. Aljarah, H. Faris and S. Mirjalili, "Optimizing connection weights in neural networks using the whale optimization algorithm," *Soft Computing*, vol. 22, no. 1, pp. 1–15, 2018.

[31] L. T. Akin Sherly and T. Jaya, "Improved firefly algorithm-based optimized convolution neural network for scene character recognition," *Signal Image and Video Processing*, vol. 15, no. 5, pp. 885–893, 2021.

[32] K. Li, Y. Zhang and S. Wang, "An intrusion detection system based on PSO-GWO hybrid optimized support vector machine," in *Proc. IJCNN*, Shenzhen, China, pp. 1–7, 2021.

[33] P. Ghosh, D. Sarkar, J. Sharma and S. Phadikar, "An intrusion detection system using modified-firefly algorithm in cloud environment," *International Journal of Digital Crime and Forensics (IJDCF)*, vol. 13, no. 2, pp. 77–93, 2021.

[34] X. Zhao, S. Chen, Y. Yu and Z. Sun, "Genetic algorithm based intrusion detection system for software-defined network architecture," in *Proc. PIC*, Shanghai, China, pp. 309–313, 2020.

[35] V. Hajisalem and S. Babaie, "A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection," *Computer Networks*, vol. 136, pp. 37–50, 2018.

[36] G. Çetin, "An effective classifier model for imbalanced network attack data," *Computers, Materials & Continua*, vol. 73, no. 3, pp. 4519–4539, 2022.

[37] H. Dalmaz, E. Erdal and H. M. Ünver, "A new hybrid approach using GWO and MFO algorithms to detect network attack," *Computer Modeling in Engineering & Sciences*, vol. 136, no. 2, pp. 1277–1314, 2023.

[38] A. Hamdan Mohammad, T. Alwada'n, O. Almomani, S. Smadi and N. ElOmari, "Bio-inspired hybrid feature selection model for intrusion detection," *Computers, Materials & Continua*, vol. 73, no. 1, pp. 133–150, 2022.

[39] Intrusion Detection Evaluation Dataset (CICIDS2017), 2017. [online] Available at: https://www.unb.ca/cic/datasets/ids-2017.html

[40] CSE-CIC-IDS2018 on AWS, 2018. [online] Available at: https://www.unb.ca/cic/datasets/ids-2018.html

[41] DDoS Evaluation Dataset (CIC-DDoS2019), 2019. [online] Available at: https://www.unb.ca/cic/datasets/ddos-2019.html

[42] M. Mjahed, "Higgs search at LHC by neural networks," *Nuclear Physics B*, vol. 140, pp. 799–801, 2005.

[43] S. Haykin, *Neural networks and learning machines*, Third Edition ed., Upper Saddle River, New Jersey: Pearson Education, Inc, 2009.

[44] J. Timmis, A. Hone, T. Stibor and E. Clark, "Theoretical advances in artificial immune systems," *Theoretical Computer Science*, vol. 403, no. 1, pp. 11–32, 2008.

[45] I. Fister, I. Fister Jr, W. -S. Yang and J. Brest, "A comprehensive review of firefly algorithms," *Swarm and Evolutionary Computation*, vol. 13, pp. 34–46, 2013.

[46] A. R. Mehrabian and C. Lucas, "A novel numerical optimization algorithm inspired from weed colonization," *Ecological Informatics*, vol. 1, no. 4, pp. 355–366, 2006.

[47] A. S. Joshi, O. Kulkarni, G. Kakandikar and V. M. Nandedkar, "Cuckoo search optimization- a review," *Materials Today: Proc.*, vol. 4, pp. 7262–7269, 2017.

[48] N. V. Chawla, K. W. Bowyer, L. Hall and W. P. Kegelmeyer, "SMOTE: Synthetic minority over-sampling technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002.

[49] M. Mjahed and J. Proriol, "Tagging of jets and partons in e+e− events by discriminant analysis," *Physics Letters B*, vol. 217, no. 4, pp. 560–562, 1989.

[50] Y. Zhang, H. Zhang and B. Zhang, "An effective ensemble automatic feature selection method for network intrusion detection," *Information-an International Interdisciplinary Journal*, vol. 13, no. 7, pp. 314, 2022.

[51] A. Rosay, E. Cheval, F. Carlier and P. Leroux, "Network intrusion detection: A comprehensive analysis of CIC-IDS2017," in *Proc. ICISSP*, Vienna, Austria, pp. 25–36, 2022.

[52] R. I. Farhan, T. M. Abeer and F. H. Nidaa, "Performance analysis of flow-based attacks detection on CSE-CIC-IDS2018 dataset using deep learning," *Indonesian Journal of Electrical Enginering and Computer Science*, vol. 20, no. 3, pp. 16–27, 2020.

[53] M. A. Khan, "HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system," *Processes*, vol. 9, pp. 834, 2021.

[54] A. A. Hagar and B. W. Gawali, "Deep learning for improving attack detection system using CSE-CICIDS2018," *Neuro Quantology*, vol. 20, no. 7, pp. 3064–3074, 2022.

[55] M. S. Elsayed, N. -A. Le-Khac, S. Dev and A. D. Jurcut, "DDosNet: A deep-learning model for detecting network attacks," in *Proc. WoWMoM*, Cork, Ireland, pp. 391–396, 2020.

[56] D. C. Can, H. Q. Le and Q. T. Ha, "Detection of distributed denial of service attacks using automatic feature selection with enhancement for imbalance dataset," in *Proc. ACIIDS*, Phuket, Thailand, pp. 386–398, 2021.

[57] A. Chartuni and J. Márquez, "Multi-classifier of DDoS attacks in computer networks built on neural networks," *Applied Sciences*, vol. 11, pp. 10609, 2021.