Computers, Materials & Continua
DOI:10.32604/cmc.2021.016113
Article

Tech Science Press

A Hybrid Model Using Bio-Inspired Metaheuristic Algorithms for Network Intrusion Detection System

Omar Almomani*

Department of Computer Network and Information Systems, The World Islamic Sciences and Education University, Amman, 11947, Jordan
*Corresponding Author: Omar Almomani. Email: omar.almomani@wise.edu.jo
Received: 23 December 2020; Accepted: 24 January 2021

Abstract: Network Intrusion Detection System (IDS) aims to maintain computer network security by detecting several forms of attacks and unauthorized uses of applications which often can not be detected by firewalls. The features selection approach plays an important role in constructing effective network IDS. Various bio-inspired metaheuristic algorithms used to reduce features to classify network traffic as abnormal or normal traffic within a shorter duration and showing more accuracy. Therefore, this paper aims to propose a hybrid model for network IDS based on hybridization bio-inspired metaheuristic algorithms to detect the generic attack. The proposed model has two objectives; The first one is to reduce the number of selected features for Network IDS. This objective was met through the hybridization of bio-inspired metaheuristic algorithms with each other in a hybrid model. The algorithms used in this paper are particle swarm optimization (PSO), multi-verse optimizer (MVO), grey wolf optimizer (GWO), moth-flame optimization (MFO), whale optimization algorithm (WOA), firefly algorithm (FFA), and bat algorithm (BAT). The second objective is to detect the generic attack using machine learning classifiers. This objective was met through employing the support vector machine (SVM), C4.5 (J48) decision tree, and random forest (RF) classifiers. UNSW-NB15 dataset used for assessing the effectiveness of the proposed hybrid model. UNSW-NB15 dataset has nine attacks type. The generic attack is the highest among them. Therefore, the proposed model aims to identify generic attacks. My data showed that J48 is the best classifier compared to SVM and RF for the time needed to build the model. In terms of features reduction for the classification, my data show that the MFO-WOA and FFA-GWO models reduce the features to 15 features with close accuracy, sensitivity and F-measure of all features, whereas MVO-BAT model reduces features to 24 features with the same accuracy, sensitivity and F-measure of all features for all classifiers.

Keywords: IDS; metaheuristic algorithms; PSO; MVO; GWO; MFO; WOA; FFA; BAT; SVM; J48; RF; UNSW-NB15 dataset

1 Introduction

Computer network operations have been developing rapidly due to an increase in the number of computers and mobile devices. In light of that, the number of network attacks has been overgrowing as well. According to "*the European Union Agency for Network and Information Security (ENISA)*," the attacks complexity and the malicious sophistication has been increasing. Therefore, network security has been receiving greater attention [1,2]. The techniques used for ensuring network security are prevention, detection, and mitigation techniques. Prevention is a proactive technique that serves as the first-line procedure for protecting the network. It aims to avoid the attacks. If the prevention fails to protect the network, the detection technique is employed. It is utilized to monitor the network and detect potential attacks. Finally, mitigation techniques used to keep devices on while it is under attack. Detection techniques are categorized into two kinds based on the place of detection or type of detection. Place of detection can be host-based detection or network-based detection. In contrast, the type of detection can be a signature or anomaly-based detection [3]. Host-based detection monitors the internal operations of the computer system to detect any illegal access to its resources. The network-based detection monitors the network traffic logs in real-time for identifying the potential intrusions launched against the network. Signature-based detection technique searches for specific trends, or signatures. The use of this technique preferred for detecting known attacks, however, this technique is not able to detect new attacks.

On the other hand, anomaly-based detection aims to identify the normal behaviour of the network and producing a warning every time a deviation occurs through using a predefined threshold. Anomalies detection defined as a two-class classifier that classifies each sample as a normal or abnormal sample. The current IDS suffers from several efficiency-related problems, such as the low rates of detection accuracy and high rates of false detection [4]. To improve the IDS performance, feature selection is a significant step in any IDS. Feature selection for IDS can be done using several approaches. One of these approaches is bio-inspired metaheuristic algorithms.

Feature selection contributes to reducing the dimensional data by removing the duplicate and unnecessary features from the dataset. In addition to that, it deletes the least essential feature from the dataset to improve the classification accuracy. Feature selection approaches play a significant role in building an optimized IDS with fewer features. Feature selection model can be either filter-based, wrapper-based and embedded-based. In this paper wrapper-based used.

Bio-inspired metaheuristic algorithms are algorithms based on certain physical and biological standards. They are classified into two types, population and single solution based algorithms [5]. Population-based detectors are deemed more suitable than single solution-based algorithms. Population-based bio-inspired metaheuristic algorithms used in this study are PSO [6–10], MVO [11], GWO [7,12], MFO [13], WOA [14], FFA [7,15] and BAT [16,17].

Through the present paper, a hybrid model based on PSO, MVO, GWO, MFO, WOA, FFA, and BAT algorithms for network IDS proposed to reduce feature selection. That main objective of this study is to enhance the network IDS performance by reducing the number of the selected features to get high detection accuracy for large scale datasets with consuming less time. The effectiveness of the proposed model tested by using well-known machine learning SVM, J48 and RF classifiers.

The new contributions of the paper include:

(a) The present study offers a proposed hybrid model for network IDS through the hybridization of every couple of PSO, MVO, GWO, MFO, WOA, FFA, and BAT algorithms to reduce the number of the selected feature to improve NIDS performance.
(b) The present study evaluates the reduced dataset of the proposed hybrid model based on SVM, J48, and RF machine learning classifiers.

The paper organized as follows: Section 2 provides a review of the relevant literature that is related to anomaly detection by using bio-Inspired Metaheuristic algorithms. Section 3 presents a discussion about the proposed model. Section 4 provides information about the performance evaluation metrics. Section 5 presents several experimental results about the proposed model. Section 6 offers a conclusion

2 Related Works

During recent years, the feature selection model for network IDS has been receiving much attention from researchers. The researchers proposed many models to improve network IDS performance using different approaches such as filter, wrapper, data processing, optimization, machine learning techniques, and Bio-inspired Metaheuristic algorithms. Bio-inspired Metaheuristic algorithms are used to improve the network IDS performance due to its ability to find the most effective solutions within the minimum time. Each bio-Inspired metaheuristic algorithm has its drawbacks and advantages. Through hybridization, each algorithm can take advantage of the strengths and address the weaknesses of other algorithms. Many recent studies suggest that hybridization improves the bio-Inspired metaheuristic algorithm performance. This section explains some of these recent studies.

Kim et al. [18] developed a hybrid IDS which includes an anomaly detection model based on multiple 1-class SVM. It consists of a misuse detection model based on the C4.5 decision tree algorithm. NSL-KDD dataset used for validating the proposed hierarchical model in terms of detection accuracy and false alarm rate of unknown and known attacks. In comparison to other models, the proposed model can effectively reduce the false positive rate and the duration needed for the testing and training processes. In addition to that, the proposed model significantly reduces the time required for training processes by 50% and the time required for the testing process by 40%.

Ghanem et al. [19] proposed a hybrid IDS to classify anomalies in large-scale datasets through employing the Genetic Algorithm (GA) detectors and multi-start metaheuristic system. The proposed model uses a negative selection-based detector generation method. It was evaluated by employing the NSL-KDD dataset. Based on the results of the evaluation, the model is useful in generating an appropriate number of detectors. The accuracy rate of this model is 96.1%, and the false positive rate is 3.3.

Eesa et al. [20] developed a hybrid model that includes the cuttlefish optimization algorithm (CFA) and the decision tree classifier. It aims to detect network intrusions. In this model, the CFA employed for selecting significant features, while the decision tree algorithm used for identifying the types of abnormal events. The performance of this model tested on the KDDCup99 Dataset. The results showed that, when the number of features is less than 20, the detection rate and accuracy is significantly high.

Asahi-Shahri et al. [21] developed a hybrid model that includes GA and SVM. This model reduced the features from 45 to 10 features. The GA algorithm categorized those features into three types based on priority. This model shows an outstanding true positive value and a low false-positive value using the KDD 99 dataset. The results of the proposed hybrid model showed a true positive value of 0.973 and the false-positive value is 0.017.

Guo et al. [22] developed a two-level hybrid model to detect the intrusions by utilizing the strengths of the misuse-based and anomaly-based detection approach. This model consists of two anomaly detection components (ADCs) and one misuse detection component (MDC). ADC one detects abnormal connections by employing the ADBCC method. After that, the declared abnormal and normal links sent to the ADC two and the MDC respectively in parallel to be assessed by K-NN. This hybrid approach tested experimentally using KDDCup99 and the Kyoto University Benchmark Dataset (KUBD). Based on the results of the trial using the dataset of KDD99, the proposed model can effectively detect unknown attacks and known ones. It can effectively detect network anomalies by showing a high detection accuracy value and a low false-positive rate value. Based on the results of the experiment using the dataset of KUBD, the proposed model was highly effective in collecting attack traffics without having a specific label compared to KDDcup99 and KDD99.

Al-Yaseena et al. [23] developed a multi-level hybrid IDS that employs extreme learning machine (ELM) and SVM which they were used to improve the performance efficiency of the model in detecting known and unknown attacks. The proposed model tested using the KDD-Cup99 dataset. Based on the results of the trial, the accuracy of the proposed model is 95.75%. The false alarm rate of the model is 1.87%.

Hajisalem et al. [24] developed a hybrid classification model based on an artificial bee colony (ABC) and artificial fish swarm (AFS) algorithm. The performance level of the model assessed by employing two datasets (NSL-KDD and UNSW-NB15). Based on the results of the trial, the detection accuracy of the model is 99%. The false-positive rate is 0.01%.

Li et al. [25] developed a model that includes the Gini index. This model consists of the gradient boosting decision tree (GBDT) and PSO. The optimal feature subset was chosen by Gini index. The gradient lifting decision tree algorithm was used to detect a network attack. The parameters of GBDT were optimized using the PSO algorithm. The model assessed in terms of detection rate, accuracy, F1-score, precision, and false alarm rate. Such an assessment conducted by employing the NSL-KDD Dataset. Based on the results, it was found that the model is accurate and able to detect intrusion effectively. The detection rate of the model was 78.48%, the precision rate was 96.44%, the F1-score was 86.54% and the false acceptance rate was 3.83%.

Hosseini et al. [26] developed a hybrid model for detecting intrusion. This model consists of two phases. The first phase is the feature selection phase. The second phase is the attack detection phase. Through the first phase, a wrapper method called (MGA-SVM) employed. This model includes features of SVM and GA with multi-parent crossover and multi-parent mutation (MGA). In the second phase, an artificial neural network (ANN) employed for detecting attacks. A hybrid gravitational search (HGS) conducted, and a PSO is used to improve the performance of the proposed model. The proposed model is named MGA-SVMHGS-PSO-ANN. The performance of MGA-SVMHGS-PSO-ANN compared to the performance of GS-ANN, DT, GD-ANN, GAANN, PSO-ANN, and GSPSO-ANN. Using the NSL-KDD Dataset, data showed that the proposed MGA-SVMHGS-PSO-ANN model has a high detection accuracy rate of 99.3%.

The features of NSL-KDD reduced from 42 to 4 features and the training time of this model is 3 seconds maximum.

Khraisat et al. [27] developed a hybrid IDS (HIDS) model, which includes a C5.0 decision tree classifier and a one-class support vector machine (OC-SVM). HIDS used the strengths of the Signature-based IDS and the anomaly-based IDS. The signature-based IDS created based on the C5.0 decision tree classifier, while the anomaly-based IDS established based on the OC-SVM. It aims to identify the well-known intrusions and zero-day attacks by showing a high level of detection accuracy and a low false-alarm rate. The proposed HIDS assessed by employing the NSL-KDD datasets and the Australian defence force academy (ADFA) datasets. It found that the performance of HIDS has improved compared to Signature-based IDS and anomaly-based IDS in terms of the detection rate, false alarm rate, true negative rate, false-negative rate, false-positive rate, recall rate, precision, sensitivity, and F-Measure.

Mohmmadzadeh et al. [28] proposed a new hybrid model combining WOA and flower pollination algorithm (FPA). This model is called HWOAFPA. It employs natural processes of WOA and FPA for solving the problem of feature selection optimization. On the other hand, it operates the opposition-based learning (OBL) method to ensure that the convergence rate and accuracy of the proposed model are high. In fact, in the proposed model, WOA creates solutions in their search space by using the prey siege and encircling process, bubble invasion. It searches for prey methods and seeks to enhance the solutions of the feature selection problem; along with this model. FPA improves the solution of the issue of the feature selection by carrying out two global and local search processes in an opposite space with the solutions of the WOA. WOA and FPA using all the possible solutions to solve the feature selection problem. They assessed the level of the proposed model performance using an experiment consisting of two stages. Through the 1st stage, the investigation carried out on ten feature selection datasets that obtained from the UCI data repository, and in the second stage, WOA and FPA assessed the performance level of the model in terms of detecting spam email messages. Based on the results obtained from the first stage, the model performance on ten UCI datasets is more effective than other basic metaheuristic algorithms in terms of the average size of selection and classification accuracy, whereas in the second stage, the proposed model shows higher accuracy than other similar algorithms in terms of having spam emails detected.

3 Proposed Hybrid Model

This model aims to increase the performance efficiency of the network IDS by hybridizing the following PSO, MVO, GWO, MFO, WOA, FFA, and BAT meta-heuristic algorithms. Fig. 1 presents a proposed hybrid model architecture. The performance efficiency is enhanced by reducing the number of effective features in classifying the dataset to detect generic attacked. The following subsection illustrates each stage of the proposed model in detail.

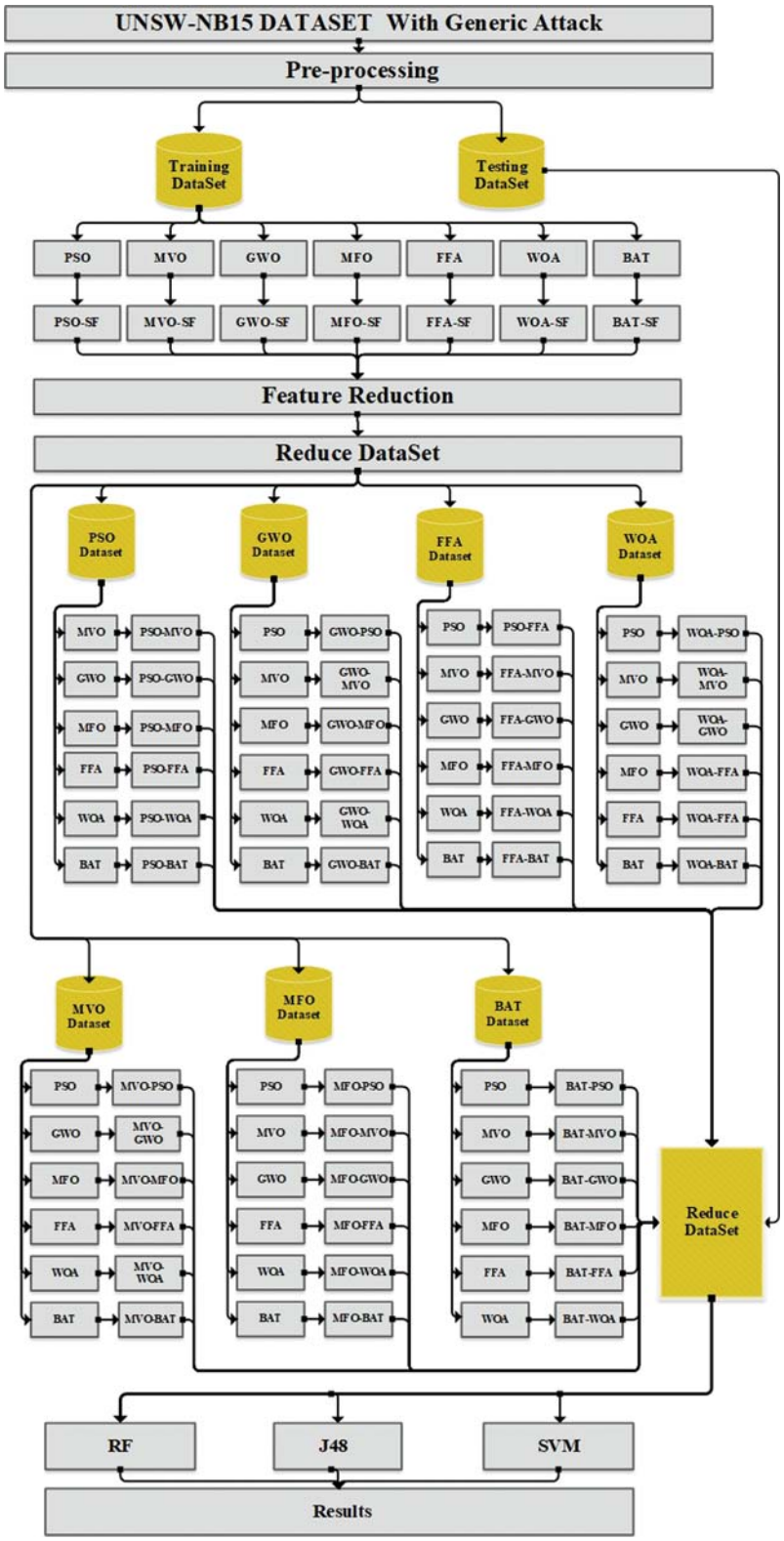

Figure 1: The proposed hybrid model architecture

3.1 UNSW-NB15 Dataset

The UNSW-NB15 dataset [29] created by utilizing an IXIA PerfectStorm tool. A tcpdump tool used to capture 100 GB of raw network traffic (pcap files). Each pcap file contains 1000 MB to make the analysis of the packets easier. Argus and Bro-IDS techniques were used, and 12 procedures carried out to generate 49 features with the class label. This dataset divided into a training set and a testing set. The training set includes 175,341 records, while the testing set contains 82,332 records and these records can be either attack or normal. The relevant attacks launched against the UNSW-NB15 dataset are 9 types which include; analysis, backdoor, DoS, Exploits, Fuzzers, Generic, Reconnaissance, Shellcode and Worms. The generic attack represented by 18,8712 records in the testing set and 40,000 records in the training set which is the highest attacks among other attacks. Tab. 1 presents a list of features that are in UNSW-NB15 dataset.

Table 1: UNSW-NB15 dataset features list

Features no	Features name	Features no	Features name	Features no	Features name	Features no	Features name
1	id	12	dttl	23	dtcpb	34	ct_dst_ltm
2	dur	13	sload	24	dwin	35	ct_src_dport_ltm
3	proto	14	dload	25	tcrptt	36	ct_dst_sport_ltm
4	service	15	sloss	26	synack	37	ct_dst_src_ltm
5	state	16	dloss	27	ackdat	38	is_ftp_loain
6	spkts	17	sinpkt	28	smean	39	ct_ftp_cmd
7	dpkts	18	dinpkt	29	dmean	40	ct_flw_http_mthd
8	sbytes	19	sjit	30	trans_depth	41	ct_src_ltm
9	dbytes	20	djit	31	response_body_len	42	ct_srv_dst
10	rate	21	swin	32	ct_srv_src	43	is_sm_ips_p orts
11	stt1	22	stcpb	33	ct_state_ttl	44	attack_cat
						45	label

3.2 Pre-Processing Stage

The UNSW-NB15 dataset has to go through the following pre-processing steps to use the EvoloPy-FS optimization framework [30–33]:

(a) The label removal: Each feature in the original UNSW-NB15 dataset has a label. It's necessary to remove this label to adapt the dataset with the EvoloPy-FS context.
(b) The removal of features: The original UNSW-NB15 Dataset has 45 features, 2 of these include class labels i.e attack cat and label. The attack cat is not considered as a feature, thus, deleting it is necessary.
(c) Label encoding: Within the Dataset, the labels i.e state, protocol, and service type have string values and it is crucial to have these values encoded in numerical values.
(d) Binarisation of data: The numerical data in the dataset poses challenges over the classifier in the training process. Thus, it is very important to standardize the values in each feature. Therefore, the minimum value should be 0 in each feature and the maximum value should be 1 in each feature. This will make the group more homogeneous and maintain the contrast between the values of every feature.

3.3 Bio-Inspired Metaheuristic Algorithms

Selecting the features was done based on the following Bio-inspired metaheuristic algorithms:

3.3.1 PSO

PSO created by Eberhart et al. [6]. Through PSO, the information gets optimized through having social contact within the community; the learning is considered personal and social. PSO based on the ability to interpret each solution in the swarm as a particle. Regarding each particle as a position in the search space that represented as follows:

$$x_{i=(x_{i1},x_{i2},x_{i2},x_{i3},\ldots,x_{iD},)} \tag{1}$$

D refers to the search space dimensionality. Particles move to search for the optimal solutions within the search space, considering each particle has a velocity which is identified as follows

$$v_{i=(v_{i1},v_{i2},v_{i2},v_{i3},\ldots,v_{iD},)} \tag{2}$$

Regarding each particle, it has its position and velocity, such a position and velocity updated throughout the movement of the position. The best initial position of the particle reported as the best personal pbest. The best position of the population is called gbest. PSO looks for optimal solutions based on gbest-pbest. It looks for them through having the velocity and position of each particle updated by the equations below:

$$x_{id}^{t+1} = x_{id}^{t} + v_{id}^{t+1} \tag{3}$$

$$v_{id}^{t+1} = w * v_{id}^{t} + c_1 * r_1 * \left(p_{id} - x_{id}^{t}\right) + c_2 * r_2 * \left(p_{gd} - x_{id}^{t}\right) \tag{4}$$

t denotes the tth iteration within the process of evolutionary. $d \in D$ indicates the dth dimension in the search space. w refers to the weight of the inertia that controls the impact of the previous velocities on the current velocities. *c1*, along with *c2* are considered acceleration constants. *r1*, along with *r2*, are considered random values that are in the range of [0, 1]. *pid* refers to pbest. pgd refers to gbest in the dth dimension.

3.3.2 MVO

MVO is a new metaheuristic algorithm that was developed by Mirjalili et al. [11]. It mimics the principles of a multi-versa theory. It was developed based on the idea of multiple existences universes that include white, black and wormholes and their interactions. Regarding the algorithm, it is a stochastic algorithm that based on the population. It approximates the optimum global for problem optimization with a solution collection.

MVO has two parameters for having the solution updated. Those parameters are wormhole existence probability (WEP) and travelling distance rate (TDR). They determine how much and how often the solutions change during the process of optimization. WEP is calculated based on the equation below:

$$WEP = a + t * \left(\frac{b-a}{T}\right) \tag{5}$$

Where the minimum is b, the maximum is a current iteration is t, and the maximum number of allowed iterations is T. TDR i is calculated based on the equation below:

$$TDR = 1 - \frac{t^{\frac{1}{p}}}{T^{\frac{1}{p}}} \tag{6}$$

where the exploitation accuracy is p. Finally, the position of the solutions modified after calculating WEP and TDR.

3.3.3 GWO

GWO developed based on a social hierarchy and the hunting approach of grey wolves. It proposed by Mirjalili et al. [12]. It consists of four levels.

Level-1: Alpha (α): It is responsible for the process of making the decisions (e.g., decisions related to hunting, wake-up time, sleep place).

Level-2: Beta (β): It is probably the strongest wolf candidate for replacing alpha. β operates as an advisor to α.

Level-3: Delta (δ): They refer to the wolves that respect α-β wolves at this stage. They monitor x wolves. They serve as scouts, sentinels, sentinels, elders, in-pack caretakers and hunters.

Level-4: Omega (ω): Regarding the wolves at the fourth level, they deemed the weakest wolves. They carry out the role of the scapegoat. They must obey the order issued by certain people.

GWO mathematics model has three parts. Those parts are encircling, hunting and attaching behaviour. the encircling behaviour, it represented in the equation below:

$$\vec{X}(t+1) = \vec{x}_p + \vec{A} \cdot \vec{D} \tag{7}$$

whereas:

$\vec{x}_p$ is prey's position, $\vec{X}$ is grey wolf's position, (t) is the number of iterations,

$\vec{A}$ is represented in the equation below:

$$\vec{A} = 2\vec{a} \cdot \vec{r1} - \vec{a} \tag{8}$$

$\vec{D}$ described in the equation below

$$\vec{D} = \left| \vec{C} \cdot \vec{x}_p(t) - \vec{X}(t) \right| \tag{9}$$

$\vec{C}$ is described in the equation below

$$\vec{C} = 2 \cdot \vec{r_2} \tag{10}$$

The hunting behaviour defined in the equation below

$$\vec{D_\alpha} = \left| \vec{C_1} \cdot \vec{X_\alpha} - \vec{X} \right|, \quad \vec{D_\beta} = \left| \vec{C_2} \cdot \vec{X_\beta} - \vec{X} \right|, \quad \vec{D_\delta} = \left| \vec{C_3} \cdot \vec{X_\delta} - \vec{X} \right| \tag{11}$$

$$\vec{x_1} = \vec{X_\alpha} - A_1 \cdot \left(\vec{D\alpha}\right), \quad \vec{x_2} = \vec{X_\beta} - A_2 \cdot \left(\vec{D_\beta}\right), \quad \vec{x_3} = \vec{X_\delta} - A_3 \cdot \left(\vec{D_\delta}\right) \tag{12}$$

$$\vec{X}(t+1) = \frac{X_1 + \vec{X_2} + X_3}{3} \tag{13}$$

The attaching behaviour represented in the equation below

$$\vec{a} = 2 - t \cdot \frac{2}{\max ter_i} \tag{14}$$

$\vec{a}$ vector set to decrease over iterations linearly from two to zero.

$\vec{r_1}$, $\vec{r_2}$ are values that were selected randomly. They are within the range of [0–1].

3.3.4 MFO

MFO proposed by Mirjalili [13]. Regarding Moth, an insect related to the butterflies' family. It starts carrying out its primary activities at night. The primary concept for MFO comes from investigating the moth cycle when looking for light in nature, that's called transverse orientation. The moth location is regulated based on a fixed angle of motion concerning the incoming light. Moths travel in a spiral shape and seek to hold angle that similar to the angle of the light produced by man. They update their location for a specific flame according to the following equation:

$$S\left(M_i, F_j\right) = D_i \cdot e^{bt} \cdot \cos(2\pi t) + F_j \tag{15}$$

Whereas:

D_i Euclidian distance of the i moth for the j flame. It calculated as follows:

$$D_i = \left|F_j - M_i\right| \tag{16}$$

M_i is i Moth, F_j is j flame, t refers to any random value that is within the range of [−1, 1]. Where the number of the flames inside MFO calculate as follows:

$$Number\ of\ flames = round\left(N - l \cdot \frac{N-1}{T}\right) \tag{17}$$

l stands for the number of iterations, N stands for the maximum number of flames, T stands for the maximum number of iterations

3.3.5 FFA

FFA created by Yang et al. [34]. It based on tropical firefly's communication behaviour. This behaviour described by using three idealized rules. These rules are:

(a) Regarding all the fireflies as unisex.
(b) The brightness of the fireflies is proportionate to their attractiveness.
(c) The firefly's brightness is determined and influenced by the environment of the objective functions.

The movement of a firefly i that is attracted to firefly j represented in the equation below:

$$x_i = x_i + \beta_0 e^{-\gamma r_{ij}^2}\left(x_j - x_i\right) + \alpha(rand - 0.5) \tag{18}$$

Where:

(rand −0.5) is a random number that is within the range of [−0.5 −0.5], β_0 set to 1, α is range from [0,1].

$\beta_0 e^{-\gamma r_{ij}^2}$ stands for the approximation of the light intensity that got lost due to distance. The distance that is between firefly i and firefly j is calculated through the equation below

$$r_{ij} = \left\| x_i - x_j \right\| \tag{19}$$

Whereas:

xi refers to the position of firefly I, xj refers to the position of firefly j.

3.3.6 WOA

A WOA created by Mirjalili [14]. It imitates the natural behaviour of the humpback whales. The simulation of this algorithm involves three operators simulating the prey search (exploration phase), the encircling prey, and the humpback whales behaviour of bubble-net foraging (exploitation phase). The encircling prey, it represented in the equation below:

$$\vec{X}(t+1) = \vec{X^*}(t) - \vec{A} \cdot \vec{D} \tag{20}$$

$$\vec{D} = \vec{C} \cdot \vec{X^*}(t) - \vec{X}(t) \tag{21}$$

$$\vec{A} = 2\vec{a} \cdot \vec{r} - \vec{a} \tag{22}$$

$$\vec{C} = 2 \cdot \vec{r} \tag{23}$$

Where:

$\vec{X^*}$ refer to the location of the best solution obtained. $\vec{a}$ refer to reduced linearly from two to 0. r refers to a random number that's within the range of [0–1].

The phase of exploitation: This phase is also called the attacking bubble-net. It works with two approaches: Shrinking encircling and spiral updating position. Both shrinking circlings in a spiral updating position are applying in whale movement in the direction of its prey.

3.3.7 BAT

BAT proposed by Yang [16]. It represents the behaviour of the bats, which is described by employing three idealized rules as follows:

(a) All the bats use echolocation to predict the distance. They know in some magical manner the difference between food/prey and background barriers.
(b) A bat *bi* flies randomly at velocity *vi* with a specific frequency *fmin* at position *xi*, varying wavelength λ and loudness *A0* to hunt for prey. The frequency or wavelength of they emit is changed automatically. The pulse emission rate is adjusted r ∈ [0,1] based on their target proximity.
(c) Loudness varies in several aspects. It differs from a large positive *A0* to a minimum constant value *Amin* as it's suggested by Yang [12].

Virtual bat movement updates its velocity and position through using the following equations:

$$f_i = f_{min} + (f_{min} - f_{max})ß \tag{24}$$

$$v_i^j(t) = v_i^j(t-1) + \left[\hat{x}^j - x_i^j(t-1)f_i\right] \tag{25}$$

$$x_i^j(t) = x_i^j(t+1) + v_i^j(t) \tag{26}$$

where:

ß is a random number that is within the range of [0, 1], *Xi* stands for the initial position, *Vi* stands for the velocity, *Fi* stands for the *initial* frequency

3.4 Feature Selection Model

The proposed model selects important features as follow:

(a) Binariz data [−1, 1]
(b) Define a set of binary individuals.
(c) Individual and population represented by [1-D, 2-D] array.
(d) Reduce dataset generated where 1s indicates to feature selected, and 0s mean feature not selected feature.
(e) Knn classifier used to evaluate the suitable solution and produce fitness value of reducing dataset.
(f) Finally, repeat these steps to reach the maximum number of iterations.

3.5 Hybrid Bio-Inspired Metaheuristic Model

Tab. 2 presents the hybridization of bio-inspired metaheuristic algorithms hybridization.

Table 2: Hybridization of bio-inspired metaheuristic algorithms

A1	A2	Hybrid model	A1	A2	Hybrid model	A1	A2	Hybrid model
PSO	MVO	PSO-MVO	***WOA***	PSO	WOA-PSO	***MFO***	PSO	MFO-PSO
	GWO	PSO-GWO		MVO	WOA-MVO		MVO	MFO-MVO
	MFO	PSO-MFO		GWO	WOA-GWO		GWO	MFO-GWO
	WOA	PSO-WOA		MFO	WOA-MFO		WOA	MFO-WOA
	FFA	PSO-FFA		FFA	WOA-FFA		FFA	MFO-FFA
	BAT	PSO-BAT		BAT	WOA-BAT		BAT	MFO-BAT
MVO	PSO	MVO-PSO	***FFA***	PSO	FFA-PSO			
	GWO	MVO-GWO		MVO	FFA-MVO			
	MFO	MVO-MFO		GWO	FFA-GWO			
	WOA	MVO-WOA		MFO	FFA-MFO			
	FFA	MVO-FFA		WOA	FFA-WOA			
	BAT	MVO-BAT		BAT	FFA-BAT			
GWO	PSO	GWO-PSO	***BAT***	PSO	BAT-PSO			
	MVO	GWO-MVO		MVO	BAT-MVO			
	MFO	GWO-MFO		GWO	BAT-GWO			
	WOA	GWO-WOA		MFO	BAT-MFO			**A1 Algorithm 1**
	FFA	GWO-FFA		WOA	BAT-WOA			**A2 Algorithm 2**
	BAT	GWO-BAT		FFA	BAT-FFA			

3.6 Machine Learning Classifiers

Classifier employed for classifying the incoming data as abnormal data or a normal. The present study sheds light on J48, SVM and RF classifiers. These classifiers were select because they are the most famous classifiers used in the literature for network IDS [21,35–39].

3.6.1 SVM

SVM is a binary classifier. In SVM, the data gets divided into two class through the use of statistical methods, fixed rules and quadratic equations. The binary classification of the data is carried out through employing a separating hyperplane to maximize the space of the margin based on the functions of the kernel, and the extracted data are stored in the vector, leading to the best solution for the problem. Due to its use for the structural risk minimization method, the SVM has a strong generalization capability. Several previous [21,35,36] studies showed that SVM is a highly effective classifier.

3.6.2 J48

The algorithm of J48 is considered a tree classifier that was proposed by Quinlan [40]. It employed the improved technique of tree pruning for reducing the number of classification-related errors. It follows the following steps for creating a decision tree:

(a) Selecting the attribute as root that has the enormous gain value.
(b) Building a branch for any value.
(c) Repeating the procedure for each branch until the branches have the same class for all the cases.

Several researchers explored the influence of employing the J48 algorithm for enhancing the accuracy level of IDS [36,37].

3.6.3 RF

RF classifier proposed by L.Breiman [41]. It is a tree-based ensemble learning classifier [42]. It constructed by combining the predictions of various trees, each of which trained in individual. The decision takes by RF classifier is based on most of the trees selected. The RF classifier has several benefits, for instance, it has the chance of over-fitting and it is associated with less duration of time for the training process. It shows a high level of accuracy and it runs efficiently in large databases. Through predicting of the missing data, it makes highly accurate predictions. Several previous studies [38,39], showed that the RF classifier has a significant positive impact on the accuracy of IDS.

4 Performance Evaluation Metrics

For assessing the performance efficiency of the proposed model, the following metrics were used: true-positive (TP), true-negative (TN), false-positive (FP) and false-negative (FN) rates [43,44]. The confusion matrix presented in Tab. 3. Based on these metrics, other metrics are calculated, such as sensitivity, precision, accuracy, F-measure and building time.

Table 3: Confusion matrix

		Predicted	
		Normal	Attack
Actual	Normal	(TP)	(FN)
	Attack	(FP)	(TN)

Metrics calculated as below:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{27}$$

$$\text{Precision} = \frac{TP}{TP + FP} \tag{28}$$

$$\text{Sensitivity} = \frac{TP}{TP + FN} \tag{29}$$

$$\text{F-Measure} = \frac{2 * \text{Precision} * \text{Sensitivity}}{\text{Precision} + \text{Sensitivity}} \tag{30}$$

5 Discussion and Results

5.1 First Experiment: Features Selection

The experiment was done using anaconda python open-source. Tab. 4 presents the simulation parameters setting.

Table 4: Simulation parameters

Parameter	Optimizers	Datasets	Attack	Number of runs	Population size	Iterations
Value	Combination of PSO, MVO, GWO, MFO, WOA, FFA, and BAT (see Tab. 2)	UNSW-NB15	Generic	30	20	20

Tab. 5 presents the results of selected features based on the hybridization of Bio-Inspired metaheuristic algorithms.

Tab. 5 presents the results of selected features based on the hybridization of Bio-Inspired metaheuristic algorithms. Based on Tab. 5, it was found that PSO-MVO model reduces the number of features into 12 features. In contrast, MVO-WOA, GWO-MVO and GWO-MFO model reduces the number of features into 14 features, while MFO-PSO and MFO-MVO model reduces the number of features into 12 features. Meanwhile, WOA-GWO minimizes the number of features into 9 features, FFA-MVO model reduces the number of features into 8 features and BAT-GWO reduces features to 18 features.

Table 5: Selected features-based hybridization model

Hybrid model	Features number	Selected features
PSO-MVO	**12**	**F8, F12, F14, F18, F19, F20, F21, F22, F26, F27, F36, F42**
PSO-GWO	19	F2, F3, F8, F9, F12, F13, F14, F15, F17, F18, F21, F23, F25, F26, F27, F33, F35, F36, F42
PSO-MFO	14	F3, F4, F13, F15, F16, F18, F19, F20, F21, F25, F26, F27, F30, F32
PSO-WOA	18	F3, F4, F12, F15, F16, F18, F19, F20, F21, F22, F23, F25, F26, F27, F30, F33, F35, F38
PSO-FFA	20	F2, F3, F4, F9, F15, F16, F17, F18, F19, F20, F21, F22, F26, F27, F30, F32, F35, F36, F38, F42
PSO-BAT	19	F2, F4, F8, F12, F13, F14, F15, F19, F20, F21, F22, F23, F25, F26, F30, F32, F33, F36, F42
MVO-PSO	15	F5, F6, F7, F9, F10, F15, F19, F21, F22, F24, F28, F29, F36, F37, F40
MVO-GWO	15	F2, F3, F5, F6, F7, F9, F10, F11, F16, F19, F22, F35, F36, F37, F41
MVO-MFO	16	F2, F4, F6, F7, F11, F15, F16, F17, F18, F19, F21, F29, F32, F37, F39, F43
MVO-WOA	**14**	**F10, F16, F17, F18, F19, F21, F22, F24, F32, F33, F37, F40, F41, F43**
MVO-FFA	19	F2, F3, F4, F5, F6, F7, F8, F16, F18, F19, F21, F24, F28, F29, F33, F35, F36, F39, F40
MVO-BAT	24	F2, F3, F4, F5, F6, F9, F10, F11, F15, F16, F17, F19, F21, F22, F24, F29, F32, F33, F35, F36, F37, F40, F41, F43
GWO-PSO	17	F2, F3, F7, F9, F11, F12, F15, F18, F19, F21, F23, F26, F33, F35, F36, F37, F41
GWO-MVO	**14**	**F2, F3, F4, F9, F15, F18, F20, F21, F31, F32, F35, F37, F39, F41**
GWO-MFO	**14**	**F3, F4, F7, F11, F12, F15, F18, F19, F26, F28, F35, F37, F41, F43**
GWO-WOA	17	F2, F4, F9, F12, F18, F19, F20, F21, F23, F26, F28, F32, F33, F36, F39, F42, F43
GWO-FFA	15	F3, F4, F7, F11, F15, F18, F19, F23, F26, F31, F32, F33, F36, F37, F41
GWO-BAT	17	F3, F7, F9, F11, F15, F18, F21, F23, F27, F28, F31, F32, F35, F36, F39, F42, F43
MFO-PSO	**12**	**F5, F8, F11, F15, F19, F20, F23, F28, F32, F35, F38, F41**
MFO-MVO	**12**	**F4, F8, F9, F15, F18, F20, F24, F28, F32, F35, F38, F41**
MFO-GWO	13	F3, F5, F9, F17, F18, F19, F20, F23, F26, F32, F35, F37, F41

(Continued)

Table 5: Continued

Hybrid model	Features number	Selected features
MFO-WOA	15	F1, F4, F5, F11, F15, F17, F18, F20, F24, F26, F28, F32, F37, F39, F41
MFO-FFA	14	F3, F4, F8, F11, F15, F18, F19, F24, F26, F28, F32, F35, F38, F41
MFO-BAT	19	F3, F5, F8, F9, F11, F17, F18, F19, F20, F23, F24, F26, F28, F32, F35, F37, F38, F39, F41
WOA-PSO	12	F4, F8, F15, F17, F23, F30, F32, F33, F36, F40, F42, F43
WOA-MVO	13	F4, F5, F19, F21, F22, F23, F24, F25, F32, F33, F40, F42, F43
WOA-GWO	**9**	**F2, F8, F11, F15, F17, F25, F32, F40, F43**
WOA-MFO	15	F2, F4, F8, F11, F17, F21, F23, F24, F25, F30, F32, F33, F34, F42, F43
WOA-FFA	11	F4, F5, F15, F22, F23, F24, F25, F33, F34, F42, F43
WOA-BAT	19	F2, F4, F5, F8, F11, F15, F17, F19, F21, F22, F23, F25, F30, F32, F33, F34, F36, F42, F43
FFA-PSO	13	F1, F4, F7, F10, F12, F15, F18, F27, F29, F33, F37, F41, F43
FFA-MVO	**8**	**F3, F4, F12, F22, F29, F31, F33, F37**
FFA-GWO	15	F1, F2, F3, F4, F7, F10, F12, F14, F15, F19, F22, F31, F33, F39, F42
FFA-MFO	15	F1, F3, F4, F8, F14, F15, F18, F22, F31, F33, F35, F39, F41, F42, F43
FFA-WOA	18	F2, F8, F10, F12, F14, F15, F18, F19, F22, F27, F29, F31, F33, F35, F37, F39, F41, F42
FFA-BAT	19	F1, F2, F4, F7, F8, F12, F13, F14, F15, F18, F22, F27, F31, F33, F35, F37, F39, F42, F43
BAT-PSO	22	F1, F2, F5, F7, F10, F11, F12, F13, F16, F17, F21, F22, F23, F25, F26, F27, F30, F33, F35, F36, F39, F42
BAT-MVO	22	F2, F5, F7, F10, F12, F13, F16, F17, F20, F21, F22, F23, F25, F26, F28, F31, F33, F34, F36, F38, F39, F42
BAT-GWO	**18**	**F1, F2, F5, F7, F9, F11, F12, F13, F21, F25, F27, F28, F29, F31, F32, F34, F35, F37**
BAT-MFO	23	F3, F5, F7, F9, F10, F11, F12, F13, F17, F21, F23, F25, F26, F28, F29, F30, F33, F34, F36, F38, F39, F42, F43
BAT-WOA	19	F3, F5, F7, F9, F11, F12, F13, F16, F17, F28, F29, F30, F32, F33, F34, F35, F37, F42, F43
BAT-FFA	22	F1, F2, F3, F5, F9, F10, F11, F13, F16, F17, F20, F22, F25, F26, F27, F28, F32, F34, F36, F38, F42, F43

5.2 Second Experiment: Classification

The hybrid model in Tab. 5 evaluated based on three ML classifiers. These classifiers are J48, SVM and RF classifier. The results of the J48, SVM and RF classifier shown in Tab. 6.

Table 6: Results of J48, SVM and RF

	J48				SVM				RF			
	Accu %	**Sens %**	**F-M %**	**Ts**	**Accu %**	**Sens %**	**F-M %**	**Ts**	**Accu %**	**Sens %**	**F-M %**	**Ts**
All Features	92.80	90.60	94.34	2.35	92.79	90.57	94.33	193.53	92.80	90.60	94.34	26.26
PSO-MVO	92.67	90.38	94.23	**0.38**	92.67	90.38	94.23	182.7	92.67	90.38	94.23	**11.15**
PSO-GWO	92.59	90.39	94.17	0.99	92.47	90.15	94.07	**104.89**	92.59	90.39	94.17	16.1
PSO-MFO	91.68	88.91	93.4	0.76	91.67	88.89	93.39	251.88	91.68	88.91	93.40	19.18
PSO-WOA	91.52	88.72	93.27	0.60	90.90	87.73	92.74	182.61	91.52	88.72	93.27	16.92
PSO-FFA	92.60	90.39	94.18	0.93	92.49	90.16	94.08	311.36	92.60	90.39	94.18	20.00
PSO-BAT	**92.76**	**90.57**	**94.31**	0.69	**92.75**	**90.55**	**94.31**	109.93	**92.76**	**90.57**	**94.31**	15.2
MVO-PSO	92.59	90.39	94.17	0.6	92.48	90.16	94.07	176.28	92.59	90.39	94.17	**11.44**
MVO-GWO	90.65	87.41	92.52	0.65	90.65	87.41	92.52	135.82	90.65	87.41	92.52	13.61
MVO-MFO	92.64	90.42	94.21	0.72	92.56	90.24	94.14	125.38	92.64	90.42	94.21	14.08
MVO-WOA	92.77	90.56	94.32	0.75	92.75	90.55	94.31	95.27	92.76	90.57	94.31	13.99
MVO-FFA	92.76	90.57	94.31	0.98	92.75	90.55	94.31	**86.14**	92.76	90.57	94.31	12.39
MVO-BAT	**92.80**	**90.60**	**94.34**	**1.24**	**92.79**	**90.57**	**94.33**	116.58	**92.80**	**90.60**	**94.34**	16.00
GWO-PSO	**92.79**	**90.60**	**94.33**	0.67	**92.77**	**90.57**	**94.32**	86.06	**92.77**	**90.57**	**94.33**	14.68
GWO-MVO	92.49	90.16	94.08	**0.63**	92.49	90.16	94.08	110.68	92.49	90.16	94.08	14.52
GWO-MFO	92.63	90.41	94.2	0.64	92.54	90.23	94.13	144.79	92.63	90.41	94.25	**13.03**
GWO-WOA	**92.79**	**90.60**	**94.33**	1.28	**92.77**	**90.57**	**94.32**	**80.73**	**92.77**	**90.57**	**94.33**	14.12
GWO-FFA	**92.79**	**90.60**	**94.33**	0.61	92.76	90.56	94.31	90.34	**92.77**	**90.57**	**94.33**	13.41
GWO-BAT	**92.79**	**90.60**	**94.33**	0.97	92.55	90.24	94.13	139.65	92.55	90.24	94.13	17.02
MFO-PSO	86.78	81.58	89.10	0.60	86.64	81.32	88.97	68.12	86.78	81.58	89.10	**7.30**
MFO-MVO	90.90	87.73	92.74	**0.44**	90.84	87.63	92.68	**44.56**	90.90	87.73	92.74	7.88
MFO-GWO	89.62	85.90	91.64	0.89	89.61	85.88	91.63	86.06	89.62	85.90	91.64	8.78
MFO-WOA	**92.53**	**90.22**	**94.12**	0.74	**92.53**	**90.21**	**94.11**	71.73	**92.62**	**90.40**	**94.19**	9.50
MFO-FFA	90.21	90.12	90.41	1.26	92.53	90.21	94.11	69.14	92.54	90.22	94.12	11.36
MFO-BAT	90.61	87.38	92.50	1.24	90.61	87.37	92.49	92.92	90.61	87.37	92.49	11.22
WOA-PSO	92.72	90.42	94.27	**0.47**	92.71	90.41	94.26	**33.76**	92.71	90.44	94.26	**8.59**
WOA-MVO	92.75	90.56	94.30	0.55	92.71	90.47	94.26	66.89	92.74	90.55	94.29	11.24
WOA-GWO	84.37	77.8	86.83	0.51	84.37	77.80	86.83	29.56	84.38	77.81	86.84	12.02
WOA-MFO	92.75	90.46	94.29	0.55	**92.75**	90.46	94.29	36.76	92.74	90.45	94.29	11.06
WOA-FFA	92.72	90.42	94.27	0.95	92.71	90.41	94.26	16.67	92.72	90.42	94.27	8.93
WOA-BAT	**92.77**	**90.60**	**94.32**	1.45	92.73	**90.51**	**94.28**	71.38	**92.77**	**90.60**	**94.32**	11.01
FFA-PSO	92.72	90.41	94.27	0.83	92.71	90.41	94.26	41.77	92.70	90.42	94.26	**7.02**
FFA-MVO	88.15	83.52	90.32	**0.51**	88.15	83.52	90.32	**38.59**	88.15	83.52	90.32	8.29
FFA-GWO	***92.76***	***90.57***	***94.31***	*0.76*	***92.74***	***90.53***	***94.29***	*50.22*	***92.76***	***90.57***	***94.31***	*10.55*
FFA-MFO	92.72	90.42	90.42	0.60	92.71	90.41	94.26	68.82	92.72	90.42	94.27	12.39
FFA-WOA	92.75	**90.57**	94.30	0.65	92.73	**90.53**	94.28	99.47	92.75	**90.57**	94.30	12.75
FFA-BAT	92.73	90.47	94.28	1.07	92.72	90.46	94.28	85.03	92.74	90.47	94.28	8.74
BAT-PSO	**92.75**	**90.46**	**94.29**	0.88	**92.75**	**90.46**	**94.29**	96.3	**92.75**	**90.46**	**94.29**	14.01
BAT-MVO	92.67	90.38	94.23	1.92	92.67	90.38	94.23	442.01	92.67	90.38	94.23	14.34
BAT-GWO	92.56	90.24	94.14	0.83	92.56	90.24	94.14	86.17	92.56	90.24	94.14	**10.83**
BAT-MFO	92.73	**90.46**	94.28	1.03	92.73	**90.46**	94.28	99.79	92.73	90.45	94.28	13.26
BAT-WOA	89.74	86.00	91.74	**0.49**	89.74	86.00	91.74	**49.94**	89.74	86.00	91.74	11.03
BAT-FFA	89.62	85.80	91.63	1.25	89.62	85.80	91.63	116.89	89.62	85.80	91.63	20.13

*Accuracy = Accu Sensitivity = Sens F-measure = F-M Time in second to build detection model = Ts

Based on obtained results from Tab. 6, it was found that PSO-BAT model with 19 features outperformed other PSO combination in terms of accuracy, sensitivity and F-measure, concerning J48, SVM and RF classifiers. In terms of building time, PSO-BAT required less time to compare all features and J48 needed the lowest time than SVM and RF. Whilst MVO-BAT model with 24 features outperformed other MVO combination and gave the same accuracy, sensitivity and F-measure of all features for all mentioned classifiers. MVO-BAT model needed less building time to compare all features and J48 needed the lowest time compared to the other classifiers. Regarding GWO combination model, the GWO-PSO and GWO-WOA models with 17 features performed better than other GWO combination and required less building time of all features, GWO-PSO and GWO-WOA models produced close accuracy, sensitivity and F-measure to all features. J48 again required less time than SVM and RF. In the case of the MFO combination, the MFO-WOA model reduces feature to 15, it outperformed other MFO combination with respect to accuracy, sensitivity and F-measure. The time required to build MFO-WOA model with J48 classifier is less than SVM and RF. The WOA-BAT model reduces feature to 19, it produces better performance compare to other WOA combination in terms of accuracy, sensitivity and F-measure. J48 needed less time to build WOA-BAT model than SVM and RF. Regarding FFA combination, the FFA-GWO with 15 features has the best performance among other FFA combination concerning the accuracy, sensitivity and F-measure for J48, SVM and RF classifiers. The FFA-GWO model builds takes less time compare to SVM and RF. Finally, BAT-PSO model reduces features to 22 and shows the best results among other BAT combination. Again J48 shows a higher efficiency relative to SVM and RF in term of needed time to build the model.

My data suggest that the proposed hybrid models improve network IDS by reducing features and time required to build a detection model. In addition to that my results show the dominance of J48 on SVM and RF in term of the required time. Concerning the features reduction and the classification, results show that the MFO-WOA and FFA-GWO models reduce features to 15 features with close accuracy, sensitivity and F-measure of all features, whereas MVO-BAT model reduces features to 24 features with the same accuracy, sensitivity and F-measure of all features for all classifiers.

6 Conclusion

Using metaheuristic algorithms can help to find optimal features sets. Hybridization of metaheuristic algorithms can reduce the number of features and improve the accuracy of the classification process with less time. Therefore, In this study, a hybrid model based on metaheuristic algorithms is developed to reduce selected features for network IDS. PSO, MVO, GWO, MFO, WOA, FFA and BAT algorithms used by this study. The proposed hybrid model was evaluated using UNSW-NB15 dataset and J48, SVM, RF classifier. The experiment conducted throughout two phases. The first phase aims to choose features through using Metaheuristic algorithm and the second phase is represented in evaluating proposed hybrid models based on R48, SVM and RF classifiers. The results obtained of the first phase showed that proposed hybrid models reduce the number of features. The results of the second phase show the dominance of J48 on SVM and RF in terms of required time to build the model. MFO-WOA and FFA-GWO models reduce features to 15 features with good classification rate. Finally, the MVO-BAT model reduces features to 24 features with the same results of all features. The proposed hybrid model is capable to detect generic attack more effectively.

Funding Statement: This work was funded by The World Islamic Sciences and Education University.

Conflicts of Interest: The author declares that they have no conflicts of interest.

References

[1] M. Adil, M. A. Almaiah, A. Omar Alsayed and O. Almomani, "An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 20, no. 8, pp. 2311–2330, 2020.

[2] A. almaiah and O. Almomani, "An investigator digital forensics frequencies particle swarm optimization for detection and classification of apt attack in fog computing environment (IDF-FPSO)," *Journal of Theoretical and Applied Information Technology*, vol. 98, no. 7, pp. 937–952, 2020.

[3] H. Rajadurai and U. D. Gandhi, "A stacked ensemble learning model for intrusion detection in wireless network," *Neural Computing and Applications*, S.I.: New Trends in Brain Computer Interface, pp. 1–9, 2020.

[4] A. El Omri and M. Rida, "An efficient network ids for cloud environments based on a combination of deep learning and an optimized self-adaptive heuristic search algorithm," *7th Int. Conf. in Networked Systems, NETYS 2019*, vol. 11704, pp. 235–249, 2019.

[5] G. Dhiman, "ESA: A hybrid bio-inspired metaheuristic optimization approach for engineering problems," *Engineering with Computers*, vol. 37, no. 1, pp. 1–31, 2019.

[6] J. Kennedy and R. Eberhart, "Particle swarm optimization," *ICNN'95—Int. Conf. on Neural Networks*, vol. 4, pp. 1942–1948, 1995.

[7] O. Almomani, "A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA algorithms," *Symmetry (Basel)*, vol. 12, no. 6, pp. 1046, 2020.

[8] F. Marini and B. Walczak, "Particle swarm optimization (PSO). A tutorial," *Chemometrics and Intelligent Laboratory Systems*, vol. 149, pp. 153–165, 2015.

[9] A. K. Al Hwaitat, M. A. Almaiah, O. Almomani, M. Al-Zahrani, R. M. Al-Sayed *et al.,* "Improved security particle swarm optimization (PSO) algorithm to detect radio jamming attacks in mobile networks," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 4, pp. 614–625, 2020.

[10] A. H. Mohammad, T. Alwada'n and O. Al-Momani, "Arabic text categorization using support vector machine, Naïve Bayes and neural network," *GSTF Journal on Computing*, vol. 5, no. 1, pp. 108–115, 2016.

[11] S. Mirjalili, S. M. Mirjalili and A. Hatamlou, "Multi-verse optimizer: A nature-inspired algorithm for global optimization," *Neural Computing & Applications*, vol. 27, no. 2, pp. 495–513, 2016.

[12] S. Mirjalili, S. M. Mirjalili and A. Lewis, "Grey wolf optimizer," *Advances in Engineering Software*, vol. 69, pp. 46–61, 2014.

[13] S. Mirjalili, "Moth-flame optimization algorithm: A novel nature-inspired heuristic paradigm," *Knowledge-Based System*, vol. 89, pp. 228–249, 2015.

[14] S. Mirjalili and A. Lewis, "The whale optimization algorithm," *Advances In Engineering Software*, vol. 95, no. 12, pp. 51–67, 2016.

[15] X. S. Yang, "Firefly algorithm, stochastic test functions and design optimisation," *International Journal of Bio-Inspired Computation*, vol. 2, no. 2, pp. 78–84, 2010.

[16] X. S. Yang, "Bat algorithm for multi-objective optimisation," *International Journal of bio-inspired computation*, vol. 3, no. 5, pp. 267–274, 2011.

[17] X. S. Yang, "A new metaheuristic bat-inspired algorithm," in *Nature Inspired Cooperative Strategies for Optimization (NICSO 2010)*, Berlin, Germany: Springer, pp. 65–74, 2010.

[18] G. Kim, S. Lee and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Systems with Applications*, vol. 41, no. 4, pp. 1690–1700, 2014.

[19] T. F. Ghanem, W. S. Elkilani and H. M. Abdul-Kader, "A hybrid approach for efficient anomaly detection using metaheuristic methods," *Journal of Advanced Research*, vol. 6, no. 4, pp. 609–619, 2015.

[20] A. S. Eesa, Z. Orman and A. M. A. Brifcani, "A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems," *Expert Systems with Applications*, vol. 42, no. 5, pp. 2670–2679, 2015.

[21] B. M. Aslahi-Shahri, R. Rahmani, M. Chizari, A. Maralani, M. Eslami *et al.,* "A hybrid method consisting of GA and SVM for intrusion detection system," *Neural Computing and Applications*, vol. 27, no. 6, pp. 1669–1676, 2016.

[22] C. Guo, Y. Ping, N. Liu and S.-S. Luo, "A two-level hybrid approach for intrusion detection," *Neurocomputing*, vol. 214, pp. 391–400, 2016.

[23] W. L. Al-Yaseen, Z. A. Othman and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," *Expert Systems with Applications*, vol. 67, no. 4, pp. 296–303, 2017.

[24] 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.

[25] L. Li, Y. Yu, S. Bai, J. Cheng and X. Chen, "Towards effective network intrusion detection: A hybrid model integrating Gini index and GBDT with PSO," *Journal of Sensors*, vol. 2018, no. 6, pp. 1–9, 2018.

[26] S. Hosseini and B. M. H. Zade, "New hybrid method for attack detection using combination of evolutionary algorithms, SVM, and ANN," *Computer Networks*, vol. 173, pp. 107–168, 2020.

[27] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman and A. Alazab, "Hybrid intrusion detection system based on the stacking ensemble of C5 decision tree classifier and one class support vector machine," *Electronics*, vol. 9, no. 1, pp. 173–191, 2020.

[28] H. Mohmmadzadeh and F. S. Gharehchopogh, "A novel hybrid whale optimization algorithm with flower pollination algorithm for feature selection: Case study Email spam detection," *Preprints*, pp. 1–28, 2020. https://doi.org/10.1111/coin.12397.

[29] N. Moustafa and J. Slay, "The evaluation of network anomaly detection systems: statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," *Information Security Journal: A Global Perspective*, vol. 25, no. 1–3, pp. 18–31, 2016.

[30] H. Faris, I. Aljarah, S. Mirjalili, P. A. Castillo and J. J. M. Guervós, "EvoloPy: An open-source nature-inspired optimization framework in python," in *8th Int. Conf. on Evolutionary Computation Theory and Applications IJCCI*, Portugal, pp. 171–177, 2016.

[31] H. Faris, A. A. Heidari, A. Z. Ala'M, M. Mafarja, I. Aljarah *et al.,* "Time-varying hierarchical chains of salps with random weight networks for feature selection," *Expert Systems with Applications*, vol. 140, no. 5, pp. 1–17, 2020.

[32] R. A. Khurma, I. Aljarah, A. Sharieh and S. Mirjalili, "EvoloPy-FS: An open-source nature-inspired optimization framework in python for feature selection," in *Evolutionary Machine Learning Techniques*, Berlin, Germany: Springer, pp. 131–173, 2020.

[33] I. Aljarah, M. Mafarja, A. A. Heidari, H. Faris, Y. Zhang *et al.,* "Asynchronous accelerating multi-leader salp chains for feature selection," *Applied Soft Computing*, vol. 71, no. 3, pp. 964–979, 2018.

[34] X. S. Yang, "Firefly algorithm," *Nature-Inspired Metaheuristic Algorithms*, vol. 20, pp. 79–90, 2008.

[35] P. Nagar, H. K. Menaria and M. Tiwari, "Novel approach of intrusion detection classification deep learning using SVM," in *Int. Conf. on Sustainable Technologies for Computational Intelligence*, Singapore: Springer, pp. 365–381, 2020.

[36] M. Madi, F. Jarghon, Y. Fazea, O. Almomani and A. Saaidah, "Comparative analysis of classification techniques for network fault management," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 28, no. 3, pp. 1442–1457, 2020.

[37] S. Aljawarneh, M. B. Yassein and M. Aljundi, "An enhanced J48 classification algorithm for the anomaly intrusion detection systems," *Cluster Computing-the Journal of Networks Software Tools and Applications*, vol. 22, no. 5, pp. 10549–10565, 2019.

[38] P. Negandhi, Y. Trivedi and R. Mangrulkar, "Intrusion detection system using random forest on the NSL-KDD dataset," *Emerging Research in Computing, Information, Communication and Applications, Springer*, vol. 906, pp. 519–531, 2019.

[39] N. Farnaaz and M. A. Jabbar, "Random forest modeling for network intrusion detection system," *Procedia Computer Science*, vol. 89, no. 1, pp. 213–217, 2016.

[40] J. R. Quinlan, *C4.5: Programs for Machine Learning*, Amsterdam, Netherlands: Elsevier, 2014.

[41] L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[42] O. Alzubi, J. Alzubi, S. Tedmori, H. Rashaideh and O. Almomani, "Consensus-Based combining method for classifier ensembles," *International Arab Journal of Information Technology*, vol. 15, no. 1, pp. 76–86, 2018.

[43] S. Smadi, N. Aslam and L. Zhang, "Detection of online phishing email using dynamic evolving neural network based on reinforcement learning," *Decision Support Systems*, vol. 107, pp. 88–102, 2018.

[44] J. Cheng, R. M. Xu, X. Y. Tang, V. S. Sheng and C. T. Cai, "An abnormal network flow feature sequence prediction approach for DDoS attacks detection in big data environment," *Computers, Materials & Continua*, vol. 55, no. 1, pp. 95–119, 2018.