Expert Systems With Applications 228 (2023) 120404

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

Sin-Cos-bIAVOA: A new feature selection method based on improved African vulture optimization algorithm and a novel transfer function to DDoS attack detection

Zakieh Sharifian [a], Behrang Barekatain [a,b,*], Alfonso Ariza Quintana [a,c], Zahra Beheshti [a,b,*], Faramarz Safi-Esfahani [a,b]

[a] Faculty of Computer Engineering, Najafabad Branch, Islamic Azad University, Najafabad, Iran
[b] Big Data Research Center, Najafabad Branch, Islamic Azad University, Najafabad, Iran
[c] E.T.S.I. Telecomunicación, Universidad de Málaga, Spain

ARTICLE INFO

Keywords:
Internet of Things (IoT)
DDoS attack
Feature selection problem
African Vulture Optimization Algorithm (AVOA)
Gravitational Fixed Radius Nearest Neighbor (GFRNN)
Compound transfer function

ABSTRACT

Internet of Things (IoT) services and devices have raised numerous challenges such as connectivity, computation, and security. Therefore, networks should provide and maintain quality services. Nowadays, Distributed Denial-of-Service (DDoS) attack is the most important network attacks according to recent studies. Among the variety of DDoS detection methods, Machine Learning (ML) algorithms have attracted researchers. In ML, the selection of optimal subset of features can have a significant role to enhance the classification rate. This problem called the feature selection problem is in the class of NP-hard problems and exact algorithms cannot obtain the best results in acceptable time. Therefore, approximate algorithms like meta-heuristic algorithms are employed to solve the problem. Since these algorithms do not search all solution space, they fall in local optima and provide a premature convergence rate. Several methods have been introduced so far to address these challenges but researchers try to find new strategies for enhancing the performance of methods. In this study, a binary Improved African Vulture Optimization Algorithm (Sin-Cos-bIAVOA) is proposed to select effective features of DDoS attacks. The method applies a novel compound transfer function (Sin-Cos) to increase exploration. To select the optimal subset of features, Gravitational Fixed Radius Nearest Neighbor (GFRNN) is employed as the classifier in the method. Moreover, AVOA is improved in three phases including exploration, balancing exploration and exploitation, and exploitation phases. Hence, Sin-Cos-bIAVOA explores promising areas to achieve the best solution and avoid the local optima traps. The proposed method's performance is compared with some recent state-of-the-art in two datasets, CIC-DDOS2019 and NSL-KDD for the DDoS attack detection. The experiment results show that the proposed method achieves the minimum feature selection rate (0.0184) with the high average accuracy (99.9979%), precision (99.9979%), recall (100.00%), and F-measure (99.9989%) compared with competitors in the first scenario with 1% attack rate in CIC-DDOS2019 dataset. In addition, the results of Friedman test based on fitness functions indicate that Sin-Cos-bIAVOA has the first rank among comparative algorithms. The source code of Sin-Cos-bIAVOA is publicly available at https://www.mathworks.com/matlabcentral/fileexchange/129409-sin-cos-biavoa-a-new-feature-selection-method.

1. Introduction

The cyber threat landscape continues to evolve at a rapid pace, with hackers launching more Distributed Denial of Service (DDoS) attacks than ever before. The first known denial of service attack occurred in 1996 when Panix Service was crippled by a hacker attack. The oldest Internet service provider was shut down for several days to an SYN flood which is an attack evolving into a DDoS attack (Brooks, Ozcelik, Yu, Oakley, & Tusing, 2021). DDoS attacks have become common over the next few years which can have several forms such as SYN flood, UDP flood, SYN-ACK-ACK flood, ICMP flood, and so on. Cisco company predicts that the total number of DDoS attacks will rise from 7.9 million

* Corresponding authors at: Faculty of Computer Engineering, Najafabad Branch, Islamic Azad University, Najafabad, Iran.
E-mail addresses: zak.sharifian@gmail.com (Z. Sharifian), Behrang_Barekatain@iaun.ac.ir (B. Barekatain), aarizaq@uma.es (A.A. Quintana), z-beheshti@iaun.ac.ir (Z. Beheshti), fsafi@iaun.ac.ir (F. Safi-Esfahani).

https://doi.org/10.1016/j.eswa.2023.120404
Received 17 January 2023; Received in revised form 1 May 2023; Accepted 5 May 2023
Available online 10 May 2023

in 2018 to almost 15.4 million by 2023 (Cisco & Internet, 2020). Meanwhile, cybercriminals benefit from the widespread use of Internet of Thing (IoT) devices. The enormous IoT networks which are included a huge number of vulnerable devices are game-changing in terms of security. In addition, most of the IoT devices have limitations due to low memory, computational power, and energy consumption. IoT applications comprise lightweight communication protocols (Omolara et al., 2022; Rana, Mamun, & Islam, 2022; Sharifian, Barekatain, Ariza Quintana, Beheshti, & Safi-Esfahani, 2022; Sheibani, Barekatain, & Arvan, 2022; Yi, Clausen, & Bas, 2012). Perceptibly, security applications and solutions entailing high computational resources cannot be applied to IoT. Intending to detect cyber threats against IoT applications, it is indispensable to be developed cyber-security mechanisms such as some traditional mechanisms firewalls, software updates, bandwidth provisioning, antivirus, intrusion detection systems (IDS), and so on (Pundir et al., 2019).

As a result, it is necessary to protect IoT networks by intellectual security mechanisms. The common methods used for intrusion detection among all existing techniques are based on data-driven anomaly detection and classification (Chou & Jiang, 2022). This technique is utilized to predict anomaly by dividing all the tuples of the dataset into binary classes; normal and attack (Ma et al., 2021). The DDoS attack is broadly detected by this approach (Eliyan & Di Pietro, 2021). The approach predicts based on a training dataset by finding a model which discriminates between distinct classes. The training classes include labeled data, and the test datasets are unlabeled. Datasets consist of several features of each packet, either benign or attack packets which compose of a network monitoring tool, such as Wireshark which observes network traffic and amasses raw packet data all through routine network operation. It must be mentioned that distinguishing between abnormal and normal traffic is dubious and hackers can manufacture malicious traffics which can be altered as benign. There are two main challenges in this detection approach. The first challenge is imbalanced datasets (Sun & Chen, 2021) and the second challenge is the selection of the best subset of features to detect DDoS attacks with high accuracy (Agrawal, Abutarboush, Ganesh, & Mohamed, 2021; Chandrashekar & Sahin, 2014).

Machine learning methods have been widely applied to DDoS attacks detection such as decision tree (Chen, Pei, & Li, 2019), random forest (Wang, Lu, & Qin, 2020), Naive Bayes (Alsirhani, Sampalli, & Bodorik, 2019), k-Nearest Neighbor (k-NN) (Aamir & Ali Zaidi, 2021), Support Vector Machines (SVM) (Pande, Khamparia, & Gupta, 2021), Neural Networks and logistic regression (Yadav & Selvakumar, 2015).

There are several intrusion network detection systems which are specifically designed for DDoS attack detection employed k-NN strategies (Dong & Sarem, 2020). The basic k-NN is a successful method to prediction (Chen & Shah, 2018; Wu et al., 2008). k-NN has a simple principle with high appraisal performance. A pattern-oriented extension of k-NN is the k Exemplar-based Nearest Neighbor (kENN) (Li & Zhang, 2011) which has generally two steps, selects the hinge positive (POS) patterns, and increases the distance between objects and Gaussian balls which leads to a closer best neighbors. Subsequently, Zhang and Li introduced a Positive-biased Nearest Neighbor (PNN) (Zhang & Li, 2013). PNN enhanced kENN by utilizing two parameters, r and k for comparing distances between the k^{th} nearest local neighbor and the r^{th} nearest POS pattern and the object. However, PNN has no training phases. Another approach in k-NN extensions is the distribution-oriented strategies such as Class Confidence Weighted k-NN algorithm (CCW-k-NN) (Liu & Chawla, 2011). This method assessed weights by Bayesian networks and assigned weights to objects as the confidence parameter. The Informative k Nearest Neighbor (Ik-NN) comprehending Locally Informative-k-NN (LIk-NN) and Globally Informative-k-NN (GIk-NN) was proposed by Song et al. (2007). The Ik-NN is a cost-sensitive method. The method outperformed several k-NN and SVM. Later, some methods were headed merging both the pattern and the distribution-oriented approaches, such as the fuzzy knowledge-based extensions of k Nearest Neighbor Algorithm (Sun & Chen, 2021). Gravitational Fixed Radius Nearest Neighbor (GFRNN) (Zhu, Wang, & Gao, 2015) is a classifier based on the Fixed Radius Nearest Neighbor search strategy (FRNN) (Bentley, 1975) and the concept of gravitation. GFRNN reduces the high time complexity by employing a fixed radius nearest neighbor search strategy to remove improper examples. These classifiers can be applied to detect DDoS attacks.

Moreover, many unrelated, inappropriate, redundant features can be removed in DDoS datasets. The selection of effective features is one of the critical and challenging problems in DDoS detection. The feature selection can enhance the classification performance due to choosing the optimal subset of features and has several benefits such as minimum consumption of resources with cost-sensitive applications, reducing execution time, increasing the detection rate, and so on (Maldonado, Riff, & Neveu, 2022). There are several feature selection strategies to find the best subset of features. Since this problem is in the class of NP-hard problems, the approximate algorithms like meta-heuristic algorithms can be employed to solve it with the lowest cost (Agrawal et al., 2021; Arivudainambi, Varun, & Sibi Chakkaravarthy, 2019; Bouzoubaa, Taher, & Nsiri, 2021; SaiSindhuTheja & Shyam, 2021).

Nowadays, in order to light computation and fast processing of intricate data of the network in different areas specifically IDS, machine learning and meta-heuristic algorithms are extensively employed to attain cost-effective performance. The hybrid supervised learning methods are utilized for DDoS attack detection and reasonable results are achieved. These methods provided better detection accuracy on zero-day attacks (Hosseini & Azizi, 2019). In a study, Artificial Bee Colony (ABC) and the AdaBoost were applied for the feature selection and classification. This research evaluated detection rate, running time, and false alarm rate. The AdaBoost algorithm is used to deal with the imbalanced dataset problem (Mazini, Shirazi, & Mahdavi, 2019). Even for real-time DDoS attack detection, several metaheuristic optimization methods are used. In the web environment (Prasad, Reddy, & Rao, 2020), the authors applied Cuckoo, Bat, and Shark optimization algorithms. Among algorithms, binary clustering cuckoo strategy achieved the best performance with the highest prediction accuracy and minimum cost overhead. Additionally, in the cloud environment, a DDoS detection model using the Random Harmony Search (RHS) optimization algorithm and Restricted Boltzmann Machine (RBM) was implemented which had significant results (Mayuranathan, Murugan, & Dhanakoti, 2021). Also, Recurrent Neural Network (RNN) was deployed for classification in DDoS attack detection problems with a concurring Lion optimization algorithm in cloud computing environment (Arivudainambi et al., 2019). A model is developed by a multi-dimensional sketch structure with a daub 4 wavelet transform for enhancing the performance of detecting LRDDoS attacks (Liu, Ren, He, Wang, & Song, 2021). In this model, the average detection time is less than other comparative methods; however, the accuracy is not as good.

The present study introduces a DDoS attack detection method. In the proposed method, AVOA is enhanced in three phases and a powerful compound transfer function, Sin-Cos, is applied to select the best subset of features. The Gravitational Fixed Radius Nearest Neighbor (GFRNN) (Zhu et al., 2015) is employed for the most accurate DDoS attack detection. The proposed method called Sin-Cos-bIAVOA is evaluated by three different scenarios with a variety of Imbalanced Ratios (IR) on CIC-DDOS2019 (Sharafaldin, Lashkari, Hakak, & Ghorbani, 2019) and NSL-KDD (Tavallaee, Bagheri, Lu, & Ghorbani, 2009) datasets. Therefore, the significant contributions of this study can be provided as follows:

- Proposing a compound Sin-Cos transfer function to enhance the population diversity
- Improving the AVOA in three phases and adapting the algorithm to the binary search space
- Applying Sin-Cos transfer function and GFRNN classier in bIAVOA to detect DDoS attacks in IoT with high accuracy

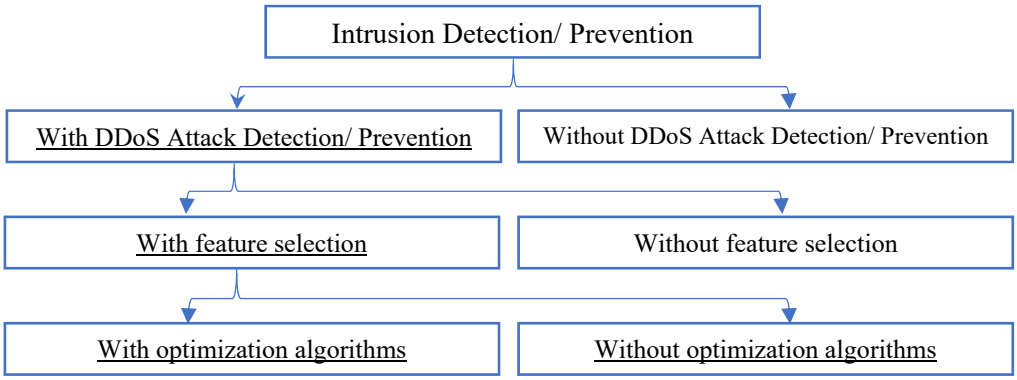

Fig. 1. Three-fold categorization of reviewed work.

- Evaluating the performance of Sin-Cos-bIAVOA by CIC-DDOS2019 and NSL-KDD datasets and comparing its results with some recent state-of-the-art feature selection and DDoS attack detection methods
- Achieving the minimal subset of features and the highest accuracy in all compared datasets by the proposed Sin-Cos-bIAVOA

This paper is structured as follows: Section 2 provides a brief explanation of the feature selectin problem. Section 3 includes a critical literature survey and Section 4 outlines the problem statement. Section 5 presents the proposed method, including a brief outline of AVOA, the details of Sin-Cos-bIAVOA's phases, the novel transfer function presenting by this research, and the employed classifier. In Section 6, the method is evaluated and the results and discussion are provided. Finally, the conclusion and feature studies are presented in Section 7.

2. Feature selection

Nowadays, the amount of generating data is exponentially growing. It leads to create datasets with high number of features and samples. Some of these features are irrelevant and have negative effect on the accuracy of classifiers. The selection of effective features is useful to avoid wasting resources during classifier training and testing. Feature selection methods try to handle the dimensionality problem by finding the most effective subset of features and eliminating the unnecessary features. The feature selection problem is an NP-hard problem (Abu Khurma et al., 2022); and the search space exponentially develops when the number of features increases. Feature selection methods are divided into three general categories namely wrapper, filters and filter-wrapper-based.

Wrappers use learning approaches to evaluate the subsets of features. Filters use data priority and evaluate its dependency one by one by generating subsets and search strategies. These methods have fewer consuming resources but they are usually less accurate than wrapper methods. The hybrid methods have the advantages of both techniques. The feature selection problem is a multi-objective problem, attempts to achieve the minimum number of selected features with maximum performance (high accuracy or low error). These objectives are in conflict with each other; therefore, researchers try to design methods that can support both objectives.

3. Related work

Many DDoS attack detection methods have been introduced to address the DoS and DDoS attacks in different networks such as IoT, Cloud, Fog, Edge, SDN, and so on. In these methods, different techniques have been applied such as Machine learning, Natural Language Processing (NLP), Artificial Neural Network (ANN), Optimization Algorithms and so on. This section mainly focuses on attack detection using classification and feature selection methods as it is depicted in Fig. 1.

Wang et al. (2020) presented a DDoS attack detection method called SBS-MLP in which they used the combination of sequential selection of features and multilayer perceptron method. They also introduced a feedback mechanism to improve the false negative rate (FNR) and false positive rate (FPR) in case of detection errors. In this research, the authors used three categories of ISOT and ISCX datasets (Saad et al., 2011) to evaluate the presented method. Each of the datasets contains five features, for each of them, the cost function of the method is calculated, in other words, training and testing operations of the neural network are performed according to the number of available features. Finally, a selected subset of all features is introduced as the best with the least number and the highest accuracy. Also, in this work, they try to update the set of selected features every time. But, when the traffic parameters are changed and the selected features are not sufficient, the method cannot distinguish the normal and attack traffics. This method has a high computational complexity because the neural network training and testing operations are performed with $O(n^2)$ complexity according to the number of features. Moreover, this method cannot guarantee finding global optimal features.

A DDoS attack detection for low rate attack was suggested (Liu et al., 2021). The authors presented a detection method by combining a multi-dimensional sketch structure with a daub 4 wavelet transform for enhancing the performance of detecting LRDDoS attack. The average detection time is less than other comparative methods; however, the accuracy is not good enough for MAWI20200501, BOUN DDoS, and SUEE8 datasets.

RM et al. (2020) highlighted a hybrid of a deep neural network, Principal Component Analysis (PCA) and Grey Wolf Optimization (GWO) algorithm namely PCA-GWO to introduce an effective Intrusion Detection System (IDS) that detects attacks in an Internet of Medical Things (IoMT). They adjusted and tuned the hyper parameters to boost the performance of the method. The method was assessed on a Kaggle dataset. The results showed an improvement in accuracy and complexity by 15% and 32%, respectively.

Roopak et al. (2020) employed the NSGA-II algorithm to select optimal features for DDoS attack detection on CICID2017 dataset. The aforementioned dataset includes 81 features and the method selected 6 features.

In another research conducted by Singh and De (2020), the authors benefited from the combination of filters for the feature selection. The proposed technique combined Information Gain, Chi Squared, Gain Ratio, Correlation Ranking, and Symmetric Uncertainty Ranking filters. Features were selected based on the total threshold value. In this research, the CAIDA2007 dataset was used, which includes 16 features, and 6 features were selected by their method. The method was implemented in MATLAB and Weka. The results were compared with similar methods, which obtained the best result by obtaining 98.3% accuracy.

Aamir and Ali Zaidi (2021) tried to prevent DDoS attack using a clustering-based semi-supervised voting-based machine learning

Table 1
The related works for the DDoS Attack Detection.

Reference	Feature Selection/ Detection Method	System/ Object	Feature Selection Rate	Description	Dataset	Accuracy %
(Wang et al., 2020)	MLP	DDoS	12/31	High Fault tolerance High complexity No guarantee to find optimized global features	NSL-KDD ISOT - ISCX	97.66
(Liu et al., 2021)	Detection low-rate DDoS Sketch + Daub 4 wavelet transform	LDDoS	–	Threshold and filtering methods	MAWI20200501 + BOUN DDoS + SUEE8	98
(Roopak et al., 2020)	NSGAII, ELM	IDS	6/41	Best performance among other compared method Evaluate the method by just one dataset	CICID 2017	99.9
(Singh & De, 2020)	Filtering Gain, Chi-Squared, Gain Ratio, Correlation ranking filter, RiliefF, SVM	DDoS	6/16	Filtering method is applied to solve the feature selection problem Evaluate the method by just one dataset	CAIDA2007	98.3
(Wang et al., 2020)	MLP	IoT/ DDoS	6/12	High complexity in the process of feature selection	ISCX – ISOT NSL-KDD	99.9
(Aamir & Ali Zaidi, 2021)	Clustering based Semi-Supervised-ML (KNN, SVM & RF)	–	35/41	No guarantee for inline traffic flow detection, Evaluating the method by just one dataset	CICIDS2017	96.6
(Pande et al., 2021)	ML (SVM, perceptron, KNN, stochastic gradient descent, and XGBoost)	WSN/ DoS	11/41	Taking more time than usual for online traffic flow detection	KDD	99.87
(Kshirsagar & Kumar, 2021)	information gain (IG) and correlation (CR), J48 classifier	IDS	14/82	A feature reduction method using information gain (IG) and correlation (CR) feature selection techniques to DDoS attack detection	CICDoS 2019 and KDD Cup 1999	99.9
(Sanchez et al., 2021)	analysis of Variance (ANOVA) to identify and rank features,	IoT/ DDoS	28/76	A feature reduction approach for DL-based DDoS detector using the Analysis of Variance (ANOVA)	ISCXIDS 2012, CICIDS 2017, CSE-CIC-IDS 2018, and CICDDoS 2019	99.93
(SaiSindhuTheja & Shyam, 2021)	CSA, OBL, RNN	Cloud/ DDoS	10/41	The feature selection using the OCSA algorithm and RNN as the classifier	KDD cup 99	94.12
(Varma et al., 2021)	RF, WOA	IoT/ DDoS	11/80	Feature selection using Whale Optimization Algorithm (WOA) and RF as classifier	CICDDOS2019	99.92
(Fatani et al., 2021)	CNNs, TSO, DE	IoT/IDS	–	Having the high cost of calculations	KDDCup-99, NSL-KDD, BoT-IoT, and CICIDS-2017	99.6
(Kumar, Kumar, Gupta, & Tripathi, 2021)	RF + XGBoost	Fog/ DDoS	10/19	A distributed framework for detecting DDoS attacks using leveraging fog computing in smart contract-based Blockchain-IoT systems	BoT-IoT	99.9
(Golchin, Kundel, Steuer, Hark, & Steinmetz, 2022)	Ensemble Feature Selection (Pearson correlation filtering)	DDoS	34/71	Using filtering methods to DDoS attacks	CICDDoS2019	–
(Kim, Kim, & Kim, 2022)	DT, RF, k-NN and stacking algorithm for the feature selection	IoT/ DDoS	10/55	Creating an experimental environment and structure for 5G network, using DT, RF, k-NN machine learning techniques and stacking method to detect attacks	Generated Data by Tools	91
(Khanday, Fatima, & Rakesh, 2023)	A lightweight IDS with a new data pre-processing technique	IoT/ DDoS	20/46	Extraction of traffic patterns with DDoS attack label vs. all attack labels by the proposed feature selection method and classified by deep learning and machine learning classifiers	BOT-IoT and TON- IoT	99.9

mechanism and optimized values based on the feedback from k-fold cross-validation. The algorithm was evaluated based on five different classifiers such as Random Forest (RF) and Support Vector Machine (SVM) on CICIDS2017 dataset. The best accuracy was attained for Random Forest which was about 96%.

A stack of five feature selections is introduced by Pande et al. (2021). They combined SVM, perceptron, K-nearest neighbor, stochastic gradient descent, and XGBoost for detection DDoS attack by testing their method with the KDD dataset. The best results were achieved with eleven features. Even they claimed the aim of reduction time is fulfilled, the duration time of the operation is still high which is not suitable for such attacks that have to detect online.

In another research, a framework based on Combination of Information Gain (IG), Correlation (CR), and J48 classifier was introduced (Kshirsagar & Kumar, 2022). The proposed method evaluated their DDoS detection method by the CICDDoS2019 dataset. The framework is implemented by Weka. The authors claimed the minimum and maximum feature reduction by 56% and 82%, respectively.

Sanchez et al. (2021) suggested DLDDoS. The proposed method is a combination of a Feed-Forward NN and Analysis of Variance for feature selection to reduce input data. They used ISCXIDS 2012, CICIDS 2017, CSE-CIC-IDS 2018, and CICDDoS 2019 datasets for assessing their method. The method achieved 97.473–99.932 detection accuracy.

A combined DDoS detection method (SaiSindhuTheja & Shyam, 2021) was introduced using an Improved Crow Search Algorithm (ICSA) and the Opposition Based Learning (OBL) and the Recurrent Neural Network (RNN) as its classifier. The results showed that the performance of the proposed method is the best among other compared methods. A DDoS detection method (Varma, Raju, Ruthala, & Suresh, 2021) was designed based on Whale Optimization Algorithm (WOA) and several classifiers namely RF, J48 trees, Naïve Bayes and MLP to select the best subset of features of the CIC-DDOS2019 dataset. In this research, the best detection accuracy was about 99.92% with reducing the number of features from 80 to 11. In another study (Fatani, Elaziz, Dahou, Al-qaness, & Lu, 2021), the Convolutional Neural Networks (CNNs) and the Transient Search Optimization (TSO) algorithm were employed to select effective features of KDDCup-99, BoT-IoT, NSL-KDD, and CICIDS-2017 datasets. The results showed substantial improvement in some of the scenarios. A brief review of mentioned researches and other related works is provided in Table 1.

4. Problem statement

The IoT faces various challenges due to its different characteristics

Algorithm 1: Pseudocode of AVOA

Inputs: The population size N and maximum number of iterations ($Maxiterations$)
Outputs: The position of Best Vulture and its fitness value
Initialize the random population x (i = 1,2, ..., N)
while $iteration < Maxiterations$ **do**
    Calculate the fitness values of Vulture
    Select $BestVulture_1$ and $BestVulture_2$
    Divide the other $Vultures$ into groups
    for (each Vulture (x)) **do**
        Select R
        Update the F using $F = (2 \times rand() + 1) \times z \times \left(1 - \frac{iteration}{maxiterations}\right) + t$
        if (|F| ≥ 1) **then** % **Exploration phase**
            if ($P_1 \geq rand()$) **then**
                Update the position Vulture using $x = R - D \times F$
            else
                Update the position Vulture using $x = R - F + rand() \times ((ub - lb) \times rand() + lb)$
        if (|F| < 1) **then** % **Exploitation phase**
            if (|F| ≥ 0.5) **then**
                if ($P_2 \geq rand()$) **then**
                    Update the position Vulture using $x = D \times (F + rand()) - d$
                else
                    Update the position Vulture using $x = R - (S_1 + S_2)$
            else
                if ($P_3 \geq rand()$) **then**
                    Update the position Vulture using $x = \left(\frac{A_1 + A_2}{2}\right)$
                else
                    Update the position Vulture using $x = R - |d| \times F \times Levy(d)$
return $BestVulture_1$

Fig. 2. The pseudocode of AOVA (Abdollahzadeh et al., 2021).

and novelty of related technologies and standards; hence, the attentions of many researchers have been attracted toward this new technology. One of the most important challenges in the IoT is the security due to many attacks. For example, the most frequent and costly attack is the DDoS attack (Akgun, Hizal, & Cavusoglu, 2022). To tackle these challenges, researches are trying to proposed methods for detecting and preventing the DDoS attack. Regarding the characteristics of DDoS attack, it is possible to select effective features from traffic flows in order to detect the attack more accurate. Also, the choosing an optimal subset of features has a lower cost for the system. The feature selection problem is known as an NP-hard optimization problems (Amaldi & Kann, 1998) because $2^n - 1$ subsets (excluding empty set) are evaluated to achieve the optimal subset. Since this problem is in the class of NP-hard problems, approximate algorithms are able to solve it in a reasonable time. But, these algorithms do not return the exact result; therefore, several methods have been proposed to enhance the results so far (Beheshti, 2021, 2022; Houssein, Oliva, Çelik, Emam, & Ghoniem, 2023; Hu, Pan, Song, Wei, & Shen, 2023; Karthick Kumar, Vadivukkarasi, Dayana, & Malarvezhi, 2022; Kaushik, Sharma, Dhama, Chadha, & Sharma, 2023), and this problem is still a hot research topic. Among the approximate algorithms, binary meta-heuristic algorithms have shown significant results in the feature selection problem (Altarabichi, Nowaczyk, Pashami, & Mashhadi, 2023; Alzaqebah, Aljarah, & Al-Kadi, 2023; Sahu, Singh, & Nirala, 2023; Xu et al., 2023; Yedukondalu & Sharma, 2023). In these algorithms, a proper transfer function and a powerful search strategy have key roles to achieve the best results and to avoid the local optimum (Ahmed, Ghosh, Mirjalili, & Sarkar, 2021; Guo, Wang, & Guo, 2020; He, Zhang, Mirjalili, & Zhang, 2022; Mirjalili & Lewis, 2013). In the next section, the proposed method, Sin-Cos-bIAVOA, is introduced based on a novel transfer function and an improved version of AVOA to achieve these goals.

5. Sin-Cos-bIAVOA: the proposed method

This study introduces a wrapper feature selection method based on the binary improved AVOA. The aim in the proposed method is to reduce the classification error and select the minimum effective features. The AVOA obtains the result during the exploration and exploitation phases. The algorithm swaps between two phases based on the random function *F*. Since these phases are randomly selected, the algorithm has no good performance in different phases. Hence, the phases in the improved AVOA are carried out in three separate phases, exploration, balancing exploration and exploitation and exploitation. Then, the improved AVOA (IAVOA) is mapped to the binary search by a novel compound Sin-Cos transfer function. The method called Sin-Cos-bIAVOA is applied for the feature selection of DDoS attack datasets.

5.1. A brief overview of African vulture Optimization algorithm (AVOA)

The African Vulture Optimization Algorithm (AVOA) (Abdollahzadeh, Gharehchopogh, & Mirjalili, 2021) is motivated by vultures' lifestyle as carnivorous birds with the purpose of foraging behavior. The algorithm simulates how these birds search for food resources, and fight in the different groups of vultures with each other for more food. The vultures are divided into two groups, first, the birds, which are more powerful, eat the best food and the other group eat the leftover flesh of the stronger group's food. The number of vultures in an environment is simulated as the population (*N*) in AVOA. The pseudocode of AOVA has

Algorithm 2: Pseudocode of Sin-Cos-bIAVOA

1: **Inputs:** population size (N), Dimension (D), and maximum number of iterations ($Maxiterations$)
2: **Outputs:** The position of Best Vulture and $BestVulture_1$
3: Initialize the random population x_{ij} (i = 1,2, ..., N), (j = 1,2, ..., D)
4: **while** $iteration < Maxiterations$ **do**
5: **Call Sin-Cos Transfer Function**
6: Calculate the fitness values of Vultures
7: Select $BestVulture_1$ and $BestVulture_2$
8: Divide the other $Vultures$ into groups
9: **for** (each Vulture (x_i)) **do**
10: **if** $iteration < Maxiterations/3$ **then**
11: **Call Exploration Function**
12: **if** $iteration \geq Maxiterations/3$ and $iteration \leq 2Maxiterations/3$ **then**
13: Compute $WorstVulture$
14: $prob = \frac{f(x_i)-f(WorstVulture)}{f(BestVulture_1)-f(WorstVulture)}$
15: **if** $prob$ f 0.4 **then**
16: **Call Exploitation Function**
17: **else**
18: **Call Exploration Function**
19: **else**
20: **Call Exploitation Function**
21: **endfor**
22: **endwhile**
23:. **return** $BestVulture_1$

Fig. 3. The pseudocode of Sin-Cos-bIAVOA.

been shown in Fig. 2.

After initializing, the fitness values are computed, and the best vulture is selected as the best vulture of the first group ($BestVulture_1$) and the second-best vulture is chosen as the best vulture of the second group ($BestVulture_2$). The other vultures move to the first or second group based on the Roulette wheel mechanism (Abdollahzadeh et al., 2021). The parameter F, as the vultures are satiated, is calculated as follows:

$$F = (2 \times rand() + 1) \times \text{ } \times \left(1 - \frac{iteration}{maxiterations}\right) + \text{ } \quad (1)$$

where *iteration* is the current iteration and *maxiterations* is the maximum number of iterations. *rand*() is a random number in [0,1]. donates a random number in [-1,1]. If is bigger than 0, vulture is satiated; otherwise, if is less than 0, the vulture is starved. The vultures fly towards resources to find the food. When the vultures have not had enough energy, they will fight with their neighbors and the stronger ones get the food. The behavior is modeled by as follows:

$$= \left(\times \left(sin^{w}\left(\frac{\pi}{2} \times \frac{iteration}{maxiterations}\right)\right) + cos\left(\frac{\pi}{2} \times \frac{iteration}{maxiterations}\right) - 1\right) \quad (2)$$

where is a random number in [-2,2] and w is set to a fixed number set. $Sin(.)$ and $Cos(.)$ are Sine and Cosine functions, respectively. When $|F| \geq 1$, the algorithm explores the space to find the new spaces (Exploration phase) and If $|F|\langle 1$, the algorithm exploits around the good solutions (Exploitation phase).

In the **exploration phase**, the vultures' positions are updated as follows:

$$x = \begin{cases} R - D \times F & if p_1 \geq rand() \\ R - F + rand() \times ((ub - lb) \times rand() + lb) & if p_1 < rand() \end{cases} \quad (3)$$

where R is one of the best vultures in the current iteration, p_1 is a constant value and is set to 0.6. *ub* and *lb* are the upper and lower bounds of problem. D is computed as follows:

$$D = |2rand() \times R - x| \quad (4)$$

In the **exploitation phase**, the vultures' positions are updated as follows:

if $|F| > 0.5$ then

$$x = \begin{cases} D \times (F + rand()) - d & if p_2 \geq rand() \\ R - (S_1 + S_2) & if p_2 < rand() \end{cases} \quad (5)$$

else

$$x = \begin{cases} \left(\frac{A_1 + A_2}{2}\right) & if p_3 \geq rand() \\ R - |d| \times F \times Levy(d) & if p_3 < rand() \end{cases} \quad (6)$$

where R is one of the best vultures in the current iteration, p_2 and p_3 are constant values and set to 0.4 and 0.6, respectively. d is the distance of the vulture to one of the best vultures of the two groups. $Levy(d)$ is Levy flight (X.-S. Yang, 2010). S_1, S_2, A_1, and A_2 are computed as follows:

$$S_1 = R \times \left(\frac{rand() \times x}{2\pi}\right) \times cos(x) \quad (7)$$

Algorithm 3: Pseudocode of Exploration Function

Function Exploration
Inputs: *All parameters,* Vultures' positions (x)
if P_1 f $rand()$ **then**
    $x = R - D \times F$
else
    $x = R - F + rand() \times \left((ub - lb) \times rand() + lb\right)$
return x

Fig. 4. The pseudocode of Exploration phase.

$$S_2 = R \times \left(\frac{rand() \times x}{2\pi}\right) \times sin(x) \tag{8}$$

$$A_1 = BestVulture_1 - \frac{BestVulture_1 \times x}{BestVulture_1 - x^2} \times F \tag{9}$$

$$A_2 = BestVulture_2 - \frac{BestVulture_2 \times x}{BestVulture_2 - x^2} \times F \tag{10}$$

where $BestVulture_1$ and $BestVulture_2$ are the best and the second best positions in the current iteration.

5.2. The phases of Sin-Cos-bIAVOA

Sin-Cos-bIAVOA is designed in three phases. In the first phase, the algorithm explores new promising spaces to avoid the premature convergence rate and falling in the local optima. In the second phase, the algorithm gradually switches from exploration to exploitation and in the last phase, Sin-Cos-bIAVOA exploits around the good solutions to achieve the best solution. The details of different steps of algorithm are shown in Fig. 3. After initializing the population, the Sin-Cos transfer function is invoked to generate binary positions.

All fitness functions are calculated, and $BestVulture_1$, and $BestVulture_2$ as the best and the second best fitness are computed. The population searches the space in the exploration phase to find new space.

- **Exploration phase**

If $iteration < Maxiterations/3$; the algorithm is in the exploration phase. The positions' Vultures are updated based on Eq. (3) and new positions are generated. The pseudocode of Exploration phase has been shown in Fig. 4.

- Balancing exploration and exploitation phase

When $iteration \geq Maxiterations/3$ and $iteration \leq 2Maxiterations/3$, the algorithm gradually switches from exploration to exploitation. In this phase, the worst fitness ($WorstVulture$) is computed and the distance of the current vulture (x_i) from the best solution ($BestVulture_1$) is obtained as follows:

$$prob = \frac{f(x_i) - f(WorstVulture)}{f(BestVulture_1) - f(WorstVulture)} \tag{11}$$

where $f()$ is fitness value. $f(BestVulture_1)$ and $f(WorstVulture)$ are the fitness of the best and worst solutions.

The $prob$ is in the range of [0,1]. If the current vulture (x_i) is near the best solution, the $prob$ will be close to one. Meanwhile, the current vulture (x_i) is close to the worst solution, the $prob$ will be near zero. If $prob \succ 0.4$, the Exploitation function is called; otherwise, the Exploration function is called to balance the exploration and exploitation in this phase.

- Exploitation phase

If $iteration > 2Maxiterations/3$; the algorithm is in the exploitation phase. The positions' Vultures are updated based on Eqs. (5) and (6) and new positions are obtained. The pseudocode of this phase has been

Algorithm 4: Pseudocode of Exploitation Function

Function Exploitation
Inputs: *All parameters,* Vultures' positions (x)
if $|F|$ p 0.5 **then**
    if P_2 f $rand()$ **then**
        $x = D \times (F + rand()) - d$
    else
        $x = R - (S_1 + S_2)$
if $|F| \geq 0.5$ **then**
    if P_3 f $rand()$ **then**
        $x = \left(\frac{A_1 + A_2}{2}\right)$
    else
        $x = R - |d| \times F \times Levy(d)$
return x

Fig. 5. The pseudocode of Exploitation phase.

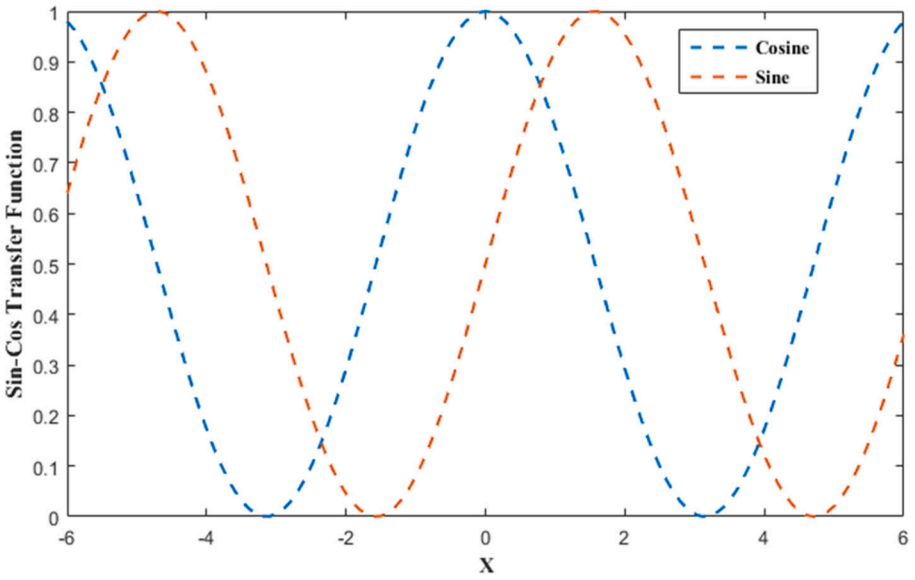

Fig. 6. The Sin-Cos Transfer Function.

Algorithm 5: Pseudocode of Sin-Cos Transfer Function

Function Sin-Cos
Inputs: Vultures' positions (x), dimension

1. **for** $j=1$ to *dimension* **do**
2. $S_1(x_{ij}) = Cos(x_{ij}) / 2 + 0.5$
3. **if** $S_1(x_{ij})$ p $rand_1()$ **then**
4. $x'_{ij} = 1$
5. **else**
6. $x'_{ij} = 0$
7. $S_2(x_{ij}) = \mathrm{Sin}(x_{ij}) / 2 + 0.5$
8. **if** $S_2(x_{ij})$ p $rand_2()$ **then**
9. $x''_{ij} = 1$
10. **else**
11. $x''_{ij} = 0$
12. Compute Fitness value $x'_i : f(x'_i)$
13. Compute Fitness value $x''_i : f(x''_i)$
14. **if** $f(x'_i)$ **is better than** $f(x''_i)$
15. $x_i = x'_i$
16. $f(x_i) = f(x'_i)$
17. **else**
18. $x_i = x''_i$
19. $f(x_i) = f(x''_i)$
20. **End**
21. **return** $x_i, \quad f(x_i)$

Fig. 7. The pseudocode of Sin-Cos Transfer function.

illustrated in Fig. 5.

According to Fig. 5, the compound Sin-Cos transfer function is run once per iteration. Therefore, the time complexity of proposed method is $O(T \times N \times D)$. T shows the maximum number of iterations, N, and D represent the population size and the number of dimensions, respectively.

5.3. The compound Sin-Cos transfer function

In this section, a novel compound transfer function is introduced to convert continuous positions to the binary ones. The transfer function improves the exploration capability in BAVOA by generating the high diversity population. The transfer function called Sin-Cos has been shown in Fig. 6. It employs the following functions and rules to convert the continuous search space to the binary one:

$$S_1(x_{ij}) = Cos(x_{ij})/2 + 0.5 \tag{12}$$

$$x'_{ij} = \begin{cases} 1 & if\ rand_1() < S_1(x_{ij}) \\ 0 & if\ rand_1() \geqslant S_1(x_{ij}) \end{cases} \tag{13}$$

$$S_2(x_{ij}) = Sin(x_{ij})/2 + 0.5 \tag{14}$$

$$x''_{ij} = \begin{cases} 1 & if\ rand_2() < S_2(x_{ij}) \\ 0 & if\ rand_2() \geqslant S_2(x_{ij}) \end{cases} \tag{15}$$

$$x_i = \begin{cases} x'_i & if\ f(x'_i)\ is\ better\ than\ f(x''_i) \\ x''_i & if\ f(x''_i)\ is\ better\ than\ f(x'_i) \end{cases} \tag{16}$$

where x_{ij} is the current continuous position of the i^{th} vulture in the j^{th} dimension, and $f(.)$ is the fitness function. $Sin(.)$ and $Cos(.)$ are Sine and Cosine functions, respectively.

The functions $Sin(.)$ and $Cos(.)$ generate two values in the range of [0,1] and according to Eq. (12) and Eq. (14), two new binary positions are created. The best position based on their fitness values is selected as x_i (the new position in the binary search space).

Two functions $Sin(.)$ and $Cos(.)$, and rules produce various solutions and improve the exploration of algorithm. Fig. 7 shows the pseudocode of the Sin-Cos transfer function.

5.4. The fitness function

As mentioned, the feature selection problem is a multi-objective optimization problem. The aim in the problem is to select the optimal subset of features with the maximum accuracy (or minimum error). The multi-objective fitness function can be designed as a single-objective function as follows:

$$Fitness = \alpha.ClassificationError + \beta.\frac{NumberofSelectedFeatures}{Total\quad Features} \tag{17}$$

where the ratio of the number of selected features to the total features is defined as feature selection rate. Parameters α and β are limited between [0,1] and $\beta = \alpha - 1$.

The Sin-Cos-bIAVOA generates binary solutions vectors (vultures' positions). Each element in the vectors is one or zero. One shows the feature has been selected and zero is vice versa. The selected features are evaluated by a classifier and the accuracy or error of classification is determined. The classifier used in this study is Gravitational Fixed Radius Nearest Neighbor (GFRNN).

5.5. The Classifier-Gravitational Fixed Radius Nearest Neighbor (GFRNN)

GFRNN Zhu et al. (2015) is a learning algorithm based on gravitational rules. The algorithm has a simple structure and applies for the imbalanced data. Since the DDoS attack datasets are usually in the class of imbalanced data, GFRNN has been selected as the classifier in this study. The DDoS attack datasets are classified as majority (normal) class or minority (attack) class. GFRNN chooses a candidate set ($X_{Candidate}$) based on Fixed Radius Nearest Neighbor (FRNN) algorithm for every test sample y.

The gravitational forces acting on y, $F(y)$, is calculated based on the following equations and the class of y is determined. If $F(y) < 0$, y is classified in the majority class; otherwise, y belongs to the minority class. Each member of $X_{Candidate}$, x_i, has a mass (m_{x_i}) computed as follows:

$$m_{x_i} = \begin{cases} IR & x_i \in X_{minority} \cap X_{Candidate} \\ 1, & x_i \in X_{majority} \cap X_{Candidate} \end{cases} \tag{18}$$

$$IR = \frac{N_{majority}}{N_{minority}} \tag{19}$$

where IR is called Imbalanced Ratio and calculated based on the number of majority samples ($N_{majority}$) and the number of minority samples ($N_{minority}$). If x_i belongs to the minority class, m_{x_i} is IR; otherwise, it is one.

$$F(y) = \sum_{i=1,2,\cdots,x_i} \varphi_i D(y, x_i), x_i \in X_{Candidate} \tag{20}$$

$$D(y, x_i) = G\frac{m_y m_{x_i}}{d(y, x_i)^2} \tag{21}$$

where x_i is a member of $X_{Candidate}$ and m_{x_i} is its mass. m_y is the mass of y. $d(y, x_i)^2$ shows the Euclidian distance between y and x_i. φ_i is a constant value and is set to 1 for the minatory samples and is set to -1 for the majority samples. G is also the Gravitational constant and is set to 1.

Table 2
Parameter settings of algorithms.

Algorithms	Parameter/Value
Population size (N)	30
Maximum number of iterations	100
Number of independent runs	16
Search dimension	[0,1]
Fitness function	$\alpha = 0.99$, $\beta = 0.01$ (Beheshti, 2021; Mafarja, Eleyan, Jaber, Hammouri, & Mirjalili, 2018)
All BAVOAs	$\alpha = 0.8$, $\beta = 0.2$, γ=2.5
BSSA	C1, C2 = [0,1]
QBHHO	$\beta = 1.5$
BGWO	a $\in$ [0,2]
BDE	$\beta = 1.5$
BASO	$\alpha = 50$, $\beta = 0.2$, $\varepsilon = 0.001$
SBS	Decision Variables Matrix Size = Number of Features
GA	Crossover Percentage = 0.8, Mutation Percentage = 0.3, Mutation Rate = 0.05, Selection Pressure = 8

6. Experimental results

In this section, Sin-Cos-bIAVOA's performance is compared with some state-of-the-art methods to select optimal subset features for the DDoS attack detection. Other compared methods are binary AVOA algorithms with different transfer functions such as Quadratic (Jordehi, 2019) (QbAVOA), V-Shaped (Mirjalili & Lewis, 2013) (VbAVOA), and U-Shaped (Mirjalili & Lewis, 2013) (UbAVOA).

Also, some recent well-known binary meta-heuristic algorithms introduced for the feature selection problem have been chosen for comparison with the proposed method such as Binary Salp Swarm Algorithm (BSSA) (Rizk-Allah, Hassanien, Elhoseny, & Gunasekaran, 2019), Quadratic Binary Harris Hawk Optimization (QBHHO) (Too, Abdullah, & Mohd Saad, 2019), binary Grey Wolf Optimizer (bGWO) (Emary, Zawbaa, Hassanien, & Ella, 2016), Binary Differential Evolution (BDE) (Zhang et al., 2020), and Binary Atom Search Optimization

Table 3
The details of the Datasets in three scenarios

Scenario No.	Dataset	Attack rate	Number of normal records	Number of Attack records	Imbalance Ratio	Number of features	Number of classes
1	CIC-DDOS2019	1%	9900	100	99	71	2
2	CIC-DDOS2019	4%	9600	400	24	71	2
3	NSL-KDD	46.6%	13,449	11,743	1.1	41	2

(BASO) (Too & Rahim Abdullah, 2020).

The GFRNN classifier is used for the DDoS attack detection in the mentioned methods. Moreover, Sin-Cos-bIAVOA is compared with the feature selection methods of hybrid GA and MLP (GA-MLP) (Yang & Honavar, 1998), a dynamic MLP-based feature selection method and feedback (SBS-MLP) (Wang et al., 2020), and a dynamic GFRNN-based feature selection method and feedback (SBS-GFRNN).

All these algorithms are run on two IoT intrusion datasets, where each dataset is divided into two parts; training and testing sets, where 70% of each dataset is applied for training and the remaining 30% is for testing purposes. The parameter settings of algorithms are based on their references as shown in Table 2.

The experiments are performed by MATLAB 2018 on the portable computer with Intel Core i7-11370H CPU@ 3.30 GHz, 3302 Mhz, 4 Core (s), 8 logical processors, 16.0 GB RAM, and Microsoft Windows 11 Enterprise.

6.1. The description of the datasets

The proposed method is design to detect the DDoS attack evaluated by CIC-DDOS2019 (Sharafaldin et al., 2019) and NSL-KDD (Tavallaee et al., 2009) datasets. These datasets are the benchmark datasets widely used in recent studies. The Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick (UNB) created the CIC-DDOS 2019 labeled dataset. This dataset is generated by keeping realistic background traffic; the developers have used an abstract behavior of human interactions and generated normal traffic. Packets using the TCP connection can be distinguished from the TCP packets by the SYN, ACK, PSH, RST, URG, FIN, ECE, and CWR flag sections in the header elements. This dataset contains 85 features along with label attributes and both attack and normal data. This dataset is divided into training data and test data. Also, two scenarios are designed with different attack rates 1% and 4% for the dataset. In this dataset, some of the columns are redundant; hence, the number of features is turned to 72 including the label column.

The NSL-KDD dataset contains Internet traffic records, which includes 42 features in each record, 41 of which refer to the traffic input, and the last feature is the normal and attack labels. NSL-KDD is an improved version of the KDD'99 dataset (Tavallaee et al., 2009). The NSL-KDD dataset has no redundant records but the KDD'99 dataset includes duplicate records (Tavallaee et al., 2009). The details of datasets are demonstrated in Table 3. In the table, the dataset name, the attack rate, the number of normal and attack records, Imbalance Ratio (*IR*), the number of features and classes are illustrated. *IR* shows the imbalanced level of dataset based on the ratio of the number of records in the majority and minority classes. The classification of datasets with the higher imbalanced ratio is more difficult for classifiers.

6.2. Results and discussion of the proposed method

To evaluate the proposed method's performance, several metrics are applied in this study such as Accuracy, Precision, Recall, F-measure and the Feature Selection Rate defined as follows:

$$Accuracy = \frac{TN + TP}{TN + TP + FN + FP} \tag{22}$$

$$Precision = \frac{TP}{TP + FP} \tag{23}$$

$$Recall = \frac{TP}{TP + FN} \tag{24}$$

$$F - measure = 2^{*}\frac{Precision.Recall}{Precision + Recall} \tag{25}$$

$$Feature\ Selection\ Rate = \frac{Number\ of\ Selected\ Features}{Total\ Features} \tag{26}$$

where *TP* is the number of DDoS attack records correctly classified, *TN* is the number of normal records correctly classified, *FN* and *FP* are the number of DDoS attack records and normal records which are wrongly classified.

The results of algorithms on datasets are provided in Table 4 to Table 10. In these tables, the best results are illustrated in bold. The results of algorithms for CIC-DDOS2019 dataset with Attack Rate = 1% and Attack Rate = 4% are shown in Table 4 and Table 5, respectively. Since *IR* is very high in the dataset, the GFRNN classifier is applied in all binary AVOAs, BSSA, QBHHO, bGWO, BDE, and BASO for fair comparison. Also, their performance of algorithms are compared with GA-MLP (Yang & Honavar, 1998), SBS-GFRNN, and SBS-MLP (Wang et al., 2020). The results show that the proposed method, Sin-Cos-bIAVOA, performs well compared with other comparative algorithms in terms of solution accuracy, precision, recall, F-measure, and feature selection rate.

Sin-Cos-bIAVOA achieves the minimum feature selection rate which

Table 4
Results on CIC-DDOS2019 dataset, Scenario 1– Attack Rate = 1%.

CIC-DDOS2019 Dataset – Attack Rate = 1%						
Algorithm	Average Fitness	Average Accuracy (%)	Average Precision (%)	Average Recall (%)	Average F-Measure (%)	Average Feature Selection Rate
Sin-Cos-bIAVOA	**0.0002**	**99.9979**	**99.9979**	**100.0000**	**99.9989**	**0.0185**
QbAVOA	0.0135	98.8531	98.8816	99.9598	99.4178	0.2183
VbAVOA	0.0107	99.0438	99.3668	99.6700	99.5182	0.1215
UbAVOA	0.0109	99.0625	99.0845	99.9681	99.5243	0.1637
BSSA	0.0186	98.5896	98.6209	99.9531	99.2825	0.4604
QBHHO	0.0156	98.7229	98.7558	99.9532	99.3508	0.2914
bGWO	0.0201	98.5146	98.5412	99.9573	99.2442	0.5396
BDE	0.0187	98.5917	98.6275	99.9489	99.2838	0.4780
BASO	0.0147	98.7250	98.7812	99.9298	99.3522	0.2033
SBS-GFRNN	0.0054	99.5146	99.1244	69.5683	81.7571	0.0563
SBS-MLP	0.0030	99.7563	86.7188	90.1061	88.3800	0.0563
GA-MLP	0.0045	99.8958	97.0695	93.2432	95.1179	0.3493

Table 5
Results on CIC-DDOS2019 dataset, Scenario 2– Attack Rate = 4%.

CIC-DDOS2019 Dataset – Attack Rate = 4%						
Algorithm	Average Fitness	Average Accuracy (%)	Average Precision (%)	Average Recall (%)	Average F-Measure (%)	Average Feature Selection Rate
Sin-Cos-bIAVOA	**0.0003**	**99.9813**	**99.9848**	**99.9956**	**99.9902**	**0.0150**
QbAVOA	0.0147	98.7458	98.8354	99.8554	99.3428	0.2315
VbAVOA	0.0132	98.8229	98.8974	99.8751	99.3838	0.1532
UbAVOA	0.0127	98.8833	98.9319	99.9036	99.4154	0.1673
BSSA	0.0195	98.5000	98.5910	99.8440	99.2136	0.4621
QBHHO	0.0161	98.7104	98.7909	99.8641	99.3246	0.3371
bGWO	0.0216	98.3542	98.4476	99.8351	99.1365	0.5273
BDE	0.0187	98.5750	98.6413	99.8726	99.2531	0.4577
BASO	0.0161	98.5870	98.6495	99.8769	99.2594	0.2130
SBS-GFRNN	0.3678	99.6292	98.9298	92.7927	95.7630	0.0704
SBS-MLP	0.0420	99.9583	99.2649	99.7190	99.4914	0.0704
GA-MLP	0.0041	99.8145	99.8059	99.5505	99.6780	0.2254

Table 6
Results on NSL-KDD dataset, Scenario 3.

NSL-KDD Dataset						
Algorithm	Average Fitness	Average Accuracy (%)	Average Precision (%)	Average Recall (%)	Average F-Measure (%)	Average Feature Selection Rate
Sin-Cos-bIAVOA	**0.0074**	**99.4245**	**99.2949**	**99.6348**	**99.4645**	**0.0038**
QbAVOA	0.0093	99.3699	99.2517	99.5733	99.4123	0.0048
VbAVOA	0.0089	99.3600	99.2539	99.5526	99.4030	0.0040
UbAVOA	0.0093	99.3736	99.1964	99.6357	99.4155	0.0040
BSSA	0.0106	99.3612	99.1682	99.6374	99.4023	0.0046
QBHHO	0.0095	99.3302	99.1886	99.5610	99.3744	0.0038
bGWO	0.0123	99.2645	99.0264	99.6010	99.3128	0.0046
BDE	0.0112	99.2893	99.1286	99.5454	99.3365	0.0054
BASO	0.0129	98.9916	98.9455	99.1737	99.0595	0.0048
SBS-GFRNN	0.0437	95.8251	92.8131	98.1442	95.4042	0.0296
SBS-MLP	0.0428	95.9218	94.1023	97.0615	95.5590	0.0318
GA-MLP	0.0280	97.5640	95.9942	98.7210	97.3385	0.0171

is one of the main goals in the feature selection problem. The selected features by other various binary AVOAs (QbAVOA, VbAVOA, and UbAVOA) are significantly more than Sin-Cos-bIAVOA. This indicates that the proposed compound Sin-Cos transfer function and improved AVOA have enhanced the exploration capability of Sin-Cos-bIAVOA to find the promising area. Also, Sin-Cos-bIAVOA in the second and third phases has good performance to achieve the best solution. In other words, Sin-Cos transfer function generates solutions with high diversity to avoid falling algorithm in the local optima. Also, the proposed transfer function with improved algorithm can obtain the most effective features for GFRNN because the classification measures for Sin-Cos-bIAVOA are obviously more than competitors. In imbalanced datasets, F-measure is one of the most important measures to evaluate the classifier's performance because it shows the balance of precision and recall. As seen in these tables, the obtained F-measures by the proposed method for both scenarios 1 and 2 are the highest. In other words, Sin-Cos-bIAVOA can significantly distinguish attack records from normal records. In these tables, the SBS method has the second rank for the feature selection rate.

The results of feature selection methods for NSL-KDD dataset is

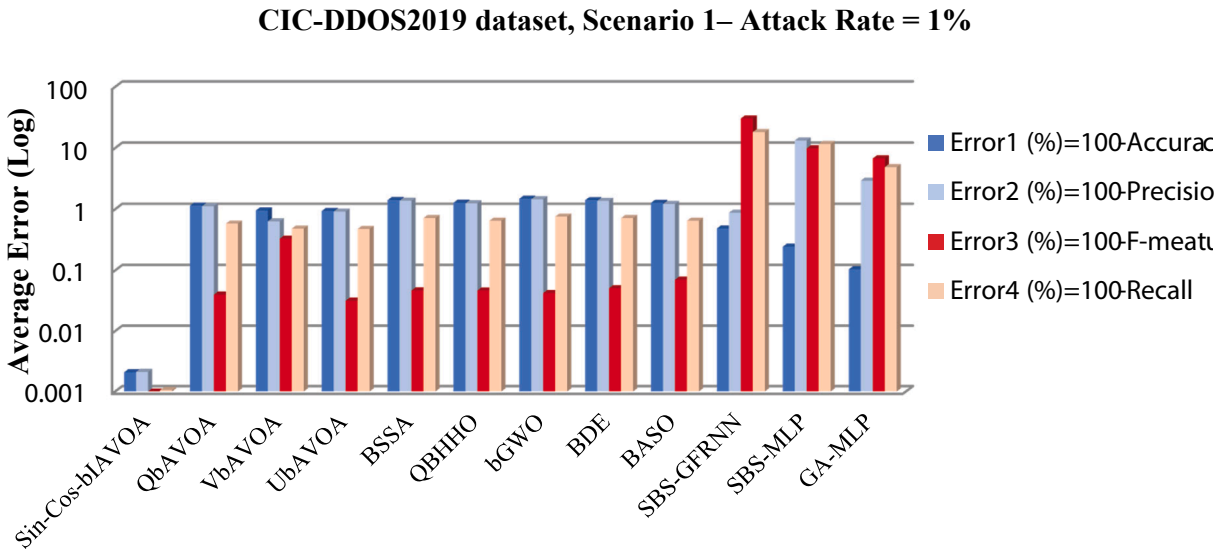

Fig. 8. The average error of algorithms for Scenario 1.

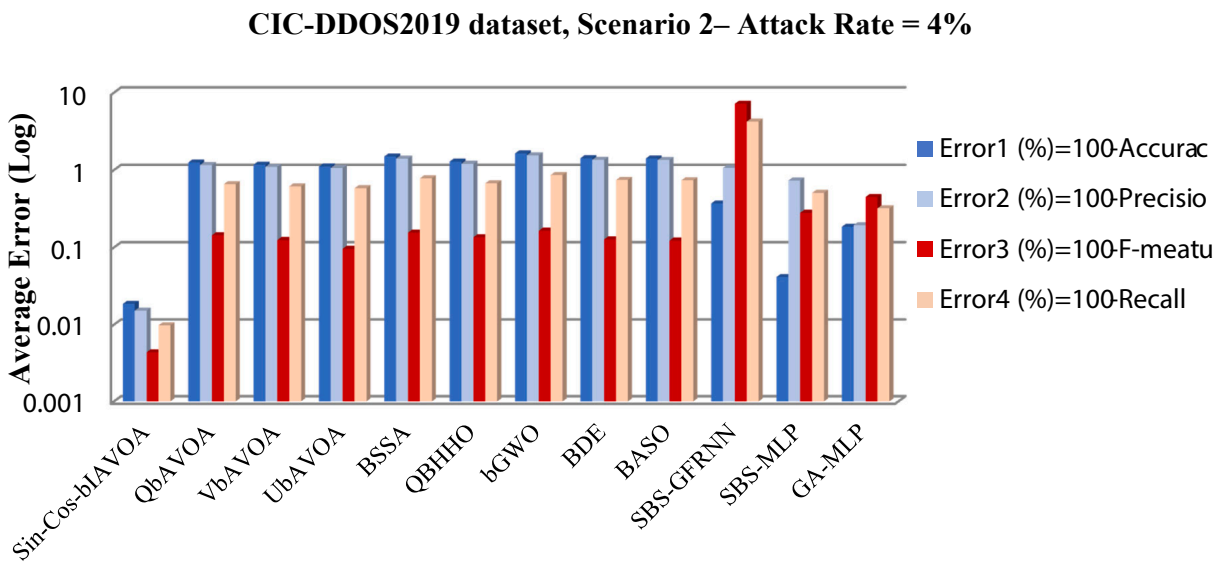

Fig. 9. The average error of algorithms for Scenario 2.

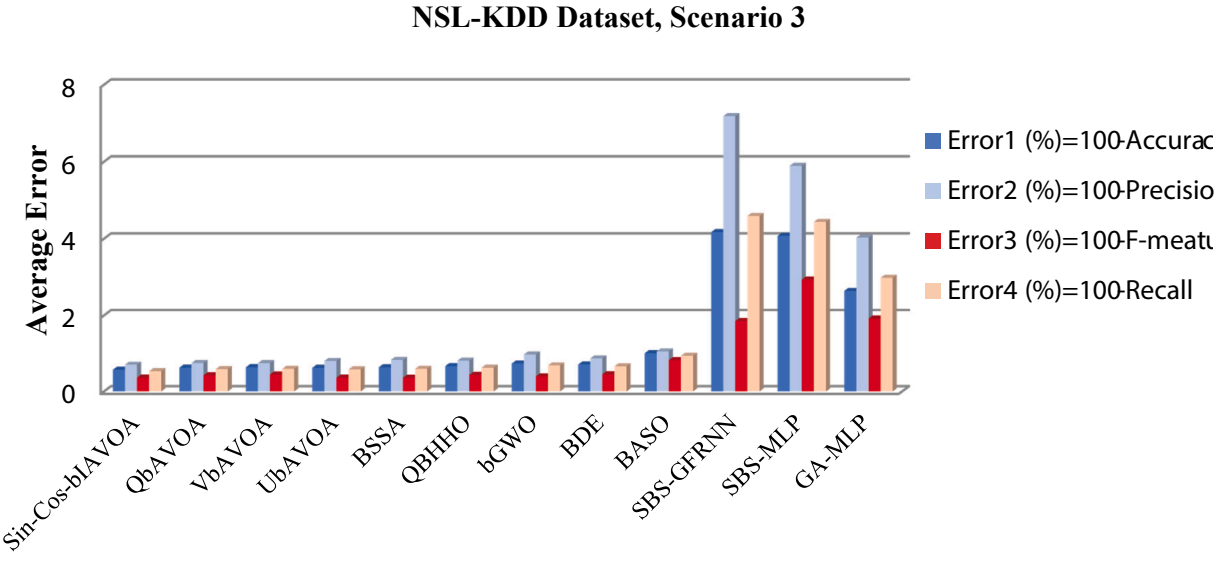

Fig. 10. The average error of algorithms for Scenario 3.

shown in Table 6. The *IR* in this dataset is 1.1 (close to one). It means that the dataset is approximately balanced dataset. If *IR* is very high in a dataset, standard classification algorithms set their parameters based on the majority classes because they should decrease the average classification error.

Hence, the classification of balanced dataset has no the challenges of imbalanced dataset and the accuracy can be considered as the main measure for the performance of methods. As observed in the table, Sin-Cos-bIAVOA achieves the maximum accuracy with the minimum feature selection rate. The SBS method has no good the average feature selection rate compared with the results of Table 4 and Table 5.

The average errors of methods to classify the datasets in three scenarios have been shown in Figs. 8–10. The superiority of Sin-Cos-bIAVOA is clearly evident in the results obtained in the three figures because the proposed method searches promising spaces. Also, Sin-Cos-bIAVOA has achieved a high diversity population to find the best feature selection due to the novel transfer function compared with other methods. It should be noted that the scenarios include imbalanced and balanced ratios and Sin-Cos-bIAVOA obtains the best performance in high imbalanced and balanced datasets.

The averages of feature selection ratio for three scenarios are demonstrated in Fig. 11. As shown in this figure, Sin-Cos-bIAVOA selected the minimum number of features among the other methods with a high difference in three scenarios. It is noticeable that the aims in the feature selection problem are to select the optimal subset of features with the high accuracy (or minimum error). From these figures, it can be concluded that Sin-Cos-bIAVOA achieves these objectives.

Moreover, all methods in three scenarios are separately ranked based on their fitness functions in Table 7 by the Friedman test (Gabor, 2012). The Friedman test is a non-parametric statistical test applied to detect differences in treatments across multiple test attempts. In the table, the minimum value is a better result. As seen in this table, Sin-Cos-bIAVOA achieves the first rank in three scenarios. None of the methods could obtain the second rank in this table in all three scenarios. Although the SBS methods reach the second rank in the first and second scenarios, their results are very poor in the third scenario. Among comparative methods, BSSA, bGWO, and BDE show the worst results in three scenarios.

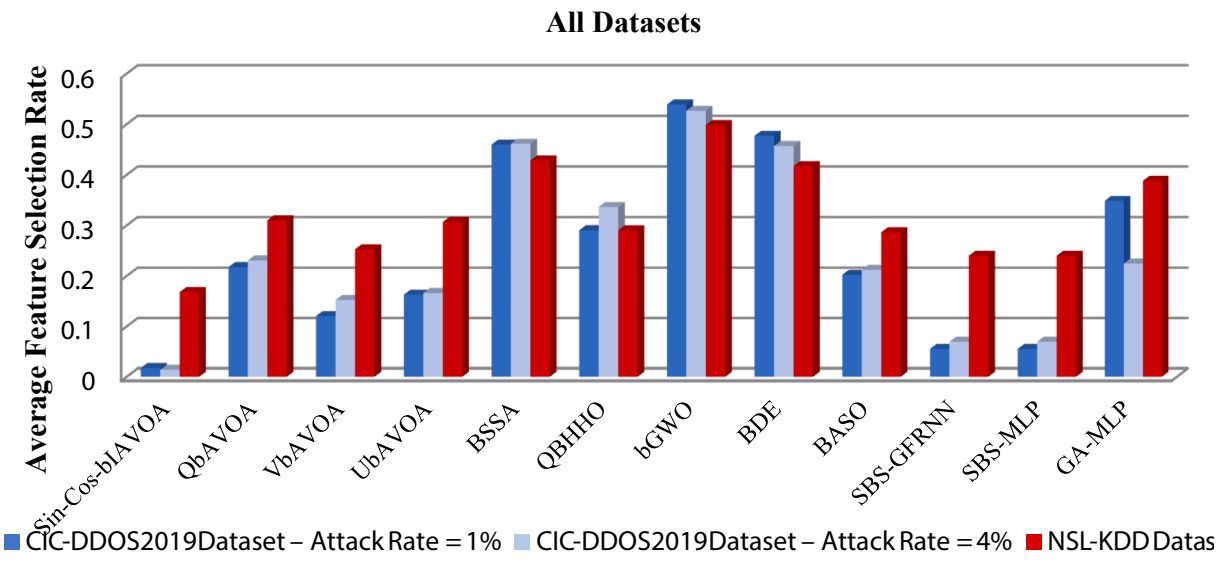

Fig. 11. The average feature selection rate of algorithms for all scenarios.

Table 7
Friedman test results of methods in three scenarios.

Algorithms	CIC-DDOS2019		NSL-KDD
	Attack rate = 1%	Attack rate = 4%	
Sin-Cos-bIAVOA	**1.0625**	**1.1250**	**1.1875**
QbAVOA	7.0313	7.5625	4.3750
VbAVOA	5.5625	6.3125	3.5000
UbAVOA	5.6875	6.3125	4.3750
BSSA	10.5625	10.3125	6.5625
QBHHO	8.3125	7.6875	3.6875
bGWO	11.5625	11.4375	7.8125
BDE	10.5000	9.7500	6.8125
BASO	7.3750	8.0625	6.6875
SBS-GFRNN	3.7500	3.7500	11.5625
SBS-MLP	2.9063	2.0625	11.3750
GA-MLP	3.6875	3.6250	10.0625

Table 8
The average number of misdetection records of methods in three scenarios.

Algorithms	CIC-DDOS2019		NSL-KDD
	Attack rate = 1% Record#=10000	Attack rate = 4% Record#=10000	Record#=25192
Sin-Cos-bIAVOA	0.21	1.87	144.98
QbAVOA	114.69	125.42	158.73
VbAVOA	95.62	117.71	161.23
UbAVOA	93.75	111.67	157.79
BSSA	141.04	150.00	160.92
QBHHO	127.71	128.96	168.73
bGWO	148.54	164.58	185.29
BDE	140.83	142.50	179.04
BASO	127.50	141.30	254.04
SBS-GFRNN	48.54	37.08	1051.75
SBS-MLP	24.37	4.17	1027.38
GA-MLP	10.42	18.55	666.80

Sin-Cos-bIAVOA achieves the minimum average misdetection of attack and normal packets in three scenarios among comparative algorithms as illustrated in Table 8. In the first scenario, the misdetection record of proposed method is under one. It shows that Sin-Cos-bIAVOA has correctly classified all data in the many runs. In other scenarios, the proposed method provides considerably lower errors compared with comparative algorithms. In other words, Sin-Cos-bIAVOA can detect DDoS attack with the high accuracy in IoT networks in where the traffic of packets is enormous.

Table 9
The average execution time of algorithms on CIC-DDOS2019 and NSL-KDD datasets.

Algorithm	Dataset	
	Average Execution Time (Sec.)	
	CIC-DDOS2019 Dataset	NSL-KDD Dataset
Sin-Cos-bIAVOA	169.99	149.93
QbAVOA	81.09	74.19
VbAVOA	82.16	75.07
UbAVOA	82.17	75.12
BSSA	89.46	77.22
QBHHO	153.27	137.32
bGWO	78.03	74.32
BDE	79.68	75.35
BASO	**75.01**	74.54
SBS-GFRNN	82.21	**27.70**
SBS-MLP	336.35	116.36
GA-MLP	406.66	377.37

The feature selection is a pre-processing technique carried out offline; therefore, selecting an optimal subset of features with high accuracy is more important than the execution time in the problem. As a result, the minimum selected features lead to DDoS attack detection with high speed and accuracy in online (real-time) processing. In Table 9, the average execution time of algorithms has been shown on 1000 records of CIC-DDOS2019 and NSL-KDD datasets. As seen in the table, the classifier of GFRRN has less execution time than the MLP classifier. GA-MLP has the maximum execution time in the table. Although BASO for CIC-DDOS2019 dataset and SBS- GFRNN for NSL-KDD dataset show the minimum execution time compared with competitors, they did not provide good results in terms of evaluation criteria of the feature selection. In addition, the SBS methods are highly dependent on the number of features. In CIC-DDOS2019 dataset, the number of features is 71 and in NSL-KDD, the number of features is 41. The number of records in both datasets is equal in this experiment. As observed, the execution time of the SBS methods in the CIC-DDOS2019 dataset is about three times more than that of the KDD dataset, while such a difference is not in metaheuristic algorithms.

In Table 10, the performance of proposed compound transfer function (Sin-Cos) in bIAOVA is compared with other transfer functions such as V-Shaped (Mirjalili & Lewis, 2013) (V-bIAVOA), and U-Shaped

Table 10
Results on CIC-DDOS2019 dataset, Scenario 1– Attack Rate = 1%.

CIC-DDOS2019 Dataset – Attack Rate = 1%						
Algorithm	Average Fitness	Average Accuracy (%)	Average Precision (%)	Average Recall (%)	Average F-Measure (%)	Average Feature Selection Rate
Sin-Cos-bIAVOA	**0.0002**	**99.9979**	**99.9979**	**100.0000**	**99.9989**	**0.0185**
V-bIAVOA	0.00217	99.82500	99.82539	99.99786	99.91103	0.04401
U-bIAVOA	0.00058	99.96038	99.96000	**100.0000**	99.97997	0.01878
S-bIAVOA	0.00061	99.96044	99.96006	**100.0000**	99.9800	0.02201

(Mirjalili & Lewis, 2013) (U-bIAVOA) and S-shaped (Kennedy & Eberh, 1997) (S-bIAVOA). These algorithms are run 16 times on the CIC-DDOS2019 dataset with Attack Rate = 1% and the average results are shown in the table. As observed, the Sin-Cos outperforms other transfer functions in terms of achieving the minimum feature selection rate and maximum accuracy.

7. Conclusion and future studies

The DDoS attack detection is one of the main challenges, especially in IoT networks. The identification of effective features in the DDoS attack is among the most attractive researches in this field. In this regards, the feature selection methods play a main role to identify the most effective features from the original datasets of attack network traffic. In this study, a feature selection method has been introduced to select the most relevant features with a significant impact to increase the classification accuracy. An improved AVOA equipped with a transfer function is used to select the optimal subset of features with the minimum classification error for the DDoS attack. The proposed method called Sin-Cos-bIAVOA divides the algorithm's phases into three separate phases. The method employs a novel Sin-Cos transfer function to improve the exploration capability. Also, it applies GFRNN classifier to detect the DDoS attack in CIC-DDOS2019 with attack rate 1% and 4% dataset, and NSL-KDD dataset. The method provides a high detection rate and finds a minimum efficient subset of features in both balanced and imbalanced datasets. The results show that the proposed method performs well among all compared methods. For future studies, the Sin-Cos-bIVAOA can be employed to solve other binary optimization problems. Also, the transfer function can be employed in other meta-heuristic algorithms and their performances are compared with algorithms in this study. Moreover, a multi-objective Sin-Cos-bIVAOA can be developed to solve binary multi-objective problems. Further, the proposed method can be applied to select effective features and to detect other networks attacks.

CRediT authorship contribution statement

Zakieh Sharifian: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Writing – original draft, Writing – review & editing. **Behrang Barekatain:** Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Writing – original draft, Writing – review & editing, Supervision, Project administration. **Alfonso Ariza Quintana:** Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Writing – original draft, Writing – review & editing, Supervision, Project administration. **Zahra Beheshti:** Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Writing – original draft, Writing – review & editing, Supervision, Project administration. **Faramarz Safi-Esfahani:** Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Writing – original draft, Writing – review & editing, Supervision, Project administration.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Datasets are available on the Internet for everyone

References

Aamir, M., & Ali Zaidi, S. M. (2021). Clustering based semi-supervised machine learning for DDoS attack classification. *Journal of King Saud University - Computer and Information Sciences, 33*(4), 436–446. https://doi.org/10.1016/j.jksuci.2019.02.003

Abdollahzadeh, B., Gharehchopogh, F. S., & Mirjalili, S. (2021). African vultures optimization algorithm: A new nature-inspired metaheuristic algorithm for global optimization problems. *Computers and Industrial Engineering, 158*, Article 107408. https://doi.org/10.1016/j.cie.2021.107408

Abu Khurma, R., Aljarah, I., Sharieh, A., Abd Elaziz, M., Damaševičius, R., & Krilavičius, T. (2022). A review of the modification strategies of the nature inspired algorithms for feature selection problem. *Mathematics, 10*(3), 464.

Agrawal, P., Abutarboush, H. F., Ganesh, T., & Mohamed, A. W. (2021). Metaheuristic algorithms on feature selection: A survey of one decade of research (2009–2019). *IEEE Access, 9*, 26766–26791. https://doi.org/10.1109/ACCESS.2021.3056407

Ahmed, S., Ghosh, K. K., Mirjalili, S., & Sarkar, R. (2021). AIEOU: Automata-based improved equilibrium optimizer with U-shaped transfer function for feature selection. *Knowledge-Based Systems, 228*, Article 107283. https://doi.org/10.1016/j.knosys.2021.107283

Akgun, D., Hizal, S., & Cavusoglu, U. (2022). A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. *Computers & Security, 118*, Article 102748. https://doi.org/10.1016/J.COSE.2022.102748

Alsirhani, A., Sampalli, S., & Bodorik, P. (2019). DDoS detection system: Using a set of classification algorithms controlled by fuzzy logic system in apache spark. *IEEE Transactions on Network and Service Management, 16*(3), 936–949.

Altarabichi, M. G., Nowaczyk, S., Pashami, S., & Mashhadi, P. S. (2023). Fast Genetic Algorithm for feature selection-A qualitative approximation approach. *Expert Systems with Applications, 211*, Article 118528.

Alzaqebah, A., Aljarah, I., & Al-Kadi, O. (2023). A hierarchical intrusion detection system based on extreme learning machine and nature-inspired optimization. *Computers & Security, 124*, Article 102957.

Amaldi, E., & Kann, V. (1998). On the approximability of minimizing nonzero variables or unsatisfied relations in linear systems. *Theoretical Computer Science, 209*(1), 237–260. https://doi.org/10.1016/S0304-3975(97)00115-1.

Arivudainambi, D., Varun, V. K., & Sibi Chakkaravarthy, S. (2019). LION IDS: A meta-heuristics approach to detect DDoS attacks against Software-Defined Networks. *Neural Computing and Applications, 31*(5), 1491–1501. https://doi.org/10.1007/s00521-018-3383-7

Beheshti, Z. (2021). UTF: Upgrade transfer function for binary meta-heuristic algorithms. *Applied Soft Computing, 106*, Article 107346. https://doi.org/10.1016/j.asoc.2021.107346.

Beheshti, Z. (2022). BMPA-TVSinV: A Binary Marine Predators Algorithm using time-varying sinus and V-shaped transfer functions for wrapper-based feature selection. *Knowledge-Based Systems, 252*, Article 109446. https://doi.org/10.1016/j.knosys.2022.109446

Bentley, J. L. (1975). *Survey of techniques for fixed radius near neighbor searching* (No. SLAC-186; STAN-CS-75-513). Stanford Linear Accelerator Center, Calif. (USA).

Bouzoubaa, K., Taher, Y., & Nsiri, B. (2021). Predicting DOS-DDOS attacks: Review and evaluation study of feature selection methods based on wrapper process. *International Journal of Advanced Computer Science and Applications, 12*(5), 132–145. https://doi.org/10.14569/IJACSA.2021.0120517.

Brooks, R. R., Ozcelik, I., Yu, L., Oakley, J., & Tusing, N. (2021). Distributed denial of service (DDoS): A history. *IEEE Annals of the History of Computing, 6180*(c), 1–12. https://doi.org/10.1109/MAHC.2021.3072582

Chandrashekar, G., & Sahin, F. (2014). A survey on feature selection methods. *Computers & Electrical Engineering, 40*(1), 16–28. https://doi.org/10.1016/j.compeleceng.2013.11.024

Chen, G. H., & Shah, D. (2018). Explaining the success of nearest neighbor methods in prediction. *Foundations and Trends in Machine Learning, 10*(5–6), 337–588.

Chen, Y., Pei, J., & Li, D. (2019, May). DETPro: a high-efficiency and low-latency system against DDoS attacks in SDN based on decision tree. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

Chou, D., & Jiang, M. (2022). A survey on data-driven network intrusion detection. *ACM Computing Surveys, 54*(9), 1–36. https://doi.org/10.1145/3472753

Cisco, T., & Internet, A. (2020). Cisco: 2020 CISO Benchmark Report. *Computer Fraud & Security, 2020*(3), 4. https://doi.org/10.1016/s1361-3723(20)30026-9

Dong, S., & Sarem, M. (2020). DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks. *IEEE Access, 8*, 5039–5048. https://doi.org/10.1109/ACCESS.2019.2963077

Eliyan, L. F., & Di Pietro, R. (2021). DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems, 122*, 149–171. https://doi.org/10.1016/j.future.2021.03.011

Emary, E., Zawbaa, H. M., Hassanien, A. E., & Ella, A. (2016). Binary grey wolf optimization approaches for feature selection. *Neurocomputing, 172*, 371–381. https://doi.org/10.1016/j.neucom.2015.06.083

Fatani, A., Elaziz, M. A. B. D., Dahou, A., Al-qaness, M. A. A., & Lu, S. (2021). IoT intrusion detection system using deep learning and enhanced transient search optimization. *IEEE Access, 9*, 123448–123464. https://doi.org/10.1109/ACCESS.2021.3109081

Gabor, M. R. (2012). A "new" non-parametrical statistics instruments: Friedman test. Theoretical considerations and particularities for marketing data. *Proceeding of International Day in Statistics & Economics in Prague*, 395-403.

Golchin, P., Kundel, R., Steuer, T., Hark, R., & Steinmetz, R. (2022, April). Improving DDoS Attack Detection Leveraging a Multi-aspect Ensemble Feature Selection. In *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium* (pp. 1-5). IEEE.

Guo, S.-S., Wang, J.-S., & Guo, M.-W. (2020). Z-shaped transfer functions for binary particle swarm optimization algorithm. *Computational Intelligence and Neuroscience, 2020*, 6502807. https://doi.org/10.1155/2020/6502807

He, Y., Zhang, F., Mirjalili, S., & Zhang, T. (2022). Novel binary differential evolution algorithm based on Taper-shaped transfer functions for binary optimization problems. *Swarm and Evolutionary Computation, 69*, Article 101022. https://doi.org/10.1016/j.swevo.2021.101022

Hosseini, S., & Azizi, M. (2019). The hybrid technique for DDoS detection with supervised learning algorithms. *Computer Networks, 158*, 35–45. https://doi.org/10.1016/j.comnet.2019.04.027

Houssein, E. H., Oliva, D., Çelik, E., Emam, M. M., & Ghoniem, R. M. (2023). Boosted sooty tern optimization algorithm for global optimization and feature selection. *Expert Systems with Applications, 213*, Article 119015. https://doi.org/10.1016/j.eswa.2022.119015

Hu, J., Pan, K., Song, Y., Wei, G., & Shen, C. (2023). An improved feature selection method for classification on incomplete data: Non-negative latent factor-incorporated duplicate MIC. *Expert Systems with Applications, 212*, Article 118654. https://doi.org/10.1016/j.eswa.2022.118654

Jordehi, A. R. (2019). Binary particle swarm optimization with quadratic transfer function: A new binary optimization algorithm for optimal scheduling of appliances in smart homes. *Applied Soft Computing, 78*, 465–480. https://doi.org/10.1016/j.asoc.2019.03.002.

Karthick Kumar, A., Vadivukkarasi, K., Dayana, R., & Malarvezhi, P. (2022). Botnet Attacks Detection Using Embedded Feature Selection Methods for Secure IOMT Environment. In *Pervasive Computing and Social Networking: Proceedings of ICPCSN 2022* (pp. 585-599). Singapore: Springer Nature Singapore.

Kaushik, B., Sharma, R., Dhama, K., Chadha, A., & Sharma, S. (2023). Performance evaluation of learning models for intrusion detection system using feature selection. *Journal of Computer Virology and Hacking Techniques*, 1–20.

Kennedy, J., & Eberhart, R. C. (1997, October). A discrete binary version of the particle swarm algorithm. In *1997 IEEE International conference on systems, man, and cybernetics. Computational cybernetics and simulation* (Vol. 5, pp. 4104-4108). IEEE.

Khanday, S. A., Fatima, H., & Rakesh, N. (2023). Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks. *Expert Systems with Applications, 215*, Article 119330. https://doi.org/10.1016/J.ESWA.2022.119330

Kim, Y. E., Kim, Y. S., & Kim, H. (2022). Effective feature selection methods to detect IoT DDoS attack in 5G core network. *Sensors, 22*(10), 3819. https://doi.org/10.3390/s22103819

Kshirsagar, D., & Kumar, S. (2022). A feature reduction based reflected and exploited DDoS attacks detection system. *Journal of Ambient Intelligence and Humanized Computing*, 1–13.

Kumar, P., Kumar, R., Gupta, G. P., & Tripathi, R. (2021). A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing. *Transactions on Emerging Telecommunications Technologies, 32*(6), 1–31. https://doi.org/10.1002/ett.4112

Li, Y., & Zhang, X. (2011). Improving k nearest neighbor with exemplar generalization for imbalanced classification. In *Advances in Knowledge Discovery and Data Mining: 15th Pacific-Asia Conference, PAKDD 2011, Shenzhen, China, May 24-27, 2011, Proceedings, Part II 15* (pp. 321-332). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-20847-8_27.

Liu, W., & Chawla, S. (2011). Class confidence weighted k NN algorithms for imbalanced data sets. In *Advances in Knowledge Discovery and Data Mining: 15th Pacific-Asia Conference, PAKDD 2011, Shenzhen, China, May 24-27, 2011, Proceedings, Part II 15* (pp. 345-356). Springer Berlin Heidelberg.

Liu, X., Ren, J., He, H., Wang, Q., & Song, C. (2021). Low-rate DDoS attacks detection method using data compression and behavior divergence measurement. *Computers and Security, 100*, Article 102107. https://doi.org/10.1016/j.cose.2020.102107

Ma, X., Wu, J., Xue, S., Yang, J., Zhou, C., Sheng, Q. Z., & Akoglu, L. (2021). A comprehensive survey on graph anomaly detection with deep learning. *IEEE Transactions on Knowledge and Data Engineering*. https://doi.org/10.1109/TKDE.2021.3118815

Mafarja, M., Aljarah, I., Heidari, A. A., Faris, H., Fournier-Viger, P., Li, X., & Mirjalili, S. (2018). Binary dragonfly optimization for feature selection using time-varying transfer functions. *Knowledge-Based Systems, 161*, 185–204. https://doi.org/10.1016/j.knosys.2018.08.003

Maldonado, J., Riff, M. C., & Neveu, B. (2022). A review of recent approaches on wrapper feature selection for intrusion detection. *Expert Systems with Applications, 198*, Article 116822.

Mayuranathan, M., Murugan, M., & Dhanakoti, V. (2021). Best features based intrusion detection system by RBM model for detecting DDoS in cloud environment. *Journal of Ambient Intelligence and Humanized Computing, 12*, 3609–3619.

Mazini, M., Shirazi, B., & Mahdavi, I. (2019). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. *Journal of King Saud University - Computer and Information Sciences, 31*(4), 541–553. https://doi.org/10.1016/j.jksuci.2018.03.011

Mirjalili, S., & Lewis, A. (2013). S-shaped versus V-shaped transfer functions for binary Particle Swarm Optimization. *Swarm and Evolutionary Computation, 9*(Supplement C), 1–14. https://doi.org/10.1016/j.swevo.2012.09.002

Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., Alshoura, W. H., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security, 112*, Article 102494. https://doi.org/10.1016/J.COSE.2021.102494

Pande, S., Khamparia, A., & Gupta, D. (2021). Feature selection and comparison of classification algorithms for wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, 1–13.

Prasad, K. M., Reddy, A. R. M., & Rao, K. V. (2020). BARTD: Bio-inspired anomaly based real time detection of under rated App-DDoS attack on web. *Journal of King Saud University - Computer and Information Sciences, 32*(1), 73–87. https://doi.org/10.1016/j.jksuci.2017.07.004

Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J., & Park, Y. (2019). Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges. *IEEE Access, 8*, 3343–3363.

RM, S. P., Maddikunta, P. K. R., Parimala, M., Koppu, S., Gadekallu, T. R., Chowdhary, C. L., & Alazab, M. (2020). An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. *Computer Communications*, 160, 139-149.

Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems, 129*, 77–89. https://doi.org/10.1016/J.FUTURE.2021.11.011

Rizk-Allah, R. M., Hassanien, A. E., Elhoseny, M., & Gunasekaran, M. (2019). A new binary salp swarm algorithm: Development and application for optimization tasks. *Neural Computing and Applications, 31*(5), 1641–1663. https://doi.org/10.1007/s00521-018-3613-z

Roopak, M., Tian, G. Y., & Chambers, J. (2020). Multi-objective-based feature selection for DDoS attack detection in IoT networks. *IET Networks, 9*(3), 120–127. https://doi.org/10.1049/iet-net.2018.5206

Saad, S., Traore, I., Ghorbani, A., Sayed, B., Zhao, D., Lu, W., Felix, J., & Hakimian, P. (2011, July). Detecting P2P botnets through network behavior analysis and machine learning. In *2011 Ninth annual international conference on privacy, security and trust* (pp. 174-180). IEEE. https://doi.org/10.1109/PST.2011.5971980.

Sahu, P., Singh, B. K., & Nirala, N. (2023). An improved feature selection approach using global best guided Gaussian artificial bee colony for EMG classification. *Biomedical Signal Processing and Control, 80*, Article 104399.

SaiSindhuTheja, R., & Shyam, G. K. (2021). An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment. *Applied Soft Computing, 100*, Article 106997.

Sanchez, O. R., Repetto, M., Carrega, A., Bolla, R., & Pajo, J. F. (2021, June). Feature selection evaluation towards a lightweight deep learning DDoS detector. In *ICC 2021-IEEE International Conference on Communications* (pp. 1-6). IEEE.

Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2019, October). Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In *2019 International Carnahan Conference on Security Technology (ICCST)* (pp. 1-8). IEEE.

Sharifian, Z., Barekatain, B., Ariza Quintana, A., Beheshti, Z., & Safi-Esfahani, F. (2022). LOADng-AT: A novel practical implementation of hybrid AHP-TOPSIS algorithm in reactive routing protocol for intelligent IoT-based networks. *The Journal of Supercomputing, 78*(7), 9521–9569.

Sheibani, M., Barekatain, B., & Arvan, E. (2022). A lightweight distributed detection algorithm for DDAO attack on RPL routing protocol in Internet of Things. *Pervasive and Mobile Computing, 80*, Article 101525. https://doi.org/10.1016/J.PMCJ.2021.101525

Singh, K. J., & De, T. (2020). Efficient classification of DDoS attacks using an ensemble feature selection algorithm. *Journal of Intelligent Systems, 29*(1), 71–83. https://doi.org/10.1515/jisys-2017-0472

Song, Y., Huang, J., Zhou, D., Zha, H., & Giles, C. L. (2007). Iknn: Informative k-nearest neighbor pattern classification. In *Knowledge Discovery in Databases: PKDD 2007: 11th European Conference on Principles and Practice of Knowledge Discovery in Databases, Warsaw, Poland, September 17-21, 2007. Proceedings 11* (pp. 248-264). Springer Berlin Heidelberg.

Sun, B., & Chen, H. (2021). A survey of k nearest neighbor algorithms for solving the class imbalanced problem. *Wireless Communications and Mobile Computing, 2021*, 1–12.

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009, July). A detailed analysis of the KDD CUP 99 data set. In *2009 IEEE symposium on computational intelligence for security and defense applications* (pp. 1-6). IEEE. https://doi.org/10.1109/CISDA.2009.5356528.

Too, J., Abdullah, A. R., & Mohd Saad, N. (2019). A new quadratic binary Harris hawk optimization for feature selection. *Electronics, 8*(10), 1130.

Too, J., & Rahim Abdullah, A. (2020). Binary atom search optimisation approaches for feature selection. *Connection Science, 32*(4), 406–430. https://doi.org/10.1080/09540091.2020.1741515

Ravi Kiran Varma, P., Subba Raju, K. V., & Ruthala, S. (2021). Application of whale optimization algorithm in DDOS attack detection and feature reduction. In *Inventive Computation and Information Technologies: Proceedings of ICICIT 2020* (pp. 93-102). Springer Singapore.

Wang, M., Lu, Y., & Qin, J. (2020). A dynamic MLP-based DDoS attack detection method using feature selection and feedback. *Computers & Security, 88*, Article 101645.

Wu, X., Kumar, V., Ross Quinlan, J., Ghosh, J., Yang, Q., Motoda, H., … Steinberg, D. (2008). Top 10 algorithms in data mining. *Knowledge and information systems, 14*, 1–37. https://doi.org/10.1007/S10115-007-0114-2

Xu, Z., Heidari, A. A., Kuang, F., Khalil, A., Mafarja, M., Zhang, S., Chen, H., & Pan, Z. (2023). Enhanced Gaussian bare-bones grasshopper optimization: Mitigating the performance concerns for feature selection. *Expert Systems with Applications, 212*, Article 118642.

Yadav, S., & Selvakumar, S. (2015, September). Detection of application layer DDoS attack by modeling user behavior using logistic regression. In *2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions)* (pp. 1-6). IEEE.

Yang, J., & Honavar, V. (1998). Feature subset selection using a genetic algorithm. *IEEE Intelligent Systems and their Applications, 13*(2), 44–49.

Yang, X. S. (2010). *Nature-inspired metaheuristic algorithms*. Luniver press.

Yedukondalu, J., & Sharma, L. D. (2023). Cognitive load detection using circulant singular spectrum analysis and Binary Harris Hawks Optimization based feature selection. *Biomedical Signal Processing and Control, 79*, Article 104006.

Yi, J., Clausen, T., & Bas, A. (2012, November). Smart route request for on-demand route discovery in constrained environments. In *2012 IEEE International Conference on Wireless Information Technology and Systems (ICWITS)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICWITS.2012.6417755.

Zhang, X., & Li, Y. (2013). A positive-biased nearest neighbour algorithm for imbalanced classification. In *Advances in Knowledge Discovery and Data Mining: 17th Pacific-Asia Conference, PAKDD 2013, Gold Coast, Australia, April 14-17, 2013, Proceedings, Part II 17* (pp. 293-304). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-37456-2_25.

Zhang, Y., Gong, D., Gao, X., Tian, T., & Sun, X. (2020). Binary differential evolution with self-learning for multi-objective feature selection. *Information Sciences, 507*, 67–85. https://doi.org/10.1016/j.ins.2019.08.040.

Zhu, Y., Wang, Z., & Gao, D. (2015). Gravitational fixed radius nearest neighbor for imbalanced problem. *Knowledge-Based Systems, 90*, 224–238.