Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.037948
Article

Feature Selection for Detecting ICMPv6-Based DDoS Attacks Using Binary Flower Pollination Algorithm

Adnan Hasan Bdair Aighuraibawi[1,2], Selvakumar Manickam[1,*], Rosni Abdullah[3], Zaid Abdi Alkareem Alyasseri[4,5,*], Ayman Khallel[6], Dilovan Asaad Zebari[9], Hussam Mohammed Jasim[7], Mazin Mohammed Abed[8] and Zainb Hussein Arif[7]

[1]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, 11800, Malaysia
[2]Baghdad College of Economic Sciences University, Baghdad, Iraq
[3]School of Computer Sciences, Universiti Sains Malays, Penang, 11800, Malaysia
[4]Information Technology Research and Development Center, University of Kufa, Najaf, Iraq
[5]College of Engineering, University of Warith Al-Anbiyaa, Karbala, Iraq
[6]Faculty of Computing and Informatics, Universiti Malaysia Sabah, Sabah, Malaysia
[7]Business Administration, College of Administration and Financial Sciences, Imam Ja'afar Al-Sadiq University, Baghdad, 10001, Iraq
[8]College of Computer Science and Information Technology, University of Anbar, Ramadi Anbar, Iraq
[9]Department of Computer Science, College of Science, Nawroz University, Duhok, 42001, Kurdistan Region, Iraq
*Corresponding Authors: Selvakumar Manickam. Email: selva@usm.my; Zaid Abdi Alkareem Alyasseri. Email: zaid.alyasseri@uokufa.edu.iq
Received: 22 November 2022; Accepted: 10 March 2023; Published: 26 May 2023

Abstract: Internet Protocol version 6 (IPv6) is the latest version of IP that goal to host 3.4×10^{38} unique IP addresses of devices in the network. IPv6 has introduced new features like Neighbour Discovery Protocol (NDP) and Address Auto-configuration Scheme. IPv6 needed several protocols like the Address Auto-configuration Scheme and Internet Control Message Protocol (ICMPv6). IPv6 is vulnerable to numerous attacks like Denial of Service (DoS) and Distributed Denial of Service (DDoS) which is one of the most dangerous attacks executed through ICMPv6 messages that impose security and financial implications. Therefore, an Intrusion Detection System (IDS) is a monitoring system of the security of a network that detects suspicious activities and deals with a massive amount of data comprised of repetitive and inappropriate features which affect the detection rate. A feature selection (FS) technique helps to reduce the computation time and complexity by selecting the optimum subset of features. This paper proposes a method for detecting DDoS flooding attacks (FA) based on ICMPv6 messages using a Binary Flower Pollination Algorithm (BFPA-FA). The proposed method (BFPA-FA) employs FS technology with a support vector machine (SVM) to identify the most relevant, influential features. Moreover, The ICMPv6-DDoS dataset was used to demonstrate the effectiveness of the proposed method through different attack scenarios. The results show that the proposed method BFPA-FA achieved the best accuracy rate (97.96%) for the ICMPv6 DDoS detection with a reduced number of features (9) to half the total (19) features. The proven proposed method BFPA-FA is effective in the ICMPv6 DDoS attacks via IDS.

Keywords: IPv6; ICMPv6; DDoS; feature selection; flower pollination algorithm; anomaly detection

1 Introduction

The world has witnessed drastic, rapid changes in networking technology, as well as the rapid advancement and expansion of the Internet and networking technologies [1]. With the advancement of digital and communication technologies, societies have progressively become global knowledge through the use of intelligent computing environments in every area. However, the security guidelines that protect these environments have not evolved at the same pace [2]. More specifically, because of frequent network breaches to access confidential information or make information and networks vulnerable or inaccessible [3], cybersecurity has become one of the most prominent fields of study in the real world. New technologies and systems are almost always fraught with security concerns. The same is true for the new Internet communication protocols, such as Internet Protocol version 6 (IPv6). IPv6 was designed to address several Internet Protocol version 4 (IPv4) problems, as IPv6 has many features and newly supported services as the efficiency of packet processing, auto-configuration, versatility, and extend the Internet address space and virtually facilitates an unlimited number of device to the Internet-connected [4]. Mobility options and security support were among the concerns addressed during the IPv6 transition and the Internet Engineering Task Force worked hard to improve IPv6 over IPv4 [5]. On the other hand, the implementation of IPv6 has created security issues for networks, require to find efficient methods for identifying and being aware of the need to predict vulnerability in the IPv6 network, however, must use a robust algorithm to identify vulnerability and comprehend the network's specifications [6]. As shown in Fig. 1 [7], the proportion of clients using Google services via IPv6 increased from 0.0% in 2010 to 25.88% on 9 March 2020 to 32.62% on 5 March 2021 until 9 Nov 2022 became 37.48%, and the proportion is rising.

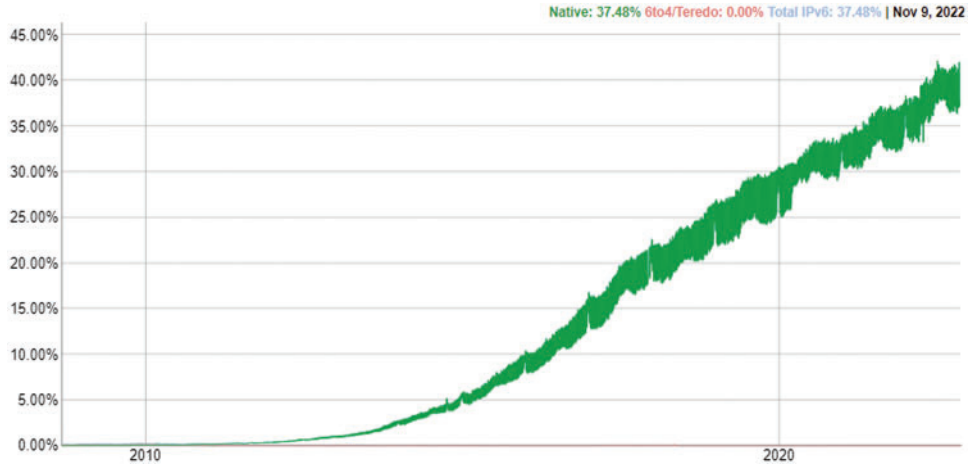

Figure 1: Internet protocol version 6 traffic percentage accessing google services

IPv6's expansive address space enables an incalculable number of devices with the help of neighbour discovery messages (NDP) messages and the ICMPv6 protocol, where ICMPv6 is based on NDP in detecting every new device or discovers neighbours and routers [8]. ICMPv6 is a crucial protocol because it accounts for the backbone of IPv6 networks and is susceptible to all types of

exploitation, including misusage and multicast attacks, reconnaissance attacks, fragmentation-related attacks, and Distributed Denial of Service (DDoS) attacks. In addition, the design of Internet Control Message Protocol version 6 (ICMPv6) messages contains security flaws, such as sending addresses, making it possible for any user to conduct a reconnaissance attack [5]. In return, security defects exploit can lead to a DDoS attack in a variety of ways, such as sending ICMPv6 packets with multiple interfaces to the same site, where the error messages disable the connection and cause the session to terminate. The most common type of DDoS attack is the Flood Attack (FA), in which network traffic is sent in large quantities to the network device, resulting in network flooding [9].

While recent developments have brought new technologies in network security, such as Intrusion Detection Systems (IDS), firewalls, and antivirus. IDS is the most widely used security technique for detecting unpermitted traffic and detect unwanted activities in either systems or networks. IDS is divided into Network-based IDSs (NIDS) and Host-based IDSs (HIDS) [10]. Anomaly-based Intrusions Detection Systems (AIDS) record and analyse both normal and anomalous traffic [11]. Regular traffic is defined, but anything anomalous is treated as an intrusion [12]. AIDS uses matching algorithms to distinguish normal and abnormal traffic, resulting in a higher detection rate than Signature-based Intrusion Detection Systems (SIDS). Researchers designed algorithms used by AIDS to automatically keep learning normal behaviour in the network [13]. AIDS has seen rapid advancements in building descriptive profiles of regular traffic in the IPv6 network [14–16]. There are two types of AIDS: rule-based and Artificial Intelligence-based. Many approaches have been proposed to detect cyber threats using Anomaly detection is one of these approaches that define the boundaries behavior of normal and abnormal. However, these solutions should have the capability and adjust to environmental changes that prompt behavioral aberrations, except they only assume that these nodes show the same behavior. This assumption does not hold due to the heterogeneity of network topology and the cost is heavy. Consequently, the model becomes unstable and adversely affects its accuracy and robustness [17].

Extracting data meaningful to anomaly detection will be very difficult. Any attack contains its own features and behaviour which determines the type of attack. Therefore, some attacks may contain similar patterns and behaviours and are only different in some adjectives [18]. By selecting the most relevant features from the input data set using the features selection technique, IDS can be faster and more accurate detection rates, which is an important stage to select the optimal subset of features that contribute to the faster training process and reduce time and complexity while maintaining on system performance [19]. Despite all of these existing techniques, the IDS still requires a comprehensive approach to detect ICMPv6 DDoS flooding attacks. Therefore, the Flower Pollination Algorithm (FPA) [20] has been proposed to address the problem of detecting ICMPv6-DDoS flooding attacks. The FPA is a bio-inspired optimization algorithm that mimics the natural pollination process of flower plants. The propositioned approach (BFPA-FA) employs a wrapper method in features selection technology to select the best subset of features for detecting ICMPv6-DDoS flooding attacks. A Support Vector Machine (SVM) has been utilized to classify traffic networks as normal or abnormal for evaluation. They are trained in optimum plane formation which classifies the values of unknown input vectors based on their position on the plane [21].

The main challenge with the topic of DDoS Attacks is how to select the most relevant feature which can provide the highest accuracy rate [14]. For that, many researchers proposed different techniques for selecting the best features one of these techniques is using metaheuristic algorithms such as the flower pollination algorithm (FPA) [12]. In this work, FPA with SVM is proposed for detecting ICMPv6 DDoS. Real datasets are used to test the performance of the proposed method which was collected at the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia [14].

The main contributions of this study are as follows:

- The flower pollination algorithm (FPA) is proposed for detecting ICMPv6 DDoS flooding attacks. The FPA is a bio-inspired optimisation algorithm that mimics flower plant pollination.
- The proposed method employs a wrapper method in features selection technology to generate optimal subset features for detecting ICMPv6 flooding attacks, with the Support Vector Machine (SVM) used for evaluation.
- Experiments were carried out to evaluate the performance of the proposed method, which is demonstrated by using datasets generated in a NAv6 laboratory [22].

The research paper is divided into several sections. Section 2 describes the flower pollination algorithm. Section 3 conducts a literature review, which is divided into two parts: Part A presents the concept of IDS for ICMPv6, and Part B discusses the principle of FS. Section 4 discusses the proposed model's methodology. Section 5 contains the findings and discussions. Finally, Section 6 concludes the paper and suggests future research directions.

2 Flower Pollination Algorithm (FPA)

Flower Pollination Algorithm (FPA) [12] is inspired by pollination behaviour in flowering plants and was developed in 2012, it demonstrated the interest of many researchers in resolving various optimisation problems. FPA Contains two operators: local and global and outperforms other metaheuristic algorithms in real-world optimisation challenges due to its adaptability and scalability. In addition, FPA has many examples of optimization challenges such as wireless sensor networking [23], electrical and power systems [24,25], signal and image processing [26,27], clustering and classification [28,29], computer gaming, structural and mechanical engineering optimisation [30,31], global function optimisation [32], and various variants [33,34]. In some studies, FPA is used in hybridised, modification, with parameter-tuning to resolve complex problems related to optimisation [35]. Sensors are required to identify people based on EEG signals, but the number of sensors required is excessive. Reference [21] tested the FPA algorithm against other optimisation algorithms for sensor reduction, including Binary GA, Binary PSO, Binary FA, Binary HS, and Binary Charged System Search. A binary version of FPA and optimum path forest classifiers are used to obtain a minimum subset of channels for identifying people, yielding significant results when compared to other methods. The recognition rate was around 87%. Although the FPA was originally designed to solve continuous optimisation problems, [36] modified it into a binary FPA for feature selection purposes by testing it on six datasets. In comparison to PSO, HS, and FA, the results were promising. In the convergence process, PSO is the best, but HS has the lowest computational cost and BFPA is the most accurate.

It is difficult for any metaheuristic method to strike a balance between global exploration and neighbourhood exploitation. In the global search process, FPA employs discarded pollen-operator to improve exploration and thus avoid neighbourhood exploitation. According to a study by [37] enhanced FPA's exploration capability by incorporating PSO. Wideband infinite impulse response digital differentiators and integrators were created. The FPA outperformed many existing methods in terms of the smallest function evaluations.

Another study by [38] used Pattern Search (PS) to implement a multi-objective FPA for retinal vessel localization. For the best collection of retina images, a driving dataset was used as a benchmark. This method was compared to other optimisation algorithms to assess sensitivity, precision, and other characteristics.

3 Related Work

The big challenge in the network deployment environment is the growing cyber-attacks. To protect the network environment from unforeseen cyber-attacks, many researchers are functioning in this field for providing different mothed for network securing from cyber-attacks [39]. Detection systems use feature selection techniques to overcome issues such as distinguishing between normal and abnormal data, lopsided information circulation, large datasets, precision, and so on. As a consequence, it is necessary to discuss intrusion detection systems (IDS), which present machine learning algorithms designed primarily to detect attacks, and feature selection (FS), which presents principles of bio-inspired algorithms designed to detect attacks [40].

3.1 Intrusion Detection System (IDS) For ICMPV6

Despite recent advancements in network security, such as IDS, firewalls, antivirus applications, etc., the IDS remains the most popular security technique for detecting undesirable traffic and reporting malicious packets that flow to devices [41,42]. IDS checks and analyses network data using a set of criteria and can detect undesirable traffic. A typical IDS consists of three steps: 1) data collection, 2) data analysis, and 3) action items, [43,44]. The traffic is examined by an IDS network system utilizing traffic tools that collected and analyze traffic data using Intrusion detection algorithms [45]. DDoS is the most common attack on computing which focused the computing and security professionals on the growth of detection and preventive processes from DDoS attacks. Due to the widespread prevalence of DDoS attacks, becomes hard for Some DDoS attack methods based on network flow features to distinguish DDoS attacks of different types [46]. This study uses the anomaly-based IDS to detect the ICMPv6 DDOS flooding attacks.

IDS software is widely used to detect potential attacks through the classification algorithms that are commonly used to build accurate IDSs due to their efficiency and autolearning ability to detect ICMPv6-based DDoS attacks [47,48]. In addition, IDS uses a benchmark dataset for the evaluation of intrusion detection systems in IPv6 environments, and evaluation through the accuracy in detecting IPv6 attacks [36]. IDS has a significant role in detecting potential attacks, the huge traffic flow leads to severe challenges of technology relating to monitoring and spotting network activities. However, the DDoS attack's devastating nature appears as a major cyber-attack regardless of the Network architecture emergence [49].

Learning techniques used seven classifiers to detect any attacks ICMPv6-based DDoS attack. The ten packet header attributes used. flow-based datasets are generated from packet-based datasets by constructing flows based on the extracted attributes The proposed flow-based approach achieved a good accuracy range and few false-positive rates [50]. In addition, [51] proposed five classifications for detecting ICMPv6-based DDoS attacks, using flow-based datasets due to their online availability and containing the targeted attacks and labelled traffic. The experimental results showed that the classifiers had detected most of the included attacks, resulting in true-positive rates ranging from 73% to 85%.

The absence of publicly available IPv6 datasets impedes advancement in the field of IPv6 network security and due to specification differences between the two protocols IPv4 and IPv6 existing benchmarked IPv4 datasets such as DARPA [52] and NSL_KDD [53] cannot be used for modelling IPv6 IDSs. As a result, numerous factors must be considered in order to create a reliable dataset. A new dataset must meet all requirements before it can be used. A dataset must include both normal and abnormal traffic data representing diverse scenarios, as well as all important and relevant features labelled. Therefore, [22] the dataset that contains the ICMPv6 DDoS attacker will be used

3.2 Feature Selection (FS)

Feature Selection (FS) is the most commonly used dimensionality reduction approach. FS is used to clean up the noisy, redundant, and irrelevant data and a subset of features is selected from the original set of features based on features redundancy and relevance [54]. Usually, FS is used to solve an objective optimisation problem whose objectives are classification accuracy and the number of features [55]. IDS is supposed to track and inspect massive network traffic, which unfortunately exceeds IDS's computational capabilities. Recent advancements in network technology are complicating matters. As a consequence, it is critical that the IDS must be able to process information to detect abnormal activities in networks [26,35]. To improve IDS' performance accuracy efficiency, it is necessary to use a technique of Feature Selection to reduce the complexity and time involved in computations [56]. Reference [57] proposed IDS using a feature selection approach based on the mathematical set theory for extracting efficient subsets of features. The IDS has three stages: a data preprocessing phase, feature selection, and classification using IG and GR filter-based approaches to produce the top subsets of features for the IoTID20 and NSL-KDD datasets. The method has provided better results in classification performance and eliminating irrelevant features before the training process. The experiments demonstrated a significant improvement in the realms of accuracy.

Fig. 2 depicts a four-stage process for feature selection. The first stage involves selecting a subset, and the second involves evaluating the chosen subset. The third stage includes a criterion evaluation for stopping, and the fourth stage is the validation of the results. The FS is divided into two categories: filter methods and wrapper methods [58].

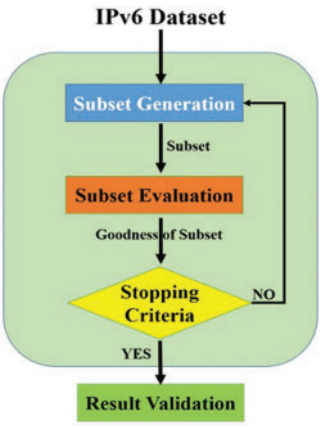

Figure 2: Feature Selection process

Feature selection provides an effective way to solve this problem by removing irrelevant and redundant data, which can reduce computation time, improve learning accuracy, and facilitate a better understanding of the learning model or data, wrapper methods can obtain better subsets than filter methods, but they are more computationally demanding than filter methods. They do, however, outperform in terms of feature selection [59]. In this study, we use the wrapper method is often used as a learning aid for evaluating the subset of the evaluation measures for feature selection methods that accuracy is used to predict the subset, which is widely applied in machine learning problems.

4 Proposed Method

Among the challenges of evaluating the proposed approach is the difficulty obtaining of a standard dataset (benchmark datasets) which we will use in evaluating the proposed approach, and if it is obtained now, it contains a limited number of features. Furthermore, a dataset containing normal and abnormal traffic must be available to analyse security issues and identify gaps that can be exploited to create network threats. Another barrier is the use of security testing tools in the main networks (local and global networks). Diverse IDS have been proposed to address the issue of ICMPv6 DDoS-based. Unfortunately, these IDSs are unable to accurately detect attacks and suffer from many issues, including precision, large datasets, lopsided circulation of information, and, most problematically, the inability to distinguish between normal and abnormal data This is primarily due to a lack of consideration for attack-related features in those techniques. This technique may be used by an IPv6 network to determine unrivalled features in the detection of network attacks [60].

The FPA [20] is one of the bio-inspired algorithms for the natural pollination of plants, with the main goal of survival of the fittest and optimum reproduction of plants. It is essentially an optimisation of plant species that are managed through four basic rules applied to many real-world problems and has proven successful in engineering problems [61,62].

The proposed strategy is divided into three main goals. First, using one of the types of feature selection technology, the FPA algorithm is used to solve the attack detection problem. Second, an SVM classifier is used in machine learning algorithms to distinguish between normal and malicious data, as well as to evaluate the algorithm's performance. Third, the experiments are carried out to evaluate the performance of the proposed method using datasets generated in a NAv6 laboratory [14]. The process of creating and generating the dataset consists of three steps packet capture, packet filtering, and packet labelling. The packet capture step utilizes the Wireshark packet capture tool to capture and collect packet traffic. The collected traffic is filtered using a specific Wireshark filter command to discard all non-ICMPv6 or IPv4 packets. After collection and filtration, the resulting data is formatted using Comma Separated Values (CSV) and saved. Labelling the data entails adding a field called (class) to each record in the file. The GNS3 tool used the simulated dataset generated because the monitoring port was not obtained due to the privacy of the data when the dataset was generated(normal). As for the abnormal (attack) dataset, THC-IPv6 toolkits were used in a virtual network because their use in a real network disrupts network operations. The dataset contains 19,880 samples (7565) normal and (9315) abnormal.

This section proposes a method for detecting DDoS flooding attacks based on ICMPv6 messages using a Flower Pollination Algorithm (FPA-FA). Fig. 3 depicts the general stages of the proposed approach. This section also summarises the methodology, and structure design, and provides an overview of the details and stage of the proposed method. Overall, the proposed method is divided into two stages: 1) ICMPv6 packet preparation and 2) Feature selection using BFPA-FA for detection via anomaly-based detection.

4.1 Stage (1) ICMPV6 Packets Preparation

This stage is divided into two major steps: ICMPV6 packet transformation and ICMPV6 packet normalization. In the transformation step, the captured dataset includes 21 features in addition to the category labelling (normal or attack). These characteristics are extracted via an IPv6 network communication exchange using ICMPv6 messages. These features have various data types, such as package protocol, package length, and ICMPv6 code ICMPv6, ICMPv6-TA, ICMPv6-CHL, ICMPv6-AF, ICMPv6-RL, ICMPv6-RH, and ICMPv6-RT.

These fields with numerous attributes undergo ICMPv6 transformation to a single numeric format. During the normalization step, the dataset contains several attributes and data in different formats, such as data in an alphabetical format and other numerical formats, including symbolic data. As a consequence, the transformation implements the symbolic map attributes to numeric attributes to reduce data processing time and resource consumption. Normalization of the ICMPv6 message dataset is an important step in preparing the dataset for use with the proposed method. The benchmark dataset contains various formats with different features such as alphanumeric, numerical, and symbolic. Normalization is used to standardize the coordination of all features or records in a database and reduce the volume of data, time of analysis, and resource waste by converting them to a digital or ordinal format.

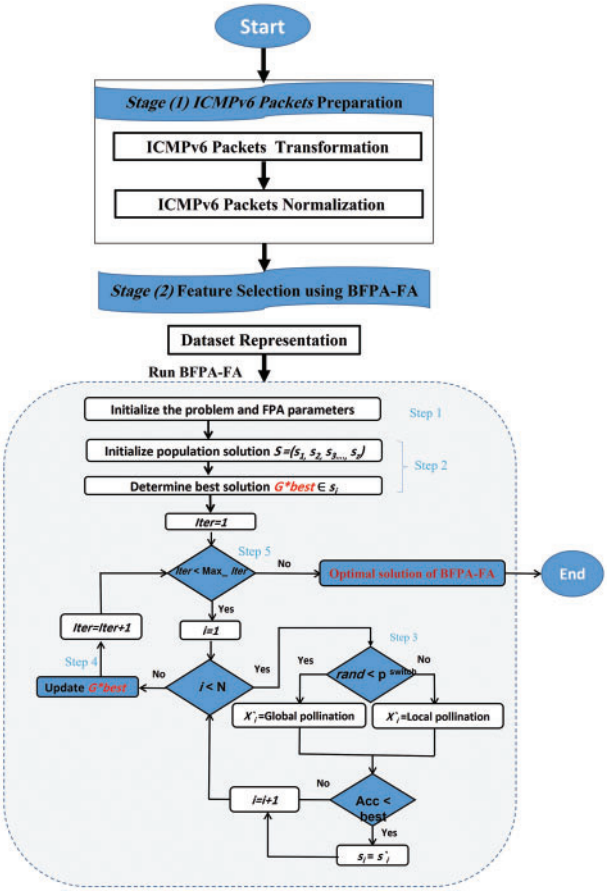

Figure 3: Proposed method binary flower pollination algorithm flooding attack

4.2 Stage (2) Feature Selection Using B FPA-FA

The primary goal of this stage using FS technology in the FPA is to validate its functionality in the proposed approach as well as to improve and increase detection using FS technology. Furthermore, this stage contains five steps to achieve the main goal of using this algorithm in the proposed approach, namely, dataset representation, FPA parameter initialisation, optimal subset selection, current optimal subset evaluation using SVM, and optimal best solution update. As a result, select of a DDoS flooding attack's feature is checked for benefit by using anomaly-based machine learning with classification to

detect and train. The features chosen using machine learning by SVM classification are included in the testing dataset. The list of parameters, as shown in Table 1, was used for the proposed FPA algorithm.

Table 1: Proposed settings of the parameter for the Binary Flower Pollination Algorithm

Settings of parameter	Values
Number of features (N)	19
Number of Iterations	100
Number of Runs	25
The dimension of Solution	20
Search domain	[0;1]

The employing FS technology is to adopt the BFPA algorithm in the IDS to detect DDoS FA in the IPv6 network. The FS stage helps to reduce the size of the dataset while improving attack detection accuracy and distinguishing between normal and abnormal data. The process of building attributes and selecting the algorithm is one of the most important factors influencing the steps of the proposed approach and increasing detection performance and accuracy. Adapting the FPA algorithm in the use of FS technology in determining the best features (reducing the number of features used) has positive effects, including reduced training time due to reduced data volume and retention of many resources, as shown in Fig. 4.

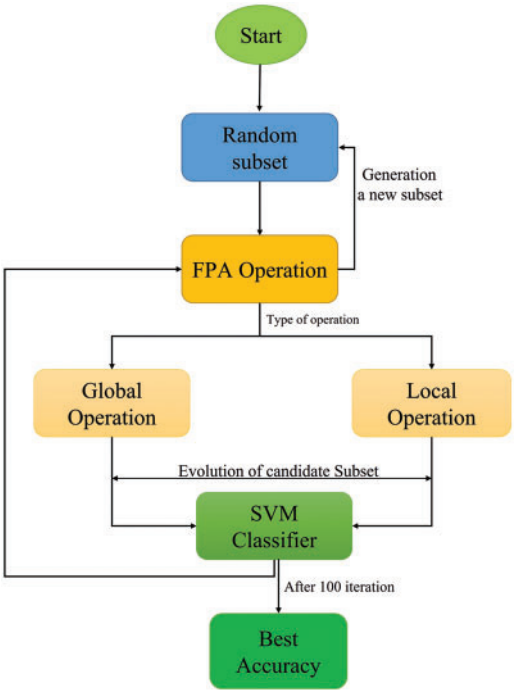

Figure 4: Process of feature selection binary flower pollination algorithm-flooding attacks

Fig. 4 depicts the FPA algorithm, which includes two operators: the local operator and the global operator. The switching probability (P) is responsible for selecting the most appropriate operators. If

P-value is greater, the global search operation is used; otherwise, the local search operation is used. Furthermore, depicts the FPA algorithm's feature selection process; the algorithm collaborates with the SVM classifier to evaluate the candidate subset of selected features; the algorithm has the authority to decide whether the subset is worthy or worthless. The procedure is then repeated until the condition is met (100 Iterations, see Table 1). Meanwhile, if the algorithm meets the stopping criteria, it generates a random subset and repeats the process 25 times (see Table 1). This section describes the FS steps for using FPA-FA.

4.2.1 Dataset Representation

The reference data represented by the set of ICMPv6 messages generated and prepared in the two previous stages are the inputs of the dataset representation step, which consists of 19 attributes in addition to the category of the attribute that the classifier uses for distinguishing between attack and natural data. These characteristics are represented as a 2D matrix (n ∗ m) in the proposed algorithm BFPA. As previously stated, vector (n) represents the matrix's 19 attributes or features, and (m) represents the number of solutions produced by the proposed algorithm. Fig. 5 presents the ICMPv6 Message Dataset Representation

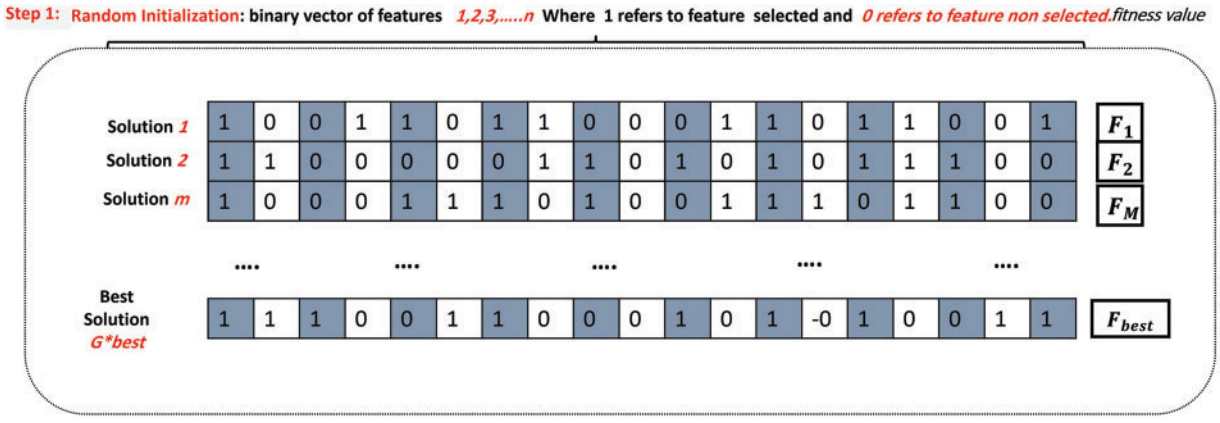

Figure 5: Represented solution

4.2.2 Initialised FPA Parameters

There are two types of parameters: FPA algorithm parameters and problem parameters. Both parameters must be initialised for a solution to be found. The initialised parameter must be within a possible range value (x). The following general formulation can be used to initialise FPA parameters:

$$Max\, f(x) \mid x \in X \tag{1}$$

where $f(x)$ is an objective function (in this work $f(x)$ refers to accuracy rate).

$x = \{xi|i=1;..n\}$ represents the group of variables of decision, $x = \{xi|i=1;..n\}$ represents the possible range of values for each variable of decision, and Where

$Ci \in [Lower\ (Bi);\ Upper\ (Bi)]$, where $[Lower\ (Bi)\ and\ Upper\ (Bi)]\ Upper\ (Bi)$ represent the highest and lowest bounds of the variable of decision Ci, respectively, and n represent the number of variables of decision.

Algorithm parameters must also be initialized. The FPA parameters are as follows:

- FPA_s: shows the population size of solutions,

- G^*_{best}: represents the best solution population size currently from the initialization,
- *Switch probability (P):* represents (*P*-value) selected in either local or global search in *FPA*, and.
- L_{dis}: represents the size of the step, that is, the pollination strength.

FPA population memory (FPM) Initialization. It is represented as a 2D matrix. The matrix sizecontains a group of vectors such as FPAs that are located as the flower. where the flowers are generated randomly as follows:

$$X_j^i = LowerB_i + (UpperB_i - LowerB_i) * U(0;1) \tag{2}$$

$$\forall_i = 1;2;\ldots;z \text{ and } \forall_j = 1;2;\ldots;FPA_s, \text{ and } U(0;1) \tag{3}$$

The range between 0 and 1 is used to generate random numbers. The solutions are arranged in ascending order based on the objective function's value:

$$fx^1 \leq fx^2 \leq \ldots \leq fx^{FPAs}$$

$$FPM = \begin{bmatrix} x_1^1 & x_2^1 \ldots & x_d^1 \\ x_1^2 & x_2^2 \ldots & x_d^2 \\ \vdots & \vdots & \vdots \\ x_1^{FPMs} & x_d^{FPMs} \ldots & x_d^{FPMs} \end{bmatrix} \tag{4}$$

In addition, the best location of the flower in global search is stored, where $G^*_{best} = x^1$. The solution (flower) FPA is like a 2D matrix. A row represents a set of features, and a column represents a several solutions. The binary vector of features is (1,2,3, ... n), where a non-selected feature is represented by value 0 and the selected feature is represented by value 1. The best solution for the search space among the solutions is the best subset of features that can be used to reach a high detection rate for the ICMPv6 flooding attack in this paper. Fig. 6 represents the solution (flower). The general formulation can be used to initialize problem parameters as follows:

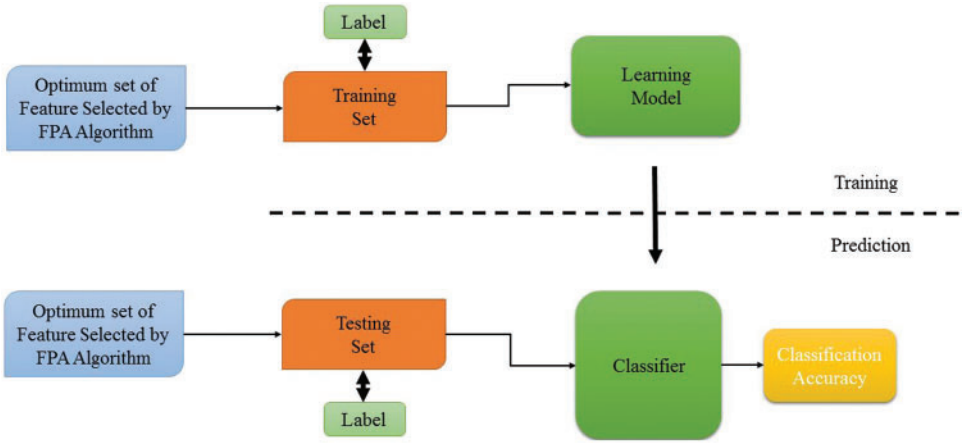

Figure 6: Procedure of detection stage

Initialise (N) equals the number of features (19) in the pack and initialise a population random length solution dimension of the solution equals (20) population solution.

4.2.3 Selecting the Optimal Subset

The columns are chosen to form a matrix. Selecting an optimal subset from such a matrix is a fundamental problem in many learning tasks, including FS. The optimal subset resulting from the proposed algorithm is chosen after applying the path to follow in pollination, global search, or local search. Fig. 5 shows the proposed FPA algorithm's process. Flower constancy and local pollination are represented as under:

$$x_i^{t+1} = x_i^{t+1} x_i^t + \xi \left(x_j^t - x_k^t\right) \tag{5}$$

where (x_j^t) and (x_k^t) are the pollen of stand from distinct flowers; (j) and (k) belong to the same class of the plant This Equation represents the flower constancy in the limited neighborhood. Mathematically, if (x_j^t) and (x_k^t) are obtained from the identical population or same class, and $\in$ is drawn from a uniform distribution in [0, 1], then it becomes a local random walk.

Global pollination is shown as under:

$$x_i^{t+1} = x_i^1 + L(G_{best}^* - x_i^t) \tag{6}$$

In the current iteration, (G_{best}^*) is the best solution, and x_i^{t+1} is the pollen (i) or solution vector x_i at iteration t. The step size is the strength of the population represented as Parameter L_{dis}. The insects usually move over a long distance with distinct steps; therefore, a Levy flight can be used to mimic this characteristic. $L_{dis} > 0$ is taken through a Levy distribution.

$$\mathrm{L} \sim \frac{\lambda \Gamma(\lambda) \sin\left(\frac{\pi\lambda}{2}\right)}{\pi} \frac{1}{\boldsymbol{\delta 1} + \lambda}, s \ll 0 \tag{7}$$

In all the simulations in this research, the distribution remains acceptable for large steps $\delta > 0$. In this paper, $\lambda = 1.5$.

A subset feature generation is a heuristic search technique in which each sample in the search area in order defines the evaluation of the candidate subset's solution. One of the fundamental problems determines the method of selecting the feature by technique. The starting point of the search should be determined first because it determines the search path. To begin, an empty set is used to start the FS's search operation, followed by the insertion of the attributes one after the other; or vice versa, it begins with a full set of attributes and then reduces one after the other. As a consequence, the proposed approach BFPA algorithm then starts producing a random subset.

The dataset is represented as a vector with a length of 19 attributes or features, patterns and behaviours of normal and abnormal data are represented by features. The expression represents a random candidate generated by the proposed algorithm, and each feature is associated with a feature or feature with the dataset, i.e., the number of cells of bytes vector (x) equals the number of attributes o (x = 19 bytes) matrix length. The value [1; 0] represents the representation of the value of (x) in the vector cells of the matrix. If (x) equals 1, the FS of a specific feature is observed, but if (x) equals 0, the cell has no specific feature. Fig. 6 depicts a randomly generated FPA algorithm using the algorithm. The random matrix generated during the FS (FPA-FA) stage consists of (0) and (1). Fig. 7 represents an example of an FPA algorithm for generating a candidate solution. After the proposed algorithm completes random solution generation, the value of each solution's fitness function is ultimately calculated and evaluated by using the workbook. After completing all the iterations of the algorithm, the optimal subset is selected based on the accuracy rate or the accuracy rate and the number of features.

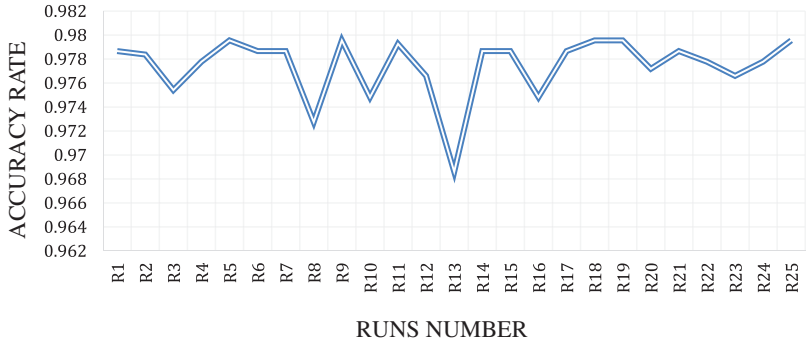

Figure 7: Detection accuracy rate proposed mothed binary flower pollination algorithm flooding Attacks m for each run

4.2.4 Evaluate Current Optimal Subset Using SVM

The fitness function is used to evaluate the proposed algorithm's generated solution value after the standard criterion is given to select the optimal subset or select the best solution. This function is used in many studies to determine the detection accuracy rate of the proposed algorithm by using the classifier after selecting a subset, and the best subgroup is chosen by calculating the detection accuracy rate using the following Equation:

$$Accuracy\ Rate = \frac{TP + TN}{TP + TN + FP + FN} \tag{8}$$

FP: the sum of the samples in the attack class that the classifier incorrectly predicted, namely the false positive; FN: the sum of the samples in the normal class that the classifier incorrectly predicted, notably false negative; TP: the sum of the samples in the class of attack that the classifier correctly predicted, also known as the true positive; TN: the sum of the samples in the normal class that the classifier correctly predicted, also known as the true negative.

Precision is the percentage of the correctly detected attack samples from the total number of samples that are classified as attacks. It can be calculated using Eq. (10)

$$Precision = \frac{TP}{TP + FP} \tag{9}$$

Recall is a metric that quantifies the number of correct positive predictions made out of all positive predictions that could have been made.

$$\text{Recall} = \frac{TP}{TP + FN} \tag{10}$$

F1−score is the weighted harmonic mean of the precision and recall values. The F1−score value ranges from 0 to 1; 1 means that the decision of attacks is accurate. The F1−score value is calculated using Eq. (9).

$$\text{F1} - \text{score} = 2 * \frac{Precision * \text{Recall}}{Precision + \text{Recall}} \tag{11}$$

The advantages of the objective function depend on the selected feature when evaluating the detection accuracy rate. Therefore, more time and resources are required if the optimal solution for a large subset contains selected features. The accuracy rate evaluating the current optimal subset selection process is responsible for selecting the optimal solution that contributes to optimal subset

selection. In this paper, an SVM classifier is used to calculate detection accuracy and evaluate the proposed approach. It considers an example of real-world applications due to machine learning rigidity. It can solve the binary classification problem by using the simplest separated hyperplane model defined by support vectors, which are classified during training as a subset of data to distinguish between normal and abnormal traffic. The SVM classifier divides the dataset into two parts: the testing dataset and the training dataset. The latter is made up of records that contain features chosen in the previous step and are divided into two categories: normal data and attack data. The test dataset includes one known offensive category and one unknown. All types of attacks in the dataset are aware of it while finding the attacks that are known to exist in the test dataset, to obtain a strong classifier model that can predict the target samples using database features via an SVM classifier. Fig. 6 represents model training and testing detection. The current optimal subset step employing the FS (BFPA-FA) stage assesses the best solution using machine learning algorithms (SVM classifier).

Fig. 6 presents the process of optimizing specific features or the resultant subset to build a robust learning model. These specific features of the training dataset are used to fit the SVM classifier parameters, such as hyper boundaries of lines. In practice, training data is a set of data whose inputs are pairs (scalar or vector) and the corresponding outputs (vector or scalar), which are denoted by (target or label). As shown in Eq. (6), the optimum subset features are evaluated by relying on different measures (measurement evaluation). In this paper, the model is evaluated to detect and verify the detection's strength and rigidity. After training the classifier on the training dataset, a test dataset that contains an optimal subset is selected by the BFPA algorithm to ensure the classified SVM in the ICMPv6 DDoS dataset. In addition, cross-verification test approaches are used for attack detection testing, and it uses test data that is part of the training dataset and is based on the ratio.

4.2.5 Update the Optimal Best Solution

The optimal solution is to update G^*_{best}. The flower location (G^*_{best}) for global best (solution) modified with each iteration's most recent results,

$$if\ x^i_j < f\ G^*_{best}$$

BFPA repeats the third and fourth stages until the completion criterion is met. The end benchmark satisfies several normally dependent criteria, such as the number of iterations, or obtains a satisfactory result.

Iteratively calculating the fitness function of the subset generated by the proposed algorithm after it has been evaluated by the classifier (SVM) and compared to the previous solutions because it contains the optimal subset of features that affect detection accuracy yields the optimal solution. In case the new solution (subset) has the highest detection accuracy rate, it replaces the old solution. If its detection accuracy rate is lower, it is ignored. As we explained in the previous steps and according to Table 1, solutions (subgroups) generated randomly by the BFPA algorithm do not even fall in location (minimum and maximum). Randomly generated solutions in the form of a 2D matrix (n ∗ m), which are the total features represented by the vector (n) and the total solutions (subgroup) (20) generated randomly by the vector (M). For each solution, a fitness function calculation is performed and evaluated using the classifier, and the best optimal solution with the highest detection accuracy is chosen. The new solution is compared to the previous optimal solution. If the new solution has a higher accuracy rate than the old optimal solution, it becomes the optimal solution; otherwise, it is ignored. This process is repeated for all iterations (100 iterations).

5 Result and Discussion

This section describes the evaluation metrics and experimental environments used to evaluate the proposed approach. the performance of the proposed approach in detecting DDoS attacks based on. a set of classifiers is selected which are Decision Tree, Support Vector Machine (SVM), Naïve Bayes, K-Nearest Neighbours (KNN), Neural Networks, and Random Forest Trees to detection accuracy. The classifiers selected are ready-made without any changes to the parameters since the aim is to choose the best classifier in terms of detection accuracy after applying the optimal solution of the BFPA algorithm in a set of classifiers to select the better classifier that achieves a higher detection accuracy show in Table 2.

As illustrated in Table 2 after applying six classifiers to the optimal subset solution to the BFPA algorithm by using the ICMPv6-DDoS dataset. Support Vector Machine (SVM) classifier obtained high detection accuracy. These results indicate that the SVM is the most efficient in detecting ICMPv6 DDoS flooding attacks; therefore, it is the most suitable for evaluating the proposed BFPA-FA.

Table 2: Comparison of classifiers detection accuracy using cross-validation

Type of classifiers	Accuracy
Decision tree	97.70
Support vector machine	97.96
Naïve bayes	95.61
K-nearest neighbours	97.73
Neural networks	97.71
Random forest	97.33

The experiment results show that the BFPA-FA method for detecting DDoS flooding attacks in an ICMPv6 message dataset, Table 3 shows the results of experiments conducted using the parameters shown in the confusion matrix and applied to the SVM classifier and the BFPA-FA method for detecting DDoS flooding attacks in the ICMPv6 message dataset. The TP parameter in the BFPA-FA method outperformed the SVM classifier. As a result, the BFPA-FA method improves the detection of abnormal traffic in the ICMPv6 message dataset. In terms of FP parameter outcome, the BFPA-FA method achieved a lower false alarm rate than the SVM classifier. The fitness function aims to improve the accuracy of detection and reduce the number of false alarms; consequently, the observed outcome was expected.

Table 3: Experimental results of confusion matrix parameters

Measures	Full set of features with SVM	BFPA-FA with SVM
TP	1768	1823
FP	63	26
TN	1479	1484
FN	48	43

For the TN parameter, the BFPA-FA method yielded the best results for DDoS flooding attack detection in ICMPv6 messages, while the SVM classifier yielded the worst results. Finally, the BFPA-FA method produced the best results for DDoS flooding attack detection in ICMPv6 messages for the FN parameter. These findings demonstrate the effectiveness of the BFPA-FA method in reducing the number of anomalous instances incorrectly classified.

The **B**FPA-FA method and the SVM classifier achieve the number of features and detection accuracy shown in Table 4.

Table 4 shows the detection accuracy rate calculated from the experiment runs, as well as the iterations mentioned previously. Eq. (8) was used to solve for the detection accuracy rate of the SVM classifier and FPA-FA method. The FPA-FA method achieved the highest detection accuracy (97.95) compared to the SVM classifier when detecting DDoS flooding attacks via ICMPv6 message. It shows that the FPA-FA method achieved fewer features (9) in the best detection accuracy rate during the experiment runs and several features in the worst detection accuracy rate (11). Table 4 shows the lowest detection accuracy rate achieved by (9) features compared to several SVM classifier features (19).

Table 4: The number of selected features with maximum accuracy of classification

Type of method	Accuracy	Precision	Recall	F1−score	Number of features
All features	96.71%	96.55%	97.30%	96.49%	19
BFPA-FA	97.95%	98.59%	97.69%	97.49%	9

Table 4 presents the Precision, recall, and F-score metrics from the experiment runs, as well as the iterations, mentioned previously. Eqs. (9)–(11) was used to obtain the Precision, recall, and F-score rate of the SVM classifier and FPA-FA method, proposed FPA-FA algorithms obtained the best rates in Precision, recall, and F-score metric evaluation metrics compared to the SVM classifier.

Fig. 7 shows the BFPA-FA method detection accuracy rate for 25 runs of DDoS flooding attack detection runs via ICMPv6 message. Table 1 shows the number of iterations (100) in each run of the FPA algorithms. The chart shows that the BFPA-FA method achieved the highest detection accuracy rate (97.95%) for five number runs (5,9,18,19,25) but achieved the lowest detection accuracy rate (97.27%) achieved the highest detection accuracy rate from the classifier (96.71 features), as shown in Table 4.

Fig. 8 shows the features obtained by the BFPA-FA method for 25 runs of DDoS flooding attack detection through ICMPv6 message and the algorithm executed for 100 iterations to produce the number of selected features in each run, as shown in Table 1. It shows that the FPA-FA method achieved fewer features (9) in the best detection accuracy rate during the experiment runs and several features in the worst detection accuracy rate (11). The lowest detection accuracy rate was achieved through (9) features compared to several features of the SVM classifier (19) as indicated in Table 4.

Table 5 shows the best, average, mean, and worst results of the BFPA-FA proposed detection accuracy rate and several features for DDoS flooding attack detection ICMPv6 message, which was obtained from 25 runs of the experiment, the best detection accuracy rate of BFPA-FA proposed (97.95) and the number of features (9) and the worst (97.27) and the number of features (11). As for the medium detection accuracy rate (97.86) and mean (97.74), the number of features for medium and mean was (9, 10), respectively.

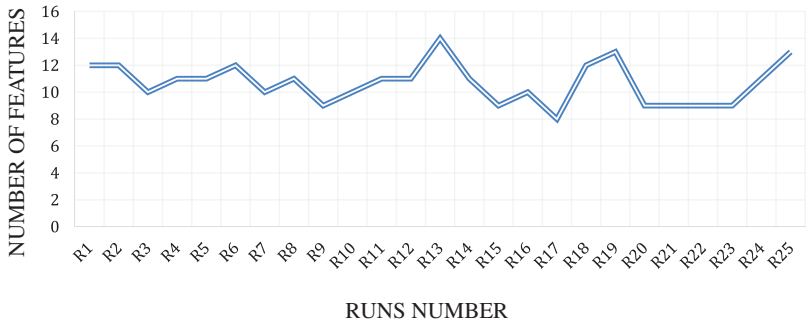

Figure 8: Number of features rate of proposed mothed binary flower pollination algorithm flooding attacks for each run

Table 5: The number of features and best, average, median, and worst detection accuracy results of the proposed mothed binary flower pollination algorithm flooding attacks proposed and

Measures	Accuracy rate	Selected features
Best	97.95%	9
Mediam	97.86%	9
Average	97.74%	11
Worst	96.86%	14

This study presented the experimental results of the proposed method BFPA-FA achieved a low number of features (9) and a good (97.95) detection accuracy rate compared to the classifier only used for DDoS flooding attack detection via the ICMPv6 message dataset.in addition, the BFPA algorithm obtained an optimal subset by FS had a significant impact on detecting the attack. The BFPA algorithm outperformed the classifier alone in terms of detection accuracy. Furthermore, the number of features in the proposed BFPA-FA was lower. As for the medium detection accuracy rate (97.86) and Mean (97.74), the number of features for medium and mean was (9, 10), respectively.

The proposed method BFPA-FA contributed to improving detection accuracy by determining optimal features using FS technology, it was the number of features was reduced to half (9) of the total (19) the number of features. The detection accuracy rate of the proposed method converging of values in the average, maximum, median, and worst detection, as a result, the proposed method is stable. The experimental results indicate BFPA-FA method is effective in detecting attacks and its ability to obtain the optimal subset which contributes to detecting the attack to solve the binary problem (normal and attack) also contributed to a lower time, data volume, and complexity.

Despite the high accuracies and lower number of features achieved by the proposed approach representation in the cross-validation test and presentation of simulation and parameter settings of the BFPA algorithm (see Table 2), which were not achieved when nonqualified features with data amount and complexity were used. The features lead the classifier to consider specific values (such as an IP address, protocol, or source) to differentiate between normal and abnormal traffic. Consequently, a dataset containing the same attack set with a different best subset of features yielded superior results.

In contrast, the proposed method achieved fewer features with high detection accuracy on the same or a different testing and training dataset (see Tables 4 and 5). The BFPA has determined the

dependability and robustness of the detection model constructed with these novel features. In general, using the selected features, the proposed approach achieved an acceptable and high accuracy detection rate in both testing approaches. Furthermore, when the dataset is compared to the full features in the dataset for the classifier, the selected feature and approach proposed show high accuracy rates. In the classifier's cross-validation test, the IDSs achieved lower accuracy rates. However, the proposed method represents an optimal subset of the dataset's features that have achieved high rates of accuracy, proving that the features obtained by the BFPA can be used in any input dataset for any detection system. The number of features and maximum accuracy were improved by executing the experiment 25 times using the proposed method. Minimum, average, and maximum values were used to calculate the number of features and accuracy of detection for the proposed method.

Several ground truth experiments were carried out to determine the effectiveness of the features and the proposed dataset representation. The first such experiment was carried out by utilizing the basic features of the SVM classifier. An acceptable detection accuracy rate was achieved. The second experiment demonstrated that the BFPA-FA method aided in the generation of an optimal subset of features. The number of features was reduced, and the classifier's detection accuracy was improved to a greater extent when the selected features were compared to the existing features. Overall, the proposed BFPA algorithm can enhance the detection accuracy of IDS by optimally selecting a set of features that contributed to high classification accuracy.

6 Conclusion and Future Work

The proposed approach's primary goal is to ensure that the BFPA algorithm improves the performance of ICMPv6 DDoS flooding attack detection in the IPv6 network. The BFPA algorithm, which was used by the FS technique to select the best optimal subset, contributed to an increase in classification accuracy. To evaluate the efficacy of the BFPA-FA. This paper relied on dataset generation, preparation, and analysis by the FS technique to determine and select the best optimal feature from the dataset. These stages were critical to the success of the proposed approach (BFPA-FA) and demonstrated the efficacy of anomaly-based detection (IDS) for attack detection. Furthermore, the proposed approach (BFPA-FA) can detect attacks with fewer features (9), compared to a total of 19 features with high accuracy. The proposed algorithm in the future can be modified to be more adaptive in selecting the best optimal features to solve the binary problem of detecting flooding attacks in the ICMPv6 message dataset. The hybridization of the proposed algorithm with other bio-inspired algorithms can solve a problem for local search (local minima) and contribute to improving anomaly-based detection (IDS) and achieving a high accuracy detection rate. BFPA algorithms can also be used in a multi-objective function to solve a binary problem (optimisation problem) and obtain a high detection accuracy rate with a smaller number of features. Finally, novel techniques can be used to counter new types of IPv6 network attacks. Finally, apply the proposed approach (BFPA-FA) to a real-world dataset to validate the performance and accuracy detection for future work.

Acknowledgement: The authors would like to acknowledge the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM) for providing the necessary facilities and support. The funding for this research was provided by Universiti Sains Malaysia (USM) and Iraq Airways Company (IA).

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

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

References

[1] A. H. Bdair, R. Abdullah, S. Manickam and A. K. Al-Ani, "Brief of intrusion detection systems in detecting ICMPv6 attacks," in *Computational Science and Technology*, Singapore: Springer, pp. 199–213, 2020.

[2] M. Tahir, M. Li, N. Ayoub, U. Shehzaib and A. Wagan, "A novel DDoS floods detection and testing approaches for network traffic based on linux techniques," *International Journal of Advanced Computer Science And Applications*, vol. 9, no. 2, pp. 341–357, 2018.

[3] O. Brun, Y. Yin, E. Gelenbe, Y. M. Kadioglu and J. Augusto-Gonzalez, "Deep learning with dense random neural networks for detecting attacks against IoT-connected home environments," in *Int. ISCIS Security Workshop*, Cham, Springer, pp. 79–89, 2018.

[4] M. Education, M. A. Sadat and P. Meel, "Lab implementation of IPv6 in enterprise network using cisco packet tracer," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 10, pp. 6564–6580, 2021.

[5] O. E. Elejla, B. Belaton, M. Anbar and I. M. Smadi, "A New set of features for detecting router advertisement flooding attacks," in *Proc. - 2017 Palestinian Int. Conf. on Information and Communication Technology*, Gaza (Palestine), pp. 1–5, 2017.

[6] A. Rosli, A. Mat Taib, W. N. A. Wan Ali and R. S. Hamid, "Application of grounded theory in determining required elements for ipv6 risk assessment equation," in *MATEC Web of Conf.*, France, vol. 150, 2018.

[7] "Google," Statistics about ipv6 connectivity among google users. 2022. [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html?safe=active

[8] A. K. Al-Ani, M. Anbar, S. Manickam, A. Al-Ani and Y. B. Leau, "Proposed DAD-match mechanism for securing duplicate address detection process in ipv6 link-local network based on symmetric-key algorithm," in *Int. Conf. on Computational Science and Technology*, Singapore, Springer, pp. 108–118, 2017.

[9] R. Khader and D. Eleyan, "Survey of DoS/DDoS attacks in IoT," *Sustainable Engineering and Innovation*, vol. 3, no. 1, pp. 23–28, 2021.

[10] A. H. B. Aighuraibawi, R. Abdullah, S. Manickam and Z. A. A. Alyasseri, "Detection of ICMPv6-based DDoS attacks using anomaly based intrusion detection system: A comprehensive review," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 6, pp. 5216–5228, 2021.

[11] M. Sheikhan and H. Bostani, "A Hybrid intrusion detection architecture for internet of things," in *2016 8th Int. Symp. on Telecommunications (IST)*, United States, IEEE, pp. 601–606, 2016.

[12] V. Jyothsna, "A review of anomaly based intrusion detection systems," *International Journal of Computer Applications*, vol. 28, no. 7, pp. 975–8887, 2011.

[13] J. P. Amaral, L. M. Oliveira, J. J. P. C. Rodrigues, G. Han and L. Shu, "Policy and network-based intrusion detection system for ipv6-enabled wireless sensor networks," in *2014 IEEE Int. Conf. on Communications (ICC)*, Sydney, Australia, IEEE, pp. 1796–1801, 2014.

[14] M. Manninen, "Using artificial intelligence in intrusion detection systems," *Helsinki University of Technology*, vol. 13, pp. 69–76, 2002.

[15] O. E. Elejla, M. Anbar and B. Belaton, "ICMPv6-based DoS and DDoS attacks and defense mechanisms: Review," *IETE Tech. Rev. Institution Electron. Telecommun. Eng. India*, vol. 34, no. 4, pp. 390–407, 2017.

[16] O. E. Elejla, B. Belaton, M. Anbar and A. Alnajjar, "Intrusion detection systems of ICMPv6-based DDoS attacks," *Neural Computing and Applications*, vol. 30, no. December, pp. 1–12, 2016.

[17] K. Albulayhi and F. T. Sheldon, "An adaptive deep-ensemble anomaly-based intrusion detection system for the internet of things," in *2021 IEEE World AI IoT Congress*, Seattle, USA, pp. 187–196, 2021.

[18] F. Safara, A. Souri and M. Serrizadeh, "Improved intrusion detection method for communication networks using association rule mining and artificial neural networks," *IET Communications*, vol. 14, no. 7, pp. 1192–1197, 2020.

[19] F. Pascale, E. A. Adinolfi, S. Coppola and E. Santonicola, "Cybersecurity in automotive: An intrusion detection system in connected vehicles," *Electronics*, vol. 10, no. 15, pp. 1–16, 2021.

[20] X. -S. Yang, "Flower pollination algorithm for global optimization," in *Int. Conf. On Unconventional Computing and Natural Computation*, Berlin, Heidelberg, Springer, pp. 240–249, 2012.

[21] C. Ioannou and V. Vassiliou, "Classifying security attacks in iot networks using supervised learning," in *Proc. - 15th Annu. Int. Conf. Distrib. Comput. Sens. Syst. DCOSS 2019*, Santorini Island, Greece, pp. 652–658, 2019.

[22] S. Manickam, A. Aighuraibawi, R. Abdullah, Z. Alyasseri and K. Abdulkareem, "Labelled dataset on distributed denial-of-service (DDoS) attacks based on internet control message protocol version 6 (ICMPv6)," *Wireless Communications and Mobile Computing*, vol. 2022, no. April, pp. 1–13, 2022.

[23] F. Hajjej, R. Ejbali and M. Zaied, "An efficient deployment approach for improved coverage in wireless sensor networks based on flower pollination algorithm," *NETCOM, NCS, WiMoNe, GRAPH-HOC, SPM, CSEIT*, vol. 2016, no. 23, pp. 117–129, 2016.

[24] A. Y. Abdelaziz, E. S. Ali and S. M. Abd Elazim, "Flower pollination algorithm to solve combined economic and emission dispatch problems," *Engineering Science and Technology, an International Journal*, vol. 19, no. 2, pp. 980–990, 2016.

[25] K. Rajalashmi and S. U. Prabha, "A hybrid algorithm for multiobjective optimal power flow problem using particle swarm algorithm and enhanced flower pollination algorithm," *Asian Journal of Social Sciences & Humanities*, vol. 7, no. 1, pp. 923, 2017.

[26] S. Ouadfel and A. Taleb-Ahmed, "Social spiders optimization and flower pollination algorithm for multilevel image thresholding: A performance study," *Expert Systems with Applications*, vol. 55, pp. 566–584, 2016.

[27] D. Rodrigues, G. F. A. Silva, J. P. Papa, A. N. Marana and X. S. Yang, "EEG-based person identification through binary flower pollination algorithm," *Expert Systems with Applications*, vol. 62, pp. 81–90, 2016.

[28] P. Agarwal and S. Mehta, "Enhanced flower pollination algorithm on data clustering," *International Journal of Computer Applications*, vol. 38, no. 2–3, pp. 144–155, 2016.

[29] H. Chiroma, A. Khan, A. Abubakar, Y. Saadi and M. Hamza, "A new approach for forecasting opec petroleum consumption based on neural network train by using flower pollination algorithm," *Applied Soft Computing*, vol. 48, pp. 50–58, 2016.

[30] S. M. Nigdeli, G. Bekdas and X. S. Yang, "Application of the flower pollination algorithm in structural engineering," in *Metaheuristics and Optimization in Civil Engineering*, Cham: Springer, pp. 25–42, 2016.

[31] O. K. Meng, O. Pauline, S. C. Kiong, H. A. Wahab and N. Jafferi, "Application of modified flower pollination algorithm on mechanical engineering design problem," *IOP Conference Series: Materials Science and Engineering*, vol. 165, no. 1, pp. 012032, 2017.

[32] E. Nabil, "A modified flower pollination algorithm for global optimization," *Expert Systems with Applications*, vol. 57, no. 15, pp. 192–203, 2016.

[33] C. B. Pop, V. R. Chifu, I. Salomie, D. S. Racz and R. M. Bonta, "Hybridization of the flower pollination algorithm a case study in the problem of generating healthy nutritional meals for older adults," *Modeling and Optimization in Science and Technologies*, vol. 10, pp. 151–183, 2017.

[34] S. Pant, A. Kumar and M. Ram, "Flower pollination algorithm development: A state of art review," *International Journal of System Assurance Engineering and Management*, vol. 8, no. S2, pp. 1858–1866, 2017.

[35] Z. A. A. Alyasseri, A. T. Khader, M. A. Al-betar, M. A. Awadallah, X. Yang *et al.,* "Variants of the flower pollination algorithm: A review," *Springer*, vol. 744, no. October 2017, pp. 91–118, 2018.

[36] J. A. Regalado, B. E. Emilio and E. Cuevas, "Optimal power flow solution using modified flower pollination algorithm," in *2015 IEEE Int. Autumn Meeting on Power, Electronics and Computing (ROPEC)*, Ixtapa, Mexico, pp. 1–6, 2015.

[37] S. Mahata, S. K. Saha, R. Kar and D. Mandal, "Optimal design of wideband digital integrators and differentiators using hybrid flower pollination algorithm," *Soft Computing*, vol. 22, no. 11, pp. 3757–3783, 2018.

[38] E. Emary, H. M. Zawbaa, A. E. Hassanien and B. Parv, "Multi-objective retinal vessel localization using flower pollination search algorithm with pattern search," *Advances in Data Analysis and Classification*, vol. 11, no. 3, pp. 611–627, 2017.

[39] J. Nayak, S. K. Meher, A. Souri, B. Naik and S. Vimal, "Extreme learning machine and bayesian optimization-driven intelligent framework for iomt cyber-attack detection," *The Journal of Supercomputing*, vol. 78, no. 13, pp. 14866–14891, 2022.

[40] N. Acharya and S. Singh, "An IWD-based feature selection method for intrusion detection system," *Soft Computing*, vol. 22, no. 13, pp. 4407–4416, 2018.

[41] L. Xue, X. Ma, X. Luo, E. W. Chan, T. T. Miu *et al.,* "Linkscope: Toward detecting target link flooding attacks," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2423–2438, 2018.

[42] A. Hendrawan, A. F. Daru and A. M. Hirzan, "Intrusion detection with wireless sensor network (WSN) internet of things," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 13, no. 2, pp. 45–48, 2021.

[43] M. Rezvani, "Assessment methodology for anomaly-based intrusion detection in cloud computing," *Journal of AI and Data Mining*, vol. 6, no. 2, pp. 387–397, 2018.

[44] W. Li, W. Meng and L. F. Kwok, "Investigating the influence of special on-off attacks on challenge-based collaborative intrusion detection networks," *Futur Internet*, vol. 10, no. 1, pp. 1–16, 2018.

[45] A. Sharon, P. Mohanraj, T. E. Abraham, B. Sundan and A. Thangasamy, "An Intelligent intrusion detection system using hybrid deep learning approaches in cloud environment," in *IFIP Advances in Information and Communication Technology*, United States, vol. 651, pp. 281–298, 2022.

[46] A. Thangasamy, B. Sundan and L. Govindaraj, "A Novel framework for DDoS attacks detection using hybrid LSTM techniques," *Computer Systems Science and Engineering*, vol. 1, no. 100, pp. 1–15, 2023.

[47] M. Schrötter, T. Scheffler and B. Schnor, "Evaluation of intrusion detection systems in IPv6 networks," in *ICETE 2019 - Proc. of the 16th Int. Joint Conf. on e-Business and Telecommunications*, Prague, Czech Republic, vol. 2, pp. 408–416, 2019.

[48] O. E. Elejla, B. Belaton, M. Anbar, B. Alabsi and A. K. Al-ani, "Comparison of classification algorithms on ICMPv6-based DDoS attacks detection," in *Computational Science and Technology*, Singapore: Springer, pp. 347–357, 2019.

[49] J. E. Varghese and B. Muniyal, "An Efficient IDS framework for ddos attacks in sdn environment," *IEEE Access*, vol. 9, pp. 69680–69699, 2021.

[50] O. E. Elejla, M. Anbar, B. Belaton and B. O. Alijla, "Flow-based IDS for ICMPv6-based DDoS attacks detection," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 7757–7775, 2018.

[51] O. E. Elejla, B. Belaton, M. Anbar, B. Alabsi and A. K. Al-Ani, "Comparison of classification algorithms on icmpv6-based ddos attacks detection," in *Computational Science and Technology: 5th ICCST 2018, Kota Kinabalu, Malaysia, 29-30 August*, Singapore: Springer, pp. 347–357, 2019.

[52] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba and K. Das, "1999 DARPA off-line intrusion detection evaluation," *Comput. Networks*, vol. 34, no. 4, pp. 579–595, 2000.

[53] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis and P. K. Chan, "Cost-based modeling for fraud and intrusion detection: Results from the JAM project," in *Proc. - DARPA Information Survivability Conf. and Exposition, DISCEX 2000*, South Carolina, USA, vol. 2, pp. 130–144, 2000.

[54] B. Venkatesh and J. Anuradha, "A review of feature selection and its methods," *Cybernetics and Information Technologies*, vol. 19, no. 1, pp. 3–26, 2019.

[55] Y. Xue, Y. Tang, X. Xu, J. Liang and F. Neri, "Multi-objective feature selection with missing data in classification," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 6, no. 2, pp. 1–10, 2021.

[56] Saraswat Ayush, "Intrusion detection system (IDS) and its detailed working function – SOC/SIEM," 2017. [Online]. Available: https://professionalhackers.in/intrusion-detection-system-ids-and-its-detailed-working-function-soc-siem/

[57] K. Albulayhi, Q. A. Al-Haija, S. A. Alsuhibany, A. A. Jillepalli and M. Ashrafuzzaman, "IoT intrusion detection using machine learning with a novel high performing feature selection method," *Applied Sciences (Switzerland)*, vol. 16, no. 10, pp. 1–30, 2022.

[58] M. Tubishat, S. Ja'afar, M. Alswaitti, S. Mirjalili, N. Idris *et al.,* "Dynamic salp swarm algorithm for feature selection," *Expert Systems with Applications*, vol. 1, no. 164, pp. 113873, 2021.

[59] B. Kumari and T. Swarnkar, "Filter versus wrapper feature subset selection in large dimensionality micro array: A review," *International Journal of Computer Science and Information Technologies*, vol. 2, no. 3, pp. 1048–1053, 2011.

[60] M. Zulkiflee, M. Ahmad, S. Sahib and M. Ghani, "A framework of features selection for ipv6 network attacks detection," *WSEAS Trans. Commun*. vol. 14, no. 46, pp. 399–408, 2015.

[61] Z. A. A. Alyasseri, A. T. Khader, M. A. Al-Betar and O. A. Alomari, "Person identification using EEG channel selection with hybrid flower pollination algorithm," *Pattern Recognit*., vol. 105, no. 2020, pp. 107393, 2020.

[62] Z. A. A. Alyasseri, A. T. Khader, M. A. Al-Betar, J. P. Papa and O. A. Alomari, "Classification of EEG mental tasks using multi-objective flower pollination algorithm for person identification," *International Journal of Integrated Engineering*, vol. 10, no. 7, pp. 102–116, 2018.