International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v10i6.5557
***Article Received**: 10 April 2022 **Revised**: 18 May 2022 **Accepted**: 02 June 2022 **Publication**: 30 June 2022*

Adaptive Learning Based Whale Optimization and Convolutional Neural Network Algorithm for Distributed Denial of Service Attack Detection in Software Defined Network Environment

S Renuka Devi[1], L Shyamala[2]*, S Saraswathi[3]
[1,2]Associate Professor, School of Computer science and engineering, Vellore Institute of Technology, Chennai
[3] Associate Professor, Department of Computer science and engineering, SSN College of Engineering, Chennai

Abstract

SDNs (Software Defined Networks) have emerged as a game-changing network concept. It can fulfill the ever-increasing needs of future networks and is increasingly being employed in data centres and operator networks. It does, however, confront certain fundamental security concerns, such as DDoS (Distributed Denial of Service) assaults. To address the aforementioned concerns, the ALWO+CNN method, which combines ALWOs (Adaptive Learning based Whale Optimizations) with CNNs (Convolution Neural Networks), is suggested in this paper. Initially, preprocessing is performed using the KMC (K-Means Clustering) algorithm, which is used to significantly reduce noise data. The preprocessed data is then used in the feature selection process, which is carried out by ALWOs. Its purpose is to pick out important and superfluous characteristics from the dataset. It enhances DDoS classification accuracy by using the best algorithms. The selected characteristics are then used in the classification step, where CNNs are used to identify and categorize DDoS assaults efficiently. Finally, the ALWO+CNN algorithm is used to leverage the rate and asymmetry properties of the flows in order to detect suspicious flows specified by the detection trigger mechanism. The controller will next take the necessary steps to defend against DDoS assaults. The ALWO+CNN algorithm greatly improves detection accuracy and efficiency, as well as preventing DDoS assaults on SDNs. Based on the experimental results, it was determined that the suggested ALWO+CNN method outperforms current algorithms in terms of better accuracies, precisions, recalls, f-measures, and computational complexities.

Keywords: Software Defined Network (SDNs), Distributed Denial of Service (DDoS) attacks, Adaptive Learning based Whale Optimization and Convolution Neural Network (ALWO+CNN) algorithm.

1. Introduction

SDNs are critical technologies that rely on the fundamental principle of separating the network's control and data planes [1]. This attribute offers various benefits, including flexibility, simplicity, and cheaper costs. It does, however, have a number of shortcomings that are mostly caused by the centralised control paradigm. One of the most major issues associated with centralization is security. DDoS assaults are particularly relevant to the SDNs environment in this sense.

When subjected to DDoS assaults, the controller of SDNs get disconnected from the rest of the networks and lose centralized controls [2]. The primary benefit of SDN's centralized network controls can be jeopardized by DDoS assaults, and is one of the most critical security concerns in SDNs. It is very vital to explore DDoS detections and in SDNs of data centres and cloud computing environments for network security assurances.

In DDoS attacks, SDNs controllers receive large number of data packets with forged source/destination IPs for which switches fail to find matches and forwards it back to the controllers or forward them directly [3] using SDNs. Major portions of DDoS attacks are camouflaged as legitimate traffic resulting in depletion of controller's resources and making them unable to analyze regular and lawful packets [4]. The SDNs then go offline even if there are backup SDNs.

For picking the most informative features from the original input data, FSs (Feature Selections) are introduced. FS has a significant role in attack detection since it is effective in improving learning efficacy, enhancing generalisation impact, and obtaining data visualization. In

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v10i6.5557
***Article Received**: 10 April 2022 **Revised**: 18 May 2022 **Accepted**: 02 June 2022 **Publication**: 30 June 2022*

the context of feature selection, a relevant feature contains crucial information about a class, whereas an irrelevant feature has minimal information about the output class and is referred to as an uninformative feature to the output class [5]. The key to resolving the issues is to look for informative features that include as much information about the output class as feasible. Figure 1 depicts the SDN ecosystem.

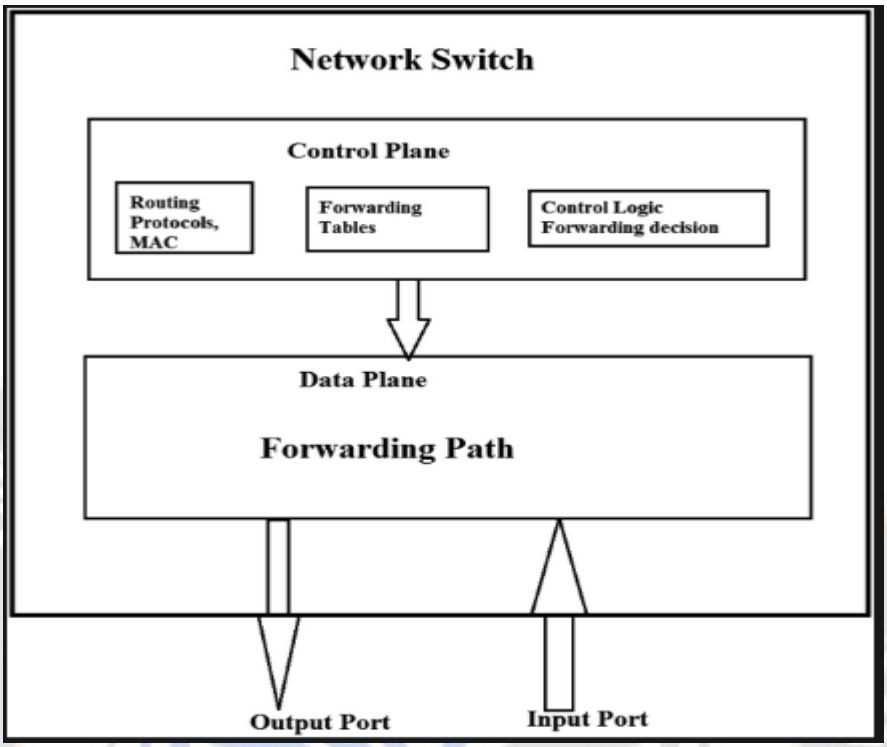

Fig 1 SDNs environment

The technique of anticipating label categories is called classifications which are done using training sets and values for classifying attributes. Classification can also be referred to as class prediction, discriminant analysis, or supervised learning. Classification model used to forecast class labels and test the built model on test data to assess the classification rules' accuracy. DLTs (Deep Learning Techniques) are used to monitor and evaluate enormous amounts of network data, classifying it as abnormal or normal [6]. Because data originates from a variety of sources, network traffic is high. DLTs are used to efficiently create attack detection models.

The primary goal of this research is to identify DDoS attacks in an SDNs environment. Several studies and approaches have been developed, however the accuracy of DDoS attack detection has not improved considerably. The present methods have drawbacks such as computing cost and imprecise attack categorization findings. To address the aforementioned difficulties, the ALWO+CNN algorithm is presented in this study to improve the overall SDNs system performance. This study's key contribution is the development of an SDNs model, preprocessing, feature selection, and detection procedure. The suggested technique employs effective algorithms to produce more accurate IDS findings for the provided dataset.

2. Related Work

Kalkan et al. (2017) emphasized security as one of the most major difficulties associated with centralization in [7]. DDoS assaults are particularly relevant to the SDNs environment in this sense. This article provides a comprehensive overview of DDoS mitigation techniques for software-defined networks. Furthermore, numerous mechanisms are investigated and compared it with other techniques. This study assisted researchers in identifying flaws in these solutions and, as a result, mitigating such attacks with more effective protection measures.

Varghese et al (2021) presented a unique framework in [8] to solve issues in IDSs (intrusion detection systems) and SDN designs and overcome DDoS attacks. The framework integrated data layer's intelligences using DPDKs (Data Plane Development Kits) as a part of their SDN architectures. The framework called D3 (DPDKs-based DDoS Detections) where DPDKs rapidly process and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v10i6.5557
***Article Received**: 10 April 2022 **Revised**: 18 May 2022 **Accepted**: 02 June 2022 **Publication**: 30 June 2022*

monitor packets. The framework's use of VNFs (Virtual Network Functions) in operations of DPDKs helps in quick identifications of DDoS attacks. The study's proposed D3 framework experimental findings corroborated with IDSs in terms of efficiency and efficacy. The publicly accessible CIC DoS statistics also prove that a single statistical anomaly detection technique has a detectable effect against the DDoS attack.

In [9], Alghazzawi et al (2021) proposed hybrid DLTs using CNNs with BiLSTMs (bidirectional long/short-term memories) for DDoS assaul predictions. The study's choice of relevant characteristics and results of the experiments show that their CNNs-BiLSTMs achieved higher accuracies.

In [10], Eslamnezhad et al (2014) proposed novel IDSs based on MinMax KMCs to overcome starting center issues in KMCs and improving clustering quality. Their experimentations on NSL-KDD data set showed that their approach was more efficient than KMCs. Furthermore, the approach has a greater detection rate and a lower risk of false positive detection.

Ravi Kiran Varma et al (2021) addressed the problem of higher dimensionality of datasets, which increases the computational complexity of the detection technique in [11]. To address the aforementioned issue, WOAs is used to minimize dataset features using wrappers and classifier accuracy as the fitness function. This study takes into account the CICDDOD2019 dataset, which has 80 features. The studies are carried out, and the findings show that the overall classification accuracy is not affected, even if the number of characteristics is lowered from 80 to 11, consequently optimizing the detection of DDOS attacks.

Tan et al (2020) filtered abnormal network traffics with their detection triggers in [12]. Hybrid MLTs combining KMCs (K-Means clusters) and KNNs (K-Nearest Neighbors) rated asymmetry properties of data and thus identified suspicious flows with detection triggers. The riggers would intimate controllers to handle the attack which would then adopt proper defenses. The study's co-operative controls and detection methodologies were successful in mitigating DDoS attacks on SDNs.

Wang et al. (2020) suggested DDoS attack detections based on information entropies and DLTs in [13]. Their controller analyzed suspicious traffic using information entropies. Then, using CNNs their model discriminated between normal and attack traffics using fine-grained packet-based detections. Finally, their controller employed defense strategy to thwart onslaughts. Experiments showed that their approach had higher accuracies in identifying DDoS attacks on SDNs effectively.

3. Proposed Methodology

In this paper, the ALWO+CNN technique is developed for detecting DDoS attacks on SDNs. The proposed effort entails the development of an SDNs model, data pre-processing, feature selection, classification, and outcome assessment. Figure 2 depicts the general block diagram of the proposed system.

3.1 SDNs model

In SDNs, controllers are separated from data/ application planes [14] and get connected with applications and data through APIs (Application Programming Interfaces) [14] where network equipments of data plane can be switches, routers, and hubs and security devices, resource monitoring tools, and application management tools are all part of application planes. Controllers are network's brain where device settings and programming tasks take place. DDoS assaults have been proved to be serious dangers to architectures of SDNs as controller are vulnerable to DDoS assaults [15]. In data planes, attackers target routers, switches and even security equipment including firewalls.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v10i6.5557
Article Received: 10 April 2022 Revised: 18 May 2022 Accepted: 02 June 2022 Publication: 30 June 2022

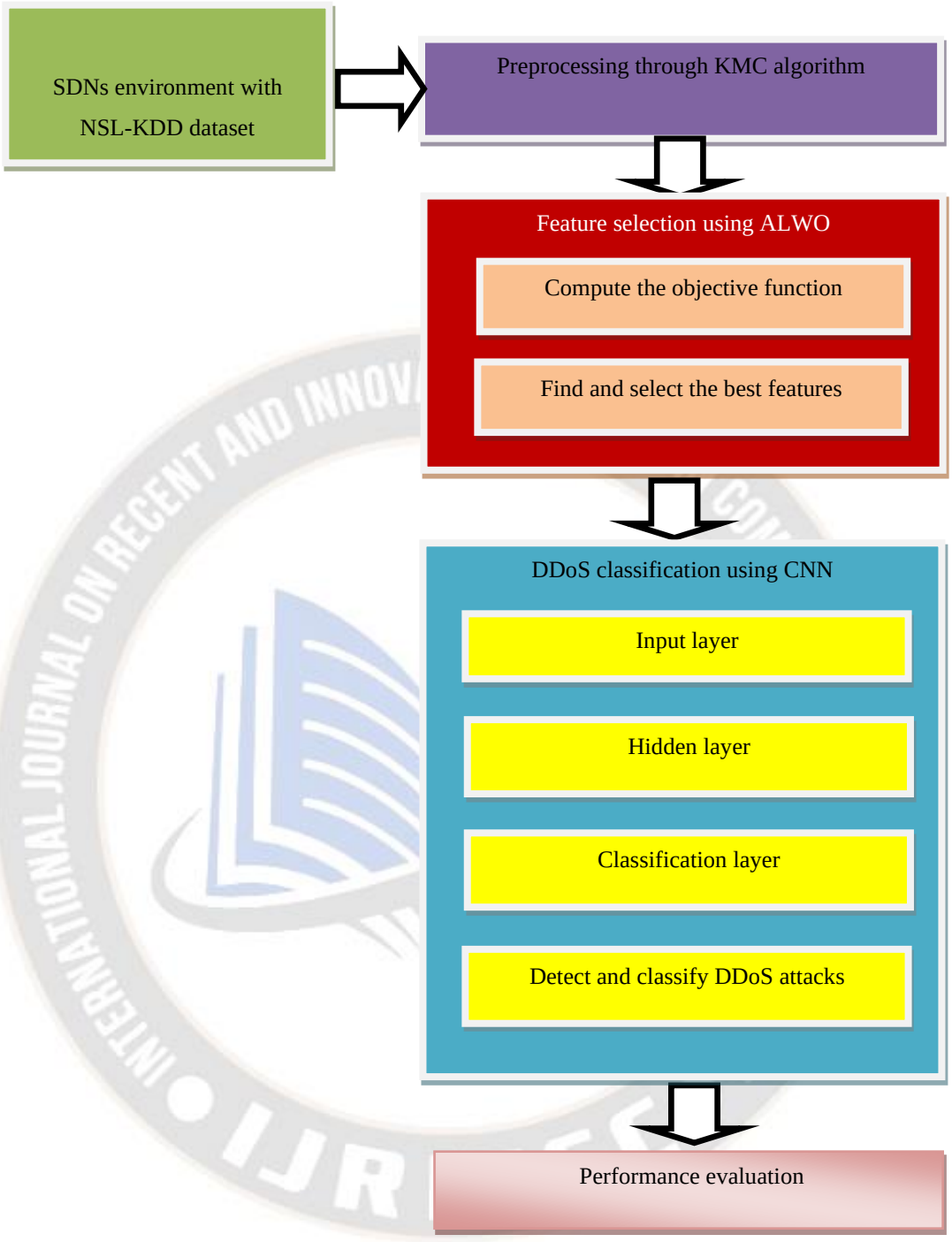

Fig 2 overall block diagram of the proposed system

The data plane in SDNs is in charge of processing and forwarding packets as well as collecting switch information. Core equipments of data planes are switches which are different from conventional networking forwarding equipments. SDN's data plane switches only forward while being optimized for high-speed packet forwards. Since, data planes and controllers in SDNs are different, controllers transmit forwarding strategies of all packets to switches using southbound interface protocols in addition to management of network configurations. This results in reduced complexities of forwarding equipments while considerably improving network administrations and control efficiencies.

3.2 Data pre-processing using Improved K-Means Clustering (KMC) algorithm

Data pre-processed using KMCs enhances DDoS detection accuracies for given datasets (NSL-KDD). In pre-processing, missing values are filled, noises are smoothened,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v10i6.5557
Article Received: 10 April 2022 Revised: 18 May 2022 Accepted: 02 June 2022 Publication: 30 June 2022

redundant information eliminated and inconsistencies resolved. KMCs are sophisticated clustering methods that categorize similar data based on cluster beginning centroids [16] where Euclidean distances determine cluster centroids. Starting with random partitioning, current cluster centres or average vector of clusters in data are computed and data reassigned to the nearest cluster till the assignments of data are complete. Intra-cluster variances get reduced and are defined as the sum of squares of the differences between data attributes and their associated cluster centres. Using preprocessed datasets result in less use of memory, resources and quicker training. Figure 3 illustrates a KMC algorithm example.

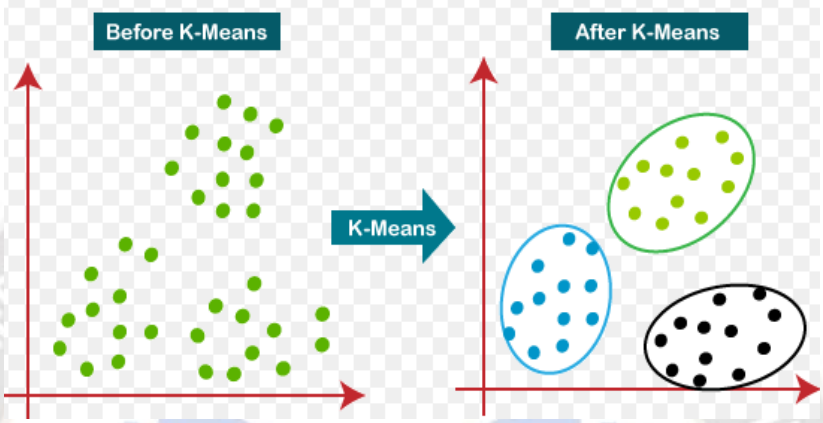

Fig 3 Example of KMC algorithm

The successions of data packets containing identical multiple tuples are called network flows. They signify data packets in networks with same Source/Destination IPs, and Protocos. $S = n\,p(1), p(2), \ldots, p(l), \ldots, p(n)$ o can be utilized to describe a network flow with n packets, where $p(l)$ $(1 \leq l \leq n)$ represents the l-th packet of S. Packet headers include information on source/destination IP addresses with other details. Following the acquisition of the packet header, we partition the data packets into separate network flows based on the quintuple.

The strength of KMCs their runtimes, which are linear to data counts and ease of implementations. In this work, cluster counts are kept constant and equivalent to classes counts. The Euclidean distances between centroids of clusters can be computed using Equation (1).

$$d(i,j) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \qquad (1)$$

Where x_i and y_i are two points in Euclidean n-space

1. Select k clusters from the dataset (D)
2. Set up cluster centres µ1,… µk
3. Select k data points and assign cluster centres to these data points.
4. Assign points to clusters at random and compute cluster means.
5. Determine the cluster centre nearest to each data point and compute the distance measure for locating missing values using (1)
6. Put the data point in this cluster.
7. Re-compute cluster nodes (mean of cluster data points)
8. Locate and eliminate all errors and missing data.
9. When there are no fresh reassignments, stop.

Cases with missing attributes are separated in original datasets which are divided into two groups: those with complete cases and no missing values, and those with incomplete cases with missing values. KMCs create clusters of entire examples resulting in instances being processed one at a time, and filling missing attributes with relative values. Newly added instances are examined if they belong to correct classes in the KMCs clustered dataset. If it is in the correct cluster, the provided value is saved and the procedure repeated for the next instance. In the case of incorrect clusters, the next possible values for data are allocated and compared until instances are placed in correct clusters. Thus, the preprocessing approach is employed to successfully increase the intrusion detection accuracy by employing the KMC algorithm.

3.3 Feature selection using ALWOs

ALWOs are used in this work for efficient feature selections across the DDoS dataset as they discover significant features from provided data in order to determine the existence or absence of DDoS in SDNs. WOAs (Whale

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v10i6.5557
Article Received: 10 April 2022 Revised: 18 May 2022 Accepted: 02 June 2022 Publication: 30 June 2022

Optimization Algorithms) are used to discover the best solution and pick significant characteristics in numerous optimization situations. WOAs algorithm focused on picking relevant features and shown that WOAs performance could be improved further to produce better results, and WOAs could be utilised for feature selection in IDS datasets to achieve reliable detection.

WOAs are inspired by the hunting strategy of humpback whales and the development of a mathematical model for the hunting strategy. The whales utilise a bubble-net technique to circle around the prey, which is generally tiny fish, and consume. Whales swim deep beneath the fish and begin to rise to the surface, generating a large circle of bubbles. The bubbles operate as a trap, forcing the fish to the surface. Whales search for surface-dwelling fish [17]. The hunting process is technically divided into three stages: circling, exploitation, and exploration. The grade of fish consumed is determined by the quality of exploitation and exploration. Encircling phase: During this phase, whales recognise and surround the position of the fishes. Initially, the optimal site is not specified and is chosen at random. Other agents change their position based on the random initiation, and the new position becomes the ideal location to the target.

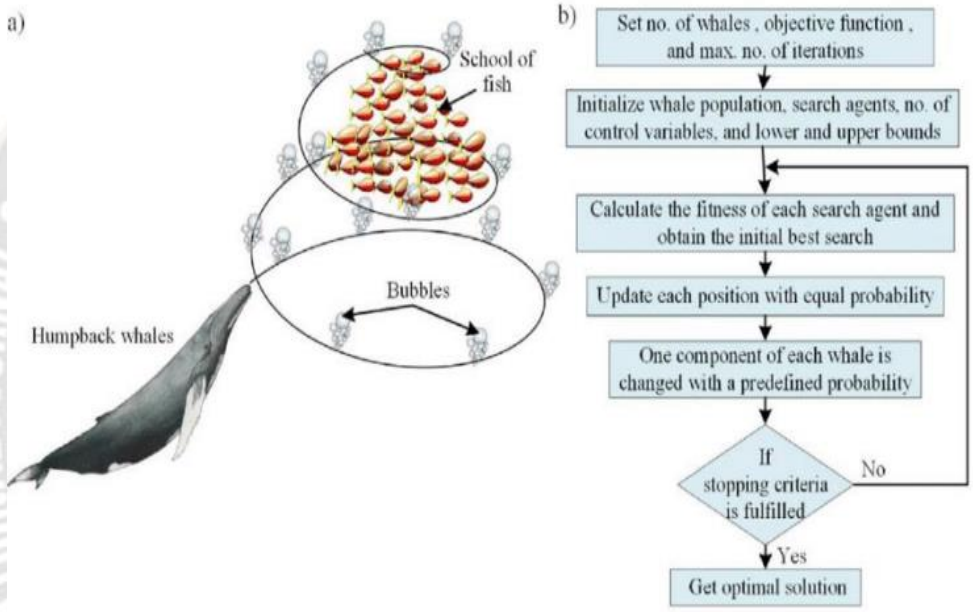

Fig 4 (a) Nature of WOAs and (b) Flowchart of WOAs

In exploitation phases, WOAs mimic current best solution behaviours thus reducing diversities in the population. Learning from random individuals have flaws and lack effective information flows across groups during explorations in WOAs which impact their convergence rates. As a result, standard WOAs have concerns with sluggish convergence speed. ALWO is presented as a solution to the aforementioned problem by increasing the convergence speed.

Individuals learn from both elite and other members of the neighbourhood in animal swarms improving their quality. Adaptive social learning approach [18] included evaluating individual social ranks and influences, as well as building social networks to establish neighbourhoods. This study's approach builds whales' adaptable neighbourhoods for improving group interactions, and unique strategies based on neighbourhood updates are used to increase population varieties and calculation accuracies.

The position of the whale and the encircling can be represented by equation (2) and (3)

$$\vec{H} = |\vec{C} x \vec{X} * (t) - \vec{X}(t)| \quad (2)$$

$$\vec{X}(t+1) = \vec{X}(t) - \vec{A} \times \vec{H} \quad (3)$$

The term $\vec{A}$ and $\overrightarrow{C}$ gives vector coefficients, t represents the present iterations, term $\vec{X}$ gives the position vector and $\vec{X} *$ said to be the best solution (position) started at random. The vector $\vec{A}$ and $\overrightarrow{C}$ coefficients are calculated using equation (4) and (5)

$$\vec{A} = 2\vec{a} \times \vec{r} - \vec{a} \quad (4)$$

$$\vec{C} = 2x\vec{r} \quad (5)$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v10i6.5557
Article Received: 10 April 2022 Revised: 18 May 2022 Accepted: 02 June 2022 Publication: 30 June 2022

The components of $\vec{a}$ are decreased from 2 to 0 during each iteration linearly and represents the random value between 0 and 1

The bubble-net technique is used by humpback whales to loop around and pursue prey [19]. Whales encircle their preys, such as fish, and then strive to update their locations in order to find the best option. Eqs. (6) and (7) show the basic mathematical components of the WOAs (7).

$$X(t+1) = X^*(t) - A.|C.X^*(t) - X(t)| \; if \; p < 0.5 \quad (6)$$

$$X(t+1)|C.X^*(t) - X(t)|.e^{bl} \cos(2\pi t) + X^*(t) \; if \; p \geq 0.5 \quad (7)$$

Where, X represents whales' location vector, t stands for iteration count, and X* represents identified best solutions. A=2a. (r-a);C=2.r stands for coefficient vectors that linearly reduce to zero from two in iterations; r represents randomized vector values in the range (0,1); b represents constant values of logarithmic spirals based on routes and is set to 1; In Eqs. (6) and (7), l has random values in the range(-1,1) while p gets random values in the range (0,1) utilised for switching between (4) and (5) while updating whale locations. The odds are 50% and 50%, respectively, implying that whales choose either option at random with an equal likelihood during the optimization process. The random value for A during the bubble-net phase is in the interval [- 1, 1], while in searched A's value might be larger or lesser than 1. Equation (8) depicts the search procedure

$$X(t+1) = X_{rand} - A.|C.X_{rand} - X(t)| \quad (8)$$

Random searches with a |A| values > 1 compel WOAs on global searches. WOAs start their searches with generated random solutions which are updated iteratively using technique shown in Table 1. The searches go on until they reach predetermined maximum iterations.

Exploitation phase: This phase consists of two phases. I encircling and ii) spirally updating the location Encircling behaviour may be expressed by linearly reducing a from 2 to 0 for each repetition. Spiral position should be updated: The location of the whale in relation to the fish, as well as the whales' helical movement, is given by

$$\vec{X}(t+1) = \vec{D}xe^{b1}xcos(2\pi l) + \vec{X} * (t) \quad (9)$$

Where $\overrightarrow{D'} = |\vec{X} * (t)\_\vec{X}(t)|$ is the current position between the fish and the whale, b unchanging factor or constant that represents the spiral migration of the whales and b also a random vector of $[-1, 1]$. Also, there exists a probability of choice: either diving deep through circling and forming spiral is given mathematically by equation 6 or the random vector of value is p [0,1]

Exploration phase: Exploration for fishes is a global search and whales search for the fishes moving to the surface. The choice of switching between exploitation and exploration is based on $\vec{A}$, a vector with values of [0,1] where 0 implies exploration and 1 exploitation. And the whale's new position is given by the equation 7 and 8

$$\vec{H} = |\vec{C}x\vec{X}_{rand} - \vec{X}| \quad (10)$$

$$\vec{X}(t+1) = \vec{X}_{rand} - \vec{A}x\vec{H} \quad (11)$$

Where $\vec{X}_{rand}$ gives the new position of the whale which is chosen at random from the other whales

Adaptive social learning strategy

Constructing neighbourhood membership relationships of whales by mimicking social learning principles, imitations of current best solutions can be changed, information sharing between groups and algorithm's ability to avoid local optimal solution can be improved in terms of the present population

$$G(t) = \{x_1(t), x_2(t), \ldots., x_N(t)\} \quad (12)$$

where Nis the population size. The fitness of each individual is calculated and arranged from small to large to obtain the sorted population

$$G_1(t) = \{x_{(1)}(t), x_{(2)}(t), \ldots., x_{(N)}(t)\} \quad (13)$$

and the social ranking of $x_{(i)}(t)$ is

$$I_{(i)}(t) = \frac{R_{(i)}(t)}{N} \qquad i = 1,2, \ldots, N \quad (14)$$

Where $R_{(i)}$ is random number and $I_{(i)}(t)$ that an individual has an increased connection with another individual

As a result, the algorithm's exploitation stage is mostly focused on optimal solution search, and the exploration ability is completed by group cooperation; a new whale search method is built based on adaptive social neighbourhood strategy.

Algorithm 2: ALWOs

1. Begin
2. establish the whale population's positions (DDoS) X
3. calculate fitness of whales (higher accuracy)
4. initialize $a \; and \; r$, calculate A and C

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v10i6.5557
Article Received: 10 April 2022 Revised: 18 May 2022 Accepted: 02 June 2022 Publication: 30 June 2022

5. initialize $X*$ as the best hunter whale's location
6. initialize $t = 1$
7. while $t \leq max$ iterations do
8. for each hunting whale do
9. if $p < 0.5$
10. if $|A| < 1$
11. update the current hunting whale's location using (6)
12. else if $|A| \geq 1$
13. Choose different search agent randomly (feature)
14. Modify current hunting whale's location using (7)
15. end if
16. else if $p \geq 0.5$
17. Modify current hunting whale's location using (8)
18. end if
19. compute local optimal solution using (12) & (13)
20. update exploitation stage using (14)
21. end for
22. update X* if there is a better solution
23. $t = t + 1$
24. end while
25. output $X*$ obtain best solution as higher accuracy
26. End

ALWOs feature selections ensure the effectiveness of selected characteristic subsets in normal and abnormal traffic's discriminations. ALWOs guarantee that all preset characteristics are picked from flows irrespective of they being initial packets or later packets. The algorithm selects best subset fits of features.

3.4 DDoS classification using CNN algorithm in SDNs environment

Fundamental CNNs include inputs, outputs and many hidden layers where hidden layers include convolution, pooling and totally linked layers. Convolution layers convolve inputs and pass it on subsequent layers. Convolutions simulate single neuron's reactions to sensory inputs. Convolution networks merge outputs of neuron clusters of one layer into single neurons of subsequent layers using local or global pooling. The average values of neuron clusters in preceding layers are used in mean pooling. Neuron of one layer communicate with neurons of subsequent layers through fully linked layers. CNNs, in principle, are similar to MLPs (multi-layer Perceptrons) based NNs (neural networks) [20]. This work's CNNs have input, convolution, and classification layers and improved ALWOs produce apparent benefits for analyzing high-dimensional data. They use parameter sharing strategy to control and reduce parameter counts in convolution layers. Figure 5 displays the basic DLCNN architecture..

In order to appropriately provide data to the next layer, the input layer gets DDoS characteristics from training samples and converts the data into a uniform form. This layer also specifies the basic settings, such as the size of the local receptive fields and the various filters.

Convolution layer (Cx) analyses the incoming data using a convolution algorithm and generates numerous layers termed feature maps, which are made up of the convolution calculation results from preceding layers. It is primarily used to extract critical characteristics and lower the network's computational complexity..

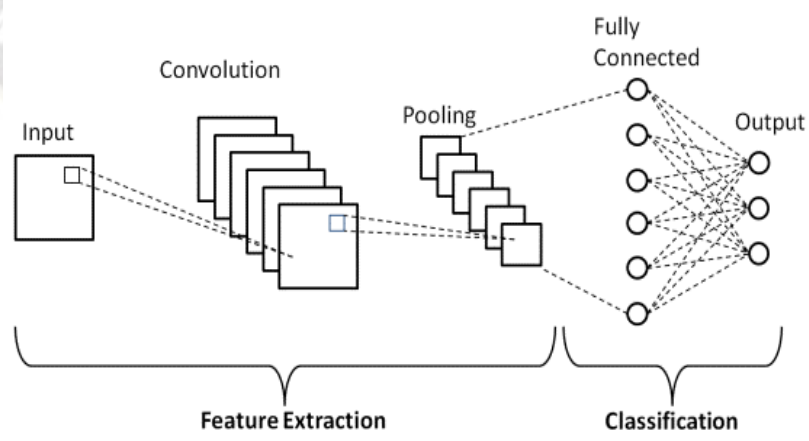

Fig 5 Basic DLCNN architecture

Activation functions are used in convolution layers and they map outputs to succession of inputs, resulting in non-linear network structures. All specified feature values are included in initial connection weights resulting in computing new input patterns.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v10i6.5557
Article Received: 10 April 2022 Revised: 18 May 2022 Accepted: 02 June 2022 Publication: 30 June 2022

$$y(n) = f(\sum_{i=1}^{i=N} w_i(n)x_i(n) \quad (15)$$

$$\text{Where } f(x) = \begin{cases} +1 & if\ x \geq 0 \\ -1 & if\ x < 0 \end{cases} \quad (16)$$

Where n is the iteration index

Connection weights are updated according to

$$w_i(n+1) = w_i(n) + \eta(d(n) - y(n)x_i(n), \quad i = 1,2,..N \quad (17)$$

Where η is the gain factor

Then apply standard deviation

$$\sigma = \sqrt{\frac{1}{n} f_i(x_i - \overline{x)^2}} \quad (18)$$

These weighted DDoS characteristics are fed into the proposed CNN network, yielding more accurate classification results. The major conclusions of the study done on the same set of data are confirmed by the polynomial distribution function.

Classification Layer: As the input passes through numerous convolution layers, the size of the output feature maps gradually shrinks. Every feature map for the classification layer consists of only one neuron and is converted into a feature vector. A classifier is entirely related to the vector. The accuracy and effectiveness of DDoS attack detection and classification are greatly enhanced by more accurately locating DDoS attacks.

Algorithm 3: Steps in CNN

1. Procedure DDoS attack dataset
2. For all input feature, describe DDoS feature ∈ given dataset do
3. For neurons, input features do
4. Train CNN for the given dataset using (18)
5. Convert the input into convolution and classification layers
6. Detect DDoS features using (15)
7. Select more informative and relevant features
8. Perform training and testing process for given dataset using (16) and (17)
9. Copy predefined DDoS feature label for each feature as per the input dataset
10. Detect more accurate DDoS attack results

SDNs are a flow-based network that can handle massive amounts of network traffic while being administered from a centralized location. This section includes five categories, four of which represent attack traffic and one of which represents typical traffic. DoS, Probe, R2L, and U2R are the attack types. Each has a variety of attacks. During the training process, attacks are introduced to validate the ALWO+CNN model. The ALWO+CNN system might identify DDoS attacks efficiently or not.

4. Experimental Result

In this section, the trained model is deployed as A web service on the SDNs controller is tested for success in DDoS attack prediction. The SDNs controller receives packets destined for the target host with a high traffic burst of around 484 Mbps, which the classification algorithm labels as DDoS traffic. The SDNs controller identifies the traffic as malicious, and new packets arriving with a pattern resembling a DDoS attempt are routed to a honeypot. Because there is a huge volume of traffic directed at the target host, it takes approximately 60 seconds for the SDNs controller to redirect all malicious traffic to the honeypot, where it can be further analyzed to discover the source of the attack and other essential header information. After around 60 seconds, the honeypot begins to receive traffic at a rate of 415.6 Mbps. The majority of traffic identified as DDoS assault based on the detection algorithm utilized is sent to a honeypot, with just a minor portion of traffic, roughly 13 Mbps, reaching the target server within the margin of error. NSL-KDD dataset [21], the most frequently used has been utilized in this study to test the performance of current and new DDoS attack detection systems. The NSL-KDD dataset improves on the KDD 99 dataset. It also comprises 41 network flow statistics such as duration, protocol type, src bytes, dst bytes etc.. Existing methods like MLPs, KNNs, and CNN-BiLSTMs are examined in this paper, along with the suggested ALWO+CNN approach in terms of their accuracies, precisions, recalls, f-measures, and computational complexities as performance indicators.

4.1 Accuracy

Accuracy determines overall correctness of models and computed as total actual classification parameters ($T_p + T_n$) segregated by sum of classification parameters ($T_p + T_n + F_p + F_n$). It can be computed as :

$$\text{Accuracy} = \frac{T_p + T_n}{(T_p + T_n + F_p + F_n)} \quad (19)$$

Where Tp is true positive, Tn is true negative, Fp is false positive and Fn is false negative

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v10i6.5557
Article Received: 10 April 2022 Revised: 18 May 2022 Accepted: 02 June 2022 Publication: 30 June 2022

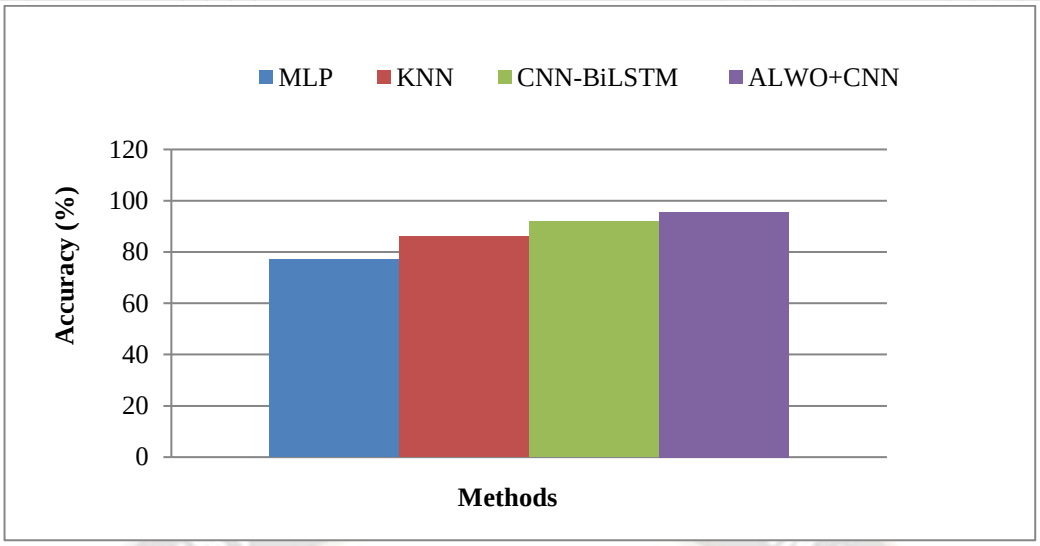

Fig 6 Accuracy

Accuracies of existing and suggested methods are depicted in Figure 6 where techniques are represented in the x-axis while y-axis depicts accuracies. Existing approaches, such as MLP, KNN, and CNN-BiLSTM algorithms, provide lesser accuracy for the provided NSL-KDD dataset, however the suggested ALWO+CNN methodology gives superior accuracy. As a consequence, the proposed ALWO+CNN method improves DDoS detection accuracy by the optimal selection of features.

4.2 Precision

The precision is calculated as follows:

$$\text{Precision} = \frac{\text{True positive}}{\text{True positive+False positive}} \quad (20)$$

Precisions are measures of accuracies or qualities, whereas recalls are measures of completeness or quantities. Generally, high precisions imply algorithms deliver more relevant results and lesser irrelevant outcomes. The accuracies of classified classes is the number of genuine positives divided by the total number of objects classified as belonging to the positive class.

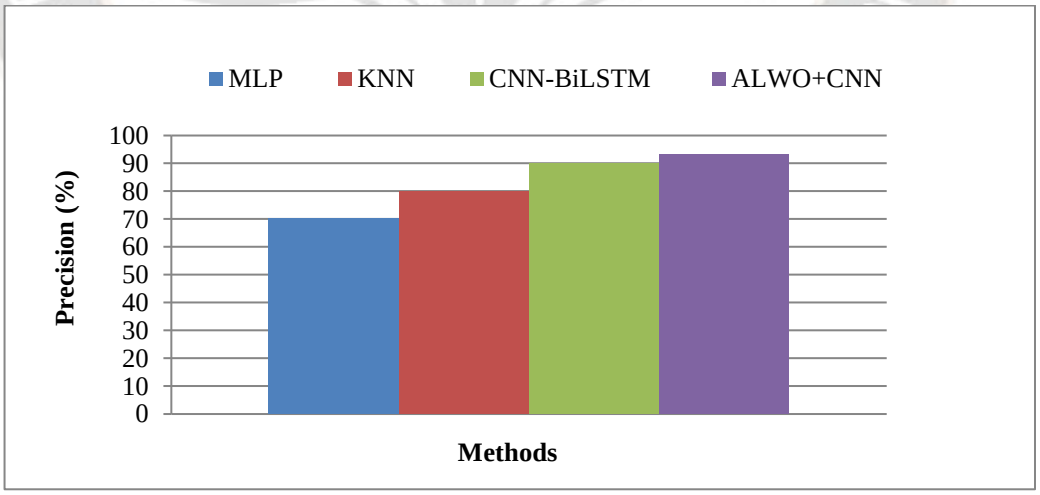

Fig 7 Precision

Precisions of existing and suggested methods are depicted in Figure 7 where techniques are represented in the x-axis while y-axis depicts their precisions. Existing approaches, such as MLP, KNN, and CNN-BiLSTM algorithms, provide lesser precision for the provided NSL-KDD dataset, however the suggested ALWO+CNN methodology gives higher accuracy. As a consequence, the proposed ALWO+CNN algorithm improves the protection against DDoS assaults in SDNs by the optimum feature selection.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v10i6.5557
Article Received: 10 April 2022 Revised: 18 May 2022 Accepted: 02 June 2022 Publication: 30 June 2022

4.3 Recall

The calculation of the recall value is done as follows:

$$\text{Recall} = \frac{\text{True positive}}{\text{True positive+False negative}} \quad (21)$$

The comparison graph is depicted as follows:

The number of relevant documents recovered by a search divided by the total number of existing relevant documents is described as recall, while precision is defined as the number of relevant documents obtained by a search divided by the entire number of documents retrieved by that search.

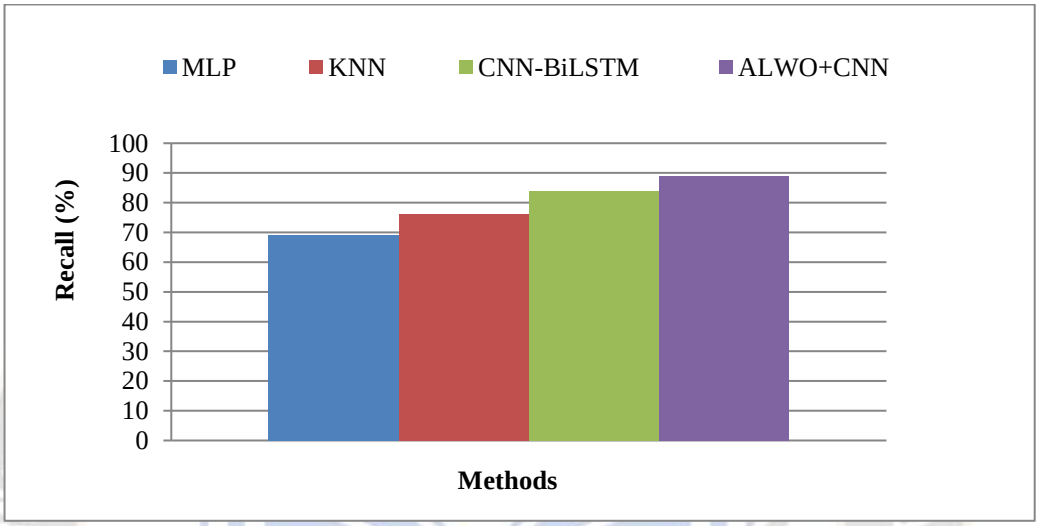

Fig 8 Recall

Recall values of existing and suggested methods are depicted in Figure 8 where techniques are represented in the x-axis while y-axis depicts recall values. Existing approaches, such as MLP, KNN, and CNN-BiLSTM algorithms, provide lesser recall for the provided NSL-KDD dataset, however the suggested ALWO+CNN algorithm gives greater recall. As a consequence, the proposed ALWO+CNN method improves DDoS detection accuracy by the optimal selection of features.

4.4 F-measure

F-measure is the combination of precision P and recall R,

$$F = 2.\frac{PR}{P+R} \quad (22)$$

For assessing the classification algorithms, depends upon the F-measure since it is a standard measure of summarizing precision P as well as recall R

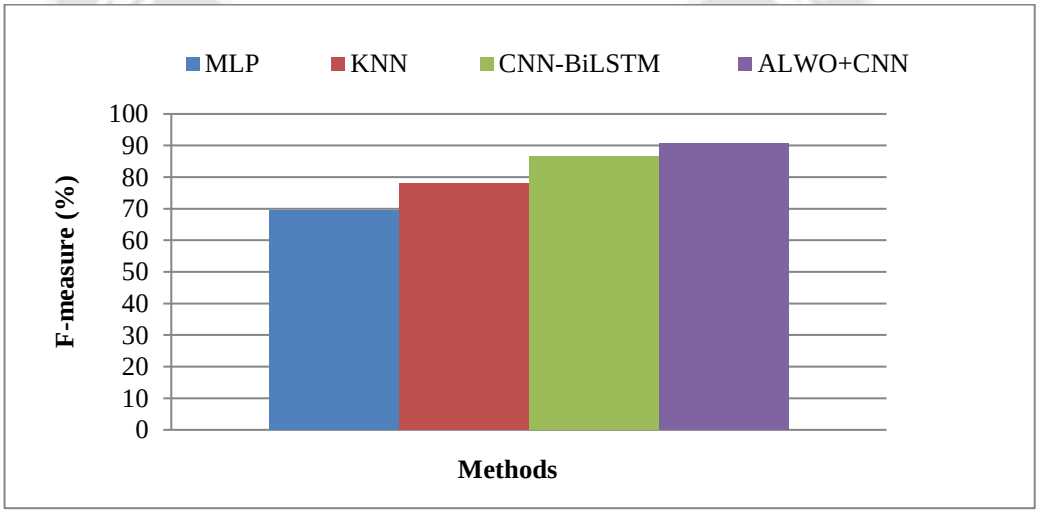

Fig 9 F-measure

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v10i6.5557
***Article Received**: 10 April 2022 **Revised**: 18 May 2022 **Accepted**: 02 June 2022 **Publication**: 30 June 2022*

F-measures of existing and suggested methods are depicted in Figure 9 where techniques are represented in the x-axis while y-axis depicts F-measures. Existing approaches, such as MLP, KNN, and CNN-BiLSTM algorithms, provide lower F-measures for the provided NSL-KDD dataset, however the suggested ALWO+CNN algorithm delivers greater F-measures. As a consequence, the proposed ALWO+CNN algorithm improves the protection of DDoS assaults in SDNs environments.

4.5 Computational complexity

The system is better when the proposed method provides lower computational complexity

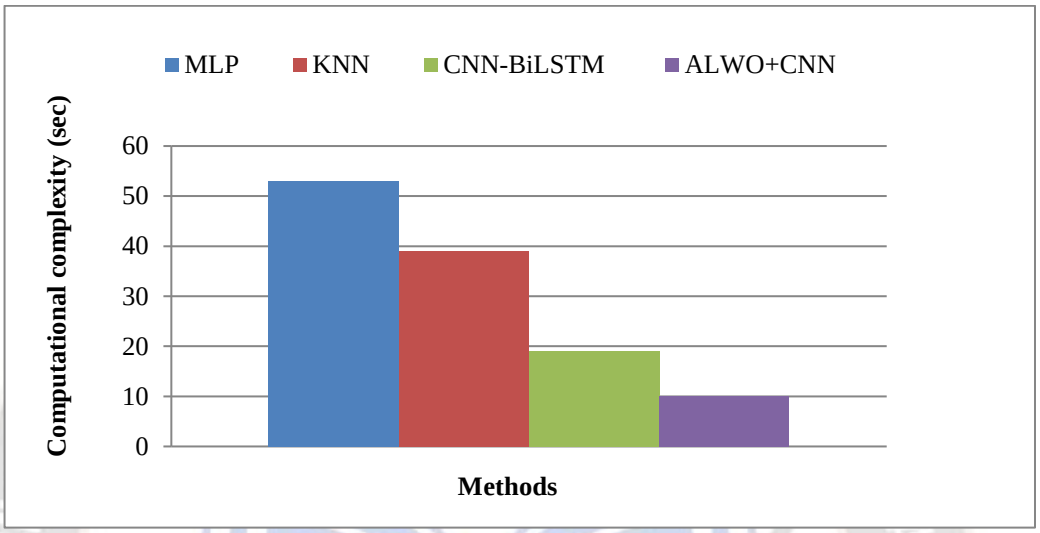

Fig 10 Computational complexity

Computational complexities of existing and suggested methods are depicted in Figure 10 where techniques are represented in the x-axis while y-axis depicts their Computational complexities. Existing approaches, such as centralised MLP, KNN, and CNN-BiLSTM algorithms, have a greater computing complexity for the provided NSL-KDD dataset, however the suggested ALWO+CNN algorithm has a reduced computational complexity. As a consequence, the suggested ALWO+CNN algorithm boosts security against DDoS assaults while simultaneously providing higher detection performance due to the optimum feature selection.

Table 1 shows the comparison values for DDoS attack detection dataset using existing and proposed methods

Table 1 Comparison values for given dataset

Methods/Metrics	**MLP**	**ANN**	CNN-BiLSTM	**Proposed ALWO+CNN**
Accuracy (%)	77	86	92	95.6
Precision (%)	70	80	90	93
Recall (%)	69	76	84	89
F-measure (%)	69.5	78	86.5	90.5
Time complexity (sec)	53	39	19	10

5. Conclusion

Although SDNs have numerous advantages, it also confronts the possibility of DDoS assaults, the most prevalent network security concern. As a benefit of SDNs, centralised control renders the controller more exposed to security concerns such as DDoS assaults. In response to this issue, the detection and defence mechanism of DDoS assaults via SDNs is examined in this study, which combines SDNs' inherent advantages with deep learning algorithms and employs a more efficient algorithm to detect and fight against DDoS attacks in the SDNs controller. To identify DDoS assaults successfully, an Adaptive Learning

based Whale Optimization and Convolution Neural Network (ALWO+CNN) method is suggested in this study. After building the SDNs model, the dataset is pre-processed using the KMC technique to remove missing and incorrect values. The ALWO algorithm is used to choose the optimum fitness characteristics for feature selection. The CNN is then offered as an effective DDoS detection method on the supplied dataset. The results show that the suggested ALWO+CNN method outperforms the current techniques in terms of accuracies, precisions, recalls, f-measures, and Computational complexities. In the future, we will look at the examination of an unsupervised machine learning model that will thoroughly analyse all unknown traffic. Also, use streaming computing technology to lessen the strain on a single controller while ensuring the efficiency of DDoS detection and network quality in large-scale networks.

References

1. Alshamrani, Adel, et al. "A defense system for defeating DDoS attacks in SDNs based networks." *Proceedings of the 15th ACM international symposium on mobility management and wireless access*. 2017.
2. Makuvaza, Auther, Dharm Singh Jat, and Attlee M. Gamundani. "Deep neural network (DNN) solution for real-time detection of distributed denial of service (DDoS) attacks in software defined networks (SDNs)." *SN Computer Science* 2.2 (2021): 1-10.
3. Pawan Kumar Tiwari, P. S. . (2022). Numerical Simulation of Optimized Placement of Distibuted Generators in Standard Radial Distribution System Using Improved Computations. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(5), 10–17. https://doi.org/10.17762/ijrmee.v9i5.369
4. Saharan, Shail, and Vishal Gupta. "Prevention and Mitigation of DNS based DDoS attacks in SDNs Environment." *2019 11th International Conference on Communication Systems & Networks (COMSNETS)*. IEEE, 2019.
5. Santos, Reneilson, et al. "Machine learning algorithms to detect DDoS attacks in SDNs." *Concurrency and Computation: Practice and Experience* 32.16 (2020): e5402.
6. Ambusaidi, Mohammed A., et al. "A novel feature selection approach for intrusion detection data classification." *2014 IEEE 13th international conference on trust, security and privacy in computing and communications*. IEEE, 2014.
7. Ghazaly, N. M. . (2022). Data Catalogue Approaches, Implementation and Adoption: A Study of Purpose of Data Catalogue. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(1), 01–04. https://doi.org/10.17762/ijfrcsce.v8i1.2063
8. Abubakar, Atiku, and Bernardi Pranggono. "Machine learning based intrusion detection system for software defined networks." *2017 seventh international conference on emerging security technologies (EST)*. IEEE, 2017
9. Kalkan, Kubra, Gurkan Gur, and Fatih Alagoz. "Defense mechanisms against DDoS attacks in SDNs environment." *IEEE Communications Magazine* 55.9 (2017): 175-179.
10. Varghese, Josy Elsa, and Balachandra Muniyal. "An efficient ids framework for ddos attacks in sdn environment." *IEEE Access* 9 (2021): 69680-69699.
11. Alghazzawi, Daniyal, et al. "Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection." *Applied Sciences* 11.24 (2021): 11634.
12. Eslamnezhad, Mohsen, and Ali Yazdian Varjani. "Intrusion detection based on MinMax K-means clustering." *7'th International Symposium on Telecommunications (IST'2014)*. IEEE, 2014
13. Ravi Kiran Varma, P., K. V. Subba Raju, and Suresh Ruthala. "Application of whale optimization algorithm in DDOS attack detection and feature reduction." *Inventive Computation and Information Technologies*. Springer, Singapore, 2021. 93-102.
14. Tan, Liang, et al. "A new framework for DDoS attack detection and defense in SDNs environment." *IEEE Access* 8 (2020): 161908-161919.
15. Wang, Lu, and Ying Liu. "A DDoS attack detection method based on information entropy and deep learning in SDNs." *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*. Vol. 1. IEEE, 2020.
16. Rehman, A. U., Rui L. Aguiar, and João Paulo Barraca. "Fault-tolerance in the scope of software-defined networking (sdn)." *IEEE Access* 7 (2019): 124474-124490.
17. Polat, Huseyin, Onur Polat, and Aydin Cetin. "Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models." *Sustainability* 12.3 (2020): 1035.
18. Mohamad, Ismail Bin, and Dauda Usman. "Standardization and its effects on K-means clustering algorithm." *Research Journal of Applied Sciences, Engineering and Technology*6.17 (2013): 3299-3303
19. Jin, Qibing, Zhonghua Xu, and Wu Cai. "An Improved Whale Optimization Algorithm with Random Evolution and Special Reinforcement Dual-Operation Strategy Collaboration." *Symmetry* 13.2 (2021): 238
20. Fan, Q.; Chen, Z.; Zhang, W.; Fang, X. ESSAWOA: Enhanced Whale Optimization Algorithm integrated with Salp Swarm Algorithm for global optimization. Eng. Comput. 2020, 1–18
21. Sayed, G.I.; Darwish, A.; Hassanien, A.E. A New Chaotic Whale Optimization Algorithm for Features Selection. J. Classif. 2018, 35, 300–344
22. Parwez, Md Aslam, and Muhammad Abulaish. "Multi-label classification of microblogging texts using convolution neural network." *IEEE Access* 7 (2019): 68678-68691

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v10i6.5557
Article Received: 10 April 2022 Revised: 18 May 2022 Accepted: 02 June 2022 Publication: 30 June 2022

23. Nsl-kdd data set for network-based intrusion detection systems. available on: http://nsl.cs.unb.ca/nsl-kdd/, march 2009
24. M. S. Kiran and P. Yunusova, "Tree-Seed Programming for Modelling of Turkey Electricity Energy Demand", Int J Intell Syst Appl Eng, vol. 10, no. 1, pp. 142–152, Mar. 2022.

S. Renuka Devi received her doctorate degree in Information and Communication Engineering from Anna University, Chennai, India in the year 2015. She is currently working as an Associate Professor in the School of Computing Science and Engineering, VIT University, Chennai, India. Her area of interest includes Network Security and Cryptography.

L. Shyamala working as Associate professor in VIT, Chennai campus from 2016 onwards. She did her B.E in ECE at Madras university, PG and Ph.D in CEG, Anna University. Her area of interest for research includes Cloud computing, Data analytics. and networks.

Dr. S. Saraswathi completed her Ph.D in the Faculty of Information and Communication Engineering, Anna University Chennai, India in the year 2015. Presently she is working as an Associate Professor in Sri Sivasubramaniya Nadar College of Engineering. Her fields of interests include Network Security, Cryptography, information security, Cyber Forensics, IOT.