

SECURING GOVERNMENT NETWORKS: ADVANCED TRAFFIC ROUTING AND ANOMALY DETECTION VIA SEAGULL OPTIMIZATION AND DEEP LEARNING WITH SDN

Aswini C*, Malavika R*, Suguna T*, Gladson Oliver S*

*Assistant Professor, Information Technology,
Government College of Technology, Coimbatore.

ABSTRACT

The transformation of local self-governance into digital form requires continuous availability of services through the internet, including permit applications, taxation, and access to public documents. Nonetheless, the increase in traffic along with growing threats of DDoS attacks jeopardizes the work of the administrative system where server response time is an important parameter which is often ignored by current load balancers. The research provides the idea of using hybrid Artificial Intelligence for securing the local government networks and optimizing their functioning. More precisely, a combination of Artificial Fish Swarm algorithm along with a CNN-RNN model was used for effective detection of DDoS attacks in software-defined networking. At the same time, a metaheuristic method of seagull optimization is used to calculate fitness function for finding the optimal routes for load balancing in case of high traffic. The empirical evaluation revealed the considerable improvements in terms of Root Mean Square Error: the proposed model achieved a better result compared to CNN (16.13%) and RNN (22.91%). In addition, the new approach increased the network throughput by 31.98% and 33.96% compared to OpenFlow and Linux ProGFE, correspondingly.

Keywords: Software Defined Networking (SDN), Information-Centric Networking (ICN), Artificial Fish Swarm Algorithm (AFSA), Convolutional Neural Network-Recurrent Neural Network (CNN-RNN), Seagull Optimization, Multicast Routing.

1. Introduction

SDN [1] is the emerging technology, finds a major part of network system by providing efficient solutions for the user expectations. It [2] provides high level of feasibility to the network by providing improved level of programming facility to ease the innovations in network. The major differentiation among the SDN when compared with the IP based networks [3] is it is composed of three planar structures namely control plane, data plane and application plane. The control plane is commonly referred to as the controller which resembles the action of human brain in the network. The data plane constitutes the topology of the network to forward the data packets as directed by the control plane of the network. The application plane is the complementary plane when compared to the other planes of the SDN. The controller [4] decides the topology of the network and the route to transfer the data from source point to destination.

The use of SDN is motivated because of its robustness, easy scalability and security features. IP based network requires high level of network-oriented policies followed by the excessive work load for the administrators of the network in configuring each and every network. The network device in IP based network mitigates the flexibility of the network and innovations in the network. Whereas, in SDN, the control plane and the application plane are isolated from the data plane to incorporate the facilities of flexibility and implementation speed of the network. Even though the SDN possess flexible facilities performed by the control planes, certain drawbacks still persist. SDN experiences certain critical challenges like security aspect, poor level of scalability and adaptability. Security concern is a leading challenge among the aforementioned critical aspects in which the controller of the SDN literally fails to maintain the network. The failure of the functions of the control plane affects the efficiency and the authentication of the entire network. One of the major threatening aspects to the security of SDN is the Distributed Denial of Service (DDoS) attacks [5]. The DDoS attacks can be launched in multiple planes namely, Data plane DDoS attack [6], control plane DDoS attack [7], and application plane DDoS attack [8]. The internet provides multi-facilities to the users which involve, high range of availability, easy scalability, and reduced loss of data. Besides the advantages of internet, it experiences a major setback of security concern proving highly vulnerable to the different types of attacks. The vulnerabilities to the internet may be of different types ranging from virus, worms, and Trojan horses launching different types of attacks classified under the active and passive methodologies.

The Denial of Service (DoS) attacks are the most common attacks launched against most of the internet based service to prevent the availability of service to the genuine users. The DoS attack is deliberately performed to prevent the benign users from accessing the resources of the internet based services. This research work aims in

introducing a novel framework for providing security against the DDoS attack in SDN along with the efficient multicast routing mechanism with an objective to provide a load balancing in the network path. The proposed research work concentrates of the detection of DDoS attack and to provide a proper load balancing using hybrid model composed of Artificial Fish Swarm Algorithm (AFSA) [9] with Convolutional Neural Network-Recurrent Neural Network (CNN-RNN) model [10].

This research work is organized in such a way that the literature survey is performed in Section 2 with a detailed illustration in Section 3. The performance evaluation of the proposed method is performed in Section 4 with a conclusion in Section 5.

2. Literature Review

SDN is the emerging technology in the communication sector, not only attracts the users and IT professionals but also attracts numerous researchers to involve in active findings to improve the efficiency of the SDN. The researchers concentrated on two major aspects of development in the SDN namely routing mechanism and the security authentication processes.

P. T. Dinh et al. (2021) had designed a framework [11] for detecting the DDoS attack in the large scale SDN. The proposed framework overcomes the pitfalls of the traditional methods of data processing and detects the intensive DDoS attacks in the network. H. Nurwarsito et al. (2021) had designed an early detection and mitigation system for the SDN using Random forest algorithm and Ryu framework [12]. The proposed random forest algorithm will classify the incoming packets to detect the anomaly behavior packets, resulting in detection of the DDoS attack in the network. The accuracy of the proposed method is measured to be 98.38% and is measured with an average of 15672 incoming packets. The CPU usage of the proposed system is measured to be 44.9%.

Y. Cao et al. (2021) had designed DDoS detection and mitigation system [13] in SDN using Spatial Temporal graph convolution network. The spatial temporal graph convolution network senses the condition of the switches through the In-Band Network Telemetry using sampling process. The evolution results prove that the proposed method effectively identifies the DDoS attack in SDN. M. Klymash et al. (2021) had employed Machine Learning algorithm [14] in detecting the DDoS attack in the SDN. The author implemented Kulbak- Leibler (KL) approach for the detection of anomalies in the incoming data pattern of the SDN. The KL approach detects the anomalies by comparing the average session duration of the packet with the ML database.

H. S. Abdulkarem et. al (2020) had proposed a DDoS attack detection and mitigation mechanism in the data plane layer [15] of the SDN. The detection of DDoS attack is performed by detecting the anomalous behavior of the packets in the data traffic. The analysis of the proposed method exhibits a minimum of 100 to 150sec for the detection of DDoS attack in the SDN. R. Sanjeetha et al. (2020) had mitigates the existence of the DDoS attack in the SDN and its primary server by employing priority [16] on the inflowing traffic variation. The existence of the DDoS attack in the primary server is detected by compromising certain host to transmit the data packets with spoofed IP addresses. J. A. Pérez-Díaz et al. (2020) had designed a flexible architecture for detecting and mitigating the Low rate DDoS in the SDN using Machine Learning algorithm [17]. The author employed six Machine Learning models namely J48, Random forest algorithm, Random tree, REP tree ad Multi Layer Perceptron (MLP) algorithm for the detection of DDoS attack in the SDN.

Table 1 Comparison of DDoS mitigation techniques with state of art methodologies

Ref.No.	Architecture of SDN	DDoS	Load Balancing	Data plane DDoS	Control Plane DDoS	Application Plane DDoS
[11]	✓	x	x	x	✓	x
[12]	✓	x	x	✓	✓	✓
[13]	✓	x	x	x	x	✓
[14]	✓	x	x	x	✓	x
[15]	✓	x	x	✓	x	✓
[16]	✓	x	x	x	x	✓
[17]	✓	✓	x	x	✓	x
[18]	✓	x	x	x	x	✓
[19]	✓	✓	x	x	✓	x
[20]	✓	x	x	x	x	✓
Proposed	✓	✓	✓	✓	✓	✓

A. T. Kyaw et al. (2020) had proposed a Machine Learning based DDoS attack classifier [18] in SDN. The proposed method detects the anomaly behavior of the incoming data packets to identify the DDoS attack. The

author employed polynomial Support Vector Machine as a packet generating tool to achieve 3% more accuracy than the existing methods. B. Nugraha et al. (2020) had employed Deep Learning based algorithm [19] to detect the DDoS attack in the SDN. The author employed the hybrid method of Convolution Neural Network- Long short Term Memory (CNN-LSTM) for detecting the DDoS attack in the SDN. W. Sun et al. (2019) had introduced an improved method [20] of detecting the DDoS attack in the controller of the SDN) The author employed BiLSTM-Recurring Neural Network (RNN) algorithm to detect the anomalies in the incoming data patter.

The performance analysis proves that the proposed model is quite impressive than the existing state of art methodologies. Based on the aforementioned studies performed in the detection of the Denial of Service (DDoS) attack in the Software Defined Network, the following key observations were made which were illustrated in the Table 1.

The Table 1, represents the identified pitfalls of the state of art methodology in detecting and mitigating the DDoS attack occurring in the Software Defined Network (SDN). The objectives of the proposed research work are listed as follows.

- a) To design a hybrid framework for enhancing the security against the Distributed Denial of Service at a slower rate in the SDN using Artificial Fish Swarm Algorithm (AFSA) [21] with Convolutional Neural Network- Recurrent Neural Network (CNN-RNN) [22] model.
- b) To provide an efficient load balancing [23] in the SDN by performing effective routing using Seagull Optimization Algorithm.

Current research works have concentrated on improving the aspects of security and routing efficiency in SDN using machine learning algorithms and optimization. Elsheway et al. (2025) presented an innovative model involving a Hybrid CNN-GRU algorithm for DDoS attacks classification in SDN networks [26]. The CNN-GRU model was able to identify the spatial and temporal traffic features of the network, thus leading to increased efficiency in detecting such attacks. On the same note, Kalafy et al. (2026) have also presented a DGNN model, which made use of graph structure representation of the behavior of network traffic in improving DDoS attacks detection performance [27].

Apart from the security of the network, other researchers have conducted investigations on the use of optimization algorithms in route creation and load-balancing in SDNs. For instance, Chen et al. (2024) proposed a dynamic optimization framework for route creation and resource allocation through the use of a metaheuristic approach [28]. Additionally, Tache et al. (2024) carried out an exhaustive review on the use of optimization algorithms for SDN routing, load balancing, and delay reduction [29]. It is shown that the use of optimization algorithms inspired by nature is effective in enhancing the performance of the network. Besides, Jayaprakash and Devi Priya (2024) have also used the lion optimization algorithm to optimize routing in SDN-enabled IoT networks [30]. While all these studies have focused individually on DDoS detection and routing optimization separately, very few efforts have been put in finding ways of merging intelligent attack detection with load-balanced routing. It is due to the lack of such integration that motivated the development of the framework to be discussed.

3. Proposed Work

The proposed work is a two folded methodology in which the first module deals with the security enhancement by effectively detecting and mitigating the Distributed Denial of Service which invades the SDN at a slower rate. The first module is composed of hybrid algorithm using Artificial Fish Swarm Algorithm and Convolutional Neural Network amalgamated with the Recurrent Neural Networks (CNN-RNN). The second fold of the proposed research work is with the objective of performing effective routing mechanism using Seagull Optimization Algorithm.

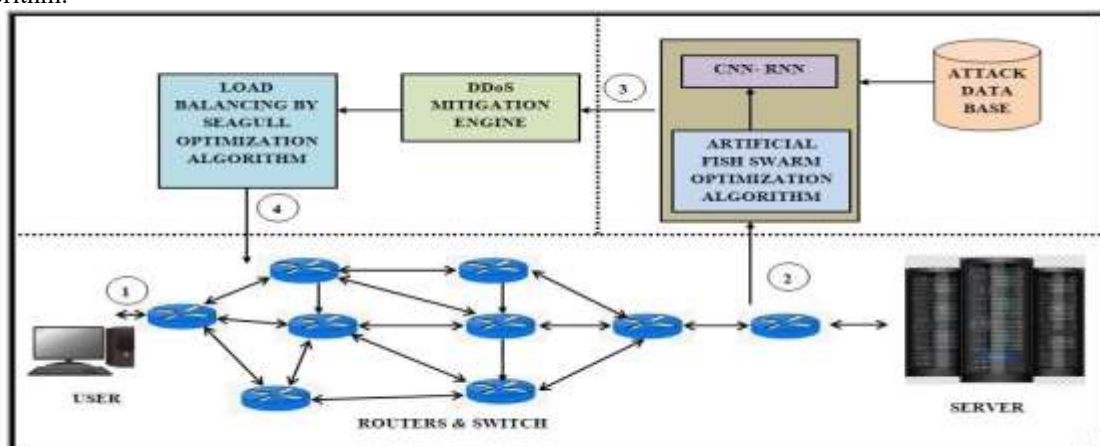


Figure 1 Proposed Architecture for detecting and Mitigation of DDoS with Load balancing in SDN enabled ICN

Figure 1 depicts the architecture of the proposed method for detecting and mitigating the DDoS attack in the SDN along with the efficient routing mechanism for achieving load balancing objectives.

3.1 Detecting and Mitigating DDoS attack using Hybrid Technology

DDoS attack is a critical concern in the SDN, and it pretends to be a legitimate packet entering into the network. These packets escape the detection methodologies by not exhibiting any anomaly behavior in the network traffic, creates critical attack of DDoS attack. The successful launch of such attacks will question the availability of service to the legitimate users resulting in deterioration of network's performance. To detect this DDoS attack, this research work proposed a hybrid technology composed of Artificial Fish Swarm Algorithm amalgamated with the Convolution Neural Network – Recurring Neural Networks.

The major reason of choosing and employing the Artificial Fish Swarm Algorithm is its special features of better level of robustness, good global search ability. The AFSA is proved to be least sensitive to the initial input values. The CNN-RNN amalgamation yields major advantages by neutralizing the pitfalls mutually and obtaining the advantages as a cumulative function. The integrated version of CNN-RNN accepts inputs of arbitrary length and involved minimized level of pre-processing aspects.

3.1.1 Artificial Fish Swarm Algorithm

The Artificial Fish Swarm Algorithm is a stochastic method with salient features of easily understandable, least sensitive to the initiating values and high level of fault tolerance. The AFSA is composed of five processes namely selection of behavior, searching behavior, swarming behavior, following behavior and bulletin. In AFSA, the individual element, "the fish" tends to move leading to modification of fish position in the entire population. The general characteristic of the fish is it accumulated in a point or move towards the point where the adequate amount of food is available. Similarly, the data in the network will be routed through the switch or router which has larger or free bandwidth such that it can be transmitted without any additional jitter or congestion concern. The malicious packet tends to utilize this condition to transmit the DDoS intended packets, and it can bypass the detection and mitigation engine activities in the network. The functional blocks involved in performing detection of malicious packet in the network.

The process flow the Artificial Fish Swarm Algorithm in the proposed method of detecting the DDoS attack in SDN. The network router size is designated as "M" and the total iteration count is fixed to be "I_T". Consider there are "N" number of positions for the artificial fish and is expressed as the $X_p = \{X_1, X_2, \dots, X_N\}$ and it is assumed that the "M" artificial fish can take any of the "N" number of position. The objective function of the AFSA algorithm is expressed in equation 1.

$$f_i(t) = Y(X_i(t))J \quad (1)$$

The line of separation between any two fish is expressed in equation 2.

$$d_{x,y} = \|X_x - X_y\| \quad (2)$$

where, the $d_{x,y}$ is the distance represented in x and y coordinate system and it is the line of separation between any two fish. The X_x and X_y represent the position vectors of the fish. .

3.1.1.1 Search Behavior:

Consider the new position of the artificial fish at the present instant time (t) as $X_x(t)$ and $X_y(t)$ and is chosen in a random manner to select an optimum position represented in equation 3.

$$X_y(t) = X_x(t) + \rho \quad (3)$$

Where, the ρ is the value chosen randomly within a range of 0 to 1. The migration of fish from one router to another is mathematically represented as in equation 4.

$$X_x(t+1) = X_x(t) + \frac{X_y(t) - X_x(t)}{\|X_y(t) - X_x(t)\|} * \epsilon * \alpha \quad (4)$$

Where, the ϵ is the step size of the fish taken for a single hop in the SDN and " α " is the random value selected between 0 to 1. The fish in the AFSA redirects its movements if the necessitated conditions are not satisfied and it tends to the new pattern of migration as represented in equation 5.

$$X_x(t+1) = X_x(t) * \epsilon * \alpha \quad (5)$$

The ϵ and α values are chosen between 0 to 1 such that they are not equal.

3.1.1.2 Swarm Behavior

The swarm behavior is the vital process to determine the path through which the DDoS intended packets travel towards the SDN. DDoS packet resembles a normal packet and intends to migrate through the path which the other packets are choosing. The swarm behavior of the fish is compared with the swarm movement of malicious packet to escape from the enemies (Mitigation tool). In this, consider the present position of the artificial fish is the $X_x(t)$ and the fish number as f_N . The visual centre position of the fish swarm is represented in equation 6.

$$X_c(t) = \sum_{i=1}^{f_N} \frac{X_{y_i}(t)}{f_N} \quad (6)$$

where, the $X_c(t)$ is the centre position of the swarm and f_N is the fish numbers. During this period, the artificial fish (malicious packet) moves to the centre of the cluster as per the equation 7.

$$X_x(t+1) = X_x(t) + \frac{X_c(t) - X_x(t)}{\|X_c(t) - X_x(t)\|} * \varepsilon * \alpha \quad (7)$$

Using the equation 7, the artificial fish (malicious packet) can be migrated to the centre of the cluster so that to trap it easily.

3.1.1.3 Follow Behavior

The follow behavior is the pattern of the artificial fish in moving towards the cluster of the high food concentration (high packet concentration in a router) at the present time $X_x(t)$. In this cluster, the identification of artificial fish with minimal objective is performed using the position vector as represented in equation 8.

$$X_x(t+1) = X_x(t) + \frac{X_{min}(t) - X_x(t)}{\|X_{min}(t) - X_x(t)\|} * \varepsilon * \alpha \quad (8)$$

The minimum objective function of the artificial fish is mathematically represented in equation 9.

$$X_{min} = \frac{Y_{min}(t)}{f_N} \quad (9)$$

The packet with the minimum objective function is considered as the malicious packet with the objective of launching DDoS attack in the SDN network is made to move to the cluster.

3.1.1.4 Behavior Selection

The behavior of the artificial fish is in random manner and the identification of that random behavior is done for the purpose to detecting its movement towards the high food concentration. The artificial fish possess multiple types of behavior in moving towards the high food concentration area. Among those multiple behaviors, the identification of tail is the successive method which relates to the identification of malicious packet with anomaly header mentioning unknown source address, routing address which were not registered IP addresses are identified. The major process employed to determine the artificial fish is to identify the tail end of the artificial fish (unfamiliar header file pattern) is considered to be easier, failing on which, is followed by the clustering process. In the clustering process, the artificial fish migrates towards the high food concentration area, where the detection of artificial fish with minimum objective function is easier. The algorithm for the Artificial Fish Swarm algorithm (AFSA) is illustrated in Table 2. The algorithm illustrates the step by process of detecting the malicious packet creating the DDoS attack in the SDN.

3.1.2 Convolution Neural Networks – Recurring Neural Network (CNN-RNN)

The Convolution Neural Networks (CNN) has been widely used in many recent applications with an objective to execute the tasks in an efficient manner. The CNN is a classification of neural network works on the principle of feed forward mechanism and is composed of three layers namely convolution layer, pooling layer and interconnected layer. The convolution layer possesses certain input features and it involves kernels to produce the chaotic mapped outputs.

The standard convolution process is involved in detecting and mitigating the DDoS attack in the SDN due to its identifying nature. The CNN tends to compare the entire incoming service request packet to detect the anomaly behavior of the incoming service request packets. This process is performed using standard convolution process namely depth wise convolution and point wise convolution. The 1x1 convolution kernels amalgamates the output features produced in the previous convolution process. The combined version of CNN-RNN model experiences the advantages of both CNN and RNN model and overcome the pitfalls of the aforementioned model mutually. The input to the proposed integrated network of CNN-RNN is composed of two major modules namely CNN and RNN to identify the local and the targeted features of the incoming packets to the SDN.

Table 2 Algorithm for Artificial Fish Swarm Algorithm (AFSA) in SDN

Algorithm: Artificial Fish Swarm Algorithm (AFSA) in SDN

Input:

Parameter Limit Ranges – “ α ”; “ ϵ ”; “ Θ ”
Defining Inertia Weight Setting – “ ω ”
Population: Network size (Fish count) – “N”
Acceleration factor; maximum particle speed.
Total Iteration count – “ I_T ”

Processes:

- Initialize the network population “N”, maximum particle speed.
- Outline the fitness function using equation 1.
- if MOD(t,x) = 0; then

-
- Restart the fish population “N”; $N = 1, 2, 3 \dots N-1$.
 - Perform the arbitrary selection and arbitrary drop of artificial fish.
 - end if
 - for $k=1$ to N do
 - If $k=\text{best}$, then
 - Perform mutation to generate new position $x(t+1)$
 - Else Perform artificial fish searching to generation cluster centric position
 - End if
 - End if
 - End for Perform arbitrary drop of fish in the population using equation 6 and 7.
 - Check whether iteration count is met
 - If $I_N > I_T$, update the artificial fish details
 - Else Repeat iteration process.
 - End
-

The RNN module identifies the dependencies among the incoming service request packets. The convolution model is composed of multiple layers and the kernel weight. The maximum pooling operation was employed to identify the maximum value of the incoming data packets and to generate the chaotic map functions for the incoming service request packets. CNN module’s hyper parameters which involves numerous kernels and the module is composed of 128 vectors with a capacity of [30,1]. The output is mapped with a 128 dimensional sequence. The output features are produced by the GRU layer which is fed forward as the input the successive GRU layers. The featured output produced by the CNN module will retain the information of the spectral process and after performing convolution process for several numbers of times, the extracted features by the CNN module are given as the input the GRU model. To mitigate the risk of DDoS to get success, the output of the RNN network is flattened by the RNN network in which one neuron will produce the anomalies in the incoming service requesting packets. The algorithm for the proposed CNN-RNN network model is illustrated in Table 3.

Table 3 Algorithm for proposed CNN-RNN network

Algorithm: CNN-RNN Network Model

Input:

Initialization of input parameters and data.

Hyper parameters: Kernel range, filter, batch size, pool size, Rate.

Process:

Initialize the process.

Normalizing(train a, train b)

First Convolution process: $\text{Conv1_model} = \text{Sequential}(\text{Kernel range, filter, batch size, pool size})$

$\text{Conv1_model}(\text{train a, train b, batch size})$

$\text{Conv1_output}(\text{feature model_predict}(\text{train a}))$

Determine the input gate by passing the output of stage 1 to successive stages.

$$I_g = \rho(W_i[x_{t-1}, x_t]) \quad (10)$$

Determine the intermediate node state by forwarding the input of the present GRU to next GRU.

$$C_t = \tanh(W_i[x_{t-1}, x_t]) \quad (11)$$

Determine the output stage from the final GRU.

$$O_t = \sigma(W_i[x_{t-1}, x_t]) \quad (12)$$

The CNN-RNN model and the output stage retrieved from the final GRU module denies the incoming DDoS packet from further forwarding to the server.

3.1.3 Seagull Optimization Algorithm

Most objectives associated with the routing in the networking is of complex computation process, and consumes large volume of solution spaces. To overcome these concerns and to solve the objective functions effectively, metaheuristic algorithm that do perform optimization process is employed which possess the cumulative effects of advantages and overcomes the drawbacks the existing systems. Numerous metaheuristic approaches have been introduced such as single solution algorithm and algorithms based on the population. The solutions in the single solution approach is generated in a random manner and for population based approach, the solution is generated in the search space.

The proposed method employs metaheuristic seagull optimization algorithm [24] for easy implementation process and with reduced number of input parameters. The seagull is a bird categorized under omnivorous and has a special ability to flush the salt away from their body. The seagulls are the habitats that do live in a group called colonies, and it employs its skills in identifying and attacking their prey. The concept of seagull hunting their prey

is employed to determine the shortest path in the SDN for the genuine incoming service requesting packets. The malicious packets are detected and mitigated using the aforementioned algorithms.

Migration is the major process of seagulls in search of the prey. The seagulls tend to migrate in all directions thus achieving three major conditions.

- **Collision avoidance:** The seagulls when performing the migration process during the search of prey, tends to follow the collision avoidance migration process. A redundant variable “A” is used here for the determination of new search agent. The position agent is mathematically represented in equation 13.

$$N_{ps} = A \times P_s(t) \quad (13)$$

Where, N_{ps} is the new position of the seagulls and $P_s(t)$ is the current position of the seagulls. The redundant variable “A” can be defined as mentioned in equation 14.

$$A = f_c - (t, I_{max}) \quad (14)$$

Where, the f_c is the control frequency.

- **Migration aiming best neighbor:** The collision avoidance condition is followed by the migration of seagulls towards the best neighbor. The movement of seagulls towards the best neighbor is performed based on the best seagull and is represented in equation 15.

$$M_s = D * (P_{bs}(t) - P_s(t)) \quad (15)$$

Where M_s is the migration of the seagull and P_{bs} is the position of best seagull.

- **Close Affinity towards best search agent:** The final condition of the migration of seagull in detecting the prey is to maintain close affinity towards the best search agent. The updated or new position of the seagull is mathematically represented in equation 16 to 20.

$$D_s = |N_{ps} - M_s| \quad (16)$$

The new location of the best seagull in terms of x_n , y_n , and z_n coordinate system is represented in equation 17 to 19.

$$x_n = r * \cos(t) \quad (17)$$

$$y_n = r * \sin(t) \quad (18)$$

$$z_n = r * \tan(t) \quad (19)$$

The new position of the best seagull is represented in equation 20.

$$P_s(t) = (D_s * x_n * y_n * z_n) + P_{bs}(t) \quad (20)$$

The algorithm of the proposed seagull optimization algorithm in determining the best multipath routing for load balancing mechanism is illustrated in Table 4.

Table 4 Seagull Optimization algorithm for best multipath routing with load balancing mechanism

Algorithm: Seagull Optimization algorithm for best multipath routing with load balancing mechanism

Input:

Population of seagulls (routers): N_R

Process:

- Initialization of parameters. A, f_c , I_{max} .
- Predefine: $f_c = 4$
- Predefine: $u=1$ [any value between 0 to 1]
- Predefine: $v=1$ [any value between 0 to 1]
- while ($t < I_{max}$)
- do
- $P_{bs}(t) = \text{Det fitness}(P_s)$
- Choose random number: $rn=[0,1]$
- Choose prey $k: k=[0,1]$
- Determine the distance using the equation 16.
- Determine the location of the best seagull in terms of x , y and z using equations 17, 18 and 19.
- Determine the position of new seagull using equation 20.
- end do
- end process

The objective of the proposed work is fulfilled using the aforementioned algorithms and methodology. The incoming malicious packet intended with slow rate DDoS attack reaching the SDN is detected and mitigated using the Artificial Fish Swarm Algorithm (AFSA) and the amalgamated model of CNN-RNN. The remaining genuine service requesting packets are treated using Seagull optimization algorithm for multipath routing mechanism by providing load balancing concept.

4. Results and Discussion

The proposed work is a two folded methodology intended to provide security to the SDN from the malicious packet creating slow rate Distributed Denial of Service (DDoS) attack and to provide a load balancing in the SDN through multipath routing mechanism.

The proposed work is analyzed based on the security analysis and the routing parameters like throughput, latency, and jitter. The analysis of the proposed research work is performed on the raw personal computer oriented implementation using Linux forwarding and is compared with the performance of the Open flow [25] and Linux ProGFE SDN models. It is designed and tested using Mininet emulator operated on the Linux Fedora 64 bit Operating System.

An Openflow Version 1.10 is employed to determine the topology of the SDN. For the purpose of analyzing the proposed research work, a simple linear network topology is employed with varying quantity of fan outs. A unique dataset is created for detecting the DDoS attack in the SDN network rather than preferring the existing datasets. The unique dataset is composed of one hundred recording oriented on the statistical features like duration, byte count, packet rate, packet per flow measured in the protocol namely UDP, TCP and ICMP. The unique dataset is fed with the usual data pattern which is used during the analysis of the incoming service requesting packets.

In synthesis, Figure 2 demonstrates that the proposed framework holistically addresses the tripartite challenge of modern local e-governance: it secures the network against cyber threats, stabilizes the end-user experience, and scales administrative capacity. By embedding intelligent, response-time-aware optimization into the SDN-enabled ICN architecture, this framework empowers local authorities to deliver resilient, high-trust digital public services that meet the escalating demands of contemporary smart city ecosystems.

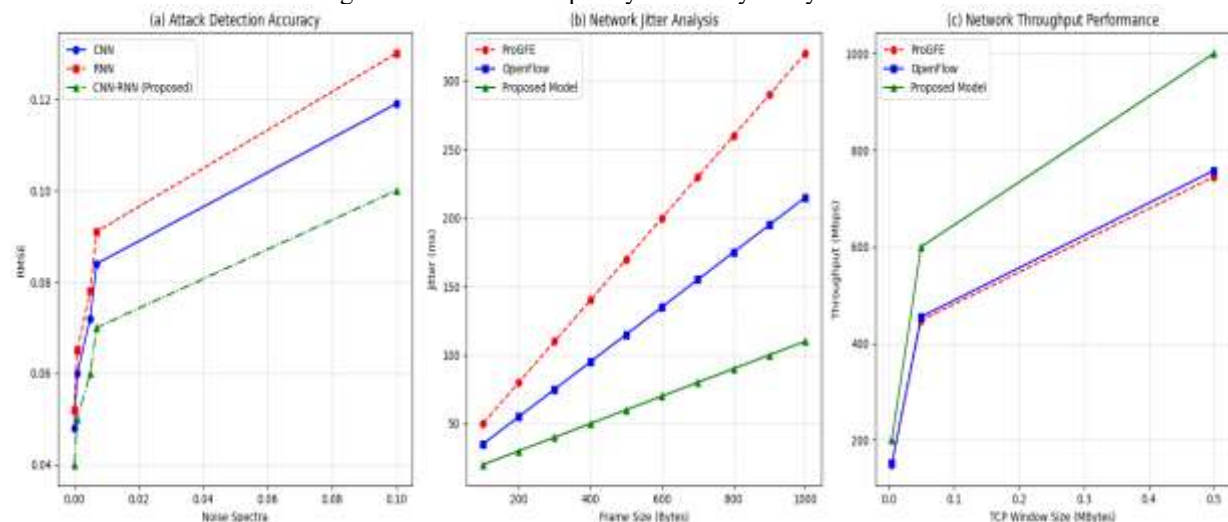


Figure 2. The performance evaluation of the developed AI-enabled load balancing scheme for local governments' computer networks.

In panel (a), the superiority of the hybrid CNN-RNN scheme (using AFSA optimization approach) is demonstrated by the fact that it gives the lowest RMSE values when tested with various noise spectra. The lower network jitter demonstrated by the routing scheme in panel (b) compared to other schemes such as OpenFlow and ProGFE proves the stability in the delivery of government citizen services. From panel (c), it can be seen that the network throughput improves substantially at different TCP window sizes.

5. Conclusion

The exponential surge in web demands intelligent and adaptive network management strategies, particularly in Software Defined Networking enabled Information Centric Network architecture. This paper addressed the two critical, intertwined challenges in such environments: Early detection of DDoS attacks and dynamic selection of optimal, load- balanced routes- a process often undermined by existing solutions that neglect crucial server response time. This paper sought to address these challenges through a new optimization approach that is twofold. First, for security purposes, a hybrid deep learning model combining AFSA with CNN-RNN was designed, which made use of the ability of AFSA to search globally to optimize the hyperparameters of the deep network, which helped in improving feature extraction and temporal pattern detection in the network traffic. On the other hand, for efficiency in routing, a Seagull Optimization Algorithm metaheuristic was used to define a custom fitness function capable of balancing the network load and congestion, and implicitly, server response.

From the empirical testing of this framework, it became evident that promising results have been obtained, proving the usefulness of the approach. The hybrid AFSA-CNN-RNN model proved effective in terms of attack detection

in that the RMSE was reduced by 16.13% and 22.91% when compared to individual CNN and RNN, respectively. Moreover, incorporation of seagull optimization-based routing scheme led to an impressive improvement in network performance as network throughput increased by 31.98% and 33.96% when compared to conventional OpenFlow protocol and Linux ProGFE approach, respectively. Thus, the combination of quantitative improvements validates the efficiency of the proposed design in terms of improving the security of the network while providing high-quality network performance.

It is possible to further expand the metaheuristic routing scheme to include energy consumption as the third criterion, thus bringing green networking concepts into the scope of the developed design, and ensuring sustainable scalability in the future development of 6G and IoT-based ICNs.

References

- [1]. Madhusanka Liyanage; Andrei Gurtov; Mika Ylianttila, "Software Defined Networking Concepts," in *Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture*, Wiley, 2015, pp.21-44, doi: 10.1002/9781118900253.ch3.
- [2]. Guy Pujolle, "SDN (Software-Defined Networking)," in *Software Networks: Virtualization, SDN, 5G, and Security*, Wiley, 2020, pp.13-32, doi: 10.1002/9781119694748.ch2.
- [3]. T. Zhang, P. Agrawal and Jyh-Cheng Chen, "IP-based base stations and soft handoff in all-IP wireless networks," in *IEEE Personal Communications*, vol. 8, no. 5, pp. 24-30, Oct. 2001, doi: 10.1109/98.960337.
- [4]. S. Ejaz, Z. Iqbal, P. Azmat Shah, B. H. Bukhari, A. Ali and F. Aadil, "Traffic Load Balancing Using Software Defined Networking (SDN) Controller as Virtualized Network Function," in *IEEE Access*, vol. 7, pp. 46646-46658, 2019, doi: 10.1109/ACCESS.2019.2909356..
- [5]. Q. Yan, F. R. Yu, Q. Gong and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602-622, Firstquarter 2016, doi: 10.1109/COMST.2015.2487361.
- [6]. H. S. Abdulkarem and A. Dawod, "DDoS Attack Detection and Mitigation at SDN Data Plane Layer," 2020 2nd Global Power, Energy and Communication Conference (GPECOM), 2020, pp. 322-326, doi: 10.1109/GPECOM49333.2020.9247850.
- [7]. S. K. Yadav, P. Suguna and R. L. Velusamy, "Entropy based mitigation of Distributed-Denial-of-Service (DDoS) attack on Control Plane in Software-Defined-Network (SDN)," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-7, doi: 10.1109/ICCCNT45670.2019.8944426.
- [8]. R. M. Thomas and D. James, "DDoS detection and denial using third party application in SDN," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017, pp. 3892-3897, doi: 10.1109/ICECDS.2017.8390193.
- [9]. P. Leng et al., "Logistic Regression Based on Artificial Fish Swarm Algorithm with T-Distribution Parameters," 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 2020, pp. 1912-1915, doi: 10.1109/ITAIC49862.2020.9338804.
- [10]. F. A. Uçkun, H. Özer, E. Nurbas and E. Onat, "Direction Finding Using Convolutional Neural Networks and Convolutional Recurrent Neural Networks," 2020 28th Signal Processing and Communications Applications Conference (SIU), 2020, pp. 1-4, doi: 10.1109/SIU49456.2020.9302448.
- [11]. P. T. Dinh and M. Park, "BDF-SDN: A Big Data Framework for DDoS Attack Detection in Large-Scale SDN-Based Cloud," 2021 IEEE Conference on Dependable and Secure Computing (DSC), 2021, pp. 1-8, doi: 10.1109/DSC49826.2021.9346269.
- [12]. H. Nurwarsito and M. F. Nadhif, "DDoS Attack Early Detection and Mitigation System on SDN using Random Forest Algorithm and Ryu Framework," 2021 8th International Conference on Computer and Communication Engineering (ICCCE), 2021, pp. 178-183, doi: 10.1109/ICCCE50029.2021.9467167.
- [13]. Y. Cao, H. Jiang, Y. Deng, J. Wu, P. Zhou and W. Luo, "Detecting and Mitigating DDoS Attacks in SDN Using Spatial-Temporal Graph Convolutional Network," in *IEEE Transactions on Dependable and Secure Computing*, doi: 10.1109/TDSC.2021.3108782.
- [14]. M. Klymash, O. Shpur, N. Peleh and O. Maksysko, "Concept of Intelligent Detection of DDoS Attacks in SDN Networks Using Machine Learning," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 609-612, doi: 10.1109/PICST51311.2020.9467963
- [15]. H. S. Abdulkarem and A. Dawod, "DDoS Attack Detection and Mitigation at SDN Data Plane Layer," 2020 2nd Global Power, Energy and Communication Conference (GPECOM), 2020, pp. 322-326, doi: 10.1109/GPECOM49333.2020.9247850.

- [16]. R. Sanjeetha, S. Srivastava, A. Kanavalli, A. Pattanaik and A. Gupta, "Mitigation of Combined DDoS attack on SDN Controller and Primary Server in Software Defined Networks using a priority on traffic variation," 2020 International Conference for Emerging Technology (INCET), 2020, pp. 1-5, doi: 10.1109/INCET49848.2020.9153998.
- [17]. J. A. Pérez-Díaz, I. A. Valdovinos, K. -K. R. Choo and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," in IEEE Access, vol. 8, pp. 155859-155872, 2020, doi: 10.1109/ACCESS.2020.3019330.
- [18]. A. T. Kyaw, M. Zin Oo and C. S. Khin, "Machine-Learning Based DDOS Attack Classifier in Software Defined Network," International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2020, pp. 431-434, doi: 10.1109/ECTI-CON49241.2020.9158230.
- [19]. B. Nugraha and R. N. Murthy, "Deep Learning-based DDoS Attack Detection in SDN-based Networks," 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2020, pp. 51-56, doi: 10.1109/NFV-SDN50289.2020.9289894.
- [20]. W. Sun, Y. Li and S. Guan, "An Improved Method of DDoS Attack Detection for Controller of SDN," 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET), 2019, pp. 249-253, doi: 10.1109/CCET48361.2019.8989356.
- [21]. Y. Cheng, M. Jiang and D. Yuan, "Novel Clustering Algorithms Based on Improved Artificial Fish Swarm Algorithm," 2009 Sixth International Conference on Fuzzy Systems and Knowledge Discovery, 2009, pp. 141-145, doi: 10.1109/FSKD.2009.534.
- [22]. F. A. Uçkun, H. Özer, E. Nurbaş and E. Onat, "Direction Finding Using Convolutional Neural Networks and Convolutional Recurrent Neural Networks," 2020 28th Signal Processing and Communications Applications Conference (SIU), 2020, pp. 1-4, doi: 10.1109/SIU49456.2020.9302448.
- [23]. A. H. Alawadi and S. Molnár, "Risk Analysis of Blocked Rate Predictions for SDN Load Balancing Using Monte Carlo Simulation," 2019 IEEE Symposium on Computers and Communications (ISCC), 2019, pp. 1028-1033, doi: 10.1109/ISCC47284.2019.8969746.
- [24]. H. Jia, Z. Xing and W. Song, "A New Hybrid Seagull Optimization Algorithm for Feature Selection," in IEEE Access, vol. 7, pp. 49614-49631, 2019, doi: 10.1109/ACCESS.2019.2909945.
- [25]. S. Midha and K. Triptahi, "Extended TLS security and Defensive Algorithm in OpenFlow SDN," 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2019, pp. 141-146, doi: 10.1109/CONFLUENCE.2019.8776607.
- [26]. Elsheway A.M., Abbas, S., Osman, A.M. et al. DDoS classification of network traffic in software defined networking SDN using a hybrid convolutional and gated recurrent neural network. Sci Rep 15, 29122 (2025). <https://doi.org/10.1038/s41598-025-13754-1>
- [27]. Kalafy, S.A.A., Pashazadeh, S. & Salehpour, P. Dynamic graph neural network-based framework to increase detection accuracy in SDN under DDOS. Sci Rep 16, 2305 (2026). <https://doi.org/10.1038/s41598-025-32102-x>
- [28]. Chen, J., Xiao, W., Zhang, H. et al. Dynamic routing optimization in software-defined networking based on a metaheuristic algorithm. J Cloud Comp 13, 41 (2024). <https://doi.org/10.1186/s13677-024-00603-1>
- [29]. Tache, M.D.; Păscuțoiu, O.; Borcoci, E. Optimization Algorithms in SDN: Routing, Load Balancing, and Delay Optimization. Appl. Sci. 2024, 14, 5967. <https://doi.org/10.3390/app14145967>
- [30]. Jayaprakash, M., & Devi Priya, R. (2024). An Optimized Routing Scheme in SDN-Based IoT Using the Lion Optimization Algorithm. IETE Journal of Research, 70(8), 6745–6756. <https://doi.org/10.1080/03772063.2024.2305846>