International Journal of Advanced Trends in Engineering and Management
(ISSN 2583-7052)

Vol. IV, No. 01, pp. 23-34, February

A Hybrid Deep Learning for DDoS attack detection: feature selection with ACO and classification with Attention CNN

P. Malathi[1], Kannaki[2]

[1]Department of Electrical and Electronics Engineering, Government College of Engineering, Tirunelveli, India.
[2]Department of Electronics and Communication Engineering, Assistant Professor, Dhanalakshmi Srinivasan College of Engineering, Coimbatore. 641105
Corresponding Author E-mail: Kannaki@dsce.ac.in

ABSTRACT: Distributed Denial-of-Service (DDoS) attacks are a security challenge for the Software-Defined Network (SDN). Effective traffic is critical for network durability and routine, necessitating intelligent and adaptive mechanisms. This paper presents a novel hybrid approach integrating Ant Colony Optimization (ACO) with Attention Convolutional Neural Network (CNN) to enhance cyber-attack. ACO optimizes Attention CNN parameters to improve learning efficiency and convergence, enabling dynamic adaptation to real-time network conditions. By using the global search capability of ACO and the predictive strength of Attention CNNs, the proposed method achieves better network traffic compared to other techniques. Using python software the ACO-Attention CNN significantly increase precision recall accuracy and ROC curve for cyber-attack. The proposed framework contributes to the development of intelligent, network traffic for DDoS attack, ensuring sustainable and resilient network communication.

Keywords: Distributed Denial of Service attack (DDoS), Ant Colony Optimization (ACO), Attention Convolutional Neural Network (CNN), Data cleaning, Data Exploration.

1. Introduction

DDoS attacks have emerged as one of the most persistent network security issues. The Computer Incidence Advisory Capability reported that the first attack incidence is done in 1999. Although the numerous protection strategies that have been put out in both academics and industry, DDoS attacks continue to constitute a serious danger and are becoming more frequent every year [1]. The main objective of DoS attack detection is to identify the attack and take the required step to reduce its destruction [2]. Conversely, uses a particular device to detect and stop malicious traffic, observing system performance, and analysing network traffic. DoS attacks be identified using a variety of techniques, such as behaviour-based detection, network-based detection, anomaly-based detection, and signature-based detection [3-4]. However, organizations employ tactics like traffic filtering, increasing system capacity, redundancy, and the use of specialist security technologies made especially to detect and stop DoS assaults in order to fight them [5- 6]. Whereas, the primary goal is protecting the targeted system's functioning and availability for authorized users [7]. Moreover, DDoS assaults fall into three primary kinds of behaviour these include application, traffic, and bandwidth attacks. Attackers that use traffic-based attacks bombard the victim server with a large amount of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets, which lowers the victim server's overall performance [8]. Figure 1 shows the DDoS attack. To identify DDoS attacks machine learning technique are used for prediction algorithms.

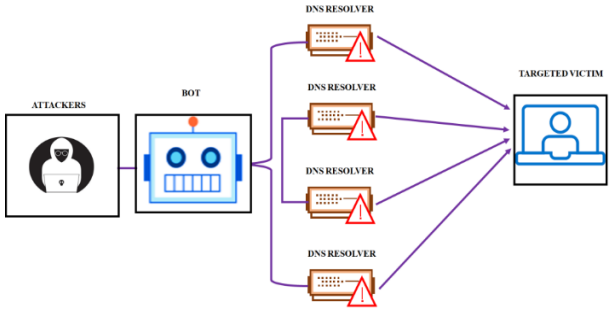

Figure 1: *DDoS attack*

A machine learning method called Random Forest (RF) and XG Boost is used to categorize and estimate different types of DDoS attack. However, the trained model also undergoes model optimization in terms of kernel scaling and kernel hyper parameter change in order to boost model efficiency. The drawbacks are less interpretable, computationally costly and prone to over fitting [9]. For the detection of DDoS attack packets a Multi-Layer Perceptron (MLP) is used. It detects the attacks packets with higher accuracy and performance. The proper functioning of the MLP depends on the quality of the training [10]. Whereas a modified Long Short Term Memory (LSTM) based intrusion detection for identifying DDoS attack. The protection of secrecy and denial-of-service is a major advantage of employing secure traffic. These methods have performance and network concern [11]. Moreover to improve the classification accuracy of DDoS attack a Convolution Neural Network (CNN) is used. Here, the traffic is recognized for protecting data key management techniques. It takes more time to access for secure traffic and network [12]. However, using Artificial Neural Network (ANN) the prediction accuracy is improved with high performance. Data network traffic is not identified because encircle in the data network is not covered perfectly [13]. Whereas, to detect the DDoS attack Deep Neural Network (DNN) and Deep Belief Neural Network (DBNN) is used with low traffic. They have yet to attain the degree of accuracy. Additionally, its effectiveness under diverse large-scale attack scenarios requires further evaluation [14-15]. When analysing network traffic, DDoS attack able to identify the attack in difference among malicious and legitimate traffic. The variety of network traffic characteristics and attack types in DDoS attack presents another challenge for DL. To overcome this problem Ant Colony Optimization with Attention CNN is used.

2. Related work

Salmi *et al* [16] (2023) have proposed CNN-LSTM, hybrid model, to effectively detect DoS attacks using network traffic data. Hybrid representations merging CNN in addition LSTM have the highest accuracy as well as recognition rates. The precision as well as recall is low when using the hybrid models combining CNN and LSTM compared to other techniques.

Adhao *et al* [17] (2020) have invented a Genetic Algorithm (GA) as well as Principal Component Analysis (PCA) for detecting DDoS attack. Here, the attack is detected using Decision Tree (DT) classifier. Using a decision tree in combining with PCA-GA the accuracy is increased with higher performance. It takes more time to find the network traffic compared to other technique.

Chanu *et al* [18] (2023) have proposed a Multi-Layer Perceptron with Genetic Algorithm (MLP-GA) as a classifier outperforms the conventional classifiers for detecting the DDoS attacks. Finally, given to classifier, which uses it to categorize various types of network traffic. The drawback is that in order to increase the model's capabilities, they reassign the weights of time-based features.

Hussan *et al* [19] (2024) have proposed an improved Elman Recurrent Neural Network (ERNN) based on Chaotic Bacterial Colony Optimization (CBCO) to detect DDoS attack. Employs CBCO to determine the ideal ERNN architecture structure (number of hidden neurons) and parameters (weights and biases). To enhance BCO's probe and manipulation capabilities the chaos theory initialized the bacterial population and choosing the proper chemo taxis step size value. To improve the convergence rate and prevent local optima, the ERNN model is trained using the CBCO technique.

Rizvi *et al* [20] (2024) have proposed a K-Nearest Neighbor (KNN) model for DDoS assault detection using Genetic Algorithm based optimization. KNN-GA have consistently proven to be effective or reliable in identifying and thwarting attacks using statistical analysis and established patterns. The disadvantage of this method is the type of the attack in not predicted correctly in the network. The contribution of this study is summarized as follows:

- The work evaluates the impact of dataset selection on the performance of DDoS attack, specifically using DDoS SDN dataset.
- Introduces data cleaning and data exploration to improve the reliability and quality of input data for network traffic analysis.
- Develops an Ant Colony Optimization and Attention CNN classifier to enhance DDoS attack accuracy and efficiency.
- Validates the proposed model using metrics like accuracy, precision, recall, F1-score, and AUC, demonstrating significant improvement over existing methods.

3. Proposed work

The block diagram in figure 2 shows the proposed ACO and Attention CNN technique. In order to increase the usefulness and robustness of the datasets, first data pre-processing is implemented. This includes data cleaning to collect the input data by handling missing values, removing outliers, and normalizing. The pre-processed data is then subjected to a strategy of data pre-processing based on data exploration. The exploration technique visualizes a graph to detect the network traffic.

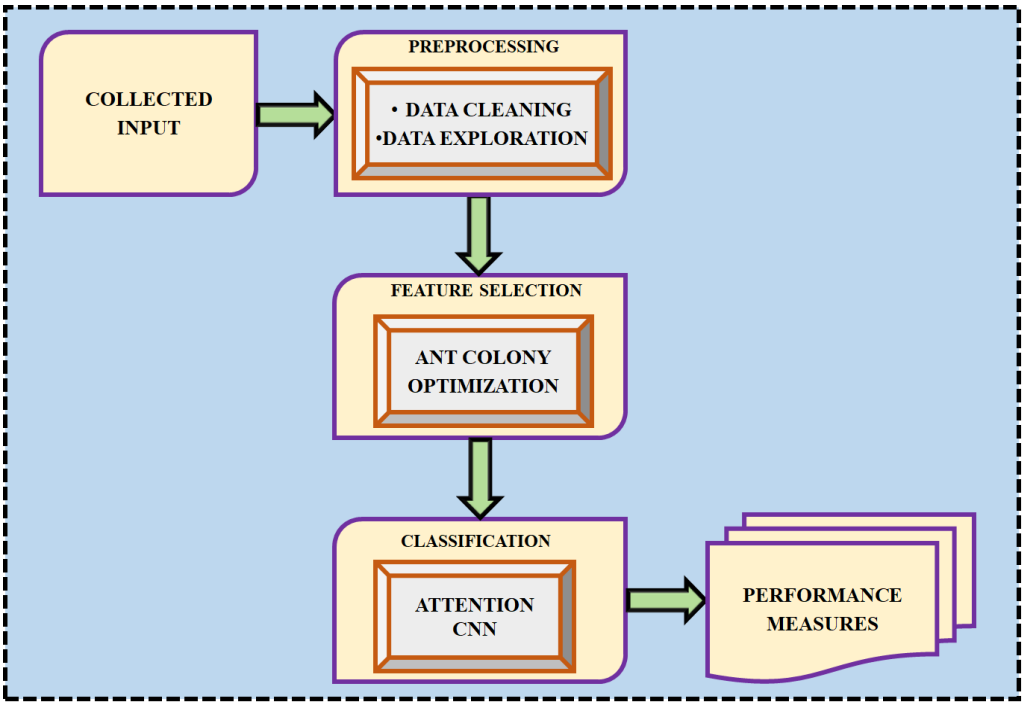

Figure 2: *Proposed block diagram*

Then feature selection based on Ant Colony Optimization algorithm. Finally, the classifier verifying the performance using the technique called Attention CNN. The Attention CNN classifier model is block Convolutional Neural Networks use a technique called attention to highlight significant elements when flopping irrelevant ones. Then trained output is classified to get high accuracy and better network traffic in DDoS attack. The results are validated and calculated by evaluation metrics alike F1-score,

precision, recall, and accuracy to get better accuracy compared to the existing systems.

3. 1 Data pre-processing

Data cleaning and exploration are the initial stages of data pre-processing.

3.1.1 Data cleaning

The process of eliminating or correcting corrupted, incorrect, duplicate, from datasets is known as data cleaning in DDoS-SDN dataset. Cleaning up the dataset is the primary objective in order to standardize data analysis and make it easier to locate the right data for a query.

3. 2 Feature Selection

In feature selection Ant Colony Optimization (ACO) is used to optimize the DDoS attack.

3.2.1 Ant Colony Optimization

The idea behind the ACO algorithm is influenced by the way ants use pheromone trails to find food a source is in figure 3. This approach is regarded as an optimization strategy that seeks to determine the best route between two points in a network. An ant colony is recognised at the initial stage before start the ACO algorithm. Depending on the quantity of pheromones on connected edges and other useful information, each ant travels between nodes. Until a particular halting condition is satisfied, the ants' solutions are continuously assessed to update the pheromone pathways.

3.1.2Data exploration

Exploration utilizes statistical methods in the first stage of data analysis to comprehend the nature of data. DDoS attack aids a security administrator in intuitively identifying anomalous activity. Due to the intuitive nature of attack, visualization facilitates quick analysis and reaction. A network-based visualization technique for DDoS uses a visual graph to represent the source, destination, port, and other information of the network's packets. Therefore, this technique identifies a traffic when an attack deviates from the graph's usual state and extract the attack's diagnostic properties to implement DDoS. Nevertheless, these techniques display audit data rather than notifications directly. Next, the pre-processed data is given to the feature selection.

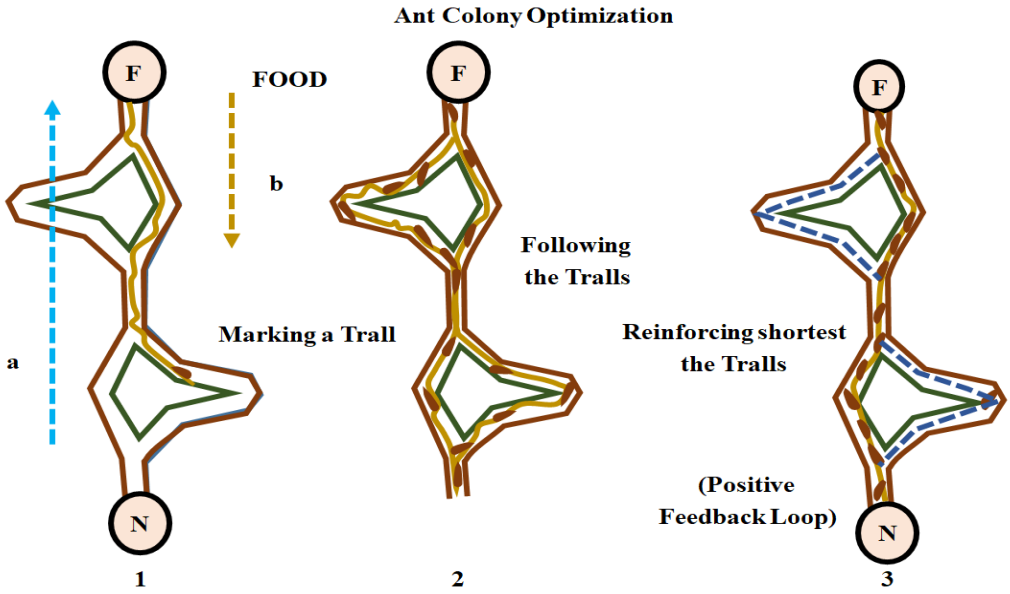

Figure 3: *Ant Colony Optimization*

Algorithm 1 contains the entire pseudocode for ACO method, which is frequently employed to solve optimization issues. ACO is distinguished for producing excellent solutions via its iterations, proving its capacity to effectively and efficiently strengthen security measures in WSNs.

Algorithm 1 ACO Algorithm Pseudo code

Initiate
modify parameters
while stopping condition not mollified **do**
Put the ACO ant in the starting node.
repeat
for ACO ant **do**
Use the state transition rule to determine the next node.
Apply the pheromone update step-by-step.
end for
until each ant has developed a remedy
update the optimal solution
relate disconnected pheromone apprise
end while=0

Pheromone evaporation rate, ant population, pheromone deposit factor, and exploration factor are some of the programmable characteristics of the ACO algorithms that might enhance their effectiveness. These factors affect the quantity of pheromone deposited, the rate at which pheromone trails evaporate, the number of ants utilized, and the ratio of exploration to exploitation. To enhance performance, other problem-specific factors are also changed, including the number of iterations, problem encoding, and heuristic information.

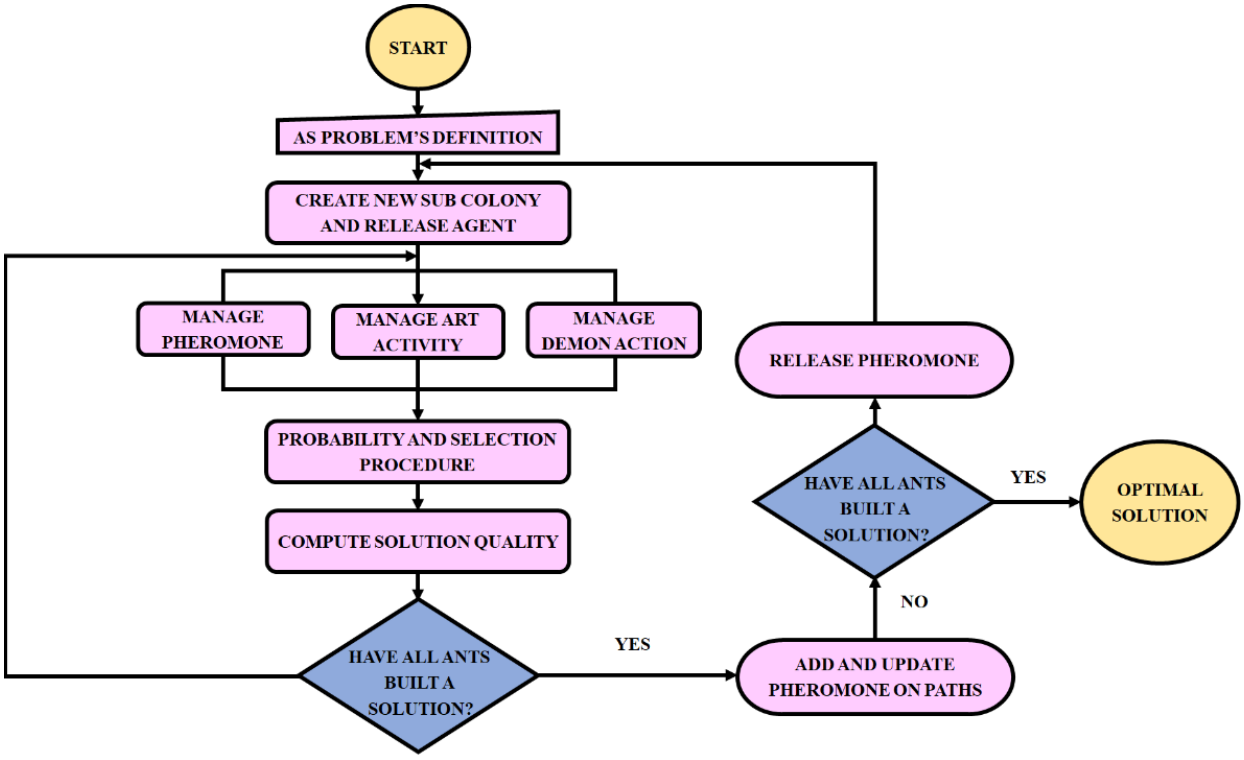

Figure 4: *Flow chart for ACO*

The best configurations require several experiments to find ideal parameter settings, which vary depending on particular problem being tackled in figure 4. The number of ants, nodes, iterations, and the effectiveness of the nodes' pheromone selection and updating all affect Algorithm 1 performance. The computational capacity is determined by the aforementioned criteria. As a result, the ACO algorithm's lower bound is (n), and its upper bound is $O(n^2)$.

3. 3 Classification

3. 3. 1 Attention CNN

Deep learning models' attention mechanisms appeal inspiration from how the human brain interprets data. Attention mechanisms in deep

learning models be implemented in a variety of ways, with the particular implementation varying based on the job at hand and the model type. When implementing the attention mechanism in an attention-based CNN, an extra layer is usually added to the model to learn the attention weights for each input component. These weights are subsequently added to the CNN model's output, enabling it to concentrate on the input's most pertinent aspects.

3. 3. 2 Input Layer

To obtain the initial vector representation, the input layer must substitute the relevant word vector for each word in the phrase.

Convolution Layer: The convolution layer is wide, meaning that the sentence's edges are zeroes. The sentence's words are indicated by $v1, v2, \dots, vs, ci \in Rw \cdot d0, 0 < i < s + w$ means that w denotes window length, and $vi - w + 1, \dots, vi$ convolved to produce the sentence. $vi - w + 1, \dots, vi$ demonstration. This is provided by the equation that follows.

$$P_i = \tanh(W.c_i + b) \qquad (1)$$

Where $W \in Rd1 \times wd0$ are the convolutional network's parameters.

Average pooling Layer: Average pooling for all columns is carried out for the final convolutional layer in the network structure; this is known as all-ap. Depending on the window size w, average pooling is carried out for successive w columns for the remaining convolutional layers in the network. This structure enables multi-layer superposition into a deeper network structure to obtain more abstract features. When the convolutional network window size is w, the input s column feature becomes $s + w - 1$ columns after the convolutional layer, and then returns to $s$columns after pooling.

3. 3. 3 Output Layer

Various tasks determine the output layer. Furthermore, the authors discovered that the model is enhanced if each convolutional layer's output is pooling over all columns (all-ap) and subsequently utilized as features in the output layer.

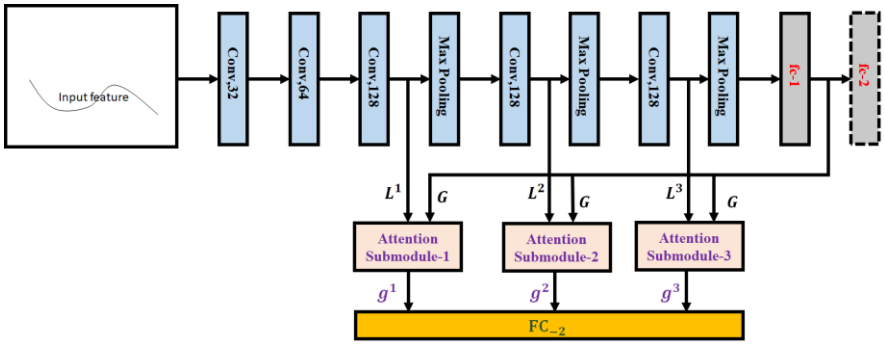

Figure 5: *Attention CNN*

For DDoS attack the Local Attention Module mostly finishes the current convolutional layer's channel and spatial attention methods and implements them specifically. The attention mechanism in the model in figure 5 is composed of the attention derived from each convolutional layer and the CNN's subsequent feature output. Through a training procedure, these tensors attention mechanism are ultimately coupled to determine the proper attention factors for that DDoS SDN dataset is used. The original feature is processed independently by the two sub-modules to produce two intermediate tensors. The refined feature is then obtained by performing element-wise multiplication operations on the original features and the two intermediate tensors.

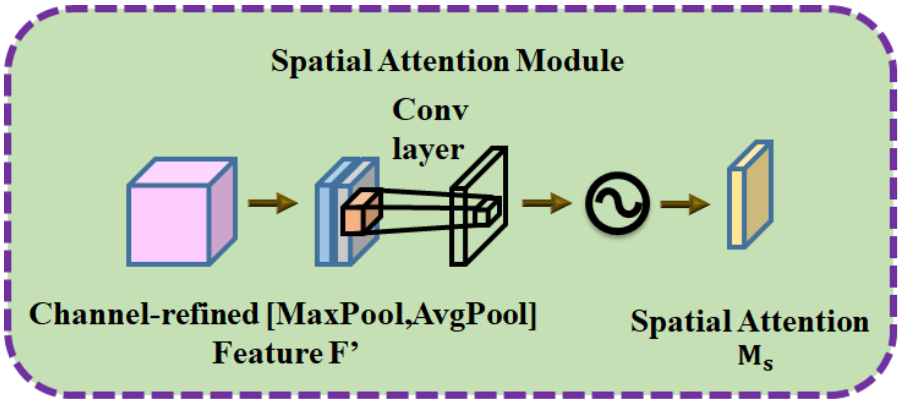

Figure 6: *Spatial attention module*

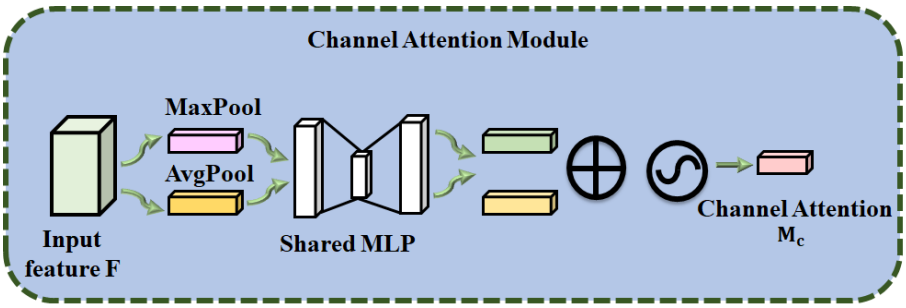

Figure 7: *Channel attention module*

Figures 6 and 7 show the basic specifics of two sub-modules, channel attention and spatial attention. The Channel Attention sub-module applies Global AvgPool and Global MaxPool to this feature tensor. The dual intermediaries are then added element-wise after they both have passed through a fully connected layer. Lastly, the optimization tensor through the channel attention device is obtained by multiplying the summing effect by the unique feature tensor element-wise. These feature tensors were subjected to AvgPool in the spatial attention sub-module. The subsequent convolutional layer then extracted the new features. Finally, the new feature tensor is multiplied by the old feature tensor element-wise for DDoS assault to obtain the optimization tensor with the spatial attention mechanism attached.
The following formula is used to illustrate the Spatial Attention implementation basis.

$$SA(F) = f \otimes \text{conv}(\text{Avgpool(f)}) \quad (2)$$

The following formulas is used to express channel attention

$$path1(f) = Dense(GlobalAvgPool(f) \quad (3)$$

$$path2(f) = Dense(GlobalMaxPool(f) \quad (4)$$

$$CA(f) = f \otimes \left(\text{Path1(f)} \otimes \text{Path2(f)}\right) \quad (5)$$

Where, $\otimes$ denotes element-level multiplication, and f is the input feature. Convolutional layer operation is referred to as $Conv$, and average pooling is called $AvgPool$.

4. Results and Discussion

The simulation configuration is designed for ACO and Attention CNN in DDoS attacks. This section presents the effectiveness of future procedure employing ACO and Attention CNN, along with a discussion and comparative analysis.

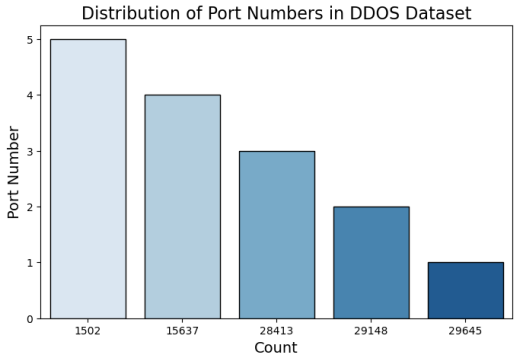

Figure 8: *Distribution of port number in DDoS dataset*

Figure 8 the distribution of port number in DDoS dataset is mentioned. Here the port number is from 0 to 5. Some of the counts for DDoS attack is 1502, 15637, 28413, 29148 and 29645.

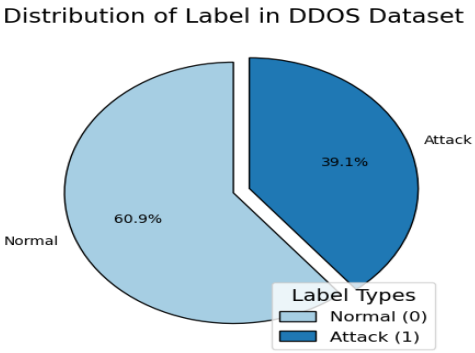

Figure 9: *Distribution of label in DDoS dataset*

Figure 9 the distribution of label in DDoS dataset is ploted. Here label types "1" indicate that it is DDoS attack and "0" indicates it is normal. The label types are attacked by 39.1% and normal by 60.9% respectively.

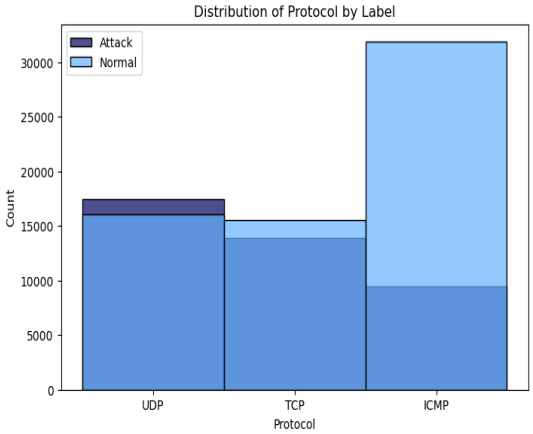

Figure 10: *Distribution of protocol by label*

DDoS by label types have both service and count is to feature the normal and attack using the tcp, udp and icmp protocol. The count ranges from 0 to 30000 where the tcp ranges from 0 to 14000 at that time it is attack and from 14000 to 15000 it is normal in the network traffic, udp is normal from 0 to 16000, attack from 16000 to 18000 and the icmp is normal in the range of 8000 to 30000 and attack from 0 to 8000. Distribution of protocol by label is shown in figure 10.

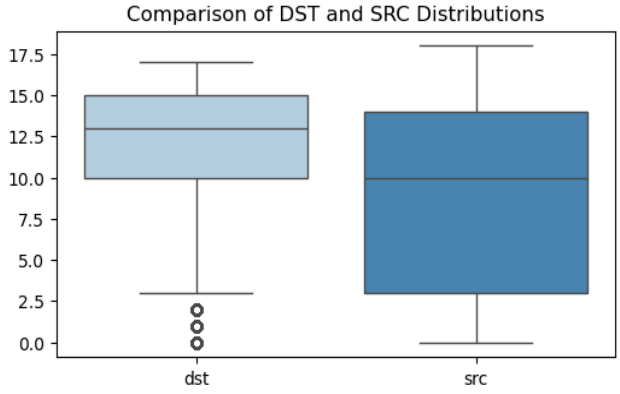

Figure 11: *Comparison of Destination (DST) and Source (SRC) distribution*

Figure 11 shows the comparison of Destination (DST) and Source (SRC) distributions. Here the source count is distributed from count 2.5 to 13 and the destination cunt from 10 to 15 respectively.

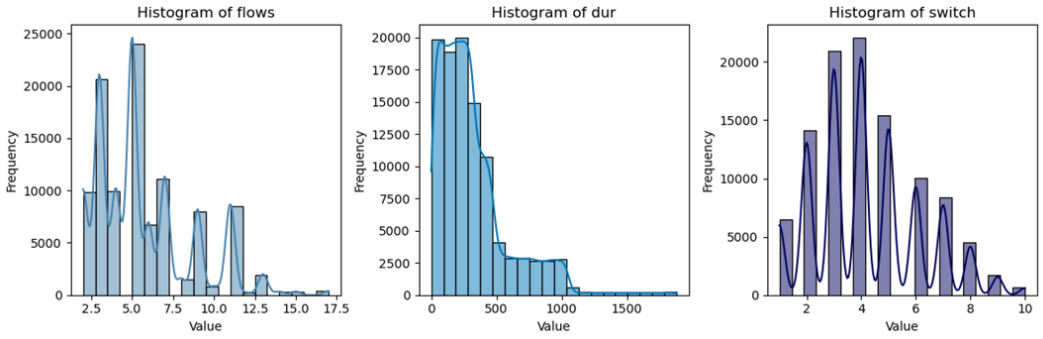

Figure 12: *Histogram value for each label types*

Whereas, histogram of switch the frequency ranges from 0 to 20000 it is going on increasing and decreasing in the value of 2 to 10 and it is very low in the value of 10 respectively.

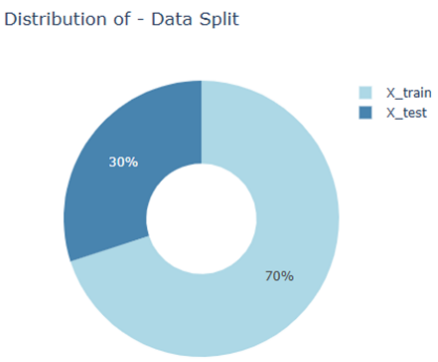

Figure 13: *Distribution of data split*

Figure 13 show the distribution of data split for DDoS attack. Here the input DDoS SDN data is splitted as 70% for x_train and 30% for x_test.

4. 1. Performance metrics

By examining accuracy, precision, sensitivity, specificity, Area under the Curve (AUC), classification with "positive" and "negative" labels, the performance of each classification model in this study explained in table 1.

Table 1: *Performance metrics*

Performance metrics	Formula
Accuracy	$\frac{(TN+TP)}{TS}$
Precision	$\frac{(TP)}{TP+FP}$
Recall	$\frac{(TP)}{(TP+FN)}$
$F1-score$	$\frac{(2 * \text{Precision} * \text{Recall})}{(Precision\ + Recall)}$

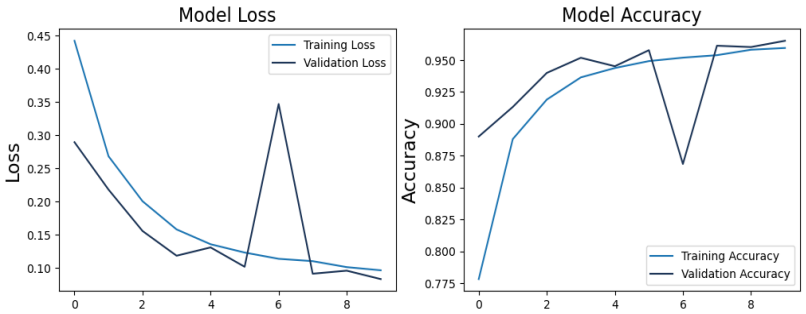

Figure 14: *Model loss and model accuracy*

Figure 14 shows the model loss and model accuracy. Here in model loss the training loss is going on decreasing and the validation loss is going on increasing then decreased below training loss. The accuracy value is trained using the Attention CNN to optimize the model to get the higher accuracy of 96%. When compared to the existing method proposed methods have better accuracy.

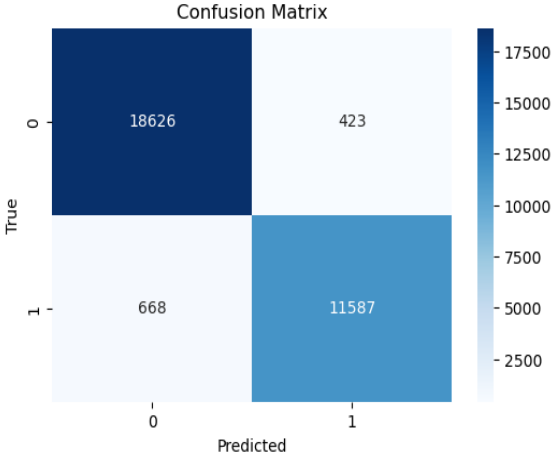

Figure 15: *Confusion matrix for Attention CNN*

Figure 15 illustrates the confusion matrix for Attention CNN for DDoS attack. This matrix shows the values for true and predicted labels. Confusion matrices are commonly utilized to evaluate the performance of classification models, particularly those tasked with predicting categorical labels for input instances.

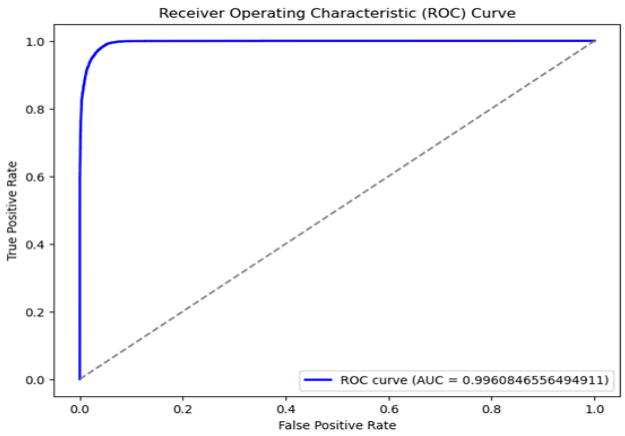

Figure 16: *ROC curve*

According to the results shown in Figure 16, the DDoS attack, the suggested Attention CNN continues to have the highest AUC value of 0.99, demonstrating the unique overview and flexibility of this approach.

4. 2 Comparison for the proposed method

The comparison of proposed method with existing method is presented in table 2. The Random Forest have classification accuracy of 89% [9] and XG Boost have accuracy of 90% [9] The proposed Attention CNN have the higher accuracy of 96% compared to the existing method in table 2. The proposed Attention CNN have better performance.

Table 2: *Comparison for the proposed method*

Study	Method	Accuracy
Mohmand *et al.* [9]	Random Forest	89%
Mohmand*et al.*[9]	XG Boost	90%
Proposed approach	Attention CNN	96%

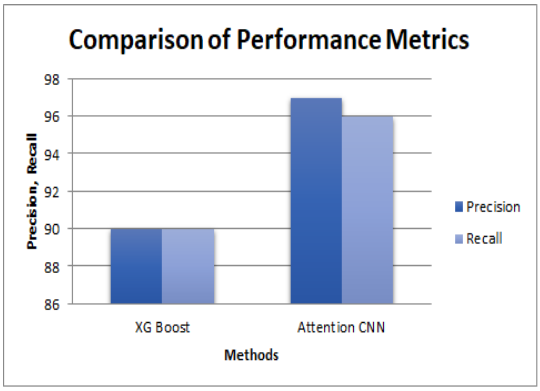

Figure 17: *Comparison of performance metrics*

The Precision and recall value for classifiers XG Boost and the proposed is presented in Figure 17. The XG Boot have the precision value of 90% and recall value of 90% [9] and proposed Attention CNN methods have the precision value of 97% and recall of 96% respectively.

5. Conclusion

This research introduces a comprehensive and efficient framework for detection and classification of DDoS attack using Attention CNN. The integration of advanced data preprocessing techniques, such as cleaning and exploration, ensures that the input data are optimized for feature selection. Additionally, the ACO for ants hunt for food using pheromone trails to navigate toward food sources to certain format data feature selection of the input data, capturing crucial patterns for effective classification. The performance evaluation, conducted on DDoS-SDN dataset, demonstrating the superior capabilities of Attention CNN compared to existing state-of-the-art methods. By using deep learning, the model focuses on critical features, resulting in improved accuracy of 96%.

References

1. Rami Ahmad; Raniyah Wazirali; Qusay Bsoul; Tarik Abu-Ain; Waleed Abu-Ain; Year: 2021, "Feature-selection and mutual-clustering approaches to improve DoS detection and maintain WSNs' lifetime", Sensors, Vol: 21, No: 14, pp.: 4821.

2. M. Premkumarand; T. V. P. Sundararajan, Year: 2020, "DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks", Microprocessors and Microsystems, Vol: 79, pp. 103278.

3. RajaSekhar Reddy NV; N. SreeDivya; B. N. Jagadesh; Ramu Gandikota; Kranthi Kumar Lella; Bhasha Pydala; Ramesh Vatambeti, Year: 2024, "Enhancing anomaly detection: a comprehensive approach with MTBO feature selection and TVETBOOptimized Quad-LSTM classification", Computers and Electrical Engineering, Vol: 119, pp. 109536.

4. M. Mayuranathan; S. K. Saravanan; B. Muthusenthil; A. Samydurai, Year: 2022, "An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique" Advances in Engineering Software, Vol: 173, pp. 103236.

5. Gebrekiros Gebreyesus Gebremariam; J. Panda; S. Indu, Year: 2023, “Localization and detection of multiple attacks in wireless sensor networks using artificial neural network”, Wireless Communications and Mobile Computing, Vol: 2023, No: 1, pp. 2744706.

6. Cheng-Chi Lee, Year: 2020, “Security and privacy in wireless sensor networks: Advances and challenges”, Sensors, Vol: 20, No: 3, pp. 744.

7. Sharmin Aktar; Abdullah Yasin Nur, Year: 2023, “Towards DDoS attack detection using deep learning approach”, Computers & Security, Vol: 129, pp. 103251.

8. Swathi Sambangi; Lakshmeeswari Gondi, Year: 2020, “A machine learning approach for ddos (distributed denial of service) attack detection using multiple linear regression”, In Proceedings, Vol: 63, No: 1, pp. 51.

9. Muhammad Ismail Mohmand; Hameed Hussain; Ayaz Ali Khan; Ubaid Ullah; Muhammad Zakarya; Aftab Ahmed; Mushtaq Raza; Izaz Ur Rahman; Muhammad Haleem, Year: 2022, “A machine learning-based classification and prediction technique for DDoS attacks." IEEE Access, Vol: 10, pp. 21443-21454.

10. Ashfaq Ahmad Najar; S. Manohar Naik, Year: 2022, “DDoS attack detection using MLP and Random Forest Algorithms”, International Journal of Information Technology, Vol: 14, No: 5, pp. 2317-2327.

11. Kuburat Oyeranti Adefemi Alimi; Khmaies Ouahada; Adnan M. Abu-Mahfouz; Suvendi Rimer; Oyeniyi Akeem Alimi, Year: 2022, “Refined LSTM based intrusion detection for denial-of-service attack in Internet of Things”, Journal of sensor and actuator networks Vol: 11, No: 3, pp: 32.

12. Yizhen Jia; Fangtian Zhong; Arwa Alrawais; Bei Gong; Xiuzhen Cheng, Year: 2020, “Flowguard: An intelligent edge defense mechanism against IoT DDoS attacks”, IEEE Internet of Things Journal, Vol: 7, No: 10, pp. 9552-9562.

13. Saurabh Deshpande; J. Gujarathi; P. Chandre; Pravin Nerkar. Year: 2021, “A comparative analysis of machine deep learning algorithms for intrusion detection in wsn”, Security Issues and Privacy Threats in Smart Ubiquitous Computing, pp. 173-193.

14. Auther Makuvaza; Dharm Singh Jat; Attlee M. Gamundani, Year: 2021, “Deep neural network (DNN) solution for real-time detection of distributed denial of service (DDoS) attacks in software defined networks (SDNs)”, SN Computer Science, Vol: 2, No: 2, pp.107.

15. S. Manimurugan; Saad Al-Mutairi; Majed Mohammed Aborokbah; Naveen Chilamkurti; Subramaniam Ganesan; Rizwan Patan, Year: 2020, “Effective attack detection in internet of medical things smart environment using a deep belief neural network”, IEEE Access, Vol: 8, pp. 77396-77404.

16. Salim Salmi; Lahcen Oughdir, Year: 2023, “Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network”, Journal of Big Data 10, No: 1, pp.17.

17. Rahul Adhao; Vinod Pachghare, Year: 2020, “Feature selection using principal component analysis and genetic algorithm”, Journal of Discrete Mathematical Sciences and Cryptography, Vol: 23, No: 2, pp. 595-602.

18. Usham Sanjota Chanu; Khundrakpam Johnson Singh; Yambem Jina Chanu, Year: 2023, “A dynamic feature selection technique to detect DDoS attack”, Journal of Information Security and Applications, Vol: 74, pp. 103445.

19. MI Thariq Hussan; G. Vinoda Reddy; P. T. Anitha; A. Kanagaraj; Pannangi Naresh, Year: 2024,

"DDoS attack detection in IoT environment using optimized Elman recurrent neural networks based on chaotic bacterial colony optimization", Cluster Computing, Vol: 27, No: 4, pp. 4469-4490.

20. Fizza Rizvi; Ravi Sharma; Nonita Sharma; Manik Rakhra; Arwa N. Aledaily; Wattana Viriyasitavat; Kusum Yadav; Gaurav Dhiman; Amandeep Kaur, Year: 2024, "An evolutionary KNN model for DDoS assault detection using genetic algorithm based optimization." Multimedia Tools and Applications, Vol: 83, No: 35, pp. 83005-83028.