FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 2 | Pages 308-314 | e-ISSN: 2347-470X

Attack Detection using DL based Feature Selection with Improved Convolutional Neural Network

Dr. V. Gokula Krishnan[1*], S. Hemamalini[2], Praneeth Cheraku[3], K. Hema Priya[4], Sangeetha Ganesan[5] and Dr. R. Balamanigandan[6]

[1]Professor, Department of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai, Tamil Nadu, India, gokul_kris143@yahoo.com

[2]Associate Professor, Department of CSE, Panimalar Engineering College, Poonamallee, Chennai, Tamil Nadu, India, hemamalini.selvamani@gmail.com

[3]Assistant Professor, Department of Information Technology, PVP Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India, chpraneeth@hotmail.com

[4]Assistant Professor, Department of CSE, Easwari Engineering College, Ramapuram, Chennai, Tamil Nadu, India, hemu.june3@gmail.com

[5]Department of AIDS, R M K College of Engineering and Technology, Kavaraipettai, Tamil Nadu, India, gsangeethakarthik@gmail.com

[6]Associate Professor, Department of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai, Tamil Nadu, India, balamanigandanr.sse@saveetha.com

***Correspondence:** Dr. V. Gokul Krishnan; gokul_kris143@yahoo.com

ABSTRACT- Decentralized wireless networks that may connect without a central hub are named Mobile Ad-hoc Networks (MANET). Attacks and threats of the most common kind can easily penetrate MANETs. Malware, APTs, and Distributed Denial of Service (DDoS) assaults all work together to make Internet services less reliable and less secure. Existing methods have been created to counter these assaults, but they either need more hardware, result in significant delivery delays, or fall short in other key areas like as energy consumption. This research therefore provides an intelligent agent system that can automatically choose and classify features to identify DDoS assaults. In this study, we provide an automated attack detector for MANETs based on a multilayer, (1D) convolutional neural network (CNN). Grey relational analysis classifiers are employed to screen attack levels in the classification layer because of their simple mathematical operation. The sunflower optimization technique is also used to fine-tune the classifier's weight. The research suggested a supervised feature classifier and fed the compressed data from an unsupervised auto encoder to it. In our experiment, conducted on the custom-generated dataset CICDDoS2018, the system outperformed state-of-the-art deep learning-based DDoS attack finding methods by a factor of 98%. Our suggested technique utilizes the freshest CICDDoS2018 dataset in combination with automated feature selection and classification to achieve state-of-the-art detection accuracy at a fraction of the processing time.

Keywords: Mobile Ad-hoc Networks; Convolutional neural network; Sunflower Optimization; Distributed Denial of Service; CICDDoS2019.

ARTICLE INFORMATION

Author(s): Dr. V. Gokula Krishnan, S. Hemamalini, Praneeth Cheraku, K. Hema Priya, Sangeetha Ganesan and Dr. R. Balamanigandan;

Received: 02/05/2023; **Accepted**: 19/05/2023; **Published**: 30/05/2023;
e-ISSN: 2347-470X;
Paper Id: IJEER 0205-01;
Citation: 10.37391/IJEER.110209
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-11/ijeer-110209.html

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

Ad-hoc networks have evolved in many ways due to the rapid development and growth in volume of wireless mobile computing technology that has spurred a revolution inside the computing industry [1-2]. Without the need for permanent infrastructure or centralized base stations, mobile ad hoc networks may quickly be assembled by direct communication between mobile wireless nodes within the network's radio coverage area [3]. With a MANET, the act of communicating between devices is simpler, and the network itself is unstable since it operates via an open media and is self-configured. This causes unpredictable and abrupt shifts in the network's architecture [4 and 5]. The backbone of a wireless network, routing protocols move data between nodes and determine the optimal path to complete a given task as quickly and efficiently as possible [6]. Additionally, there are routing protocols designed specifically for low-power wireless networks [7].

The ever-changing nature of MANETs makes them vulnerable to a wide range of security threats, making it difficult to design effective adaptive security solutions for them [8]. From this vantage point, intrusion detection systems based on anomalies assist safeguard networks from attackers [9]. There are a few hurdles that must be overcome [10] before outlier detection may be used in MANETs for intrusion detection to improve security and performance.

First, since there isn't a single, reliable supervisor node in MANETs, attack signatures need to be managed in a decentralized fashion [11].

1. There is more overhead because of the higher likelihood that routing tables will need to be generated and modified repeatedly due to the network's robustness and high degree of topological change. This requires more power and results in a greater number of packets being transmitted.
2. The lack of a clearly defined border in MANETs makes security a top priority [12 and 13]. Security can only be implemented through the use of a cooperative detection method for the detection and prevention of major assaults.
3. To counteract these evolving threats, we need to build and apply procedures that may be roughly categorized as proactive, reactive, or hybrid; this in turn necessitates the development of novel detection techniques. For resource-constrained networks, the goal should be to build more advanced protocols and lighter mechanisms that can deliver optimal output.
4. Fifth, the MANET's bandwidth is constrained since the mobile sensor devices that make up the network have limited processing capabilities and memory [14]. High bandwidth is needed for the exchange of dense traffic between nodes in a MANET anomaly detection system.
5. The limited battery life and power of MANET nodes necessitates regular or intermittent recharging, necessitating either a centralized or decentralized approach for achieving maximum quality-of-service. Threats to Intrusion Detection Systems (IDS) might arise from MANET's dispersed, low-resource environment. There are five components that must exist in a secure MANET. Lightweight techniques with less hardware and software needing reduced energy intake have to be implemented to provide
   i. availability,
   ii. secrecy,
   iii. authentication & authorization,
   iv. key management, and
   v. Non-repudiation [15].
6. When the IDS in MANETs are intended to be a lightweight mechanism, it can make mistakes during the training phase when arranging data and during attacks when pattern changes rapidly.

To perform multiclass classifications that can distinguish between normal and attack conditions with nonlinear separability, this study uses a fully connected layer informed by grey relation analysis (GRA) that is linked from the convolutional layer to the pooling layer. To further boost classification precision, a deep learning-based auto-encoder model selects the most relevant characteristics.

1.1 Organization of Paper

The remaining parts of the paper have the following layouts: The relevant literature is presented in Section 2, and the suggested perfect is described in outline form in Section 3. Consequences from the validation investigation are presented in Section 4. Section 5 then offerings its conclusion

2. RELATED WORK

With automated feature extraction and selection, Abu Bakar et al. [16] present an intelligent agent system to identify DDoS assaults. In our trial using the custom-generated dataset CICDDoS2019, the system outperformed the DDoS attack detection methods by a factor of 99.7. In this system, we also developed an apparatus that utilizes a mix of machine learning methods and sequential feature selection. When DDoS attack traffic was dynamically identified, the learning phase of the system picked the best attributes and rebuilt the DDoS detection agent. Our suggested technique achieves state-of-the-art detection accuracy while providing quicker dispensation than the existing standard by employing the latest.

Using a Gas Solubility Optimization (EHGSO), Ninu, S.B. *et al.* [17] suggested an efficient intrusion detection approach for MANET. In the preliminary stages of secure routing, the newly developed EHGSO algorithm is employed to choose the best possible paths. Energy, distance, neighbourhood quality, and connection quality are the fitness criteria that characterize this method. By fusing HGSO with EWMA (Exponential Weighted Moving Average), the proposed EHGSO achieves greater efficiency. The intrusion detection phase begins at the base station during the second phase, when the transmitted data packets are modified and the Knowledge discovery in databases (KDD) characteristics is extracted. The KDD characteristics are extracted, and then the data is augmented. Before conducting intrusion detection, the Deep Neuro Fuzzy Network is trained with the recommended EHGSO approach. When compared to other methods already in use, the suggested technique clearly performs better. Taking into account the metrics of energy, throughput, packet loss, jitter, (PDR), accuracy, and recall, the suggested technique achieves values of 95.877%, 0.950, and 0.924 in a no-attacks scenario.

To reliably anticipate the assigned label, Prashanth et al. [18] plan to use combined optimization and classification strategies. Pre-processing, feature extraction, optimization, and classification are the functional elements that make up this system. To begin, the input datasets undergo pre-processing, during which time the blanks are filled in and the duplicates are removed. Then, to further enhance classification accuracy, a collection of characteristics is chosen using the (PCA) method. Therefore, the Grey Wolf Optimisation (GWO) method is used to pick the best characteristics with the highest fitness value, simplifying the IDS process as a whole. After the results have been categorised, the (DCNN) method is used to forecast whether or not the results are malicious. During the analysis, we evaluated a number of performance measures, and we compared our findings to those of the most up-to-date, state-of-the-art models to ensure the accuracy of our conclusions.

Three distinct varieties of deep learning algorithms were combined into one by Elubeyd et al. [19]. Both theoretical analysis and empirical testing showed that our method obtained high accuracy rates on two separate datasets. Our work significantly advances the state of the art in SDN-based network security. The suggested technique might improve SDN security and shield networks from DoS and DDoS assaults. Given the growing prevalence of SDNs in today's network infrastructure, it's critical that they be safeguarded against attacks in order to preserve the reliability and accessibility of those resources. Abdel Hamid et al. [20] propose a solution for identifying black hole attacks by employing anomaly detection founded on a (SVM). The purpose of this detection system is to monitor network activity and spot any out-of-the-ordinary behaviour from individual nodes. Black hole assaults include nodes with peculiar behavioural traits that set them apart from average nodes. Our lightweight detection technology is able to successfully detect these features. An OMNET++ simulator is utilized to create traffic while under a black hole attack to test the efficacy of this approach. The discovered malicious node is used to categorize the traffic as malicious or benign. The suggested approach has been shown to identify black hole assaults with a high degree of accuracy.

In the network layer, the "Malicious Packet Dropping Attack" is investigated by Vijayalakshmi et al. [21]. A unique approach is offered using game theory to provide security against this assault. Secure communication among nodes that talk to one another to route traffic from source to journey's end is made possible thanks to the suggested system, which analyses the behaviour of neighbouring nodes and overcomes the drawbacks, such as false positives, of conventional IDS. The suggested approach has increased the ratio by 42% despite the presence of hostile nodes.

3. PROPOSED SYSTEM

In order to counteract dispersed assaults, the suggested methodology implements a DL agent. This agent functions as a network node, always monitoring the system and sending out notifications if any problems are detected. By coordinating judgments and modifying routing regulations, the agent is able to effectively identify and block malicious traffic. The agent's perceptual and cognitive modules provide it the ability to respond to and anticipate its environment. When malicious traffic is found, a stationary agent takes over control of the destination host, while other agents notify intermediate nodes about the bad traffic they've been tracking. In addition to monitoring high-volume IP traffic, these agents may leverage the data transfer rates between nodes to compile TTL, ACL, and packet labels. If an attack or admission block causes a failure, these agents may switch to backup routes and adjust router settings accordingly.

Source-end, (IPS) firewalls are the standard defence measures against DDoS assaults. While the third option is preferred by scientists, it comes with the problem of having massive resources to react rapidly upon detection. Once DDoS attackers get access to a system, they may rapidly ramp up their attack strength and claim the vast majority of the system's resources. Since researchers may now launch attacks without impersonating IPs and use simulations to test out intricate connections of database requests, it is difficult to rule out such interactions when determining whether questions are legitimate.

3.1 Feature Selection using DL based Auto Encoder

We employed feature compression and a comparison of unsupervised neural network feature selection auto encoders to feed into supervised DL classifiers.

3.1.1. Auto Encoder

In an auto encoder, the neural network is given the capacity to learn the pictures on its own, making it a form of unsupervised dimensionality reduction. The encoder and the decoder are the two primary mechanisms of any auto encoder. Input features are transformed into a latent vector, a space with less dimensions, and then returned to their original form by the decoder. In order to reduce the gap between input and output characteristics, a loss function is applied.

Table 1 details the auto encoder settings employed in this study, which used a sparse auto encoder representation. An attempt was made to reduce mistake and provide a flattened representation with the optimal score by encoding the input characteristics beneath this single hidden layer. A sparse penalty term is added to the auto encoder model, which tightens up the requirements for extracting the latent vector and improving feature learning to create the sparse auto encoder. The network employed the sigmoid activation function. A sparse penalty was added into the hidden layer neuron to decrease the activation function value. This sparsity may cause occasional accidental activation of the buried layer. It is possible to express the activation function as;

$$a = sig(Wx + b) \tag{1}$$

$Where: W \;=\; weight\ matrix. b \;=\; deviation\ vector.$

Table 1: Sparse auto encoder limits

Values	Parameters
3	Sparse penalty weight
0.1	Sparsity
200	No. of epochs
20^{-5}	Weight decay
Lbfgs	Optimization technique

The neuron activation purpose in layer can be signified as shadows:

$$p_j = \frac{1}{n}\sum_{i=1}^{n}\left[a_j x(i)\right] \tag{2}$$

As a kind of punishment, the (KL) divergence technique is employed. The formula for KL divergence is:

$$kl(p||p_j) = pln\frac{p}{p_j} + (1-p)ln\frac{1-p}{1-rho_j} \tag{3}$$

Kullback-Leibler (KL) gradually approaches 0 as it diverges from p as a result of the divergence. This network's loss value is denoted by the function C(w,b). Addition of the thin penalty term to the loss function is represented by the following equation.

$$C_{sparse} = C(w,b) + \beta \sum_{j=1}^{S_2} kl(p||p_j) \tag{4}$$

Where β is the weight of the thin penalty term and S2 is the neuron total in the interior layer [22].

3.2 Classification using GRA based DL Model

The GRA-based classifier uses the degree of similarity or dissimilarity between process variables to assign a label to each potential class, and it also offers data on the intensity of the grey connection to aid in prediction and decision-making. It uses a pattern recognition approach to complete the classification process, which eliminates the need for optimization and iterative calculations [23]. The classification layer of the multilayer fully connected network was where the GRA-based classifier was established. Other layers in the network included an input layer, a summation layer, and an output layer. In the GRA layer, we employed the grey levels, represented as Gaussian functions, to evaluate how similar a reference feature signal (the testing feature signal) was to a set of compared feature signals (the training feature signals).

$$x0 = [x_1(0), x_2(0), x_3(0), \dots, x_i(0), \dots, x_{100}(0)]$$

And $x_k = [x_1(k), x_2(k), x_3(k), \dots, x_i(k), \dots, x_{100}(k)]$,

$$k = 1, 2, 3, \dots, K,$$

Correspondingly. The output of the grey grade, *g(k)*, can be clear as shadows:

$$g(k) = exp\left(-\frac{1}{2}\left(\frac{ED(k)^2}{\sigma^2}\right)^2\right), k = 1,2,3,\dots,K \tag{5}$$

Where $ED(k)$ is the *(ED); K* is the sum of training feature signs, and *s* is the standard nonconformity, which can be signified as shadows:

$$ED(k) = \sqrt{\sum_{i=1}^{100}(\Delta d_i(k))^2}, d_i(k) = x_i(0) - x_i(k), i = 1,2,3,\dots,100, k = 1,2,3,\dots,K, \tag{6}$$

$$\sigma^2 = (\Delta d_{max} - \Delta d_{min})^2, \begin{cases} \Delta d_{min} = \underset{\forall i \forall k}{min}(\Delta d_i(k)) \\ \Delta d_{max} = \underset{\forall i \forall k}{max}(\Delta d_i(k)) \end{cases}, (\Delta d_{max} - \Delta d_{min}) \neq 0 \tag{7}$$

Where *d_max* and *d_min* are the deviation values, and *d_i (k)* is the change between a testing feature signal and a training feature signal; K training data are generated by ear signals, with *(1)* normal condition data, *(2)* outlier data, and *(3)* missing data, and the standard deviation, s, is calculated automatically using *d_max d_min.* $(Nor{:}\, 0.42 < CTR \leq 0.50)$, *(2)* mild/moderate attack$(0.50 < CTR \leq 0.60)$, and *(3)* severe attack $(CTR > 0.60)$. Then, classifier's production can be regularised as shadows:

$$y_i = \frac{\sum_{k=1}^{K} w_{kj} g(k)}{\sum_{k=1}^{K} g(k)} = \sum_{k=1}^{K} w_{kj} s_j, s_j = \frac{g(k)}{\sum_{k=1}^{K} g(k)}, \quad j = 1,2,\dots,m \tag{8}$$

$$\Upsilon_j = \begin{cases} 1, & y_j \geq 0.50 \\ 1, & y_j < 0.50 \end{cases} \tag{9}$$

Where *w_kj* represents the weighted values of the network between the GRA layer and the summing layer, output training data may determine these weights (as 1s and 0s); In a vector representation, the output weighted values are (1) Nor: [1,0,0], (2) Mild/Moderate attack: [0,1,0], and (3) Severe attack: [0,0,1] for the three possible severity levels of assault. At a 0.5 threshold, it is possible to rule with 100% certainty that an attack has happened (value 1) or that it has not (value 0). For the goal of optimizing the parameters of the suggested model, we provide the sunflower optimization strategy....

3.2.1 Basic sunflower optimization (SFO) procedure

One of the most recent meta-heuristics is the sunflower optimization (SFO) method presented by Gomes et al. (2019). The sunflower's unique behaviour in its hunt for the optimal orientation towards the sun inspired the development of the program. The SFO method simulates pollination by producing seeds at random while taking into account the shortest possible path between two flowers. Although millions of pollen gametes exist in each real bloom, the algorithm considers only a single created pollen gamete for each sunflower in order to get an optimization solution quickly. In addition to what has already been mentioned, the algorithm mimics the sunflower inverse square law radiation, which decreases in strength directly as a function of distance of the distance. The primary goal of the algorithm is to keep the plant as close to the sun as possible so that it can absorb its light and remain stable.

In addition, heat is lost proportionally to distance. This behaviour aids the algorithm in its exploration efforts, bringing it closer to the global answer (the sun). Below is a method for calculating the amount of heat (H) the plant has received.

$$H_i = \frac{P_s}{4\pi d_i^2} \tag{10}$$

Where *d* is the plant's distance from the optimal location at the moment and *Ps* is the power coming from the source.

Here is the formula for the mathematical model that describes how sunflowers face the sun.

$$\vec{D}_i = \frac{Z^* - Z_i}{\|Z^* - Z_i\|} \tag{11}$$

Where *Z** represents the optimal plantation and *Z* describes the existing plantation.

Following is a model for orienting sunflowers toward *S_i*, the direction of the sun.

$$S_i = \omega \times \|Z_i + Z_{i-1}\| \times P_i(\|Z_i + Z_{i-1}\|) \tag{12}$$

Where *P_i (X_i + X_(i-1)* is the likelihood of pollination for plant *i* and affects the plants' inertial motion.

Candidates nearer and further from the sun have distinct algorithm update processes. The algorithm takes fewer steps while moving closer to a candidate and larger steps when moving farther away. The following formula determines the greatest gain for the contestants.

$$S_{max} = \frac{\|Z_{max} - Z_{min}\|}{2 \times N_p} \tag{13}$$

Where, N_p labels the total sum of plants, and Z_{max} and Z_{min} stand for the extreme and the minimum limits.
Here is the updated precise formulation for the estate:

$$\vec{Z}_{i+1} = \vec{Z}_i + S_i \times \vec{D}_i \tag{14}$$

The SFO method first generates populations at random. After the optimal solution has been reached by calculation of the cost function, the procedure is done to move the plats into a more solar-friendly orientation.

3.2.2 Developed sunflower optimization (DSFO) process

Although SFO provides a number of benefits (Gomes et al., 2019), its early convergence on some issues is a major negative. In response to this criticism, we created a novel implementation of SFO for the optimization issue under consideration. The first innovation is the use of self-adaptive weighting to fine-tune the algorithms toward the optimal answer. A random value depending on the plantation keywords has been evaluated for updating the plants. In this scenario, the algorithm seeks to strike a balance between exploration and exploitation by beginning its search with a large divergence and narrowing its focus as it progresses. The revised form of this enhancement is as follows:

$$\vec{Z}_{i+1}^{new} = \begin{cases} \vec{Z}_{i+1} + \gamma \times S_i \times \vec{D}_i \times f(\vec{Z}_{i+1}), & rand > 0.5 \\ \vec{Z}_{i+1} + \gamma \times S_i \times \vec{D}_i \times f(\vec{Z}_{i+1}), & rand \leq 0.5 \end{cases} \tag{15}$$

Where,

$$\gamma = \begin{cases} \left(\frac{f(\vec{Z}_{i+1}^{best})}{f(\vec{Z}_{i+1}^{worst})} \right)^2, & if\ f(\vec{Z}_{i+1}^{worst}) \neq 0 \\ 1, & if\ f(\vec{Z}_{i+1}^{worst}) = 0 \end{cases} \tag{16}$$

Where, $f(\vec{Z}_{i+1}^{worst})$, and $f(\vec{Z}_{i+1}^{best})$ signify the function cost values for the nastiest and finest solutions for plantation, correspondingly.

This enhancement broadens the algorithm's search space, bringing better and worse answers closer together. The mechanism of the logistic map is used in this research to further enhance the system and prevent premature convergence. As a type of chaotic mechanism, the logistic map is frequently used to escape the "local optimum" in optimization problems. Pseudorandom values are used in the logistic map's calculations. The following revised equations were developed by applying this method to the total sum of plants:

$$N_{p+1}^{new} = N_p^{new} + \beta_i \times N_p^{new} \tag{17}$$

Where,

$$\beta_{i+1} = 4 \times (\beta_i - \beta_i^2) \tag{18}$$

Where _*i* is a number describing the *i*th chaotic iteration and 0 is the starting point _*i* characterizes a haphazard number between zero and one.

4. RESULTS AND DISCUSSION

We compare the three models with different structures to find in order to categorize network traffic, the detection system makes use of varying sample rates inside a regulated network environment. The CSE-CIC-IDS2018 datasets and local testbed traffic were utilized to run the experiment. Five virtual computers, each with four vCPUs and 4 GB of RAM, were employed in the experiment. False alarm rates were reduced by the intelligent detection system.

4.1 Description of the Benchmark Datasets

Researchers recommend using several data sets, to assess the success of their detection and prevention techniques. The problem is that these databases include old records. Both the locally-produced LOIC and HOIC datasets contained examples of these modern threats and DoS tools.

4.1.1 The CIC-DoS Dataset

DoS assaults at the application layer are the focus of the CIC-DoS dataset, which complements the ISCXIDS2012 track. The application layer was the source of eight DoS assaults [24]. Results are publicly obtainable at https://www.unb.ca/cic/datasets/dos-dataset.html (last visited January 20, 2021)) and include 4.6 GB of 24-hour network traffic. Tables 2 and 3 highlight, using separate data sets, the occurrences and tools related to CIC-DoS attacks. The default setting of attack traffic in slow http test, a tool used to simulate high-low-volume assaults, is 50 connections per attack. According to [24], this raises suspicions about assaults.

4.1.2 CSE-CIC-IDS2018 Dataset

This data set (CIC) is openly nearby at https://www.unb.ca/cic/datasets/ids-2018.html and was developed in collaboration with the (CSE) and the Canadian Cyber Security Institute (CCSI). The complete dataset contains information on seven different types of attacks, such as Heartbleed, Brute Force, Botnets, Web Attacks, DoS assaults, and DDoS attacks. There are 250 computers in the attacker's infrastructure and 620 workstations and 40 servers in the victim's network. There is a wealth of literature outlining the fundamentals of data analysis and related topics. The drive of this work was to detect DDoS and DoS-like attacks inside data. The instruments of attack include Slow HTTP Test, Slow http test, Hulk, LOIC, and HOIC.

Accuracy, sensitivity, was used to verify the proposed system's validation. Parameter analysis, as well as a qualitative comparison of the new method to the old, is described below.

4.2 Evaluation Parameters

Several parameters are examined in this part to validate the proposed system against existing methods. The estimate metrics are used to validate the functionality of the proposed system and provide context for both theoretical and practical developments. Included in this are the metrics that were developed from a shared perspective at the outset. Sensitivity, specificity, the f-measure, and accuracy are the estimation metrics. Below are the formulae used to calculate the spread for the aforementioned metrics.

$$Sensitivity = \frac{TP}{TP+FN} \times 100 \quad (19)$$

$$Specificity = \frac{TN}{TN+FP} \times 100 \quad (20)$$

$$F - Measure = \frac{(2 * Precision * Recall)}{(Precision + Recall)} \quad (21)$$

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (22)$$

In next section, the enactment of proposed system is analysed in relations of measure able and qualitative terms.

Table 2: Analysis of classifier without Auto-encoder (AE)

Classifiers	Sensitivity (%)	Specificity (%)	F-measure (%)	Accuracy (%)
DBN	73.90	84.23	79.78	80.25
RNN	75.53	85.98	86.05	82.35
CNN	77.01	87.54	83.32	86.47
CNN-DSFO	86.41	90	89.84	92.77

When the modes are tested with accuracy, the proposed model achieved 92.77%, CNN has 86.47%, RNN has 82.35% and DBN model achieved 80.25%. When the models are tested without AE, even the proposed model achieved poor performance, i.e., 90% of specificity, 89.84% of F-measure and 86.41% of sensitivity. The other existing techniques such as RNN, Sensitivity was from 73% to 77%, specificity from 84% to 87%, and F-measure from 79% to 83% for CNN and DBN, respectively.

Table 3: Analysis of classifier with Auto-encoder

Classifiers	Sensitivity (%)	Specificity (%)	F-measure (%)	Accuracy (%)
DBN	75.56	89.97	86.45	96.54
RNN	80.55	89.27	89.34	98.11
CNN	81.16	92.55	89.86	97.44
CNN-DSFO	93.42	98.97	91.65	98.85

When the feature selection technique is implemented for selecting the relevant features, the proposed model achieved nearly 93.42% of sensitivity, 98.97% of specificity, 91.65% of F-measure and 98.85% of accuracy. Not even the proposed model, the existing techniques are also achieved better performance. The reason for better performance is that the important features are used for classification of attacks. For instance, the existing models such as DBN, RNN and CNN achieved 75% to 81% of sensitivity, 89% to 92% of specificity, 86% to 89% of F-measure and 96% to 97% of accuracy. Figure 1 to 4 represents the graphical analysis of proposed model with existing techniques.

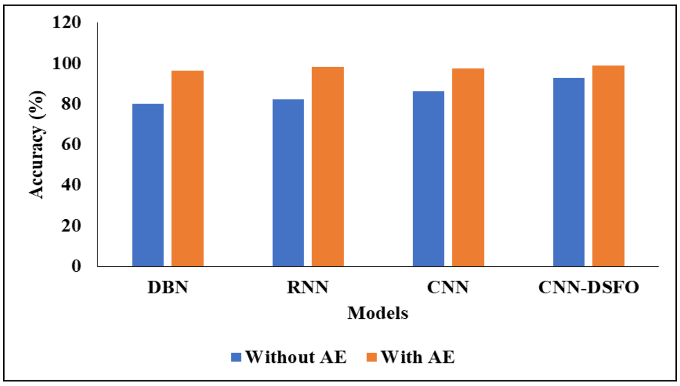

Figure 1: Accuracy Analysis

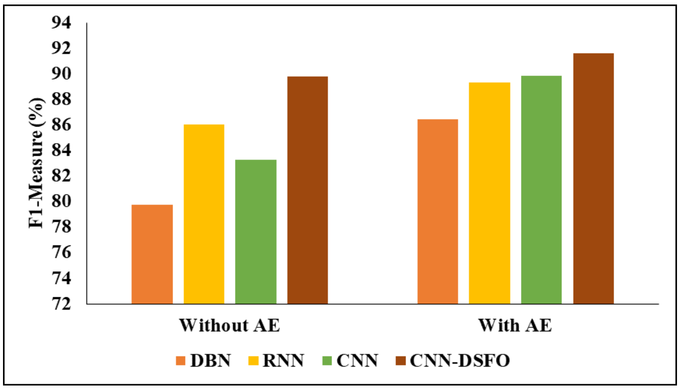

Figure 2: F-measure Analysis

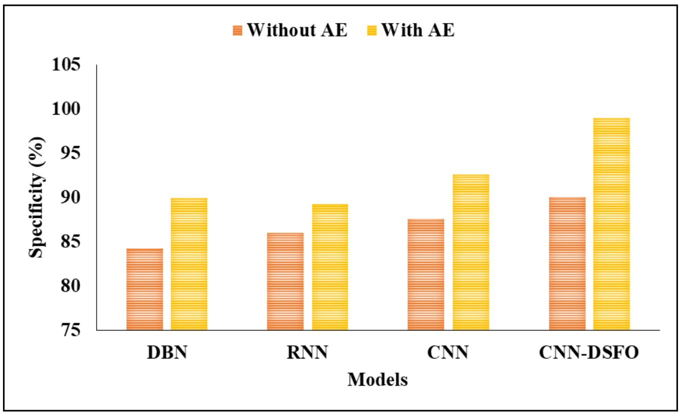

Figure 3: Specificity Comparison

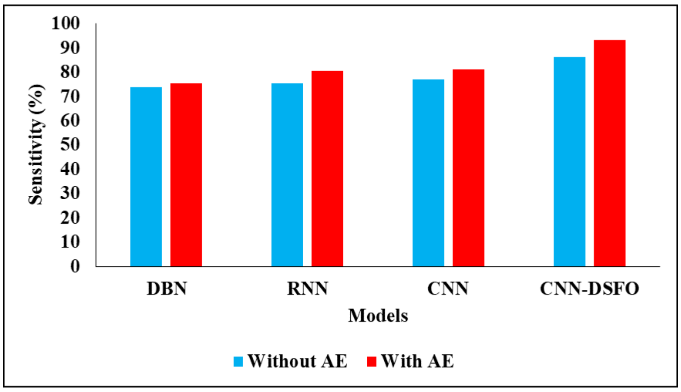

Figure 4: Sensitivity Analysis

5. CONCLUSION

This study investigates the use of deep learning procedures for DDoS detection and proposes a solution for intelligent DDoS detection agents. Up to 98% detection rates, reduced false alarm rates, and reduced calculation and transmission costs are all possible because to the suggested solution's usage of an effective adaptive feature selection technique (auto-encoder). The deep learning bots have been taught to monitor network activity and perform packet analysis in order to spot malicious activity. Since it is preferable to avoid problems in the first place, the recommended strategy puts an emphasis on pre-emptive defence. The research examines all possible assault types, methods, and defences. We found that the suggested method has the capacity to significantly guard against DDoS assaults, which validates the findings of our study. We do, however, recognize that there is scope for development and more study. This article presents a detailed analysis on the usage of three common deep learning algorithms to identify DDoS assaults, the proposed model achieved nearly 93.42% of sensitivity, 98.97% of specificity, 91.65% of F-measure and 98.85% of accuracy. Not even the proposed model, the existing techniques are also achieved better performance underlining the need of a proactive defence apparatus and laying the groundwork for future multi-directional research on the issue. The proposed technique may not be fool proof, but it does make a major advance in the fight against DDoS attacks.

REFERENCES

[1] Salunke, K. and Ragavendran, U., 2021. Shield techniques for application layer DDoS attack in MANET: a methodological review. Wireless Personal Communications, 120(4), pp.2773-2799.

[2] Kolandaisamy, R., Noor, R.M., Kolandaisamy, I., Ahmedy, I., Kiah, M.L.M., Tamil, M.E.M. and Nandy, T., 2021. A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET. Journal of Ambient Intelligence and Humanized Computing, 12, pp.6599-6612.

[3] Rajpoot, C.S., Bairwa, A.K. and Sharma, V.K., 2021. Mitigating the impact of DDoS attack on upsurge network performance in MANET. In Proceedings of International Conference on Communication and Computational Technologies: ICCCT-2019 (pp. 153-164). Springer Singapore.

[4] DHINDSA, K.S. and SINGH, K., 2021. Entropy-based DDoS Attack Detection in Cluster-based Mobile Ad Hoc Networks. Adhoc & Sensor Wireless Networks, 49.

[5] Kurian, S. and Ramasamy, L., 2021. Securing service discovery from denial of service attack in mobile ad hoc network (MANET). International Journal of Computer Networks and Applications, 8(5), pp.619-633.

[6] Revathi, M., Ramalingam, V.V. and Amutha, B., 2021. A machine learning based detection and mitigation of the DDOS attack by using SDN controller framework. Wireless Personal Communications, pp.1-25.

[7] Mahajan, R. and Zafar, S., 2021. DDoS attacks impact on data transfer in IOT-MANET-based E-Healthcare for Tackling COVID-19. In Data Analytics and Management: Proceedings of ICDAM (pp. 301-309). Springer Singapore.

[8] Yungaicela-Naula, N.M., Vargas-Rosales, C. and Perez-Diaz, J.A., 2021. SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning. IEEE Access, 9, pp.108495-108512.

[9] Mittal, M., Kumar, K. and Behal, S., 2022. Deep learning approaches for detecting DDoS attacks: A systematic review. Soft Computing, pp.1-37.

[10] Bhayo, J., Jafaq, R., Ahmed, A., Hameed, S. and Shah, S.A., 2021. A time-efficient approach toward DDoS attack detection in IoT network using SDN. IEEE Internet of Things Journal, 9(5), pp.3612-3630.

[11] Hadi, R.M., Abdullah, S.H. and Abedi, W.M.S., 2022. Proposed neural intrusion detection system to detect denial of service attacks in MANETs. Periodicals of Engineering and Natural Sciences, 10(3), pp.70-78.

[12] Agarwal, A., Khari, M. and Singh, R., 2021. Detection of DDOS attack using deep learning model in cloud storage application. Wireless Personal Communications, pp.1-21.

[13] Talukdar, M.I., Hassan, R., Hossen, M.S., Ahmad, K., Qamar, F. and Ahmed, A.S., 2021. Performance improvements of AODV by black hole attack detection using IDS and digital signature. Wireless Communications and Mobile Computing, 2021, pp.1-13.

[14] Alsumayt, A., 2022, April. Detect Denial of Service Attack (DoS) in MANETs Partition Scenario Using Puzzle Map Method. In Journal of Physics: Conference Series (Vol. 2224, No. 1, p. 012081). IOP Publishing.

[15] Lin, H., Wu, C. and Masdari, M., 2022. A comprehensive survey of network traffic anomalies and DDoS attacks detection schemes using fuzzy techniques. Computers and Electrical Engineering, 104, p.108466.

[16] Abu Bakar, R., Huang, X., Javed, M.S., Hussain, S. and Majeed, M.F., 2023. An Intelligent Agent-Based Detection System for DDoS Attacks Using Automatic Feature Extraction and Selection. Sensors, 23(6), p.3333.

[17] Ninu, S.B., 2023. An intrusion detection system using Exponential Henry Gas Solubility Optimization based Deep Neuro Fuzzy Network in MANET. Engineering Applications of Artificial Intelligence, 123, p.105969.

[18] Prashanth, S.K., Iqbal, H. and Illuri, B., 2023. An Enhanced Grey Wolf Optimisation–Deterministic Convolutional Neural Network (GWO–DCNN) Model-Based IDS in MANET. Journal of Information & Knowledge Management, p.2350010.

[19] Elubeyd, H. and Yiltas-Kaplan, D., 2023. Hybrid Deep Learning Approach for Automatic Dos/DDoS Attacks Detection in Software-Defined Networks. Applied Sciences, 13(6), p.3828.

[20] Abdelhamid, A., Elsayed, M.S., Jurcut, A.D. and Azer, M.A., 2023. A Lightweight Anomaly Detection System for Black Hole Attack. Electronics, 12(6), p.1294.

[21] Vijayalakshmi, S., Bose, S., Logeswari, G. and Anitha, T., 2023. Hybrid defense mechanism against malicious packet dropping attack for MANET using game theory. Cyber Security and Applications, 1, p.100011.

[22] Wroge, T.J.; Özkanca, Y.; Demiroglu, C.; Si, D.; Atkins, D.C.; Ghomi, R.H. Parkinson's disease diagnosis using machine learning and voice. In Proceedings of the 2018 IEEE Signal Processing in Medicine and Biology Symposium (SPMB), IEEE, Philadelphia, PA, USA, 1 December 2018.

[23] Lin, C.-H.; Wu, J.-X.; Li, C.-M.; Chen, P.-Y.; Pai, N.-S.; Kuo, Y.-C. Enhancement of Chest X-ray Images to Improve Screening Accuracy Rate Using Iterated Function System and Multilayer Fractional-Order Machine Learning Classifier. IEEE Photon. J. 2020, 12, 1–18.

[24] Kasongo, S.M. A Deep Learning Technique for Intrusion Detection System Using a Recurrent Neural Networks Based Framework. Comput. Commun. 2023, 199, 113–125.