JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DISTRIBUTED DENIAL OF SERVICE ATTACK DETECTION USING MACHINE LEARNING FOR INTERNET OF THINGS

Pravin Tukaram Zhunjare[1], Prof. Lalita B. Randive[2],
[1]M.Tech Scholar, [2]Assistant Professor ,
[1, 2,]Department of Computer Science and Engineering,
[1,2]Marathwada Institute of Technology, Aurangabad, M.H., INDIA
[1,2] Dr. Babasaheb Ambedkar Technological University Lonere, Raigad, M.H., INDIA

Abstract : In this research work discuss on the nature of the threats posed by Distributed Denial of Service (DDoS) attacks on large networks, such as the Internet, demands effective detection and response methods. These methods must be deployed not only at the edge but also at the core of the network. This paper presents methods to identify DDoS attacks by computing entropy and frequency-sorted distributions of selected packet attributes. The DDoS attacks show anomalies in the characteristics of the selected packet attributes. The detection accuracy and performance are analyzed using live traffic traces from a variety of network environments ranging from points in the core of the Internet to those inside an edge network. The results indicate that these methods can be effective against current attacks and suggest directions for improving detection of more stealthy attacks. We also describe our detection-response prototype and how the detectors can be extended to make effective response decisions.

Keywords— *Distributed denial of service (DDoS), Attack Detection, Machine Learning, Neural Network, ANN Approach, MATLAB, 5G Network.*

I. INTRODUCTION

1.1 Background Distributed Denial of Service (DDoS)

Denial of service (DoS) attacks disrupt the availability of resources and services on the Internet. DoS attacks sometimes include sending an overwhelming number of communication requests to the victim's system, which prevents it from responding to legitimate traffic. This is a standard method of causing interruptions in service. The idea seems fine in theory, but it may be exploited in a distributed denial of service attack (DDoS) to interrupt the victim's service by sending these requests from a huge number of compromised computers throughout the globe. These seemingly valid queries might knock a system down because they use up resources like memory and bandwidth. DDoS attacks are commonplace and happen every day. Twitter and Facebook, two of the most popular websites, were not immune to the effect it had on their users. [10][103] The New York Stock Exchange, NASDAQ, the White House, the Federal Trade Commission, the Treasury, the Washington Post, and many more were all victims of distributed denial of service assaults. Over time, we've seen a rise in both attack traffic and overall threats

1.2 Classification of DDoS

DDoS assaults are categorised based on their level of automation, the weaknesses they exploit, the pace at which they are launched, the source addresses they use, the spoofing techniques they use, the types of victims they target, and their longevity. This thesis investigates DDoS assaults using High-Rate Flooding (HRF) on networks and computers. It uses a valid connection to carry out the assault. It requires fewer connections to initiate the assault.

- Both the volume of data and the amount of bandwidth used are very modest during a slow DoS attack. Normal defences will be unable to detect it. Several techniques [8,9] have been developed for spotting sluggish DoS attacks. SDN and machine learning based techniques have already been used to identify slow DoS assaults [12][102].
- In this research, we present a deep learning and flow-based slow DoS classifier. This article introduces a novel approach to the detection of sluggish HTTP DoS by using deep neural network classification to flow data. The advantages of the proposed method over host-based delayed DoS attack detection are as follows.

A network gateway may collect and evaluate traffic flow information to identify and stop slow DoS assaults before they reach their intended target

- The slow DoS classifier may be used on any webserver without any modifications to the server's software, operating system, or host. Citizen services, cloud services, banking, and financial services are only a few examples of the rising popularity of web-based services in the modern service sector.
- The effects of slow DDoS assaults on web servers in such situations might be catastrophic. Because of its emphasis on online applications, the proposed technique may be used to detect and avoid sluggish HTTP DoS in such situations. Traffic

characteristics such source IP address, source port, and destination port enable a powerful quantitative evaluation to differentiate regular traffic from assault and spike of lawful access[101]. This strategy was selected because it is the most effective way to accomplish the goal of the thesis. The arrival of traffic is very unpredictable and is mostly dependent on its originating IP address. An approach to computing the entropy of the originating IP address is also covered in this chapter. In contrast to the lack of attack traffic traces, the Centre for Applied Internet Data Analysis (CAIDA) dataset has a wealth of useful information. The research's practical components relied on real-time traffic traces collected from the web server of the Institute of Engineering (IOE).

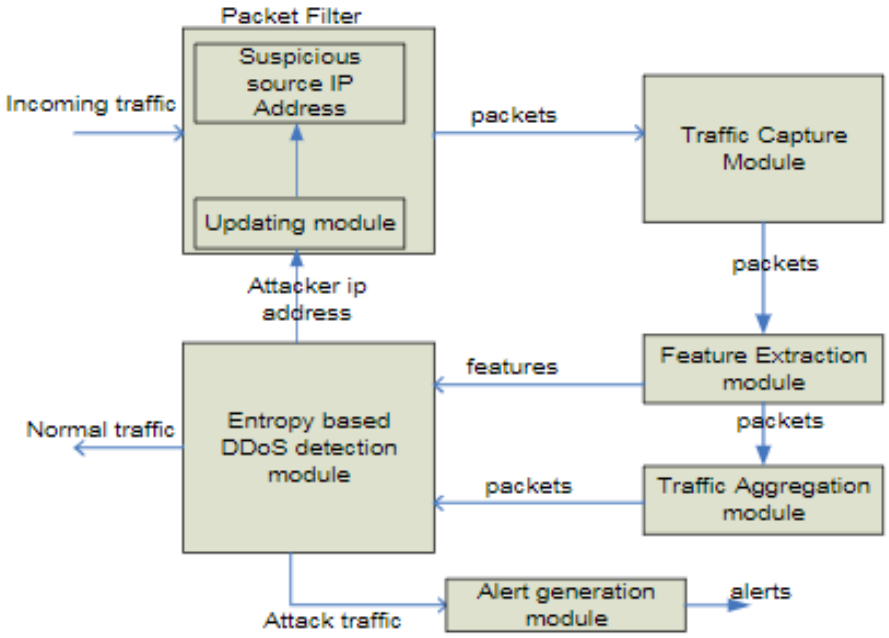


Fig.1.1: Block Diagram of DDoS detection System

II. LITERATURE SURVEY

At present times, the user wants faster data transmission speed and secures services. 5G NR promise to deliver all the basic as well as advanced facilities in contrast to prior. This technology allows users to high-definition and volume data within a second. 5G Technology 5G can handle larger traffic to cover the massive demand of the devices. 5G NR uses mm Wave, tiny cells, massive MIMO, beam forming, and full-duplex to achieve this goal. But these technologies are still in their early stages and haven't been independently tested. **Sura Abdulmunem Mohammed Al-Juboori et.al. (2023) -** Man-in-the-middle (MTM) and denial of service (DoS) attacks are two types of network assaults that let multiple attackers access and steal crucial data from physically linked devices in any network. This study obtained relevant datasets for MTM and DoS attacks from the Kaggle website and employed a number of machine learning algorithms to avoid these attacks and safeguard the devices. After obtaining the dataset, this research applied preprocessing techniques like fill the missing values, because this dataset contains a lot of null values. Then, we employed decision trees (DT), eXtreme gradient boosting (XGBoost), gradient boosting (GB), and random forest (RF) as machine learning techniques to identify these threats. Precision, accuracy, recall, and f1-score are only a few of the classification measures used to evaluate the algorithms' performance. In both datasets, the research produced the following findings: I All algorithms have the same performance in detecting MTM attacks, which exceeds 99% across all metrics; and ii) All algorithms have the same performance in detecting DoS attacks, which exceeds 97% across all metrics. Findings demonstrated how successfully these algorithms can identify MTM and DoS assaults, leading us to leverage their efficacy in defending devices against these threats [01]. Mustafa S. Ibrahim **Alsumaidaie et.al. (2023) -** Distributed Denial of Service (DDoS) assaults have become more common and sophisticated due to the quick development of 5G networks, intelligent devices, and the Internet of Things (IoT), which presents serious obstacles to cyber security. The goal of this research is to provide a reliable technique for identifying and averting DDoS attacks, protecting communication networks from these kinds of risks. To improve detection accuracy, the suggested "Intelligent Distributed Denial of Service Attacks Detection (IDDOSAD) Approach" combines ensemble learning with supervised machine learning techniques such as Random Forests, Decision Trees, K-Nearest Neighbour, XGBoost, and Support Vector Machine. The steps involved in developing a model are gathering data, pre-processing it, dividing it into training and testing sets, choosing prediction models, and assessing how well they work. The suggested method showed encouraging results when tested on a dataset of 11,423 occurrences, with accuracy for the time series dataset ranging from 92% to 100%. To sum up, the suggested method reliably identifies and counteracts DDoS assaults, providing a safeguard for communication networks against this expanding cybersecurity risk [02]. **Marian Gusatu*et.al.* (2022):-** A 5G-enabling technology called Multi-access Edge Computing (MEC) seeks to deploy cloud computing capabilities closer to the end users. In the context of 5G MEC, this article focuses on mitigating Distributed Denial-of-Service (DDoS) assaults and offers solutions that incorporate the virtualized environment and the MEC architecture's management entities. The suggested fixes, which are a continuation of the research done in, are meant to lessen the possibility that DDoS assaults may disrupt genuine traffic. As an upgrade over the prior work, our study supports the notion of employing a network flow collector that forwards the data to an artificial intelligence-based anomaly detection system and helps to reroute abnormalities that are discovered for isolation to a different virtual machine. This virtual machine uses deep packet inspection tools to analyze the traffic and provides services until the final verdict. By separating the bad behavior, we make it less likely that it will spread to the virtual machine that serves

normal customers. The MEC architecture's administration entities allow us to create and destroy virtual machines and change various configurations. Hence, If an attack causes the computer that is evaluating the isolated traffic to crash, it won't affect the services for real users [03]. **Yea-Sul Kim et.al. (2022):-** Building more expansive, low-latency Internet of Things (IoT) ecosystems is the ultimate goal of the next 5G cellular networks. Insecure IoT devices may be the source of distributed denial of service (DDoS) attacks against 5G phone carriers at the Tbps level. Thus, in 5G networks, the use of machine learning (ML) technologies for autonomous network intrusion detection is becoming more popular. We expect that machine learning-based DDoS attack monitoring in a 5G network will be very quick. Because of this, it is feasible to make use of a showcase procedure that may discover characteristics crucial for learning in big datasets while simultaneously decreasing computing complexity and increasing speed. Wired Internet teaching materials are the focus of most contemporary machine learning (ML) DDoS assault detection tools. Furthermore, not enough research has been done on feature engineering for 5G traffic. As a response, our survey involved experimentation with feature selection to hasten the analysis and detection of increased DDoS assaults in real time. It's important to desire an efficient feature selection for both training and detection based on machine learning in a 5G core network. Workplace setting. The experiment's findings demonstrated that applying the feature selection procedure preserved and enhanced performance. Specifically, the difference in temporal complexity increased dramatically with dataset size. Tests show that the feature selection method may be used to quickly identify widespread DDoS attacks on 5G core networks. This highlights how crucial the feature selection procedure is for eliminating distracting characteristics prior to training and detection. Since this study employed machine learning to look at criteria for DDoS attacks on 5G networks, it should help increase the effectiveness of automated detection technologies for detecting network activity going through the 5G core with low delay [04]. **Mahmood A. Al-Shareeda et.al., (2022):-** Traffic efficiency and safety are highly valued by both the public and private transportation sectors. 5G-enabled automobile networks may wirelessly communicate data with one another to help drivers and passengers. In 5G-enabled vehicular networks, privacy and security are considered issues as the vehicle transmits traffic status data. To satisfy these requirements, a plethora of privacy-preserving and protection techniques have been created. Since these techniques need for complex elliptic curve and bilinear pair cryptography procedures, the performance efficiency in terms of communication and computing costs is insufficient, which gives rise to DoS attacks. In order to address this problem, this paper suggests a technique for 5G-enabled car networks called Modular Square Root-based Defeat of Service Attacks (MSR-DoS). Our MSR-DoS technology ensures source authenticity, message integrity, pseudonym privacy, cannot be connected, is traceable, and may be revoked when used on vehicle networks. Burrows-Abadi-Needham (BAN) logic demonstrates the safety of our work. The performance research and comparison show that the MSR-DoS system has lower communication and computation expenses than government work. The suggested MSR-DoS technique reduces the computational complexity of signing and verifying a message by 99.80% and 98.55%, respectively [05]. **Hao Wang et.al., (2022):-** Ultra dense cellular networks are fast emerging as one of the primary features of 5G cellular networks, thanks to millimetre Wave technology.In an edge computing scenario, load balancing across edge nodes is a smart concept if you want to slow down a DDoS attack.Congestion in the multiuser and multiage server models has, however, received less attention in the majority of previous research. It appears that users of the M/M/1 model are unaware of how scheduling techniques impact the task arrival process's Markov property. In this publication, the G/M/1 model is first used to edge server job scheduling in order to enhance load balancing amongst edge servers, with the goal of guaranteeing the quality of experience (QoE) for users. The MAB algorithm architecture has metrics designed to quantify its degree of homeostasis. Considerations include how many users are allocated to each edge node and how each edge node handles certain jobs. On a real-world dataset, we experimentally assessed its performance against two baseline techniques and three state-of-the-art approaches. Additionally, the experimental findings support this method's efficacy. [06].

III. PROPOSED METHOD

R A computer model based on the structure and functions of biological neural networks is known as an Artificial Neuron Network (ANN). In terms of Computer Science, it functions as an artificial human nervous system, receiving, processing, as well as transmitting data[99][100].A neural network is composed of three layers:—Input Layer of Input (All the inputs are fed in the model through this layer).

Layers that are not Visible, It's possible that more than one hidden state is employed to process the information received from the input layers.

Layer of output (The data after processing is made available at the output layer)

Here's how these layers are put together:

Proposed Training of D-DoS attack detection Bayesian Regularization Algorithm

The Bayesian regularization learning method and BPNNs are neural networks that use back propagation to learn are discussed in this section. Demuth et al. [33] provides a more in-depth explanation. Improved generalization and minimum over-fitting of the training networks are achieved using a Bayesian regularization back propagation neural network. Neural networks may be trained using D, an input and target vector pair training data set for the network model.

$$D = \{(u_{1,}z_{o1}), (u_{2,}z), \ldots, (u_{nt,}Z_{ont})\}$$

The error e is calculated for every key (u) toward the system based on the difference between the goal output and the projected output. It is necessary to use a quantitative metric to assess the network's performance, i.e. how well it is able to match the test data. This metric is known as the network performance index, and it is used to improve the characteristics of the network. The sum of squared errors (SSE) governs the standard performance index F():

Training algorithm Using Bayesian Regularization Algorithm

$$1.\ F(\overline{w}) = E_D = \sum_{i=1}^{nt}(ei)2 = \sum_{i=1}^{nt}(z_{oi} - a_{oi})T(z_{oi} - a_{oi})$$

2. $F(\bar{w}) = \mu\bar{w}^{T}\bar{w} + vE_D = \mu E_w + vE_{D,}$

V is the regularization parameter and indicates the sum of SSW.

3. $P(\bar{w}|D, \mu, v, M_N) = \frac{P(D|w,v,M_N)\ P(w|\mu M_N)}{P\ (D\backslash\mu,V,M_N)}$

4. $P\ (D|\bar{w}, \mu, v, M_N) = \frac{\exp\ (-vE_D)}{Z_D(v)}$

Where $Z_D = (\pi/v)\ Q/2,$

5.$Q = n_t \times N^{n1},$

Prior to prior probability density, assuming a Gaussian distribution for the weights of a network, $P\ (\bar{w}|\mu, M_N)$is given as:

6. $P(\bar{w}|\mu, M_N) = \frac{\exp(-\mu E_w)}{Z_w(\mu)}$

Where $Z_w = (\pi/\alpha)K/2$

7. $P(\bar{w}|D, \mu, v, M_N) = \frac{\exp(-\mu E_w - vE_D)}{Z_F(\mu,v)} = \frac{\exp(-F(w))}{Z_F(\mu,v)},$

At the point when$Z_F(\mu, v) = Z_D(v)Z_w(\mu)$ the normalizing factor is a constant.

8. $P(\mu, v|D, M_N) = \frac{P(D|\mu,v,M_N)\ P(\mu,v|M_N)}{P(D|M_N)}$

9. $\mu^* = \frac{\gamma}{2E_w(\bar{w}^*)}$ and $v^* = \frac{Q-\gamma}{2E_D\bar{w}^*)}$

10. $\gamma = K - \mu^* tr(H^*)^{-1}$, for $0 \leq \gamma \leq K,$

11. $H^* \approx J^T J,$

$z_F(\mu, v)$ shows that

12. $Z_F(\mu, v) \approx (2\pi)^{\frac{K}{2}}(\det(H^*))^{-\frac{1}{2}}\exp(-F(\bar{w}^*))$

13. $\overline{w}^{k+1} = \bar{w}^k - [J^T J + \prec I]^{-1} J^T e,$

$J^T e$ is the error gradient.

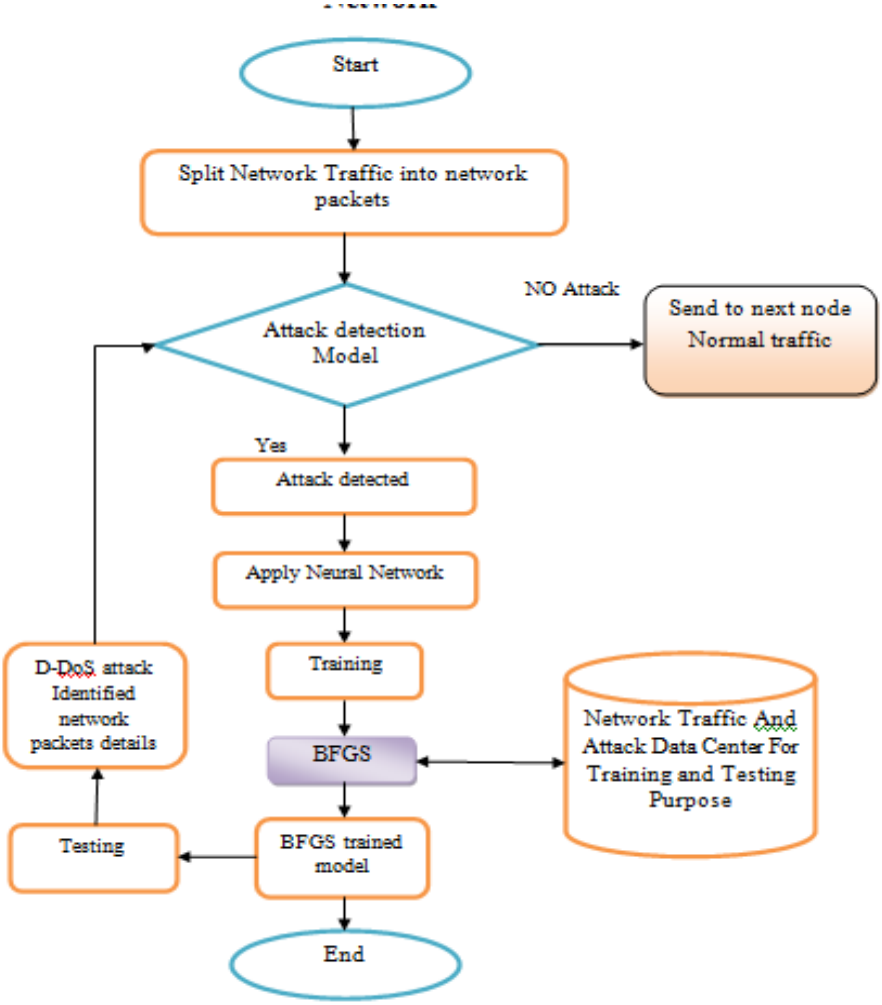


Fig. 3.1: Flow chart proposed model DDoS

IV. SIMULATION AND RESULT

The specifics of our planned research's execution and design are laid forth here. Through our research, we've learned that MATLAB 2020 is a popular tool for carrying out the techniques we propose. While conducting our experiments, we make use of the well recognised DDoS data set (Canadian Institute of Cyber security (CICIDS2017)) and the MATLAB 2020b code environment. The first part of this chapter provides an overview of the MATLAB environment; the second defines the CICIDS2017information A set that will be used in the implementations; and the third provides an inventory of the tables, snapshots and graphs that will be important to the success of the proposed task.

Data set

Intrusion detection assessment dataset from the Canadian Institute for Cyber Security (CICIDS2017) [18] is used for design training and evaluation. The study details several dangers, including DDoS attacks and botnet operations. In this research, we developed a classification model using the DoS data set. The CICIDS 2017 dataset is available in comma-separated value (.CSV) format, and each flow record has 84 variables. Each variable's data is described in great detail. Our classification relies on flow data stripped of potentially misleading information like flow ID, date, and source/destination IP addresses. This led to the selection of 80 characteristics representing the whole dataset for classification. The flow records, excluding those pertaining to the benign traffic, are designated as "Slowloris," "Slowhttptest," "Hulk," and "Begin" based on the tools used. There are five unique integer values between 1 and 5 that represent the "Benign," "Slowloris," "SlowHTTP," and "Hulk" flows, respectively.

In this section discus the different simulation outcomes of different proposed training methods. Algorithm Feed Forward of Bayesian regularization (FF-BR)

Feed forward is the reverse exercise of feedback. It's the process of replacing positive or negative feedback with future-oriented solutions. In simple terms, it means focusing on the future instead of the past. The experiment using a neural network (NN) is shown in fig. 4.1 below. This method takes in a total of 30 input features. Apply Bayesian regularisation through conjugate gradient for training. The training duration was thirteen seconds, and the mean square error was recorded at twenty-six and twenty-seven. 30 is the epoch number.

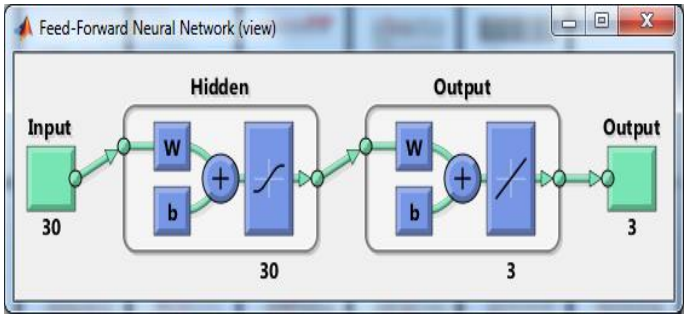


Fig. 4.1 Bayesian regularization based Feed Forward Network

In the below table shows the different input parameters for Bayesian regularization , also shown various trained result and outcomes of proposed Bayesian regularization model .

Table I : Training Input Parameters of proposed feed forward Network Using Bayesian regularization Algorithm (FFN -BR) and Training Input Parameters of proposed feed forward Network Using Bayesian regularization Algorithm (FFN -BR)

Parameters Name	Inputs of Parameter
Data Division	Random
Network Type	Feed Forward Network
Training	Bayesian regularization
Performance	Mean square Error

Parameters Name	**Inputs of Parameter**	**Training outputs**
Number of Epochs	0-30	30 iterations
Time	11 min 33 second	11 min 33 second
Performance	2.38	0.0148
Gradient	5.00	0.0288
Effective Parameters	1.0200	947
Sum Squared Parameter	127	283

In the below figures 4.2 shows the training Output of proposed Feed Forward Neural Network with Bayesian regularization. Figure 4.4 demonstrate the training outcomes of proposed method in which shows the type of network, data division, training and performance and also discuss the training input parameters and training expected outcome such as number of epochs range 0-30, Time consumed in the training processing of proposed method, Performance analysis of proposed method, optimized Gradient valued of proposed trained model output and Step Size of proposed outcomes of the method. Proposed trained model output and Step Size of proposed outcomes of the method.

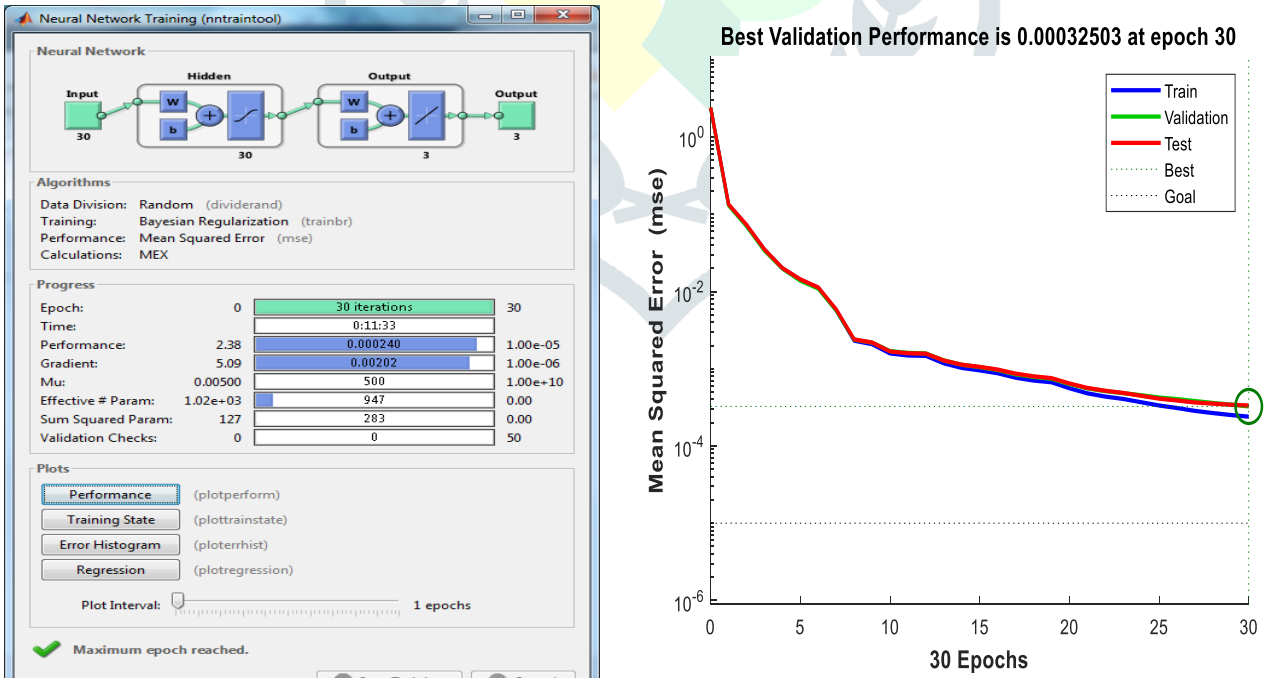


Fig. 4.2 Training of proposed Bayesian regularization with Feed Forward and Cascaded Feed Forward and Shows the Training Outcome of Proposed Bayesian Regularization in Feed Forward Network

In the below figure 4.3 shows the gradient value of proposed Bayesian Regularization outputs, gradient value of 0.002153 at 30 iterations , total number of parameters are analyzed in 946.5 , similar that sum squared parameters are analyzed 282 in the

analysis. These parameters are analysis in the training process once training process is completed no need again test, theses parameters are stored as a optimum results. When perform testing use these parameters directly.

Table II Shows the Resultant Parameters and Parameters

Parameter Name	Simulated Resultant value	**Result Parameters**	**Outcomes**
Accuracy (Acc)	99.8557	Accuracy	99.9038
True Positive (tp)	318 277 97	precision	99.8955
False Negative (fn)	0 1 0	Selectivity	99.8955
False Positive (fp)	1 0 0	Sensitivity	99.8801
True Negative (tn)	374 415 596	Specificity	66.6734
		Time Complexity	11 min. 33 second

Algorithm Cascaded Forward of Bayesian regularization (CF-BR)
Cascade-forward neural network is a class of neural network which is similar to feed-forward networks, but include a connection from the input and every previous layer to following layers. In a network which has three layers, the output layer is also connected directly with the input layer beside with hidden layer. In the below figure 4.9 shows the training of cascaded forward network. In the training the input parameters are -

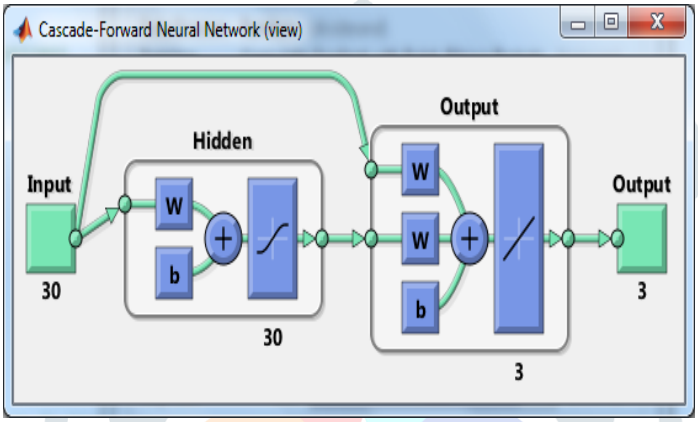
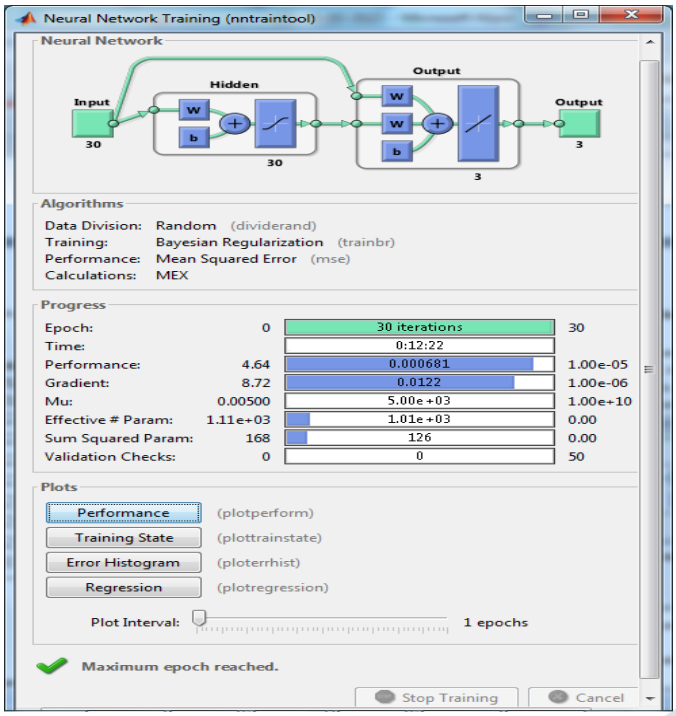


Fig. 4.3 Shows the Proposed based Bayesian regularization Cascaded Forward Neural Network (NN)

In the below table shows the input parameters for the training of proposed Bayesian regularization method for cascaded forward network. For the training of proposed method use random data division. For the measurement of training use mean square error (MSE).Training Input Parameters of Proposed Cascaded Forward Network Using Bayesian regularization Algorithm (Bayesian regularization -CFF)

In the above table shows the training outcomes of proposed Bayesian regularization method. It is observe that the proposed method taking 12 min 22 sec to simulation of training process of 30 iteration or epochs. Performance of Bayesian regularization is 4.64 that is simulated 0.000681. Gradient value of proposed method is 8.72 that better as compare to previous methods.
In the below figures 4.4 shows the training Output of proposed cascaded forward Neural Network with Bayesian regularization. Figure 4.10 demonstrate the training outcomes of proposed method in which shows the type of network, data division, training and performance and also discuss the training input parameters and training expected outcome such as number of epochs range 0-30, Time consumed in the training processing of proposed method, Performance analysis of proposed method, optimized Gradient valued of proposed trained model output and Sum squared pram of proposed outcomes of the method. In the above figure 4.11 shows the validation of proposed Bayesian Regularization for cascaded neural network. For the measurement of efficient of proposed method mean square error. In this graph horizontal access shows the number of iteration and vertical axis shows the calculation of mean square error on log graph.

In the below figure 4.4 shows the gradient value of proposed Bayesian Regularization outputs, gradient value of 0.012179 at 30 iterations , total number of parameters are analyzed in 1011.45 , similar that sum squared parameters are analyzed 126.4214 in the analysis. These parameters are analysis in the training process once training process is completed no need again test, theses parameters are stored as a optimum results. When perform testing use these parameters directly



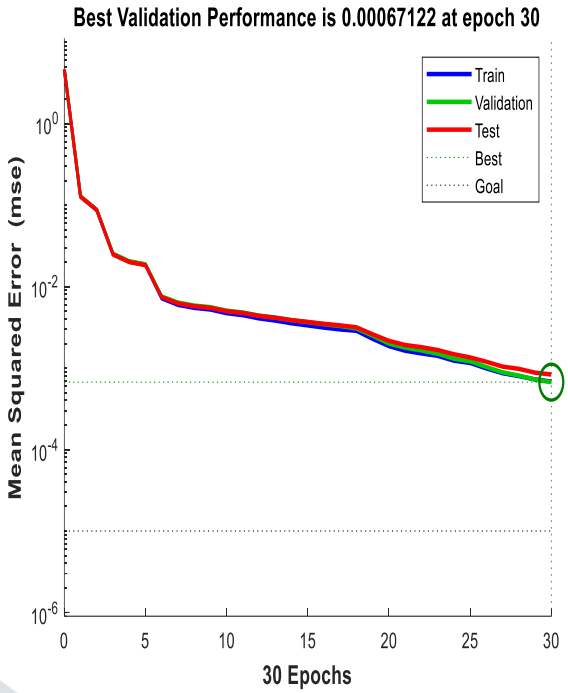


Fig. 4.4: Shows Bayesian Regularization of training of cascaded forward method and Shows the Validation outcome of proposed for Bayesian Regularization cascaded forward method

Table III : Shows Comparison of Proposed Cascaded Forward Network and Feed Forward Network Using Bayesian Regularization Algorithm

S. No.	Cascaded Forward Network		Feed Forward Network	
01	Selectivity	99.8955	Selectivity	99.8955
02	Sensitivity	99.8801	Sensitivity	99.8801
03	Precision	99.8955	Precision	99.8955
04	Accuracy	99.9038	Accuracy	99.9038
05	Complexity(Time)	12 min 22second	Complexity(Time)	11 min 33 second

In the above table shows the comparison of proposed Bayesian Regularization (BR) algorithm with two different network cascade forward network and feed forward network..

V. CONCLUSION

DDoS (Distributed Denial of Service) attacks on 5G networks can cause significant disruptions and can potentially bring down critical services. In this context, it is important to understand the impact of such attacks on 5G networks and take necessary steps to mitigate them. One of the primary challenges with 5G networks is their high reliance on software-defined networking (SDN) and network function virtualization (NFV) technologies. These technologies make the network more agile and flexible but also increase its attack surface. DDoS attacks can exploit vulnerabilities in these technologies to bring down the network.
To prevent DDoS attacks on 5G networks, various strategies can be implemented, including traffic filtering, access control, and behavioral analysis. It is also crucial to maintain up-to-date security patches, monitor network traffic for anomalies, and implement effective response and recovery mechanisms.

REFERENCES

[1] Sura Abdulmunem Mohammed Al-Juboori, Firas Hazzaa1 , Zinah Sattar Jabbar, Sinan Salih2 , Hassan Muwafaq Gheni "Man-in-the-middle and denial of service attacks detection using machine learning algorithms" Vol. 12, No. 1, February 2023, pp. 418~426,
[2] Mustafa S. Ibrahim Alsumaidaie Khattab M. Ali Alheeti 1 , Abdul Kareem Alaloosy "Intelligent Detection of Distributed Denial of Service Attacks: A Supervised Machine Learning and Ensemble Approach" March 2023.
[3] Guşatu, Marian, and Ruxandra F. Olimid. "Improved security solutions for DDoS mitigation in 5G Multi-access Edge Computing." In International Conference on Information Technology and Communications Security, pp. 286-295. Springer, Cham, 2022.
[4] Kim, Ye-Eun, Yea-Sul Kim, and Hwankuk Kim. "Effective Feature Selection Methods to Detect IoT DDoS Attack in 5G Core Network." Sensors 22, no. 10 (2022): 3819.
[5] Al-Shareeda, Mahmood A., and Selvakumar Manickam. "MSR-DoS: Modular Square Root-based Scheme to Resist Denial of Service (DoS) Attacks in 5G-enabled Vehicular Networks." IEEE Access (2022).
[6] Gao, Qinghang, Hao Wang, Liyong Wan, Jianmao Xiao, and Long Wang. "G/M/1-Based DDoS Attack Mitigation in 5G Ultradense Cellular Networks." Wireless Communications and Mobile Computing 2022 (2022).
[7] Dr. D.Ganesh, Dr.K.Suresh, Dr.M.Sunil Kumar "Improving Security in Edge Computing by using Cognitive Trust Management Model" 2022.
[8] Ling Hou , Mark A. Gregory And Shuo Li "Multi-Access Edge Computing and Vehicular Networking" 21 November 2022.

[9] Khan, Md Sajid, Behnam Farzaneh, Nashid Shahriar, NiloySaha, and Raouf Boutaba. "SliceSecure: Impact and Detection of DoS/DDoS Attacks on 5G Network Slices.(2021)".
[10] Alamri, Hassan A., VijeyThayananthan, and Javad Yazdani. "Machine Learning for Securing SDN based 5G network." Int. J. Comput. Appl 174, no. 14 (2021): 9-16.
[11] Sakib Shahriar Shafin, Sakir Adnan Prottoy , Saif Abbas , Safayat Bin Hakim, Abdullahi Chowdhury , and Md. Mamunur Rashid "Distributed Denial of Service Attack Detectionusing Machine Learning and Class Oversampling" 2021.
[12] Amit V Kachavimath, Shubhangeni Vijay Nazare and Sheetal S Akki "Distributed Denial of Service Attack Detection using Naïve Bayes and K-Nearest Neighbor for Network Forensics" 2020.
[13] Kim, Youngsoo, Jong Geun Park, and Jong-Hoon Lee. "Security threats in 5G edge computing environments." In 2020 International Conference on Information and Communication Technology Convergence (ICTC), pp. 905-907. IEEE, 2020.
[14] Ferhat Ozgur Cataka, and Ahmet Fatih Mustacoglub "Distributed denial of service attack detection using autoencoder and deep neural networks" 2019.
[15] Animesh Gupta "Distributed Denial of Service Attack Detection Using a Machine Learning Approach" 2018.
[16] Moudoud, Hajar, Lyes Khoukhi, and Soumaya Cherkaoui. "Prediction and detection of fdia and ddos attacks in 5g enabled iot." IEEE Network 35, no. 2 (2020): 194-201.
[17] Sharafaldin, Iman, Arash Habibi Lashkari, Saqib Hakak, and Ali A. Ghorbani. "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy." In 2019 International Carnahan Conference on Security Technology (ICCST), pp. 1-8. IEEE, 2019.
[18] Ni, Jianbing, Xiaodong Lin, and Xuemin Sherman Shen. "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT." IEEE Journal on Selected Areas in Communications 36, no. 3 (2018): 644-657.
[19] Li, Dong, Chang Yu, Qizhao Zhou, and Junqing Yu. "Using SVM to detect DDoS attack in SDN network." In IOP Conference Series: Materials Science and Engineering, vol. 466, no. 1, p. 012003. IOP Publishing, 2018.
[20] Larijani, Hadi, Jawad Ahmad, and Nhamoinesu Mtetwa. "A novel random neural network based approach for intrusion detection systems." In 2018 10th Computer Science and Electronic Engineering (CEEC), pp. 50-55. IEEE, 2018.
[21] Adrien Bonguet and Martine Bellaiche "A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing" 5 August 2017.
[22] Zhao, S., Li, W., Zia, T., & Zomaya, A. Y. (2017, November). A dimension reduction model and classifier for anomaly-based intrusion detection in internet of things. In 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (pp. 836-843). IEEE.
[23] Boro, Debojit, and Dhruba K. Bhattacharyya. "DyProSD: a dynamic protocol specific defense for high-rate DDoS flooding attacks." Microsystem Technologies 23 (2017): 593-611.
[24] Azhagiri, M. "HIDDEN CONDITIONAL RANDOM FIELDS FOR INTRUSION DETECTION SYSTEM USING LAYERED APPROACH."
[25] Mangaleswaran, M. "Layered Approach for Intrusion Detection System Using Hidden Conditional Random Fields." (2017).