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

Capturing the Distrubuted Denial of Service Attack Using Bayesian Regularization Algorithm

Ravi Alawe
M.Tech scholar
Department of Computer Science and Engineering
Oriental institute of science and technology
Bhopal,(M.P.) India

Shivank soni
Assistant Professor
Department of Computer Science and Engineering
Oriental institute of science and technology Bhopal
Bhopal,(M.P.) India

Abstract: This paper present the threats posed by distributed denial of service (DDoS) attacks on large networks such as the Internet require the implementation of efficient detection and response strategies. These strategies should be deployed not only at the periphery of the network but also at its core. This article introduces techniques for identifying DDoS attacks by estimating the entropy and frequency-ordered distribution of specific packet characteristics. DDoS attacks reveal inconsistencies in the characteristics of these packet attributes. The detection efficacy and performance are evaluated using real-time traffic data collected from diverse network environments spanning from core Internet points to edge networks. The findings demonstrate the effectiveness of these techniques against current attacks and propose avenues to enhance detection of more covert attacks. Furthermore, we outline our detection-response prototype and discuss how these detectors can be expanded to make informed response decisions**.**

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

I. INTRODUCTION

The emergence of 5G networks and IoT infrastructure promises to significantly enhance connectivity and communication reliability. Many IoT technologies will benefit from 5G's cutting-edge radio access technology, which is characterized by its fast response, strong availability, and remarkable efficiency. Nevertheless, 5G-enabled IoT systems must not only increase network speeds but also prioritize security and increase service dependability. A research study commissioned by the European Union outlines fears about the growing reliance on software to manage 5G cellular networks, along with growing concerns about security vulnerabilities.

If a 5G network is successfully attacked, it could have major consequences. Hackers are aware of this and are adopting new tactics to profit from their attacks, including stealing sensitive data, requesting ransom payments or causing disruption in network services. As a result, the security of 5G networks is particularly vulnerable to threats arising from both internal and external sources. Internal entities within a network, such as employees or insiders, have the potential to cause data breaches and interfere with services, increasing the risks.

A. An Attack-Resistant 5G IOT Infrastructure

A hierarchical framework has been designed to secure the upcoming 5G networks within the Internet of Things (IoT) domain. This framework incorporates diverse security protocols into its structure to identify and thwart potential attacks directed at 5G-enabled IoT networks. Let's look at the outline of a secure architecture for a 5G-enabled IoT shown in Figure 1, which is based on distributed multi-access edge computing (MEC). This architecture consists of three major phases: Access, MEC, and Cloud. In this configuration, the MEC element plays a vital role in collecting data from devices operating at the access layer. The hardware that supports MEC functionalities varies from servers to communications routers, allowing smooth device connectivity. At this stage the data captured in real time is immediately transmitted to the gateway connected to the 5G network. In particular, the fast data transmission capabilities of 5G networks align with the instantaneous data transfer demands of critical IoT applications. The primary functions of these gateways include managing machine-to-machine connections and effectively relaying command signals to their designated endpoints. This hierarchical security architecture for 5G-enabled IoT, supported by MEC, ensures strong protection against potential threats while enabling fast and reliable data exchange within the IoT framework...

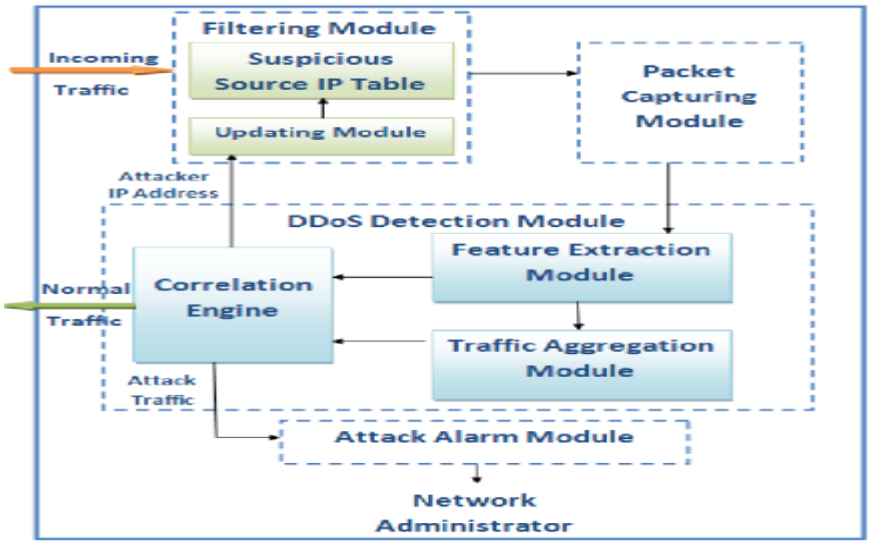

Fig.1 Entry layer to accept data from the physical universe; MEC layer to identify, recognize, and fight security attacks; this is the architecture for 5G-enabled Internet of Things applications., and cloud layer to store the data

B. Types of DDoS attacks

- Volumetric
- Protocol
- Application

II. LITERATURE SURVEY

The literature review explores users' desire for faster data transmission speeds and secure services. 5G NR is expected to fulfill both basic and advanced requirements compared to previous technologies. This advancement enables users to transmit high-definition and large volumes of data within seconds. Moreover, 5G technology can manage larger traffic loads to meet the increasing demands of numerous devices.

Sura Abdulmunem Mohammed Al-Juboori et.al. (2023) - Man-in-the-middle (MTM) and denial-of-service (DoS) attacks represent two distinct categories of network threats that allow many attackers to gain unauthorized access and steal critical data from interconnected devices within a network. Make capable. This research project acquired relevant datasets related to MTM and DoS attacks from the Kaggle platform and leveraged a variety of machine learning algorithms to counter these threats and strengthen the security of the devices involved. Following acquisition of the dataset, the study applied preprocessing methods such as handling missing values, as the dataset in question displayed a significant number of null entries [01].

Mustafa S. Ibrahim Alsumaidaie et.al. (2023) - Distributed denial of service (DDoS) attacks are becoming increasingly prevalent and sophisticated, largely due to rapid advances in 5G networks, smart devices, and the Internet of Things (IoT). These advances pose significant challenges to cybersecurity. The objective of this study is to propose a reliable method to detect and prevent DDoS attacks, thereby protecting communication networks from such threats. To enhance the detection accuracy, the proposed "Intelligent Distributed Denial of Service Attacks Detection (IDDOSAD) approach" integrates learning with supervised machine learning methods such as Random Forest, Decision Trees, K-Nearest Neighbor, XGBoost and Support Vector Machine. Is. The process of model development includes data collection, pre-processing, partitioning into training and testing datasets, selection of predictive models, and evaluation of their performance [02].

Marian Gusatuet.al. (2022):- The technology called Multi-Access Edge Computing (MEC), which supports 5G networks, aims to bring cloud computing capabilities closer to users. This article discusses the role of MEC in combating distributed denial-of-service (DDoS) attacks within 5G infrastructure. Based on prior research efforts, it proposes solutions that leverage the virtualized environment and management entities of the MEC architecture to mitigate the impact of DDoS attacks on legitimate traffic [03].

Yea-Sul Kim et.al. (2022):- The primary objective of the upcoming 5G cellular network is to create a widespread, high-speed Internet of Things (IoT) ecosystem. Insufficiently secured IoT devices have the potential to launch distributed denial of service (DDoS) attacks against 5G mobile carriers at the terabits per second (Tbps) scale. As a result, there is a growing trend to employ machine learning (ML) techniques for autonomous intrusion detection within 5G networks. It is predicted that ML-powered DDoS attack monitoring in 5G environments will demonstrate faster response[04].

Nashid Shahriar et.al(2021):- One of the key technologies facilitating 5G networks is network slicing. This technology allocates different logical resources to different applications within a shared physical network. However, the effectiveness of network slicing can be reduced by denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks. These attacks have the potential to significantly disrupt the operation and efficiency of network slices. The challenge also includes the fact that existing methods for detecting DoS/DDoS attacks rely on data obtained from simulations of 5G networks rather than real instances of network slicing. In this study, we aim to characterize how distributed denial-of-service (DDoS) attacks can impact performance metrics such as latency and bandwidth for users across network slices [05].

Vijey Thayananthan. et.al (2021):- Fifth generation (5G) networks provide stronger support for a variety of systems, especially in applications where maximum security is required. Many servers are adopting diverse cloud technology (DC) configurations to explore new network topologies, driving the growth of software-defined networking (SDN). A significant concern within this framework is the threat of distributed denial of service (DDoS) attacks. These attacks instigated by malicious actors pose a serious challenge to the security of 5G technologies based on SDN. While many strategies exist to mitigate DDoS attacks in SDN environments, securing the SDN controller remains a difficult task within the industry [06].

Amit V Kachavimath et.al. (2020) - The successful implementation and functioning of the Internet of Things (IoT) largely depends on the adoption of effective data transmission protocols. One such widely used protocol is the Publish/Subscribe Message Queuing Telemetry Transport (MQTT) protocol, which plays a vital role in IoT operations. With the increased adoption of MQTT by IoT manufacturers, there has also been an increase in cybersecurity threats targeting this protocol.A particular area of concern is the vulnerability of the MQTT protocol to protocol-based application layer denial of service (DoS) attacks. These attacks, which are notorious for causing serious service disruptions in legacy systems, can now be directed toward IoT devices due to the widespread use of MQTT. This study focuses on developing a framework to detect application layer DoS attacks on the MQTT protocol and evaluate its effectiveness against real-world attack scenarios that follow the protocol's standards.Our approach involves implementing an MQTT protocol-specific machine learning-based detection system to protect message brokers from such threats. Through extensive testing on various MQTT brokers, we assess the ability of the framework to detect and mitigate these malicious attacks. Our findings show that despite efforts to deny legitimate access and limit resources, attackers can still take over servers in some scenarios.Furthermore, our analysis of MQTT properties shows high accuracy in identifying attacks, especially leveraging attributes related to message length and field attributes. These features are proven to be effective in detecting IoT-based attacks and reducing false-positive alerts, enhancing overall security measures for MQTT-enabled systems [07].

Ferhat Ozgur Catak et.al. (2019) - Due to the increasing prevalence of botnets, fuzzers, shellcodes, and other network-related vulnerabilities, many businesses are experiencing significant levels of network traffic, the majority of which involve network attacks. These attacks are disrupting daily operations and adversely impacting the organization. The use of classification models can help quickly identify and isolate these attacks. The primary purpose of distributed denial of service (DDoS) attacks is to disrupt or reduce access to services to legitimate users. This project aims to classify network traffic by employing deep learning techniques and network flow models. A deep neural network model was employed to enhance the classification performance of the system. The classification performance of network traffic evaluated by the models used in this research is represented through figures and tables with related metrics. The results show that the proposed model can accurately identify DDoS attacks using deep learning techniques [08].

Animesh Gupta et.al. (2018) - A distributed denial of service (DDoS) attack is a type of cyber attack that aims to disrupt the services of a network or server by overwhelming it with excessive requests, making it unable to handle legitimate user requests. In Q3 2017, organizations globally faced an average of 237 DDoS attack attempts per month, or about 8 attacks per day, as reported by Corero Network Security, a company specializing in DDoS protection and mitigation. This marked a substantial increase of 91% from Q1 and 35% from Q2 of the same year. According to a study by Incapsula, the average cost of a DDoS attack to companies is $40,000 per hour. While commercial software is available to detect and mitigate DDoS attacks, its high cost can create challenges for small and medium-sized enterprises (SMEs). To bridge this gap, a proposed initiative aims to provide SMEs with a reliable, real-time web application to predict DDoS attacks, empowering them to protect their servers and networks against malicious DDoS activities.[09].

Adrien Bonguet et.al. (2017) - The concept of "cloud computing" represents a computing paradigm that provides widespread, efficient, and instant access to a shared repository of highly adaptable assets such as servers, networks, storage, applications, and services. Access to cloud services faces significant risks from denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks due to inherent vulnerabilities such as resource pooling and multi-tenancy in the cloud. This research highlights new forms of DoS and DDoS attacks within cloud computing, including XML-DoS and HTTP-DoS attacks, and explores various potential methods for mitigation and detection. Subsequent research efforts will gain insight from this investigation, which also provides an overview of existing defense mechanisms and evaluates their efficacy through experimentation and standard evaluation criteria[10].

.

III. PROBLEM FORMULATION

Detecting Distributed Denial of Service (DDoS) attacks using machine learning poses several challenges. Here are the primary issues involved:

- Rarity of DDoS attacks: DDoS attacks are relatively rare compared to regular network traffic. In the event this discrepancy can create bias in machine learning models, favoring the majority class and reducing their ability to effectively detect attacks.
- Dynamic nature of the attack: DDoS attacks exhibit a wide range of strategies, methods, and processes. This dynamic nature makes it challenging to capture diverse attack patterns in a static model, highlighting the need for machine learning models to be adaptable and flexible.

- Importance of feature selection: The complexity of network traffic requires careful selection of features for model training. Identifying relevant characteristics that accurately differentiate between normal and malicious traffic is a complex task that requires attention to detail.

- Anomaly detection vs. signature-based approaches: DDoS attacks may appear as unusual patterns or follow known signatures. Anomaly detection models may struggle to distinguish between new attack patterns and legitimate changes in network behavior, underscoring the importance of considering both types of approaches.

IV. PROPOSED METHOD

Ddistributed Denial of Service (DDoS)

Denial of service (DoS) attacks disrupt the availability of online resources and services by flooding the system with an excessive number of communication requests. This flood of requests puts pressure on the victim's system, preventing it from responding to legitimate traffic and causing interruptions in service. Although this method is a known technique for causing disruption, it can also be used in a distributed denial of service attack (DDoS). In a DDoS attack, the attacker takes advantage of the large number of compromised computers around the world to send these massive requests to the victim's system, increasing the impact. Despite appearing legitimate, these requests can cripple the system by draining resources such as memory and bandwidth. DDoS attacks are a common phenomenon, occurring regularly in various regions. Major platforms like Twitter and Facebook have also not remained untouched by these attacks, affecting the experiences of their users. Additionally, notable institutions such as the New York Stock Exchange, NASDAQ, the White House, the Federal Trade Commission, the Treasury, the Washington Post, and many others have also fallen victim to distributed denial of service attacks. Over time, both the volume of attack traffic and the overall threat posed by such attacks have increased significantly.

A. Proposed Work

An Artificial Neuron Network (ANN) is a computer model that mimics the structure and operations of biological neural networks. In the realm of Computer Science, an ANN acts as a synthetic human nervous system by receiving, processing, and transmitting data.

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)

B. Applications Should Neural Networks Be Used

They serve as universal approximators and excel in modeling systems that can tolerate a high degree of error. Neural networks belong to this class of models. Consequently, using a neural network to balance a checkbook would not be recommended! Nonetheless, they are highly effective for.:

- Capturing associations or discovering regularities within a set of patterns;
- In cases when the data is very large in terms of size, variety, or number of factors;
- There is a hazy understanding of the links between factors;
- With standard ways, it's hard to articulate the connections well

C. Proposed Training Of D-Dos Attack Detection Bayesian Regularization Algorithm

In this section, we will learn in detail about the Bayesian regularization learning method and Back Propagation Neural Networks (BPNNs), which use backpropagation for learning. A more detailed description can be found in Demuth et al. [33]. Bayesian regularization Backpropagation neural networks are used to increase generalization and reduce overfitting during training. The training data set, denoted as D and consisting of input-target vector pairs for the network model, is used for training the neural network.

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

The error "e" is computed for each key ("u") within the system by comparing the desired output with the estimated output. Utilizing a quantitative measure is imperative for evaluating the network's efficacy, specifically its capability to accurately match the test data. This measure is referred to as the network performance index, serving as a tool to enhance the network's attributes. The standard performance index F is governed by the sum of squared errors (SSE)):

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

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

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

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, $P\,(\overline{w}|\mu, M_N)$is given as:

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

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

$J^T e$ is the error gradient.

Flow Chart of proposed Method

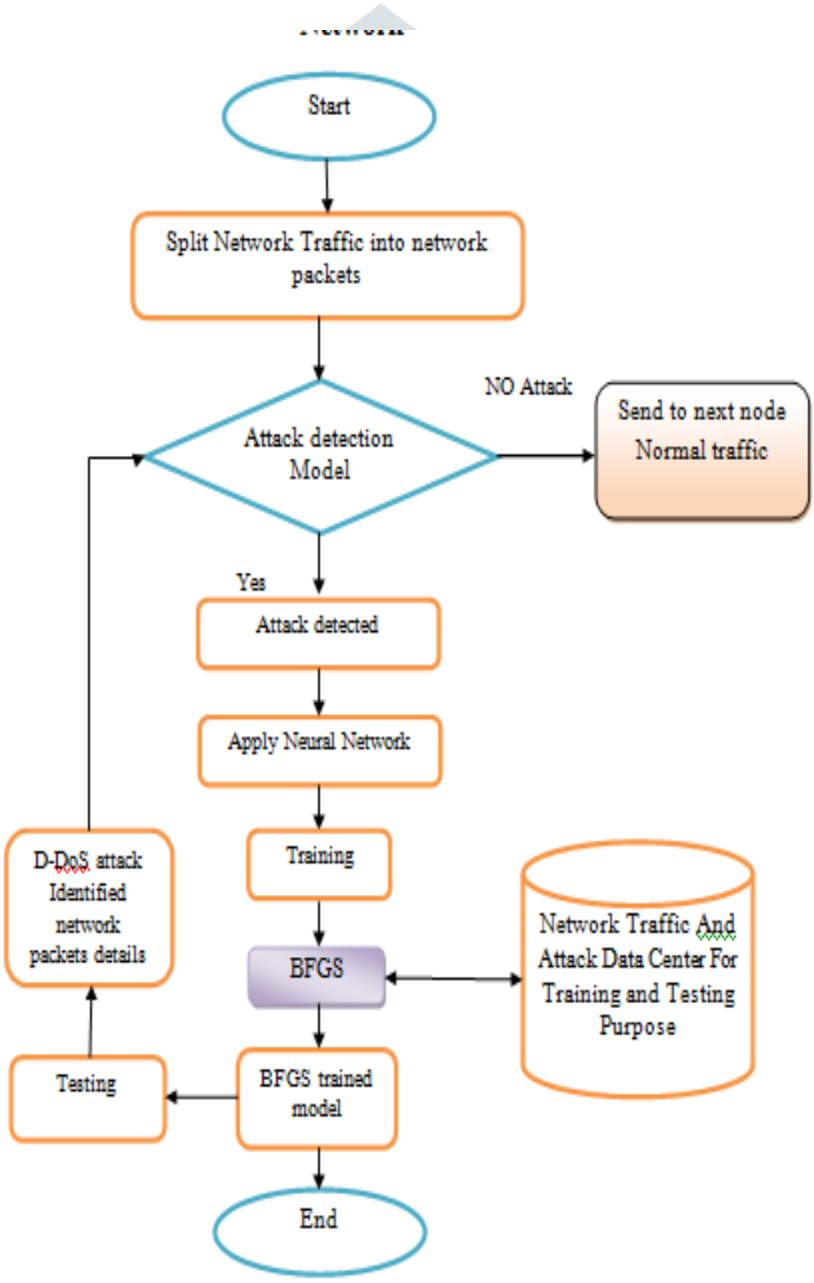

Fig. 2: There are three models—the collector model, the prediction and detection model, and the reaction model—that could secure 5G-enabled IoT device applications against DDoS assaults.

V. SIMULATION AND RESULT

This document provides a detailed overview of the execution and design aspects of our upcoming research. We have identified MATLAB 2020 as a widely used tool that matches well with the techniques we want to employ. Our experimental

framework incorporates the well-known DDoS dataset obtained from the Canadian Institute of Cyber Security (CICIDS2017) and leverages the MATLAB 2020b coding environment. The introductory section of this chapter provides a comprehensive exploration of the MATLAB environment, highlighting its relevance to our research objectives. Subsequently, the next section introduces the CICIDS2017 dataset, which serves as a fundamental component in our research implementation. Finally, the third section outlines the essential tables, snapshots, and graphs required for the successful execution of our proposed work.

A. Overview of the MATLAB

MATLAB stands out as a robust technical computing language, suitable for diverse tasks such as advanced rule generation, data visualization, information analysis, and numerical calculations. It empowers researchers to efficiently tackle complex computing challenges, outperforming traditional languages like C, C++ and algebraic languages. MATLAB finds wide utility in areas such as signal processing, image processing, communications, system design, testing, measurement, financial modeling and bioinformatics. In addition, the MATLAB community has developed several addon toolboxes containing specialized functions tailored for specific application areas, increasing its usefulness and flexibility.

B. Result Parameters

Several aspects of the outcomes are looked at in the method outlined here. Here are some of the factors that you should monitor.

True Positive (T.P.)

When the model correctly predicts the positive class, we call it a "true positive." A genuine positive is the result of an experiment where the hypothesis was right.

False Negative (F.N.)

A false negative mistake occurs when a test result falsely indicates that a condition does not hold. A false negative test is one in which the results falsely imply that a condition does not exist.

False Positive (F.P.)

When an algorithm wrongly predicts the positive class, this is known as a false positive. A false positive diagnosis of an illness occurs when there is an error in the use of binary categorization.

True Negative (T.N.)

True negatives are those for which the model provides accurate predictions for the undesirable categories of outcomes.

Accuracy(ACC)

In the context of plant disease detection, a true positive (TP) indicates the accurate discovery of a disease, while a true negative (TN) indicates that a plant leaf is disease-free. False negatives (FN) occur when diseased leaves are not detected, causing potential problems. Various industries rely heavily on FN rates to assess the overall accuracy of identification methods, especially in tasks such as weed or disease identification. Failure to locate weeds or diseased plants can lead to rapid spread and growth, causing risks that persist even after treatment. While precision-improving methods are valuable, methods with higher FN rates may carry greater risks.

$$\text{Accuracy} = (TP + TN) / S$$

When S In the validation set, there were a total of FP false positives (deaths misclassified as plants) and FNR false negatives. It's how likely it is that a diseased plant will provide a positive test result. Precision is the sum of true production (TP) and false production (TN) divided by the entire number of production (TP+TN+FP+FN).

$$\mathbf{Acc} = \frac{\mathbf{TP + TN}}{\mathbf{TP + TN + FP + FN}}$$

Where TP = Definitely Positive, FP = Definitely False, TN = Definitely Negative, and FN =Definitely Not Negative

C. Simulation Outcomes

In this section, we will discuss various simulation results generated from different proposed training methods. Specifically, we will explore the feed forward Bayesian regularization (FF-BR) algorithm. Feed forward represents a deviation from feedback mechanisms, which emphasize proactive measures rather than reactive ones. This involves shifting focus toward future-oriented strategies, overcoming past-oriented feedback loops.

The experimental setup involves the use of a neural network (NN), as shown in Figure 2 below. This approach includes a total of 30 input features. Bayesian regularization is implemented using conjugate gradient techniques during the training phase. The training process lasted thirteen seconds, with mean square error values twenty-six and twenty-seven recorded. Specifically, the epoch number for this training session was set to 30.

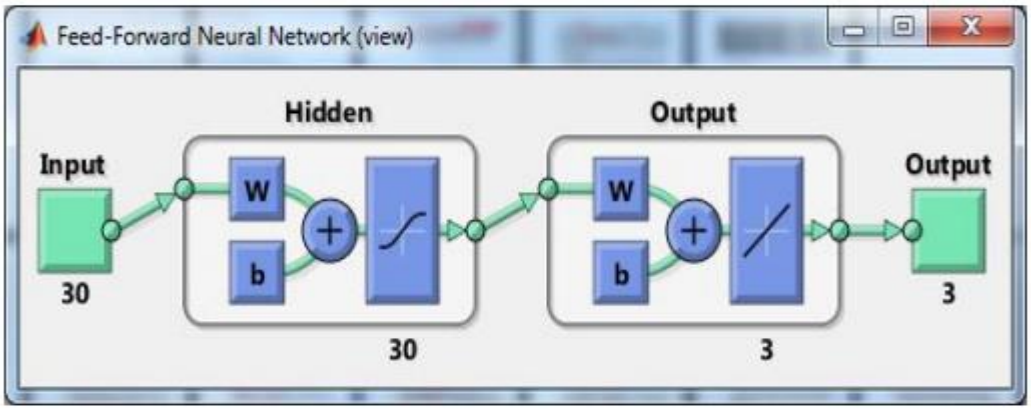

Fig.2 Bayesian regularization based Feed Forward Network

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

S. No.	Parameters Name	Inputs of Parameter
01	Data Division	Random
02	Network Type	Feed Forward Network (FFN)
03	Training	Bayesian regularization (BR)
04	Performance	Mean square Error (MSE)

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

S. No.	Parameters Name	Inputs of Parameter	Training Outputs
01	Number of Epochs	0-30	30 iterations
02	Time	11 min 33 second	11 min 33 second
03	Performance	2.38	0.0148
04	Gradient	5.00	0.0288

Figure 3 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 epoch 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

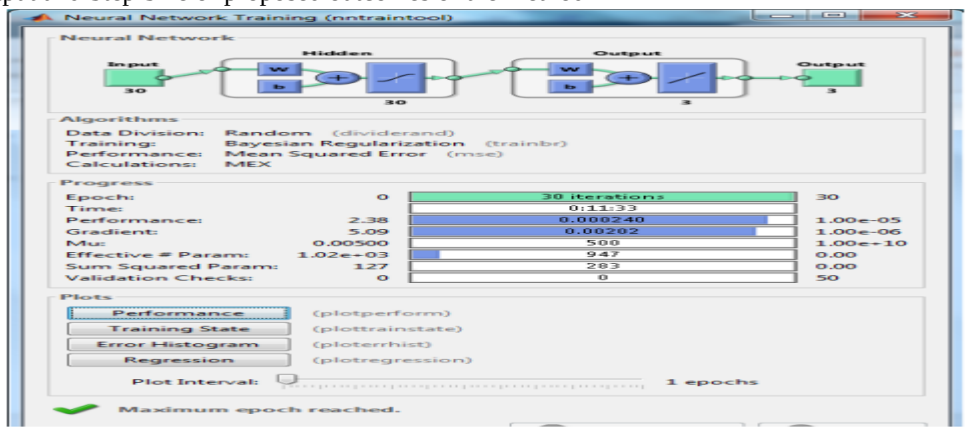

Fig.3 Training of proposed Bayesian regularization with Feed Forward and Cascaded Feed Forward

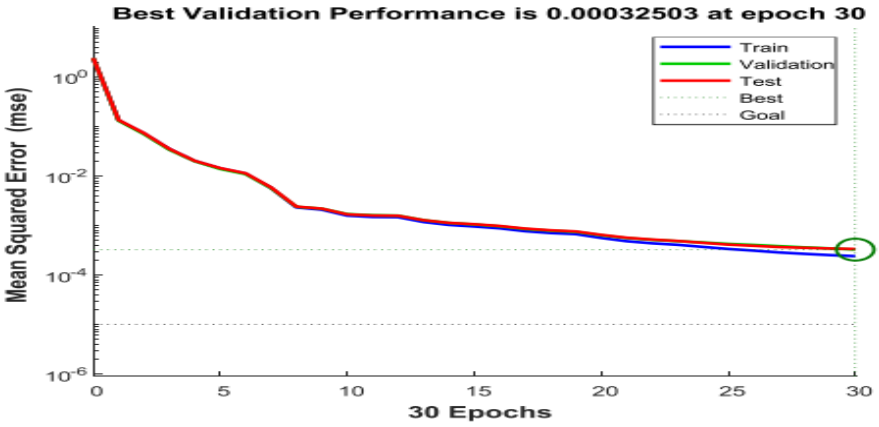

Fig -4 Shows the Training Outcome of Proposed Bayesian Regularization in Feed Forward Network

In the below figure 4 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.

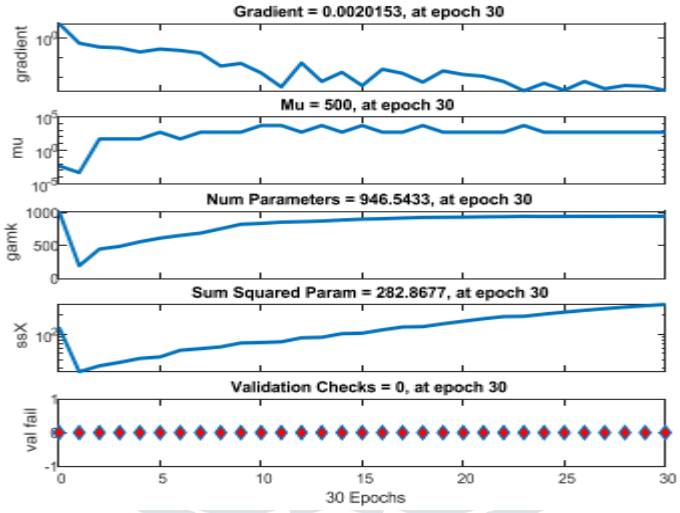

Fig 5 Shows the Gradient, Number of Parameters, Sum Squared Parameter

In the below figure Error Histogram of proposed Bayesian Regularization for feed Forward Network. In this training outcomes analysis the all three state training, test, and validation.

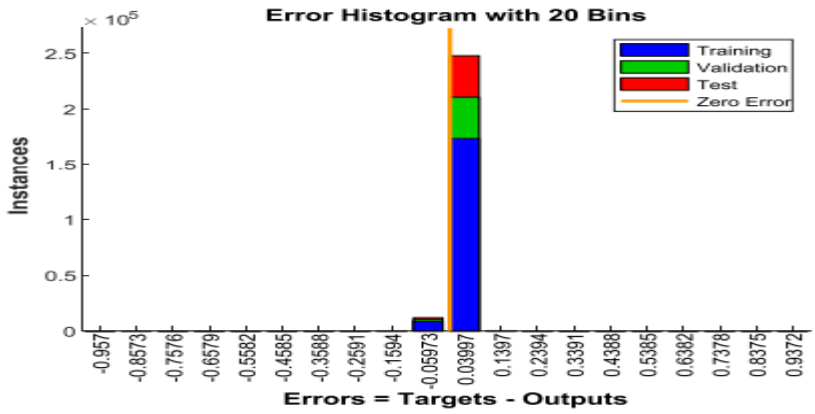

Fig 6 Shows the Error Histogram of proposed Bayesian Regularization for feed Forward Network

In the above figure 6 shows the error histogram of proposed Bayesian Regularization for feed Forward Network method in the time of training, how much error are occurs in frequency domain denoted the above figure.

VI. CONCLUSION

The findings of the proposed method underline the critical importance of addressing DDoS (Distributed Denial of Service) attacks on 5G networks. These attacks can cause significant disruption and potentially jeopardize critical services. Understanding the impact of such attacks on 5G networks is paramount, so proactive measures are needed to mitigate their impact.A major challenge with 5G networks is their heavy reliance on software-defined networking (SDN) and network function virtualization (NFV) technologies. While these technologies increase the agility and flexibility of networks, they also increase the network's vulnerability to attacks. DDoS attacks can exploit vulnerabilities in SDN and NFV, posing a significant threat to network stability. To combat DDoS attacks on 5G networks, several strategies can be deployed. These include implementing strong traffic filtering mechanisms, implementing strict access controls, and employing behavioral analysis techniques. Additionally, ensuring timely application of security patches, continuously monitoring network traffic for anomalies, and establishing effective response and recovery protocols are important steps in protecting 5G networks against DDoS threats.

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. 60

[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 serviceoriented 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).
[26] Zantedeschi, Valentina, Maria-Irina Nicolae, and Ambrish Rawat. "Efficient defenses against adversarial attacks." In Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, pp. 39-49. 2017.
[27] Boro, Debojit, Himant Basumatary, Tribeni Goswami, and Dhruba K. Bhattacharyya. "UDP flooding attack detection using information metric measure." In Proceedings of International Conference on ICT for Sustainable Development: ICT4SD 2015 Volume 1, pp. 143-153. Springer Singapore, 2016.
[28] Timotheou, Stelios. "Fast Non-Negative Least-Squares Learning in the Random Neural Network." Probability in the Engineering and Informational Sciences 30, no. 3 (2016): 379-402.
[29] Papernot, Nicolas, Patrick McDaniel, Arunesh Sinha, and Michael Wellman. "Towards the science of security and privacy in machine learning." arXiv preprint arXiv:1611.03814 (2016).