http://www.jctjournals.com ISSN(ONLINE):2278 – 3814

Volume-12, Issue-12, December 2023
JOURNAL OF COMPUTING TECHNOLOGIES (JCT)
International Journal
Page Number: 01-07

A DDoS Attack Recognition via PRP Algorithm Based Cascaded Feed Forward Approach

Kunal Kumar[1], Sanjay Kumar Pal[2]
[1]M.Tech Student of CSE , [2]Assistant Professor,
[1,2]Department of Computer Science Engineering
[1,2,] **Oriental Institute of Science and Technology (OIST), RGPV, Bhopal, INDIA**
[1]er.kunalsinghcs@gmail.com

Abstract*— In the current generation cyber attack indomitable problem between researcher. Recently march 2022 hackers used a DDoS attack to shut down the National Telecommunications Authority of the Marshall Islands. In this research work presented a Polak–Ribière–Polyak (PRP) with cascaded feed forward network for detection of DDoS cyber attack. The Polak–Ribière Polyak algorithm presents better learning efficiency as well as better accuracy. The proposed Polak–Ribière–Polyak algorithm shows better results as compared to other previous weight optimizer method based on machine learning as well as deep learning methods. For the implementation of proposed method use MATLAB 2020. This research work uses the Canadian Institute of Cyber Security (CICIDS2017) data set to perform the proposed methodology. The proposed method shows good results in terms of accuracy, precision, selectivity, sensitivity, and confusion matrix (C.M.). The presented method shows an accuracy of 98.60% and the other parameters are discussed in the simulation and result section.

***Keywords* — Polak–Ribière Polyak, Weight Optimal, Cicids, Confusion Matrix (C.M.)., DDoS, Slowloris, Slow Httptest and Hulk..**

I. Introduction

A Cyber DDoS (Distributed Denial of Service) Attack is a type of cyber-attack where a network or server is flooded with a large number of requests from multiple sources, overwhelming its capacity and causing it to become unavailable for legitimate users. Detecting and mitigating DDoS attacks is a critical task for network security.The Polak–Ribière–Polyak (PRP) Algorithm is an optimization method used to find the minimum of a function. It is commonly used in machine learning and deep learning applications.

In this approach, a Convolutional Feedforward Neural Network (CFFNN) is used to detect DDoS attacks. The PRP Algorithm is employed to optimize the network parameters and improve its accuracy in detecting DDoS attacks. The CFFNN is trained on a large dataset of network traffic data, including normal traffic and DDoS attack traffic, to learn the patterns and characteristics of each.

Once trained, the CFFNN can classify new traffic data as either normal or DDoS attack traffic, allowing for early detection and mitigation of DDoS attacks before they cause significant damage.Overall, this approach provides an effective and efficient method for detecting DDoS attacks using machine learning and optimization techniques.

A. Cyber DDoS Attack Detection

A cyber DDoS (Distributed Denial of Service) attack detection system is designed to detect and prevent DDoS attacks on a network. DDoS attacks are a type of cyber attack in which an attacker floods a network with a large number of requests, overwhelming the network and making it unavailable to legitimate users.

DDoS attacks can cause significant damage to organizations, including financial losses, reputational damage, and loss of sensitive data. A DDoS attack detection system can help organizations to identify and mitigate DDoS attacks in real-time, minimizing the damage caused by these attacks.A typical DDoS attack detection system uses a combination of techniques, including network traffic analysis, machine learning algorithms, and behavioral analysis, to detect and prevent DDoS attacks. The system may also incorporate techniques such as rate limiting, traffic shaping, and IP blocking to prevent the attack from overwhelming the network. Overall, a robust DDoS attack detection system is a critical component of any organization's cybersecurity infrastructure, helping to protect against one of the most common and damaging types of cyber attacks.

.

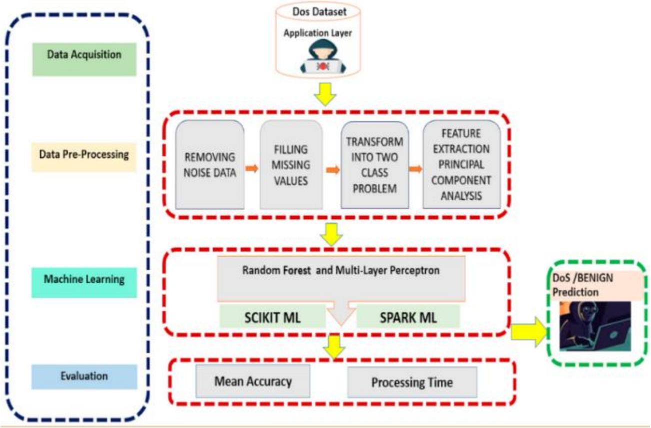


Fig. 1. Cyber DDoS Attack Detection

B. Types of Cyber Attacks

A botnet is a group of platforms and operating systems that work together to achieve a certain purpose. Because these programs, which are also called bots or robots, are spread out across a network of sensors, they are called bots or robots because they work together. we call it a "botnet." Individual bots can't do so much harm, but when they're all working together, the're strong and possibly deadly. Cyber attackers utilise botnets to carry out a variety of operations. They may aid a cyberattacker in carrying out a cognitive dissonance assault, such as flooding a website with traffic in order to knock it down. Such attacks may cost business millions of dollars in lost revenue, fines, and clients. Botnets may also be used to steal passwords and other information, send emails, and spread malware. Hackers often use hacks because of their low cost and efficacy. To protect the organization from harmful activity, you need to implement a comprehensive IT security system.

A botnet effort might infect thousands of machines and turn them into botnets, bypassing corporate firewall security measures.

C. Cross-Site Scripting Attacks

Cross-site scripting attacks exploit third-party online capabilities to support scripts in scriptable software or internet browsers. An attacker must inject a malicious JavaScript-infected payload into a website's database to carry out an XSS attack. The message is transmitted as part of the HTML body when the intended victim visits a page on this website. This is subsequently delivered to the victim device's website, where the software is launched.

The software has the capability of sending a user's data to a hacker's server. The attacker would then be able to extract it and exploit it to take control of the user's activities. When other flaws are used together, XSS can be used to take screenshots, record keyboard activity, steal network data, and even take control of a device from afar. From inside ActiveX, Flash, VBScript, and JavaScript, XSS may be used to initiate an attack. Because JavaScript is so extensively used, it is the most commonly utilised mechanism for carrying out XSS assaults.

D. Distributed Denial-of-Service DDOS

A denial-of-service (DoS) attack is used by hackers to overload a system's resources, rendering it unavailable for service requests. The platform's services are also impacted by a distributed denial-of-service (DDoS) attack, but the operation is launched from a huge number of candidate computers, most of which are hacked and under the cyberattacker's command.

DDoS attacks, which are often used in conjunction with malware, have the ability to completely bring down a website or online service. A distributed denial-of-service (DDoS) attack is a malicious attempt to stop a user, business, or network from working. or platform's regular communication by flooding the victim or its neighbouring areas with online traffic.

DDoS assaults are successful because they use numerous hacked computer networks as attacker web traffic. Machines and other linked sources, such as the Internet of things, are examples of attacked machinery. A DDoS assault is analogous to an unanticipated traffic jam obstructing the roadway, blocking ordinary flow from reaching its destination.

II. PRP ALGORITHM

Moreover, the search direction possesses the sufficient descent property independent of line search. Utilizing the standard Wolfe–Powell line search rule to yield the stepsize, the global convergence of the proposed method is shown under the common assumptions. Finally, numerical results show that the proposed method is promising compared with two existing methods:

Consider the problem of minimizing f over R^n:

$$\frac{min}{x \in R^n} f(x) \qquad (1)$$

Where $f : R^n \to \mathrm{R}$ is continuously differentiable. Throughout, the gradient of f at x is denoted by $g(x)$, i.e., $g(x)$: $=\nabla f(x)$. We know that conjugate gradient (CG) methods are very popular and effective for solving unconstrained optimization problems especially for large-scale case by means of their simplicity and low memory requirements. These preferred features greatly promote their applications in various areas such as image deploring and demising, neural network, compressed sensing, and others. We refer the interested readers to some recent works and references therein for more details. The numerical results reported in reveal that the CG method has great potential in solving image restoration problems:

$$x_{k+1} = x_k a_{k d_k} \qquad (2)$$

where $\alpha_k > 0$ is called the stepsize computed by some line search. Here, d_k is commonly known as the search direction, which is defined as follows,

$$d_k = \{\frac{-g_k}{-g_{k+\beta_k} d_k,} if \frac{K=1}{K>1} \quad (3)$$

where $\beta_k \in R$ is the so-called CG parameter and g_k is the abbreviation of $g(x_k)$, i.e., $g_k : =g(x_k)$. The two key factors that affect the numerical performance of the CG method are the step size and the CG parameter.

The exact line search rule: calculate a step size α_k satisfying

$$f(x_k + a_k d_k) = \min_{a \geq 0} f + (x_k + ad_k \quad (4)$$

The standard (weak) Wolfe–Powell (WWP) line search rule: calculate a stepsize α_k satisfying

$$f(x_k + a_k d_k) \leq f(x_k) + \delta \alpha_{k g_k^T} d_k \quad (5)$$

And

$$g(x_k + a_k d_k) T_{dk} \geq \sigma g_k^T d_k \quad (6)$$

where $0 < \delta < \sigma < 1$.

The strong Wolfe–Powell (SWP) line search rule: calculate a stepsize α_k satisfying (5) and

:

$$|g(x_k + a_k d_k) T_{dk}| \leq \sigma |g_k^T d_k| \quad (7)$$

On the other hand, different CG methods are determined by different CG parameters. The well-known CG methods include the Fletcher–Reeves (FR) [4], Polak–Ribière–Polyak (PRP) [5, 6], Hestenes–Stiefel (HS) [7], Liu–Storey (LS) [8], Fletcher (CD) [9], and Dai–Yuan (DY) [10] methods, and their CG parameters β_k are, respectively, given by:

$$\beta_k^{FR} = \frac{\|gk\|2}{\|g_{k-1}\|} \quad (8)$$

where $y_{k-1} : =g_k - g_{k-1}$ and $\|\cdot\|$ stands for the Euclidean norm. The methods yielded by the above CG parameters are called the classical CG methods, and their convergence analysis and numerical performance have been extensively studied (see, e.g., [4–12]). It has been shown that the above formulas for the CG parameters are equivalent when $f(x)$ is convex quadratic and the stepsize α_k is obtained by carrying out the exact line search rule (4). However, their numerical performance strongly depends on the CG parameter β_k. The FR, CD, and DY methods possess good convergence, but the numerical performance for these methods is somewhat unsatisfactory for solving general unconstrained nonlinear optimization problems [12–14]. On the contrary, it has been shown that the convergence properties of PRP, HS, and LS methods are not so well, but they often possess better computational performance [12–14]. Therefore, in the past few decades, based on the above formulas, plenty of formulas for β_k are designed for CG methods that possess both good global convergence properties and promising numerical performance (see [12–16] and references therein).

To our knowledge, the first hybrid CG method in the literature was proposed by Touati-Ahmed and Storey [17] (TS method), where β_k is computed as

$$\beta_k^{TS} = \{\frac{\beta_K^{PRP}}{\beta_k^{FR}} \frac{if\, 0 \leq \beta_k^{PRP} \leq \beta_k^{FR}}{otherwise\ .}\} \quad (9)$$

Apparently, the TS method has some good properties of FR and PRP methods since β_k^{TS} is a hybrid of β_k^{FR} and β_k^{PRP}. Combined with HS and DY methods, Dai and Yuan [18] proposed another hybrid CG method (hHD method), in which the hybrid CG parameter β_k is obtained by.

$$\beta_k^{hHD} = \max\{0, \min\{\beta_k^{HS}, \beta_k^{DY}\}\} \quad (10)$$

When the WWP line search rule is used to compute the stepsize, the resulting search direction in is a descent one and the global convergence for the hHD method is proved. Moreover, the numerical experiments reported in illustrated that the hHD method is competitive and practicable. For other closely related works, we refer the readers to and the references therein. It is worth noting that the CG parameters β_k defined in are restricted to positive values. As explicated in, this restriction in turn results in global convergence of the algorithm. In recent years, many hybrid CG methods were proposed on the basis of the methodology of discrete combinations of several CG parameters. The combination parameter is computed by some secant equations the conjugacy condition or by minimizing the least-squares problem consisting of the unknown search direction and an existing one (see] and the references therein).

$$\beta_k^{WYL} = \frac{\|gk\|2 - \|gk\|/\|gk-1\| g_k^T g_{k-1}}{\|gk-1\|2} \quad (11)$$

Under the assumption that d_k generated satisfies the so-called sufficient descent condition:

$$g_k^T d_k \leq -c\|gk\|2, \quad c > 0 \quad (12)$$

the WYL method is globally convergent under the WWP line search rule and possesses superior numerical performance. Subsequently, Dai and Wen proposed two improved CG methods with sufficient descent property. The CG parameters β_k :

$$\beta_k^{DHS} = \frac{\|gk\|2 - \|gk\|/\|gk-1\| \left|g_{k g_{k-1}}^T\right|}{d_{k-1 yk-1}^T + \mu |g_k^T d_{k-1}|} \quad (13)$$

$$\beta_k^{DPRP} = \frac{\|gk\|2 - \|gk\|/\|gk-1\| \left|g_{k g_{k-1}}^T\right|}{\|gk-1\|2 + \mu |g_k^T d_{k-1}|} \quad (14)$$

where $\mu > 1$. Clearly, the search direction yielded by β_k^{DPRP} satisfies the sufficient descent condition without depending on any line search. However, the sufficient descent property associated with β_k^{DHS} relies on the WWP line search rule.

Based on the above observations, it is interesting to design a hybrid CG method such that the CG parameter is nonnegative and the resulting search direction possesses the sufficient descent property independent of line search technique. Motivated by the methods in and considering that the HS method performs best among the classical CG methods, a new formula for the CG parameter β_k is given by

$$\beta_k^{hHPR} = \min\{|\beta_k^{HS}|, \frac{\|gk\|2-\|gk\|/\|gk-1\||g_k^T g_{k-1}|}{\|gk-1\|2+\mu|g_k^T d_{k-1}|} \qquad (14)$$

where $\gamma > 2$. It is not difficult to see that β_khHPR is a hybrid of β_kHS, βkWYL, and β_kDPRP.Interestingly, the above parameter β_khHPR is always nonnegative. To see this, let θ_k be the angle between g_k and g_{k-1}. Thus, we know from (14) that

$$\beta_k^{hHPR} \le \frac{\|gk\|2 - \|gk\|/\|gk-1\||g_{k}^T g_{k-1}|}{\|gk-1\|2 + \gamma|g_k^T d_{k-1}|}$$

$$= \frac{\|gk\|2(1-\cos\theta_k}{|g_{k-1}|2+\gamma|g_k^T d_{k-1}|} \le \frac{2\|gk\|2}{\|gk-1\|2+\gamma|g_k^T d_{k-1}|} \qquad (15)$$

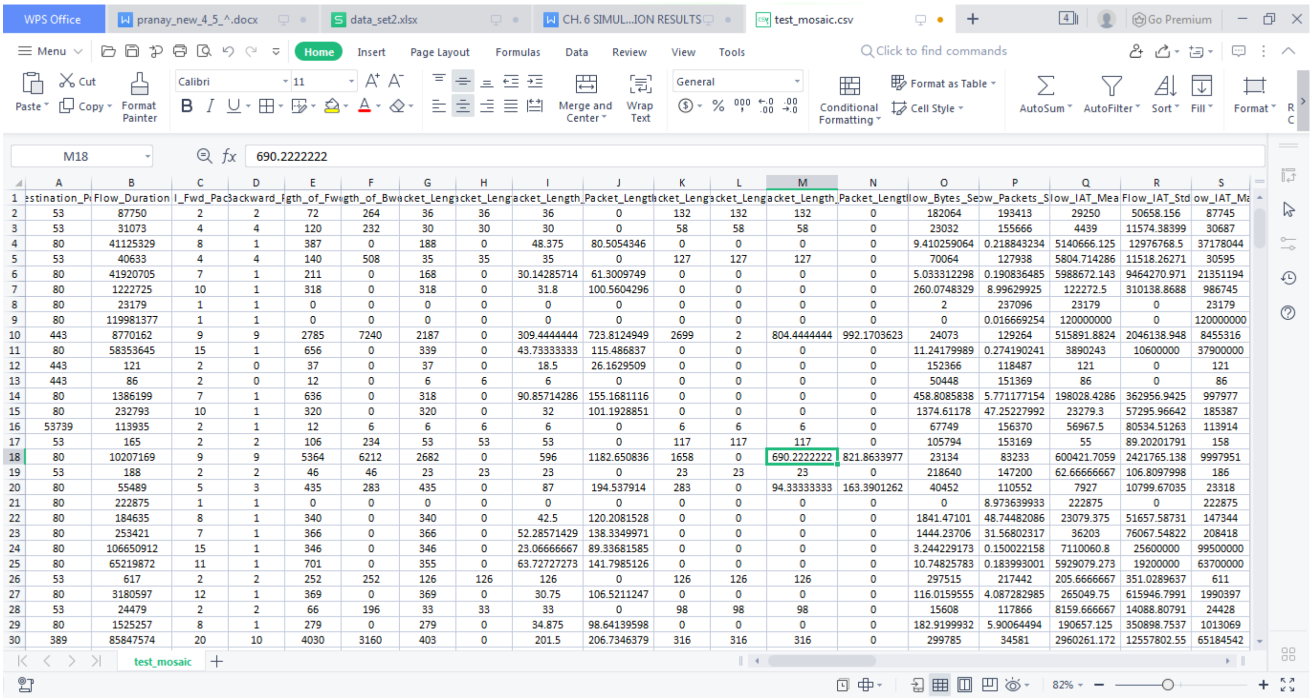
Which further implies

$$0 \le \beta_k^{hHPR} \le \frac{2\|gk\|2}{\|gk-1\|2} \qquad (16)$$

Moreover, plugging the CG parameter $\beta_k :=\beta_k$hHPR into we can show that the resulting search direction possesses the sufficient descent property independent of line search technique.

III. SIMULATION AND RESULTS

In this section, we are describing out the implementation detail and designing issues for our proposed research work. By searching, we have observed that for our proposed work the MATLAB 2020 [22]is the well-known platform to perform the suggested approach. we tend to perform some experimental tasks, these tasks perform in MATLAB 2020b [25] code, and additionally, the well-noted DDoS data set Canadian Institute of Cybersecurity (CICIDS2017)is employed provided by Canadian Institute [31].



M18 690.2222222

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	estination_P	Flow_Duration	l_Fwd_Pac	Backward_	gth_of_Fw	gth_of_Bw	acket_Leng	acket_Leng	acket_Length_	Packet_Length	acket_Leng	acket_Leng	acket_Length_	Packet_Length	low_Bytes_Se	ow_Packets_S	low_IAT_Mea	Flow_IAT_Std	ow_IAT_Ma
2	53	87750	2	2	72	264	36	36	36	0	132	132	132	0	182064	193413	29250	50658.156	87745
3	53	31073	4	4	120	232	30	30	30	0	58	58	58	0	23032	155666	4439	11574.38399	30687
4	80	41125329	8	1	387	0	188	0	48.375	80.5054346	0	0	0	0	9.410259064	0.218843234	5140666.125	12976768.5	37178044
5	53	40633	4	4	140	508	35	35	35	0	127	127	127	0	70064	127938	5804.714286	11518.26271	30595
6	80	41920705	7	1	211	0	168	0	30.14285714	61.3009749	0	0	0	0	5.033312298	0.190836485	5988672.143	9464270.971	21351194
7	80	1222725	10	1	318	0	318	0	31.8	100.5604296	0	0	0	0	260.0748329	8.99629925	122272.5	310138.8688	986745
8	80	23179	1	1	0	0	0	0	0	0	0	0	0	0	2	237096	23179	0	23179
9	80	119981377	1	1	0	0	0	0	0	0	0	0	0	0	0	0.016669254	120000000	0	120000000
10	443	8770162	9	9	2785	7240	2187	0	309.4444444	723.8124949	2699	2	804.4444444	992.1703623	24073	129264	515891.8824	2046138.948	8455316
11	80	58353645	15	1	656	0	339	0	43.73333333	115.486837	0	0	0	0	11.24179989	0.274190241	3890243	10600000	37900000
12	443	121	2	0	37	0	37	0	18.5	26.1629509	0	0	0	0	152366	118487	121	0	121
13	443	86	2	0	12	0	6	6	6	0	0	0	0	0	50448	151369	86	0	86
14	80	1386199	7	1	636	0	318	0	90.85714286	155.1681116	0	0	0	0	458.8085838	5.771177154	198028.4286	362956.9425	997977
15	80	232793	10	1	320	0	320	0	32	101.1928851	0	0	0	0	1374.61178	47.25227992	23279.3	57295.96642	185387
16	53739	113935	2	1	12	6	6	6	6	0	6	6	6	0	67749	156370	56967.5	80534.51263	113914
17	53	165	2	2	106	234	53	53	53	0	117	117	117	0	105794	153169	55	89.20201791	158
18	80	10207169	9	9	5364	6212	2682	0	596	1182.650836	1658	0	690.2222222	821.8633977	23134	83233	600421.7059	2421765.138	9997951
19	53	188	2	2	46	46	23	23	23	0	23	23	23	0	218640	147200	62.66666667	106.8097998	186
20	80	55489	5	3	435	283	435	0	87	194.537914	283	0	94.33333333	163.3901262	40452	110552	7927	10799.67035	23318
21	80	222875	1	1	0	0	0	0	0	0	0	0	0	0	0	8.973639933	222875	0	222875
22	80	184635	8	1	340	0	340	0	42.5	120.2081528	0	0	0	0	1841.47101	48.74482086	23079.375	51657.58731	147344
23	80	253421	7	1	366	0	366	0	52.28571429	138.3349971	0	0	0	0	1444.23706	31.56802317	36203	76067.54822	208418
24	80	106650912	15	1	346	0	346	0	23.06666667	89.33681585	0	0	0	0	3.244229173	0.150022158	7110060.8	25600000	99500000
25	80	65219872	11	1	701	0	355	0	63.72727273	141.7985126	0	0	0	0	10.74825783	0.183993001	5929079.273	19200000	63700000
26	53	617	2	2	252	252	126	126	126	0	126	126	126	0	297515	217442	205.6666667	351.0289637	611
27	80	3180597	12	1	369	0	369	0	30.75	106.5211247	0	0	0	0	116.0159555	4.087282985	265049.75	615946.7991	1990397
28	53	24479	2	2	66	196	33	33	33	0	98	98	98	0	15608	117866	8159.666667	14088.80791	24428
29	80	1525257	8	1	279	0	279	0	34.875	98.64139598	0	0	0	0	182.9199932	5.90064494	190657.125	350898.7537	1013069
30	389	85847574	20	10	4030	3160	403	0	201.5	206.7346379	316	316	316	0	299785	34581	2960261.172	12557802.55	65184542

Fig.4 Cyber D-DoS Attack Data Set [31]

Data set

The Canadian Institute of Cyber security (CICIDS2017) Intrusion Detection Evaluation Data set is utilized for design training and evaluation Numerous threats, such as DDoS as well as bot net activity are documented in the report. We used the DoS data set as the basis for our classification model in this study. There are 84 variables in each flow record in the CICIDS 2017 dataset, which is in comma-separated (.CSV) format. Detailed information about each variable can be found. The fields flow ID, date, source, and destination IP addresses are deleted from the flow data used for our categorization because they may bias the training process [29]. As a result, a complete data set of 80 features were picked for categorization. Except for the benign traffic, the flow records are labeled as 'Slowloris, Slow http test, Hulk, and Begin' according to the tools used. Five distinct integer values reflect the 'Benign, Slowloris, Slow HTTP, as well as Hulk' flows, each of which is assigned a numerical value between 1 as well as 5.

Result Parameters

There are different result parameters are observed in cyber D-DoS attack.

Accuracy (Acc):

Accuracy is a measure of how many right products are added to the total (TP+TN) and total number of production (TP + TN + FP + FN) .

$$\text{Acc} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \qquad (15)$$

Precision (P):

$$P = \sum\left(\frac{tp}{tp + fp}\right) \times 100 \qquad (16)$$

Sensitivity (Se)

$$Se = \sum\left(\frac{tp}{tp + fn}\right) \times 100 \qquad (17)$$

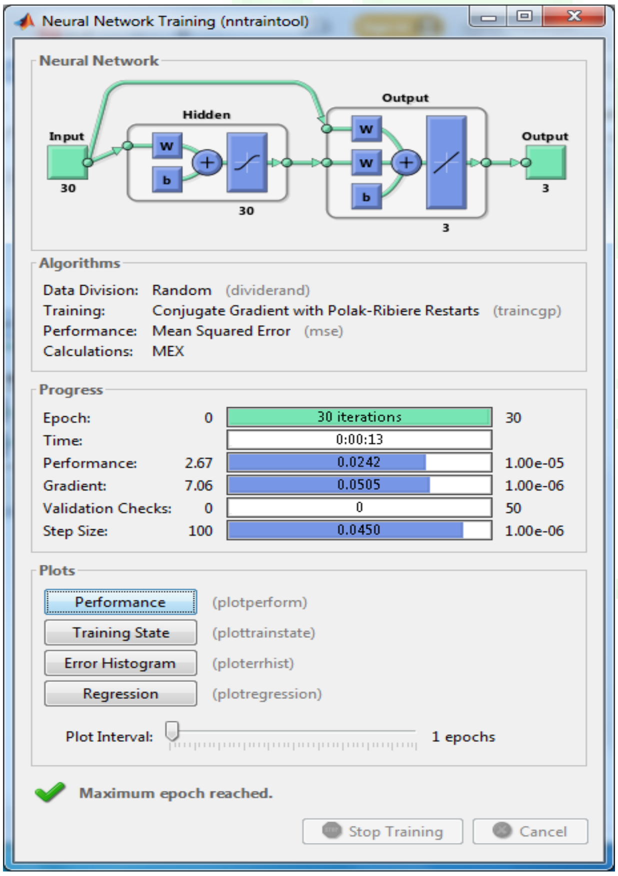
Specificity (Sp)

$$Sp = \sum\left(\frac{tp}{tn + tp}\right) \times 100 \qquad (18)$$

Where:
Tp = True positive;
fp = False positive;
tn = True negative;
Fn = False negative.

Simulation Outcomes

There's a neural network (NN) experiment depicted in the below fig.5. A total of thirty input features are used in this algorithm. For training use conjugate gradient with polok Ribiere. Performance measured by mean square error [26] [27] and thirteenth second time taken for training.



Algorithms
Data Division: Random (dividerand)
Training: Conjugate Gradient with Polak-Ribiere Restarts (traincgp)
Performance: Mean Squared Error (mse)
Calculations: MEX

Progress

Epoch:	0	30 iterations	30
Time:		0:00:13	
Performance:	2.67	0.0242	1.00e-05
Gradient:	7.06	0.0505	1.00e-06
Validation Checks:	0	0	50
Step Size:	100	0.0450	1.00e-06

Plots
Performance (plotperform)
Training State (plottrainstate)
Error Histogram (ploterrhist)
Regression (plotregression)
Plot Interval: 1 epochs

✓ Maximum epoch reached.

Stop Training Cancel

Fig.5 NN simulation model

Number of Epoch = 30, To train the suggested system, a feed-forward network is employed. There are three levels in feed forward, the first of which is the input data, which has 30 input nodes. One of these layers is referred to as a "hidden layer, and the other is referred to as an output layer".

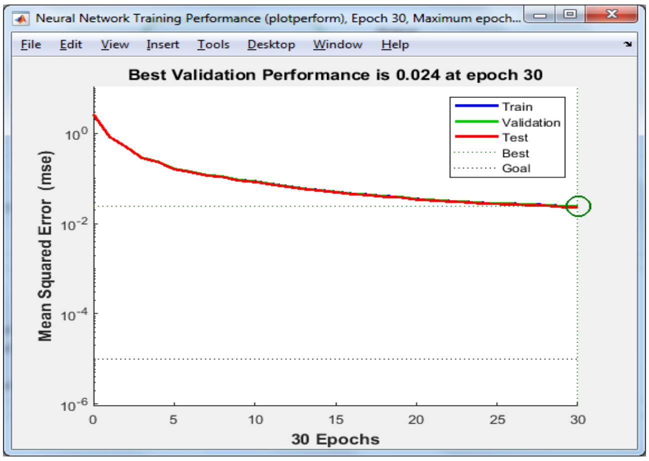


Fig**. 6: Output of training validation performance**

In the above fig. 6 shows the training, testing and validation of the proposed DDoS attack. Optimum result is occurring at 30 epochs with best validation performance at 0.024.The other performance parameters are also measured of proposed method.

TABLE I. EXPERIMENTAL RESULTS 1

Proposed Accuracy (Acc)	99.12
Acc. hybrid	98.6070
True Positive	318 274 94
False Negative	0 4 3
False Positive	3 3 1
True Negative	372 412 595

Confusion Matrix (C.M.) -

	Classes	Slowloris	Slowhttptest	Hulk
True Label	Slowloris	318	0	0
	Slowhttptest	3	274	1
	Hulk	0	3	94
	Predicted Label			

TABLE II. EXPERIMENTAL RESULTS 2

S.No.	**Performance Analysis**	
	1 ***Parameter***	2 ***Outcome***
1.	Accuracy	99.9685
2.	Precision	98.9766
3.	Selectivity	98.9766
4.	Sensitivity	98.4895

In the above table I and II shows the result of DDoS attack detection in Canadian Institute of cyber security Intrusion Detection (CICIDS2017) data set. Now discuss the result comparison of proposed method with the different previous methods.

TABLE III. RESULT COMPARISON

S.No.	Year/Ref.	Method	Accuracy (%)	Data set [31]
01	2022/ Proposed	Polak–Ribière–Polyak Based CFFNN	**99.961%**	CICID S2017
02	2022/ [29]	Bayesian Regularization Neural network	99.056%	CICID S2017
03	2020/ [30]	CNN and LSTM	99.035%	CICID S2017

.

IV. CONCLUSION

This research work presented a Polak–Ribière–Polyak (PRP) with cascaded feed forward network based machine learning approach for D-DoS attack detection. The proposed approach has been evaluated on the NSL-KDD dataset, which is a widely used benchmark dataset for DDoS attack detection. The experimental results demonstrate that the proposed approach achieves high accuracy in detecting DDoS attacks, with an accuracy of over 99% and a low false positive rate. In conclusion, the PRP algorithm-based CFFNN approach is an effective method for detecting cyber DDoS attacks. The proposed approach has demonstrated high accuracy and low false positive rate in experiments conducted on the NSL-KDD dataset. The approach can be further improved by incorporating other optimization techniques or neural network architectures to achieve even better performance.

REFERENCES

[1] Niu Varghese, Josy Elsa, and Balachandra Muniyal. "An Efficient IDS Framework for DDoS Attacks in SDN Environment." IEEE Access 9 (2021): 69680-69699.

[2] Hussain, Bilal, Qinghe Du, Bo Sun, and Zhiqiang Han. "Deep learning-based DDoS-attack detection for cyber–physical system over 5G network." IEEE Transactions on Industrial Informatics 17, no. 2 (2020): 860-870.

[3] Alhaidari, Fahd A., and Ezaz Mohammed AL-Dahasi. "New approach to determine DDoS attack patterns on SCADA system using machine learning." In 2019 International Conference on Computer and Information Sciences (ICCIS), pp. 1-6. IEEE, 2019.

[4] Dong, Shi, and Mudar Sarem. "DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks." IEEE Access 8 (2019): 5039-5048.

[5] Su, Lei, and Dan Ye. "A cooperative detection and compensation mechanism against denial-of-service attack for cyber-physical systems." Information Sciences 444 (2018): 122-134.

[6] Prakash, Aditya, and Rojalina Priyadarshini. "An intelligent software defined network controller for preventing distributed denial of service attack." In 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), pp. 585-589. IEEE, 2018.

[7] Adat, Vipindev, and B. B. Gupta. "A DDoS attack mitigation framework for internet of things." In 2017 international conference on communication and signal processing (ICCSP), pp. 2036-2041. IEEE, 2017.

[8] He, Zecheng, Tianwei Zhang, and Ruby B. Lee. "Machine learning based DDoS attack detection from source side in cloud." In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 114-120. IEEE, 2017.

[9] Razak, T. Abdul. "A study on IDS for preventing denial of service attack using outlier’s techniques." In 2016 IEEE International Conference on Engineering and Technology (ICETECH), pp. 768-775. IEEE, 2016.

[10] Guo, Yonghe, Chee-Wooi Ten, Shiyan Hu, and Wayne W. Weaver. "Modeling distributed denial of service attack in advanced metering infrastructure." In 2015 IEEE power & energy society innovative smart grid technologies conference (ISGT), pp. 1-5. IEEE, 2015.

[11] Devi, BS Kiruthika, G. Preetha, G. Selvaram, and S. Mercy Shalinie. "An impact analysis: Real time DDoS attack detection and mitigation using machine learning." In 2014 International Conference on Recent Trends in Information Technology, pp. 1-7. IEEE, 2014.

[12] Sivabalan, Sujatha, and P. J. Radcliffe. "A novel framework to detect and block DDoS attack at the application layer." In IEEE 2013 Tencon-Spring, pp. 578-582. IEEE, 2013.

[13] François, Jérôme, Issam Aib, and Raouf Boutaba. "FireCol: a collaborative protection network for the detection of flooding DDoS attacks." IEEE/ACM Transactions on networking 20, no. 6 (2012): 1828-1841.

[14] Sangwan, Munesh, Gopal Panda, and Pranay Yadav. "A Literature Survey on Different MIMO Patch Antenna." In 2020 International Conference on Inventive Computation Technologies (ICICT), pp. 912-918. IEEE, 2020.

[15] Musumeci, Francesco, Valentina Ionata, Francesco Paolucci, Filippo Cugini, and Massimo Tornatore. "Machine-learning-assisted DDoS attack detection with P4 language." In ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1-6. IEEE, 2020.

[16] Yadav, Satyajit, and Selvakumar Subramanian. "Detection of Application Layer DDoS attack by feature learning using Stacked AutoEncoder." In 2016 international conference on computational techniques in information and communication technologies (icctict), pp. 361-366. IEEE, 2016.

[17] Shabtai, Asaf, Uri Kanonov, Yuval Elovici, Chanan Glezer, and Yael Weiss. "“Andromaly”: a behavioral malware detection framework for android devices." Journal of Intelligent Information Systems 38, no. 1 (2012): 161-190.

[18] Huang, Vincent Shi-Ming, Robert Huang, and Ming Chiang. "A DDoS mitigation system with multi-stage detection and text-based turing testing in cloud computing." In 2013 27th international conference on advanced information networking and applications workshops, pp. 655-662. IEEE, 2013.

[19] Yadav, Pranay, Shachi Sharma, Prayag Tiwari, Nilanjan Dey, Amira S. Ashour, and Gia Nhu Nguyen. "A Modified Hybrid Structure for Next Generation Super High Speed Communication Using TDLTE and Wi-Max." In *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*, pp. 525-549. Springer, Cham, 2018.

[20] Yadav, Pranay, Alok Upadhyay, V. B. Prasath, Zakir Ali, and Bharat Bhooshan Khare. "Evolution of Wireless Communications with 3G, 4G, 5G, and Next Generation Technologies in India." In *Advances in Electronics, Communication and Computing*, pp. 355-359. Springer, Singapore, 2021.

[21] Tiwari, Sandeep, Nitesh Gupta, and Pranay Yadav. "Diabetes Type2 Patient Detection Using LASSO Based CFFNN Machine Learning Approach." In *2021 8th International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 602-608. IEEE, 2021.

[22] Pranay Yadav, Nishant Chaurasia, Kamal Kumar Gola, Vijay Bhasker Semwan, Rakesh Gomasta, Shivendra Dubey. ”A Robust Secure Access Entrance Method Based on Multi Model Biometric Credentials Iris and Finger Print”. *3rd International Conference on Machine Learning, Image Processing, Network Security and Data Sciences*, MIND-2021.

[23] Sharma, Bharti, Sachin Kumar, Prayag Tiwari, Pranay Yadav, and Marina I. Nezhurina. "ANN based short-term traffic flow forecasting in undivided two lane highway." *Journal of Big Data* 5, no. 1 (2018): 1-16.

[24] Maurya, Sweta, Shilpi Sharma, and Pranay Yadav. "Internet of Things based Air Pollution Penetrating System using GSM and GPRS." In *2018 International Conference on Advanced Computation and Telecommunication (ICACAT)*, pp. 1-5. IEEE, 2018.

[25] Chavate, Shrikant, Ravi Mishra, and Pranay Yadav. "A Comparative Analysis of Video Shot Boundary Detection using Different Approaches." In *2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART)*, pp. 1-7. IEEE, 2021.

[26] Yadav, Pranay. "Color image noise removal by modified adaptive threshold median filter for RVIN." In *2015 International Conference on Electronic Design, Computer Networks & Automated Verification (EDCAV)*, pp. 175-180. IEEE, 2015.

[27] Sharma, Shachi, and Pranay Yadav. "Removal of fixed valued impulse noise by improved Trimmed Mean Median filter." In *2014 IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1-8. IEEE, 2014.

[28] Semwal, Vijay Bhaskar, Kaushik Mondal, and Gora Chand Nandi. "Robust and accurate feature selection for humanoid push recovery and classification: deep learning approach." *Neural Computing and Applications* 28, no. 3 (2017): 565-574.

[29] Akhil Mishra, Dr. Ritu Shrivastava, Pranay Yadav “A Modified Cascaded Feed Froward Neural Network Distributed Denial of Service Attack Detection Using Improved Regression Based Machine Leaning Approach”, *“6th International Conference on Trends in Electronics and Informatics (ICOEI 2022).*

[30] Roopak, Monika, Gui Yun Tian, and Jonathon Chambers. "An intrusion detection system against ddos attacks in iot networks." In *2020 10th annual computing and communication workshop and conference (CCWC)*, pp. 0562-0567. IEEE, 2020.

[31] https://www.kaggle.com/datasets/cicdataset/cicids2017/code