ACCURATE AND FAST DETECTION OF DDOS ATTACK PRESENCE BASED ON BURST TIME INSTANCES

R. Rathika M.Sc., MCA, M.Phil., (Ph.D)., Research Scholar, PG and Research Department of Computer Science, Government Arts College, Coimbatore, Tamilnadu.

Dr.A. Marimuthu MCA., MBA., M.Phil, Ph.D., Associate Professor & HOD, PG and Research Department of Computer Science, Government Arts College, Coimbatore, Tamilnadu.

ABSTRACT

On the real network environment, DDOS attacks causes network corruption or whole network failure. In order to safeguard the network from failure, DDOS attack detection and prevention has to be performed. In the earlier work, DDOS attack detection and prevention is performed by bringing-in the method known as Feature Learning based DDOS Attack Detection (FL-DDOS-AD), its primary target is to identify the existence of the DDOS attack on the network perfectly. Nevertheless, the current work may be disgraced in its execution, because of rupture in transmission of data. And also current work fail to identify the DDOS attack, if there occur the non-constant variance among the packets that are transmitted. So, it is rectified in the proposed by bringing-in the method called Burst Transmission aware DDOS Attack Detection (BT-DDOSAD) method. Its primary target is to bring-in the new research techniques, which can identify the existence of DDOS attack in the network perfectly. So, different algorithms have to be established for accurate detection outcome. Along with the timing serious values (such as type of protocols, TTL values, geo-location of reflective IPs, etc.), burst time instances also has to be assumed in our work. In the suggested work, an enhanced box Cox transformation is enforced to execute the preprocessing to make data set cleaner for normal effective processing. In the NS2 simulation environment,the implementation of the presented research technique is done, which confirms that the recommended work assures the optimal performance whiledifferentiated with the present research techniques.

Keywords: DDOS attack detection, Burst transmission of data, Packet normalization, and Non constant variance

I. INTRODUCTION

For network, digital, and cyber infrastructure, Distributed denial-of-service (DDoS) attacks have been a real threat [1]. These attacks have the ability to create enormoustrouble in any information communication technology (ICT) infrastructure [2]. We have many reasons for launching the DDoS attacks. These involves financial gains [3], political gains, and disruption [4,5]. DDoS attacks can be a paralyze networks and services by overwhelming servers, network links, and network devices (routers, switches, etc.) with illegitimate traffic. This results in the deterioration of service or a complete denial of service resulting in huge losses. Maximization of reliance on Internet and data centers has provoked this issue. The requirement for an effective efficient solutions for protection against DDoS attacks [6,7], due to the increase in dependence of critical infrastructure of a country in ICT. For example, a data center running critical services, like smart grid, requires to be safeguarded to proceed highly reliable services.

For DDoS attack identificationas well as mitigation, various proprietary and open-source solutions prevails. Nevertheless, these attacks proceed to develop in frequency, sophistication, and severity [8,9]. Rapid identificationas well asmitigation of DDoS attacks has become extremely dispute as attackers continue to utilize the novel techniques to launch DDoS attacks [10]. The increase in DDoS attacks, gets coupled with growing diversity in their types, that creates causing disastrous impact, has made DDoS attack identification, mitigation, and prevention the top-most priority.

For example, Arbor Networks Inc. [11], is one of the leading DDoS threat protection solutions provider, stated a 334Gbps attack targeting a network operator in Asia recently. Also, it states various attacks, whichare higher than 100Gbps globally in 2015 [12]. Various eventstell that we require approaches to mention the DDoS attack problem. These approaches should be planned to fulfill the performance and scalability requirements of modern data centers and it should give maximum levels of protection against emerging, complex and elusive, attacks.

Burst Transmission aware DDOS attack Detection (BT-DDOSD) method is suggested in our work, its target is to bring-in the novel research techniques, in order to identify the existence of DDOS attack present in the network accurately. So, different algorithms have to be established for accurate detection outcome. Along with the timing serious values (such as type of protocols, TTL values, geo-location of reflective IPs, etc.), burst time instances also has to be assumed in our work. In the suggested work, an enhanced box Cox transformation is enforced to execute the preprocessing to make data set cleaner for normal for effective processing. The implementation of the proposed research method is done in the NS2 simulation environment, which confirms that the suggested work assures the optimal performance when distinguished with the current research techniques.

The research work is systemized as follows: In this section, precise explanation about the DDOS attacks and their causes has been explained. In section 2, different related research methodologies which are brought-in to identify and safeguard the DDOS attacks has been explained in detailed. In section 3, proposed research method has been explained in detail with respect to their working procedure and appropriate examples and explanation. In section 4, execution and result evaluation has been given with respect to the acquired result. Finally in section 5, final conclusion of the research method is provided according to the acquired results.

II. RELATED WORKS

WE have different attack detection and defense mechanisms for DDoS attack detection. In terms of to detection time and accuracy, we have two groups of DDoS attack detection techniques. One group is offline-based and the other one is online-based.

Typically, for offline detection approaches, it is divided into two groups as specific detection and anomaly based detection. In orderto confirm whether supervised traffic contain special attack features, Specific detection makes use of rule-match approaches [13]. The rule-match techniques are controlled in keeping with the flow state as well as matching packets to a pre-defined collection of rules [14] has shown a specific good capability. Nevertheless, rule-match techniques unlikely identify unknown DDoS attacks. For earlier unknown DDoS attacks, anomaly-based detection has higher accuracy when compared with the rule-match approach.

Anomaly-based detection designs the nature of normal traffic and addresses the anomalies if any. The accuratenessas well asefficacy in identifying network-wide traffic behavior irregularities, is explained by PCA, entropy and subspace approaches.Lakhinaet a1. [15] Utilizes maximum and relative entropy and subspace to mine and examine the traffic anomalies. Ringerget a1. In order to examine the origin-destination flow aggregation as well as entropy time series of traffic features,[16] Utilized PCA (principal Component Analysis). Nevertheless, these network-wide anomaly detection as well as machine-learning techniques were executed offline. Hence, it is tedious for them to have preventive measures for DDoS attacks.

The on-line identificationmethods were given much attention, for real-timely detect as well as defense DDoS attacks. Typically, on-line detection methods were statistical approaches concerning traffic feature as well as behaviors. Therefore, memory consumption,computation and detection time the major concern regarding on-line detection. Wang et a1. [17] Suggested a behavioral-distance based anomaly detection technique.

In order to find out the network security issues in home and office networks with the help of SDN,Mehdi et al. [18] makes use of maximum entropy estimation predict the benign traffic distribution. Traffic is classified into packet classes as well as maximum entropy estimation is utilized to establish the baseline benign distribution for every class. . Packet classes works on the protocols and destination port numbers. Experiments were done with the help of OpenFlow switches and a NOX controller. Nevertheless, the authors only utilize the low rate network traffic to conduct the implementation as they were concentrated much on a home environment.

Giotis et al. [19] executed an extremely utilized entropy based approach to efficiently identify DDoS, worm propagation, and ports can attacks. The flow-related traffic features helps to identify the anomolies are source and destination IP addresses and ports. Predefined thresholds are modified in the entropy values, which are utilized to detect the existence of anomalies.

Self-organizing map, which is the famous neural network models, utilized by Braga et al. [20] for identification of DDoS attacks. This work provided SDN-centered DDoS attack detection based on six traffic flow features. These features involves Average of Packets per flow (APf), Average of Bytes per flow (ABf), Average of Duration per flow (ADf), Percentage of Pair-flows (PPf), Growth of Single-flows (GSf) and Growth of Different Ports (GDP).

III. ACCURATE AND FAST DETECTION AND PREVENTION OF DDOS ATTACK

Burst Transmission aware DDOS attack Detection (BT-DDOSD) method is suggested in this work for rapid and exact identification of DDOS attacks, its primary target is to bring-in the new research techniques, which can identify the existence of DDOS attack in the network perfectly. So, different algorithms have to be established for accurate detection outcome. Along with the timing serious values (such as type of protocols, TTL values, geo-location of reflective IPs, etc.), burst time instances also has to be assumed in our work. In the suggested work, an enhanced box Cox transformation is enforced to execute the preprocessing to make data set cleaner for normal for effective processing. The steps proceeded in the suggested research works were listed as follows:

- Feature Extraction
- Data Preprocessing using improved Box Cox Transformation

- Learning using SVM learning technique

The description of the presented research technique is provided in the subsequent sub sections,

3.1. FEATURE SELECTION

Though there is no negotiation on what kind of traffic should be inspected as ”abnormal”, the conventional approaching is that the traffic created by DDoS attacks characteristically shows few unique features. Alike the load measurements explained above, a distributed set of probes is used for feature extraction. Significantly it doesn’t focus on a solitary set of characteristics nevertheless; it makes use of a set of probes to take out characteristics from a variety of protocol layers. In this research method burst time instances also assumed along with the timing serious values (such as type of protocols, TTL values, geo-location of reflective IPs, etc.).

PROTOCOL TYPES:

Network Protocol is a collection of rules that rules the interactions among computers on a network. A rule of Network Protocol involves guidelines that control the subsequentfeatures of a network: allowed physical topologies, access method,kinds of cabling, and speed of data transfer. The most general network protocols are:

- Local Talk
- Ethernet
- FDDI
- Token Ring
- ATM

AS determined in the OSI model,the protocol for data communication fills entire areas. Nevertheless, OSI model is just loosely defined. A protocol could execute the work of one or numerousOSI layers that brings-in the difficulty of accepting protocols which are appropriate to the OSI 7 layer model. We have few arguments as to where the distinctions among the layers are drawn in real-world protocols; there is no one black as well as white answer.

To establish the entire technology, which are helpful for the industry frequently a set of protocols is necessary in the similar layer or crosswisenumerousdiverse layers. Various protocols frequently explain various features of an individual communication; taken together, these produce a protocol suite. For instance, Voice over IP (VOIP), a set of protocols established by various vendors as well as standard organizations, and,in the OSI model, it has various protocols crosswise the 4 top layers. Protocols are executed in hardware or software or a combination of both. Generally, the lower layers were executed in hardware, with the higher layers being executed in software.

TTL VALUES:

Time-to-live (TTL) is known as a value in an Internet Protocol (IP) packet, which limits the life expectancy of a packet of data in a computer or network. Itdescribes a network router whether or not the packet is in the network extensively and it must be detached. In case of IPv6 the TTL field in every packet was renamed the hop limit. Initially,an IP TTL is fixed by the system transferring the packet. It is set to any value amongst 1 and 255; numerousOS set several defaults. Each router, which gets the packet subtracts as a minimum 1 from the count; when the count remainsabove 0, the router sends the packet, otherwise it remove it as well astransfers an Internet Control Message Protocol (ICMP) message back to the originating host that might trigger a resend.

In order to attain a provided host computer or to trace a route to that host,the ping as well as the traceroute utilize the TTL value. Traceroute transfers a collection of packets with consecutively higher TTLs as a resultallwould be removedin sequence by the next hop (router) on the route to the destination: The first packet contains a TTL of one as well as is removedby the first router; the second contains a TTL of two and is removedby the next router, etc. The time consumedamidthe transfer of packet as well as receiving back the ICMP message would beremoved and it is utilized to compute eachconsecutive hop travel time. In IP multicast, the TTL manages the scope or range wherein a packet could be sent. By convention:

- 0 is restricted to the same host
- 1 is restricted to the same subnet

- 32 is restricted to the same site
- 64 is restricted to the same region
- 128 is restricted to the same continent
- 255 is unrestricted

GEO-LOCATION OF REFLECTIVE IP:

Geolocation is known as the detection or prediction of the real-life geographic location of an object, like a mobile phone, radar source, or Internet-connected computer terminal. In its normal form geolocation, includes the generation of a set of geographic coordinates and is firmly works according to the utilization of positioning systems, on the other hand its helpfulness is improved with the help of coordinates to define a significant location namely a street address.

The locating engine utilizes radio frequency (RF) location approaches, for geo-locating or positioning (forinstance Time Difference Of Arrival (TDOA) for precision). A TDOA system utilizes mapping displays or other geographic info system. In order to triangulate the approximate position, geolocation applications utilizes the information from cell towers,while a GPS signal is inaccessible,a technique that isn't appropriate as GPS on the other handsignificantly enhanced recently. As a conflicting to the previous radiolocation technologies, e.g.: finding out the Direction, in which a line of bearing to a transmitter is done as part of the process.

Internet as well as computer geolocation is executed by means ofintegrating the geographic location with the Internet Protocol (IP) address, RFID, MAC address, embedded software number (like UUID, Exif/IPTC/XMP or modern steganography),hardware embedded article/production number, invoice, device fingerprint, canvas fingerprinting or device GPS coordinatesWi-Fi positioning system, , or other, possibly self-disclosed info. Geolocation generally operate by automatically searching for an IP address on a WHOIS service as well as retrieving the registrant's physical address.

IP address location data couldcompriseinformationsuch as region, country, postal/zip code,city, latitude, longitude and time zone. Deeper data sets could define the remaining parameters such as connection speed, domain name,ISP, proxies, language, US DMA/MSA, company name, NAICS codes, and home/business.

Now and then, geolocation could be more deductive, as with crowdsourcing efforts to describe the position of videos of training camps, combats, and beheadings in Syria by distinguishing the features identified in the video with publicly available map databases like Google Earth, as trained by sites for instance Bellingcat.

3.2. DATA PREPROCESSING USING IMPROVED BOX COX TRANSFORMATION

The Box-Cox transformation is utilized as a modesttechnique of transforming dependent variable in ordinary-linear regression circumstances for enhancing the Gaussian-likelihood fit as well as producing the disturbance terms of a model sensibly homoscedastic. But it delimits the sample space of the transformed variable with the intension that it isn't reliable with the consideration that the transformed variable is normally distributed. Hence in its practical applications we shouldconsider that the existing observations stay in that range or that they take huge positive values.

Here Improved Box-Cox transformation is suggested thatcontains the advantage that, when it keeps the foremostfeatures of the original Box-Cox transformation, the transformed variable contains the range (−∞, ∞) with the intension that the transformation is reliable with the normality supposition. For positive numbers x and α, set $\rho(x,\alpha)= (\log x-\log \alpha)/ \log x$; then define $x^{[\lambda]}$ for the cases (i) λ = 0,(ii) λ>0,(iii) λ<0, correspondingly by

$$\text{(i) } x^{[\lambda]} = \log x$$

$$\text{(ii) } x^{[\lambda]} = \begin{cases} \rho(x,\delta)\left(\log x + \frac{\delta^{\lambda}-1}{\lambda} - \log\delta\right) + \frac{(1-\rho(x,\delta))(x^{\lambda}-1)}{\lambda}, & \text{if } 0 < x \le \delta \\ \frac{(x^{\lambda}-1)}{\lambda} & \text{if } x > \delta \end{cases}$$

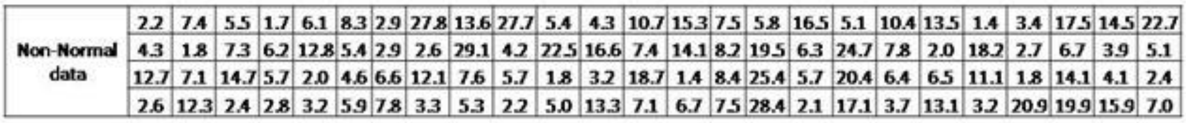
$$\text{(Iii) } x^{[\lambda]} = \begin{cases} \frac{(x^{\lambda}-1)}{\lambda} & \text{if } 0 < x \le M \\ \rho(x,M)\left(\log x + \frac{M^{\lambda}-1}{\lambda} - \log M\right) + \frac{(1-\rho(x,M))(x^{\lambda}-1)}{\lambda}, & \text{if } x > M \end{cases}$$

Whereδ and Mare positive numbers selected adequately small and large correspondingly. Note that $x^{[\lambda]}$ hence determined fulfills lim λ→0$x^{[\lambda]}$ = log *x* for any *x*, 0 < *x* < ∞,and also has the first derivative with respect to *x* in case λ>0 and 0 < *x* ≤δ, which is provided by

$$\frac{dx^{[\lambda]}}{dx} = \frac{\log\delta}{(\log x)^2 x}\left\{\log x - \frac{x^\lambda - 1}{\lambda} + \frac{\delta^\lambda - 1}{\lambda} - \log\delta\right\} + \frac{\log x - \log\delta}{\log x}\frac{1}{x} + \frac{\log\delta}{\log x}x^{\lambda-1}$$

and is seen to be continuous at *x* = δ,whereas,for λ<0 and x ≥ M, the derivative is provided by (2.1) withδsubstituted by M. Hence in either case the modified Box-Cox transformation is continuously differentiable over the domain 0 < *x* < ∞. The transformation *x*[*λ*] hence defined contains the advantage of mapping the collection of positive values onto (−∞,∞), and is exempt the constraint on the range imposed by the original Box-Cox transformation. Not only being formally consistent with the Gaussian error term that considers any value in the real line, it as well keeps numerous characteristics of the Box-Cox transformation by selecting δand Msuitably small as well as large correspondingly.It is attractive that the test result is less sensitive to a specific choice of δand M.

In the above equations, x represents an arbitrary observation and λ as parameter of power family of transformation indexed. If X has minimum, the X + λ1 can be made positive by the proper choice of λ1. Consider, we are measuring the variables x1, x2, x3, x4, x5, x6, x7, x8 and x9 respectively. That is x represents the attributes measured from the data transmission such as packet length, ip location, TTL and so on. These values would be converted into defined range by using the above mentioned equation. Here values of x and λ decides the proper conversion value range. As a first step, it would be wise to perform a primaryexamination of the data. In this research we follow the steps for detecting outlier data. E.g. a sample data (non-Normal data) that must be Box Cox transformed.



Non-Normal data	2.2	7.4	5.5	1.7	6.1	8.3	2.9	27.8	13.6	27.7	5.4	4.3	10.7	15.3	7.5	5.8	16.5	5.1	10.4	13.5	1.4	3.4	17.5	14.5	22.7
	4.3	1.8	7.3	6.2	12.8	5.4	2.9	2.6	29.1	4.2	22.5	16.6	7.4	14.1	8.2	19.5	6.3	24.7	7.8	2.0	18.2	2.7	6.7	3.9	5.1
	12.7	7.1	14.7	5.7	2.0	4.6	6.6	12.1	7.6	5.7	1.8	3.2	18.7	1.4	8.4	25.4	5.7	20.4	6.4	6.5	11.1	1.8	14.1	4.1	2.4
	2.6	12.3	2.4	2.8	3.2	5.9	7.8	3.3	5.3	2.2	5.0	13.3	7.1	6.7	7.5	28.4	2.1	17.1	3.7	13.1	3.2	20.9	19.9	15.9	7.0

Figure 1. Non normal data

The optimal l (Lambda) value is identified as 0 in this manner.

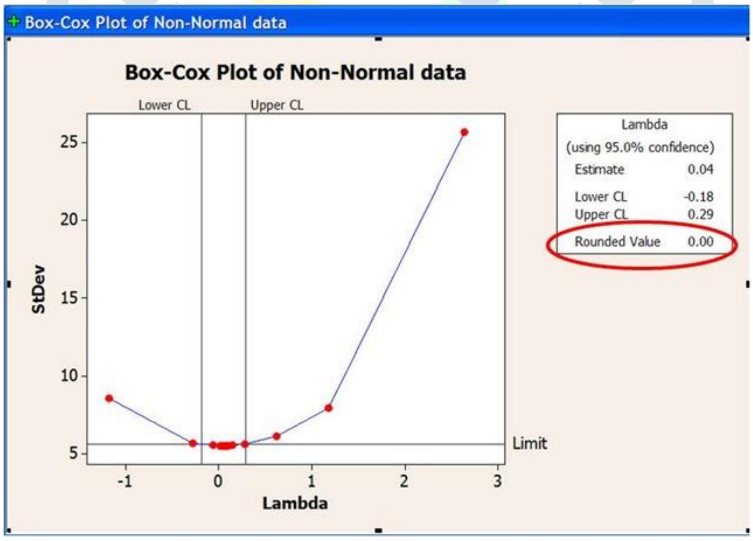


Figure 2. Box plot for non-normal data

The transformed data kept in C5 column on Minitab worksheet could be proceeded to verify that the normality reference below. The Pvalue> 0.05, specify the transformed data is Normally distributed as well as the transformation is effective.

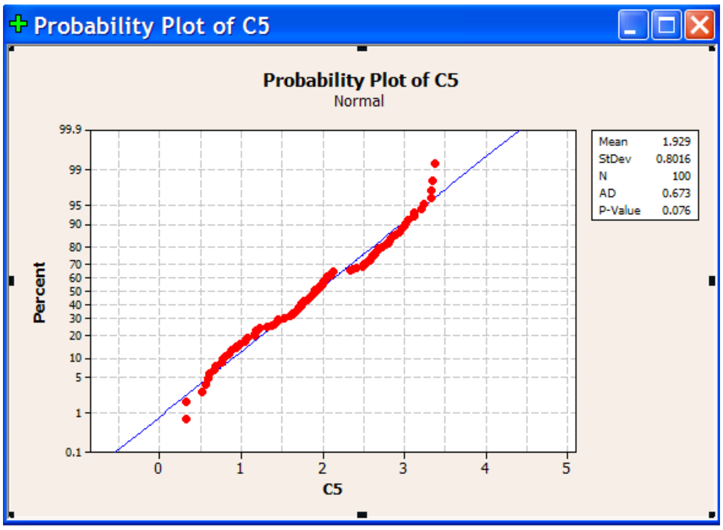


Figure 3. Box plot for transformed data

3.3. LEARNING USING SVM CLASSFIER

DDOS attack detection ratio is enhanced by bringing-in the machine learning techniques in the suggested work, such as Support Vector Machine, which will get the knowledge of features in the optimal way. Support vector machine (SVM) is a supervised algorithm and it is utilized for prediction for any provided data set. We make use of SVM, which is optimal secluding hyperplane amongst the two classes of data. SVM models helps to generate better prediction results.

Formula

Training dataset (D)

$D = \{x_i, y_i\}_{i=1}^{N}, \quad x \in R^n, y \in \{-1, 1\}$ (1)

D is training dataset, x and y is input variables

$y^i[|w^T x^i + b|] \geq 1 \quad$ i=1 to N (2)

w^T and b are separated variables

To reduce the error minimization we can use given below formula

$\Phi(w) = \frac{1}{2}||w||^2$ (3)

Estimating function

$F(x) = \sum_{i=1}^{nsv}(x_i, y_i)k(x_i, y_i) + b$ (4)

SVM Algorithm Procedure

Given network traffic information D=(x1, y1),……,(xn, yn), C // x and y –labeled samples as well as C-class

Initialize vector v=0, b=0; class) // v-vector and b-bias

Train an initial SVM and learn the model

For each $x_i \in X$ do // xi is a vector containing features describing example i

Classify x_i using f (x_i)

If y_i f (x_i) < 1 // prediction class label

```
Find $w', b'$ for known data   // $w', b'$ for new features

Add $x_i$ to known data

Minimize the error function using (3) and estimate using (4)

If the prediction is wrong then retrain

Repeat

End

Classify attributes as normal or abnormal
```

3.3.1. TRAINING SVM

Training data set involves four sub-sets, T0, T1, T2 and T3, which indicate Normal, Light, Medium, Heavy data correspondingly. There are 400 normal data in T0 and 300 attack data in T1, T2 and T3 severally. T1, T2 and T3 are mixed 3 kinds of attack dada, involving 100 SYN Flood, 100 UDP Flood and ICMP Flood data correspondingly based on the label. In a word, there are 1300 data in the training set. Extracting RLT and TRA features from the training set and training SVM correspondingly, we can get 2 × 6 SVMs, due to 1-v-1 SVM.

In supervised machine learning, when the training samples as well as the testing samples are alike, the accuratenessis made artificially high. Therefore, it is very important for these two types of samples to be different. We adopt the crossvalidation method to evaluate the accuracies of our experiment. In n-fold cross-validation technique, samples are split into n subsets of equivalent size. Sequentially, each subset is tested using the classifier trained on the remaining n-1 subsets. Thus, each instance of the whole training set is tested once and the overall cross-validation accuracy is the average across the entire data set. The prediction accuracy obtained by cross-validation is able to reflect the performance as classifying unknown data more precisely. In general, the value of n does not affect the crossvalidation accuracy much if it is small when compared to the number of samples in the entire data set. So, in the Internet traffic classification experimentation, n=10.

3.3.2. TESTING THE ATTACK DATA

To verify the training results, we execute two experiments and use two testing datasets. First dataset, has the category labels, and is gathered with the same way of training data. Second dataset comes from MIT Lincoln Lab and hasn't the category labels. There are 4 types of data, Normal, Light, Medium, Heavy, in experiment I, and every sort of dada includes 1200 data, sum is 4800.

IV. RESULTS AND DISCUSSION

In this work, we make use of NS-2 simulator to compute the performance of the proposed Burst Transmission aware DDOS attack Detection (BT-DDOSAD). Our simulations model a network comprises of 100 sensor nodes placed randomly within a 100 × 100 meters area. The two varieties of sensor nodes in the simulations are determined as: well-behaved nodes and malicious nodes. The malicious nodes can start DDOS attacks in the simulated cases. The BS has unlimited energy. The number of selected CH is fixed to 10% for one interval. The proposed system BT-DDOSAD performance is computed by distinguishing itwith the current system Feature Learning based DDOS Attack Detection (FL-DDOS-AD). The parameters utilized in this research for computing the trust system are provided in the Table 1. The performance of BT-DDOSAD model was computed by the following metrics like packet loss, packet delivery ratio, energy consumption, end-to-end delay, and mean packet latency.

Table 1 Simulation parameters

Simulation Parameters	Values
Channel	Wireless Channel
Mac	802.11
Antenna Type	Omni antenna
Routing Protocol	AODV
Initial Energy	100 joules

Traffic type	CBR
Agent	UDP
Simulation area	100X100 meters
Number of nodes	100

4.1. PACKET LOSS

The total number of data packets lost legitimately or through malicious action without any warning. Figure 4 provides the graphical indication of packet loss rate, it provides that the BT-DDOSAD method has lower packet loss rate when distinguished with the current systems FL-DDOS-AD.

Table 2. Packet loss comparison table

Time	Packet loss		
	Firecol	FL-DDOS-AD	BT-DDOSAD
10	0.19	0.14	0.06
20	0.37	0.27	0.11
30	0.5	0.4	0.22
40	0.62	0.54	0.33
50	0.74	0.65	0.43
60	0.85	0.75	0.52
70	0.93	0.88	0.57
80	1	0.8	0.6

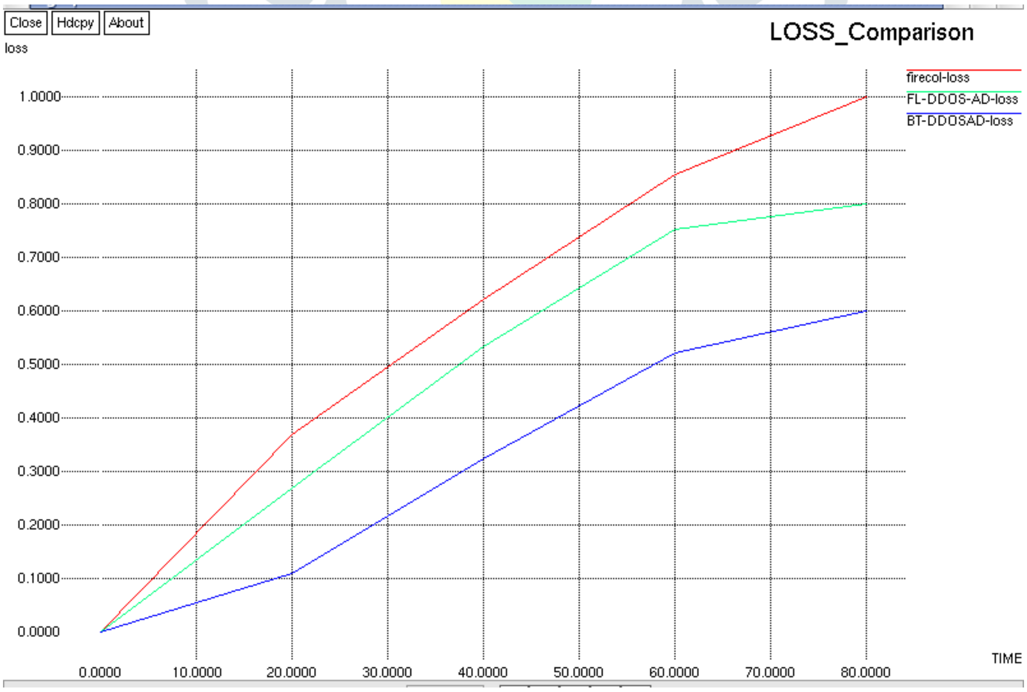


Figure 4 Comparison of packet loss in different trust model

The current system doesn’t concentrate much on difference among the genuine nodes and the malicious as it assumes every sensor node with high traffic deviation as the malicious. The proposed algorithm detects the individual malicious nodes according to the bias and variance value; hence the packet drop by the genuine nodes can be eliminated. The experimental outputprovides that proposed BT-DDOSAD have lesser packet loss rate when distinguished with the currentFL-DDOS-AD.

4.2. PACKET DELIVERY RATIO (PDR)

It is the proportion of the over-allamount of data packets received to the total number of data packets transmitted. This explains the level of delivered data to the destination.

Table 3. Packet delivery ratio comparison table

Time	Packet delivery ratio		
	Firecol	FL-DDOS-AD	BT-DDOSAD
10	0.25	0.3	0.35
20	0.5	0.6	0.7
30	0.66	0.75	0.9
40	0.8	0.9	1.1
50	0.9	1.04	1.2
60	1	1.16	1.3
70	1.15	1.27	1.4
80	1.26	1.4	1.5

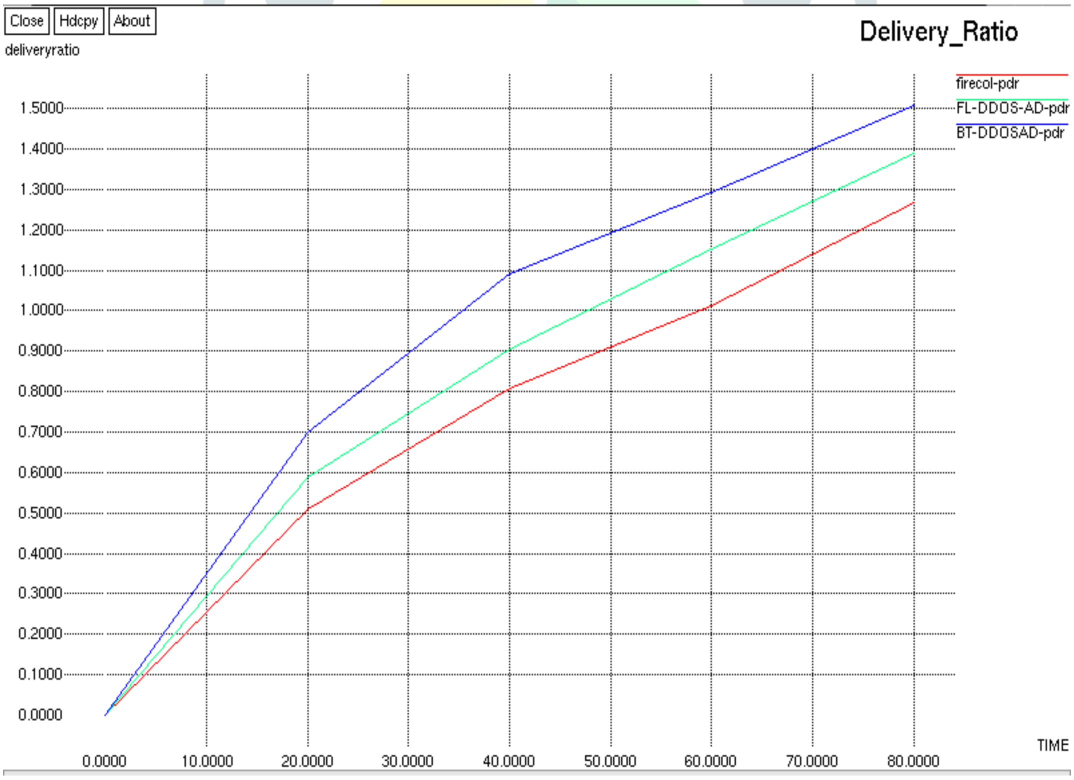


Figure 5 Comparison of packet delivery ratio for different trust system

Figure 5 provides the performance of the proposed BT-DDOSAD when distinguished with FL-DDOS-AD in terms of number of rounds and Packet Delivery Ratio (PDR). The number of packets which is efficiently received at the destination without the loss of any packets or failure for the proposed AF-FAIDS is high which provides higher PDR results.

4.3. ENERGY CONSUMPTION

The average energy consumed by every node at the time of the provided simulation time is expressed in Joules (J).

Table 4. Energy consumption comparison table

Time	Energy consumption		
	Firecol	FL-DDOS-AD	BT-DDOSAD
10	0.14	0.09	0.06
20	0.27	0.16	0.1
30	0.35	0.25	0.15
40	0.43	0.33	0.21
50	0.6	0.5	0.37
60	0.76	0.67	0.5
70	0.9	0.75	0.58
80	1.05	0.81	0.65

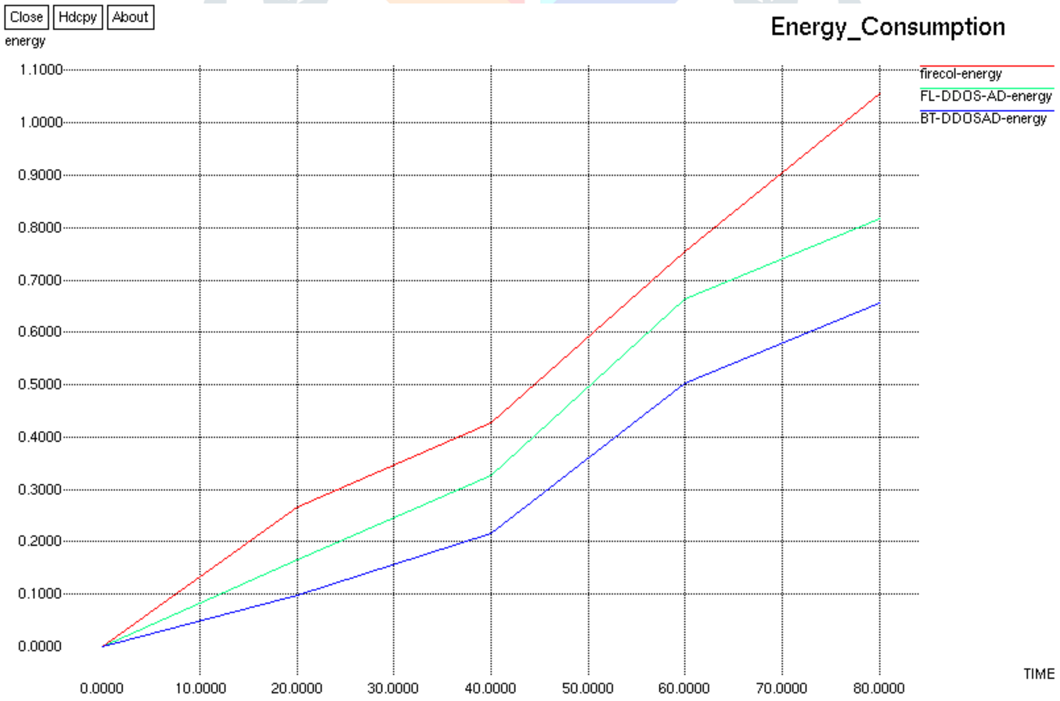


Figure 6 Comparison of energy consumption of different trust system

Figure 6 provides the graphical indication of energy consumption for various trust models in wireless sensor network of military applications. The BT-DDOSAD method has low energy consumption when distinguished with the current system FL-DDOS-AD.

4.4. END-TO-END DELAY

End-to-end points to the delay experienced by the data packet at the time of the transmission from source to BS, which involves processing, queuing and propagation delay. Figure 7 provides that the graphical indication of end-to-end delay for various trust models in wireless sensor network of military applications. If hop to hop count distance value is high, it gives high end to end Delay at the time of path communication. According to this hop to hop count distance data transmission is executed from source to destination in BT-DDOSAD system, so it shows less end to end Delay. As the proposed BT-DDOSAD system, high hop to hop count distance paths isn't considered as data transmission.

Table 5. End to end delay comparison table

Time	End to end delay		
	Firecol	FL-DDOS-AD	BT-DDOSAD
10	0.1	0.07	0.06
20	0.2	0.14	0.09
30	0.4	0.35	0.28
40	0.61	0.56	0.47
50	0.8	0.66	0.58
60	1	0.76	0.7
70	1.12	0.9	0.75
80	1.23	1.01	0.8

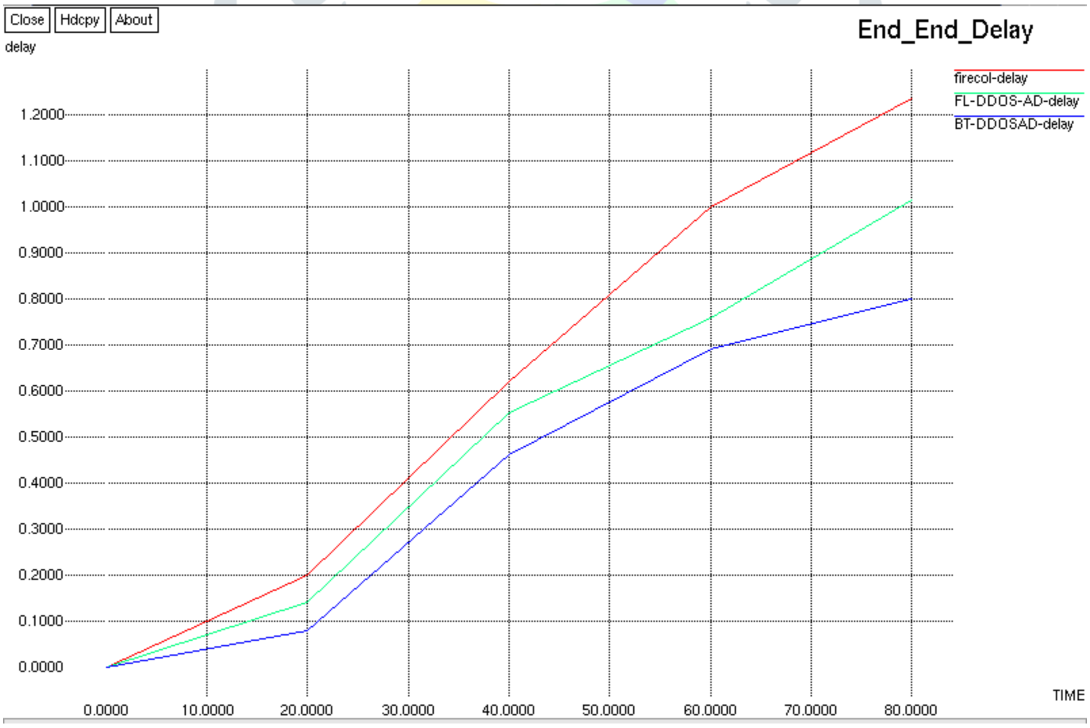


Figure 7 End-to-end delay comparisons for different trust system

The BT-DDOSAD method has low end-to-end delay when distinguished with the current system FL-DDOS-AD. Proposed BT-DDOSAD system, high hop to hop count distance paths isn't considered for data transmission and that path is assumed as attack path.

4.5. MEAN PACKET LATENCY

The mean packet latency for those packets that attained the destination is lower for BT-DDOSAD so it is competent of choosing the shortest route with the lowest number of hops. And also mean packet latency is minimized in the proposed methodology due to minimize the malicious attacks. The graphical chart of the mean packet latency is provided in the following Figure 8.

Table 6. Detection Time comparison table

Number of nodes	Detection time		
	Firecol	FL-DDOS-AD	BT-DDOSAD
5	0.3	0.25	0.2
10	0.62	0.5	0.4
15	0.74	0.66	0.47
20	0.87	0.8	0.56
25	1.03	0.9	0.73
30	1.2	1.01	0.9
35	1.3	1.15	0.95
40	1.39	1.25	1

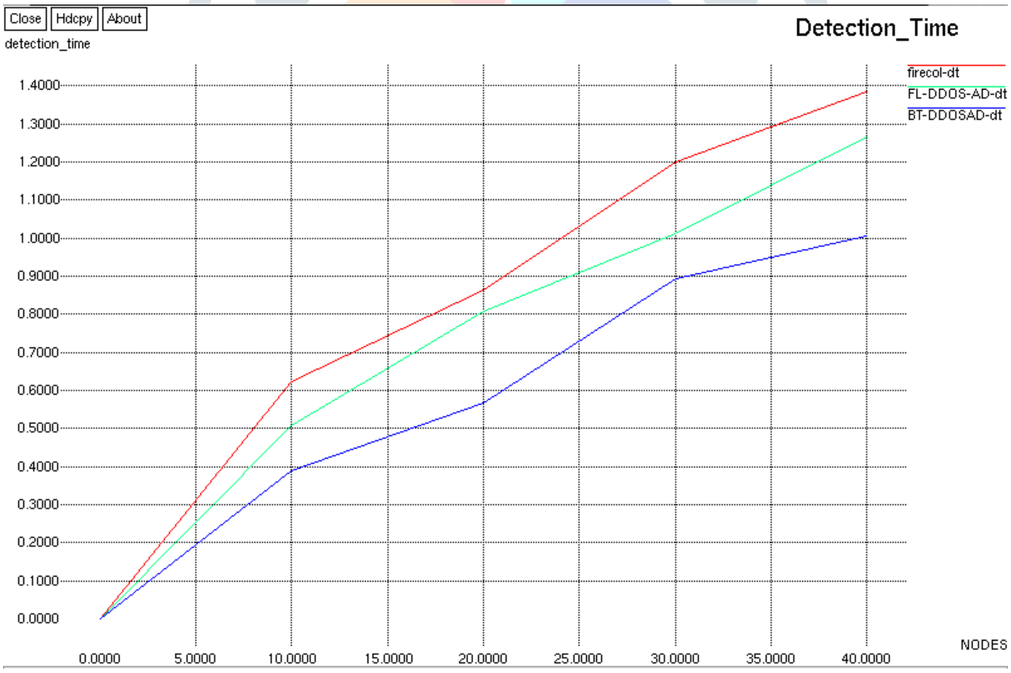


Figure 8 Mean packet latency

The BT-DDOSAD method has low packet latency when distinguished with the current system FL-DDOS-AD. Proposed BT-DDOSAD system, high hop to hop count distance paths isn’t considered for data transmission and that path is assumed as attack path.

4.6. ROUTING OVERHEAD

Routing overhead is defined as the computational overhead during routing process due presence of DDOS attacks. Routing overhead of the proposed research method would be lesser. The assessment of the research method in regard to routing overhead is depicted in the figure 9.

Table 7. Routing overhead comparison table

Time	Routing overhead		
	Firecol	FL-DDOS-AD	BT-DDOSAD
10	0.14	0.1	0.07
20	0.27	0.2	0.13
30	0.6	0.5	0.4
40	0.92	0.78	0.64
50	1.1	0.94	0.77
60	1.28	1.1	0.9
70	1.42	1.25	0.97
80	1.56	1.39	1.03

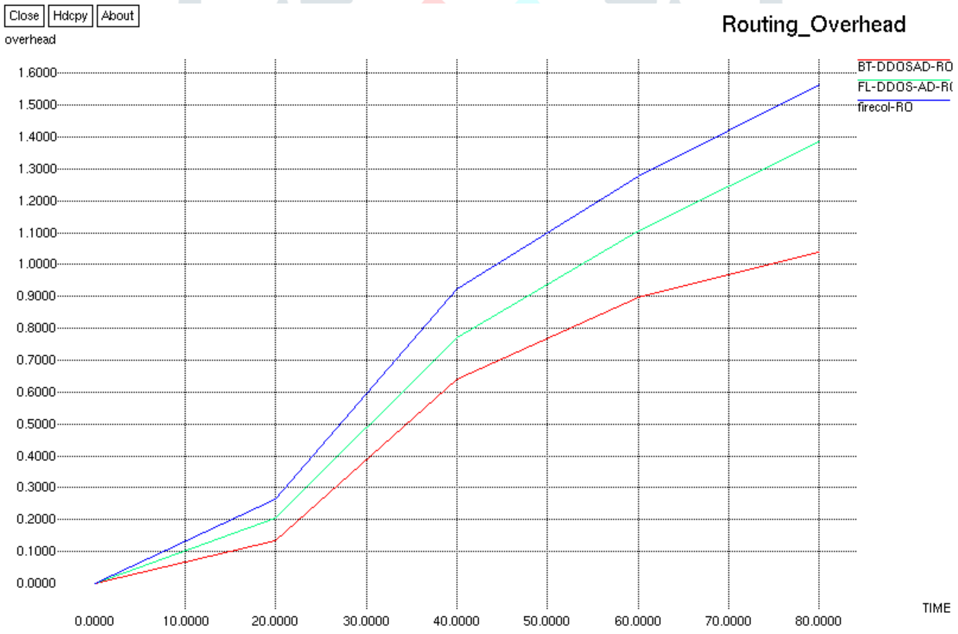


Figure 9: Routing Overhead Comparison

From the figure 9, it is confirmed that the proposedtechnique namely BT-DDOSADtechnique brings about provide better outcomematched up with the existing research methods in keeping with reduced routing overhead. This routing overhead increased linearly as the time increases but lesser than the existing research method.

4.7. FALSE POSITIVE

False positive rate is defined as the wrong prediction rate of DDOS attacks present in the environment. That is incorrectly prediction the DDOS attack as genuine behaviour is defined as false positive rate. The assessment of false positive metric is depicted in the figure 10.

Table 8. False positive comparison table

Time	False positive rate		
	Firecol	FL-DDOS-AD	BT-DDOSAD
5	0.1	0	0
10	0.2	0	0
15	0.4	1.16	0.13
20	0.62	0.33	0.25
25	0.8	0.52	0.37
30	1	0.72	0.5
35	1.12	0.78	0.56
40	1.23	0.84	0.62

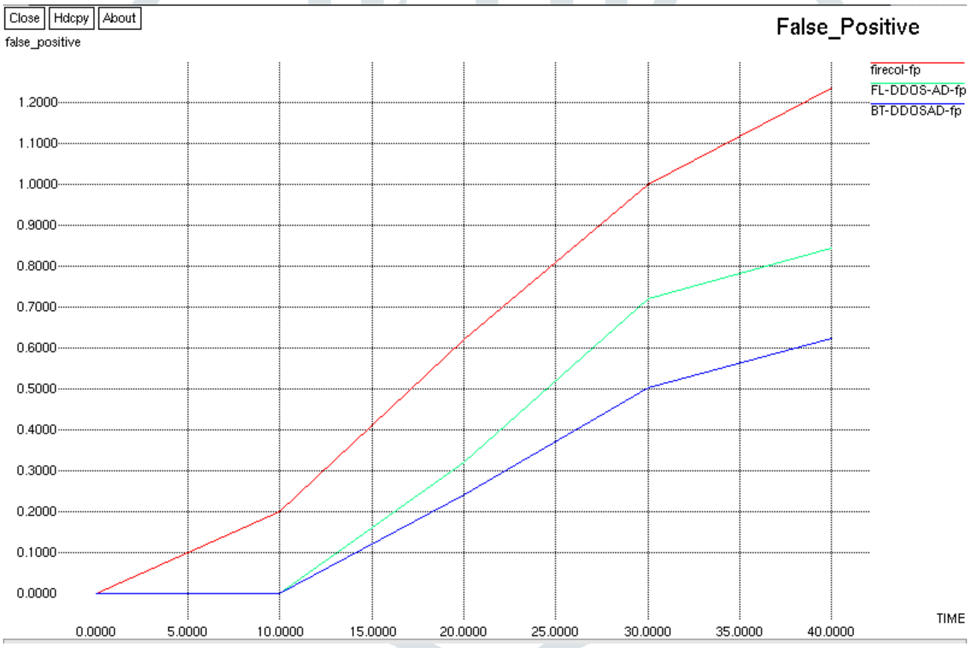


Figure 10: False Positive Rate

From this figure 10, it could be specified that the research technique brings about provide the better classification performance matched up with the existingtechnique in regard to correctly predicting the DDOS attacks behaviour present in the network environment. The proposed method BT-DDOSADproves to provide more accurate performancematched up with the existingtechnique.

4.9. DETECTION RATIO

Detection ratio is the proportion of correctly predicting the DDOS attacks present in the environment without fail. DDOS attack detection ration should higher for the proposed research method for the ensured secured environment without DDOS attacks presence. The assessment of the DDOS attack is depicted in the figure 11.

Table 9. Detection rate comparison table

Nodes	Detection rate		
	Firecol	FL-DDOS-AD	BT-DDOSAD
5	0	0.19	0.24

10	0	0.37	0.5
15	0.19	0.5	0.65
20	0.37	0.62	0.81
25	0.43	0.74	0.9
30	0.5	0.86	1
35	0.63	0.93	1.07
40	0.75	1	1.15

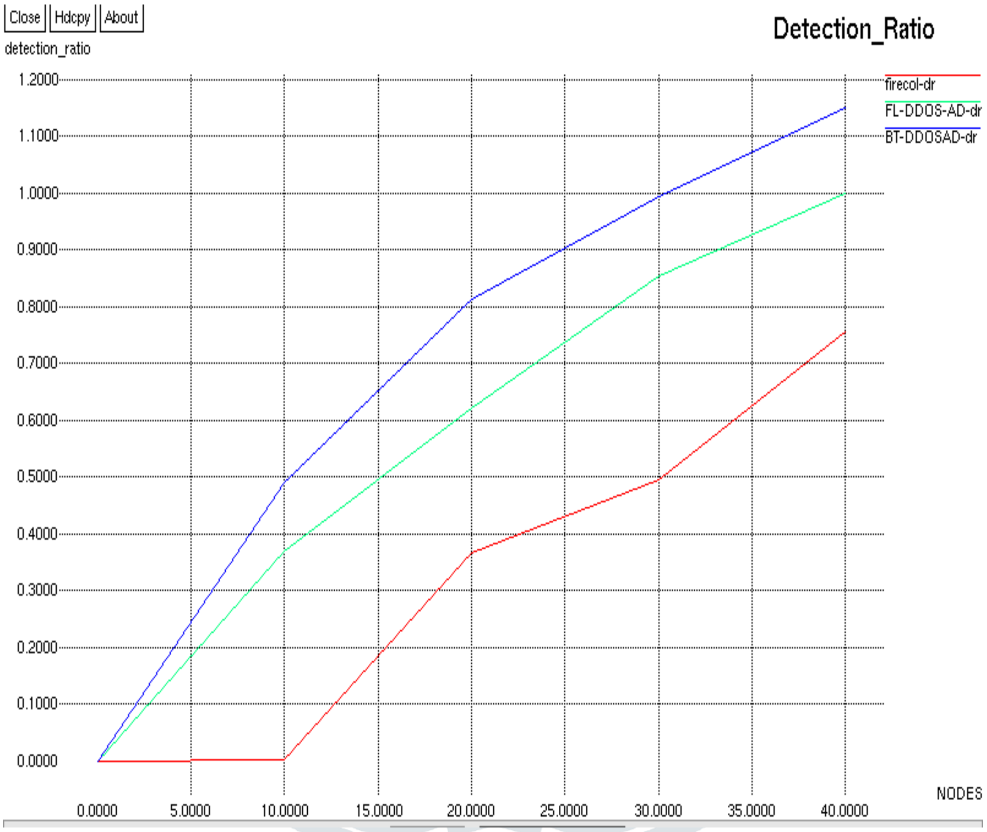


Figure 11: Detection Ratio Comparison

V. CONCLUSION

The primary target of the suggested work is to bring-in the new research techniques, which can identify the existence of DDOS attack in the network perfectly. So, different algorithms have to be established for accurate detection outcome. Along with the timing serious values (such as type of protocols, TTL values, geo-location of reflective IPs, etc.), burst time instances also has to be assumed in our work. In the suggested work, an enhanced box Cox transformation is enforced to execute the preprocessing to make data set cleaner for normal effective processing. The implementation of the proposed research method is done in the NS2 simulation environment, which confirms that the suggested work assures the optimal performance when distinguished with the current research techniques.

REFERENCE

1. Geng, X.J.; Whinston, A.B.: Defeating distributed denial of serviceattacks. IT Prof. **2**(4), 36–42 (2000)

2. Ottis, R.: Analysis of the 2007 cyber attacks against Estonia fromthe information warfare perspective. In: Proceedings of the 7thEuropean Conference on Information Warfare, p. 163 (2008)

3. Bangladesh Bank heist. (2016). https://en.wikipedia.org/wiki/2016_Bangladesh_Bank_heist

4. European renewable power grid rocked by cyber-attack. EurActiv(2012). https://www.euractiv.com/section/energy/news/European-renewable-power-grid-rocked-by-cyber-attack/

5. Musil, S.: Record-breaking DDoS attack in Europe hits400 Gbps. CNET (2014). http://www.cnet.com/news/recordbreaking-ddos-attack-in-europe-hits-400gbps/

6. Paroutis, S.; Bennett, M.; Heracleous, L.: A strategic view onsmart city technology: the case of IBM Smarter Cities during arecession. Technol. Forecast. Soc. Chang. **89**, 262–272 (2014)

7. Bawany, N.Z.; Shamsi, J.A.: Smart city architecture: Vision andchallenges. Int. J. Adv. Comput. Sci. Appl. **6**(11) (2015)

8. Yadav, V.K.; Trivedi, M.C.; Mehtre, B.M.: DDA: an approach tohandle DDoS (Ping flood) attack. Adv. Intell. Syst. Comput. **408**,11–23 (2016)

9. Saied, A.; Overill, R.E.; Radzik, T.: Detection of known andunknown DDoS attacks using artificial neural networks. Commun.Comput. Inf. Sci. **172**, 385–393 (2016)

10. Hoque, N.; Bhattacharyya, D.; Kalita, J.: Botnet in DDoS attacks:trends and challenges. IEEE Commun. Surv. Tutor. **99**, 1–1 (2015)

11. Arbor Networks Inc. http://www.arbornetworks.com

12. Arbor networks detects largest ever DDoS attack in Q12015 DDoS report. In: Arbor Networks (2015). http://www.arbornetworks.com/arbor-networks-detects-largest-ever-ddosattack-in-q1-2015-ddos-report

13. T. Peng, C. Leckie and R. Kotagiri, "Survey of network-baseddefense mechanisms countering the DoS and DDoS problems", ACMComput. Surv. 39, April 2007.

14. R. Sommer and V. Paxson, "Enhancing byte-level network intrusiondetection signatures with context", CCS, 2003.

15. X. Li, F. Bian, M. Crovella, C. Diot, R. Govindan, G. Iannaccone andA. Lakhina, "Detection and identification of network anomalies usingsketch subspaces", IMC, 2006.

16. H. Ringerg, A. Soule, J. Rexford and C. Diot, "Sensitivity of pc a fortraffic anomaly detection", SIGMETRICS, 2007.

17. Hemant Sengar, Xinyuan Wang, Haining Wang, DumindaWijesekeraand Sushil Jajodia, "Online Detection of Network Traffic AnomaliesUsing Behavioral Distance", IEEE IWQoS 2009 , Charleston, July2009.

18. Mehdi, S.,A.,S.; Khalid, J.; Khayam, S.,A.,S.: Revisiting trafficanomaly detection using software defined networking. In:Proceedings of the 14th International Conference on RecentAdvances in Intrusion Detection, pp. 161–180 (2011)

19. Giotis, K.; Argyropoulos, C.; Androulidakis, G.; Kalogeras, D.;Maglaris,V.: CombiningOpenFlowandsFlowfor an effective andscalable anomaly detection and mitigation mechanism on SDNenvironments. Comput. Netw. **62**, 122–136 (2014)

20. Braga, R.; Mota, E.; Passito, A.: Lightweight DDoS floodingattack detection using NOX/OpenFlow. In: LCN ’10 Proceedingsof the 2010 IEEE 35th Conference on Local Computer Networks,pp. 408–415. IEEE, Washington (2010)