International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 13, Number 1 (2017), pp. 101-111
© Research India Publications
http://www.ripublication.com

A Mechanism for Prevention of Flooding based DDoS Attack

Nipa Patani[1] and Rajan Patel[2]

Sankalchand Patel College of Engineering, Visnagar-384315, India.

Abstract

Flooding Attack threatens among all the flavors of DDoS (Distributed Denial of Service) causing deadliest impact in a network/Internet. As the ability of DDoS, it doesn’t need to have much computational efforts to target the destination servers and networks. Developing a mechanism against unidentified attacks on application and transport layer is a desired goal of intrusion detection and/or intrusion prevention system research. This paper presents the several vulnerabilities that explicitly attempts to interrupt legitimate users access to services at application and transport layer of TCP/IP. This paper aim to propose a technique from existing taxonomies for the detection and analysis of synchronous and non-synchronous traffic flow with the observation of network in time-slot. Furthermore, this approach uses traffic source authentication of legitimate and malicious traffic using CAPTCHA in various ways.

Keywords: DDoS · Flooding attack · Synchronous flow · Non-synchronous flow · Traffic source authentication · CAPTCHA

1. INTRODUCTION

Nowadays Internet Services become crucially important. Therefore, degradation of service quality or total denial of service can be critical. Denial of Service (DoS) attack goals to stop legitimate users from accessing network or system resources. Attacks driven from more than one node / sources in an Internet traffic it is recognized as a

Distributed Denial of service (DDoS) as illustrated in Fig.1. To blast-off a DDoS attack there are mostly two methods. The first method is taking advantage of design defects of the network. Attackers send some mimicry packets to the target server to confuse an application running on target. The second method adopts flooding traffic that either exhausts bandwidth or resource of the server [1]. The chief targets of attack launcher are routers, links, firewalls, victim's computer and network infrastructure, victim OS, current communications and victim's application.

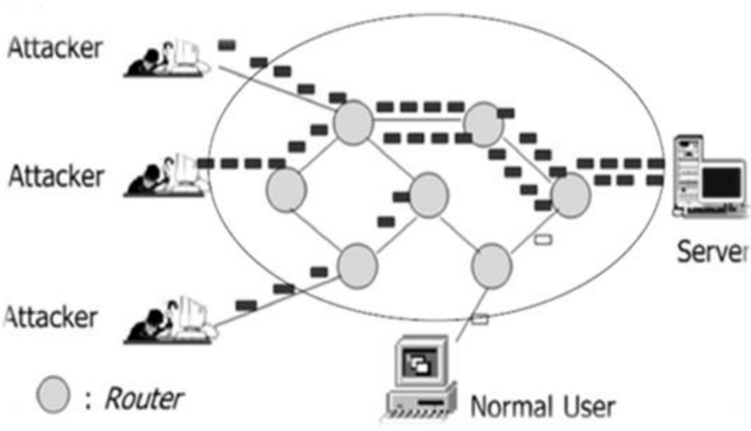

Fig. 1. Structure of typical DDoS attack

There are two main challenging features of DDoS. One is DDoS packet manages to seem as genuine packets which are not able to clarify without any influence is puzzling. Second is nearly impossible to find out the source path of an intruder due to the spoofed IP address. Due to these two main weaknesses, the network systems have often become the targets of various attacks which are transmitted illegally gain approach to useful resources. DDoS may arise due to extreme need of trustworthy users for specific resource such as flash crowd and make the server overloaded. DDoS are acute concerns for companies that have been integrating their technology to public network, allowing multiple parties or users to access data.

As stated by the research and educational communities there is a noteworthy growth in frequency and size of targeted network by the year 2015 is 20 percent of service provider repeatedly report attack over 50Gpbs. [2] The percentage of suspects sighted application-layer attacks endures to rise, up to 93 percent this year, from 90 percent last year and 86 percent in 2013.Mostobserved DDoS attacks are still comparatively small with 84 percent of observed events less than 1 Gbps in size. There is a proportion 760 Mbps attacks this year. In the world of internet, it is not considered as a large amount but it will surely degrade the business and other related firms severely in their functions. In the statistics of ATLAS data on attack duration there is an increase of about 1% from the previous two years which lasted for less than one hour. The average attack duration in 2015 was 58 minutes, which is relatively consistent with previous results [3].

DDoS attack criteria varies considerably and attackers are constantly growing the procedures they use to escape defense and make attack successful. Attacks broadly classified into three categories:

I. Volumetric Attacks [2]: These attacks are based on creating bottlenecks in a network or at the target server. It severely affects the bandwidth of a network causing delay in serving the genuine request from users. These attacks are merely about triggering crowd

II. TCP State-Exhaustion Attacks: In TCP State Exhaustion attacks**,** it efforts to exhaust the connection state tables that are present in many infrastructure components, such as load balancers, firewalls, IPS and the application servers themselves. They can record even high-capacity devices capable of maintaining state on millions of connections.

III. Application-Layer Attacks: The deadliest and hard to prevent are on application layer or also called it as a Layer 7 attack. They are the most classy and sophisticated because of their machine generating bots and they inject their worms at a low rate. Hence, this makes the traditional prevention schemes inactive for flow based monitoring of incoming traffic. An approach for detection in a real traffic requires to install an in-line or another packet-based component to your DDoS defense [3].

The paper is organized as follow. Section 2 describes the DDoS attacks approaches and their countermeasures with existing work. Section 3 provides the scope and classification of attack features. Section 4 discusses contribution of the proposed work and finally concluded remarks in section 5.

RELATED WORKS

Numerous defense and prevention mechanism already stated to combat DDoS attacks. Attacks can be grouped into types based on protocol vulnerabilities. [4] The aim of prevention system is to eliminate the maximum chance of attack, or to make the victim aware about possibility of attack in a way that it can bear an occurrence of attack without hindering the real traffic. As stated by [5] for comprehensive modules classified into modules like detection, characterization, trace back, mitigation is required. Generally, by a time DDoS attack is detected and to get the information about targeted server or network congestion, nothing can be done except disconnecting the victim or manually fixing the problem. The goal of DDoS detection methodology is traffic monitoring at the source node and in the network and for the same purpose it requires refined behavioural analysis. There is a lack of detection mechanism for Low-rate Denial of Service (LDoS). The proposed Multisampling Sampling Averaging Based on Missing Sampling takes network traffic as a signal based on a small signal model for 10ms within 30s. The results generated compared with threshold for identifying the LDoS attack [6]. Another approach for sustaining QoS of the real traffic flow they have proposed Traceback-based Defense against DDoS Flooding attack that detects attack at source end. TF, DFM, IP traceback algorithm at a victim end modules are established in a network that are proficient in discarding the attack packets at the source end [7]. To overcome the deficiency of early detection and high accuracy, a victim end based mechanism is constructed with a low false positive ratio within a short interval. The better results than Kullback-Leibler divergence when they increased the order of information divergence measures in detecting both low-rate and high-rate DDoS attack [8].

Signature based approach, anomaly based approach and entropy based approach are three methodologies for detection of DDoS attacks [9]. These methods are employed in a network according to their varied condition such as normal traffic or in a situation with high network traffic or low incoming traffic. In signature based approach, a threshold is limited so that when a DDoS attack occurs, millions of packets will be counted. To overcome this, installing a threshold to the number of detected signatures to be adopted [10]. Whenever it is increase in the value of router entropy unexpectedly it is challenging to differentiate between flash events and crowd of DDoS attack. For this purpose, concept of average entropy is calculated at the edge of ISP domain. It sends warning to its downstream router to estimate the entropy value. This approach by merging entropy, average entropy and standard deviation of flow system can identify suspect of DDoS flow.

In real Internet traffic, packets can be in synchronous long flow or low rated non-synchronous flow. It is assumed that normal traffic flows are short-lived and non-synchronous. The suggested algorithm records the address pair of source and destination address in time-slots and performing several intersecting operations in consecutive time-slots and record it for enough times. If it exceeds the threshold it is labelled with alarm and further it is detected by using HCF (Hop Count Filter) for mapping number of hops from a source to destination [11].

Another approach is fast entropy based method for maintaining detection accuracy for DDoS attacks using flow based analysis is suggested. Attack packets are generated generally by tools that are installed in a bot for flooding the link or a network. This shows that flow link among DDoS flooding attack is much higher than among random flash crowds. To identify suspicious flows, destination superpoints is used to measure flooding behavior and observation of flow similarity by using sliding window mechanism enables differentiation about random flash events and flooding traffic much efficiently [12]. In order to defend against application layer DDoS attacks the technique here proposed a traffic authentication method for traffic source. The mitigation approach uses random tree machine learning algorithm in training, cross-validation and testing phase. Bait and Decoy servers are used to regulate legality of usual and nasty traffic [13].

To determine the malicious IP address which is expected to be Command & Control (C&C) server, blacklist of malicious IPs based on different intelligence feeds at once [14]. Flow count is distinctive way by which the severity of the flooding attack cab be known. It is calculated at each entry point in a network at a fixed time intervals. DDoS attack is characterized when the difference between fast entropy of flow count at each instant and mean value of entropy in that time interval is greater than the threshold value. This shows the effectiveness in terms of computational time in comparison to conventional entropy.

For DDoS flooding attacks, consuming bandwidth or resources are the main methods to make service unavailable. The larger the number of synchronous flow in a time interval the stronger traffic is synchronized [15]. Such a traffic behaviour can deal a host or network with DDoS attacks by direct attacks or reflectors attacks using bots. There are several Information theory-based metrics in the detection of distributed DoS attacks [16]. The technique of supervised learning models takes into account traffic of a network, filtering of http headers and the process of normalization which uses Support Vector Machines (SVM) [17].

The table 1 comprises of DDoS attack prevention or detection based on deployment location, attack time, their accuracy level, traffic flow, used data set or simulator for experiments.

Table 1. Techniques and way of attack impacts

	Technique	Deployment Location	Attack time (After/ Before)	Accuracy	Data Set/ Simulator	Traffic Flow	Detection/ Prevention Mechanism	Remark
[6]	MSABMS	Source node	After	High	NS2	Asynchronous	Detection	Detection criteria is marked with the rate of common LDoS attack
[7]	TDFA	Destination node	After	High	CAIDA Data set	Synchronous	Detection	Traceback Methodology at victim end
[8]	Entropy/ Information Metrics	Destination node	After	Medium	MIT, CAIDA, TUIDS Data set	Synchronous Asynchronous	Detection Prevention	Information Metric Entropy offers improved outcome for detection of high rate & low rate DDoS attack with the increase in order of generalized entropy.
[9]	Fast Entropy	Destination node	After	Medium	CAIDA Data set	Synchronous	Detection	Adaptive Threshold Algorithm to improve Detection accuracy.
[10]	Analytical Method	Source node	After, Before	Medium	Test Bed	Synchronous	Detection	At the source node hybrid approach, of Source address analysis method and network flow analysis on IPv6 gives better result
[11]	HCF	Source node	After	High	CAIDA Data set	Synchronous	Detection	Flows of DDoS Flooding attack traffic are persistent, synchronous while most flows of normal traffic is short-lived, Non-synchronous
[12]	Sliding Window Algorithm	Destination node	After	High	MIT: LLS DDoS Data set	Synchronous	Detection	Polymerization degree of destination superpoints and TVD is introduced in a moving time window mechanism
[13]	Machine Learning	Destination node	Before	High	MAWI: NETRESEC Data set	Synchronous Asynchronous	Prevention	Traffic authentication is done by using Bait and Decoy Server for protection.

[14]	Intelligence Feeds	Source node	Before	High	Bro-Network Security Monitor	Synchronous Asynchronous	Detection	Source and destination IP address of each node is mapped with IP blacklist.
[15]	Traceroute Packet	Source node	After	Medium	CAIDA: AS Relationship Dataset	Synchronous Asynchronous	Detection	It detects the attack before a link congestion occurs.
[16]	Entropy Based	Source node or Destination node	Before	Medium	NS2 GT-ITM	Synchronous Asynchronous	Detection	Entropy calculation on basis of destination address. Not applicable to isotropic DDoS attack
[17]	SVM	Source node	After	High	Supervised Learning Model SVM	Synchronous	Detection	In SVM the results are observed with the human interaction and as per input parameters to the machine learning approach.

DDoS PREVENTION: SCOPE AND CLASSIFICATION

All attacks seek to make influence on victim. But DDoS attack differs from the point where victim demonstrated its weakness. Fig shows our comprehensive study and categorization of some familiar DDoS attack on network layer and transport layer [18].

Fig.2. illustrated scope and classification for DDoS prevention. *Degree of Automation:* in order to form the agent army attacker, it is necessary to find the way of installing the bugs into machines or zombie. *Exploited Vulnerabilities:* the attackers take a benefit of drawbacks of design issues of protocols such as TCP, UDP, ICMP, HTTP, FTP TELNET etc. Such bugs may lead to flooding, amplification or malformed packet attack to overwhelm the service of a victim. *Attack Network:* usually some attackers use proxy servers and other ways to hide its existence to be traceback after identifying the attack agents. Some of the types of malicious network like through bots or IRC network in which centralized mechanism fails [19]. *Attack Rate:* a network layer or transport layer attacks dynamics is also important to detect ongoing attacks at early stages. It can be at constant rate or variable rate. In an increasing attack rate the attack traffic gradually increasing at victim end. *Victim Type: a*ccording to the type of server host such as single host or link or an application server, the attacker takes various methods to launch DDoS attack. *Impact:* the severity of attack on network or transport layer depends on the amount of incoming traffic which is infected to bots controller. It can be destructive that demises totally without leaving any option for recovery. Secondly it can be disruptive which can be recovered afterwards [5]. *Scanning Strategy:* in scanning strategy, it will trace as numerous possible susceptible machines while creating a low traffic volume. Among them Random Scanning compromised hosts probe random addresses in the IP address space, using a different seed. Hitlist Scanning explore the externally listed IP address. In permutation scanning, pseudo-random permutation of the IP address space with indexing, semi-coordinated, comprehensive scan with benefits of random probing. Back-Chaining Propagation attack code is downloaded from the machine that exploited the system [20]. *Packet Content:* some of the incoming packet can be filtered by dynamically deployed fire-walls while another type of non-filterable packets that are continuously changing which makes difficult to detect the machine.

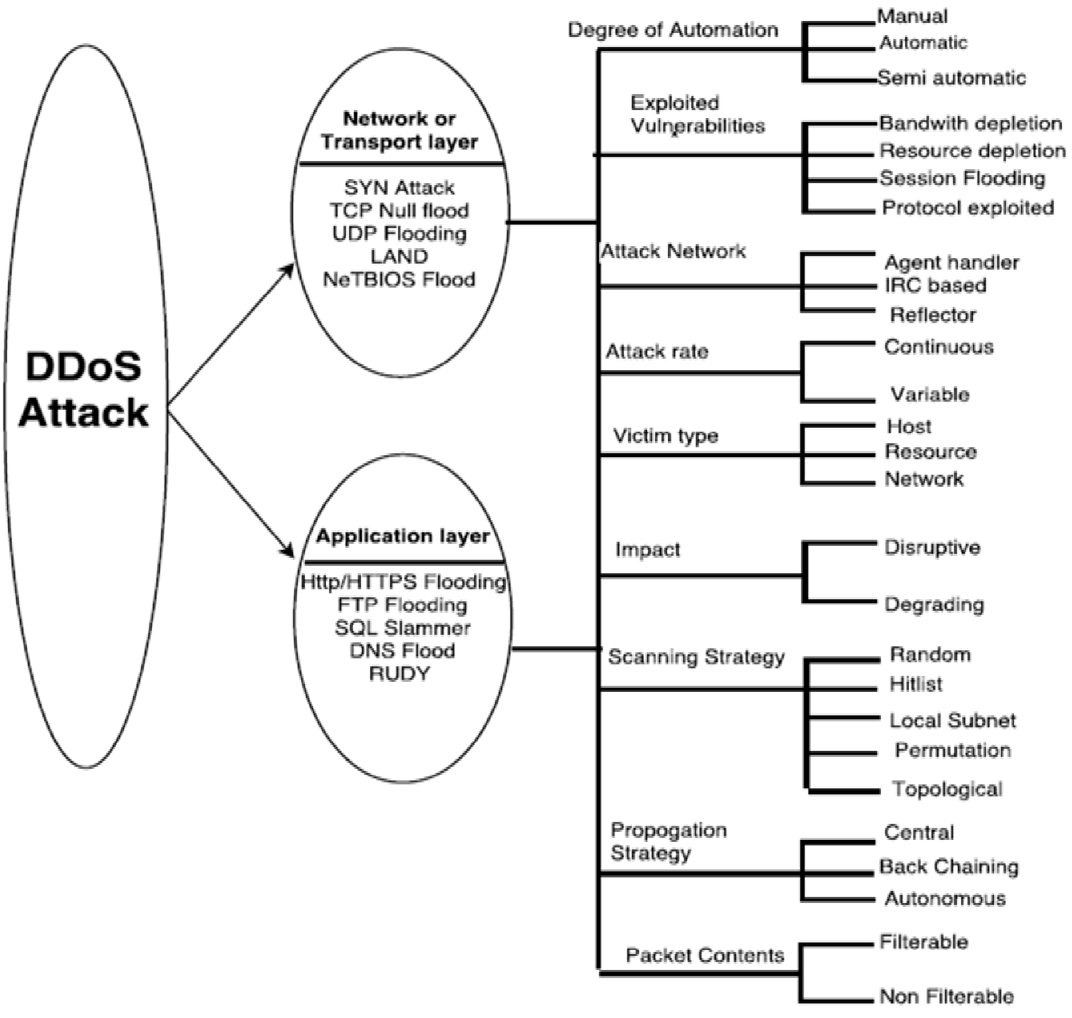

Fig 2. Taxonomy based on TCP/IP Layers

OUR CONTRIBUTION

The proposed work is focused on traffic flow analysis of both usual and malicious traffic. In initial stage, aim of the proposed algorithm is serve the entire incoming traffic request including both genuine requests as well as illegitimate request within time-slots. As shown in Fig.3, time-slot (T) 210s is divided into 30s for the observation of all incoming packets and after that it will record in observation table 2. This table describes the flow of packets along with the source and destination information and categorize according to its type in time-slots group (TGn). If server capacity (c) < frequency of packet (f), then observation TG_1, TG_2 ,.. TG_n in time-slots and record it. Else from observation table find out the frequently repeated IP address for sending the challenge through CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart).

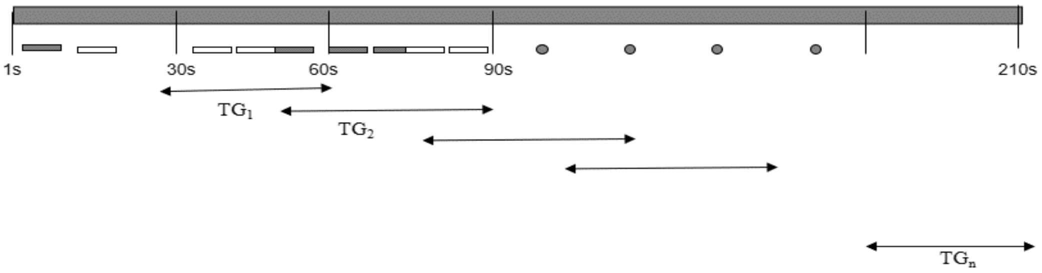

Fig.3 Traffic flow

Table 2 Observation Table

Time-slot Group	Address Pair	Packet Type
TG1	<src,dest>, <src,dest>…<src,dest>	ICMP, Ping, IPv4 packet, TCP,UDP etc.
TG2	<src,dest>, <src,dest>…<src,dest>	
TG3	<src,dest>, <src,dest>…<src,dest>	
.	.	
TGn	.	

The proposed algorithm explains the process of traffic analysis with respect to server capacity (c) and types of packets in pre-defined time-slots (T) with arrival frequency of packets (f). In the algorithm, first initialize the capacity (c) of destination server for every incoming packet within predefined time-slot (T) is monitor and record the information such as address pair (source address, destination address), packet type, source and destination port address etc. This process is continuing till the serving capacity of detonation server. If it exceeds the c then the algorithm determined the repeated IP address from recorded information during step 2. After that, step 4 execute for sending the challenge using CAPTCHA. All the CAPTCHA responses are served considering it as a genuine. Discard the traffic for those IP which doesn't get ack. This observation keep alive in next consecutive time-slot (step 6).

Proposed Algorithm

```
Step1: Initialize observation slot T, frequency of packet f, destination capacity c.
Step2: Monitor flow of arrival of request and serve till destination capacity c and
       record duplicate pairs <src,dest>, packet type.
Step3: If frequency of packet/traffic > c. (for a given time-slot, T=30s)
       then go to 4 else go to step 6.
Step4: Send reply back using CAPTCHA
Step 5: Serve only the CAPTCHA responses and drop other packets.
Step6: Observe traffic flow in next consecutive time-slots T.
```

CONCLUSION

It is precisely a necessity to remove the burden of illegal packets due to DDoS attacks in a network/Internet. This paper makes remark on several vulnerabilities that explicitly attempts to interrupt legitimate user access to services at application and transport layer of TCP/IP. Hence, it is necessity to reduce the DDoS attack from synchronous and non-synchronous traffic flow. The proposed work is able to observe some suspicious or spoofed IP addresses using recorded information for both synchronous and non-synchronous traffic flow during time-slot. Furthermore, it marked address pairs that are authenticated by challenge response mechanism i.e. CAPTCHA while other packets are dropped. In extension to this paper, the proposed work will be simulated the results with dataset and tools in future.

REFERENCES

[1] Saranya, R., S. Senthamarai Kannan, and N. Prathap: A Survey For Restricting The DDOS Traffic Flooding And Worm Attacks In Internet.In:2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). Pp. 251-256, IEEE (2015)

[2] Worldwide Infrastructure Security Report: Volume XI., https://www.arbornetworks.com/report (2015)

[3] Q1State of the Internet / Security Report, https://content.akamai.com/PG6292-SOTI-Security (2016)

[4] Bhandari, Abhinav, A. L. Sangal, and Krishan Kumar: Destination Address Entropy based Detection and Traceback Approach against Distributed Denial of Service Attacks. In: International Journal of Computer Network and Information Security 7, no. 8 (2015)

[5] Zeb, Khan, Owais Baig, and Muhammad Kamran Asif: Ddos Attacks And Countermeasures Cyberspace. In: Web Applications and Networking (WSWAN), 2015 2nd World Symposium on, pp. 1-6. IEEE, (2015)

[6] Zhi-Jun, Wu, Zhang Hai-Tao, Wang Ming-Hua, and Pei Bao-Song. MSABMS-Based Approach Of Detecting Ldos Attack. In: computers & security31, no. 4: 402-417. (2012)

[7] Foroushani, Vahid Aghaei, and A. Nur Zincir-Heywood: TDFA: Traceback-Based Defense Against Ddos Flooding Attacks.In:28th International Conference on Advanced Information Networking and Applications IEEE pp. 597-604. IEEE, (2014)

[8] Bhuyan, Monowar H., D. K. Bhattacharyya, and Jugal K. Kalita.: An Empirical Evaluation Of Information Metrics For Low-Rate And High-Rate Ddos Attack Detection. In: Pattern Recognition Letters 51: 1-7. (2015)

[9] David, Jisa, and Ciza Thomas: Ddos Attack Detection Using Fast Entropy Approach On Flow-Based Network Traffic .In: Procedia Computer Science 50: 30-36. (2015)

[10] Satrya, Gandeva B., Rizqi L. Chandra, and Fazmah A. Yulianto: The Detection Of DDOS Flooding Attack Using Hybrid Analysis In Ipv6 Networks. In: Information and Communication Technology (ICoICT), 3rd International Conference on, pp. 240-244. IEEE, (2015)

[11] Li, Chenxi, Jiahai Yang, Ziyu Wang, Fuliang Li, and Yang Yang: A Lightweight DDoS Flooding Attack Detection Algorithm Based on Synchronous Long Flows..In: IEEE, Global Communications Conference (GLOBECOM), pp. 1-6. IEEE, (2015)

[12] Jiang, Hong, Shuqiao Chen, Hongchao Hu, and Mingming Zhang:Superpoint-Based Detection Against Distributed Denial Of Service (Ddos) Flooding Attacks.In: The 21st IEEE International Workshop on Local and Metropolitan Area Networks, pp. 1-6. IEEE, (2015)

[13] Ndibwile, Jema David, A. Govardhan, Kazuya Okada, and Youki Kadobayashi. :Web Server Protection against Application Layer DDoS Attacks using Machine Learning and Traffic Authentication.In: Computer Software and Applications Conference (COMPSAC), 2015 IEEE 39th Annual, vol. 3, pp. 261-267. IEEE, (2015)

[14] Ibrahim Ghafir and Vaclav Prenosil,:Blacklist-based IP Traffic Detection.In: IEEE pp. 229-233(2015)

[15] Hirayama, Takayuki, Kentaroh Toyoda, and Iwao Sasase:Fast Target Link Flooding Attack Detection Scheme By Analyzing Traceroute Packets Flow.In: In Information Forensics and Security (WIFS), 2015 IEEE International Workshop on, pp. 1-6. IEEE, (2015.)

[16] Bhandari, Abhinav, A. L. Sangal, and Krishan Kumar:Destination Address Entropy based Detection and Traceback Approach against Distributed Denial

of Service Attacks.In: International Journal of Computer Network and Information Security 7, no. 8 (2015)

[17] Ll, Manuel S. Hoyos, Jairo I. Vélez, and Luis Castillo: Distributed Denial of Service (DDoS) Attacks Detection Using Machine Learning Prototype.In: Distributed Computing and Artificial Intelligence, 13th International Conference, pp. 33-41. Springer International Publishing, (2016.)

[18] Nazrul Hoque, Dhruba K Bhatattacharya and Jugal K Kalita,: Botnet in DDoS Attacks: Trends and Challenges. In:IEEE Communications Surveys and Tutorials VOL. X(2015)

[19] Ramanauskaite, S., & Cenys: A. Taxonomy Of Dos Attacks And Their Countermeasures. In: Springer Open Computer Science, pp 355-366. (2011)

[20] Denial of Service Attack ,https://en.wikipedia.org/wiki/Denial-of-service_attack.