International Journal of Engineering & Technology, 7 (2.7) (2018) 1051-1057

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Detection of DDOS attacks in distributed peer to peer networks

Gera Jaideep [1] *, Bhanu Prakash Battula [2]

[1] Research Scholar, CSE Dept, Acharya Nagarjuna University, Guntur, Andhra Pradesh
[2] Professor, CSE Dept, Tirumala Engineering College, Guntur, Andhra Pradesh
**Corresponding author E-mail: gera.jaideep@gmail.com*

Abstract

Peer to Peer (P2P) network in the real world is a class of systems that are made up of thousands of nodes in distributed environments. The nodes are decentralized in nature. P2P networks are widely used for sharing resources and information with ease. Gnutella is one of the well known examples for such network. Since these networks spread across the globe with large scale deployment of nodes, adversaries use them as a vehicle to launch DDoS attacks. P2P networks are exploited to make attacks over hosts that provide critical services to large number of clients across the globe. As the attacker does not make a direct attack it is hard to detect such attacks and considered to be high risk threat to Internet based applications. Many techniques came into existence to defeat such attacks. Still, it is an open problem to be addressed as the flooding-based DDoS is difficult to handle as huge number of nodes are compromised to make attack and source address spoofing is employed. In this paper, we proposed a framework to identify and secure P2P communications from a DDoS attacks in distributed environment. Time-to-Live value and distance between source and victim are considered in the proposed framework. A special agent is used to handle information about nodes, their capacity, and bandwidth for efficient trace back. A Simulation study has been made using NS2 and the experimental results reveal the significance of the proposed framework in defending P2P network and target hosts from high risk DDoS attacks.

Keywords: *DdoS Attack Detection; P2P Network; Distributed P2P Networks; Time to Live.*

1. Introduction

Peer to Peer (P2P) networks is a class of applications that are overlay networks on top of the Internet or Wide Area Network (WAN). They are decentralized networks where the peers are vulnerable to various attacks including DDoS attacks. Napster, Gnutella, Chord and Freenet are some of the well known examples for P2P networks. In the literature, it is found that they are subjected to DDoS attacks. In [30] and [31] vulnerabilities of Freenet are found. Partial Rank Correlation (PRC) technical was explored in [36] for discriminating DDoS attacks and flash crowds in P2P networks. The Flooding-based DDoS attack is one of the kinds where unwanted traffic is generated in large scale to disrupt normal functioning of targeted host and deny service in large scale. The victim under this kind of attack is exhausted shortly due to deletion of resources unnecessarily. The victim machines are generally Internet servers that render round-the-clock services to their vast number of clients.

Flooding based DDoS attacks attracted significant research. FireCol is a solution provided by Francois et al. [5] for detecting flooding-based DDoS attacks. It is nothing but a collaborative protection network. Different kinds of mechanisms for flooding-based DDoS attack are explored in [7], [39] and [40]. It is difficult to identify the source of attacks as source address spoofing is employed in launching DDoS attacks. In spite of many solutions for it, it is understood from the literature is that an effective solution for DDoS attack detection and prevention in P2P networks is still desired. Therefore, it is considered as an optimization problem in this paper. Our contributions are as follows.

- We proposed a framework for detecting and defending DDoS attacks through distributed P2P networks. The framework considers attack model where adversary launches DDoS attacks on a targeted Internet server by using the P2P network as a vehicle.
- We proposed an algorithm named P2P DDoS Detection (PDD) algorithm for detecting and defending the P2P network against DDoS attacks.
- We made NS2 simulations to demonstrate proof of the concept. The experimental results revealed the effectiveness of the proposed algorithm.

The remainder of the paper is structured as follows. Section 2 reviews literature on DDoS attacks and prevention methods. Section 3 provides information about P2P networks and DDoS attacks. Section 4 presents the methodology used to detect and defect P2P networks against DDoS attacks. Section 5 shows experimental results while section 6 provides conclusions and directions future work.

2. Related work

This section provides the review of on DDoS attacks in general and in P2P networks. Singh et al. [1] proposed a mechanism to detect DDoS attacks made through the P2P botnet. They built a distributed framework for big data analytics to achieve this. Rossow [2] studied network protocols pertaining to P2P networks, and P2P botnets in order to understand DDoS abuse. Multiplication of traffic and bandwidth amplification is the two kinds of malicious issues found in the protocols they analyzed. Bhuyan et al. [3] made a review of DDoS attacks and countermeasures. Similar kind of work is done in [12] and [24]. Yu et al. [4] proposed an approach known as Flow Correlation Coefficient (FCC) for understanding the difference between flash crowds and DDoS attacks.

Copyright © 2018 Gera Jaideep, Bhanu Prakash Battula. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Francois et al. [5] proposed a collaborative protection network known as FireCol for detecting flooding DDoS attacks.
Zhao et al. [6] proposed a methodology to detect botnet activities. They employed the concept of flow intervals for achieving this which is based on traffic patterns. Zargar et al. [7] made a survey on the DDoS flooding attacks and their defence mechanisms. And they found the need for distributed and collaborated defence mechanisms against such attacks. In the same fashion, Gave et al. [8] studied defence against bandwidth DDoS attacks where an attack is made to exceed network capacity to serve with respect to bandwidth. Yu et al. [9] opined that P2P networks do not have sufficient mechanisms to handle DDoS attacks. They investigated to the possible usage of cloud in the wake of DDoS attacks with dynamic resource allocation to combat DDoS attacks.
A Botnet is a set of nodes that are exploited by adversaries for making a DDoS attack. In fact, botnet acts as an engine for such attacks. Yu et al. [10] investigated and found that in the real world, having more number of botnets is not easy. Based on this they further understood that botnet mimicking attacks can be detected. Cholez et al. [14] focused on localized attacks on P2P networks where nodes are distributed across the globe. They used KAD network and provided a solution for detecting and mitigating localization attacks. They made many monitoring campaigns in large scale to detect attacks on P2P. The characteristics of botnets and their detection methods can be found in [11]. Gupta et al. [15] provided a solution for DDoS attacks at ISP level. They used a combined statistical approach to achieve this.
Kumar and Sharma [16] studied intrusion detection systems that handle DDoS attacks in the context of cloud computing. Lang-Yut-Fong et al. [17] proposed an algorithm known as DTopRank for anomaly detection in a distributed environment. It handles massive data and also reduces communication overhead. Heilman et al. [18] studied bit coin's peer to peer networks for exploiting them against eclipse attacks. They used Monte Carlo Simulations and measurements for analyzing attacks on Bit coin's P2P networks. They provided botnet aware countermeasures. Narang et al. [19] proposed a framework named as PeerShark that is for tracking conversations in order to detect P2P botnets. They differentiated benign traffic from P2P botnet traffic as part of protecting the system. Sandar and Sheni [20] studied XML and HTTP DDoS attacks and proposed a solution named Economic Denial of Sustainability (EDoS). They used Amazon EC2 for making cloud enabled experiments.
Gupta et al. [21] explored Artificial Neural Network (ANN) technology to quickly identify zombies that are used by adversaries to launch DDoS attacks. Hoque et al. [22] studied botnet based DDoS attacks, botnet architectures, and attack launching tools. They also discussed pros and cons of different botnet architectures. Latif et al. [23] studied wireless wearable devices for DDoS attacks in healthcare domain. It was a cloud-assisted approach. They found that in a large scale network where wearable devices are geographically distributed, DDoS attacks may cause problems to healthcare services. Gupta et al. [25] propped a framework that automatically detects DDoS attacks in ISP networks. The solution was made auto responsive to such attacks.
Purohit et al. [26] studied pollution attacks in a P2P network such as BitTorrent. They also proposed a pollution measure in order to find the damage caused by attack. Adamsky [27] studied the bandwidth related DDoS attacks on Bittorrent. The attack was related to malicious traffic with higher download rates. DeVries [28] investigated on the crypto currency known as Bitcoin with respect to security. Joshi and Chaudary [29] studied P2P botnet that is being used for launching DDoS attacks. Tian et al. [30] explored Freenet which is one of the popular P2P networks. They made trace back an attack on Freenet and found that is used to detect sources of DDoS attacks. Levine et al. [31] focused on the Freenet in order to detect downloader statistics. They found a vulnerability in Hops to Live (HTV) of Freenet. Clarke et al. [32] described the utility of Freenet. Similar kind of work is found in [33]. Meshram et al. [34] proposed an integrated approach for mitigating DDoS attacks based on filtering and admission challenges.
Gnutella is another P2P network explored in [35]. Bhuyan et al. [36] proposed a technique known as Partial Rank Correlation (PRC) for discriminating DDoS attacks into low-rate and high-rate attacks. They used rank correlation based mechanism for discrimination. Different P2P networks and their attack dynamics are explored in [37]. Shredeh [38] did similar kind of work. Khataniar et al. [39] studied attacks and counter measures in P2P overlay networks. Different attacks they explored include index poisoning attack, flooding attack, pollution attack and eclipse attack. Similar kind of work is made in [40]. Cyber attacks on medical devices and DoS attacks on caching networks are explored in [41] and [42] respectively. A solution for black hole DoS attack [43] and architecture for detecting attacks based on log data and network traffic [44] are other solutions found. In the literature, it is found that the simulation of real time P2P networks for detecting and preventing DDoS attacks is still on open research for optimization. This paper focuses on presenting a mechanism for the same with a simulation study.

3. P2P networks vs. DDOS attacks

Peer to Peer networks follow a different approach in network topology and connectivity. Their important feature is to have a collection of peers (equally capable nodes). Unlike client/server networks where one machine acts as a server while the other machines are clients, a P2P network is made up of nodes that are peers. Any node can communicate with any other node. The network is dynamic (new nodes can be added and existing nodes may be closed) and distributed in nature. The difference between C/S and P2P networks is shown in Figure 1. There are many real world P2P networks such as Gnutella, Chord, Napster and Freenet. Out of them, Napster is an example of centralized P2P, Gnutella and Freenet are pure P2P network applications, and Chord is a Distributed Hash Table (DHT) based P2P network. P2P networks are vulnerable to various kinds of attacks. The rationale is that millions of anonymous peers might take part in the network that supports mainly two functionalities. They are searching for files and sharing files. Common attacks found in P2P networks are index poisoning attack, eclipse attack, Sybil attack, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

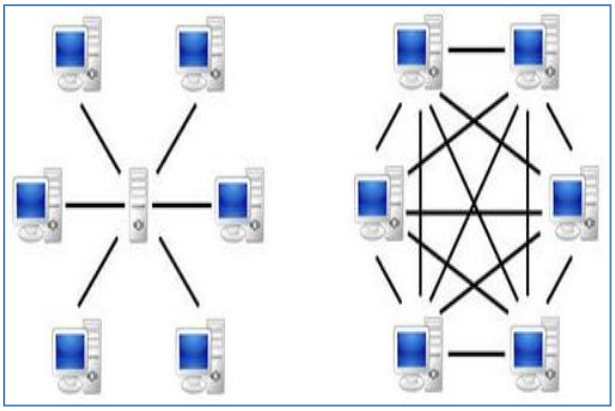


Fig. 1: P2P Network (Left) vs. Client/Server Network (Right) [45].

P2P networks are widely used a network for file sharing across the globe. They are overlay networks that are used by individuals. Users can join P2P network by opening an instance of a peer. By closing an instance of peer, users can disconnect from a P2P network. The peer instance of Gnutella Turbo 8.1.0 appears as shown in Figure 2.

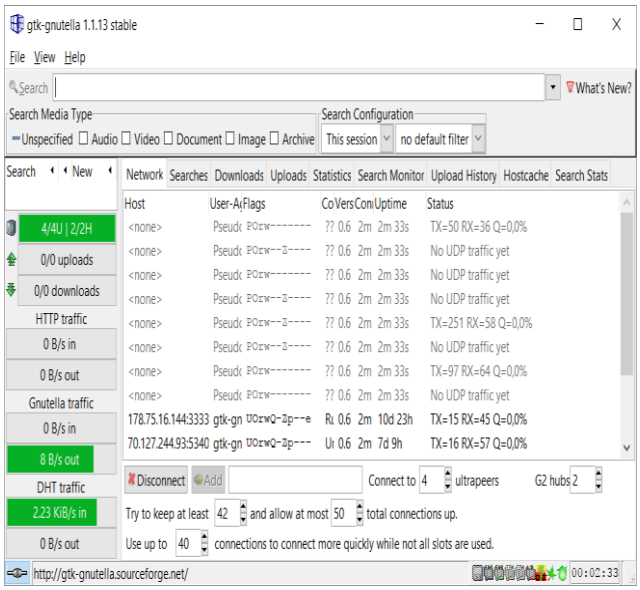


Fig. 2: Gnutella Client UI.

As can be seen in Figure2, Gnutella client provides interface for connecting to P2P network, disconnecting from it, uploading files, and viewing downloads and searching for files shared by other Gnutella users. At any given time, there might be millions of users connect to the distributed P2P network. As observed here, the application reflects client program which is nothing but the overlay peer of Gnutella network. Each node which is running on user's machine is connected to the network of peers. These peers can be used by adversaries to launch DDoS attacks on chosen targets. Thus the P2P network can act as an engine for adversaries to make attacks in large scale. In all such P2P networks, peers are mainly performing two activities. They are sharing files and searching for files. This mechanism is illustrated in Figure 3.

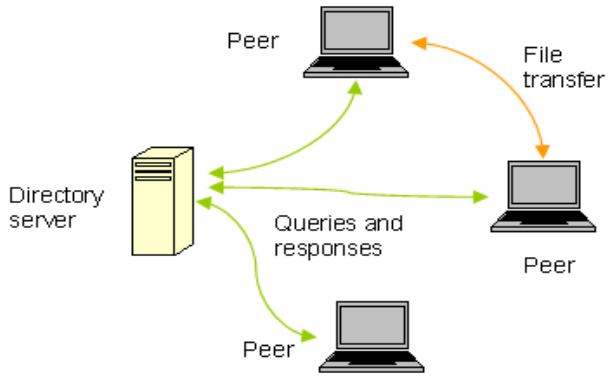


Fig. 3: Peers Participating in Query and Responses and File Transfer [46].

As shown in Figure 3, it is evident that peers in the P2P network are connected directly to each other. And they are associated with a directory server which maintains details of peers. Thus peers can discover about other peers and the peers having desired resources. The lookup for resources appear like client/server but the communication and resource transmission are still in P2P model. Different kinds of attacks are possible as mentioned above in such networks. As the P2P network is distributed across the globe on top of Wide Area Network (WAN), it is understood that P2P networks are used by adversaries to launch attacks. Since nodes are available in large scale, they can be compromised by hackers to be used as zombies to launch DDoS attacks. Different kinds of DDoS attacks are presented in Figure 4 with classification by degree of automation, vulnerability, attack rate and impact.

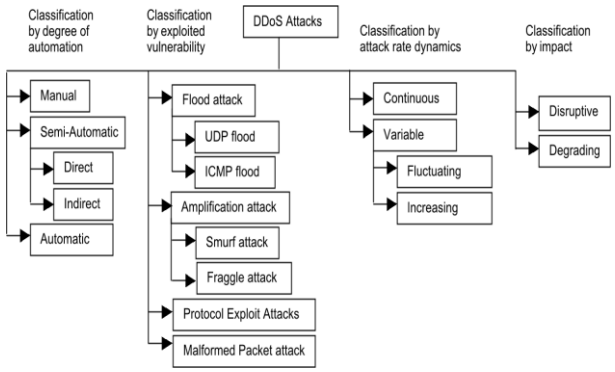


Fig. 4: Classification of DDoS Attacks [13].

As shown in Figure 4, it is evident that DDoS attacks may be launched manually, with semi-automated approach or automatic approach. The exploited vulnerability based attacks are flood attacks, amplification attacks, protocol exploits attacks and malformed packet attacks. With respect to attack rate, there are continuous and variable variants. The classification by impact reflects two kinds namely disruptive and degrading of services of the target network. With P2P network, DDOS attacks can be launched typically as shown in Figure 5.

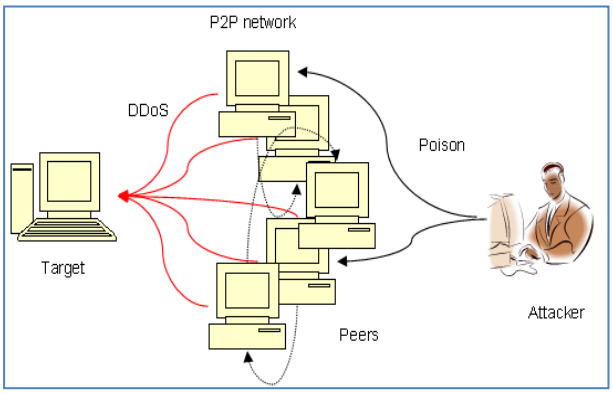


Fig. 5: Typical DDoS Attack over P2P Network [46].

As shown in Figure 5, it is evident that the P2P network or its overlay nodes are compromised by an attacker to launch a massive attack on the target server. This is the typical scenario where the P2P network is hijacked and also subjected to attack besides launching a DDoS attack to target machine by employing P2P network as an agent. The peers in the network are poisoned so as to work under the guidance of attacker in order to launch large scale denial of service attack on the chosen target. This kind of attack is considered in this paper. We proposed a methodology for detecting and preventing such attacks by exploiting distributed P2P networks.

4. Proposed methodology

This section provides a methodology that is employed for detection and prevention of DDoS attacks in P2P networks. There are two networking domains known as core networking and edge networking. The former provides high speed routers and it is the main network. The latter makes use of edge routers to connect to the core network. Both of them are prevalent in the real world WAN architectures. Generally, edge network consists less number of users and less traffic is flown. With respect to DDoS attack traffic, a defence system needs to be in place for efficient detection and prevention of such attacks. Victim end edge network can easily detect attack but cannot respond easily when the traffic is heavy. The proposed mechanism shown in Figure 6 makes use of TTL values of victim node and spoofed addresses to recognize anomalies. The notation of agent is used to effectively keep track

of node details required for effective detection DDoS attacks in P2P networks.

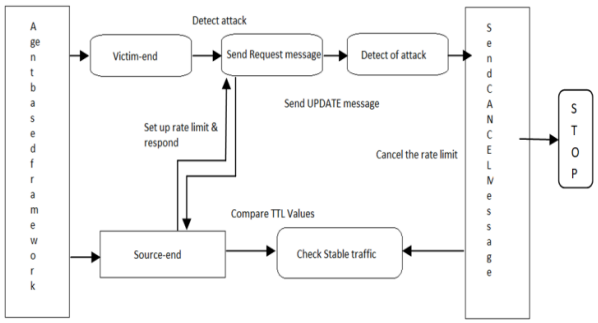


Fig. 6: Proposed Methodology.

The defense mechanism is kept at the victim end. Once the attack is detected at the victim end, the source-end edge network employs attack traffic rate limit control. Fast Internet Trace back [11] is an existing approach used to find all source-end edge networks. The distributed framework ensures that edge routers maintain the distance between nodes and IP address by changing IP header. The maximum lifetime of an IP packet is provided in the form of TTL value. As the packets go through routes on their path, the TTL value is decremented by the routers accordingly. When the TTL value reaches zero, the packet is discarded by the router. This is meant for avoiding loops in the WAN. There is three-way handshake during an attack. First, the attacker sends forged SYN request to the victim. The request reaches TCP slaves and then reaches the victim. From victim the RST packet reaches TCP slaves. RST and SYN packets do have the same source IP address. However, in case of SYM, the IP address is spoofed. Two packets, however, claim to be originated from same source. However, their TTL values differ. The rationale behind his is that the SYN packet has spoofed IP address. An important observation is that RST packet is generated by the victim in response to SYN/ACK packet coming from TCP slaves. Attacker has no control over this packet. Therefore the IP address on the RST can be considered trusted.
As shown in Figure 6, there are three kinds of alert messages being flown. They are request messages, cancel messages and update messages. These messages are appropriately used to defeat DDoS attacks. First, a request message is sent from victim end to know suggested limit value to source end. If there is an increase in the volume of attack traffic, an update message is sent to source end. This will ensure that the rate limit is under control. Based on the requirements, the source end defense mechanism can decrease the limit value. Once attack traffic is reduced to normally, then the rate limit may be increased. If any anomalous changes are not found, then a cancel message is sent to remove rate limit. Here is a problem as well. Due to flooding of attack traffic, the messages may not reach the destination. For this reason, the request and update message are send repeatedly until there is an acknowledgement from the source.

5. Experimental results

Experiments are made with NS2 simulations. The results are as presented in this section.

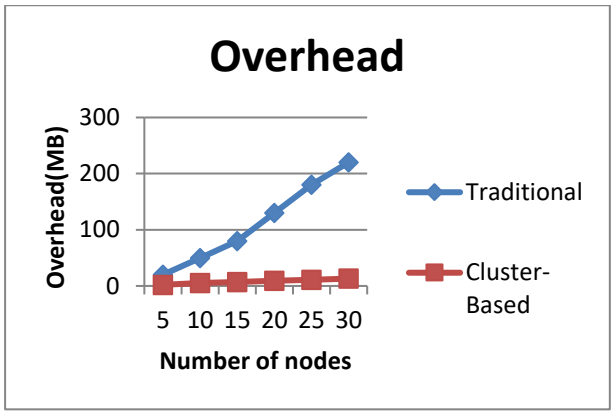


Fig. 7: Number of Nodes vs. Overhead.

The above graph shows a variation of overhead in traditional approach and cluster based approach. It shows which approach gives better performance graphically. Overhead reduction performance is better by cluster approach than by traditional approach.

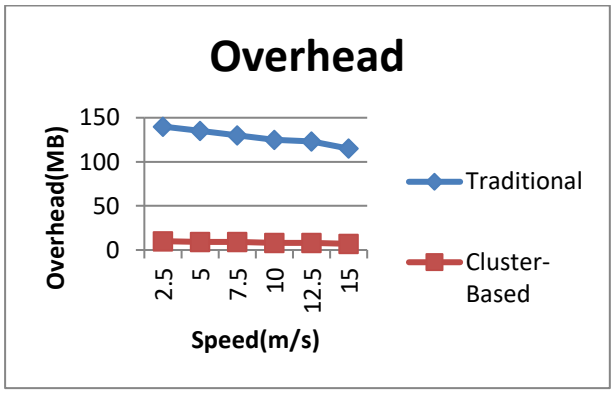


Fig. 8: Speed vs. Overhead.

The above graph shows a variation of overhead in traditional approach and cluster based approach. It shows which approach gives better performance graphically. Overhead reduction performance is better by cluster approach than by traditional approach.

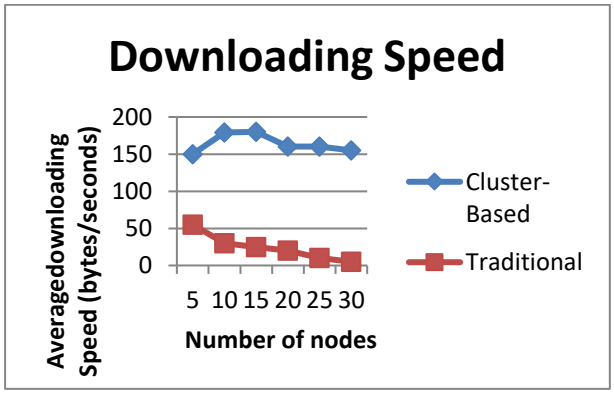


Fig. 9: Number of Nodes vs. Average Downloading Speed.

The above graph shows a variation of downloading speed in traditional approach and cluster based approach based on speed variation. It shows which approach gives better performance graphically. Speed performance is improved in cluster based approach than in traditional approach.

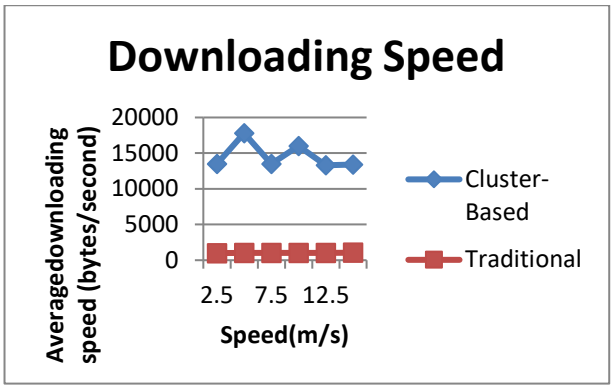


Fig. 10: Speed vs. Averaging Download Speed.

The above graph shows a variation of downloading speed in traditional approach and cluster based approach based on the number of nodes variation. It shows which approach gives better performance graphically. Speed performance is improved in cluster based approach than in traditional approach.
The above graph shows a variation of power efficiency in traditional approach and cluster based approach based on number of nodes variation. It shows which approach gives better performance graphically power efficiency performance is improved in cluster based approach than in traditional approach.

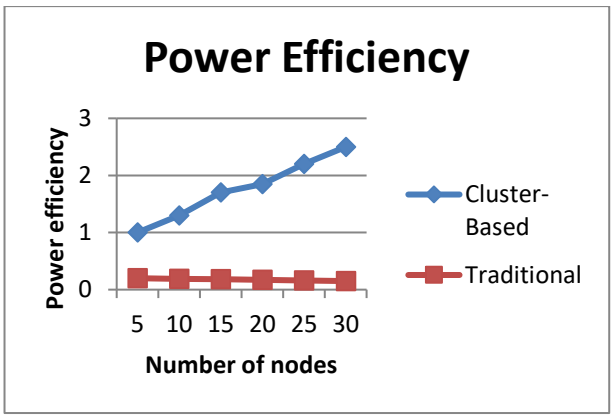


Fig. 11: Number of Nodes vs. Power Efficiency.

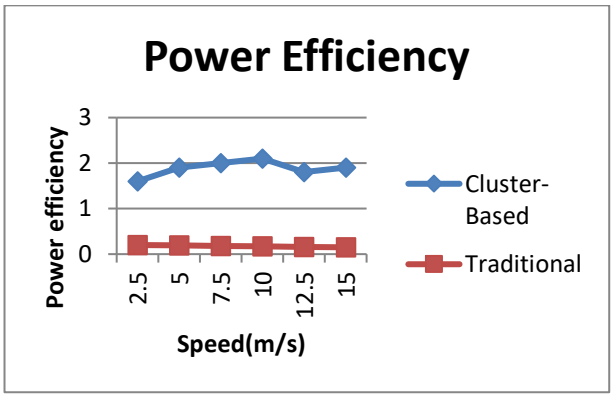


Fig. 12: Speed vs. Power Efficiency.

The above graph shows a variation of power efficiency in traditional approach and cluster based approach based on speed variation. It shows which approach gives better performance graphically .power efficiency performance is improved in cluster based approach than in traditional approach.

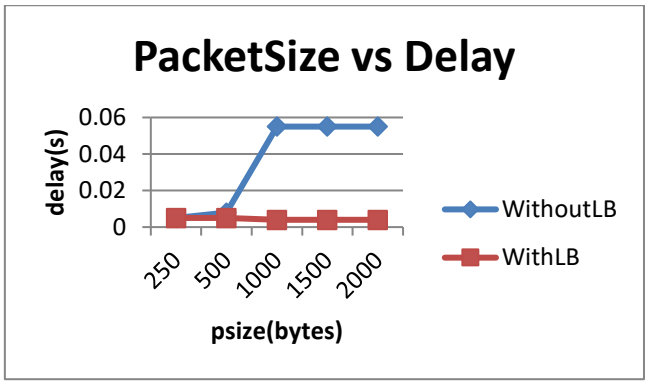


Fig. 13: Packet Size vs. Delay.

The above graph differentiates packet size and delay performance that is how much delay is presence with respect to the packet size. Here we take x axis as packet size and y axis as a delay. The packet delay can be reduced in with LB than in without LB.
The above graph differentiates packet size and delay performance that is how much delay is presence with respect to the packet size. Here we take x axis as packet size and y axis as delay. The packet delay can be reduced in with LB than in without LB.

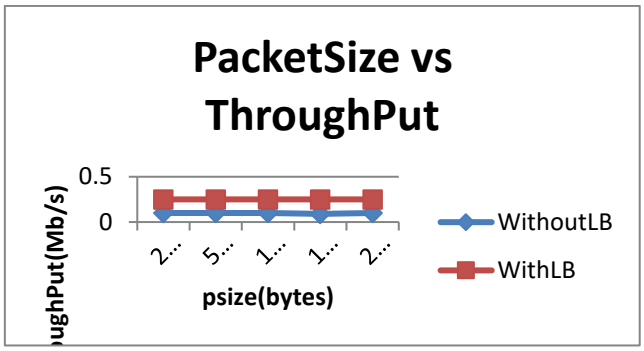


Fig. 14: Packet Size vs. Throughput.

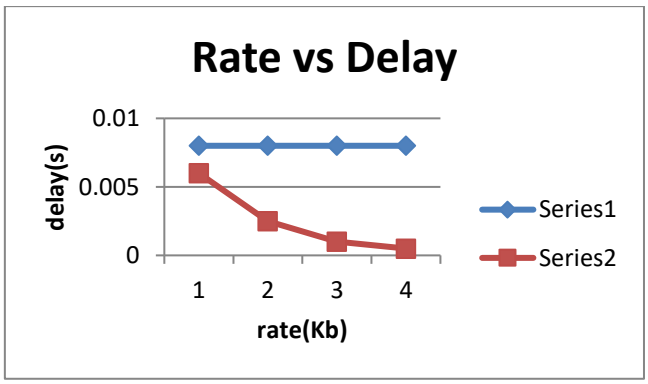


Fig. 15: Rate vs. Delay.

The above graph differentiates packet size and Throughput performance that is how much throughput is presence with respect to the packet size. Here we take x axis as packet size and y axis as Throughput. Throughput performance is better in with LB than in without LB.

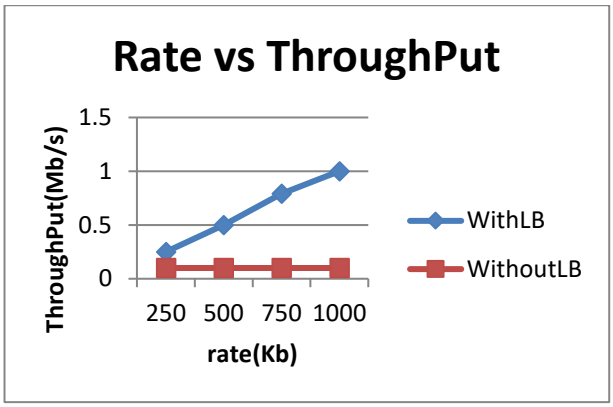


Fig. 16: Rate vs. Throughput.

The above graph differentiates rate and delay performance that is how much delay is present with respect to the delay.Here we take x axis as rate and y axis as a delay. Delay performance is better in Row165 than in Row164.
The above graph differentiates rate and Throughput performance that is how much throughput is present with respect to the rate. Here we take x axis as rate and y axis as Throughput. Throughput performance is better in with LB than in Without LB.

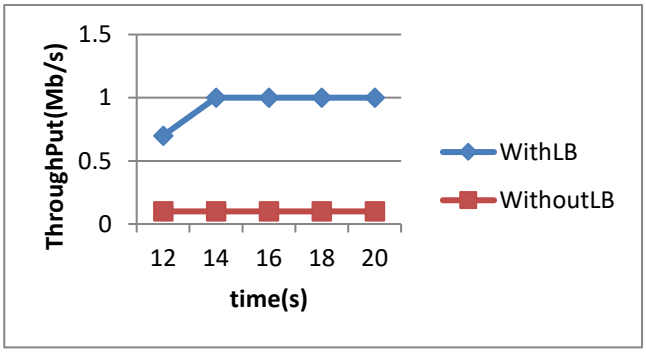


Fig. 17: Time vs. Throughput.

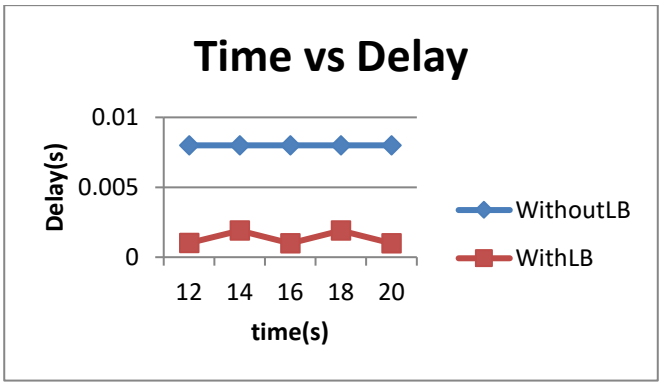


Fig. 18: Time vs. Delay.

The above graph differentiates time and delay performance that is how much delay is a variety with respect to the time. Here we take x axis as time and y axis as a delay. Delay performance is better in with LB than in Without LB.

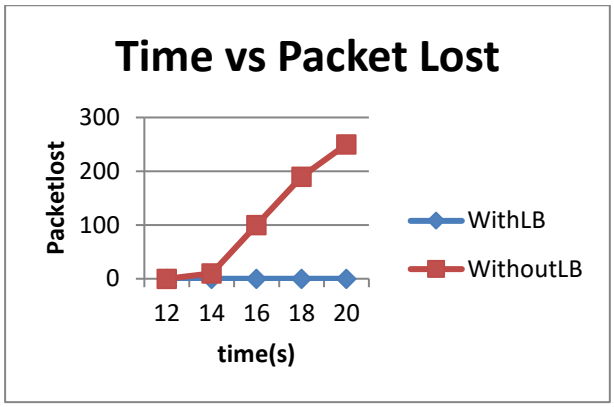


Fig. 19: Time vs. Packet Lost.

The above graph differentiates time and packet lost performance that is how many packets are lost is variant with respect to the time. Here we take x axis as time and y axis as packet lost. Packet lost performance is better in with LBthan in WithoutLB.
The above graph differentiates time and queue size performance that is a variation of queue size with respect to the time. Here we take x axis as time and y axis as queue size.

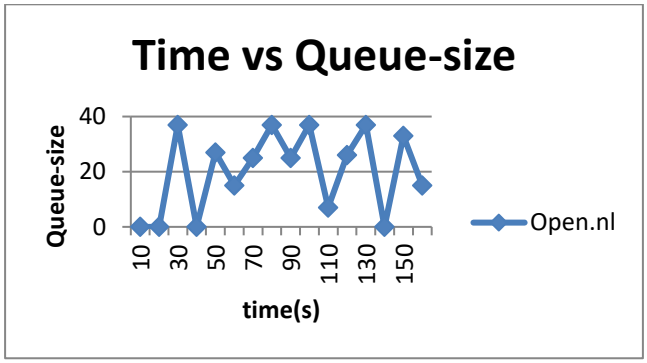


Fig. 20: Queue Size vs. Time.

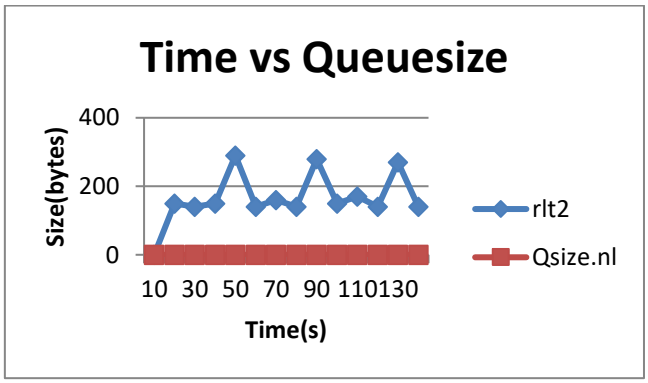


Fig. 21: Queue Size vs. Time.

The above graph differentiates time and queue size performance that is a variation of queue size with respect to the time. Here we take x axis as time and y axis as queue size. It shows the performance of queue size in rlt2 and in Qsize.nl.

6. Conclusions and future work

In this paper, we studied DDoS attacks in distributed P2P networks. It is understood that real time distributed P2P networks such as Napster, Chord, Freenet, and Gnutella are vulnerable to DDoS attacks as they are suitable for launching Denial of Service (DoS) attacks by using them as a vehicle for administering attacks. The distributed nature of P2P network has made them vulnerable to such attacks. Botnets and P2P networks are used by adversaries to launch attacks. It is very difficult to have a quick response to the DDoS attack as in flooding-based DDoS attack because of the

presence of source-address spoofed machines are involved in large scale. In the literature, many techniques was found to mitigate, detect and prevent DDoS attacks. However, it is understood that with respect to P2P networks, it is an optimization problem and still open problem to be addressed. Towards a good solution, multiple parameters are considered in the proposed framework. They are the distance between the source and victim nodes and also TTL value used for effectively identifying the presence of a DDoS attack. The concept of agent is used to maintain the dynamic information of nodes, bandwidth and the capacity of nodes for helping in efficient trace back. Simulation, study is made using NS2 for proof of the concept. The results revealed the utility of the proposed framework in detecting and defending P2P networks against DDoS attacks. There are important directions for future work. It is interesting to combine multiple approaches and investigate the performance against DDoS attacks. The investigation into blockchain, adapting it for defending P2P networks from DDoS attacks, which is an innovative technology for safeguarding not only financial transactions for virtually everything of value.

References

[1] Cho JH, Chang SA, Kwon HS, Choi YH, KoSH, Moon SD, Yoo SJ, Song KH, Son HS, Kim HS, Lee WC, Cha BY, Son HY & Yoon KH (2006), Long-term effect of the internet-based glucose monitoring system on HbA1c Reduction and glucose stability: a 30-month follow-up study for diabetes management with a ubiquitous medical care system. *Diabetes Care* 29, 2625–2631.

[2] Fauci AS, Braunwald E, Kasper DL & Hauser SL (2008), Principles of Harrison's Internal Medicine, Vol. 9, 17thedn. *McGraw-Hill*, New York, NY, pp.2275–2304.

[3] Kim HS & Jeong HS (2007), A nurse short message service by cellular phone in type-2 diabetic patients for six months. *Journal of Clinical Nursing* 16, 1082–1087.

[4] Lee JR, Kim SA, Yoo JW & Kang YK (2007), The present status of diabetes education and the role recognition as a diabetes educator of nurses in korea. Diabetes Research and Clinical Practice 77, 199–204.

[5] McMahon GT, Gomes HE, Hohne SH, Hu TM, Levine BA & Conlin PR (2005), Web-based care management in patients with poorly controlled diabetes. *Diabetes Care* 28, 1624–1629.

[6] Thakurdesai PA, Kole PL & Pareek RP (2004), Evaluation of the quality and contents of diabetes mellitus patient education on Internet. *Patient Education and Counseling* 53, 309–313.