ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

Distinguish DDoS Attacks and Suggesting Some Counter Measures For Distributed P2P Networks

[1] Gera Jaideep, [2] R.V.Kishore Kumar, [3] Dr.B.V.V.S.Prasad
[1] Research Scholar, Dept.of CSE, Acharya NagarjunaUniversity, Guntur, India
[2] Research Scholar, Dept.of CSE, Acharya Nagarjuna University, Guntur, India
[3] Associate Professor, Dept.of CSE, DRK College of Engineering and Technology, Hyderabad, India

Abstract:- **Peer-to-Peer networks became more popular in now days because of its useful delivery services. It utilizes distributed resources to perform some intended activities. Because of its distributed in nature they are widely used in file sharing. For every network there is a common problem that is an attack, it may of many types in those most complicated and highly threatening and hard to detect attack in distributed Peer-to-Peer network is Distributed Denial of Service (DDoS) attack. An attack that interrupts the services to all the users is DDoS attack. Many techniques are in existence to solve the DDoS attack but still hard to respond in short time to flooding based DDoS attacks. The reason is this attack is made by intruders or opponents who use large number of attacking machines by a method of source address spoofing. In this paper we proposed architecture, this designed structure defend and detect DDoS attacks. Here we can resolve this with the help of two important parameters. Time-to-Live (TTL) value and the distance between victims source to victim's destination. This architecture can take care of agent-based trace back, traffic control and detection of DDoS attack. The proposed methodology can detect and prevent DDoS attacks and ensure Quality of service for real traffic.**

Keywords **— DDos attack, Distributed Peer-to-Peer Networks, security, agent-based approach.**

I. INTRODUCTION

Peer-to-Peer (P2P) network are generally distributed in nature, they are widely used in file sharing services. These networks are exposed to possibility of being attacked to DDoS attack. Flooding based Attack is a common DDoS attack. It attacks on the victim's machine by sending flood of traffic continuously to make the system slow down and leads to crash. DDoS attacks the aimed resources like infrastructure, hosts on the internet and other resources by pushing different types of attacks like protocol attacks, resource exhaustion and vulnerability attacks. So a compatible solution is needed for distributed P2P networks. The main reason behind the DDoS attacks is classified into financial gain, intellectual challenge, cyber warfare, revenge etc... There are two procedures to launch DDoS attacks.

1. Sending the distorted packets to victim to confuse called as vulnerability attack.
2. In the second procedure attacker can do one of the following actions. A) Network resources and existing bandwidth. B) Exhausting server resources.

Sending the distorted packets to victim comes under flooding attack at network level and second approach attack on the resources comes under flooding attack at application level. These attacks are remotely controlled and send huge amount of traffic to target in order to make the machine slow down in rendering services or deny the services by crashing the system. DDoS attacks are massive attacks that are launched over Internet. A large scale of attack is made on Yahoo in February 2000 that caused the portal inaccessible to users for more than three hours. In the same way Amazon, eBay, CNN etc were attacked by DDoS attacks and result is either slow down services or stops functioning completely .Here we have four major steps in DDoS attacks, those are selection of agents, compromising the agents, communicate with them and then perform attack in very large scale as shown in the Figure 1

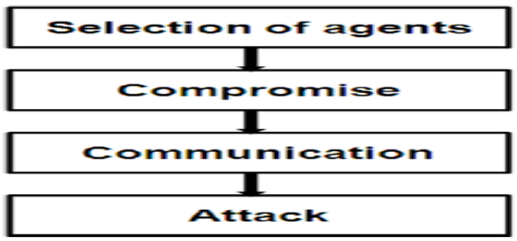


Figure 1- Steps involved in DDoS attacks

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

The primary goal of counter measures is to analyze the traffic and identify the DDoS attack in distributed P2P networks and reduce the harm .The method to handle DDoS attack should have a strong detection technique, defense framework, a good response technique and best performance analysis. In this paper we proposed an agent-based solution to DDoS attacks. Here we can resolve this with the help of two important parameters. Time-to-Live (TTL) value and the distance between sources to victim's destination. This proposed method focuses on agent-based trace back, traffic control and detection of attacks. Coming sections we discuss about the relevant literature and present state of the art on DDoS attacks on distributed P2P networks and there counter measures, methodology which contains counter measures to identify and prevent the DDoS attacks.

II. RELATED WORKS

Zhou et al. (2010) [5] made a survey of coordinated attacks such as DDoS attacks. They have discussed in detail about collaborative intrusion detection mechanisms that are classified into centralized, decentralized, hierarchical collaborative techniques. Zeidanloo et al. (2010) [3] discussed in detail about taxonomy of techniques pertaining to botnet techniques. They categorized the techniques in to host-based and network-based techniques. Locher et al. (2010) [7] discussed in detail about attacks on Kad network which is distributed hash table based P2P network. The attacks include node insertion attack, publish attack, and eclipse attack. Kad can also be used to launch DDoS attacks. Kim et al. (2009) [11] discussed in detail about byzantine attacks in P2P networks and suggested packet based signature scheme to intercept them. Hwang and Li (2010) [8] focused on data coloring and secure resources to secure cloud computing operations. Zeidanloo et al. (2010) [12] proposed a method of detecting DDoS attacks. They discussed in detail about a traffic monitoring approach based on botnet detection. They suggested a detection framework that uses similarity in traffic structures in order to detect attacks. Zin et al. (2010) [15] proposed a protocol for protecting network from primary user emulation attacks. Huang et al. (2010) [9] discussed in detail about web forms and DDoS attacks that are hard to detect. The defense mechanisms they proposed include prevention of attacks, detection and management of attacks, and launch pads and victims. Ciccarelli and Cigno (2011) [10] discussed in detail about P2P systems and security vulnerabilities. Especially they focused on survey of collusion attacks. Bhuyan et al. (2012) [2] discussed in detail about different methods of DDoS attacks and tools for preventing such attacks. Different types of DDoS attacks discussed are HTTP flood, SYN flood, ICMP flood, UDP flood, TCP attacks, DNS, SMTP, VoIP and others. DDoS detection methods are classified into statistical, knowledge based, soft computing, data mining and machine learning. Sabu M.Thampi et al.(2012)[16] discussed in detail about recent trends in computer networks and mainly focused on how to calculate distance between source to destination.
Geva et al. (2013) [4] opined that Distributed Denial of Service (DDoS) attacks cause serious threat to the Internet. They focused on Bandwidth DDoS (BW-DDoS) attacks... Yu et al. (2012) [13] studied DDoS attacks as threat to Internet and distributed applications over Internet. Their main focus was to find a mechanism that could discriminate DDoS attacks from flash crowds. These attacks make use of many hosts in order to send huge amount of traffic that is beyond the capacity of bandwidth of the network. Thus it causes packet losses and congestion besides disrupting legitimate traffic. The attacking agencies are known as puppets or zombies and root-zombies. et al. (2013) [1] made a survey of defenses against DDoS flooding attacks.
Rossow (2014) [6] studied network protocols that are exploited for DDoS abuse. Especially they focused on the amplifiers of DDoS attacks. Here the role of amplifiers is to increase the intensity or volume of attack. Francois et al. (2014) [14] proposed a framework known as FireCol for detection of flooding DDoS attacks. They proposed Intrusion Prevention Systems (IPSs) that are to be included as part of Internet Service Providers (ISPs) in order to have counter measure against DDoS attacks.

III. PROPOSED METHOD

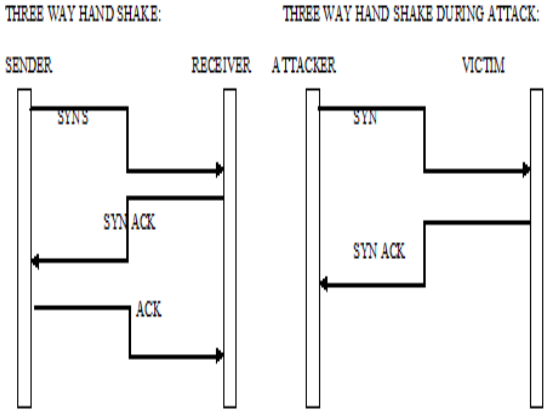
Three way handshake Process:-
In three ways handshake procedure id an user who is authorized to send packets will send SYN packet to victim. It will get ACK and again ack is send to victim. If Intruder send SYN packet to victim it will get SYN ACK but never sends ACK packet to Victim. Whenever victim didn't get acknowledgement from source then it is identified as Intruder.

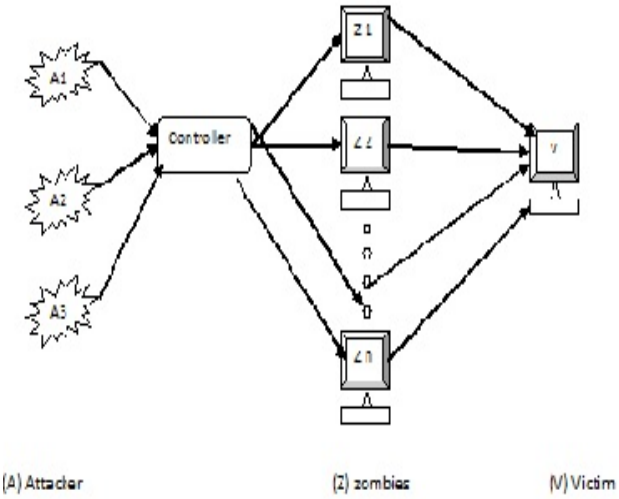
DoS attack:-

The ultimate goal of Denial-of-service (DoS) attack is to make unavilability of a machine or network resource to its authorized users .That means Attacker blocks the connection between user and service. Here the problem is same as DoS attack but the difference is the attacker blocks the connection between multiple users and service.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

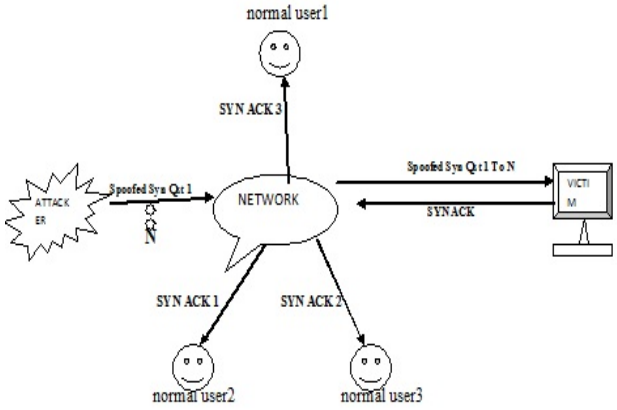




Mechanisms of Flooding based DDoS attack:-
It involves agents or reflectors sending a huge amount of unwanted traffic to the victim. Basically these attacks are of two types

1. Direct flooded based DDoS attack
2. Reflector flooded based DDoS attack.

Direct flooded based DDoS attack Attacker will send packets directly to victim using IP spoofing method it means hiding the real address of valid user. Victim receives the request packet from attacker and revert back the acknowledgement packets to valid users. In these process valid users known's someone is hacking our account after getting acknowledgement from victim. In a reflector attack, the response packets from reflectors truly attack the victim. No response packets need be sent back to reflectors from the victim.



Direct Flood Based DDoS Attack

Time-to-Live (TTL):
It is used to fix the life span of the data in a network; data gets killed from the network if the prescribed TTL time elapses. This mechanism is used to avoid any data packet from circulating indefinitely in a network. It means the number of hops that a packet travels in network until it kills. This TTL is present in IP header. A hop means travelling of a packet from one router to another router in a network on the way to its destination. Packet can travel through routers, bridges, gateways. Each time packet are passed to the next device a new hop occurs. Hop count and packet travel path is shown in Figure 2.

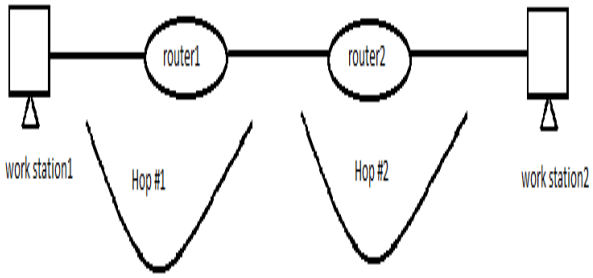


Figure 2: shows the count of the hop

Here in the above diagram work station 1 is source and work station 2 is destination and we have two routers so TTL status is 2, TTL status can be identified by hop count .If the count of TTL is greater than zero then router sends the packet to next level or else kills the packet and triggers cancel message to the source .We can assign any value from 1 to 255 to TTL. For Example: If Hop count is 3 and if we assign TTL value as 255, then for every interface TTL value subtracts by 1 and at the time of destination TTL value will become 252.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

In this method first step is source sends request to victim's destination. Victim checks the TTL status for the packet. Here every packet has some TTL value, if packet comes from attacker it has some TTL value and for genuine user it has some TTL value. By the TTL status we can detect the attack even users were attacking by spoofing process.

If TTL status matches with user at victim side, it grants the permission to access services by sending update message.

If TTL status does not match with the user at victims end , then victim will identify source as a intruder or attacker and send cancel message to attacker.

If many number of attackers attacking the victim at same point of time then traffic increases aggressively, at this time TTL status for every user is verified and sends the cancel message to the intruder and update message to genuine user. But this will take some time to process so it may slightly increase the burden on victim.

Due to this unnecessary flooded traffic, There is a chance that victim sends the message to source end may not even reach the source node. To provide solution for the above problem, request and update message will sent more number of times to source end by victim until it gets proper acknowledgement that is received from the source.

Distance between Source and Destination:

Based on the time taken by the packet to travel from source end to destination end is taken into consideration. We have two steps to find out the distance.

1. Identifying the number of hops or nodes present in between source and destination.
2. Identifying the distance between sources to next hop.
3. Identifying the distance between sources to destination.

By calculating the number of hops in between source and destination and distance between source and next hop we can calculate the distance from source to destination. From this we can get the distance a packet has to travel from source to destination.[16]

Whenever the expected time reaches the limit then the node decides that there is an attacker and kills the packet and sends cancel message to attacker and requests the genuine user to send the packet again.

With the help of TTL and distance, when ever attack occurs agent will apply the counter measure that is proposed in this paper. The agent checks distance and TTL values of packets to identify unwanted and mischievous traffic, whenever agent finds that traffic it kills the packet and sends cancel message.

IV. CONCLUSION

We have studied many DDoS attacks and its counter measures, major challenge in detecting and preventing DDoS attack is speed, how much speed in which detection mechanism works .The focus of this paper is to detect and preventing the DDoS attack in distributed P2P networks. We proposed agent-based mechanism to detect and prevent DDoS attacks .In this proposed mechanism we have three major phases. First we have to detect the DDoS attack by analyzing the traffic to find inconsistencies in distance and TTL.IN second phase at victims end defense mechanism will find all the edge nodes through which traffic is forwarded. Thereafter source side defense mechanism is modified in the way to exercise the limits on edge nodes with respect to traffic rate. Then the retrieval process is started when traffic at victims end came to normal. This work can be extended further to make more effective performance by combining two or more defense mechanisms to have very comprehensive approach to prevent DDoS attacks in Distributed P2P networks.

REFERENCES

[1] Saman Taghavi Zargar, James Joshi and David Tipper. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, p1-24.

[2] Monowar H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya and J. K. Kalita. (2012). Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions. The Computer Journal, p1-20.

[3] Hossein Rouhani Zeidanloo, Mohammad Jorjor Zadeh shooshtari, Payam Vahdani Amoli, M. Safari and Mazdak Zamani. (2010). A Taxonomy of Botnet Detection Techniques. IEEE , p1-5.

[4] Moti Geva, Amir Herzberg and Yehoshua Gev. (2013). Bandwidth Distributed Denial of Service: Attacks and Defenses. IEEE. 10, p1-10.

[5] Chenfeng Vincent Zhou, Christopher Leckie and Shanika Karunasekera. (2010). A survey of coordinated attacks and collaborative intrusion detection. Elsevier, p1 2 4 – 1 4 0.

[6] Christian Rossow. (2014). Amplification Hell: Revisiting Network Protocols for DDoS Abuse. Internet Society, p1-15

[7] Thomas Locher, DavidMysicka, Stefan Schmid, and Roger Wattenhofer. (2010). Poisoning the Kad Network. Springer-Verlag Berlin Heidelberg , p195–206.

[8] Kai Hwang and Deyi Li. (2010). Trusted Cloud Computing with Secure Resources and Data Coloring. IEEE , p1-9.

[9] Scott C.-H. Huang, David MacCallum and Ding-Zhu Du. (2010). Network Security. Springer , p1-284

[10] Gianluca Ciccarelli and Renato Lo Cigno. (2011). Collusion in Peer-to-Peer Systems. Computer Networks. 55 , p3517–3532

[11] MinJi Kim, Luısa Lima, Fang Zhao, Joao Barros, Muriel Medard, Ralf Koetter, Ton Kalker and Keesook J. Han. (2009). On Counteracting Byzantine Attacks in Network Coded Peer-to-Peer Networks. IEEE , p1-26.

[12] Hossein Rouhani Zeidanloo, Azizah Bt Manaf, Payam Vahdani, Farzaneh Tabatabaei, Mazdak Zamani. (2010). Botnet Detection Based on Traffic Monitoring. 201O International Conference on Networking and Information Technology, p1-5.

[13] Shui Yu, Wanlei Zhou, Weijia Jia, Song Guo, Yong Xiang, and Feilong Tang. (2012). Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS. 23 (6), p1-8.

[14] Jerome Francois, Issam Aib and Raouf Boutaba, Fellow. (2014). FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks. IEEE , p1-15

[15] Z. Jin, S. Anand and K. P. Subbalakshmi. (2010). Robust Spectrum Decision Protocol against Primary User Emulation Attacks in Dynamic Spectrum Access Networks. IEEE, p1-5

[16] Sabu M.Thampi , Albert Y.Zomaya, Thorsten Strufe, Jose M.Alcaraz Calero and Tony Thomas(2012).Recent Trends in Computer Networks and Distributed Systems Security , International Conference, SNDS 2012, Trivandrum.

[17] B.V.V.S. Prasad, Multicasting in MANET's Through Scalable Mobility – Aware Virtual Tree Based Geographic routing Protocol, Voluem 4, Issue 1, January 2013. ISSN: 2229 – 5518