International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

A Survey on DDOS Attack in Manet

Avantika Bhate

[1]*Masters in Computer Science & Engineering, VIT University, SCOPE School, Vellore, India.*

Abstract - *As we can see in the modern computer world, it is difficult to maintain the information. There is a possibility that interrupts may occur in local system(attack) or network-based system. One of such attacks are identified in MANET (Mobile Ad hoc network). MANET is a collection of nodes with a self-configuring network connected through wireless links and a network without infrastructure. This paper aims to explore the security issues which are significantly affecting the performance of MANET. The attack identified is DDoS (Distributed Denial of Service) attack in which malicious user creates high traffic by sending large amount of data due to which the licensed user cannot use resources properly. In this paper a new algorithm is proposed to stop DDoS attack which will provide more security to the system.*

Key Words: MANET, misbehaviour, detection, attacking node

1. INTRODUCTION

In today's scenario, we can see the use of internet has increased for communicating with each other. We can see currently internet is not only used for sending mail and chats but also plays a huge role in the field of business, education, media and many more. Internet has changed the lifestyle of people and made our life easier. It has a huge impact in our business, education and in everyday life. But there arises a question whether it is safe or not, whether is provides security. The answer is 'no' it is not secure enough to use. This is because as internet grows, number of attack and security issues also increases. And one of the major attacks and security issue raised is DDoS (Distributed Denial of Service) attack. DDoS attack typically exhaust bandwidth, capacity of processing or about the memory of target machine, service or network. Despite of enormous efforts applied to solve the issues in past decade, DDoS attack still have a serious threat to the security of cyberspace. As we know security is considered as the main issues which has to handled effectively for the network to work properly. The main aspects to be considered for secured ad hoc are:

Confidentiality: It ensures that none of unauthorized user is getting the access for transmitting the data.

Availability: Data and resources should be available when required. This is a major issue due to DoS and DDoS attack in MANET.

Authentication: it ensures that only the authenticated user is getting the data rather than the other attacker node.

Integrity: ensures that the data is transmitted without any change.

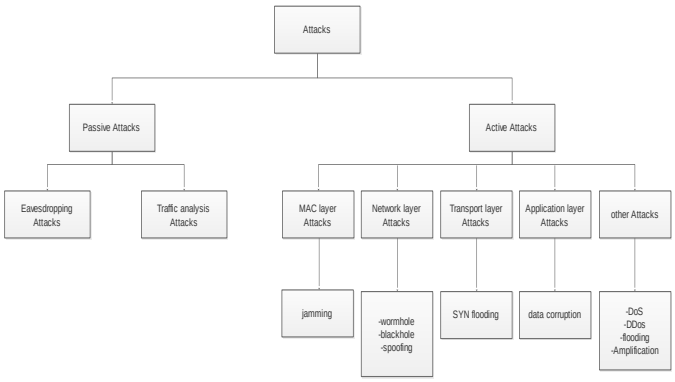

FIG-1: Attacks in the MANET

Types of Attack: Frequently occurred attack on MANET are:

Jamming attack: One of the attacks caused in the physical layer. When the interference is occurred in the authorized wireless communication which causes interrupts in real traffic source from sending and receiving the packets.

Wormhole attack: Another type of attack which has a huge effect on network layer. In these nodes fakes the route that are shorter within the network then the original one which creates the confusion to the routing mechanism that depends on the knowledge about the distance between the nodes. In these the attacker collects the packets from one location and send it to another located node. The attacker can easily launch the wormhole attack without having any knowledge of network.

Denial of service attack: Another type of attack the creates a security issues in the MANET. It is a security event which occurs when the attacker injects the large number of junk packets within the network and prevents users from accessing the network resources. It is typically a flood servers or networks with heavy traffic which overwhelm the victim resources and make it difficult for user to use the resources.

Flooding attack: This is one of the DDOs attack which are launched due to the flooding of network by sending the fake RREQs or by sending the Data packets which creates

congestion in the network which results in the reduction of probability of data transmission of the nodes.

Amplification/Reflection attack: It is one of the DDoS attacks which results in large number of packets to flood the target node without alerting the intermediary, which results in large number of replies to the generated request. These attacks can be handled by blocking the spoofed source packets. One of the types of Amplification attack is DNS amplification attack.

2. REVIEW OF THE SYSTEM

Distributed Denial of Service attack: Denial of service or Distributed Denial of Service attack is one of the attacks which has been evolved from few decades. It is attempt to make resources unavailable for the intended user. In these the multiple users attack the target node and make the services unavailable by sending false packets and acknowledgment. DDoS attack is frequently followed by the attacker, in these the master and agent terminal controls the attacker packets and the master sends the message for attacking the target and then the multiple user sends off multitudes of camouflaged packets to attack the target, which results in consumption of huge resources of the target and crashing of system. With the study of network and communication the attacker can attack in various form and can create security issues in MANET.

We have now the security attacks has increased on the internet which has increased the threat rate and the data transmitted over the internet is not safe and we have to apply many safety measures for transmitting data.

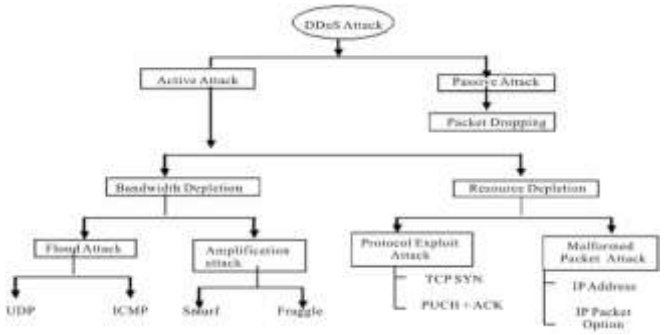

FIG-2: DDOS Attack Taxonomy

DDoS attack has a huge impact on the MANET due to increase in attacker the data transmission becomes difficult and because of unauthorized usage the intended users don't get the resources. In DDoS attack one of the attacks identified is Amplification/Reflection attack we occur due to the large number of packets which are transmitted over to the flood the target. To solve the problem Defense scheme are applied.

In these paper, two techniques have been adopted for DDoS attack i.e. Amplification and Reflection attack. In the reflection attack it exploits the IP spoofing vulnerability. In these the attacker sends the forged IP address to the server which are exploited as a reflector which directs its responses to the fake address. This technique is performed on the TCP and UDP protocol.

The impact of this attack can be measured when number of generated responses increases by larger rate as compare to the number of requests. Such effect can be referred as Amplification.

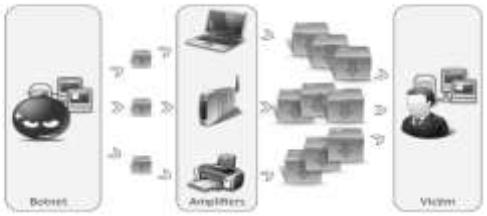

FIG-3: Amplification/reflection DDoS attack schema

3. THE DEFENCE SCHEME AGAINTS AMPLIFICATION ATTACK:

DNS (Domain name system) amplification attack and NTP (Network time protocol) are most of the frequently used protocols which are employed to perform the Amplification and Reflection DDoS attack.

DNS Amplification attack:

It is one of the protocols named as domain name system used as a distributed hierarchical system which is used for resolving the names of network hosts. It is defined on RFC 1034 and RFC 1035. DNS queries has been classified into two categories: Recursive and Non-Recursive. In these the larger number of DNS server are involved. In these the attacker sends the DNS name look-up request to server by spoofing the IP address of the target. Attacker tries to collect as much as information possible by amplifying the DNS response which has been sent to the target.

NTP Amplification attack:

It is a protocol which is designed to show the clock synchronization of system. It has a capability to increase the local time precision over the packet routing over the variable latency. The function which is performed on the NTP is **monlist** command. This sends the details of the at least 500 hosts that has generated the request of time from the NTP server back to the requester.

Both protocols are used for solving Amplification attack and for comparing the protocol NESSI network simulator has been developed.

4. SIMULATION MODEL:

Network Security Simulator is a research-based technique which aims on security-based research. It has been designed on three tier plugin architecture which are categorized as: Graphical Frontend, agent-based simulation as backend and the database.
The frontend deals with the creation and modification of network topologies and also specifies the behavior of the network element.
The backend is component which is used to carry out the simulation process. It is used to create and setup the simulation environment. It is connected to the database which store the simulation data.
The simulation results which are obtained is stored in the database so that they can be used for further evaluation. With this is becomes easy to track the traffic generated on the server.
The simulation model which has been developed consists of three entities i.e. **master**, **Zombie** and **server**.

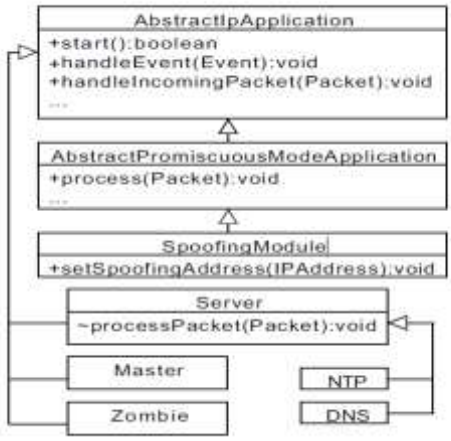

Chart -1: Simulation Model

It consists of three methods namely a) **start** setup the application parameters, b) **handleEvent** used for handling the events and for generating and scheduling the new events and c) **handleIncomingPacket** which is used to deal the incoming packets. The classes used have different working in the model i.e. the master class designs the behavior of attacker. It searches for all the attacker agents and sends them the UDP packets. The zombie class models the behavior of each malicious code and the code which has been transmitted affects the attacker machine. When the packets are transmitted and received over the network by the zombie it extracts the information stored in it for configuring the attack.

5. SIMULATION RESULT:

The model was proposed for comparing the effects of DNS and NTP amplification attacks. The scenarios consisting of 200 botnet zombies and 5 exploits servers which consisting of 250 Mbits/s of bandwidth. The effect where calculated by considering some of the points:

- Link inside zombie subnet which is used for evaluating the bandwidth,
- Link which is related to the server subnet which is used for evaluating the traffic,
- Link between server and the victim subnet which is used for observing the power.

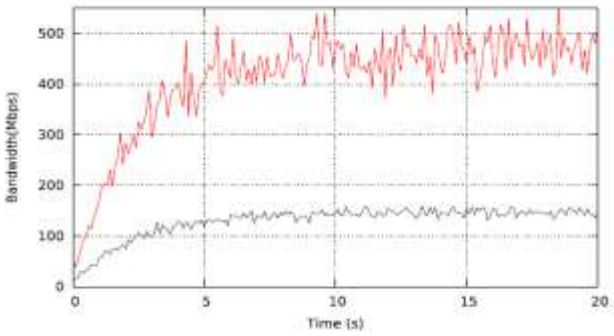

Chart -2: Comparison between DNS and NTP impact on victim link

In the above graph the continuous line obtained show the amount of traffic generated by the NTP server and the dashed line represents the traffic generated by the DNS server.

Table -1: Statistics table for victim link:

Protocols	DNS	NTP
Packet	78456	193546
Time-interval	2100	20030
Average of packets/second	5000	114795
Average Mbits/second	150	410
Max. bandwidth	250	500

On the basis of above observation, the graph for the incoming and outgoing packets for the server has been generated.

	DNS	NTP
Avg. of incoming packet	1,3	1,5
Avg. of outgoing packet	50,8	150,8

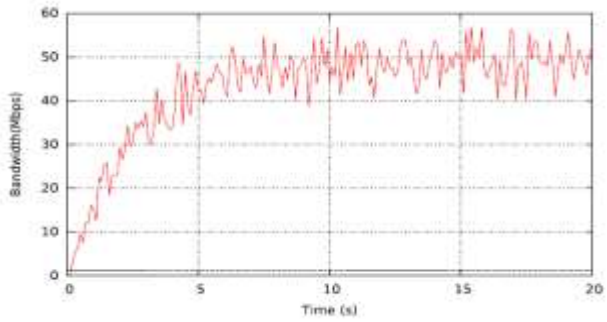

Chart -3: DNS Server in-out

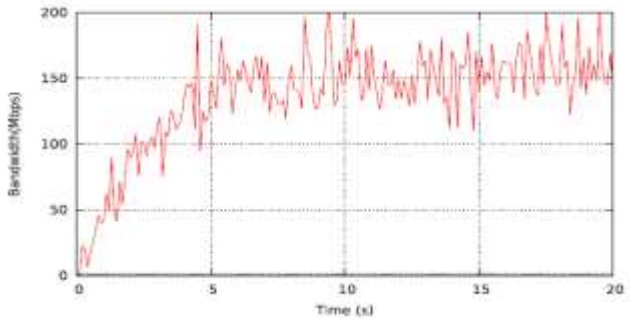

Chart -4: NTP Server in-out

6. CONCLUSION:

Simulation model has been developed for evaluating the DDoS attack. The results obtained tell about the dangerous effect of amplification attack on network and how the single host can create a large amount of traffic and generate the problem in data transmission. But the model helps in reducing the effect of amplification effect on the network and with the help of above model it is easy to develop some new techniques to handle the attack.

ACKNOWLEDGEMENT:

Thanks to VIT University for providing the access for the IEEE scholar publications which helped to refer ample number of publications and also for me to complete the work with ease and additionally the research gate website in which the scholarly articles also provided great reference in finding the problem abstract and which helped me in improving the QOS in terms of the processing in the research.

REFERENCES

[1] TANG Lin, TANG Zhi-de, MA Chao. "Application of Neural Network and IP Marking in DDoS Attack Defense". Computer Simulation, 2008, 25(2): 149-152.

[2] Ahmad Sanmorino1, Setiadi Yazid2, DDoS Attack detection method and mitigation using pattern of the flow,2013 International conference of Information and communication technology (ICoICT).

[3] Muhammad Aamir, Muhammad Arif, Study and Performance Evaluation on Recent DDoS Trends of Attack & Defense, I.J. Information Technology and Computer Science, 2013, 08, 54-65.

[4]]. PyungKoo Park, SeongMin Yoo, Chungnam Nat, Service-Oriented DDoS Detection Mechanism Using Pseudo State in a Flow Router, 2013 International Conference on Information Science and Applications (ICISA).

[5] Saman Taghavi Zargar, Joshi, Member, IEEE, and David Tipper,A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION (2013).

[6] S. Yu, "An overview of DDoS attacks," in Distributed Denial of Service Attack and Defense. Springer, 2014, pp. 1–14.