



Implementing DoS Attack Defence Scheme in Manet

Lovely

CSE & Kurukshetra University,
Haryana, India

Abstract— *Mobile Ad-hoc network is the network comprised of wireless nodes. It has basically no infrastructure . A mobile ad hoc network (MANET) is a spontaneous network that can be established with no fixed infrastructure. Aim of the DOS attack is to overload the server's bandwidth and other resources. A bandwidth depletion and resource depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system. A Scheme is used for the mitigation of DDoS attacks in mobile Adhoc Networks. Performance metrics are used to evaluate the performance of DDoS attacks using packet Delivery Ratio(PDR) and no. of collision. The research objective is the prevention of existing attack and defense mechanisms .*

Keywords— *DDoS, security attacks , Packet delivery ratio, Wireless mobile adhoc network, defense mechanisms.*

I. INTRODUCTION

1.1 MANET

A mobile ad hoc network (MANET) is a spontaneous network that have no fixed infrastructure which is self configured. All of its nodes behave like a routers and take part in its discovery and maintenance of routes to other nodes in the network i.e. nodes communicate with each other via wireless links. Its routing protocol has to be able to support the new challenges that a MANET creates like nodes mobility, security maintenance, (QoS) quality of service, limited bandwidth and only limited power supply. These challenges put a new demands on MANET routing protocols.

Security in mobile ad hoc networks is a hard to achieve due to dynamically changing and fully decentralized topology as well as the vulnerabilities and limitations of wireless data transmissions. The solutions that are already exist that are applied in wired networks can be used to obtain a certain level of security. these solutions are not always be best or always be suitable to wireless networks. Therefore ad hoc networks have their own vulnerabilities that cannot be always tackled by these wired network security solutions.

One of the very distinct characteristics of MANETs is that all participating nodes have to be take part in the routing process. Traditional routing protocols have designed for infrastructure networks cannot be applied in ad hoc networks, thus the ad hoc routing protocols were designed to satisfy the needs of infrastructure less networks. Due to this distinct characteristics of wired and wireless media the task of providing seamless environments for wired and wireless networks is very complicated. One of the major fact is that the wireless medium is inherently less secure than their wired counterpart. this traditional applications do not provide user level security schemes based on the fact that physical network wiring provides some level of security. The routing protocol sets the security in any packet network. If routing can be misdirected, the entire network can be paralyzed. This problem enlarged in ad hoc networks since routing usually needs to rely on the trust worthiness of all nodes that are participating in the routing process. the main difficulty is that it is hard to distinguish compromised nodes from nodes that are suffering from broken links.

1.2 DDoS Attacks in MANETs

Denial of Service or Distributed denial of Service attacks usually occurs in MANETS or in wireless networks. It is an attack where multiple systems comprised together and target a single system causing a denial of service. The victim node is flooded with the data packets that system shutdowns. A Denial of service attack is an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system . A DDoS attack is a distributed, in which large no.of attackers uses to flood the victim network with number of packets. This distrupts the victim network of resources such as bandwidth, computing power, resources etc. The victim is unable to provide services to its legitimate clients. Or in another way we can say that a Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. The services which are under attack are those of the "primary victim", while the compromised systems used to apply the attack are often called the "secondary victims." The secondary victims are used in a (DDoS) Distributed Denial of service attack provides the attacker with the ability to wage a much larger and more disruptive attack while remaining anonymous since the secondary victims actually perform the attack making it more difficult for network forensics to track down the real attacker.

First, it involves the target host that has been chosen to receive the brunt of the attack. Second, it involves the presence of the attack daemon agents. These are agents that actually conduct the attack on the target victim. Attack daemons are usually deployed in host computers. These Attack daemons affect both the target and the host computers.

The main Aim of deploying these attack daemons is to gain access the host computers. The third component of a (DDoS) distributed denial of service attack is the control master program. the task of the control master program is to coordinate the attack. Finally, there is the real attacker, i.e, the mastermind behind of the attack. By using a control master program, the real attacker can stay behind the scenes of the attack. Some of the steps take place during a distributed attack:

- ❖ The real attacker sends an “execute” message to the control master program.
- ❖ The control master program receives the “execute” message and propagates the command to the attack daemons under its control.
- ❖ on receiving the attack command, the attack daemons begin the attack on the victim.

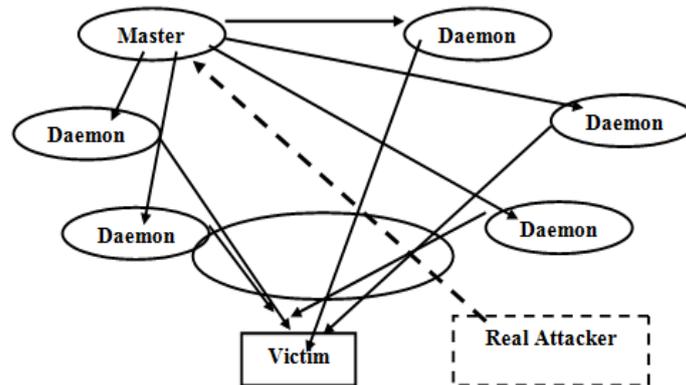


Figure 1.1 : The four Components of DDoS Attacks.

II. RELATED WORK

Distributed framework for defending DoS attacks

The Author Rocky K. C. Chang in 2002 proposed [1] that the behavior of DoS attacks while they are affecting the stability's of computer systems as well as exploit a distributed framework which will monitor, detect, and prevent from the DoS attacks. This includes several distributed monitors implemented at the critical components and a management center which is used to detect and prevent DoS attacks.

Using Target Customer Behaviour

The Authors Srikanth Kandula, Dina Katabi, Matthais Jacob and Arthur Berger in 2005 proposed [2] that, DDOS Distributed denial of service attacks are growing in equal proportion. Sharing of information is being carried out in terms of server and the client. The client requests for the data from the server and then server gives the response for the client-request. Here the client can disrupt the server performance by sending continuous requests. and then result is that the server performance becomes degraded. Author prevent the performance from degradation using some algorithm proposed in the methodology.

DoS Attack and Detection Programming

The Author Wentao Liu in 2009 proposed [3] that Denial of service attack is the most popular attack in the network security with the development of network and internet. Author describes that the (DoS)Denial of service attack principle is discussed and some Denial of service attack methods are deeply analyzed. The DoS attack detection technologies presented network traffic detection and packet content detection. The Distributed Denial of service based on Denial of service is introduced and some DDoS tools are described and the important TCP flood DoS attack theory is discussed. The Denial of service attack program and a Denial of service attack detection program based on Winpcap for experiment are designed and the network packet generation and capture are implemented. Author expressed the key progress of DoS attack and detection in detail.

Wireless MANET

The Author Prajeet Sharma in 2012 proposed [4] that Wireless Mobile ad-hoc network (MANET) is an emerging technology and have great strength to be applied in critical situations like battlefields and commercial applications. MANET has no infrastructure, with no any centralized controller exist and also each node contain routing capability, In MANET each device can independently move in any direction. So most important challenges in wireless MANET face today is security. MANETs are a type of wireless ad hoc networks that usually has a routable networking environment on top of a link layer ad hoc network. Ad hoc contains a sensor network so the problems that is facing by sensor network is also faced by MANET. There are many security attacks in MANET and DDOS (Distributed denial of service) attack is one of them. with these parameters we build secure IDS to detect this kind of attack. In this paper author discussed about attacks on MANET and DDOS and provide the security against the DDOS attack.

IP Broadcast Using Disable Technique

The Author Mukesh kumar in 2013 proposed [5] that Ad-hoc network is the network comprised of wireless nodes. It has no any infrastructure which is self configured. MANET can be accessible to both legitimate network users and malicious attackers. one of the main Aim in MANET is to design the robust security solution that can prevent MANET from various Distributed denial of service attacks. different cryptographic techniques have been proposed to countermeasures these attacks against MANET. These techniques are not better for MANET, because they introduced heavy traffic load to exchange. Therefore Mobile ad hoc networks have their own vulnerabilities that cannot be always tackled by these wired network security solutions. Distributed Denial of Service attacks has also become a problem for users of computer systems connected to the Internet. In this paper, a technique is used that can prevent a specific kind of DDoS attack. The scheme is distributed in nature it has the capability to prevent Distributed DoS (DDoS) attack. The performance of the scheme shows that the proposed scheme provides a better solution than existing schemes.

Denial of Service Attack in MANET

The Authors Mamta Jha, Rajesh Singh, S.S. Dhakad, in 2015 proposed [6] that MANET is an emerging method and have high strength to be applied in the serious conditions like commercial applications and battlefields such as traffic surveillance, building, MANET is organization less, with no any central supervisor exist and also all node hold routing capability, Every device in the MANET is independently free to move in every direction, and will therefore modification its connections to other devices frequently. Denial of Service (DoS) and Distributed DoS (DDoS) attacks are two of the most harmful threats to the network functionality. Many of the protection methods are established in a fixed wired network are no applicable to this novl in a mobile environment. How to thwart the Denial of Service attacks differently effectively and save the vital secure-sensitive ad hoc networks obtainable for its intended use are needed. The DOS (denial of service), DDoS (Distributed denial-of-service) attacks are a rapidly rising problem. The variation of both the attacks and the defense approaches is overwhelming. These attacks lead to the degradation or the prevention of legitimate use of network resources. Author describe that type of attacks which are attacked on an ad-hoc network

III. PROPOSED METHODOLOGY

The performance simulation environment used is based on GloMoSim, a network simulator that provides support for simulating multi-hop wireless networks complete with physical and IEEE 802.11 MAC layer models. The simulated environment consists of 50 wireless mobile nodes roaming in 1000 meters × 1000 meters.

Table 3.1 shows the parameters used in Simulation

PARAMETER	VALUE	DESCRIPTION
Number of Nodes	0-49	Network Nodes
Network Area	(1000,1000)	X,Y Dimension of motion in m.
Bandwidth	2Mbps	Node’s Bandwidth
Simulation Time	0 – 15min	Simulation Duration
Node-placement	Uniform	Node placement policy
Mobility	Random Waypoint Motion	Change Direction Randomly
Mobility	0 - 20 m/s	Mobility of Nodes
Traffic Model	CBR	Constant bit rate protocol
MAC Protocol	CSMA	MAC protocol used
Routing Protocol	Bellman ford	Routing protocol used
Pause Time	0	Non-mobility time at the terrain boundary
CBR connections	8	Number of CBR connections

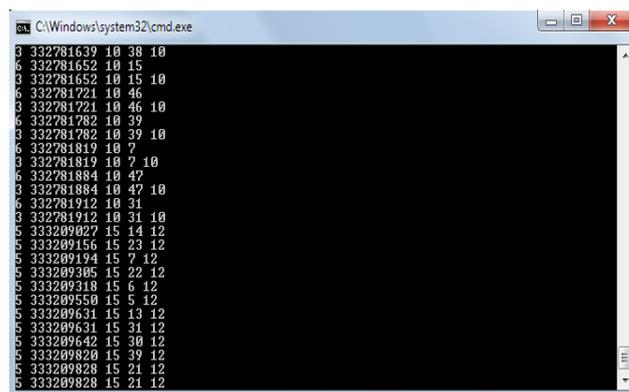


Figure 3.2 : shows the Simulation of Number of Nodes

IV. RESULTS AND DISCUSSION

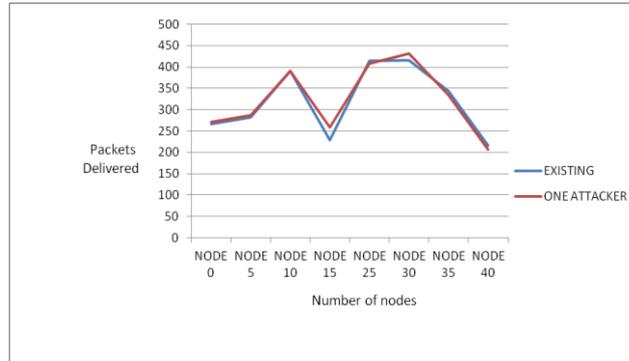


Figure 4.1 : Packet Delivered Vs Number of nodes

Figure 4.1 and Figure 4.2, In case of exiting, without applying detection scheme the total no. of packets delivered are 2556. In case of one attacker when detection scheme is applied the total no. of packets delivered are 2587 and In case of two attacker when detection scheme is applied the total no. of packets delivered are 2587. It can be concluded that in both the cases the number of packets delivered are same.

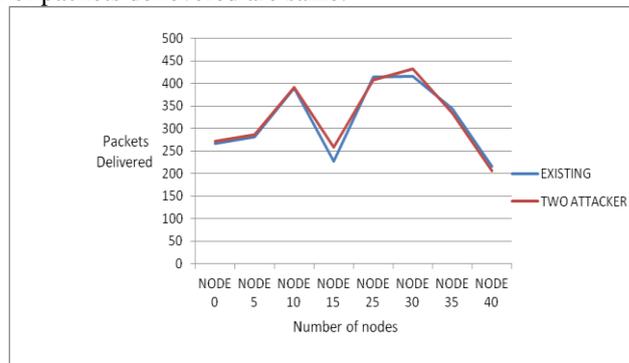


Figure 4.2 : Packet Delivered Vs Number of nodes

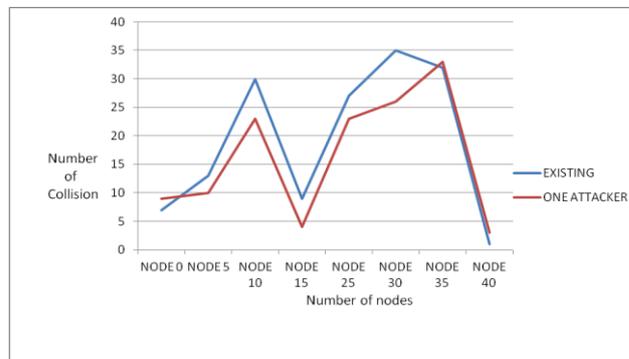


Figure 4.3 : Number of Collision and Number of nodes

Figure 4.3 and Figure 4.4, In case of exiting, without applying detection scheme the total no. of collisions are 154. In case of one attacker when detection scheme is applied the total no. of collisions are 131 and In case of two attacker when detection scheme is applied the total no. of collisions are 131. It can be concluded that in both the cases the number of collisions are same.

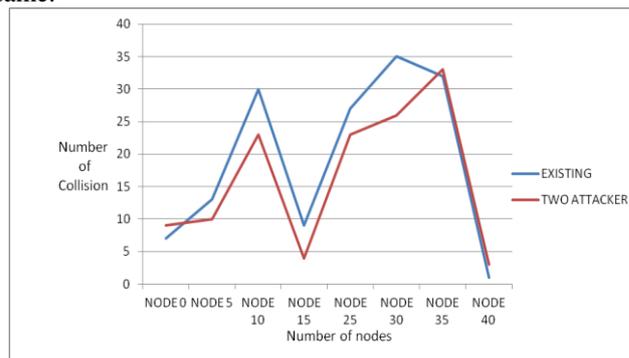


Figure 4.4 : Number of Collision and Number of nodes

V. CONCLUSION

It can be concluded that Denial of service attack uses a distributed framework that could be used to detect and prevent the legitimate use of service. Different techniques of DoS attack in MANET have been studied. The ultimate aim of this attack is to achieve a clear view of the DDoS attack problem and find more effective solution for the problem. DDoS attack make a networked system or service available to legitimate users and uses multiple machines to protect the resources and gives a defense scheme to mitigate the attack in wireless Adhoc networks. From above discussion the graph shows the relationship between packet delivered and number of nodes and also shows the relationship between number of collisions and number of nodes. Above Table shows the parameters used in the Simulation.

REFERENCES

- [1] Rocky K. C. Chang, "Defending against flooding-based distributed denial of service attacks: a tutorial," IEEE Communication Magazine, vol. 40, no. 10, pp. 42-51, Oct. 2002.
- [2] Srikanth Kandula, Dina Katabi, Matthais Jacob and Arthur Berger, "Surviving Organized DDoS Attacks that Mimic Flash Crowds", NSDI'05 Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation, 2005, Vol.2.
- [3] Wentao Liu "Research on DoS Attack and Detection Programming" Third International Symposium on Intelligent Information Technology Application 2009.
- [4] Prajeet Sharma " A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network" International Journal of Computer Applications (0975 – 8887) Volume 41– No.21, March 2012.
- [5] Mukesh kumar "Detection and Prevention of DDOS attack in MANET'S using disable IP broadcast Technique" International Journal of Application or Innovation in Engineering & Management (IJAIEEM). Volume 2, Issue 7, July 2013.
- [6] Mamta Jha, Rajesh Singh, S.S. Dhakad, " A Review: Denial of Service Attack MANET" International Journal for Scientific Research & Development| Vol. 3, Issue 01, 2015.