DOS Attack Mitigation In MANET

Er. Inakshi Garg
M.Tech, CSE
Kurukshetra University, India
Inakshigarg28@gmail.com

Er. Meenakshi Sharma
HOD,CSE deptt
Kurukshetra University, India
er.meenakshi1000@gmail.com

Abstract— Mobile Ad hoc Network is one of the kind of wireless networks which utilizes multi-hop radio relaying and it has no infrastructure Network because of its capability of operating without any support of fixed infrastructure or without any centralized administration. MANET has no clear line to prevent so both legitimate network users and malicious attackers can access it. There are major challenges in MANET in case of malicious nodes, it is to designs the robust security solution which helps to prevent MANET from various DDOS attacks.Security plays a vital role in mobile ad hoc network (MANET) because of its applications like disaster-recovery or battlefield networks. MANETs are more vulnerable as compared to wired networks because lacking of a trusted centralized authority and limited resources.The main objective of this survey is comparative study of various kinds of DDOS attacks and various detection methods as well as defense mehanisms like Disable IP broadcast detection technique, profile based detection and prevention of DOS attack using target customer behavior and existing solutions to protect MANET protocols.

Keywords— MANET, DOS attack, Malicious code, DSDV,Security, Defense Methods**.**

I. INTRODUCTION

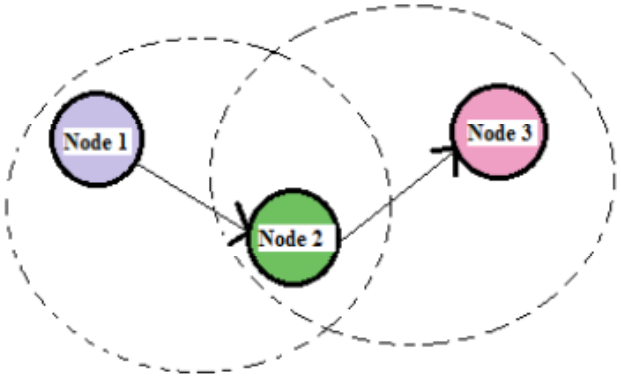
1.1 MANET

MANET(Mobile Ad Hoc Network).MANETS are just a mobile, they also use wireless connections to make a connection with various types of connections. This can be also a standard Wi-Fi connection, or another medium, like cellular or satellite transmission. Some MANETs are prohibited to a local area of wireless devices (such as a group of laptop computers) For example, A VANET (Vehicular Ad Hoc Network), is one of a type of MANET which allows vehicles to communicate with roadside equipment. Basically vehicles can not have direct connection, the wireless roadside equipment may be connected to the Internet,which helps to allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to countermeasure the traffic conditions.Due to the dynamic nature of MANETs, they are typically not very secure, so it is important to be aware what data is sent over a MANET.

1.2 Architecture of MANET

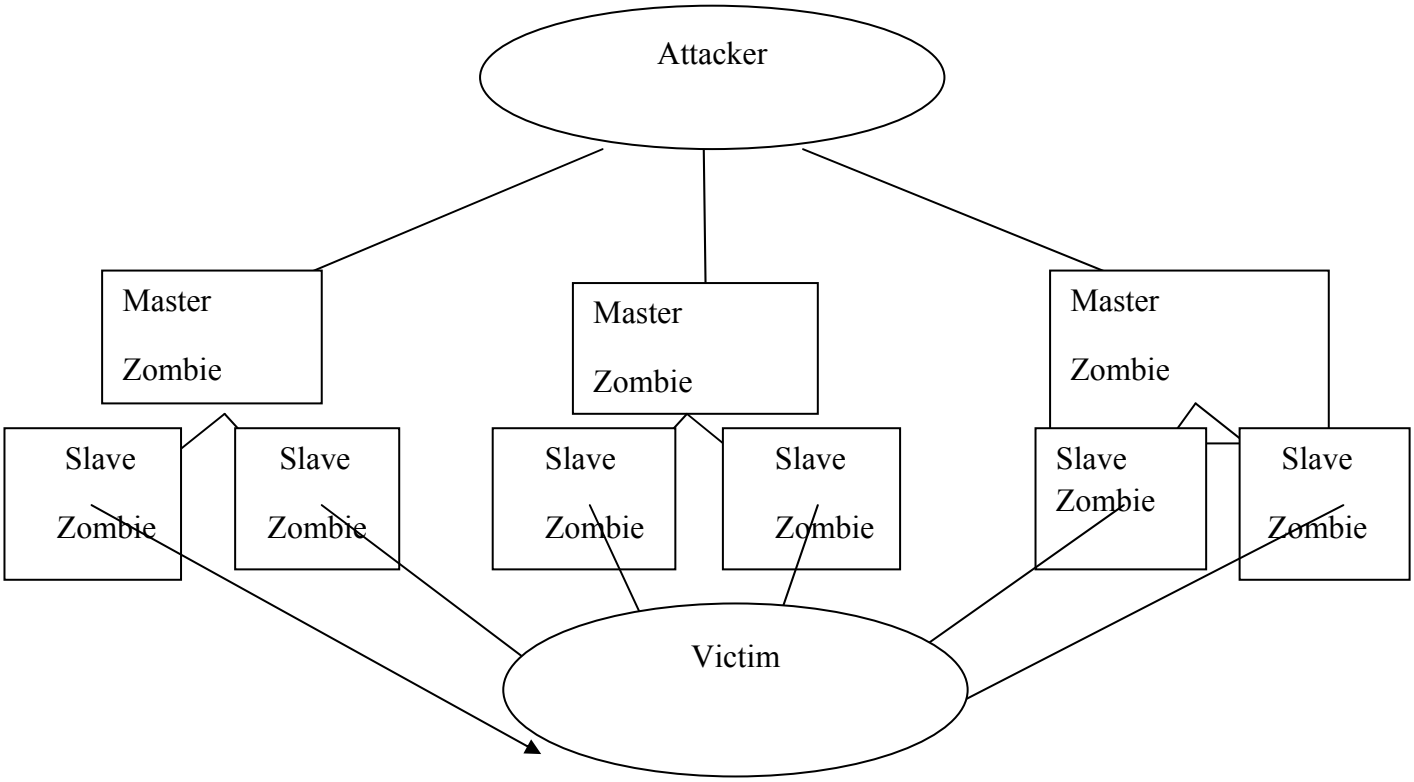
A mobile ad hoc network is simply defined as a network that has many free , often composed of mobile devices or other mobile parts, that can arrange by own in different ways and operate without strict top-down network administration. There are many various kinds of setups that may be called as MANETs and the potential for this sort of network is still being studied. Mobile Ad hoc Network (MANET) consisting autonomous mobile nodes that dynamically and form multi-hop conversation facilities to attack includes Denial of Service (DoS) attack, selfish misbehaving, etc.. Among these security threats, MANET are particularly doubtable to DoS attacks because of the facts on mobile nodes that are limited and broadcast mechanism is resource consuming. There is a challenging issue to keep communication secure in MANET. Firstly, general security mechanisms are used in structural networks can be non applicable to MANET because oh its uniqueness includes unreliability of wireless links, not a presence of a certification authority, dynamically changing topology and the lack of a centralized observation

Example of mobile ad-hoc network



1.3 DOS and DDOS Attack In MANET

Denial of Service (DoS) attack uses one computer to flooding a server with packets. The goal of this attack is to flood the bandwidth of server and other resources. A distributed denial of service attack is a strict form of DOS which uses multiple machines to prevent the legal use of a service. It is an type of active attack and very powerful technique to attack resources of internet. It adds to the many-to-one dimension to the DoS problem. To make a prevention and mitigation schemes for them are more complicated. But its impact is proportionally strict. DDoS is composed as shown in figure. First attacker made a network of malicious nodes which initiates the attack. The malicious nodes called zombies are then installed with attack tools, which allows them to carry out attacks under the control of the attacker.The zombies are classified into masters and slaves.The attacker motivates the masters to start the attack, the masters then motivate the slaves. The slaves flood the victim.



II. Literature Survey

A.DDOS ATTACKS AND DEFENSE MECHANISMS

This authors Christos Douligeris, Aikaterini Mitrokotsa in 2003 proposed the Denial of Service (DoS) attacks is one of the major threats and the hardest security problem. A DDoS attack can easily release the communication and computing resources of its cheated person within a short period of time. Many protective mechanisms proposed to combat these attacks due to seriousness of the problem .This paper presents a layout approach to the DDoS problem by developing a categorization of DDoS attacks and DDoS protective mechanisms. Further,more significant feature of each attack and protective system type are discussed and pros and cons of each proposed scheme are outlined. The aim of the paper is to place into the existing attack and defense mechanisms, for better understanding of DDoS attacks can be achieved and more efficient and effective algorithms, techniques and procedures to conflict between these attacks may be developed.

B. ROQ DDOS ATTACK IN MANET

The authors Wei Ren,Dit-Yan Yeung,Hai Jin,Mei Yang in 2007 focused on the reduction of Quality and response mechanisms. The response scheme is based on the ECN marking mechanism. Through extensive ns2 network simulations, Demonstration of the existence high good output and delay jitters under the pulsing attack mode. Increases in delay (by 110 times under five attacking flows) and decreases in goodput (to 77% under five attacking flows) can be observed specially when more attacking flows occurs. Moreover, the author shows through simulations that has similar behaviors which can also be observed for TCP flows as well as networks of other types of topology.

C. DETECTION AND RESEARCH ON DOS ATTACK

The author Wentao Liu in 2009 proposed that DoS attack is the most popular attack in the network security with the development of network and internet. In this paper, the DoS attack rule is discussed and some DoS attack methods are core analyzed. The DoS attack detection techniques which includes network traffic detection and packet content detection. The DDoS attack is based on DoS attack which is introduced and some of DDoS tools are discussed and the significant TCP flood DoS attack theory is described. The DoS attack program and a DoS attack detection program which is based on Winpcap. The typical DoS attack progress consists following steps which are related to each other. First of all, an attacker sends a huge number of service requests with wrong address. The server sends a response message back to the sender and waits for response from the client. Because of the addresses are forged, the server can't get any information and must wait for a long time and the connection will be cut due to time out. The resource which is allocated for this request cannot be released. If the request number is very huge, the server resource will be used up finally. SO the new user can't get the service and the attack is placed successfully.The experiment expressed the key progress of DoS attack and detection in detail.

D. DDOS ATTACK IN WIRELESS AD HOC NETWORKS

The authors S.A.Arunmozhi,Y.Venkataramani in 2011 proposed that the wireless ad hoc networks are highly vulnerable to distributed denial of service(DDoS) attacks due to its unique characteristics like open network architecture, shared wireless medium and stringent resource constraints. The tcp throughput heavily and decreases the quality of service(QoS) to end systems gradually rather than refusing the clients from the services in a complete manner. In this paper, there is a discussion about DDoS attacks and proposed a protected scheme which helps to improve the performance of the ad hoc networks. The proposed ptotect mechanism which uses the medium access control (MAC) layer information which detect the attackers. The status values of MAC layer that can be used for detection are Frequency of receiving RTS/CTS packets, Frequency of sensing a busy channel and RTS/DATA retransmissions. Once the attackers are identified, all the packets from those nodes will be stopped. The network resources are made available to the legal users.

E.USING TARGET CUSTOMER BEHAVIOUR

The authors K.Kuppusamy ,S.Malathi in 2012 proposed that the possibility of sharing information through networking has been growing in geometrical progression. The network attacks are to be noted in this connection, on other hand, DDoS attacks are also rising in equal parts. Sharing of information is carried out by means of client and server. The client requested for data to the server and the server provided the response to the client-request. Here the client can violate the server performance by sending anomaly requests. As a result,the server performance is degraded. In This paper discussions about best degradation of the performance which can be prevented using some kind of algorithm proposed in the methodology in which manner. In this work the blocking is done using a different types of mechanism based on category of a client.

F. IP BROADCAST USING DISABLE TECH.

The authors Mukesh Kumar and Naresh Kumar in 2013 proposed that Ad-hoc network is the network consisted of wireless nodes. This network is infrastructure less which is self configured i.e. the connections are made without any centralized administration. MANET has no clear line of defense so it is accessible to both legal network users and harmful attackers. When malicious nodes are present ,one of the main challenge in MANET which designs the robust security solution that can prevent MANET from different DDOS attacks. Different mechanisms are proposed using different cryptography techniques to measure these attacks against MANET. These mechanisms are not suited for MANET resource constraints, i.e., limited bandwidth and battery power due to huge load of traffic which is introduced to exchange and verifying keys. Therefore ad hoc networks have their own vulnerabilities that cannot be ever handled by these wired network security solutions. Distributed Denial of Service (DDoS) attacks also becoming a problem for computer users, which are connected to the Internet. In this paper, a technique is proposed that can prevent a specific type of DDoS attack. The proposed scheme is distributed which has the ability to prevent from Distributed DoS (DDoS) attack. The performance of the proposed scheme in a terms of simulations which shows the proposed scheme to provide a better solution than existing schemes.

G. PREVENTION OF ATTACKS IN WIRELESS NETWORKS

The authors Bala Veeravatnam, D. Suguna Kumari, P. Sowmya in 2015 proposed in the network environment most of the time there could be more chances of the attacks. It means mostly it does not guarantee about the packets can be easily transfer on the network. It degrades network performance . To overcome this problem of network traffic and performance implementing a Packet Hiding Scheme that can be securely sent packets on the

network. While eavesdropping and message injection can be prevented using cryptography method. It has been shown to actualize severe Denial-of-Service attacks against networks. In the simplest form of jamming, the interferes with the reception of messages by transmitting a continuous jamming signal or several short jamming pulses. Generally, jamming attacks are considered under an external threat model, in which the jammer is not part of the network. In this paper, there is a developing and surveying on the two schemes that prevent real-time packet classification by combining Cryptography Puzzles and SHCS. In this, there is analyzing the security of methods and evaluate their computational and system overhead.

TABLE

Author's Name	Year	Technique Name	Findings
Christos Douligeris , Aikaterini Mitrokotsa	In 2003	Defense mechanisms are used for better understanding of DDoS attacks	Author tried to achieve a clear view of the DDoS attack problem and find more effective solutions to the problem.
Srikanth Kandula, Dina Katabi [5].	In 2005	Prevention of attacks using target customer behaviour	Authors proposed an efficient methodology to prevent the attack on server performance and to improve the reliability on the clients.
Wei Ren and Dit-Yan Yeung	In 2007	Reduction of quality(ROQ) is a new style used for distributed denial of service (DDoS)	Author proposed that the congestion-based RoQ DDoS attacks in MANETs and detection scheme that monitors three MAC layer signals and a response scheme based on ECN marking.
Wentao Liu	In 2009	Detection and research on DOS attack	DoS attack is designed by use of the WinPcap toolkit and the program of DoS detection is also implemented
S. A. Arunmozhi [9].	In 2011	Defense scheme to mitigate attack in wireless ad hoc networks	Author discussed the DDoS attacks and proposed a defense scheme to mitigate the attack in wireless ad hoc networks and achieved higher bandwidth.
K.Kuppusamy and S.Malathi	In 2012	Prevention of attacks using target customer behaviour	Authors proposed an efficient methodology to prevent the attack on server performance and to improve the reliability on the clients
Mukesh Kumar & Naresh Kumar	In 2013	Disable IP broadcast technique used for prevention of DDOS attack in MANETs	Author proposed that prevention technique is better than existing techniques. It helps to prevent flooding.
Bala Veeravatnam, D. Suguna Kumari, P. Sowmya	In 2015	Prevention of black hole attacks in wireless networks.	Author proposed that the selective jammer can significantly impact performance with very low effort.

III. CONCLUSION

In this paper, we have presented an overview of DOS and DDoS defense schemes. Security is one of the most important feature for deployment in Mobile Adhoc Network. The different types of attacks and tools have been represented for the implementation of the DDoS attacks Distributed Denial of Service attacks are more complex and serious problem, and as a result, several approaches have been proposed to detect them. This paper discussed the various methods available in the literature with regard to various defense mechanisms for DoS and DDoS attacks on MANET.

REFERENCES

[1] Bala Veeravatnam, D. Suguna Kumari, P. Sowmya“ Preventing Black Hole Attacks in Wireless Networks” Volume 5, Issue 11, November 2015.
[2] 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 (IJAIEM). Volume 2, Issue 7, July 2013.
[3] Saurabh Ratnaparikhi , Anup Bhange “ DDOS Attacks on Network; Anomaly Detection using Statistical Algorithm” Volume 2, Issue 12, December 2012.
[4] K.Kuppusamy and S.Malathi “ Prevention of Attacks under DDoS Using Target Customer Behavior” Vol. 9, Issue 5, No 2, September 2012.
[5] S.A.Arunmozhi “DDoS Attack and Defense Scheme in Wireless Ad hoc Networks” International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.
[6] Wentao Liu “Research on DoS Attack and Detection Programming ” Third International Symposium on Intelligent Information Technology Application,2009.
[7] Wei Ren and Dit-Yan Yeung “Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks” International Journal of Network Security, Vol.4, No.2, PP.227-234, Mar. 2007.
[8] Stephen M. Specht “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures” International Journal of Advanced Research in Computer Science and Software Engineering Sep. 2004.
[9] Christos Douligeris , Aikaterini Mitrokotsa “DDoS attacks and defense mechanisms: classification and state-of-the-art” Department of Informatics accepted 13 october 2003.
[10] Rizwan Khan, A. K. Vatsa “Detection and Control of DDOS Attacks over Reputation andScore Based MANET ” VOL. 2, NO. 11, October 2011.