INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Survey on DDOS Attack Prevention and Detection Techniques

RANJU[1], NEERAJ MADAAN[2]

[1]CSE, Department,KUK University
Haryana, India
garg.ranju@gmail.com

[2]CSE, Department,KUK University
Haryana, Indiia
neeraj.k.madaan@gmail.com

Abstract: Today secure communication is the primary aspects in the networks. Internet has become the primary medium for communication which is used by number of different users across the network. Denials of Service attacks have become a major problem to wireless systems such as MANETs. MANET is wireless ad-hoc network that allows collaboration in real time. Wireless ad- hoc networks are formed by a set of hosts that communicate with each other over a wireless channel. The Attacks on MANET interrupts network performance and reliability. Denial of service attack consumes a large amount of network bandwidth or occupies network equipment resources by flooding them with packets from the machines distributed all over the world. Now my objective is to study various detection and prevention techniques of DDOS attack. Detection mechanism such as profile based detection, specification based detection, and flow based detection. And prevention technique include new cracking algorithm and disable IP broadcast technique.

***Keywords*:** DDos attack mitigation, MANET, traffic, security

1. INTRODUCTION

In the modern computer world, maintaining the information is very difficult. Some interference may occur on the local system or network based system. Without security measures and controls in place our data might be subjected to an attack. Now a day's several attacks are evolve. The Dos attack is the most popular attack in network and internet. This kind of attack consumes a large amount of network bandwidth and occupies network equipment resources by flooding them with packet from the machines distributed all over the earth. Dos attacks are usually performing by following methods: 1 Teardrop attack.2 Executing malwares.3 Send unlimited amount of packets to the server.4 Application level flood. DDos attack has been regular in the works attacks that badly intimidate the stability of the internet. According to CERT coordination centre (CERT/CC), there are mainly three categories of DDos attacks: protocol attack, logical attack and flood attack.

2. COMPOSITION OF DDOS

DDoS is composed as shown in Fig.1First attackers build a network of vulnerable nodes which are used to initiate the attack. The unsafe nodes called zombies are then installed with attack tools, which allow them to carry out attacks under the control of attacker. The zombies are divided into masters and slaves .The attacker motivates the masters to start the attack, then the masters motivate the slaves. At the end The slaves flood the victim.

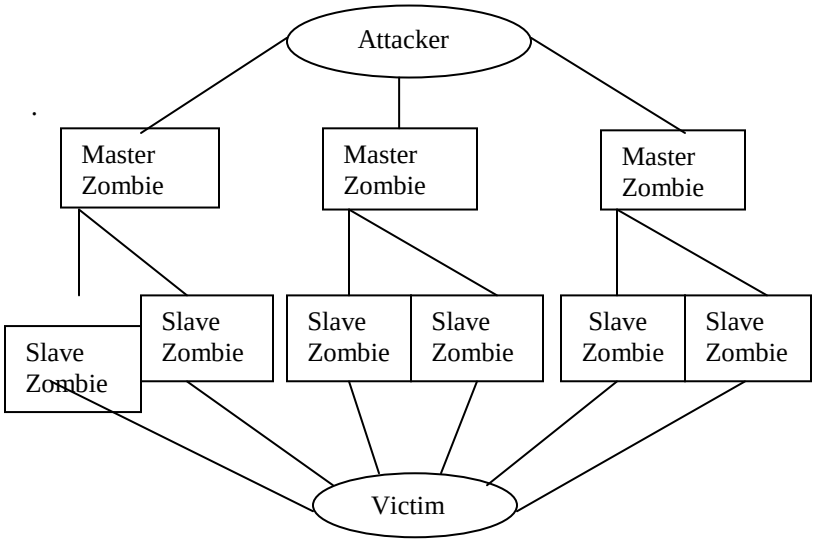

Figure 1: Composition of ddos

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

3. DDOS ATTACK IN MANET

Distributed denial of services attack usually occurs in MANETS or in wireless networks. It is an attack where numerous systems comprise together and target a single system causing a denial of service. A denial of service is an attack with a purpose of preventing legitimate users from using a specified network resource such as web service, website or computer system. A DDos attack is distributed a large scale attempt by malicious users to flood the victim network with an enormous numbers of packets.

3.1 DIFFERENT TYPES OF ATTACKS IN MANET

MANET is affected by various attacks as shown

Table1: various attacks

Security Attacks (External Vs Internal)				
Passive attacks	**Active attacks**			
-Eavesdropping attacks -Traffic analysis & Monitoring	**MAC Layer Attack**	**Network Layer Attack**	**Transport Layer Attack**	**-Session Hijacking -SYN flooding**
	Jamming	Wormhole -Black hole Information -disclosure -IP spoofing Modification	Session Hijacking -SYN flooding	Repudiation Data Corruption

4. LITERATURE REVIEW

Wentao Liu[1] the DoS attack principle is discussed and some DoS attack methods are deeply analyzed. The DoS attack is the most popular attack in the network security with the development of network and internet. The DoS attack detection technologies which include network traffic detection and packet content detection are presented. The DDoS based on DDoS is introduced and some DDoS tools are described and the important TCP flood DoS attack theory is discussed.

Rajdeep Singh[2] discussed some attacks on MANET and DDOS also provide the security against the DDOS attack. Each device in a MANET is independently free to move in any route, and therefore change its connections to other devices frequently. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a link layer ad hoc network. There are many security attacks in MANET and DDoS (Distributed denial of service) is one of them.

Dr. K. Kuppusamy[3] a new cracking algorithm is implemented to stop that DDos attack. Now a day's several attacks are evolved. One common method of attack involves sending enormous amount of request to server or site and server will be unable to handle the requests and site will be offline for some days or some years depends upon the attack. This is most critical attack for network called distributed denial of service attack. In our algorithmic design a practical DDOS defence system that can protect the availability of web services during severe DDOS attacks. The expected system identifies whether the number of entries of client exceeds more than five times to the same sever, then the client will be saved as an attacker in blocked list and the service could not be provided. So our algorithm protects legitimate traffic from a huge volume of DDOS traffic when an attack occurs.

Yu Chen[4] propose a strategy to mitigate DDoS attacks in MANETs. Mobile Ad Hoc Networks (MANETs) allow mobile hosts to form a communication network without a prefixe framework. Although it provides high mouldability, it also brings more challenges for MANETs to fight against malicious attacks. However, the property of moving and redundancy also inspires new ideas to design defence strategy. Assume that a malicious attacker normally targets specific sufferer.The attacker will give up if the attack failed to achieve the desired goals after a certain length of attacking time. In our protection scheme, we take advantage of high redundancy and select a protection node. Once a DDoS attack has been observed,the doubtful traffic will be redirected to the defence node. The sufferer will function normally, and it is sensible to expect that the attacker will stop the meaningless efforts

.Dr.K.R.Valluvan[5] various attacks on MANET and defence mechanisms for DDOS attacks in MANET as reported in the literature. Mobile Ad hoc Network is the kind of wireless networks that utilize multi-hop radio relaying and it is an infrastructure less Network due to its ability of operating without the support of any fixed framework. Safety plays an important role in mobile ad hoc network (MANET) due to its applications like battlefield or disaster-recovery networks. MANET is severely affected by Distributed Denial of Service (DDoS) attack which

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

becomes a problem for users of computer systems connected to the Internet.

Yinghua Guo [6] present a detailed investigation of the flooding attack in MANET which is particularly vulnerable to flooding attacks. To elude being identified, attackers usually recruit multiple accomplices to dilute attack traffic density of each attack source, and use the address parody technique to challenge attack tracing. we design two flow based detection features, and apply the increasing sum algorithm on them to effectively and accurately detect such attack.

Saurabh Ratnaparikhi [7] defines statistical evidence that the marginal distribution of real traffic is adequately modeled with alpha stable functions. DoS/DDoS attacks are a venomous, relatively new type of Internet attacks, they have caused some biggest sites on the world owned by the most famous E-Commerce companies such as Amazon,Yahoo, eBay became inaccessible to users, customers and partners the financial losses are very huge.

Mukesh Kumar [8] a technique is proposed that can prevent a specific kind of DDoS attack named flood attack which Disable IP Broadcast.MANET has no clear line of defence so it is accessible to both malicious attackers and legitimate network users. In the presence of hostile nodes, one of the main Challenge in MANET is to design the robust security solution that can prevent MANET from various Ddos attacks. individual mechanisms have been proposed using various cryptographic techniques to countermeasures these attacks against MANET. DDOS attacks has also become a problem for users of computer systems connected to the Internet.

Christos Douligeris[9] purpose to place some order into the existing attack and defense mechanisms, so that a better understanding of DDoS attacks can be achieved and subsequently more efficient and effective algorithms, techniques and procedures to combat these attacks may be developed.

K.Kuppusamy[10]discusses how best the degradation of the performance can be prevented using some algorithm proposed in the methodology. The blocking is done using a different mechanism based on the category of the client. The possibility of sharing information through networking has been growing in geometric progression. In this connection it is to be noted network attacks, in other words, DDoS attacks also are germinating in equal amount. Sharing of information is being carried out by means of server and client. The client appeal for the data from the server and the server provides the response for the client-request. Here the client can breach the server performance by sending continuous or irregular requests. The result is the server performance becomes degraded.

Table2: Comparison of Various Detection Approaches Classified Based on Detection Activities Used

Detection category	Complexity	Detection accuracy	Limitations
Pattern Detection	Low	High	Detection of the novel attacks are not possible
Anomaly Detection	Medium	Medium	False positives and negatives rate is very high, since defining normal system behavior and setting threshold values is difficult
Hybrid Detection	High	High	Complexity and cost of implementation is very high to deployed in Practice
Third party Detection	High	Detection approach used by third party	Economic Factor,Security prone

5. CONCLUSION

DDoS attacks make a networked system or service unavailable to legal users. These attacks are an vexation at a minimum, or can be seriously harm if a critical system is the primary victim. Loss of network assests causes financial loss, work delays, and loss of communication between network users. Solutions must be developed to stop these DDoS attacks. In this work various detection and prevention techniques of Ddos attack are investigated and characterized**. T**affic detection and packet content detection are presented. The technique of preventing Ddos attack by Disabling IP broadcast is better than any other technique

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

REFERENCES

[1] 2009 Third International Symposium on Intelligent Information Technology Application. By " Wentao Liu"

[2] International Journal of Computer Applications (0975 – 8887) Volume 41– No.21, March 2012 By " Prajeet Sharma, Niresh Sharma, Rajdeep Singh"

[3] International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May- Jun 2012, pp.2263-2267 By "V. Priyadharshini, Dr.K. Kuppusamy

[4] This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011 proceedings.By "Minda Xiang,Yu Chen,Wei-Shinn Ku, Zhou Su"

[5] International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 9, September 2012 ISSN: 2277 128X By "A. Anna lakshmi, Dr.K.R.Valluvan "

[6] This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings. By "Yinghua Guo, Steven Gordon, Sylvie Perreau"

[7] International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 12, December 2012 ISSN: 2277 128X By "Saurabh Ratnaparikhi, Anup Bhange"

[8] International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 2, Issue 7, July 2013 ISSN 2319 – 4847 By "Mukesh Kumar & Naresh Kumar"

[9] C. Douligeris and A. Mitrokotsa. DDoS attacks and defence mechanisms: classification and state of- the-art. Computer Networks, 44(5): 643-666, 2004.

[10] An effective prevention of attacks using giTime frequency algorithm under DDos by Dr.K.Kuppusamy, S.Malathi, International Journal of Network Security & Its Applications (IJNSA),Vol.3,No.6,November2011 Security Applications Conference (ACSAC 2002).