ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

A Survey on DDoS Attacks and Defense Approaches

Divya Kuriakose[1] V.Praveena[2]

PG scholar, Dept. of CSE, Dr N.G.P Institute of Technology, Coimbatore, India[1]

Associate professor, Dept. of CSE, Dr N.G.P Institute of Technology, Coimbatore, India[2]

ABSTRACT: Network is collection of nodes that interconnect with each other for exchange the Information. This information is required for that node is kept confidentially. Attacker in the network may capture this confidential information and misused. So security is the major issue. There are many security attacks in network. One of the major threats to internet service is DDoS (Distributed denial of services) attack. DDoS attack is a malicious attempt to suspending or interrupting services to target node. Various schemes are developed defence against to this attack. Main idea of this paper is present basis of DDoS attack. Types of DDoS attack, components of DDoS attack, need for Distributed defense system, comparative study of different defense mechanism.

Keywords: DDoS, Attacks, Defense techniques, security.

I. INTRODUCTION

In a communication system thousands of nodes communicate with each other. Each node has confidential data that are transmitted between the nodes. The most recent issues in the networking is to provide security in transmitting and receiving of information. To overcome this issue large numbers of security mechanisms were developed. But it doesn't give satisfactory protection.

DDoS attacks are reported as one of the highly occurred attack over a past few decades. Many service providers and legitimated users have undergone a nasty experience from these attacks. DDoS attack is an intruder attempt to make a network services unavailable to the intended user. DDoS have many faces like flooding attack, logic attack and protocol-based attack [2].Flooding attack is an attack in which it covers the network with unwanted packets, i.e. either the node may send replicated packets or the node may send the unique packets which exceed its rate limit. Logic attack is an attack which has a buffer space limit and it may exceed or overflow when it accepts a large amount of packets beyond its limit. In protocol-based attack attacker does not weakens the TCP/IP functionality instead it take the expected behaviour of this protocol for the requirements of attacker. In this paper, we have gone through various types of DDoS attack and its defense mechanisms.

II. TYPES OF DDOS ATTACK.

A. SYN FLOODING

This is the most important attack occur during the three-way handshake. In three-way handshake client request a new connection by sending SYN packet server ACK sends back to client. Finally client acknowledged with ACK.If attack occur numerous SYN packet to victim. It makes open numerous connections and responds to them, and third step of the hank-shake will not perform. That makes unable to open new connections. This Because of queue is filled with full of half-way TCP request. This flooding does not targeting specific operating system. It attacks any system that support TCP connection.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

B. SMURF ATTACK

Cause of smurf attack is flooding of ICMP echo-request echo-reply. Direction of packet is to IP broadcast address from remote location to generate DoS attack. Most of time attacker generate forged echo request using spoofed IP address, i.e. it is intended to victim machine, and attacker hide its identity. The intermediate node can't identify whether it is original or not. So intermediate node immediately reply that make flood on the victim machine.

C. UDP FLOOD ATTACK

This is the second most popular attack. Main idea of this attack is to exploit UDP services. These attacks slowly down/congested the network. In this attack attacker sends to random port of victim. After receiving that packet victim system is try to find which application is waiting on the destination. But actually no application running on that port.AZ large number of UDP packet are received by the victim, it make infinite number of loop goes between the Two UDP services.

D. ICMP DOS ATTACK

In this attack Attacker simply forging the notification message. Attacker could use either Time exceed and or Destination unreached that cause immediately drop the connection Eg. Ping of Death, ICMP PING flood attack, ICMP nukes attack.

E. PING OF DEATH

In this attack, attacker sends large number of malicious ping to computer. In this case large IP packet is split in multiple IP packets. In ping death scenario receiver ends up with packet size greater than 65,535when reassembled and over flow on allocated memory with numerous packets.

F. LAND ATTACK

It consist stream of the TCP SYN packet both source and destination have same IP address and port number. Some implementations are impossible to handle this type of attacks completly.The main cause of this attack the operating system repeatedly go into the loop try to resolved repeated connection itself.

G. MAIL BOMB

It is bandwidth-based flood attack. The attacker node sends large volumes of mail to mail-server causing it to deny services to legitimate user.

H. DNS AMPLIFICATION ATTACK

Attacker use publically accessible open DNS server to flood a target system with DNS response traffic. The crucial technique consists of an attacker sending a DNS name lookup to an open DNS server with source address spoofed to be target's address. Attacker submits more requests to zone as possible to maximize the effect.

I. IGMP ATTACK.

Cause this attack is to Flood the network with random IGMP messages. It makes overload on the network. It is the type of hacking attack. Main idea this attack is to reduced broadband and memory usage. But it is useful for multimedia broadcast application.

J. SQL SLAMMER

.It is one computer worm that causes the denial of service on some internet host. Dramatically slow down internet traffic. It exploits buffer overflow vulnerability in SQL server and MSDE code.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

III. COMPONENTS OF DDOS ATTACK

The node use request/response technology attacker is able to multiply the effectiveness of DoS by misusing the resources of nodes which act as attack platform. Main components in DDoS attack platforms are

- Attacker
- Master
- Zombie
- Victim

Attacker is the agent that will perform the attack on network. It use many attack strategies for attack the network. Those are removing (node), drop all packets, flood packet, and give false information to network. Masters are the compromised node, who is capable of controlling number slaves .It provides a way of channel to communicate with the zombie. Zombies are responsible for generating packet to toward the victim. Victim is the target node.

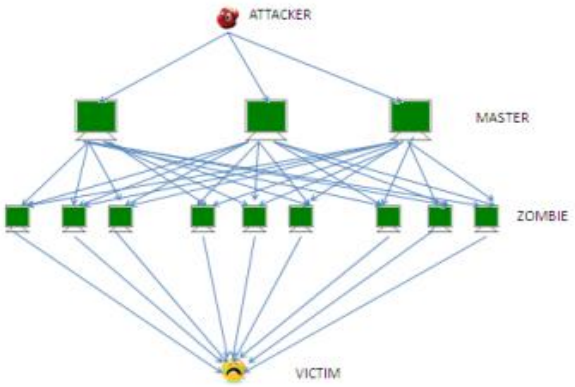

Fig1.Block diagram of DDoS Attack.

IV. NEED FOR DISTRIBUTED DEFENSE MECHANISM

Main function in defense system is traffic monitoring, traffic analysis, traffic filtering. Defense mechanism can be applied in two way centralized and distributed. In a centralized system all components are placed at same place. It is highly vulnerable to attack. No cooperation with other communication module because it consists of lesser number of resources are available for defense against DDoS attack. These resources are placed at victim site.

The Distributed system overcome shortcoming of the isolated system. These system components are placed at multiple places and it is less vulnerable to attack cooperated with the entire communication module, so required a proper communication framework. More resources are available for fighting against the attack. It deployed throughout the network .Eg.Flooding attack is affected throughout the network, it include victim node, intermediate nodes. The centralized defense mechanism only concentrated on the victim node. But distributed system can find any attacker node in network.

V. DEFENSE PRINCIPLES

A. RATE LIMITING MECHANISM

The Limiting mechanism that limit the rate of the packet arrived, which satisfied the criteria for DDoS attack. This mechanism only limits the rate of malicious packet. That does not harm legitimate flow. It does not incur lot of the overhead. It is the simpler form of the packet filtering

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

B. EGRESS/INGRESS MECHANISM

This filtering makes it difficult for attackers to launch attack using spoofed IP address.IP spoofing make it difficult to trace back the attack to actual originating host.

C. TRACE BACK.

It is the process of tracing back the forged IP packet to legitimate source rather than Spoofed IP address that was used by attacker. Three main ways to doing trackback a)Link testing scheme b)ICMP trace back message .c)packet marketing scheme.

D. THREE-WAY HANDSHAKE.

It is simple solution to defense source spoofing at the end system. It will unable to finish when source host spoofs it's IP address. But attacker can spoof the source address of first packet of the three-way handshake. It is major drawback of this technique.

E. HOP COUNT FILTERING.

It is the technique use to vanish out spoofed IP Packet at the beginning of network processing by using a hop-count filtering mapping table. Using that table we can easily identify the spoofed IP address.

VI. COMPARATIVE STUDY ON DIFFERENT DEFENSE APPROACHES

In [2], paper proposed defense scheme use medium access control information to detect the attack in the wireless network. Technique work as following way each node keep Flow monitoring table. It contain source id, destination id, packet sending rate, flow distending rate is estimated from the intermediate node. The intermediate node is updated the table by changing the bottleneck bandwidth field. Updated FM table is sent to the destination along with the flow. The destination sent explicit congestion Notification bit. It indicates any congestion the network. so sender reduced the sending rate. Channel becomes congested if sender does no reduced sending rate. It can found only using the updated table at the destination. It checks current sending rate and previous sending rate. If it is equal to or greater than the previous one, then concluded as packet is comes from the attacker. Once detected the DDoS attack all packet from that node is rejected. In the proposed scheme it uses two phase bandwidth Querying scheme and Data transmission scheme.

In [6], one approach is designed to prevent denial of service attack on wireless network particularly against multi-path communication in MANET. In this mechanism provide band-width control and per flow for each node participating in the communication. By exchanging capability message, each node can maintain a global view of throughput of the network. Then dynamically adjust constraints on each node. That prevents potential attack on the specific node or network. This approach is called CapMan.it consist two main component capability distribution and capability enforcement. Capability distribution protocol empower responder to issue and distribute capability packet to the entire node that in the routing path. Responder that accept connection from the sender it send capability packet to the sender as a notification of acceptance end to end flow and discovery of new routing path. This capability packet saved by the intermediate node to restrict number of data packet forward for the flow. The process of enforcing capability is a combination of local policing and flow-wide message exchange. The capability enforcement mechanism implements capability constraint to per-hop basis for across the multiple routing path.Muti-path routing is change dynamically. To account for this all node periodically exchange bandwidth consumption report. This report gives the global view of the network. Advantage of this mechanism is CapMan work if sender and responder is malicious node. It enable bandwidth limit in a distributed manner.

In [8], the author proposed a dynamic reactive approach using spin lock rate control. it identify malicious traffic activity to targeted node. In the proposed mechanism uses divide and conquer method to identify the malicious interface and selectively implement rate limiting based on traffic from source to destination. In the architecture three models are uesd1.monitoring, reasoning and monitoring module2.packet monitoring and measurement3.spin lock rate control. In the monitoring module check the arrival rate at each incoming interface and calculate Ratio of Collective Flow (RCF).This

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

information forward to reason module. This module is responsible for updating source based table, destination based table, packet based table, and this updated information forward to measurement module. Calculate RCF.RCF value below the predefined threshold and load on outgoing queue is below the maximum queue threshold it confirmed as normal flow otherwise it is malicious flow. Then define a rule for rate liming. Spin rate lock module is initiated rate limiting on malicious flow and it is computed by reason module. Load queue is continuously observed and the effect of the rate limit also according to this information rate limit rules are modified. Advantage of this approach is to overcome the some drawback of the previous invented technique. It do not require wide range of the monitor and log information about every packet. So it reduced computational and memory overhead. It considers the traffic of source, intermediate node, destination node. Another advantage of this paper is negligible false positive and false negative rate. And fast response handling mechanism.

In [10], the author proposed a distributed approach to defend against DDoS attack by coordinating against internet. In the proposed work defense system deployed on the network and detection is performed independently. For that it use gossip based communication mechanism, used to exchange the information about the attack in the local network collect the information from the independent place and the aggregate those information approximate the this information and can stop them more effectively. Main function of Local defense node is that local attack signature generation and rate limiting of identified attack traffic. In proposed system it uses directional gossip strategy. Gossip based protocol reduced the control message overhead still it provide reliable and scalable message delivery. Each node sends (*conf, attribute, and dest.*)Each time it aggregate attack information. According to this information each node adjusts its rate limit. If aggregate value is greater the threshold limit it confirmed the network is under attack. Advantage of this paper is that it use gossip based protocol. Those don't require much synchronization; don't require error recovery mechanism and simplicity.

In [11], it explained a new DDos attack called reduction of quality attack. In this detailed study in congestion based RQS DDoS attack in mobile network. Attacking principle based on analysis of the network capacity, based upon classify attack into four a)pulsing attack b)round robin attack c)self-whisper attack d)flooding attack .In this proposed defense approach include both detection and prevention scheme. Detection make use three of three status value that can be obtained from MAC layer.1) frequency of receiving RTS/CTS packet,2) frequency of the sensing channel, 3) number of RTS/CTS retransmissions. Number of packet received is greater than threshold value it indicate too many nodes are request for the channel. When channel is identified as busy state a node is persist in the back off region and stop CW count. If number of retransmission packet is greater than 7 and data packet is greater than 4 the packet will be dropped. Thus if the number of retransmission is exceed a threshold RET thresh, it indicate channel become congested. During the response phase the node will mark each packet with ECN bit to notify the sender node and keep list of those node. Sender seeing any packet having ECN marking then reduced the sending rate. Some of the node can't reduce the rate this node will be considered as malicious node. Packet from this node will be stopped.

In[12],the author proposed a technique that should satisfied following requirement a) accurate attack detection b)effective response to reduce the flood)precise identification of legitimate traffic and its safe delivery to the victim. The proposed work is DefCOM (Defensive cooperative Overlay Mesh).It deploy defense mechanism in a distributed manner in the internet core and through the edge network. All node form a peer-to-peer overlay to securely exchange attack related message. When attack occurs, node close to the victim detects this and alerts the rest of DefCOM overlay suppress the attack traffic using through the coordinated rate limit.

In [13], author introduced a technique Hop-count filtering is the victim based solution. This method use IP-to hop count mapping table to detect and discard spoofed IP packet.HCF is easy to implement as it does not require any support from the underlying network and any cryptographic methodology. Number hops between sender and receiver are determined by TTL field in the IP packet. When attack is detected received packets are discarded. It detected by discrepancies exist between the hop count and the table content. But this method is not more effective.

VII. CONCLUSION

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

DDoS attack is one advanced method to attacking network system it prevent legitimate user from using network resources. Major contributions of this paper are a need of distributed defense mechanism and its evaluation. This paper described a comprehensive survey of causes of DDoS attack and its defense mechanism. According to this survey most of the defense approach had used rate limiting mechanism. Egress and Ingress principle had used in defense against IPspoofing. Each method has certain features that make it more suitable to implement in one situation than another.

REFERENCE

[1] Nisha H. Bhandari, "Survey on DDoS attacks and its detection defense approach," International Journal of Science and Modern Engineering, Vol.1, Issue.3, pp.67-71, Feb 2013.
[2] S.A.Arunmozhi, Y.Venkataramani,"DDoS attack and Defense in wireless ad-hoc Network," International Journal of Network Security & Its Applications Vol.3, No.3, pp.182-187, May 2011.
[3] Monika Sachdeva, Gurvinddr Singh, Krishnan Kumar, Kuldip Singh, " A comprehensive Survey of Distributed Defense Techniques against DDoS Attack," International Journal of Computer Science and Network Security, Vol.9, No.12, pp.7-15, Dec 2009.
[4] Shibiao Lin Tzi-cker Chiueh," A Survey on Solutions to Distributed Denial of Service Attacks", Department of Computer Science Stony Brook University, pp.1-38, Sep 2006.
[5] Shuchi Juyali, Radhika Prabhakar, "A Comprehensive Study of DDOS Attacks and Defense Mechanisms," Journal of Information and Operations Management, Vol.3, Issue.1, 2012.
[6] Quan Jia, Kun Sun, Angelos Stavrou, "CapMan: Capability-based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET," proceedings of the 20th international conference on computer communication and networks, pp 1-6, 2011.
[7] Antonio Challita, Mona El Hassan, Sabine Maalouf, Adel Zouheiry, " A Survey of DDoS Defense Mechanisms ," The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
[8] Anurekha, R.,K. Duraiswamy, A. Viswanathan, V.P. Arunachalam, K. Ganesh Kumar, A. Rajivkannan" Dynamic Approach to Defend Against Distributed Denial of Service Attacks Using an Adaptive Spin Lock Rate Control Mechanism," Journal of Computer Science, pp.632-636, 2012.
[9] Puneet Zaroo," A Survey of DDoS attacks and some DDoS defense mechanisms," Advanced Information Assurance (CS 626), 2003.
[10] Guangsen Zhang, Manish Parashar,"Cooperative Defense against DDoS Attacks," Journal of Research and Practice in Information Technology, pp.1-6, 2006.
[11] Wei Ren, Dit-Yan Yeung, Hai Jin, Mei Yang, "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.
[12] Jelena MIrkovic, Max Robinson, Peter Reither, George Oikonomou, "Distributed Defense against DDoS Attacks," Available:http"//www.isu.edu/~mirkovic/publication/udel_tech_report_2005.pdf, 2005.
[13] Haining Wang Cheng Jin Kang G. Shin" Defense Against Spoofed IP Traffic Using Hop-Count Filtering," Networking, IEEE/ACM Transactions on Networking, vol. 15, pp 1-13, 2007.
[14] A.Anna lakshmi, Dr.K.R.Valluvan "A survey of Algorithms for Defending MANETs against the DDoS Attack," International Journal of Advanced Research in Computer Science and Software Engineering, vol.2, Issue 9, pp.155-164, Sep 2012.

BIOGRAPHY

Ms. Divya Kuriakose

She received her B.E degree in Information Technology from Viswajyothi College of Technology, Kerala in 2012.She is currently with the Post graduate in Dr N.G.P Institute of Technology and now works on the project in Network Security.

Mrs. V.Praveena

She received her B.E. degree in Computer Science and Engineering from Maharaja Engineering College under Bharathiyar University in 2002. She completed her M.E in Computer Science and Engineering from Karpagam University in 2011. She is pursuing her Ph.D. in Anna University Chennai. She has 11 years of Teaching Experience. Her area of interest is Network Security.