Volume 4, Issue 7, July 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey on Prevention Methods for DDOS Attacks in MANETS

Shakti Arora
HOD,CSE deptt, GEC
Kurukshetra University, India

Arushi Bansal
M. Tech, CSE,
Kurukshetra University, India

Abstract— Ad-hoc network is the network comprised of wireless nodes. It is infrastructure less network which is self-configured which means the connections are made without any centralized administration. MANET has no clear line of defence so both legitimate network users and malicious attackers can access it. In case of malicious nodes, major challenges in MANET is to design the robust security solution that can prevent MANET from various DDOS attacks. Many Different mechanisms have been proposed by using various cryptographic techniques to countermeasures these attacks against MANET. These mechanisms doesn't not suit to MANET resource constraints (limited bandwidth and battery power) because of introduction of heavy traffic load to exchange and verifying keys. Because of such problems ad hoc networks have their own vulnerabilities that are not always tackled by these wired network security solutions. Distributed Denial of Service (DDOS) attacks have also become a problem for Internet using computer systems. The researchers have examined different kinds of DDOS attacks and various detection methods like profile based detection, specification based detection and existing solutions to protect MANET protocols.

Keywords— MANET, DDOS attack, Security, Prevention Methods Malicious node.

I. INTRODUCTION

In the modern computer world, maintaining the information is very difficult. Some interrupts can 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 [3]. 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 world [6]. Dos attacks are usually doing by following methods: 1 Send unlimited amount of packets to the server.2 Executing malwares.3 Teardrop attack.4 Application level flood [3]. A DDos attack is launched by a mechanism called Botnet through a network of controlled computers [4]. Distributed denial of service(DDos) attack has been regulary in the works attacks that badly intimidate the stability of the internet. In accordance to CERT coordination center(CERT/CC), there are mainly three categories of DDos attacks: flood attack, protocol attack and logical attack [6].

II. DDOS ATTACK IN MANET

Distributed denial of services attack usually occurs in MANETS or in wireless networks. It is an attack where multiple systems comprise together and target a single system causing a denial of service. A denial of service (DOS) is an attack with a purpose of preventing legitimate users from using a specified network resource such as website, web service 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. DDOS is composed as shown in Fig. First attacker build a network of vulnerable nodes which are used to initiate the attack. The vulnerable nodes called handler and agents. These handler and agents are then installed with tools called attack tools, which allow the handler and agents to carry out attacks under the control of the attacker. The attacker motivates the handler to start the attack, the handler then motivate the agents. The agents flood the victim.

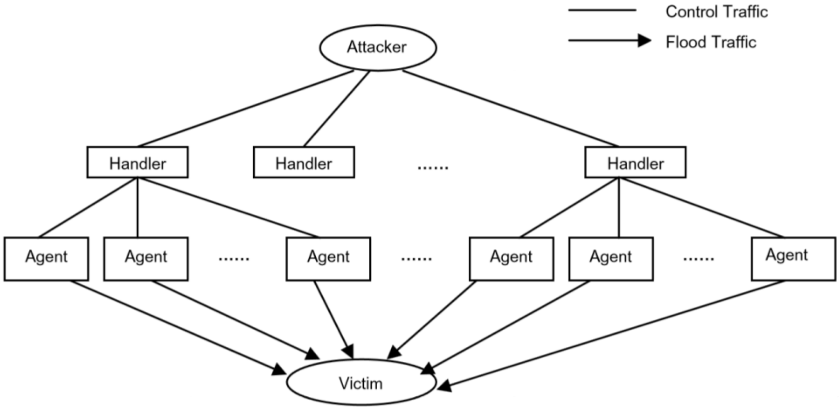
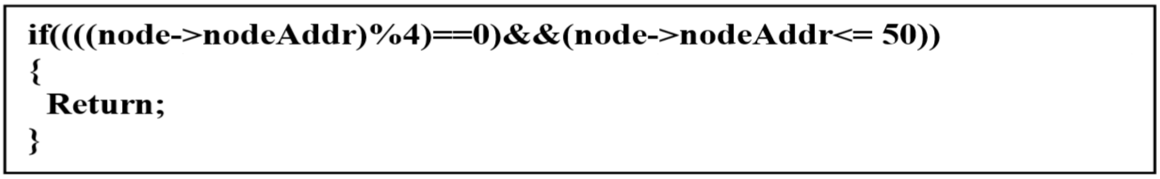


Fig. Architecture of DDoS attacks.

III. IMPLEMENTATION AND DETECTION OF DDOS ATTACK MECHANISMS IN MANET

3.1. Packet Dropping Attack:-

Here, a new attack, the Ad Hoc Packet Dropping Attack is presented which results in denial of service when used against all previously on-demand ad hoc network routing protocols. In this type of attack the attacker makes some nodes malicious, and the malicious nodes drops some or all data packets sent to it for further forwarding even when no congestion occurs [20]. Code for implementing Ad Hoc Packet Dropping attack is shown in "Fig. 1".



```
if((((node->nodeAddr)%4)==0)&&(node->nodeAddr<= 50))
{
 Return;
}
```

Figure 1. Code of Malicious Packet Dropping Based DDoS attack.

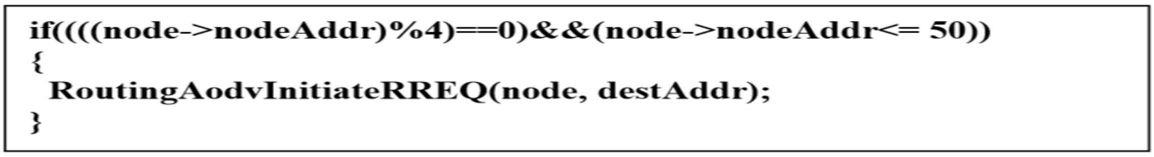
This code is placed in different functions of aodv.pc file. Code which is shown for dropping packet makes the node 0, 4, 8, 12, 16, 20, 24, 28 etcas malicious nodes. These nodes can drop some or all data packets transmitted to it for further forwarding. Unconditional Packet Dropping: It is technique to detect packet dropping attack in which we monitor the statistics Forward Percentage (FP) over a sufficiently long time period T [19].

FPM = Packets actually forwarded
Packets to be forwarded

FP determines the ratio of forwarded packets over the packets that are transmitted from M to m and that m should forward. If the denominator is not zero and FPi = 0, the attack is detected as Unconditional Packet ropping and m is identified as attacker. Here M represents the monitoring node and m the monitored node. Suppose we are sending packets from node 8 to node 9. If packets are to be forwarded by node 8 is 53 and packets received by node 9 is 0 which is the packets actually forwarded by node 8. Here denominator is not zero but FPi = 0. Hence attack detected is unconditional packet dropping and node 8 is malicious node.

3.2. Flooding Attack :-

Another type of DDOS attack is based on a huge volume of attack traffic which is termed as a Flooding based DDOS attack. Flooding-based DDOS attack attempts to congest the victim's network bandwidth with real-looking but unwanted IP data. Due to which , legitimate IP packets cannot reach the victim because of lack of bandwidth resource. Here, we introduce a new attack in the mobile ad hoc network, known as Adhoc Flooding Attack. The attack acts as an effective denial- of- service attack against all currently proposed on demand ad hoc network routing protocols,including the secure protocols. Hence on-demand routing protocols, such as Ad hoc On Demand Vector (AODV) cannot be immune from the Ad Hoc Flooding Attack. Code given for implementing Ad Hoc Flooding attack is shown in "Fig. 2".



```
if((((node->nodeAddr)%4)==0)&&(node->nodeAddr<= 50))
{
 RoutingAodvInitiateRREQ(node, destAddr);
}
```

Figure 2.Code for Flooding Based DDoS attack.

This code is placed in different functions of aodv.pc file. The Code which is given for flooding makes node 0, 4, 8, 12, 16, 20, 24, 28 etc as attack nodes. Therefore these attack nodes, send out mass RREQ packets all over the network so that the other nodes cannot build paths with each other. Malicious Flooding on SpecificTtarget: It is technique to detect flood attack in which monitor the total number of #T([m], [d]) over a period of time T for every destination d [19]. If it is larger than threshold MaxCount, the attack is a Malicious Flooding. Where # ([s],[d]) is the number of packets received on the monitored node (m) which is originated from s and destined to d.

IV. PREVENTION TECHNIQUE FOR FLOODING BASED DDOS ATTACK

4.1 Existing Prevention Techniques :

According to paper [8, 9] defence mechanisms to DDoS attacks are classified into two broad categories: local and global. As the name suggests local solutions may be implemented on the victim computer or its local network without an outsider's cooperation. Global solutions due to their different nature, requires the cooperation of many different Internet subnets, which in turn cross company boundaries.

4.1.1 Local Solutions: - Protection for individual computers falls into three areas.

4.1.2 Local Filtering: In this scheme we filter the packet at the local router level and detect them. The timeworn short-term solution is to try to stop the infiltrating IP packets on the local router by installing a filter to detect them. The stumbling block to this solution is that if an attack jams the victim's local network with enough traffic then it can overwhelms the local router and overloading the filtering software. Itcan also rendering it.

4.1.3 Changing IPs: A Band-Aid solution is to change the victim's address that is its IP address. When the whole process of changing the IP address is completed then the information will be sent to all the routers of that change and now if the attacker sends infected packets than the edge router will drop the packets.

4.1.4 Creating Client Bottlenecks: The objective behind this approach is to create bottleneck processes on the zombie computers and hencelimiting their attacking effect.

4.2 Global Solutions Clearly, as DDoS attacks target the deficiencies of the network/Internet as whole, local solutions to the problem become futile. From technological point of view global solutions are best. The main question is that whether there is a global incentive to implement them.

4.2.1 Improving the Security of the Entire Internet: Improving the security of all computers linked to the Internet would prevent attackers from finding enough vulnerable computers to break into and plant daemon programs that would turn them into zombies.

4.2.2 Using Globally Coordinated Filters: The strategy here is to prevent the accumulation of a critical mass of attackingdiffernt packets in time. Whenever filters installed throughout the Internet then a victim can send information that it has detected an attack and the filters can stop attacking the packets earlier along the attacking path, before they aggregate to get lethal proportions. That method is most effective even if the attacker has already seized enough zombie computers to pose a threat [9].

4.2.3 Tracing the Source IP Address: The goal of this approach is to trace the intruders' path back to the zombie computers and stop their attacks in order to find the original attacker and take appropriate actions. If tracing is already enough then it may help to stop the DDoS attack. Two attacker approches hinder tracing: IP spoofing that uses forged source IP addresses, the hierarchical attacking structure that detaches the control traffic from the attacking traffic and effectively hides the attackers even if the zombie computers are identified.

```
Algorithm used: DetectDosAttack(S, D) /* S is the source node and D is the Destination Node */
    Step - 1 As transmission begins it will search for all the intermediate nodes and send data on to it.
    Step - 2 The intermediate node failed forwarding the Hello Message to the next node.
    Step - 3 It will check the RESPONSE time for the intermediate node.
    Step - 4 If (Response Time>HopTime +Threshold)
        {Attacker Node is identified. Update Neighbour Node Table as well as Routing Table for the Intermediate
        Nodes.}
    Step - 5 Return
```

4.2.4 Disabling IP Broadcasts: A broadcast is a data packet that is destined for multiple hosts. Broadcasts can be occur on the data link layer and the network layer. Broadcasts which occur at data link layer are sent tohosts which are attached to a particular physical network. Broadcasts which occur at network layer are sent to all hosts attached to a particular logical network.Transmission Control Protocol/Internet Protocol (TCP/IP) supports the following types of broadcast packets:

All ones: By setting the broadcast address to all ones (255.255.255.255), all hosts on the network receive the broadcast.

Network: By setting the broadcast address to a specific network number in the network portion of the IP address and setting all ones in the host portion of the broadcast address then all the hosts on the defined network receive the broadcast. Take an example, when a broadcast packet is sent with the broadcast address of 131.108.255.255 then all the hosts on network number 131.108 get the broadcast.

Subnet: By setting the broadcast address to a specific network number and a specific subnet number. All hosts on the defined subnet receive the broadcast. Take an example when a broadcast packet is set with the broadcast address of 131.108.3.25 then all the hosts on subnet 3 of network 131.108 get the broadcast. As broadcasts are recognized by all the hosts , so a significant goal of router configuration is to control unnecessary proliferation of broadcast packets. Cisco routers support two types of broadcasts: Directed broadcast and Flooded broadcast. In directed broadcast a packet is sent to a specific network or series of networks, whereas in flooded broadcast packet is sent to every network. In IP internetworks most of the broadcast take the form of User Datagram Protocol (UDP) broadcasts. Consider the example of flooded broadcast which cause DDOS attack. A type of DDOS attack is the Smurf attack, which is made up of badly configured network devices that respond to ICMP echoes sent to broadcast addresses. The attacker sends a huge amount of ICMP traffic to a broadcast address and uses a victim's IP address as the source IP so the replies from all the devices that respond to the broadcast address will flood the victim. The main part of this type of attack is that the attacker can use a low-bandwidth connection to kill high bandwidth connections. Amount of traffic sent by the attacker is multiplied by a factor equal to the number of hosts behind the router that reply to the ICMP echo packets. The diagram in Figure 3 depicts a Smurf attack in progress. ICMP echo packets are sent by the attacker to the router at 128Kbps. Attacker can also modifies the packets by changing the source IP to the IP address of the victim's computer so replies to the echo packets will be sent to that address. Destination address of the packets is a broadcast address of the bounce site in this case it is 129.63.255.255. If the router is misconfigured to forward these broadcasts to hosts on the other side of the router (by forwarding layer 3 broadcasts to the layer 2 broadcast address FF:FF:FF:FF:FF:FF) the all of these host will give reply. In this particular example that means 630Kbps (5 x 128Kbps) of ICMP replies will be sent to the victim's system which in turn effectively disable its 512Kbps connection. Besides this target system intermediate router is also a victim and thus it is also the hosts in the bounce site. Attack that uses UDP echo packets instead of ICMP echo packets is called a Fraggle attack.

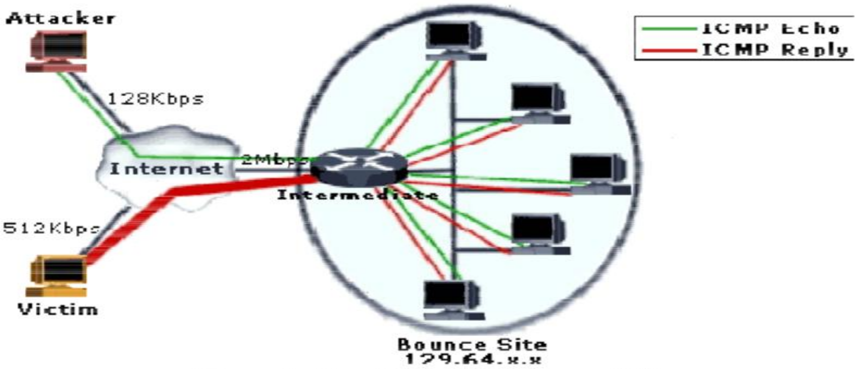


Figure 3: Smurf Attack in progress. [10]

From above example it is clear that IP broadcast cause the flood on the victim node. By disabling IP Broadcasts, host computers can no longer be used as amplifiers in ICMP Flood and Smurf attacks. However, to defend against this type of attack all neighbouring networks needs to be disable the IP broadcasts.

4.3 By calling Handle RREQ and Retry RREQ Functions: Another solution to prevent Flooding Based DDOS attack is by calling Handle RREQ and Retry RREQ functions. Flood attack occurs due to initiation of various RREQs on a particular node. Due to various RREQs that particular node is unable to handle more RREQ and becomes malicious node. When this node comes in the path of other nodes does not forward packets and busy in handling RREQ. In order to prevent network from this type of attackwe can call these functions as Handle RREQ and Retry RREQ. The Handle RREQ function helps in handling various RREQ which comes on a particular node and mitigate flood attack. Similarly, RetryRREQ function tries to find another path for forwarding packets from source to destination, this path may be larger from the path which is through malicious node but we get the path and packets are reached from source to destination. Both of these existing techniques only mitigate the effect of Flooding Based DDOS does not prevent it completely.

4.4 Proposed Prevention Technique Disabling IP Broadcasts:

Count the broadcasts done by the attacker IP and nullifying the effect of broadcast: Whenever the attacker floods the network with number of packets congestion occurs in the network due to which the traffic is not able to move. By disabling the IP of the attacker we are stopping the attacker to flood any more packets in the network but the packets already flooded by the attacker still exists in the network.By using this technique firstly we will find the attacker, disable his IP , then count the broadcast done by him with the help of an array and buffer and after counting the broadcast we will nullify their effect i.e. we will delete the packets from the network.

Performance measures are compared as follow:-

Packet Delivery Ratio (PDR): It is the ratio of the number of packets actually delivered without duplicates to the destinations versus the number of data packets supposed to be received. That particular number represents the effectiveness and throughput of a protocol in delivering data to the intended receivers within the network. The Number of successfully delivered legitimate packets is given as the ratio of number of generated legitimate packets.

PDR = Total Number of packets Sent
Packets Received

Number ofCollisions: In a network whenever two or more nodes attempt to transmit a packet across the network at the same time, a packet collision occurs. When a packet collision occurs the packets are either discarded or sent back to their original stations and then retransmitted to avoid the further collision. This type of Packet collisions results in the loss of packet integrity or can impede the performance of a network. This metric is used to measure such collisions in the network.

V. CONCLUSION

The proposed scheme incurs no extra overhead as it makes minimum modifications to the existing data structures and functions related to blacklisting a node in the existing version of pure AODV.Also the proposed scheme is more efficient in terms of its resultant routes establishment, resource reservations and due to its computational complexity. If more than one malicious node collaborate then they will be restricted as well as isolated by their neighbours, since they monitor and exercise control over forwarding RREQs by nodes. Thus this method successfully prevents DDOS attacks.

VI. CITATION

- WentaoLiu 2009"Third International Symposium on Intelligent Information Technology Application"
- Pajeet Sharma, Niresh Sharma, Rajdeep Singh (0975 – 8887) " International Journal of Computer Applications"
- V.Priyadharshini, Dr.K. Kuppusamy ,May-Jun 2012" International Journal of Engineering Research and Applications (IJERA)"
- EsraaAlomari, SelvakumarManickam, B. B. Gupta, Shankar Karuppayah, RafeefAlfaris, 7, July 2012" International Journal of Computer Applications ".
- A.Annalakshmi, Dr.K.R.Valluvan, 9, September 2012 "International Journal of Advanced Research in Computer Science and Software Engineering"
- SaurabhRatnaparikhi, AnupBhange, 12, December 2012" International Journal of Advanced Research in Computer Science and Software Engineering"
- Mukesh Kumar &Naresh Kumar, **July 2013** "International Journal of Application or Innovation in Engineering & Management (IJAIEM)"

REFRENCES

[1] C. Douligeris and A. Mitrokotsa. DDoS attacks and defense mechanisms: classification and stateof- the-art. Computer Networks, 44(5): 643-666, 2004.

[2] 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, November 2011

[3] KamanshisBiswas and Md. Liakat Ali; Security Threats in Mobile Ad Hoc Network; Master Thesis; Thesis no:MCS- 2007:07; March 22, 2007.

[4] Stephen M. Specht "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures" Sep. 2004

[5] Haggerty, J.; Qi Shi; Merabti, M., "Beyond the Perimeter: the Need forEarly Detection of Denial of Service Attacks", 18th Annual ComputerSecurity Applications Conference (ACSAC 2002)

[6] Rocky K. C. Chang, "Defending against Flooding-Based DistributedDenial-of-Service Attacks: A Tutorial", IEEE Communications Magazine,October 2002, pages: 42-51

[7] S.A.Arunmozhi, Y.Venkataramani, DDoS Attack and Defense Scheme in Wireless Ad hoc Networks, International Journal of Network Security & Its Applications, Vol.3, May 2011

[8] Wei Ren, Dit-Yan Yeung, Hai Jin1, and Mei Yang, Pulsing RoQDDoS Attack and Defense Scheme in Mobile Ad Hoc Networks, International Journal of Network Security, Vol.4, Mar. 2007