Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

STUDY OF VARIOUS PREVENTION TECHNIQUES USED FOR PACKET DROPPPING BASED DDOS FLOODING ATTACKS IN MOBILE AD-HOC NETWORK (MANET)

Ms. S.Suganthy
&
Mrs. R.Srimathi
Department of computer science,
Assistant professor,
Veltech Ranga Sanku Arts College, Avadi.
suganthyssss@gmail.com
1992srimathi@gmail.com

Abstract:

Ad-hoc network is self configured infrastructure less network without wires connection. The connections are established without any centralized administration. This study is to recognize the flaws of existing solutions to combat the DDoS attack and a prevention scheme is being provided with its validation to reduce the effect of DDoS attack in MANET Environment. As Internet users are growing day by day, it is becoming more prone to attacks and new hacking techniques. People are accessing information and communicating with each other on the move. Mobile Ad-hoc Network (MANET) is responsible for this rapid change in the alive of people. With the emergence of technology, where people transfer or share important documentations on the go with the help of laptops, PDAs, notebooks, smart phones etc., the loopholes in the Internet security have also enlarged and they are becoming more difficult to handle due to the characteristics of MANET such as dynamic topologies, low battery life, multicast routing, scalability, mobile agent based routing and power conscious routing, etc. The network is becoming more prone to attacks like DDoS attack, byzantine attack, resource consumption attack, blackhole attack,grayhole attack, etc. Therefore, there is an urgent need to expression into the security issues to allow authorized users to access the information available on Internet without any risk. In this study, the proposed scheme is the capability to prevent Distributed

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

DoS(DDoS) attack. The prevention of the proposed scheme in a series of simulations shows that the proposed scheme provides a better solution than existing schemes.

Keywords:DDoS attacks, MANET, IP Broadcast, PDR, Flooding etc.

INTRODUCTION

Ad-hoc network is the infrastructure less network without wires connection. Ad-hoc network is a two device network without wireless connection. A mobile ad hoc network(MANET) is a spontaneous network with no infrastructure network. Today, Internet has reformed every aspect of the computer and communications world. The widespread need and ability to connect machines across the Internet has produced the network to be more vulnerable to intrusions. Unluckily, with the growth of the Internet, the attacks to the Internet have also improvedextremely fast. A Mobile Ad hoc Network (MANET) is aunplanned network that can be established without any fixed infrastructure or a topology. This means that all its nodes perform as routers and take part in its discovery and conservation of routes (Chhabraet al., 2013). Its routing protocol has to be able to manage with the new difficulties that an adhoc network creates such as nodes mobility, limited power supply, quality of service, bandwidth, altering topology and security issues which make MANET more vulnerable to attacks and security issues. A Denial of Service (DoS) attack is commonly characterized as an event in which a legitimate user or organization is deprived of certain services, like e-mail or network connectivity, that they would normally assume to have (CERT, 2007b; Houleet al., 2001). DoS attacks introduce maliciously designed packets into the network to deplete some or all of these resources.

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

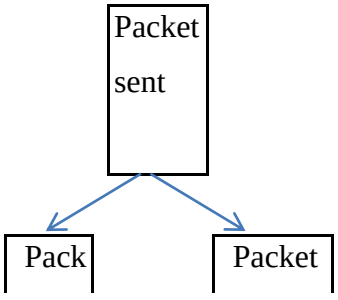
Distributed Denial of Service (DDoS) attacks has also become a problem for users of connected to the Internet. The attack power of a Distributed DoS (DDoS) attack (Lau et al., 2000) is based on the huge number of attack sources instead of the vulnerabilities of one particular protocol. DDoS attacks, which aim at overwhelming a target server with an immense volume of useless traffic from distributed and matched attack sources, are a major threat to the stability of the Internet (Elnoubiet al., 2011). Distributed Denial of Service (DDoS) attacks pose an immense threat to the Internet and many defines mechanisms have been proposed to combat the problem. Attackers constantly modify their tools to avoid these security systems and researchers in turn modify their approaches to handle new attacks Res. J. Appl. Sci. Eng. Technol., 7(10): 2033-2039, 2014 2034 (Mirkovicet al., 2004).Various DDoS attacks against high-profile websites such as yahoo, CNN Amazon and series of attacks on GRC. A recent DDoS attack reported was on Netflix and Spamhaus in March 2013 produced a great harm to these organizations.

This paper is various methods for prevention of DDoS attack. In this paper, we have proposed a method of protection against DDoSattack by using provider based deterministic packet dropping method. There are two types of DDoS attacks that Malicious Packet Dropping based DDoS attack and flooding based DDoS attack. The Malicious Packet Dropping based DDoS attack is called victim node. The attack of the victim node in order to drop some or all of the data packets sent to it for further forwarding even when no congestion occurs. The next type of DDoS attack is based on a huge volume of attack traffic, which is called as a Flooding based DDoS attack. A flooding based DDoS attack attempts to congest the victim's network. As a result, legitimate IP packets cannot spread the victim due to a lack of bandwidth resource. In this study, we compare two DDoS based attacks and propose a technique to prevent packet dropping based DDoS attack.

RELATED WORK

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

We study, a packet is sentfrom node A to node B. The expectation is that node B willrelay it to the next hop which is either the destination or anode along the route to the destination. The packet is eitherreceived by node or not received by node B. There are some causesthat may prevent a packet from being received. If Node B'sbuffer is full then it cannot accept any new packets and node dropsthem. Some packets may be despoiled due to channel errorwhich makes them unreadable and will be dropped by nodeB. Since nodes in ad hoc network mainly use Carrier SenseMultiple Access/Collision Avoidance (CSMA/CA), packetsmay collide. Collisions may be natural or intended. Naturalcollisions may happen when two nodes attempt to access themedium at the equal time. Late we will show that collisionsin ad hoc networks also depend on the traffic rate. When twoor more packets collide they will both be corrupted and notexpected at node B. Intended collisions can be caused by anode C that does not adhere to the rules of the MAC layerprotocol. These attacks are misbehavingattacks or as jamming. Lastly, jamming attacks canprevent a packet from being received.If a packet is received at node B then it may be forwardedcorrectly to the next hop, which is the best case. Node B maymaliciously try to corrupt the packet and then forward.



Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

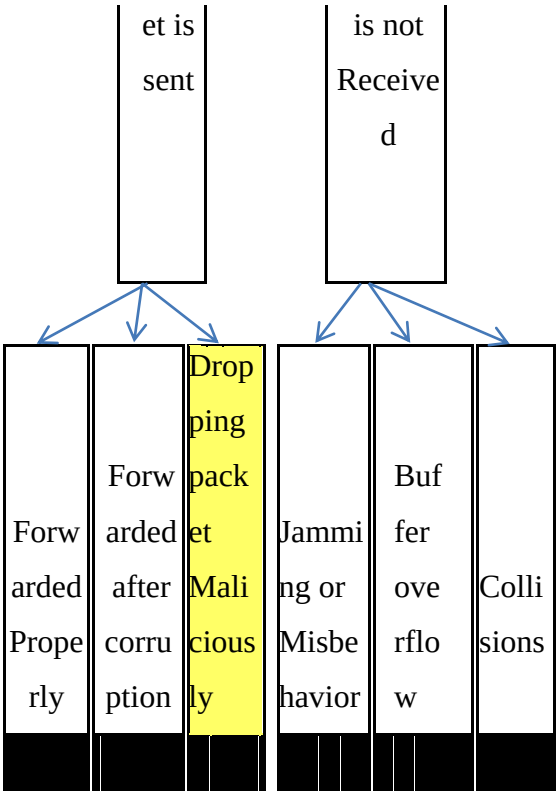


Diagram : packet drop

Distributed denial of services attack usually occurs in MANETS or in wireless networks. It is an attack where multiple systems contain 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 huge scale attempt by malicious users to flood the victim network with an enormous numbers of packets. First attacker builds a network of vulnerable nodes which are used to start 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 inspire the agents. The agents flood the victim.

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

3. DETECTION OF PACKET DROPPING BASED DDOS ATTACK IN MANET

Distributed denial of services attack commonly occurs in MANETS or in wireless networks. There are two types of attack.

3.1. Packet Dropping Attack:-

This paper, a new attack, the Ad Hoc Packet Dropping Attack is presented which results in denial of service when used against all beforehand 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.

Code for implementing Ad Hoc Packet Dropping attack is shown in Figure 1.

```
if((((node-
>nodeAddress)%4)==0)&&(node-
>nodeAddress<= 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, 28etcas malicious nodes. These nodes can drop some or all data packets transmitted to it for further forwarding. Total 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].

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

FPM = Packets truly 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 dropping and m is recognized as attacker. Here M represents the monitoring node and m the monitored node. Suppose we are sending packets from node 8 to node 9 then 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.

Flooding Attack:-

The next type of DDOS attack is based on a massive 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 spread the victim because of lack of bandwidth resource. 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 presently proposed on demand ad hoc network routing protocols, including the secure protocols. Later on-demand routing protocols, such as Ad hoc On Demand Vector (AODV) cannot be immune from the Ad Hoc Flooding Attack. Code given for applying Ad Hoc Flooding attack is shown in Figure 2.

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

```
if((((node-
>nodeAddress)%4)==0)&&(node-
>nodeAddress<= 50))

{

RoutingAodvInitiateRREQ(node,
destAddress);

}
```

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. Hence 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 Specific target: It is T 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.

Prevention Techniques:-

According to paper defense mechanisms to DDoS attacks are classified into two broad categories: local and global. As the name recommends local solutions may be implemented on the victim computer or its local network without an outsider's cooperation. Global solutions due

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

to their different environment, requires the cooperation of many different Internet subnets, which in turn cross company boundaries.

Local Solutions: -

Security for separate computers falls into three areas.

Local Filtering:

In this prevention scheme we filter the packet at the local router level and detect them. The time worn short- term solution is to attempt to stop the infiltrating IP packets on the local router by installing a filter to detect them. The uncertain 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. It can also translation it.

Changing IPs:

A Band-Aid solution is to alteration 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 modification and now if the attacker sends diseased packets than the edge router will drop the packets.

Creating Client Bottlenecks:

The objective behind this approach is to create bottleneck processes on the robot computers and hence limiting their attacking effect.

4.2 Global Solutions

Obviously, as DDoS attacks target the deficiencies of the network/Internet as whole, local solutions to the problem become wasted. From technical point of view global solutions are best. The main question is that whether there is a global incentive to implement them.

Improving the Security of the Entire Internet:

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

Improving the security of all computers linked to the Internet would prevent attackers from finding enough vulnerable computers to interruption into and plant daemon programs that would turn them into robot.

Using Globally Coordinated Filters:

The strategy here is to prevent the accumulation of a critical mass of attacking different packets in time. Every time filters connected throughout the Internet then a victim can send information that it has detected an attack and the filters can stop attacking the packets before 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.

Tracing the Source IP Address:

The goal of this method 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 methods hinder tracing: IP spoofing that uses forged source IP addresses, the hierarchical attacking structure that separates the control traffic from the attacking traffic and effectively hides the attackers even if the zombie computers are identified.

Algorithm used: DetectDDosAttack(S, D) /* S is the source node and D is the Destination Node */

Step - 1 As transmission initiates it will search for all the intermediate nodes and send data on to it.

Step - 2 The intermediate node unsuccessful 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)

Step - 5 Return

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

4.2.4 Disabling IP Broadcasts:

A broadcast is a data packet that is intended for multiple hosts. Broadcasts can be occurring on the data link layer and the network layer. Broadcasts which occur at data link layer are sent to hosts which are involved to a particular physical network. Broadcasts which ensue at network layer are sent to all hosts involved to a particular logical network.

Transmission Control Protocol/Internet Protocol (TCP/IP) maintenances 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 accept 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 well-defined subnet receive the broadcast. 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, while 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 instance of flooded broadcast which cause DDOS attack.

By calling Handle RREQ and Retry RREQ Functions:

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

An additional 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 arises in the path of other nodes does not forward packets and busy in handling RREQ. In order to avoid network from this type of attack we 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 diminish the effect of Flooding Based DDOS does not prevent it completely.

PREVENTION TECHNIQUE FOR FLOODING BASED DDOS ATTACK

The Proposed Prevention Technique Disabling IP Broadcasts:

Count the broadcasts finished 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 ending the attacker to flood any more packets in the network but the packets previously flooded by the attacker still exists in the network.By using this technique firstly we will discover 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 invalidate their effect i.e. we will delete the packets from the network.

Advantages of the Proposed Scheme:

The proposed scheme incurs no further overhead, as it makes minimal modifications to the existing data structures and functions connected to blacklisting a node in the existing version of pure AODV.Also the proposed scheme is more well-organized in terms of its resultant routes

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

established, resource reservations and its computational complexity.If more than one malicious node collaborate, they too will be constrained and isolated by their neighbors, since they monitor and exercise control over forwarding RREQs by nodes. Thus the scheme successfully prevents DDoS attacks.

PERFORMANCE MEASURES ARE COMPARED AS FOLLOW:

Packet Delivery Ratio (PDR):

It is the ratio of the number of packets actually delivered without replacements 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.

$$PDR = \frac{\text{Total Number of packets Sent}}{\text{Total number of Packets Received}}$$

Number ofCollisions:

In a network whenever two or more nodes attempt to transfer a packet across the network at the same time, a packet collision occurs. When a packet collision arises 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 block the performance of a network. This metric is used to measure such collisions in the network. In our simulations, we will study the effect of DDoS attacks under the next conditions:Different number of attackers.

RESULT:

Effect of disable IP broadcast Prevention Scheme with Different Number of

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

Attackers on PDR:

The effect of existing and proposed prevention technique on PDR with different number of attackers per network.Existing Prevention Technique procedures the function Handle RREQ & Retry RREQ to prevent flood based DDoS attack.

Effect of disable IP Broadcast Prevention Technique on Number of Collisions with varying number of attackers.

The effect of proposed prevention technique on Number of Collisions with different number of attackers and it also demonstrations comparison with the existing prevention scheme. This paper proposed prevention technique (By disabling IP Broadcast) diminish the effect of flooding based DDoS attack with larger extent. By using this technique number of collisions reductions up to 55.8% as compared to the collisions of existing prevention scheme and 46.4% as compared to flood based DDoS attack.

CONCLUSION

This paper defined implementation of DDoS attack on network and IP broadcast disable technique to prevent flooding based DDoS attack. It was found that flooding based DDoS attack have greater impact on network performance i.e. network performance reductions more in case of flooding attack. By implementing IP broadcast deactivate technique it was found that proposed prevention technique is better than existing techniques. Packet delivery ratio becomes pairs and number of collisions reduced to half by using proposed prevention technique under different number of attackers. Thus this method effectively prevents DDOS attacks.

References

[1]mukeshkumar& nares 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), July 2013 ISSN 2319 – 4847.

[2]ThaierHayajneh, Prashant Krishnamurthy, David Tipper, and Taehoon Kim, Detecting Malicious Packet Dropping in the Presence of Collisions and Channel Errors in Wireless Ad hoc Networks.

[3]MeghnaChhabra and B.B. Gupta, An Efficient Scheme to Prevent DDoS Flooding Attacks in Mobile Ad-Hoc
Network (MANET).ISSN: 2040-7459; e-ISSN: 2040-7467.

[4]ArushiBansal, Shakti Arora,:Survey on prevention Methods for DDoS Attacks in manets, International journal