DETECTION AND PREVENTION OF DDOS ATTACK IN MANET'S USING DISABLE IP BROADCAST TECHNIQUE

[1]Mukesh Kumar & [2]Naresh Kumar

[1]*Department of computer science & Engineering, HEC Jagadhri, Haryana, India*
[2]*Department of computer science & Engineering, U.I.E.T, Kurukshetra University Kurukshetra*

ABSTRACT

Ad-hoc network is the network comprised of wireless nodes. It is basically infrastructure less network which is self configured i.e. the connections are established without any centralized administration. MANET has no clear line of defence so it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can prevent MANET from various DDOS attacks. Different mechanisms have been proposed using various cryptographic techniques to countermeasures these attacks against MANET. These mechanisms are not suitable for MANET resource constraints, i.e., limited bandwidth and battery power because they introduced heavy traffic load to exchange and verifying keys. Therefore ad hoc networks have their own vulnerabilities that cannot be always tackled by these wired network security solutions. Distributed Denial of Service (DDoS) attacks has also become a problem for users of computer systems connected to the Internet. In this paper, a technique is proposed that can prevent a specific kind of DDoS attack i.e. flood attack which Disable IP Broadcast. The proposed scheme is distributed in nature it has the capability to prevent Distributed DoS (DDoS) attack. The performance of the proposed scheme in a series of simulations shows that the proposed scheme provides a better solution than existing schemes.

Keywords: MANET, DDOS attack, IP Broadcast, PDR, Flooding etc.

1. Introduction

Ad-hoc network is the network comprised of wireless nodes. It is basically infrastructure less network which is self configured i.e. the connections are established without any centralized administration [1,2]. A mobile ad hoc network (MANET) is a spontaneous network that can be established with no fixed infrastructure. This means that all its nodes behave as routers and take part in its discovery and maintenance of routes to other nodes in the network i.e. nodes within each other's radio range communicate directly via wireless links, while those that are further apart use other nodes as relays. Its routing protocol has to be able to cope with the new challenges that a MANET creates such as nodes mobility, security maintenance, quality of service, limited bandwidth and limited power supply. These challenges set new demands on MANET routing protocols. There are different major issues and sub-issues involving in MANET such as routing, multicasting/broadcasting, location service, clustering, mobility management, TCP/UDP, IP addressing, multiple access, radio interface, bandwidth management, power management, security, fault tolerance, QoS/multimedia and standards/products. Currently, routing, power management, bandwidth management, radio interface, attacks and security are hot topics in MANET research [1] [3]. Recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks. Distributed Denial of Service (DDoS) attacks have also become a problem for users of computer systems connected to the Internet. A DDoS attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets. This exhausts the victim network of resources such as bandwidth, computing power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated [2][5]. In this paper, we look into various methods for prevention of DDoS attacks.

Khan et al. [13] and Zhou et al. [16] give overview of challenges of DoS attack on MANET. Bin et al.[14] demonstrated how Distributed DoS (DDoS) attacks can be detected at an early stage. Chen et al. [15] explained Statefull DDoS attacks and targeted filtering. Siris et al. [17] and Abraham et al. [18] have proposed a method of defence against DDoS attack by using provider based deterministic packet marking and IP spoofing defence.

Here, we are discussing two types of DDoS attacks i.e. Malicious Packet Dropping based DDoS attack and Flooding Based DDoS attack [17]. The Malicious Packet Dropping based DDoS attack has the aim of attacking 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 second type of DDoS attack is based on a huge volume of attack traffic, which is known as a Flooding-based DDoS attack. A flooding-based DDoS attack attempts to congest the victim's network bandwidth with real-looking but unwanted IP data. As a result, legitimate IP packets cannot reach the victim due to a lack of bandwidth resource.

In this paper, we compare two DDoS based attacks and propose a technique to prevent Flooding based DDoS attack. The rest of the paper is organized as follows. The next section discusses the DDOS attacks in MANETS. In section 3 we discussed the Implementation and detection of DDOS attack mechanisms in MANET. In section 4, we describe the prevention technique for flooding based DDOS attack and next section presents the experimental setup to measure network performance. In section 6, we present various results which show that proposed Disable IP Broadcast Prevention technique is better than existing scheme. We conclude in Section 7.

2. DDOS Attacks in MANETs

Distributed denial of Service attacks usually occurs in MANETS or in wireless networks. It is an attack where multiple systems comprised together and target a single system causing a denial of service (DoS) [2,5]. The target node is flooded with the data packets that system shutdowns, thereby denying service to legitimate users. A Denial of Service (DoS) attack is an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system [7]. A DDoS attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets. This exhausts the victim network of resources such as bandwidth, computing power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated. Or in another way we can say that a Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. The services under attack are those of the "primary victim", while the compromised systems used to launch the attack are often called the "secondary victims." The use of secondary victims in a DDoS attack provides the attacker with the ability to wage a much larger and more disruptive attack while remaining anonymous since the secondary victims actually perform the attack making it more difficult for network forensics to track down the real attacker[6].

3. 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 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 for Malicious Packet Dropping Based DDoS attack.

This code is placed in different functions of aodv.pc file. Code shown for packet dropping makes node 0, 4, 8, 12, 16, 20, 24, 28 etc as malicious nodes. These nodes 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].

$$FP_m = \frac{\text{Packets actually forwarded}}{\text{Packets to be forwarded}}$$

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 the 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 to be forwarded by node 8 are 53 and packets received by node 9 is 0 which is the packets actually forwarded by node 8. Here denominator is not zero but $FP_i = 0$. 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 known as a Flooding-based DDoS attack. A flooding-based DDoS attack attempts to congest the victim's network bandwidth with real-looking but unwanted IP data. As a result, legitimate IP packets cannot reach the victim due to a lack of bandwidth resource. Here, we introduce a new attack in the mobile ad hoc network, which is called the Ad Hoc 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. Thus, existing on-demand routing protocols, such as Ad hoc On Demand Vector (AODV) cannot be immune from the Ad Hoc Flooding Attack. Code 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. Code shown for flooding makes node 0, 4, 8, 12, 16, 20, 24, 28 etc as attack nodes. These 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.

4. Prevention Technique for Flooding based DDOS Attack

4.1 Existing *Prevention Techniques :* According to paper [8, 9, 21] defence mechanisms to DDoS attacks are classified into two broad categories: local and global. As the name suggests, local solutions can be implemented on the victim computer or its local network without an outsider's cooperation. Global solutions, by their very nature, require the cooperation of several Internet subnets, which typically 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, it also overwhelms the local router, overloading the filtering software and rendering it inoperable. [9].

4.1.3 ***Changing IPs:*** A Band-Aid solution is to change the victim's IP address. As the whole process of changing the IP address is completed, all routers will be informed 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, limiting their attacking ability.

4.2 ***Global Solutions*** Clearly, as DDoS attacks target the deficiencies of the network/Internet as whole, local solutions to the problem become futile. Global solutions are better from a technological standpoint. The real question is 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 attacking packets in time. Once filters are installed throughout the network/Internet, a victim can send information that it has detected an attack, and the filters can stop attacking packets earlier along the attacking path, before they aggregate to lethal proportions. This method is 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 or, even better, to find the original attacker and take legal actions. If tracing is done promptly enough, it can help to abort the DDoS attack. Catching the attacker would deter repeat attacks. However, two attacker techniques hinder tracing: IP spoofing that uses forged source IP addresses, the hierarchical attacking structure that detaches the control traffic from the attacking traffic, effectively hiding attackers even if the zombie computers are identified.

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 because of initiating various RREQs on a particular node. Because of various RREQs that 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 attack, we can call these functions i.e. Handle RREQ and Retry RREQ. Handle RREQ function helps in handling various RREQ which comes on a particular node and mitigate flood attack. Similarly, Retry

RREQ 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:*

Disabling IP Broadcasts: A broadcast is a data packet that is destined for multiple hosts. Broadcasts can occur at the data link layer and the network layer. Data-link broadcasts are sent to all hosts attached to a particular physical network. Network layer broadcasts are sent to all hosts attached to a particular logical network. The 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, all hosts on the specified network receive the broadcast. For example, when a broadcast packet is sent with the broadcast address of 131.108.255.255, all hosts on network number 131.108 receive the broadcast.

Subnet: By setting the broadcast address to a specific network number and a specific subnet number, all hosts on the specified subnet receive the broadcast. For example, when a broadcast packet is set with the broadcast address of 131.108.3.255, all hosts on subnet 3 of network 131.108 receive the broadcast.

Because broadcasts are recognized by all hosts, a significant goal of router configuration is to control unnecessary proliferation of broadcast packets. Cisco routers support two kinds of broadcasts: directed and flooded. A directed broadcast is a packet sent to a specific network or series of networks, whereas a flooded broadcast is a packet sent to every network. In IP internetworks, most broadcasts take the form of User Datagram Protocol (UDP) broadcasts.

Consider the example of flooded broadcast which cause DDoS attack. Here, a nasty type of DDoS attack is the Smurf attack, which is made possible mostly because of badly configured network devices that respond to ICMP echoes sent to broadcast addresses. The attacker sends a large 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 nasty part of this attack is that the attacker can use a low-bandwidth connection to kill high-bandwidth connections. The 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. The attacker sends a stream of ICMP echo packets to the router at 128Kbps. The attacker 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. The destination address of the packets is a broadcast address of the so-called bounce site, in this case 129.63.255.255. If the router is (mis-) configured 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) all these host will reply. In the above example that would mean 630Kbps (5 x 128Kbps) of ICMP replies will be sent to the victim's system, which would effectively disable its 512Kbps connection. Besides the target system, the intermediate router is also a victim, and thus also the hosts in the bounce site. A similar attack that uses UDP echo packets instead of ICMP echo packets is called a Fraggle attack.

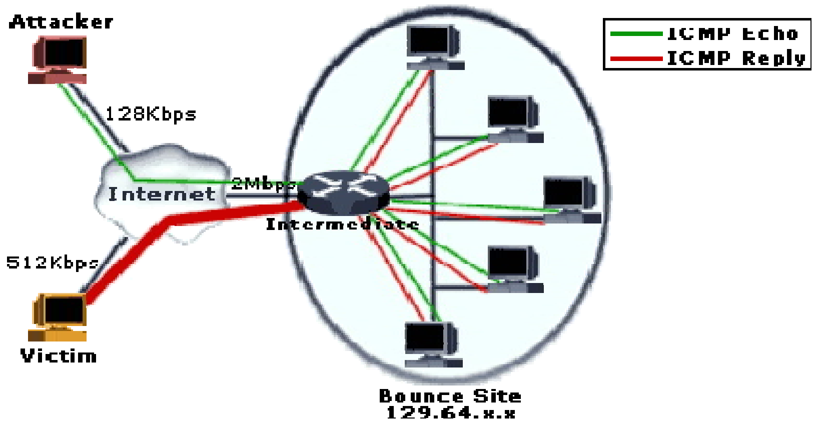

Figure 3: Smurf Attack in progress. [10]

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 attack, all neighboring networks need to disable IP broadcasts.

Advantages of the Proposed Scheme:

- The proposed scheme incurs no extra overhead, as it makes minimal 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 established, resource reservations and its computational complexity.
- If more than one malicious node collaborate, they too will be restricted and isolated by their neighbors, since they monitor and exercise control over forwarding RREQs by nodes. Thus the scheme successfully prevents DDoS attacks.

5. Experimental Setup

In this section we describe the parameters used in the simulations. The performance simulation environment used is based on GloMoSim[11][12], a network simulator that provides support for simulating multi-hop wireless networks complete with physical and IEEE 802.11 MAC layer models.

Experimental Setup and Performance Metrics are shown in Table 1.

Table 1: General Experimental Setup Parameters.

S. NO.	Parameter	Value	Description
1	Number of Nodes	0-50	Network Nodes
2	Terrain range	(1200,1200)	X,Y Dimension of motion in m.
3	Bandwidth	2Mbps	Node's Bandwidth
4	Simulation Time	0 - 20 S	Simulation Duration
5	Node-placement	Uniform	Node placement policy
6	Mobility	Random Waypoint Motion	Change Direction Randomly
7	Mobility	0 - 20 m/s	Mobility of Nodes
8	Traffic Model	CBR	Constant bit rate protocol
9	MAC Protocol	CSMA	MAC protocol used
10	Routing Protocol	AODV	Routing protocol used

The following performance measures are compared.

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. This number represents the effectiveness and throughput of a protocol in delivering data to the intended receivers within the network. Number of successfully delivered legitimate packets as a ratio of number of generated legitimate packets.

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

Number of Collisions: In a network, when 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 originating stations and then retransmitted in a timed sequence to avoid further collision. Packet collisions can result 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.

In our simulations, we will study the effect of DDoS attacks under the following conditions:

- Different number of attackers

6. Results

6.1 Effect of Proposed Prevention Scheme with Different Number of Attackers on PDR:

Table 2 and Figure 4 show the effect of existing & proposed prevention technique on PDR with different number of attackers per network. Existing Prevention Technique uses the function Handle RREQ & Retry RREQ to prevent flood based DDoS attack. The figure 4 shows that proposed prevention technique (By disabling IP Broadcast) mitigate the effect of flooding based DDoS attack with larger extent. By using this technique PDR increases up to 27.42% as compared to the PDR of existing prevention scheme and 53.14% as compared to flood attack.

Table 2: Effect on PDR of Existing & Proposed Prevention Technique with varying number of attackers.

Effect of Proposed Prevention Technique on PDR with varying number of attackers.				
Number Of Attackers Per Network	**PACKET Delivery Ratio (PDR)**			
	WITHOUT ATTACK	**FLOODING BASED DDoS ATTACK**	**EXISTING PREVENTION TECHNIQUE**	**PROPOSED PREVENTION TECHNIQUE**

2	0.926	0.32	0.57	0.89
3	0.926	0.31	0.55	0.86
4	0.926	0.22	0.47	0.79
5	0.926	0.2	0.45	0.74
6	0.926	0.175	0.44	0.69
7	0.926	0.15	0.42	0.63
8	0.926	0.12	0.39	0.61

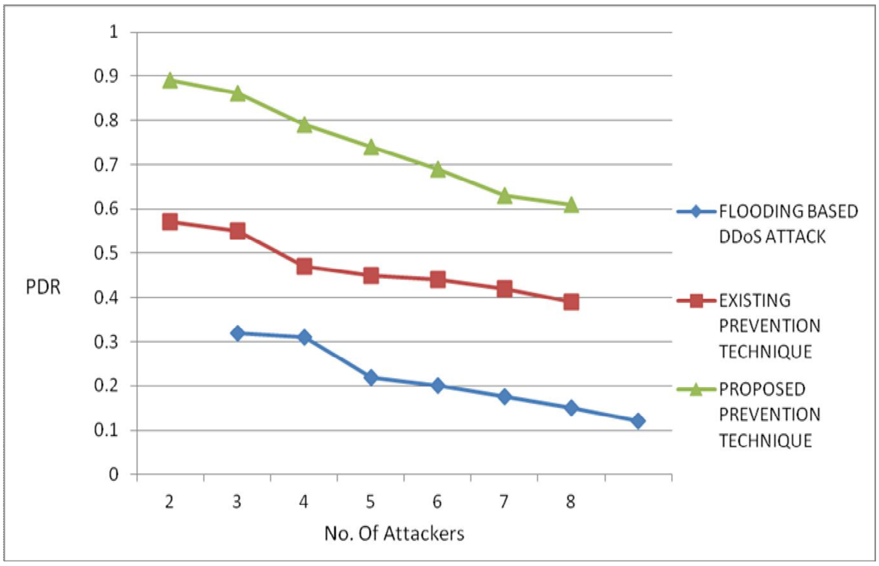

Figure 4: Effect of Proposed Prevention Technique on PDR with varying number of attackers.

6.2 Effect of Proposed Prevention Technique on Number of Collisions with varying number of attackers.

Table 3 and Figure 5 show the effect of proposed prevention technique on Number of Collisions with different number of attackers and it also shows comparison with the existing prevention scheme. This figure shows that proposed prevention technique (By disabling IP Broadcast) mitigate the effect of flooding based DDoS attack with larger extent. By using this technique number of collisions decreases up to 55.8% as compared to the collisions of existing prevention scheme and 46.4% as compared to flood based DDoS attack.

Table 3: Effect of Proposed Prevention Technique on Number of Collisions with varying number of attackers.

Number of Attackers Per Network	**Number Of Collisions Per Network**			
	WITHOUT ATTACK	**FLOODING BASED DDoS ATTACK**	**EXISTING PREVENTION TECHNIQUE**	**PROPOSED PREVENTION TECHNIQUE**
2	11	8543	7055	3755
3	11	8571	7091	3867
4	11	8685	7175	3987
5	11	8741	7233	4070
6	11	8756	7315	4115
7	11	8897	7400	4260
8	11	8918	7535	4315

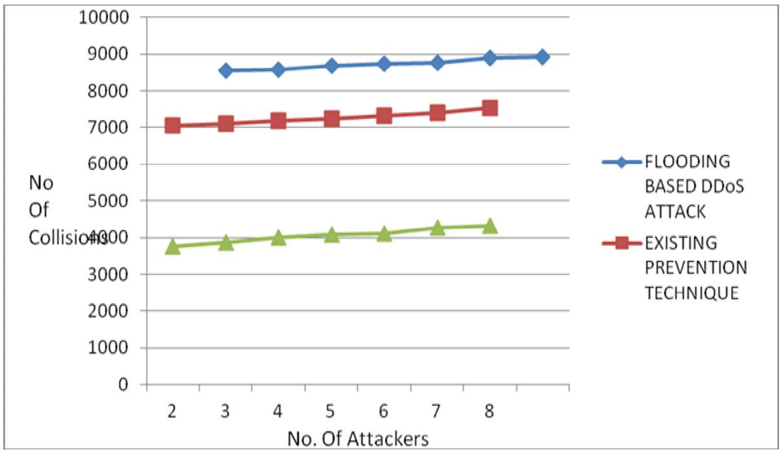

Figure 5: Effect of Proposed Prevention Technique on Number of Collisions with varying number of attackers.

7. Conclusion

This paper described 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 decreases more in case of flooding attack. By implementing IP broadcast disable technique it was found that proposed prevention technique is better than existing techniques. Packet delivery ratio becomes doubles and number of collisions reduced to half by using proposed prevention technique under different number of attackers.

References

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

[2.] Stephen M. Specht and Ruby B. Lee; Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures; Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550; September 2004.

[3.] Vesa Kärpijoki; Security in Ad Hoc Networks; Helsinki University of Technology; HUT TML 2000.

[4.] Yogesh Chaba, Yudhvir Singh, Preeti Aneja, “Performance Analysis of Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET” JOURNAL OF NETWORKS, VOL. 4, NO. 3, MAY 2009 ACADEMY PUBLISHER.

[5.] Felix Lau, Stuart H. Rubin, Michael H. Smith and Ljiljana TrajkoviC; Distributed Denial of Service Attacks; pp 2275- 2280/2004 IEEE.

[6.] Stephen M. Specht “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures” Sep. 2004.

[7.] David Karig and Ruby Lee, “Remote Denial of Service Attacks and Countermeasures,” *Princeton University Department of Electrical Engineering Technical Report CEL2001- 002*, Oct 2001.

[8.] S. Kannan, T. Maragatham, S. Karthik and V.P. Arunachalam; A Study of Attacks, Attack Detection and Prevention Methods in Proactive and Reactive Routing Protocols; International Business Management, 2011.

[9.] Hwee-Xian Tan and Winston K. G. Seah; Framework for Statistical Filtering Against DDOS Attacks in MANETs; Proceedings of the Second IEEE International Conference on Embedded Software and Systems; 2005.

[10.]TFreak; smurf.c; www.phreak.org/archives/exploits/denial/smurf.c; May 6, 2003.

[11.]GloMoSim, 2000, Available on: http://pcl.cs.ucla.edu/projects/glomosim.

[12.]X. Zeng *et al.*, “Glomosim: A library for parallel simulation of large-scale wireless networks,” In Workshop on Parallel and Distributed Bibliography 65 Simulation; Canada, May 1998, pp. 154–161.

[13.]Shafiullah Khan *et al*, “Denial of Service Attacks and Challenges in Broadband Wireless Networks,” International Journal of Computer Science and Network Security, Vol. 8, No. 7, pp. 1-6, July 2008.

[14.]Xiao Bin *et al*, “A novel approach to detecting DDoS Attacks at an Early Stage,” The Journal of Supercomputing, Springer, Volume 36, Number 3, June 2006 , pp. 235-248(14).

[15.]Shigang Chen *et al*, “Stateful DDoS attacks and targeted filtering,” Journal of Network and Computer Applications, Volume 30, Issue 3, August 2007, pp. 823-840.

[16.]Xiaobo Zhou *et al*, “Distributed denial-of-service and intrusion detection,” Journal of Network and Computer Applications, Volume 30, Issue 3, August 2007, pp. 819- 822.

[17.]Vasilios A. Siris *et al*, “Provider-based deterministic packet marking against distributed DoS attacks,” Journal of Network and Computer Applications, Volume 30, Issue 3, August 2007, pp. 858-876.

[18.] Yaar Abraham *et al* "StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense," *IEEE Journal on Selected Areas in Comunications* 24, no. 10 (October 2006): 1853-1863.

[19.] Yi-an Huang *et al.*, "A Cooperative Intrusion Detection System for Ad Hoc Networks," In *Proceedings of the* ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), Fairfax VA, October 2003.

[20.] M. Just, E. Kranakis, T. Wan, "Resisting Malicious Packet Dropping in Wireless Ad-Hoc Networks," In proceedings of 2nd Annual Conference on Adhoc Networks and Wireless (ADHOCNOW'03), Montreal, Canada, Oct 09- 10, 2003, pp. 151-163, LNCS, S. Pierre, M. Barbeau, E. Kranakis, eds., Vol. 2865.

[21.] Xianjun Geng and Andrew B. Whinston; Defeating Distributed Denial of Service Attacks; February, 2000.

[22.] Mukesh Kumar and Naresh Kumar "Study of Attack prevention methods for DDOS Attacks in Manets" IJARCSSE Volume 2, Issue 8, Aug. 2012 pp. 224-228.

Author

Mukesh Kumar received his B.Tech in Computer Science from S.K.I.E.T, Kurukshetra in 2010 and received M.Tech in Computer Science & Engineering from U.I.E.T., Kurukshetra University, Kurukshetra in 2012. He is presently working as Lecturer in HEC (Jagadhari). His research interests include Computer Networking, Theory of Computation, Data Structure and Network Security.

Naresh Kumar received his B.Tech & M.Tech degree in Computer Science & Engineering. He is presently working as Assistant professor in U.I.E.T., Department of Kurukshetra University, Kurukshetra. His research interests are in Computer Networking, Graph theory and Neural network.