A Protocol/Scheme to mitigate DDos attacks using AODV Protocol

Shanti Prakash Gehlot[1] Dr. Arun Kumar Singh[2]
[1, 2]Department of Computer Science & Engineering
[1, 2] SobhaSaria Engineering College, Sikar, Rajasthan (RTU)

Abstract—MANET(Mobile Adhoc Network) is an emerging technology and have great strength to be applied in battlefields and commercial applications such as traffic surveillance, MANET is infrastructure less without any centralized controller. Each node contains routing capability. Each device in a MANET is independent and can move in any direction. One of the major challenges wireless mobile ad-hoc networks face today is security, because no central controller exists. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a link layer ad hoc network. There are many security attacks in MANET and DDoS (Distributed denial of service) is one of them. Our main objective is seeing the effect of DDoS in routing, Packet Drop Rate, End to End Delay, no. of Collisions due to attack on network. And with these parameters and many more also we build secure IDS to detect this kind of attack and block it. In this thesis main objective is to study and implement the security against the DDOS attack. DDoS (Distributed Denial of Service) attacks in the networks are required to be prevented, as early as possible before reaching the victim node. DDos attack causes depletion of the network resources such as network bandwidth, disk space, CPU time, data structures, and network connections. Dealing with DDoS attacks is difficult due to their properties such as dynamic attack rates, big scale of botnets. DDos attack become more difficult to handle if it occurs in wireless network because of the properties of ad hoc network such as dynamic topologies, low battery life, Unicast routing Multicast routing , Frequency of updates or network overhead , scalability , mobile agent based routing ,power aware routing etc. Thus it is better to prevent the distributed denial of service attack rather than allowing it to occur and then taking the necessary steps to handle it. The following quantitative metrics Packet Delivery Ratio (PDR), Number of Collisions are to be used to evaluate the performance of DDoS attacks and their prevention techniques under different combinations in the fixed mobile ad hoc network. In our simulation, the effect of DDoS attacks under different number of attackers is studied.

I. INTRODUCTION

In view of the increasing demand for wireless information and data services, providing faster and reliable mobile access is becoming an important concern. Nowadays, not only mobile phones, but also laptops and PDAs are used by people in their professional and private lives. These devices are used separately for the most part that is their applications do not interact. Sometimes, however, a group of mobile devices form a spontaneous, temporary network as they approach each other. This allows e.g. participants at a meeting to share documents, presentations and other useful information. This kind of spontaneous, temporary network referred to as mobile ad hoc networks (MANETs) sometimes just called ad hoc networks or multi-hop wireless networks, and are expected to play an important role in our daily lives in near future.

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.

Ad hoc networks have a wide array of military and commercial applications. They are ideal in situations where installing an infrastructure network is not possible or when the purpose of the network is too transient or even for the reason that the previous infrastructure network was destroyed.

Security in mobile ad hoc networks is a hard to achieve due to dynamically changing and fully decentralized topology as well as the vulnerabilities and limitations of wireless data transmissions. Existing solutions that are applied in wired networks can be used to obtain a certain level of security. Nonetheless, these solutions are not always being suitable to wireless networks. Therefore ad hoc networks have their own vulnerabilities that cannot be always tackled by these wired network security solutions.

One of the very distinct characteristics of MANETs is that all participating nodes have to be involved in the routing process. Traditional routing protocols designed for infrastructure networks cannot be applied in ad hoc networks, thus ad hoc routing protocols were designed to satisfy the needs of infrastructure less networks. Due to the different characteristics of wired and wireless media the task of providing seamless environments for wired and wireless networks is very complicated. One of the major factors is that the wireless medium is inherently less secure than their wired counterpart. Most traditional applications do not provide user level security schemes based on the fact that physical network wiring provides some level of security. The routing protocol sets the upper limit to security in any packet network. If routing can be misdirected, the entire network can be paralyzed. This problem is enlarged in ad hoc networks since routing usually needs to rely on the trustworthiness of all nodes that are participating in the routing process. An additional difficulty is that it is hard to distinguish compromised nodes from nodes that are suffering from broken links.

Recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks. Distributed

All rights reserved by www.ijsrd.com

Denial of Service (DDoS) attacks has 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.

II. LITERATURE REVIEW

A. Wireless Ad hoc Networks [1]

Lu Han describes that the wireless ad hoc networks were first deployed in 1990's; Mobile Ad-hoc networks have been widely researched for many years. Mobile Ad-hoc Networks are collection of two or more devices equipped with wireless communications and networking capability. These devices can communicate with other nodes that immediately within their radio range or one that is outside their radio range. For the later, the nodes should deploy an intermediate node to be the router to route the packet from source toward destination. The Wireless Ad-hoc Networks do not have gateway, every node can act as the gateway. As per this paper, although, lots of research has been done on this particular field, it has often been questioned as to whether the architecture of Mobile Ad-hoc Networks is a fundamental flawed architecture. The main reason for the argument is that Mobile Ad-hoc Networks are not much used in practice, almost every wireless network nodes communicate to base station and access points instead of co-operating to forward packets hop-by-hop. As per the contents of this paper the key technologies to Wireless Ad-hoc Networks were not implemented as we expect.

B. Security Threats in Mobile ad-hoc Networks [2]

Kamanshis Biswas *et al.* mention that Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Although the ongoing trend is to adopt ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks. A number of challenges like open peer-to-peer network architecture, stringent resource constraints, shared wireless medium, dynamic network topology etc. are posed in MANET. As MANET is quickly spreading for the property of its capability in forming temporary network without the aid of any established infrastructure or centralized administration, security challenges has become a primary concern to provide secure communication. This paper gives information about various security threats an ad-hoc network faces, the security services required to be achieved and the countermeasures for attacks in each layer. As per the contents of this paper, secure routing protocol is still a burning question.

C. Denial of Service and Distributed Denial of Service Attacks [3]

Andrim Piskozub gives main types of DoS attacks which flood victim's communication channel bandwidth, is carried out their analysis and are offered methods of protection from these attacks. The DDoS attacks are considerably more effective than their DoS-counterparts because they allow performing such attacks simultaneously from several sites, that makes this attack more efficient and complicates searches of attacker. Attacker uses the client program, which, in turn, interacts with the handler program. The handler sends commands to the agents, which perform actual DoS attacks against indicated system-victim. This paper also describes various countermeasures that should be taken to prevent the network from DDoS attack.

D. Defeating Distributed Denial of Service Attacks [4]

Xianjun Geng *et al.* describe that the notorious, crippling attack on e-commerce's top companies in February 2000 and the recurring evidence of active network scanning—a sign of attackers looking for network weaknesses all over the Internet—are harbingers of future Distributed Denial of Service (DDoS) attacks. They signify the continued dissemination of the evil daemon programs that are likely to lead to repeated DDoS attacks in the foreseeable future. This paper gives information about network weaknesses that DDoS attacks exploit the technological futility of addressing the problem solely at the local level, potential global solutions, and why global solutions require an economic incentive framework.

E. Detecting DDoS attack traffic at the agent machines [5]

Vicky Laurens et al. describe that due to financial losses caused by Distributed Denial of Service (DDoS) attacks; most defense mechanisms have been deployed at the network where the target server is located. This paper believes that this paradigm should change in order to tackle the DDoS threat in its basis: thwart agent machines participation in DDoS attacks. Paper consists of developing an agent to monitor the packet traffic rate (outgoing packets / incoming packets). The deployment is based upon characterizing TCP connections; normal TCP connections can be characterized by the ratio of the sent packets to the received packets from a given destination. Preliminary results have shown that the traffic ratio values usually present larger values at the beginning of the run when there are not enough packets to make a decision on whether or not traffic is legitimate. A low value for threshold allows for faster attack detection, but it also increases the number of false-positives. Although results are promising, more research must be conducted. It is necessary to develop a more flexible attack tool to test the agent under several different attack scenarios such as pulsing attacks and higher rate attacks with a short duration. DDoS attacks with low rate transmission packets are probably the biggest challenges in detecting attack traffic at the agent machines.

F. Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures [6]

Stephen M. Specht *et al.* describe that Distributed Denial of Service (DDoS) attacks have become a large problem for users of computer systems connected to the Internet. DDoS attackers hijack secondary victim systems using them to wage a coordinated large-scale attack against primary victim systems. As new countermeasures are developed to prevent or mitigate DDoS attacks, attackers are constantly developing new methods to circumvent these new countermeasures. This paper gives us information about

All rights reserved by www.ijsrd.com

DDoS attack models and proposed taxonomies to characterize the scope of DDoS attacks, the characteristics of the software attack tools used, and the countermeasures available. These taxonomies illustrate similarities and patterns in different DDoS attacks and tools, to assist in the development of more generalized solutions to countering DDoS attacks, including new derivative attacks. It is essential, that as the Internet and Internet usage expand, more comprehensive solutions and countermeasures to DDoS attacks be developed, verified, and implemented. Thus, this paper describes that DDoS attacks make a networked system or service unavailable to legitimate users. These attacks are an annoyance at a minimum, or can be seriously damaging if a critical system is the primary victim. Loss of network resources causes economic loss, work delays, and loss of communication between network users. Solutions must be developed to prevent these DDoS attacks.

G. On the Effectiveness of DDoS Attacks on Statistical Filtering [7]

Qiming Li *et al.* mention that Distributed Denial of Service (DDoS) attacks pose a serious threat to service availability of the victim network by severely degrading its performance. There has been significant interest in the use of statistical-based filtering to defend against and mitigate the effect of DDoS attacks. Under this approach, packet statistics are monitored to classify normal and abnormal behavior. Under attack, packets that are classified as abnormal are dropped by the filter that guards the victim network. This paper gives the effectiveness of DDoS attacks on such statistical-based filtering in a general context where the attackers are "smart". They first give an optimal policy for the filter when the statistical behaviors of both the attackers and the filter are static. Next, this paper considers cases where both the attacker and the filter can dynamically change their behavior, possibly depending on the perceived behavior of the other party. This paper observes that while an adaptive filter can effectively defend against a static attacker, the filter can perform much worse if the attacker is more dynamic than perceived.

III. PROPOSED METHODOLOGY

A. 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:

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

2) *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.

3) *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.

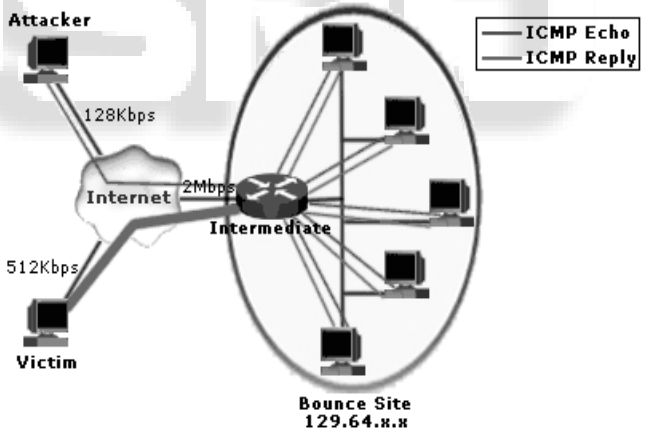

Fig. 1: Smurf Attack

The diagram in Figure 1 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

All rights reserved by www.ijsrd.com

that uses UDP echo packets instead of ICMP echo packets is called a Fragile attack.

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.

Points of the Proposed Scheme

1) 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.
2) Also the proposed scheme is more efficient in terms of its resultant routes established, resource reservations and its computational complexity.
3) 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.

Algorithm

Step. 1 : DetectDosAttack(S, D) /* S is the source node and D is the Destination Node */

Step. 2 : As transmission begins it will search for all the intermediate nodes and send data on to it.

Step. 3 : The intermediate node failed forwarding the Hello Message to the next node.

Step. 4 : It will check the RESPONSE time for the intermediate node.

Step. 5 : If (Response Time> HopTime +Threshold)
{
The Attacker Node is detected. Update Neighbor Node Table & Routing Table for the Intermediate Nodes
}

Step. 6 : Return

RREQ packets will be flooded in the network once the path discovery process is invoked in the AODV protocol. Therefore, the AODV protocol adopts some methods to reduce the network congestion. One way is that a node cannot originate excessive RREQ packets more than a limit. Another way is to setup a (Time-To-Live) value in the IP header for each RREQ packet. The RREQ packets will be dropped if their correspondent TTL value is 0. After broadcasting a RREQ, a node waits for a RREP. If a route is not received within round-trip time, the node may try again to discover a route by broadcasting another RREQ, up to a maximum retry times at the maximum TTL value.

Proposed technique to implement prevention mechanism is By Disabling IP Broadcast. IP Broadcast is used in AODV routing Protocols to broadcast RREQ packets on all the nodes in the network. Flood attack occurs because of initiating lots of RREQ packets in the network so that network becomes congested and no bandwidth is available to send packets. Hence by disabling the IP Broadcast all the RREQs which are broadcast to all nodes are disabled.

IV. RESULTS

A. Performance Metrics

The following quantitative metrics are to be used to evaluate the performance of DDoS attacks and their prevention techniques under different combinations in the fixed mobile ad hoc network.

1) 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.

$$PDR = \frac{Total\ Number\ of\ Packets\ sent}{Total\ Number\ of\ Packets\ received}$$

B. 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.

C. With Different Number of Attackers

Table 1 shows the effect of proposed prevention technique on PDR with different number of attackers and it also shows comparison when there is no attack in the network. This figure 2 shows that proposed prevention technique mitigate the effect of flooding based DDoS attack with larger extent. By using this technique PDR increases up to 31% as compared to the PDR in case of flooding attack.

NUMBER OF ATTACKERS PER NETWORK	PACKET DELIVERY RATIO (PDR)		
	WITHOUT ATTACK	FLOODING BASED DDoS ATTACK	PROPOSED PREVENTION TECHNIQUE
2	.926	0.34	0.920
4	.926	0.31	0.890
6	.926	0.20	0.855
8	.926	0.15	0.810
10	.926	.175	0.783

Table. 1: Effect of Proposed Prevention Technique on PDR with varying number of attackers

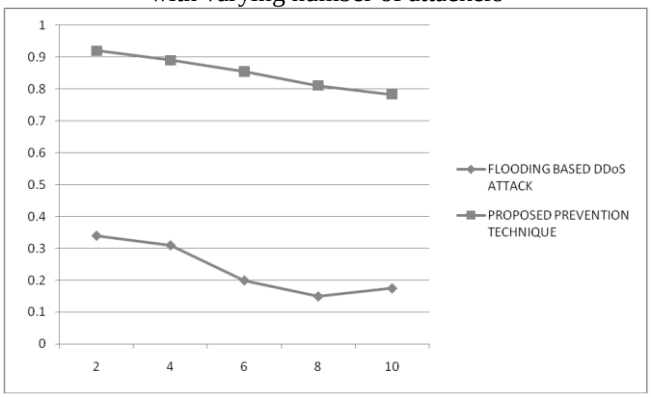

Fig. 2: Graph of Proposed Technique checked for PDR

All rights reserved by www.ijsrd.com

Table. 2 shows the effect of proposed prevention technique on Number of Collisions with different number of attackers and it also shows comparison when there is no attack in the network. This figure shows that proposed prevention technique mitigate the effect of flooding based DDoS attack with larger extent. By using this technique number of collisions decreases up to 41% as compared to the collisions in case of flooding based DDoS attack

NUMBER OF ATTACKERS PER NETWORK	NUMBER OF COLLISIONS		
	WITHOUT ATTACK	FLOODING BASED DDoS ATTACK	PROPOSED PREVENTION TECHNIQUE
2	11	8488	957
4	11	8571	1076
6	11	8741	2036
8	11	8897	3012

Table. 2: Effect of Proposed Prevention Technique on the number of collisions in the network with varying number of attackers.

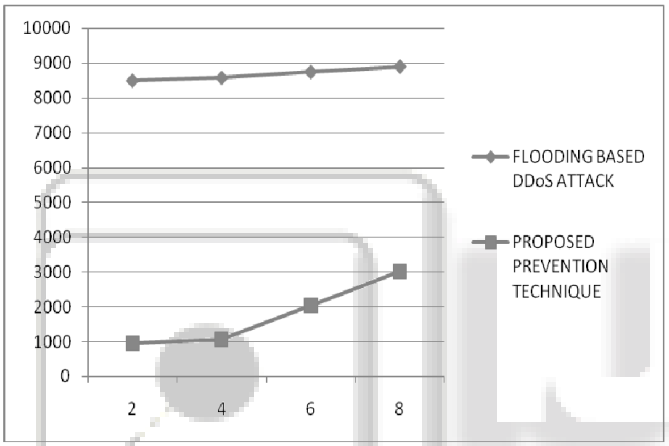

Fig. 3: Graph of Proposed Technique checked for No. of Collisions

V. CONCLUSIONS & FUTURE SCOPE

A. *Conclusion*

Detection & Prevention of DDoS attacks is a part of an overall risk management strategy for an organization. Each organization must identify the most important DDoS risks, and implement a cost-effective set of defense mechanisms against those attack types causing the highest risk for business continuity. Studies and news about real-life DDoS attacks indicate that these attacks are not only among the most prevalent network security risks, but that these attacks can also block whole organizations out of the Internet for the duration of an attack. The risk from DDoS attacks should not thus be underestimated, but not overestimated, either.

The main contributions of this thesis are the following:

First, we have implemented the DDoS attack mechanisms. Two different attack mechanisms are: Ad Hoc Packet Dropping Attack and Ad Hoc Flooding Attack.

Effect of different attack mechanisms on network performance is analyzed and we find that flooding based DDoS attack have greater impact on network performance.

Detection mechanisms to detect DDoS attack type and victim node are studied and a detection scheme is implemented which help in finding victim/malicious node. Effectiveness of detection scheme has been demonstrated by tables and figures. So that prevention technique is implemented on that particular node.

Next, two techniques to prevent flooding based DDoS attack are implemented and simulation results shows that proposed prevention technique is better than existing technique. Packet delivery ratio becomes doubles; number of collisions decreases or becomes half by using proposed prevention technique under different number of attackers.

B. *Future Scope*

In future, we will evaluate our framework for more internet topologies. In particular, we plan to investigate the following issues in more detail.

1) Detection mechanism implemented in the thesis detect only victim node not the attack type. So, we plan to implement a new detection mechanism which not only detect attacking node but also attack type.
2) During the dissertation, we have implement only two attack mechanisms for DDoS attack. But there are lots more DDoS attack types which have greater impact on network performance are yet to be implemented and we plan to implement them in future.
3) During the dissertation, we have implement prevention technique for flooding attack. Prevention scheme for Packet dropping is not implemented and we plan to find and implement prevention scheme for Packet Dropping based DDoS attack.

REFERENCES

[1] Lu Han "Wireless Ad hoc Networks" October 8, 2004.
[2] Kamanshis Biswas "Security Threats in Mobile ad-hoc Networks" March 2007.
[3] Andrim Piskozub "Denial of Service and Distributed Denial of Service Attacks ".
[4] Xianjun Geng "Defeating Distributed Denial of Service Attacks" July 2002.
[5] Vicky Laurens "Detecting DDoS attack traffic at the agent machines" May 2006.
[6] Stephen M. Specht "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures" Sep. 2004.
[7] Qiming Li "On the Effectiveness of DDoS Attacks on Statistical Filtering".
[8] Hwee-Xian Tan "Framework for Statistical Filtering against DDoS Attacks in MANETs" 2005.
[9] Antonio Challita 'A Survey of DDoS Defense Mechanisms".
[10] Yi-an Huang "A Cooperative Intrusion Detection System for Ad Hoc Networks" 2003.
[11] Mike Just "Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks"
[12] Bo-Cang Peng and Chiu-Kuo Liang "Prevention Techniques for Flooding Attacks in Ad Hoc Networks"
[13] Rizwan Khan and A. K. Vatsa "Detection and Control of DDOS Attacks over Reputation and Score Based MANET" October 2011.

All rights reserved by www.ijsrd.com

[14] HyoJin Kim, Ramachandra Bhargav Chitti and JooSeok Song "Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks" March 2011.
[15] Yogesh Chaba and Yudhvir Singh "Performance Analysis of Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET" May 2009.

All rights reserved by *www.ijsrd.com*