"DoS (JAMMING ATTACK) Prevention In MANET"

Sunil Saini*

ABSTRACT

A mobile ad hoc network (MANET) is a spontaneous network that can be established with no fixed infrastructure. Security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Denial of Service (DoS) attacks has also become a major problem in MANET. A DoS attack is a 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. In Mobile Ad hoc Networks (MANET), various types of Denial of Service Attacks (DoS) are possible because of the inherent limitations of its routing protocols. Considering the Ad hoc On Demand Vector (AODV) routing protocol as the base protocol it is possible to find a suitable solution to overcome the malicious flooding i.e. attack of initiating / forwarding Route Requests (RREQs) that lead to hogging of network resources and packet dropping is a technique in which a node drops data packets (conditionally or randomly) that it is supposed to forward hence denial of service to genuine nodes. In this dissertation, a proactive scheme is proposed that can prevent a specific kind of DoS attack and identify the misbehaving node. Since the proposed scheme is distributed in nature it has the capability to prevent DoS well. The performance of the proposed algorithm in a series of simulations reveals that the proposed scheme provides a better solution than existing approaches.

KEWORDS:DOS,MANET,AODV.

* **Research Scholar**

1. INTRODUCTION

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 Mobile 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.

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 Mobile 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 be suitable to Mobile networks. Therefore ad hoc networks have their own vulnerabilities that cannot be always tackled by these wired network security solutions.

Recent Mobile research indicates that the Mobile MANET presents a larger security problem than conventional wired and Mobile networks. Denial of Service (DoS) attacks has also become a problem for users of computer systems connected to the Internet. A DoS 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.

Preventing DoS attacks is difficult especially due to the following problems:

- Very little has been done to compare, contrast, and categorize the different ideas related to DoS attacks and defenses. As a result it is difficult to understand what a computer network user needs to do and why to prevent the threat from DoS attacks.
- There are no effective defense mechanisms against many important DoS attack types.
- There is no guidance on how to select defense mechanisms.
- Existing defense mechanisms have been evaluated according to very limited criteria. Often relevant risks have been ignored or evaluations have been carried out under

ideal conditions. No research publications exist for giving a systematic list of issues related to defense evaluation.

MOBILE AD HOC NETWORKS

A Mobile Ad Hoc Network (MANET) consists of a set of mobile hosts that carry out basic networking functions like packet forwarding, routing, and service discovery without the help of an established infrastructure [1]. Nodes of an ad hoc network rely on one another in forwarding a packet to its destination, due to the limited range of each mobile host's Mobile transmissions. An ad hoc network uses no centralized administration. This ensures that the network will not cease functioning just because one of the mobile nodes moves out of the range of the others. Nodes should be able to enter and leave the network as they wish. Because of the limited transmitter range of the nodes, multiple hops are generally needed to reach other nodes. Every node in an ad hoc network must be willing to forward packets for other nodes. Thus, every node acts both as a host and as a router. The topology of ad hoc networks varies with time as nodes move, join or leave the network. This topological instability requires a routing protocol to run on each node to create and maintain routes among the nodes [3].

Security Attacks in MANETs

The security attacks in MANETs can be categorized as **A**ctive attacks and **P**assive attacks.

- **A**ctive **A**ttack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious
- **P**assive **A**ttacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish.

Various types of attacks in MANETs are: **M**odification, **I**mpersonation, **F**abrication, **E**avesdropping, **R**eplay, **D**enial **o**f **S**ervice, **M**alicious **S**oftware and **L**ack **o**f **C**ooperation. Denial of Service attack is described below.

2. DENIAL OF SERVICE (DoS) ATTACK

A denial of service (DoS) attack is characterized by an explicit attempt by an attacker to prevent legitimate users of a service from using the desired resources. Examples of denial of service attacks include:

- attempts to "flood" a network, thereby preventing legitimate network traffic
- attempts to disrupt connections between two machines, thereby preventing access to a service
- attempts to prevent a particular individual from accessing a service
- attempts to disrupt service to a specific system or person.

A DoS (Distributed Denial-Of-Service) attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets [2]. 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. The distributed format adds the "many to one" dimension that makes these attacks more difficult to prevent. A Denial of Service attack is composed of four elements, as shown in Figure 2.3. First, it involves a victim, i.e., the target host that has been chosen to receive the brunt of the attack. Second, it involves the presence of the attack daemon agents. These are agent programs that actually conduct the attack on the target victim. Attack daemons are usually deployed in host computers. These daemons affect both the target and the host computers.

- he real attacker sends an "execute" message to the control master program.
- The control master program receives the "execute" message and propagates the command to the attack daemons under its control.
- Upon receiving the attack command, the attack daemons begin the attack on the victim.

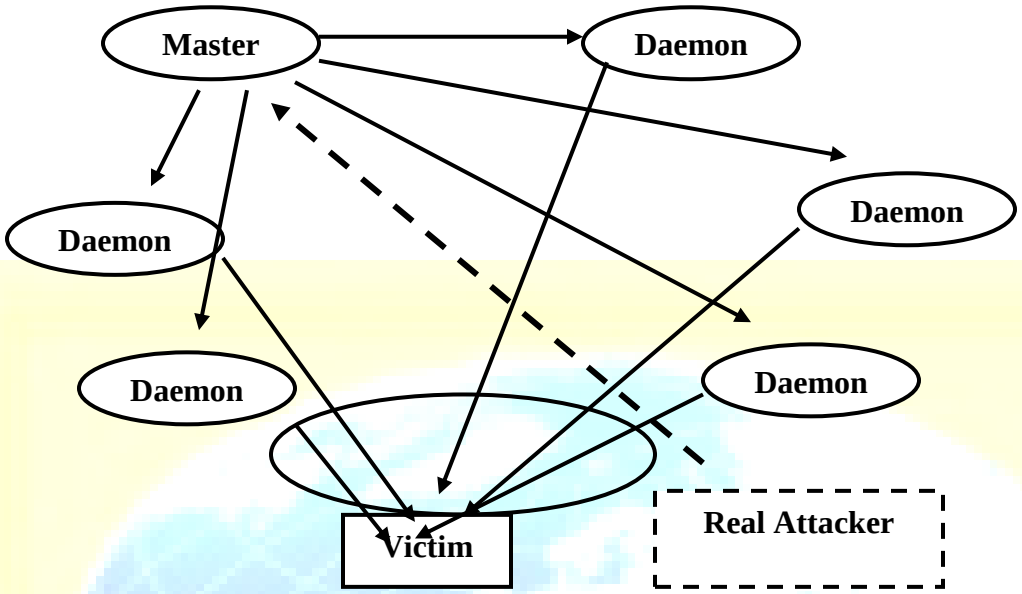

Figure 2.3: The four Components of DoS Attacks.

Architecture of DoS Attacks

Before real attack traffic reaches the victim, the attacker must cooperate with all its DoS agents. Therefore, there must be control channels between the agents and the attacker [7]. This cooperation requires all agents send traffic based on commands received from the attacker. The network which consists of the attacker, agents, and control channels is called the attack networks. In [2], attack networks are divided into three types: the agent-handle model, the Internet Relay Chat (IRC)-based model, and the reflector model.

The agent-handler model consists of three components: attacker, handlers, and agents [9]. Figure 2.4 illustrates the typical architecture of the model. One attacker sends control messages to the previously compromised agents through a number of handlers, instructing them to produce unwanted traffic and send it to the victim.

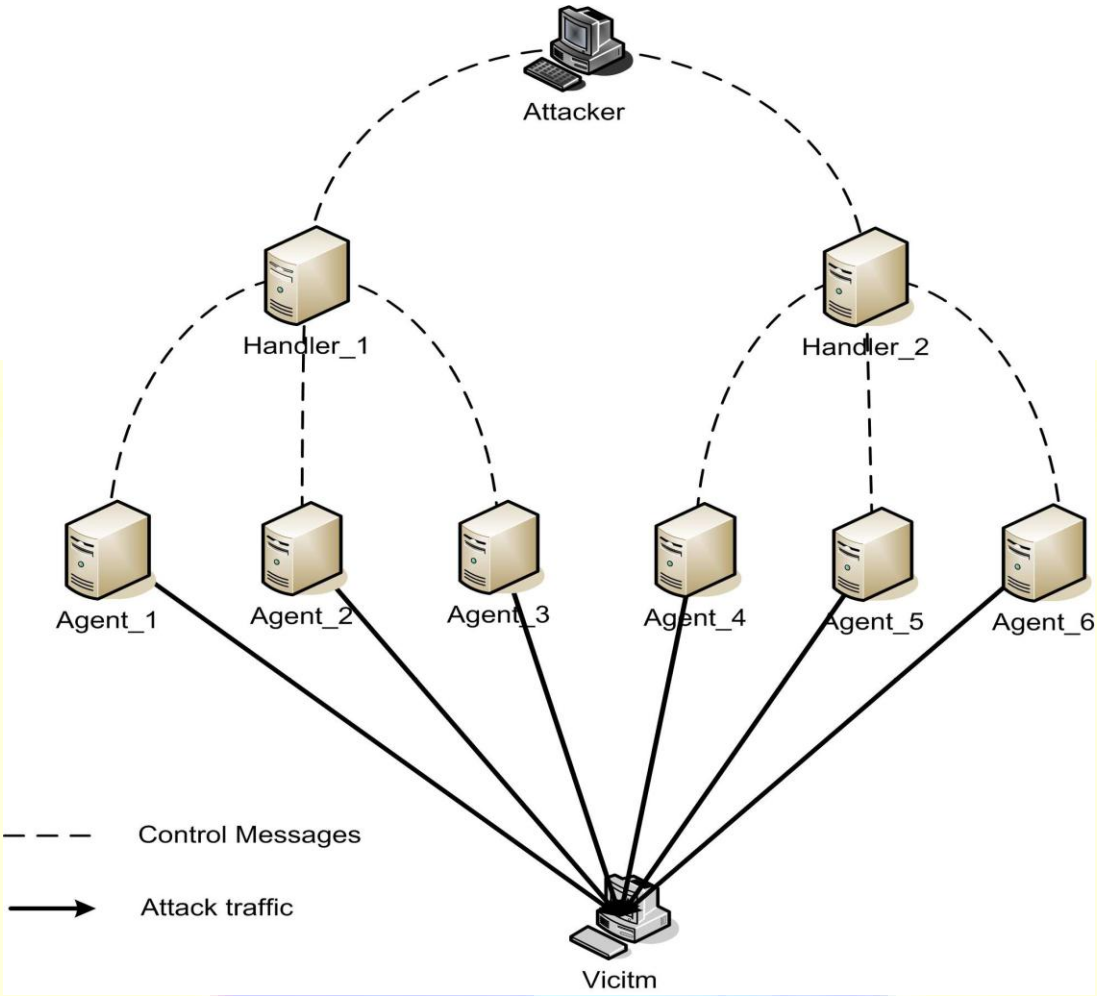

Figure 2.4: Typical architecture of a DoS attack.

The architecture of IRC-based model is not that much different than that of the agent-handler model except that instead of communication between an attacker and agents based on handlers, an IRC communication channel is used to connect the attacker to agents [2].

Figure 2.5 illustrates the architecture of an attack network in the reflector model. The reflector layer makes a major difference from the typical DoS attack architecture. In the request messages, the agents modify the source address field in the IP header using the victim's address to replace the real agents' addresses. Then, the reflectors will in turn generate response messages to the victim. As a result, the flooding traffic which reaches the victim is not from a few hundred agents, but from a million reflectors [8]. An exceedingly diffused reflector-based DoS attack raises the bar for tracing out the real attacker by hiding the attacker behind a large number of reflectors.

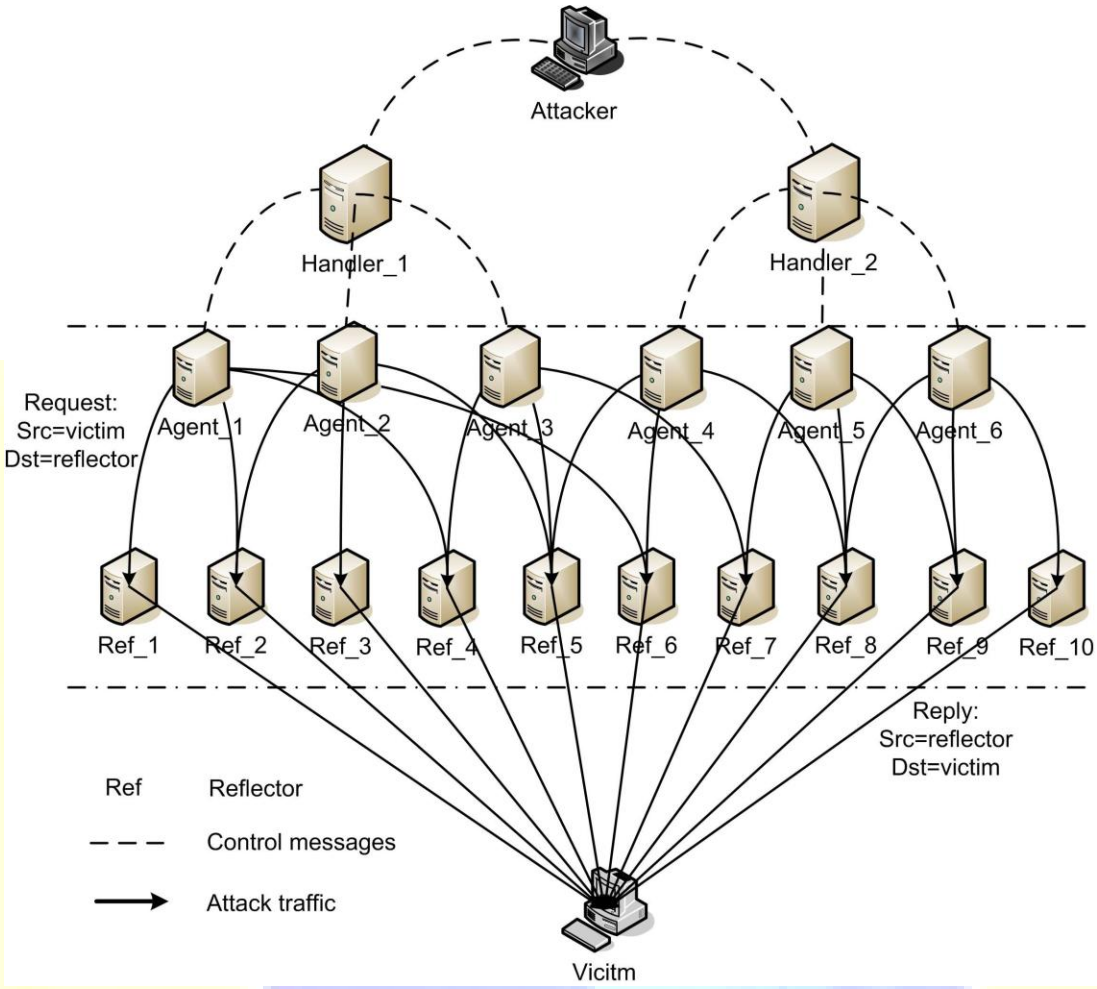

Figure 2.5: Architecture of a DoS attack using reflectors.

Unlike some types of DoS attacks, "the reflector does not need to serve as an amplifier" [8]. This means that reflectors still can serve other legitimate requests properly even when they are generating attack traffic. The attacker does not need to compromise reflectors to control their behaviors in the way that agents need to be compromised. Therefore, any host which will return a response if it receives a request can be a reflector. These features facilitate the attacker's task of launching an attack because it just needs to compromise a small number of agents and find a sufficient number of reflectors.

DoS Attack Taxonomy

There are a wide variety of DoS attacks. Two types of DoS attacks are: Active and passive attack. Packet dropping is a type of passive attack in which node drops some or all of data

packets sent to it for further forwarding even when no congestion occurs. There are two main classes of DoS attacks: bandwidth depletion and resource depletion attacks shown in Figure 2.6.

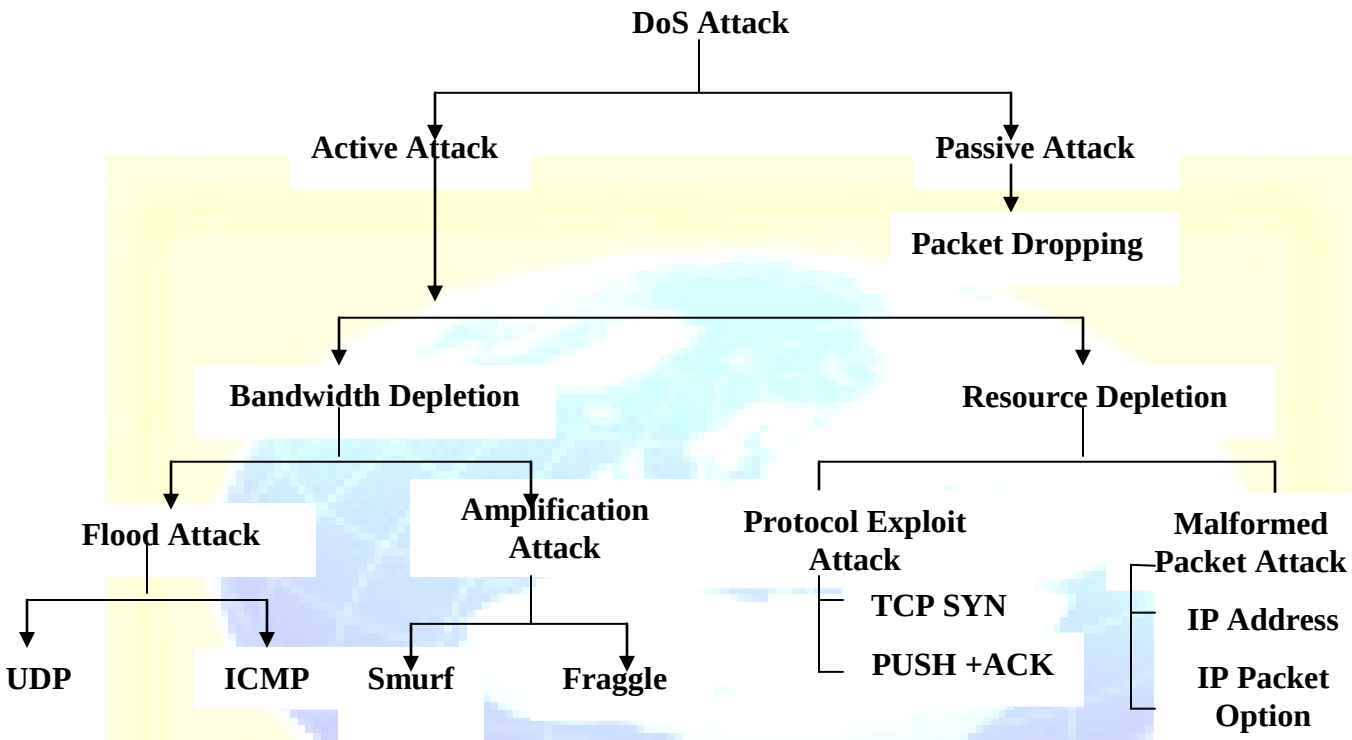

Figure 2.6: DoS Attack Taxonomy.

3. PROPOSED PREVENTION SCHEME

3.1 With Different Number of Attackers

Table 3.1 and Figure 3.1 show the effect of proposed prevention technique on PDR 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 DoS attack with larger extent. By using this technique PDR increases up to 31% as compared to the PDR of existing prevention scheme and 69% as compared to flood attack.

Table 3.2 and Figure 3.2 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 DoS attack with larger extent. By using this technique number of collisions decreases up to 41% as compared to the collisions of existing prevention scheme and 51.5% as compared to flood based DoS attack.

Table 3.1: 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 DoS ATTACK	EXISTING PREVENTION TECHNIQUE	PROPOSED PREVENTION TECHNIQUE
3	.926	.32	.57	.83
4	.926	.31	.55	.82
5	.926	.22	.47	.72
6	.926	.20	.45	.69
7	.926	.175	.44	.58
8	.926	.15	.42	.57
9	.926	.12	.39	.56

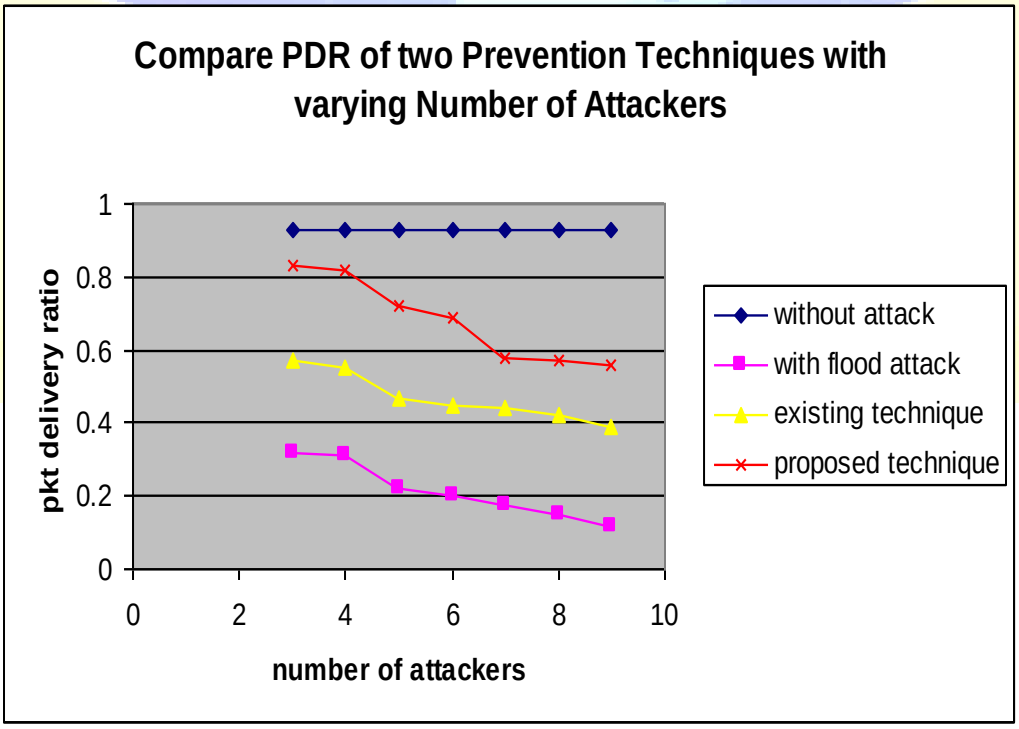

Figure 3.1: Effect of Proposed Prevention Technique on PDR with varying number of attackers.

Table 3.2: 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 DoS ATTACK	EXISTING PREVENTION TECHNIQUE	PROPOSED PREVENTION TECHNIQUE
3	11	8543	7055	3955
4	11	8571	7091	4018
5	11	8685	7175	4175
6	11	8741	7233	4210
7	11	8756	7315	4315
8	11	8897	7400	4400
9	11	8918	7535	4535

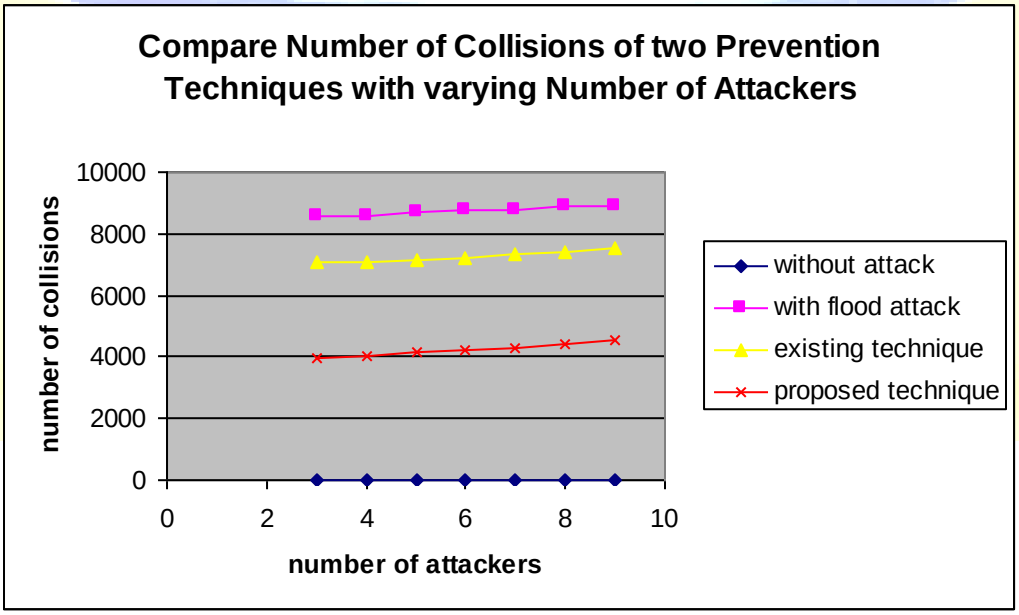

Figure 3.2: Effect of Proposed Prevention Technique on Number of Collisions with varying number of attackers.

Table 3.3 and Figure 3.3 show the effect of proposed prevention technique on Energy Consumption 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 DoS attack with larger extent.

Table 3.4: Effect of Proposed Prevention Technique on Energy Consumption with varying number of attackers.

NUMBER OF ATTACKERS PER NETWORK	ENERGY CONSUMPTION (MWHR)			
	WITHOUT ATTACK	FLOODING BASED DoS ATTACK	EXISTING PREVENTION TECHNIQUE	PROPOSED PREVENTION TECHNIQUE
3	5.010	5.16	5.15	5.080
4	5.010	5.187	5.162	5.090
5	5.010	5.200	5.179	5.114
6	5.010	5.215	5.188	5.119
7	5.010	5.22	5.197	5.139
8	5.010	5.235	5.205	5.146
9	5.010	5.257	5.210	5.180

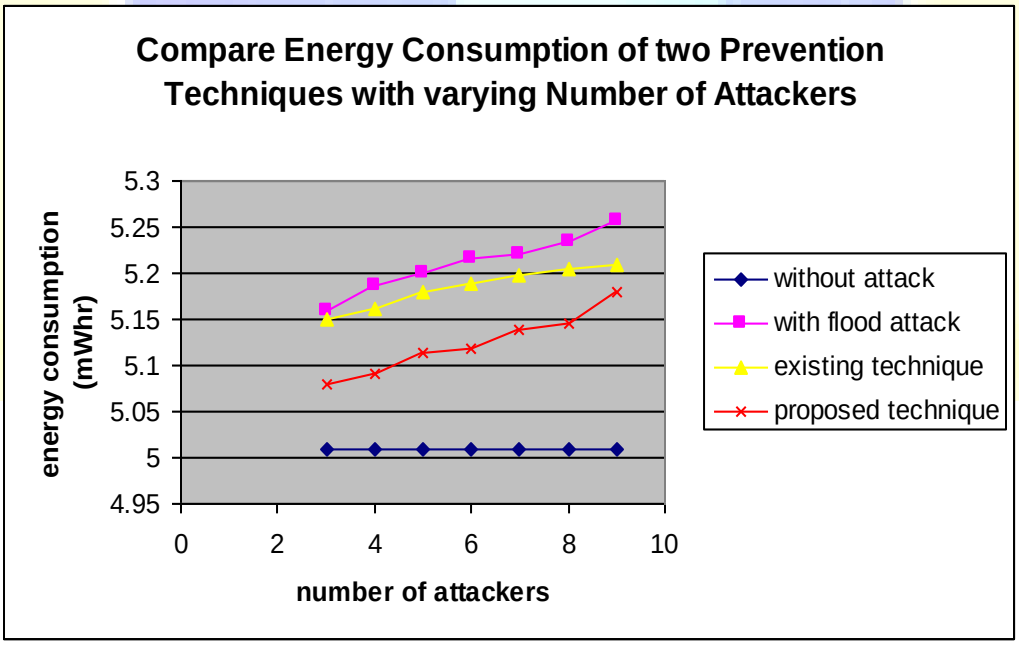

Figure 3.3: Effect of Proposed Prevention Technique on Energy Consumption with varying number of attackers.

3.2 With Varying Node Mobility

Table 3.5 and Figure 3.4 show the effect of proposed prevention technique on PDR with varying node mobility and number of attackers are 8. 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 DoS attack with larger extent. By using this technique PDR increases up to 47% as compared to the PDR of existing prevention scheme.

Table 3.5: Effect of Proposed Prevention Technique on PDR with varying node mobility.

MOBILITY	PACKET DELIVERY RATIO (PDR)			
	WITHOUT ATTACK	FLOODING BASED DoS ATTACK	EXISTING PREVENTION TECHNIQUE	PROPOSED PREVENTION TECHNIQUE
0-5	.926	.15	.42	.57
5-10	.916	.135	.38	.53
10-15	.905	.110	.36	.49
15-20	.898	.083	.24	.47

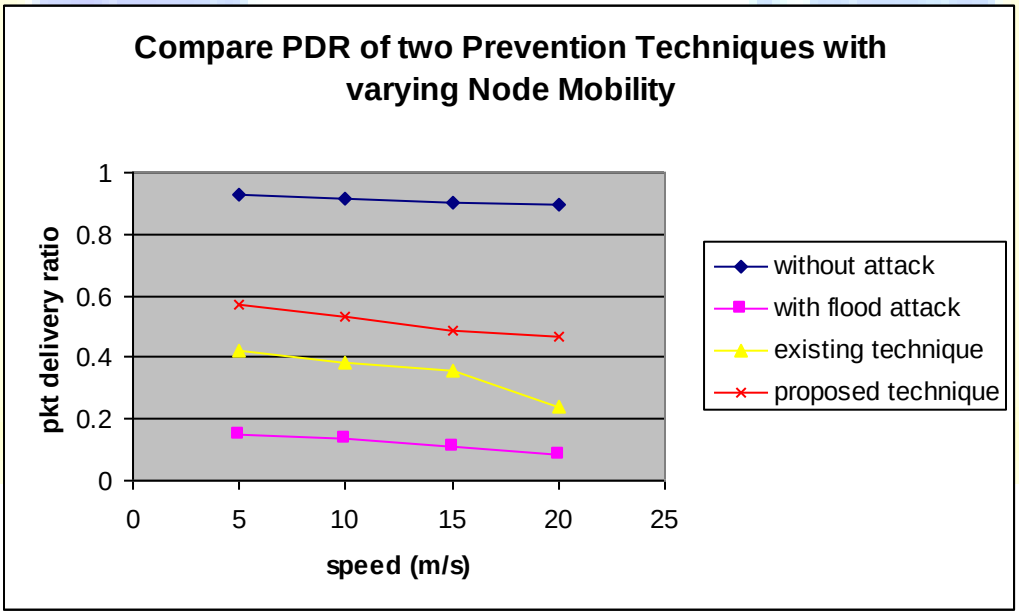

Figure 3.4: Effect of Proposed Prevention Technique on PDR with varying node mobility.

Table 3.6 and Figure 3.5 show the effect of proposed prevention technique on Number of Collisions with varying node mobility and number of attackers are 8. 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 DoS attack with larger extent. By using this technique number of collisions decreases up to 39.5% as compared to collisions of existing prevention scheme.

Table 3.6: Effect of Proposed Prevention Technique on Number of Collisions with varying node mobility.

MOBILITY	NUMBER OF COLLISIONS PER NETWORK			
	WITHOUT ATTACK	FLOODING BASED DoS ATTACK	EXISTING PREVENTION TECHNIQUE	PROPOSED PREVENTION TECHNIQUE
0-5	11	8897	7400	4400
5-10	12	9013	7535	4515
10-15	15	9117	7615	4675
15-20	19	9273	7725	4718

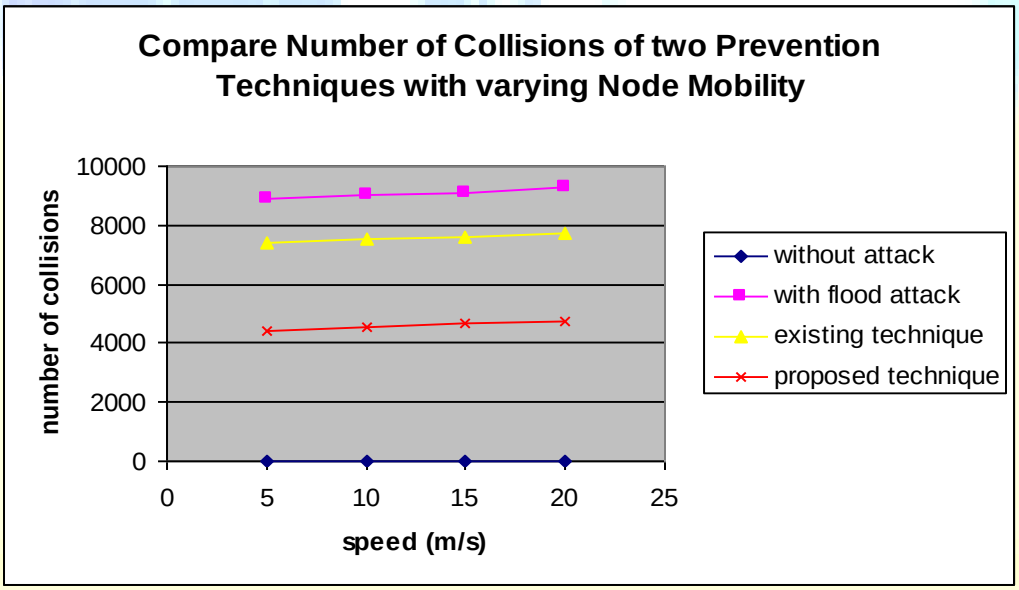

Figure 3.5: Effect of Proposed Prevention Technique on Number of Collisions with varying node mobility.

Table 3.7 and Figure 3.6 show the effect of proposed prevention technique on Energy Consumption with varying node mobility and number of attackers are 8. 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 DoS attack with larger extent.

Table 3.7: Effect of Proposed Prevention Technique on Energy Consumption with varying node mobility.

MOBILITY	ENERGY CONSUMPTION (MWHR)			
	WITHOUT ATTACK	FLOODING BASED DoS ATTACK	EXISTING PREVENTION TECHNIQUE	PROPOSED PREVENTION TECHNIQUE
0-5	5.010	5.230	5.205	5.146
5-10	5.012	5.235	5.210	5.160
10-15	5.019	5.240	5.222	5.170
15-20	5.021	5.250	5.230	5.185

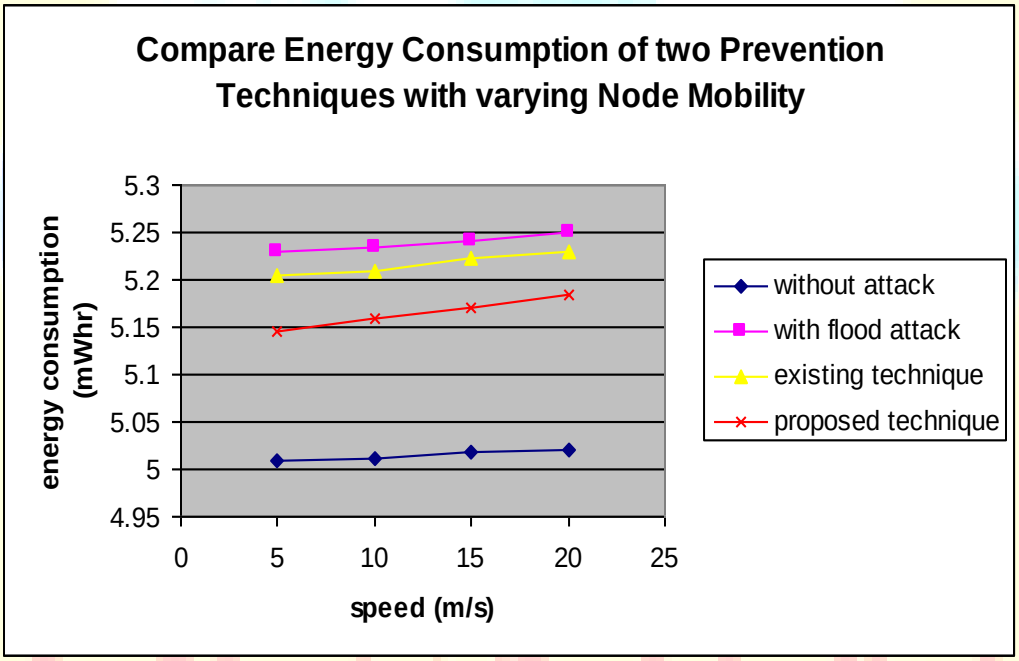

Figure 3.6: Effect of Proposed Prevention Technique on Energy Consumption with varying node mobility.

4. CONCLUSION

Detection & Prevention of DoS attacks is a part of an overall risk management strategy for an organization. Studies and news about real-life DoS 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 DoS attacks should not thus be underestimated, but not overestimated, either.

The main conclusion of this thesis are the following:

- First, we have implemented the DoS 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 DoS attack have greater impact on network performance i.e. network performance decreases more in case of flooding attack as compare to packet dropping based DoS attack their effectiveness has been demonstrated by experiments.

- Detection mechanisms to detect DoS 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 DoS attack are implemented and simulation results shows that proposed prevention technique is better than existing technique. Packet delivery ratio becomes doubles, number of collisions and energy consumption decreases or becomes half by using proposed prevention technique under different number of attackers and different node mobility. Effectiveness of proposed prevention scheme has been demonstrated by tables and figures.

REFERENCES:-

[1] Han L; Mobile Ad hoc Network; October 8, 2004.

[2] Stephen M. Specht and Ruby B. Lee; 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] A. Sun; The design and implementation of fisheye routing protocol for mobile ad hoc networks; M.S. Thesis, Department of Electrical and Computer Science, MIT; May 2002.

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

[5] Federal Computer Incident Response Center (FedCIRC); Defense Tactics for Denial of Service Attacks; Washington, DC; 2000.

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

[7] J. MÄolsÄa; Mitigating denial of service attacks in computer networks; PhD thesis; Helsinki University of Technology, Espoo, Finland; June 2006.

[8] V. Paxson; An analysis of using reflectors for distributed denial-of-service attacks; ACM SIGCOMM Computer Communication Review, vol. 31, no. 3; July 2001.

[9] Yonghua You; A defense framework for flooding-based DoS attacks; Master of Sc. Thesis; Queen's University Kingston, Ontario, Canada; August 2007.