DOS Attack Mitigation In MANET

[1]Er. Inakshi Garg, [2]Er. Meenakshi Sharma
[1]M. Tech, CSE, [2]HOD, CSE dept.
[1,2] Kurukshetra University, India

***Abstract* - Mobile Ad hoc Network is one of the kind of wireless networks which utilizes multi-hop radio relaying and it has no infrastructure Network because of its capability of operating without any support of fixed infrastructure or without any centralized administration. MANET has no clear line to prevent so both legitimate network users and malicious attackers can access it. There are major challenges in MANET in case of malicious nodes, it is to designs the robust security solution which helps to prevent MANET from various DDOS attacks. Security plays a vital role in mobile ad hoc network (MANET) because of its applications like disaster-recovery or battlefield networks. MANETs are more vulnerable as compared to wired networks because lacking of a trusted centralized authority and limited resources. The main objective of this is comparative study of various kinds of DDOS attacks and various detection methods as well as defense mechanisms like Disable IP broadcast detection technique, profile based detection and prevention of DOS attack using target customer behavior and existing solutions to protect MANET protocols. With the help of these techniques no of collisions and packet delivery ratio is also evaluated by comparing two prevention techniques existing prevention technique and proposed prevention technique. The proposed technique increases PDR (packet delivery ratio) and reduces number of collisions.**

***Keywords* - MANET, DOS attack, Malicious code, DSDV, Security, Defense Methods, PDR, No of collisions**

I. INTRODUCTION

1.1 MANET

MANET (Mobile Ad Hoc Network). MANETS are just a mobile, they also use wireless connections to make a connection with various types of connections. This can be also a standard Wi-Fi connection, or another medium, like cellular or satellite transmission. Some MANETs are prohibited to a local area of wireless devices (such as a group of laptop computers) For example, A VANET (Vehicular Ad Hoc Network), is one of a type of MANET which allows vehicles to communicate with roadside equipment. Basically vehicles cannot have direct connection, the wireless roadside equipment may be connected to the Internet, which helps to allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to countermeasure the traffic conditions. Due to the dynamic nature of MANETs, they are typically not very secure, so it is important to be aware what data is sent over a MANET.

1.3 DOS and DDOS Attack in MANET

Denial of Service (DoS) attack uses one computer to flooding a server with packets. The goal of this attack is to flood the bandwidth of server and other resources. A distributed denial of service attack is a strict form of DOS which uses multiple machines to prevent the legal use of a service. It is a type of active attack and very powerful technique to attack resources of internet. It adds to the many-to-one dimension to the DoS problem. To make a prevention and mitigation schemes for them are more complicated. But its impact is proportionally strict. DDoS is composed as shown in figure. First attacker made a network of malicious nodes which initiates the attack. The malicious nodes called zombies are then installed with attack tools, which allows them to carry out attacks under the control of the attacker. The zombies are classified into masters and slaves. The attacker motivates the masters to start the attack, the masters then motivate the slaves. The slaves flood the victim.

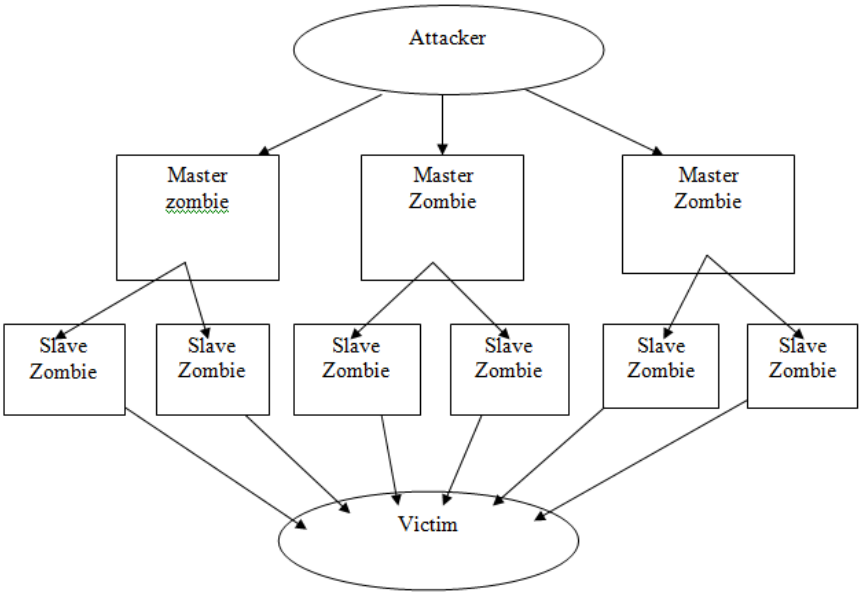


Fig 1.1 Block diagram of DDOS Attack

1.4 DSDV Protocol

It stands for Distance Sequenced Distance Vector Routing Protocol. It is also known also as Distributed Bellman-Ford or Routing Information Protocol (RIP)
In every node maintains a routing table

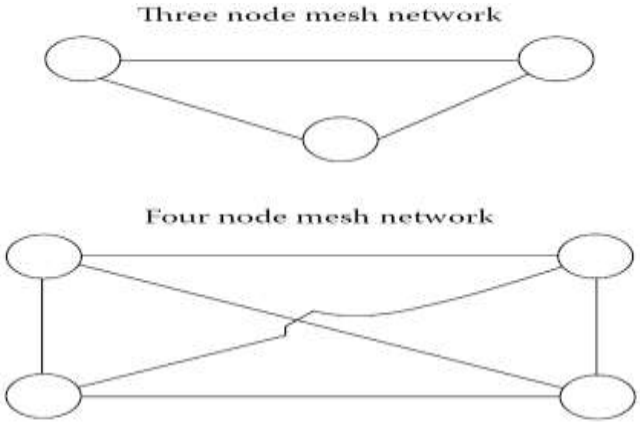
1. Maintains all available destinations
2. Maintains the next node to reach to destination
3. Maintains the number of hops to reach the destination
4. Maintains Periodically send table to all of its neighbors to maintain topology

Distance vector is not suited for ad-hoc networks in concept of loops. So new solution is **DSDV protocol.**

1.5 Mesh Networks and Wireless mesh networks

A mesh network is a type of network topology in which each node relays data for the network. All mesh nodes cooperate in a distribution of data in a network. Mesh networks can relay messages using either a routing technique or a flooding technique. With routing, the message propagates along a path by hopping from node to node until it reaches to its destination. To ensure all its path availability, the network should allow to continuous connections and must reconfigure itself a broken paths, using self-healing algorithms such as Shortest Path Bridging. In mesh networks, each and every node is connected to each and every node and it is also known as fully connected networks Fully connected wired networks or mesh networks have the advantages of security and reliability. However, in such networks, the number of cables, and therefore the cost increases rapidly as the node increases. Mesh networks can be considered a type of an ad-hoc network. Thus, mesh networks are very closely related to mobile ad hoc networks (MANETs).A mesh network allows every node can directly communicate with every other node, it has physical constraints which limits the number of nodes. Now a day's Wireless networks are becoming a part of our everyday life, as witnessed by several features: the number of mobile phone subscriptions reached 7.3 billion in 2014, short-range radio technologies such as Blue-tooth and WI-FI are widespread as well as radio frequency. WMN architecture defines 3 types of WMNs which are:

1. Infrastructure WMN 2. Client WMN 3. Hybrid WMN



II. RELATED STUDY

Lovely (2015) proposed that Mobile Ad-hoc network is a network which consists of wireless nodes. It has basically no proper management i.e. the connections are made without any centralized administration. A mobile ad hoc network (MANET) is a network that can be made with no fixed infrastructure. DOS attack aims to overload the server's bandwidth and other resources. A DDoS attack is a strict form of DOS which uses multiple machines to prevent the legal use of a service. A bandwidth reduction and resource reduction attacks are designed to flood the network with unwished traffic that prevents legal traffic from reaching the victim system. The aim is to prevent from existing attack and defense mechanisms.

RANJU (2015) author proposed that the Distributed Denial of Service (DDoS) attacks in the networks needs to be prevented or handled if it occurs, as soon as possible and before reaching the victim. Trading with DDoS attacks is difficult due to their properties such as variation attack rates, big scale of botnet, different types of goals, etc. Distributed Denial of Service (DDoS) attack is difficult to deal with because it is hard to difference legal traffic from malicious traffic, especially when the traffic is coming at a various rate from disseminated sources. DDoS attack becomes hard to handle if it occurs in wireless network due to the properties of adhoc network as low battery life, dynamic topologies, frequency of multicast routing or mobile agent based routing, network overhead, scalability etc. It is better to keep prevent distributed DOS attack rather than allowing it to occur and then taking the strictly steps to tackle it. In this paper a novel solution is proposed to tackle DDoS attacks in mobile ad hoc networks (MANETs).

A.Anna lakshmi et. al. (2012) proposed that Mobile Ad hoc Network is the type of wireless networks which utilizes multi-hop radio relaying and has no infrastructure due to its capability of operating without the support of any fixed infrastructure. Security plays a vital role MANET (mobile ad-hoc networks) because of its applications like battlefield or disaster-recovery networks. Current wireless research points out that the wireless MANET has more security problems than wireless networks and traditional wired. MANET is strictly affected by Distributed Denial of Service (DDoS) attacks which is becoming a problem for users of computer systems which are connected to the Internet. MANETs are more vulnerable compared to wired networks due to lack of a trusted centralized authority and limited resources. This paper discusses different attacks on MANET and protective mechanisms for DDOS attacks in MANET as reported in the literature.

Wei Ren et. al. (2007) focused on the reduction of Quality and response mechanisms. The response scheme which is based on the ECN marking mechanism. Through ns2 network simulations, Demonstration of the existence high good output and delay jitters under the pulsing attack mode. Increases in delay (by 110 times under five attacking flows) and decreases in goodput (77% under five attacking flows) can be observed specially when more attacking flows occurs. Moreover, the author shows through simulations that has similar behaviors which can also be observed for TCP flows as well as networks of other types of topology.

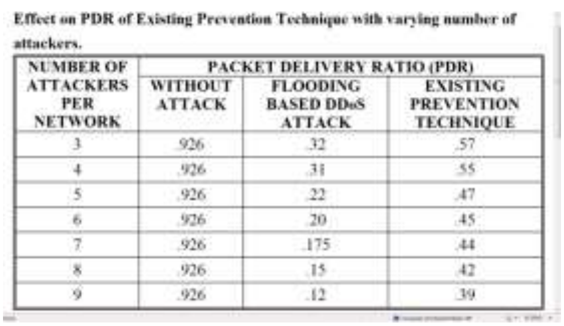
III. PROPOSED WORK

In our proposed work, we have used the two parameters which is packet delivery ratio, number of collisions to mitigate DOS and DDOS attacks. The proposed work increase packet delivery ratio and reduces number of collisions. The proposed technique prevents from flooding based attacks by disabling the IP and blacklisting particular attacker node. The GLOMOSIM (global mobile information simulator) tool is used to simulate result and implemented proposed technique.

IV. RESULTS AND DISCUSSION

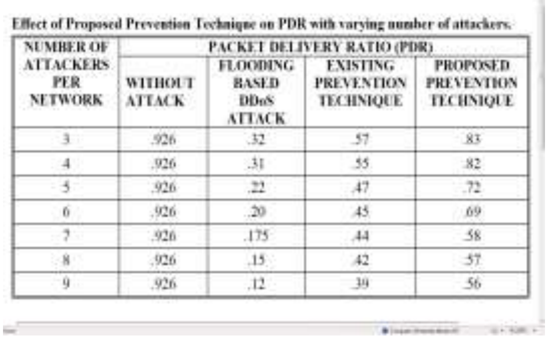
The result is implemented in GLOMOSIM tool. We get the result after simulation takes place. In this result we have compared Existing prevention technique and proposed prevention technique to prevent from flooding based DOS and DDOS attacks. Proposed technique uses 2 parameters which are PDR and no of collisions.

Comparison Table between Existing PDR and Proposed PDR: Proposed PDR is more than existing PDR.



Effect on PDR of Existing Prevention Technique with varying number of attackers.

NUMBER OF ATTACKERS PER NETWORK	PACKET DELIVERY RATIO (PDR)		
	WITHOUT ATTACK	FLOODING BASED DDoS ATTACK	EXISTING PREVENTION TECHNIQUE
3	.926	.32	.57
4	.926	.31	.55
5	.926	.22	.47
6	.926	.20	.45
7	.926	.175	.44
8	.926	.15	.42
9	.926	.12	.39

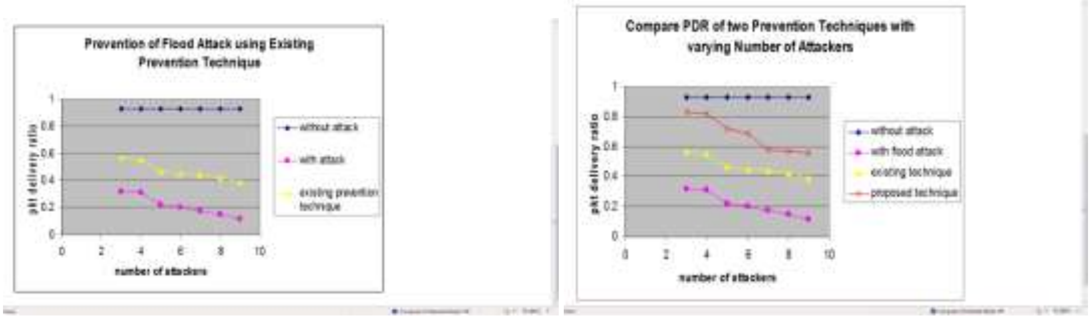


Effect of Proposed Prevention Technique on PDR with varying number of attackers.

NUMBER OF ATTACKERS PER NETWORK	PACKET DELIVERY RATIO (PDR)			
	WITHOUT ATTACK	FLOODING BASED DDoS ATTACK	EXISTING PREVENTION TECHNIQUE	PROPOSED PREVENTION TECHNIQUE
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

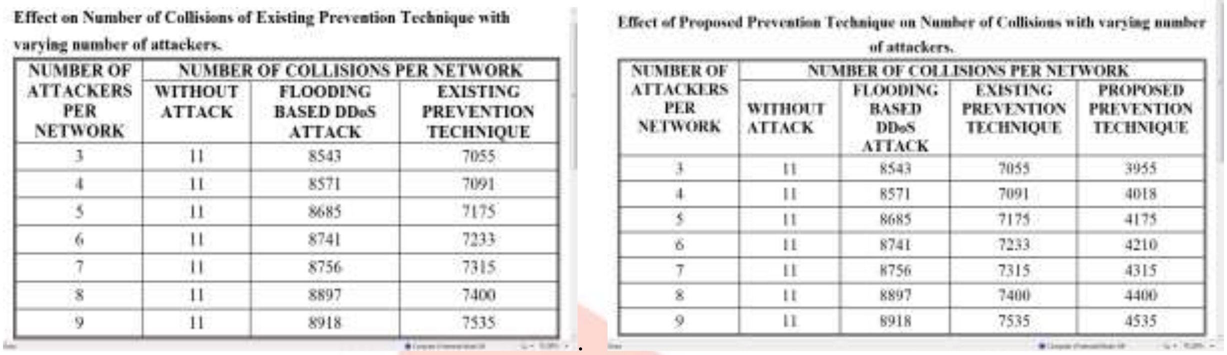
(Table 4.1- Comparison between Existing PDR & Proposed PDR)

The bar graph among Existing PDR and proposed PDR has been shown as under:



(Figure 4.1- Comparison Graph Existing PDR & Proposed PDR)

Comparison Table between Existing no. of collisions and Proposed no. of collisions: Proposed no of collisions are less than existing no. of collisions.



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

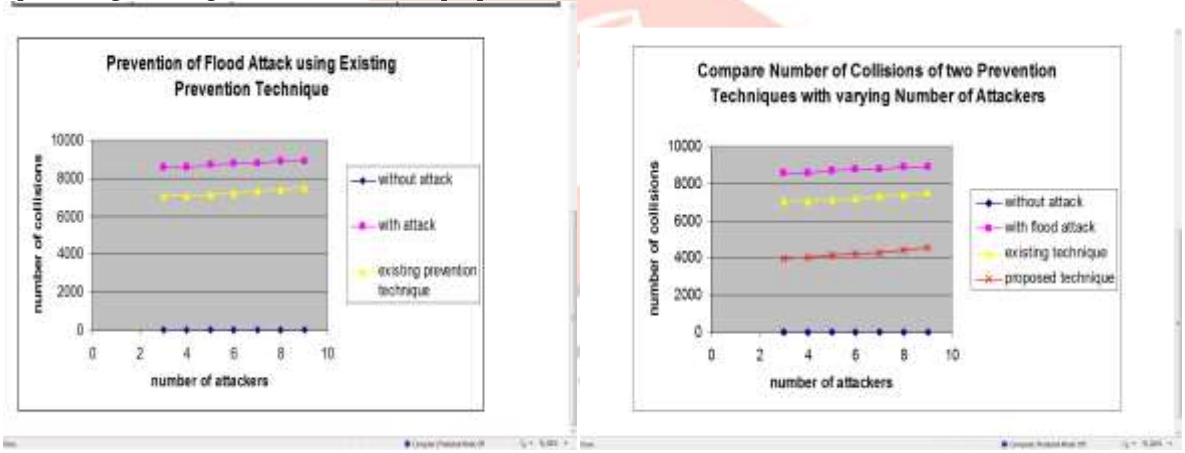
NUMBER OF ATTACKERS PER NETWORK	NUMBER OF COLLISIONS PER NETWORK		
	WITHOUT ATTACK	FLOODING BASED DDoS ATTACK	EXISTING PREVENTION TECHNIQUE
3	11	8543	7055
4	11	8571	7091
5	11	8685	7175
6	11	8741	7233
7	11	8756	7315
8	11	8897	7400
9	11	8918	7535

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
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

(Table 4.2- Comparison between Existing collisions & Proposed collisions)

The bar graph among Existing no of collisions and proposed no of collisions has been shown as under:



(Figure 4.1- Comparison Graph Existing PDR & Proposed PDR)

V. CONCLUSIONS

Security is the one of the most important feature for deployment in mobile Ad-hoc network. Distributed Denial of Service attacks are more complex and major problem, and as a result, various approaches have been proposed to counter them. The proposed mechanism nullifies the DDOS attack in MANET. In proposed work, two parameters are pdr and no of collisions are evaluated by varying no of attackers. It increases packet delivery ratio and reduces number of collisions. The results demonstrate that the presence of a DDOS doesn't affect the delivery of the packets in the network considerably. The suggested mechanism protects the network. The proposed structure is also applied for securing the network from attacks by disabling the IP to prevent from flooding and blacklisting that particular nodes which causes flood to the network.

REFRENCES

[1] Amrit Lal Sangal, Ramanpreet Kaur, krishan kumar," Modeling and Simulation of DDoS Attack using Omnet++" , IEEE (SPIN) 2014.

[2] RANJU "A Novel Solution to Nullify DDOS Attack in MANET"INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY Vol. 2, Issue VI, June, 2014.

[3] LOVELY " A Review of DoS Attack and Defence Scheme in Manet" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 4, April 2015.

[4] A.Anna lakshmi and Dr.K.R.Valluvan " A Survey of Algorithms for Defending MANETs against the DDoS Attacks" International Journal of Advanced Research in
Computer Science and Software Engineering Volume 2, Issue 9, September 2012.

[5] Wei Ren and Dit-Yan Yeung "Pulsing RoQ DDoS Attack and Defense Scheme
in Mobile Ad Hoc Networks" International Journal of Network Security, Vol.4, No.2, PP.227-234, Mar. 2007.

[6]Saurabh Ratnaparikhi , Anup Bhange " DDOS Attacks on Network; Anomaly Detection using Statistical Algorithm" Volume 2, Issue 12, December 2012.

[7] K.Kuppusamy and S.Malathi " Prevention of Attacks under DDoS Using Target
Customer Behavior" Vol. 9, Issue 5, No 2, September 2012.

[8] S.A.Arunmozhi "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.