International Journal of Multidisciplinary Research and Development

IJMRD 2015; 2(2): 384-392
www.allsubjectjournal.com
Impact factor: 3.672
Received: 03-02-2015
Accepted: 18-02-2015
E-ISSN: 2349-4182
P-ISSN: 2349-5979

Anuj Jain
Research Scholar,
Mewar University, Rajasthan, India

Dr Y.K. Jain
Professor, Mewar University, Rajasthan, India

Correspondence:
Anuj Jain
Research Scholar,
Mewar University, Rajasthan, India

Reduce flooding based DDoS attack and improve network performance parameters by using NS-2 Simulator

Anuj Jain, Dr Y.K. Jain

Abstract
Network security is a weak link in wired and wireless network systems. Malicious attacks have caused tremendous loss by impairing the functionalities of the computer networks. Denial of Service (DoS) and Distributed DoS (DDoS) attacks are two of the most harmful threats to the network functionality. Mobile Ad Hoc Networks (MANET) are even more vulnerable to such attacks. Denial of Service (DoS) is the degradation or prevention of legitimate use of network resources. In this paper we analyse the flooding attacks in mobile ad hoc networks that support anonymous communication. Then we propose a novel technique to deal with the flooding attacks. Our approach can efficiently identify and isolate the malicious node that floods the network. In addition, our technique provides a mechanism to identify detection of malicious node and its numbers. In our simulation, we have taken the following parameters and analyzed the results using Energy consumption, routing overhead, packet delivery ratio and detection rate.

Keywords: Flooding Attacks.ns-2, DDoS Attacks

1. Introduction
A MANET is an autonomous system of mobile nodes. The network may operate in isolation, or may interface with a fixed network. The nodes are equipped with wireless transmitters/receivers using antennas which may be omnidirectional (broadcast), highly-directional (point-to-point), or some combination thereof. They dynamically self-organize in arbitrary and temporary network topologies, meaning that their elements may independently or in groups form ad hoc networks, leave them, smaller networks may merge into larger and vice versa. These networks promise more commercial prospective and advantage due to their flexibility. Nevertheless, security in ad hoc networks rests heavily on the existence of secure communication. Given the fact that the environment is not conducive to centralized trusted authority, an array of significant secure routing approaches have been proposed to achieve secure communication. Although the proposals attain secure routing despite few fundamental challenges, they only target to secure functional ad hoc networks. For this reason, flooding and packet drop attacks that the availability of the network services can override the secure routing approaches. Here, we are discussing Flooding based types of DDoS attacks.

1.1. Security Issues in Manet
Security in Mobile Ad-Hoc Network (MANET) is the most critical sympathy toward the essential usefulness of system. Accessibility of system administrations, secrecy and trustworthiness of the information can be accomplished by guaranteeing that security issues have been met.

a) **Lack of centralized monitoring**: The centralized infrastructure is absent which disallows any monitoring mechanism in the network. This makes the traditional security solutions dependent on certification authorities and on-line servers inapplicable. The trust relationships among individual nodes changes particularly when some nodes are found to be compromised. Hence, security mechanisms need to be on the dynamic and not static.
b) **Cooperative algorithms:** MANET routing algorithms require mutual trust between neighbouring nodes.

c) **The absence of a certification authority.**

d) **The limited physical protection of each of the nodes:** network nodes usually do not reside in physically protected places, such as locked rooms. Hence, they can more easily vulnerable and fall under the control of an attacker.

e) **The intermittent nature of connectivity**

f) **The vulnerability of the links:** Messages can be eavesdropped and fake messages can be injected into the network without the difficulty of having physical access to the network components. Eavesdropping might give an attacker access to secret information thus violating confidentiality.

g) **Adversary inside the Network**: The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. These nodes are called compromised nodes.Ad-hoc network mobility makes it easier for a compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity. This is hard to detect that the behaviour of the node is malicious. Thus this attack is more dangerous than the external attack.

1.2. DDoS Attack

A DDoS (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. This kills the victim network of resources such as band- width, computing power, etc. The victim becomes unable to provide services to its legitimate clients and network performance is greatly affected. In brief, as the name suggests, the service to a legitimate user is being denied of the service by a malicious users by sending a large number of unwanted packets on a network or a single computer.

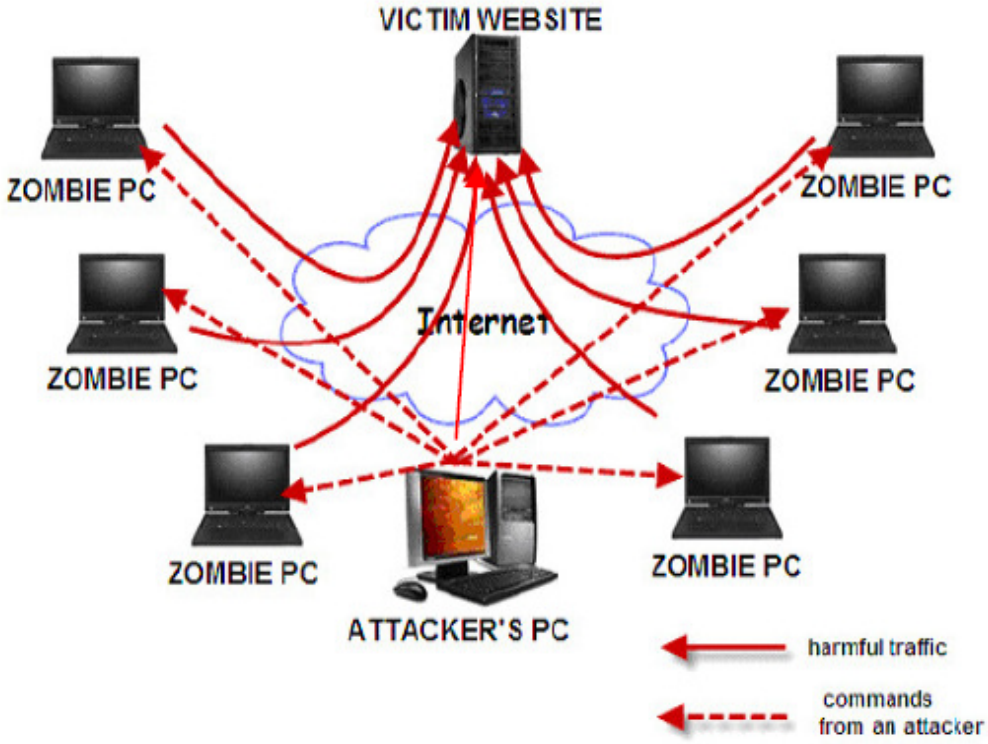


Fig 1: DDoS Attack

1.3. Flooding Attack

The Flooding attack [1] is launched at the network layer by the malicious node. It sends massive amount of control packets to the network. This attack aims at depleting the network resources like bandwidth, battery power and thereby preventing the network from providing services to legitimate users. The flooding attack can target the victim node or the network as a whole. In case of RREQ flooding attack the malicious node imitates like normal node in all aspects, except in performing unnecessary route discoveries. These malicious nodes frequently initiate route discovery to destinations with the intent to flood the network with route request packets. As it is difficult to distinguish between a route discovery initiated with a malicious intent and a legitimate route discovery for repairing broken/stale routes, this type of attack is hard to detect.

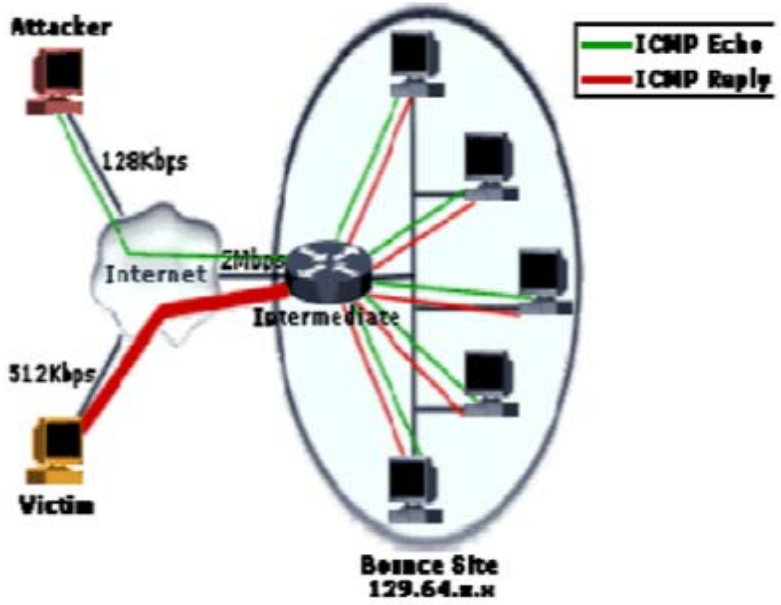


Fig 2: Flooding Attack

2. Related Work

2.1. Rate Limit Based Approach

The rate limit based [4] approach aims at detecting the route request flooding attack based on certain threshold. Every node in the network is set to adhere to the threshold limit on sending RREQ packets. However it does not hold good for dynamic environment like MANET. The static threshold values are not sufficient enough to detect the attacker.

2.2. Trust and Reputation Based Approach

Trust [5] and reputation [6] based schemes are used for identifying the attacker inside the network. Here the genuine nodes which turn to be malicious nodes are considered as inside attacker. The trust and reputation value is set as high and low based on how they co-operatively participate in the network. Here the false positive rate is high as genuine nodes can also have their value estimated as low on certain scenarios.

2.3. Behavior Based Approach

The behavior based detection [7] defines a profile for the normal behavior of nodes. Any deviation from the normal profile is considered to be malicious attempt. However the profile is collected one time from the training data and is highly static which does not hold good for dynamic scenarios.

2.4. Trace Back Scheme

In Trace back Mechanism [8] each packet is traced to its source with help of special devices monitoring the network. When these special devices are levied on nodes in the network, the nodes resource consumption will be more. Further centralized equipment is not feasible in the network.

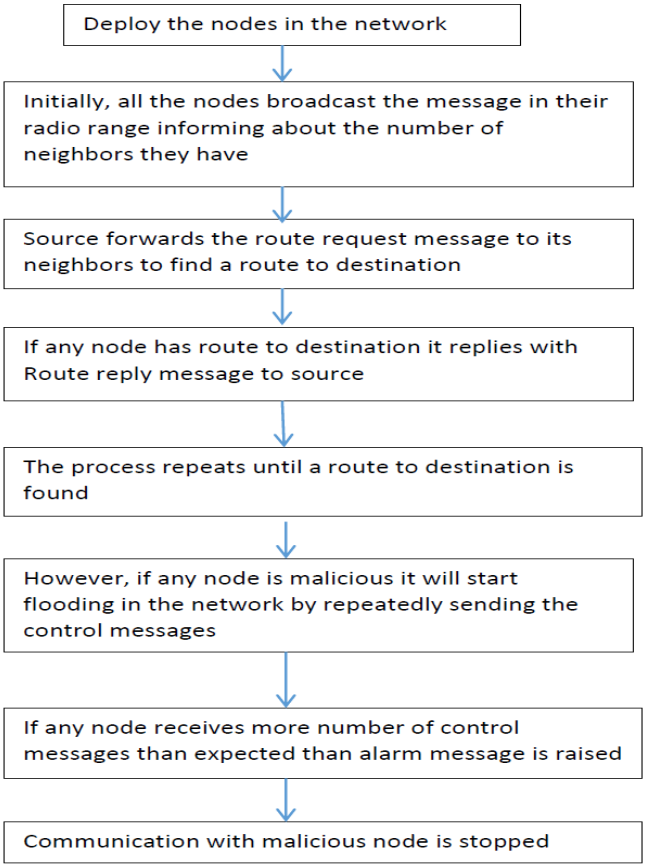
2.5. Preceptor Based Approach

The preceptor model [9] is entirely based on training data collected from past experiences. This model can be applied for only linearly separable data points. The attack instances and the normal instances are linearly separable in the space of detection metrics. This model is effective only when high attack rate is present as the data's can be easily separable in detection metrics and hence easily classified in the perception model.

3. Implementation Detection and Prevention Technique for Flooding Based DDos Attacks Mechanisms.

A malicious node is the one which have intention of getting access to the useful information in the network and not letting the packets reaching the desired user. The malicious node causes packet drop in the network and it consumes up the resources of the network. In denial of service attack, the malicious nodes sometimes consume whole bandwidth of the channel. This deprives the other nodes to use the channel resulting in long delay and sometimes breakage of communication in the network. These malicious nodes may work as a group and commonly referred to as distributed denial of service attack. In our study our focus is the denial of service attacks which is caused due to flooding in the network. In the flooding attack, the malicious node floods the request messages in the network during the route formation phase when source node sends the route request messages in the network to form a route to the destination. Here we intend to use the fact that normally a node forwards the route request messages to its neighbor node. The number of route request messages sent is equal to or less than the number of neighbors which are in the range of the node. But in case of the attacker node, it will send more number of route request messages in the network than the number of neighbors it has in order to do the flooding attack. So for the attacker node, the number of request messages sent will always be higher than then number of neighbors it has. This will be deciding factor to detect the malicious node in the network.

3.1. Detection and Prevention Algorithm



3.1.1. Detection Mechanisms

Table 1. Detection Flooding Attack

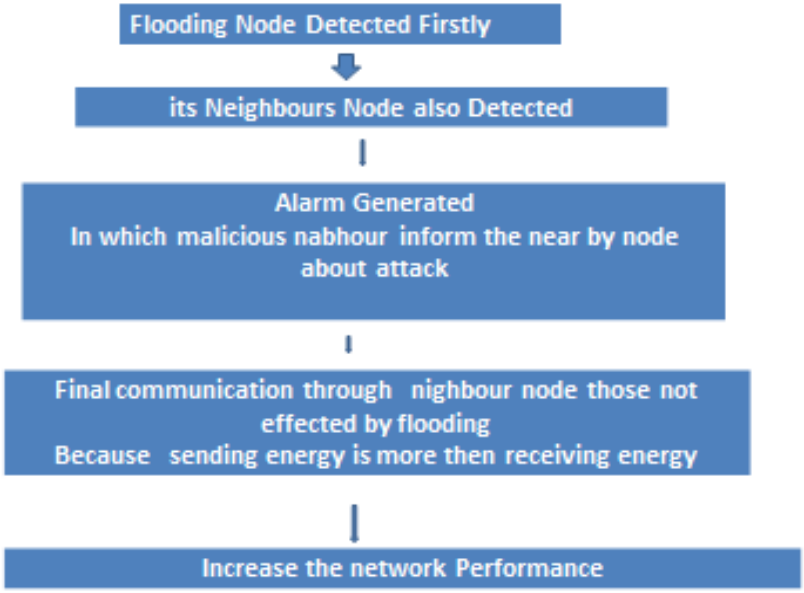
`+ -t 1.700000000 -s 0 -d -1 -p cbr -e 110 -c 2 -a 0 -i 0 -k AGT`
`- -t 1.700000000 -s 0 -d -1 -p cbr -e 110 -c 2 -a 0 -i 0 -k AGT`
`h -t 1.700000000 -s 0 -d -1 -p cbr -e 110 -c 2 -a 0 -i 0 -k AGT`
`+ -t 1.700000000 -s 0 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k RTR`
`- -t 1.700000000 -s 0 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k RTR`
`h -t 1.700000000 -s 0 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k RTR`
`r -t 1.701408322 -s 1 -d -1 -p AODV -e 48 -c 2 -a 0 -i 0 -k RTR`
	This procedure is develop after design communication link betn nodes,we are manly concern about CBR & AGT file only other file develop by network routing

`if(tim[x]>=20 && tim[x]<=30)`
`{`
`if(status[x]=="+" && atyp[x]=="AGT" && ptyp[x]=="cbr")`
`{`
`a[q]=src[x]`
`pack[q]=pid[x]`
`print a[q]" "pack[q] > "chk"`
	This is normal pattern that is develop in 20 to 30 sec. in this we found Communication pkt. From one node to its neighbour node

`if(tim[x]>=36 && tim[x]<=42)`
`{`
`if(status[x]=="+" && atyp[x]=="AGT" && ptyp[x]=="cbr")`
`{`
`a_atk[q]=src[x]`
`pack_atk[q]=pid[x]`
`print a_atk[q]" "pack_atk[q] > "chk_atk"`
	This is attack pattern develop in 36 to 42 sec in which source no.(attackers) and its node id print in another file

`if (a_atk[x]>a_atk[y])`
`{`
`temp=a_atk[x]`
`a_atk[x]=a_atk[y]`
`a_atk[y]=temp`
 	
`temp1=pack_atk[x]`
`pack_atk[x]=pack_atk[y]`
`pack_atk[y]=temp1`
	Prog .arrange these above node in proper sequence , so that finally we found how many node are malicious node and how many flooding pkt deploy

3.1.2. Prevention Mechanisms



4. Results and Discussion

In distributed denial of service attacks, the malicious node starts flooding the network with the request packets. This consumes up the resource of the network. In our simulation, we have taken the following parameters and analyzed the results using Energy consumption, routing overhead, packet delivery ratio and detection rate.

4.1. Simulation parameters

Table 2. Simulaton Parameters

Simulator	NS2.35
Channel	Wireless Channel
Propagation Model	Two Ray Ground
Queue	Drop Tail
Antenna	Omni-Directional
Number of nodes	50
Routing Protocol	AODV
Simulation Area	1300*1300
Energy Model	Radio Dissipation Energy Model
Initial Energy	100 J
Mobility Model	Random Way Point

4.2. Energy consumption

In order to check the performance of the network, energy consumption that is being done in the network must be analyzed. The energy model that has been used in our work is radio dissipation energy model which is inbuilt in NS2.35. Initially every mobile node was provided with 100 joules of energy. Since, the malicious node floods a lot of request messages in the network, this leads to decrease the average energy of the network. At the end of simulation the remaining energy was approx. 80 joules showing a consumption of 20 joules.

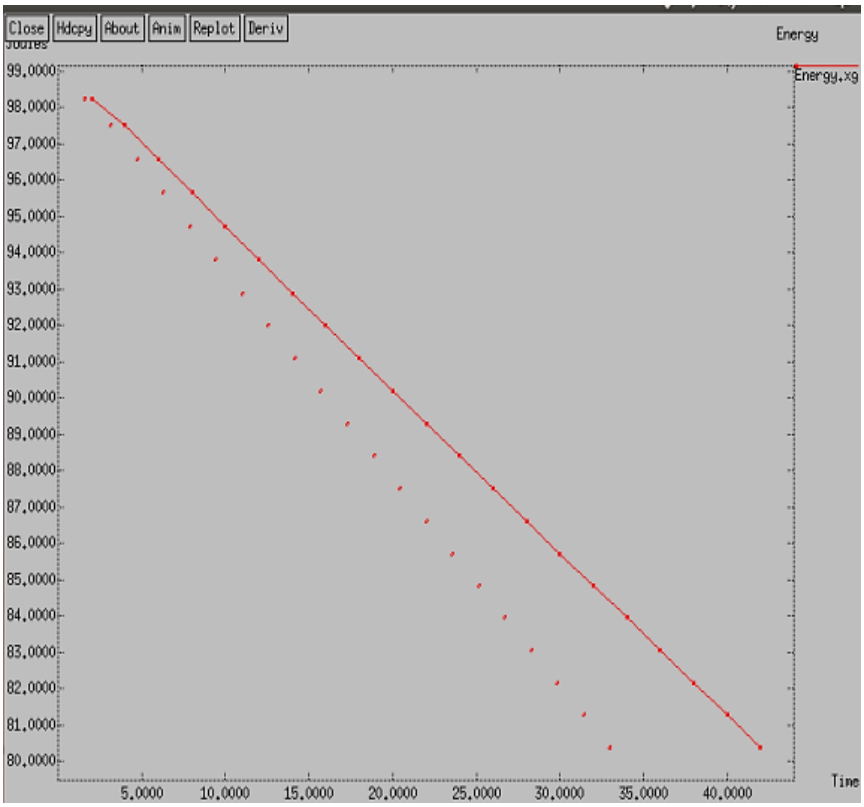


Fig 3: Energy Consumption

4.2. Malicious node detection rate

In case of the network security, the main focus is always on the detection of malicious nodes present in the network which hampers the performance of the network. Detection rate reflects on the efficiency of our proposed work, it is how many number of attackers have been successfully detected. The more the detection rate, the better is the scheme that has been used to increase the network security.

Our proposed scheme shows the detection rate of 90 percent.

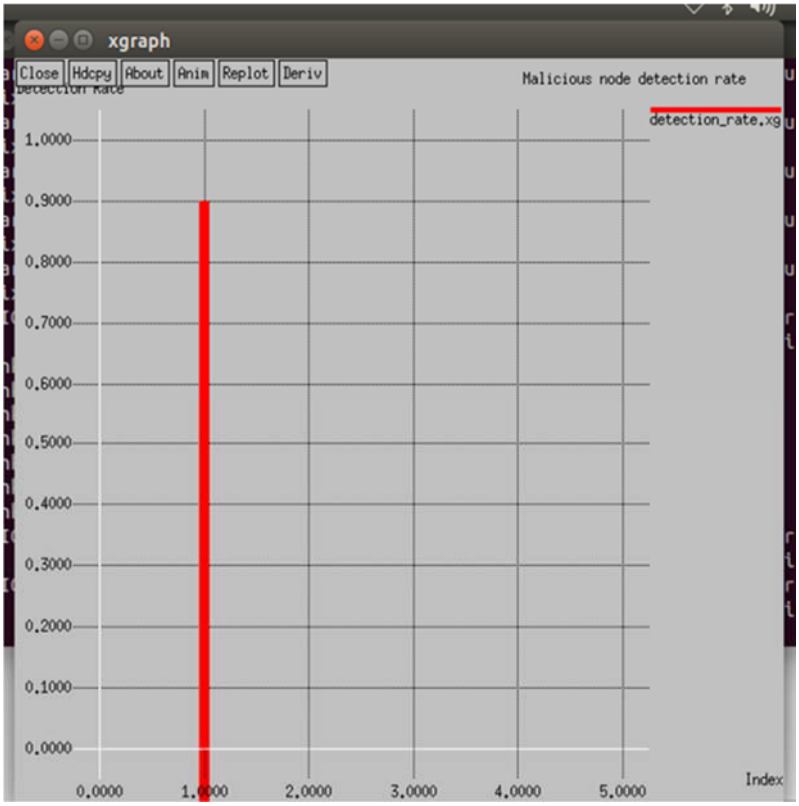


Fig 4: Detection Rate

4.3. Overhead

The excessive value of this parameter indicates the how many control packets are being routed in the network. In our simulation, during the normal network performance, the routing overhead was recorded to be at 120 but during the flooding of the control packets by the malicious attackers, the routing overhead jumped at approx 200. This abrupt increment in the value of routing overhead indicates the network is getting flooded with more number of control packets.

ov_final=pks_sent_final(RTR)/pks_rec_final(AGT)

Table: Overhead

Without Attacks	Flooding Attacks	After Prevention
120	**280**	**150**

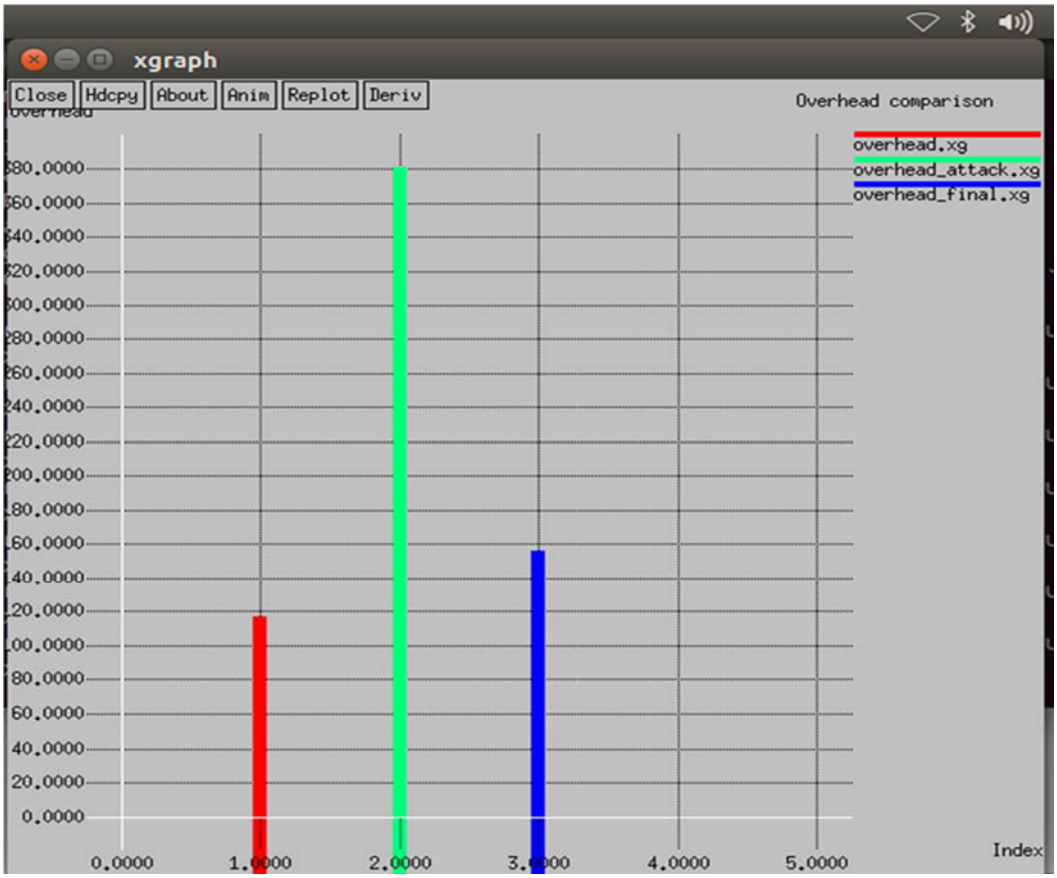


Fig 5: Routing Overhead

4.4. Packet Delivery Ratio

It is ratio of number of packets received by the destination node to the number sent by the source node. In our simulation, during the normal communication when the attackers were not present the number of packets that were being sent by the source node were being successfully delivered at the destination node, hence the value of PDR at 1. As soon as the network was attacked, the value of packet delivery ratio was dropped to almost 0.

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

Table 2. Packet Delivery Ratio

Time	PDR
45	0.232142857
46	1
47	0.97222225
48	0.833333333
49	0.985555557
50	1
51	0.953333322
52	1

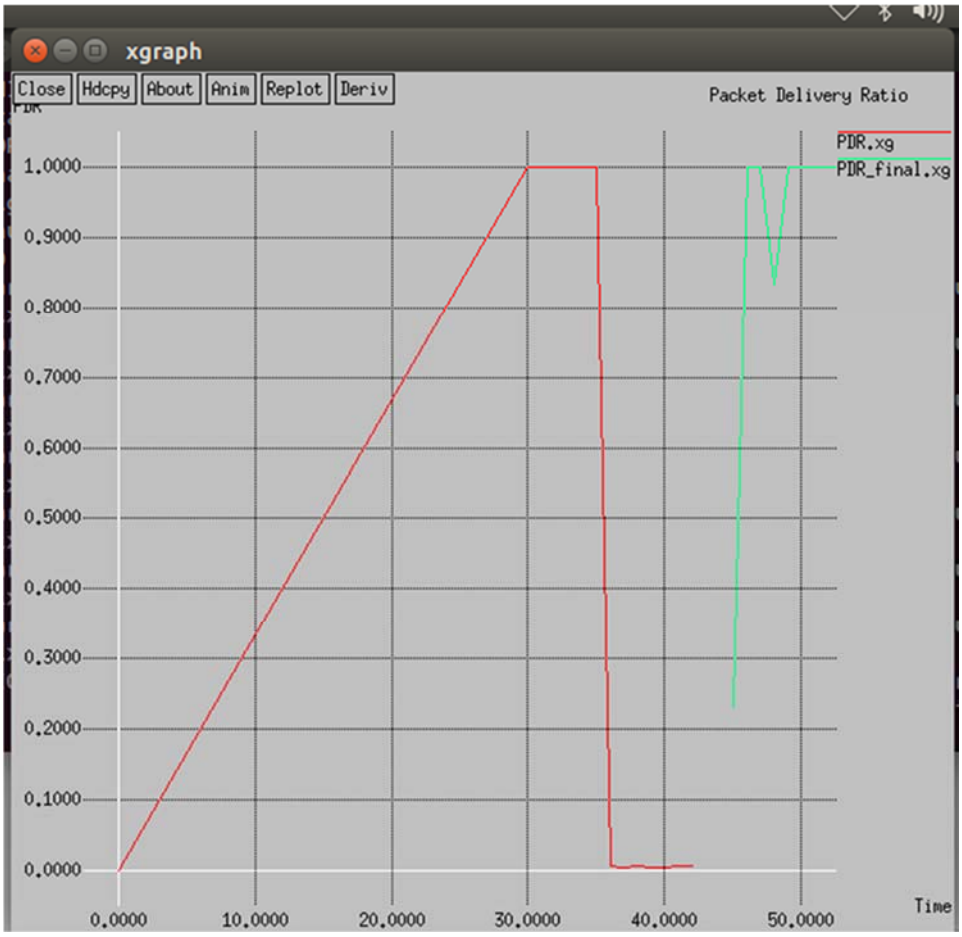


Fig 6: Packet Delivery Ratio

5. Conclusion

Technique for preventing flooding based DDoS attacks are implemented and simulation result shows that proposed prevention technique is better than existing technique.

- PDR all most 90% increase.
- Routing Overhead decrease so that network congestion problem solved.
- Detection Rate approx.80- 90 % so malicious node find easily.
- Network Energy requirement also calculated in our research Paper.

6. References

1. Tushar Saxena, Nandini Deb. A Comparative Study of Different Ad-Hoc Routing Protocols Based On Qualitative Parameters, International Journal of Engineering Research & Technology (IJERT) 2013; 2:3, ISSN: 2278-0181.
2. Eman Abdelfattah. Performance Evaluation of Mobile Ad-Hoc Routing Protocols, Novel Algorithms and Techniques in Telecommunications Automation and Industrial Electronics, 2008.
3. Sanjeev Sharma and Sanjay Singh. A Survey of Routing Protocols and Geographic Routing Protocol using GPS in Manet", Journal of Global Research in Computer Science, ISSN-2229-371X, 2012
4. ZhiAng EU, Winston Khoon Guan SEAH. Mitigating Route Request Flooding Attacks in Mobile Ad hoc Networks", Proceedings of International Conferences on Information networking (ICOIN- 2006), Sendai, Japan, 2006.
5. Shishir K. Shandilya, Sunita Sahu. A trust based security scheme for RREQ flooding attack in MANET" International Journal of Computer Applications (0975 – 8887), 2010; 5:12.
6. Samesh R. Zakhary, Milena Randenkovic. Reputation based security protocol for MANETs in highly mobile disconnection –prone environments", International conference on Wireless On-demand Network Systems and Services (WONS), 2010, 161-167.
7. Neeraj Sharma, Raina BL, Prabha Rani *et al.* Attack Prevention Methods for DDOS Attacks in MANETS AJCSIT 1.1, 2011, 18-21.
8. X. Jin, *et al*. ZSBT: A novel algorithm for tracing DOS attackers in MANETs, EURASIP Journal on Wireless Communications and Networking, 2006, 1-9.
9. Huang YA, Lee W. A cooperative intrusion detection system for ad hoc networks, In the Proc. Of 1st ACM Workshop on Ad hoc and Sensor Networks, 2003, 135-147.
10. Yinghua Guo, Steven Gordon, Sylvie Perreau. A flow based detection mechanism against flooding attack in mobile ad hoc networks" in proceedings of WCNC 2007.
11. Amit N, Thakare Mrs, Joshi MY. Performance Analysis of AODV & DSR Routing Protocol inMobile Ad hoc Networks, IJCA, 2010.

12. Patil VP. Efficient AODV Routing Protocol for MANET with enhanced packet delivery ratio and minimized end to end delay, International Journal of Scientific and Research Publications, 2012; 2:8, ISSN 2250-3153.
13. Gupta B, Student Member, IEEE, Joshi RC, Manoj Misra, Member, IEEE, Distributed Denial of Service Prevention Techniques, International Journal of Computer and Electrical Engineering 2010; 2(2):1793-8163.
14. Malik N. Ahmed1, Abdul Hanan Abdullah1, Ayman El-Sayed2, A Survey of MANET Survivability Routing Techniques", Int. J. Communications, Network and System Sciences 2013; 6:176-185
15. Kavuri Roshan, K.Reddi Prasad, Niraj Upadhayaya, Govardhan A. New-fangled Method against Data Flooding Attacks in MANET, International Journal of Computer Science & Information Technology (IJCSIT) 2012; 4; 3.
16. Minda Xiang, Yu Chen; Wei-Shinn Ku; Zhou Su, "Mitigating DDoS Attacks Using Protection Nodes in Mobile Ad Hoc Networks", Global Telecommunications Conference (GLOBECOM 2011), IEEE 2011.
17. Rupa Rani, Vatsa AK. CARD (Continuous and Random Dropping) based DRDOS Attack Detection and Prevention Techniques in MANET, International Journal of Engineering, 2012.