www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 11 Nov. 2016, Page No. 19230-19236

Analysis of Effect of Flooding on Performance of Ad hoc Network

Sumeet Dubey[1], Aaquib Ladiwala[2], Vignesh Kamath[3],Pranav Nanda[4], Shubha Puthran[5]

[1]NMIMS' Mukesh Patel School of Technology, Management and Engineering
Vile Parle,Mumbai,India.
sumeetdubey.nmims@gmail.com

[2]NMIMS' Mukesh Patel School of Technology, Management and Engineering
Vile Parle,Mumbai,India.
aaquibladiwala.nmims@gmail.com

[3]NMIMS' Mukesh Patel School of Technology, Management and Engineering
Vile Parle,Mumbai,India.
vigneshkamath.nmims@gmail.com

[4]NMIMS' Mukesh Patel School of Technology, Management and Engineering
Vile Parle,Mumbai,India.
pranavnanda.nmims@gmail.com

[5]NMIMS' Mukesh Patel School of Technology, Management and Engineering
Vile Parle,Mumbai,India.
shubha.puthran@nmims.edu

Abstract: ***Mobile Ad hoc networks (MANET) are a new paradigm of networks offering unrestricted mobility without any underlying infrastructure. The network is set up with a group of mobile wireless nodes and is devoid of any dedicated routers or base stations. The wireless nodes move around freely and mutually cooperate with each other in routing and forwarding packets without the support of any fixed infrastructure or centralized administration. The topology is highly dynamic, making the routing procedure more difficult and insecure. In this paper, the performance of the network is analyzed after flooding the network using malicious nodes. The flooding attack is done by the malicious node by sending fake RREQ packets throughout the network. The number of malicious nodes and their position is changed along with various other node characteristics to observe their respective effects on the network performance. The simulation environment is implemented by using the NS-3 network simulator.***

Keywords: AODV, MANET, flooding attack, malicious nodes.

Table 1: Abbreviations and Acronyms

Abbreviation	*Description*
MANET	Mobile Ad hoc network
AODV	Ad hoc On demand Distance Vector
OLSR	Optimal Link State Routing
RREQ	Route Request
RREP	Route Reply
Kbps	Kilo Bits Per Second

1. Introduction

Mobile ad hoc network (MANET) [1] is a group of wireless mobile hosts, which has no stationary infrastructure or base station for communication. Each individual node communicates beyond their direct wireless transmission range by cooperating with each other and forwarding packets through multi-hop links. The nodes act as routers for forwarding and receiving packets to/from other nodes. If two nodes are not within the transmission range of each other, other nodes are needed to serve as intermediate routers for the communication between the two nodes. Routing in ad hoc networks [2] [4] has been a challenging task ever since wireless networks came into existence. Due to the high mobility of nodes, interference, multipath propagation and path loss, there is no fixed topology in MANET. Hence a dynamic routing protocol is needed for these networks to function properly.

Dynamic routing protocols can be classified as proactive and reactive routing protocols, as follows: The proactive (table-driven) routing protocols like OLSR [5], etc. maintain the routing information to every other node in the network, even before it is needed. The reactive (on-demand) routing protocols like AODV [6], DSR [7] etc., do not maintain the routing informations to other nodes in the network, until and unless required. This type of protocols finds a route on demand by flooding the network with Route Request packets

In many situations, the on-demand (reactive) routing protocols have proved to perform better with significantly lower overheads than the periodic (proactive) routing protocols. This is because the on-demand protocols can react quickly to the dynamically changing topology, while reducing the routing overhead in those areas of the network, where changes are less frequent. In this paper, the focus is mainly on the reactive routing protocols (namely AODV) for MANET.

All available nodes in ad hoc networks participate in routing and forwarding, in order to maximize the total network throughput. Hence, successful operation of MANET is possible if and only if all the participating nodes fully cooperate in

communication. Due to the lack of a fixed base station, the ad hoc nodes are forced to rely on each other to maintain network stability and functionality. However, misbehaving nodes are capable of causing significant problems. A node may misbehave when it is overloaded, broken, selfish, or malicious.
A malicious node [11], also called compromised node, can sabotage the other nodes or even the whole network, by launching a denial of service attack, by either dropping packets or by flooding the network with a large number of RREQs to invalid destinations in the network, thus jamming the routes of communication. Flooding attack is one such type of DoS attack, in which a compromised node floods the entire network by sending a large number of fake RREQs to nonexistent nodes in the network or by streaming large volumes of useless DATA packets to the other nodes of the network. This results in network congestion, thus leading to a Denial of Service.
In this paper, a simulation study of impact of flooding and other node parameters in AODV [6] performance, using the NS-3 network simulator is given.

1.1 Security Issues

Due to vulnerability in ad hoc networks there are many security challenges to be faced in networks like in flooding attack the initiated malicious nodes tries to hinder or affect the network performance of the ad hoc network and since its ad hoc network the attacker node keeps changing his position due to which at various positions the attack level differs. If the attacker is near the receiver than its affect will be different and if far than it will again differ in its impact on ad hoc network performance

2. Overview of Ad Hoc Networks

Wireless communication enables information transfer among a network of disconnected, and often mobile, users. Popular wireless networks such as mobile phone networks and wireless LANs are traditionally infrastructure-based, i.e. base stations, access points and servers are deployed before the network can be used. In contrast, ad hoc networks are dynamically formed amongst a group of wireless users and require no existing infrastructure or pre-configuration. Maintaining the Integrity of the Specifications. A mobile ad hoc network is a dynamically self organizing network without any central administrator or infrastructure support. It is composed of mobile terminals that communicate one to the other through broadcast radio transmissions.

3. Overview of AODV Protocol

The Ad hoc On-demand Distance Vector (AODV) [6] routing protocol is a simple and efficient on-demand routing protocol, based on the distance vector approach. It is designed specifically for use in multi-hop wireless MANET scenario. The protocol is composed of the two main mechanisms − "Route Discovery" and "Route Maintenance". Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of routing table entries. Route Request (RREQ) message is broadcasted by a node requiring a route to another node and Route Reply (RREP) message is unicasted back to the source of RREQ. Sequence numbers are used for each routing table entry to determine whether the routing information is up-to-date. This prevents routing loops. AODV includes the route maintenance mechanism to handle the dynamic network topology. Routes are maintained by using Route Error (RERR) message, which is sent to notify other nodes about a link failure. HELLO messages are sent in periodic beacons for detecting and monitoring the links to the neighbors. If a node S wants to send data packets to a destination D that is not in its routing table, it will buffer the data packets and broadcast a Route Request (RREQ) for D into the network. The RREQ packet will be forwarded by other intermediate AODV nodes to the intended destination node D. On receiving the RREQ, D will send a Route Reply (RREP) on the reverse route back to S. S includes the known sequence number of the destination in the RREQ packet. The intermediate nodes, on receiving an RREQ packet check its routing table entries. If it possesses a fresh route toward D, i.e. a route with greater sequence number than that in the RREQ packet, it unicast an RREP packet back to its neighbour from which it has received the RREQ packet. Otherwise, it sets up the reverse path and then rebroadcasts the RREQ packet. Duplicate RREQ packets received by one node are silently dropped. As the RREP packet is propagated along the reverse path to the source, the intermediate nodes update their routing tables and set up the forward path.

4. The NS-3 Simulator

For simulation analysis, NS-3 [12] was used for implementing the network simulation environment. NS-3 is an open source discrete event network simulator targeted primarily for networking research and educational purpose. Previously, NS-2 [14] was the tool for academic networking research. But it had several disadvantages. It required the involvement of both oTcl and C++. For new modules and features, it required a lot of manual recoding and compilations. NS-3 is a new simulator. It is not an extension of NS-2. It does not support the NS-2 APIs. It is written entirely in C++, with optional Python bindings. Hence, simulation scripts can be written either in C++ or in Python. The oTcl scripts are no longer needed for controlling the simulation, thus abandoning the problems which were introduced by the combination of C++ and oTcl in NS-2. Thus, NS-3 is a more readily extensible platform and much easier to use. NS-3 has sophisticated simulation features, which include extensive parameterization system and configurable embedded tracing system, with standard outputs to text logs or PCAP (tcpdump). It is very object oriented for rapid coding and extension. It has an automatic memory management capability as well as an efficient object aggregation/query for new behaviors & states, like adding mobility models to nodes. Moreover, NS-3 has new capabilities, such as handling multiple interfaces on nodes
correctly, efficient use of IP addressing and more alignment with Internet protocols and designs and more detailed 802.11 models, etc. NS-3 integrates the architectural concepts and code from GTNetS [15], which is a simulator with good scalability characteristics. The Simulation Network Architecture looks just like IP architecture stack. The nodes in NS-3 may or may not have mobility. The nodes have “network devices”, which transfer packets over channel and incorporates Layer 1 (Physical Layer) & Layer 2 (Data Link layer). The network devices acts as an interface with Layer 3 (Network Layer: IP, ARP). The Layer 3 supports the Layer 4 (Transport

Layer: UDP, TCP), which is used by the Layer 5 (Application Layer) objects.

5. Flooding Attack

Flooding attack [11] [16] [17] [18] is a denial of service attack, in which a compromised node (malicious node) floods the network by sending large number of fake RREQs to non-existent nodes in the network or by streaming large volumes of useless DATA packets to the other nodes of the network creating ghost packets which loop around due to false routing information, efficiently using bandwidth and processing resources along the way. This attack severely affects ad hoc networks causing a huge packet loss to receiver.

5.1 RREQ Flooding attack

The RREQ Flooding Attack is a denial-of-service attack in which malicious nodes take advantage of the route discovery process of the reactive routing protocols (e.g. AODV, DSR) in MANET. In this attack, a compromised node aims to flood the network with a large number of RREQs to non-existent destinations in the network. It generates a large number of RREQs and broadcast them to invalid destinations. Since a node with such invalid destination node-id does not exist in the network, a reply packet cannot be generated by any node in the network and they keep on flooding the RREQ packet. When such fake RREQ packets are broadcasted into the network in high numbers, the network gets saturated with RREQs and is unable to transmit data packets. Thus, it leads to congestion in the network. The RREQ Flooding Attack also results in overflow of route table in the intermediate nodes so that the nodes cannot receive new RREQ packet, resulting in a denialof-service attack. Moreover, unnecessarily forwarding these fake route request packets cause wastage of precious node resources such as energy and bandwidth.

To reduce congestion in a network, the AODV protocol adopts some methods. RREQ_RATELIMIT [19] is the maximum allowable number of RREQs that a node can sent per second. After broadcasting a RREQ, a node waits for a RREP. If a route is not received within round-trip milliseconds, the node may again try to discover a route by broadcasting another RREQ, until the numbers of retries reach the maximum TTL value. The default value for the RREQ_RATELIMIT is 10 as proposed by RFC 3561. However, a malicious node can override the restriction put by RREQ_RATELIMIT by increasing it or disabling it, thus allowing it to send large number of RREQ packets per second. A node can do so because of its self-control over its parameters. This allows it to flood the network with fake route requests, leading to a kind of DoS attack due to the network-load imposed by the fake RREQs.

5.2 Data Flooding attack

Once an attacker node has set up the paths to all the nodes in the networks, it may cause DATA Flooding Attack by streaming large volumes of useless DATA packets to them along these paths. The excessive DATA packets in network clog the network and reduce the available network bandwidth for communication among the other nodes in the network. The destination node gets busy on receiving the excessive packets from the attacker and cannot work normally. The available network bandwidth for communication also gets exhausted, so that the other nodes cannot communicate with each other due to the congestion in the network. Moreover, the process of receiving the attack packets consumes a lot of resource in all the intermediate nodes. If an attacker combines both types of flooding attacks, it will result in the whole network crashing. Due to flooding attack, a non-malicious genuine node cannot fairly serve other nodes due to the network-load imposed by the fake RREQs and useless data packets. This leads to several problems, as follows: x Wastage of bandwidth x Wastage of nodes' processing time, thus increasing the overhead x Overflow of the routing table entries, causing exhaustion of an important network resource like memory x Exhaustion of the nodes' battery power x Degraded throughput Most of the network resources are wasted in trying to generate routes to destinations that do not exist or routes that are not going to be used for any communication. In this paper we use RREQ flooding attack.

6. Simulation Setup

The simulation was done using the NS-3 simulator [12], which provides a scalable simulation environment for wireless networks. In order to measure the impact of flooding attack in MANET performances, the AODV routing protocol was modified to simulate a flooding attack scenario. The simulated network consists of 20 nodes placed randomly with in 100x100, 500x500, 1500x1500 area. Each node has a transmission range of 250m and moves at a speed of 20m per second. In each of the scenario network is first simulated with no attacking node. The number of attacking nodes are then gradually increased and the performance of the network is the analyzed and noted. The simulation parameters along with their values are listed down in Table 2**.**

Table 2: Abbreviations and Acronyms

Routing protocol	Aodv
Simulation time	50 seconds
No of mobile nodes	20
Transmission area	100x100,500x500,1500 x1500
Transmission power	12.5 dbm
Flooding rate	50

6.1 Performance Metrics

6.1.1 Transmission Time

It is the amount of time from the beginning until the end of a message transmission. In the case of a digital message, it is the time from the first bit until the last bit of a message has left the transmitting node. The packet transmission time in seconds can be obtained from the packet size in bit and the bit rate in bit/s as:

Packet transmission time = Packet size / Bit rate

6.1.2 Packets Dropped

It's the number of data packets dropped during transmission by a node.

6.1.3 Throughput

It is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot

7. Simulation Results

7.1 Network Architecture

Figure 1 shows the network topology wherein Red nodes- Attacker Nodes i.e. the nodes flooding the network with RREQ packets with false addresses. Green nodes:- Sender nodes i.e. the nodes sending genuine data across the network to a existing destination. Blue Nodes:- Sink nodes i.e. the destination or receiver nodes.

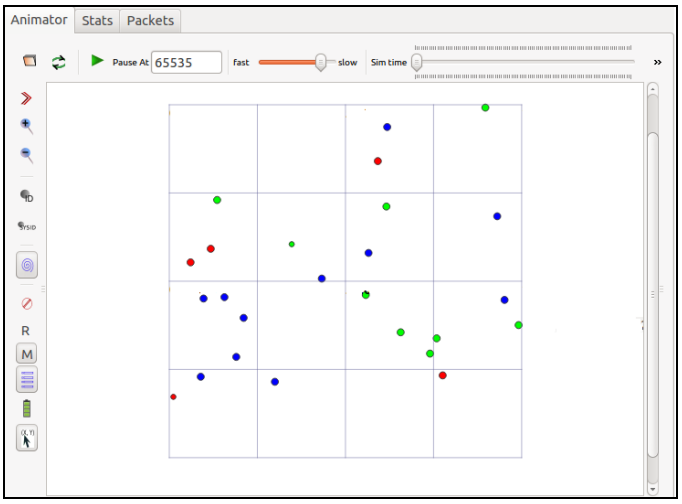

Figure 1: Network Topology

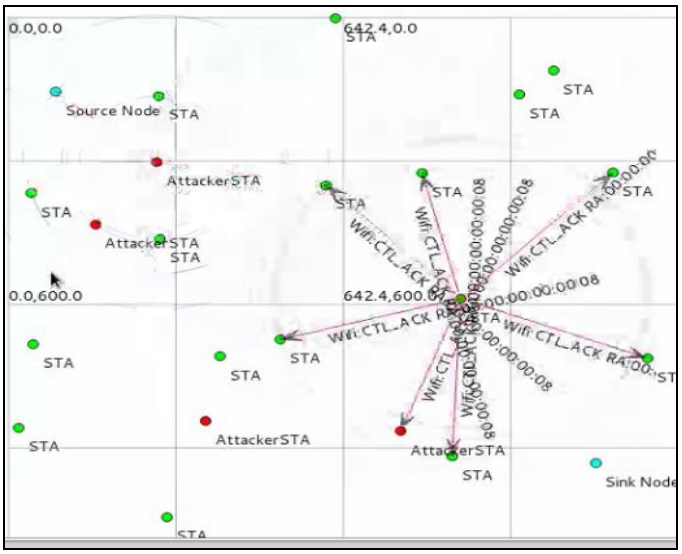

Figure 2: The attacker node sends RREQ packets to all the nodes in its range, effectively taking up bandwidth.

7.2 Simulation metrics

- Transmission power is constant at 12.5 decibel-mill watts.
- Simulation time is 50 seconds in all cases
- Number of malicious packets increase as: 1 – 3 – 7 – 10
- Total number of packets sent in all cases is 1000
- Area of the network changes as: 100*100 – 500*500 – 1500*1500

7.3 Simulations

7.3.1 Area 100*100

(a) Throughput

Table 3: Throughput for area 100*100

Sr No	*Total no. of nodes*	*Total no. of malicious nodes*	*Total Packets Sent*	*Total Packets Received*	*Max Throughput (kbps)*
1	20	1	1000	998	64.51
2	20	3	1000	995	52.22
3	20	7	1000	988	47.58
4	20	10	1000	982	45.33

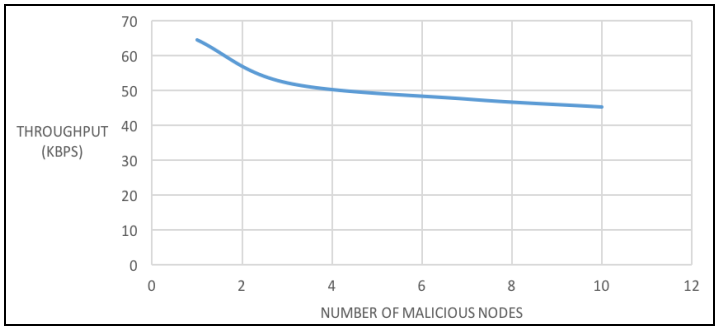

Figure 3: Throughput when area is 100*100

(b) Delay

Table 4: Delay when area is 100*100

Sr No	*Total no. of nodes*	*Total no. of malicious nodes*	*Max Delay in packet delivery (secs)*
1	20	1	1.02816
2	20	3	1.13176
3	20	7	1.74067
4	20	10	2.86734

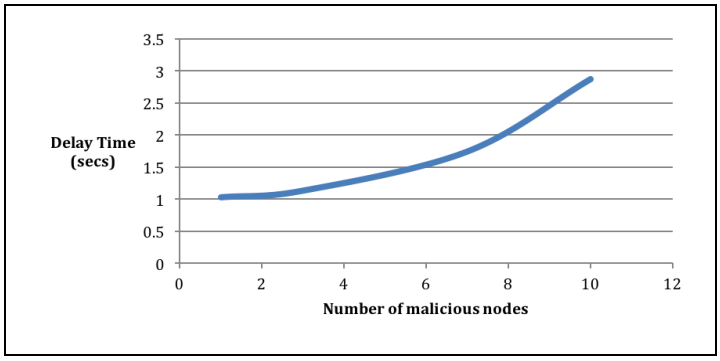

Figure 4: Delay when area is 100*100.

(c) Packet Loss

Table 5: Packet Loss when area is 100*100.

Sr No	Total no. of nodes	Total no. of malicious nodes	Packets lost	% Loss of packets
1	20	1	2	0.2
2	20	3	5	0.5
3	20	7	12	1.2
4	20	10	18	1.8

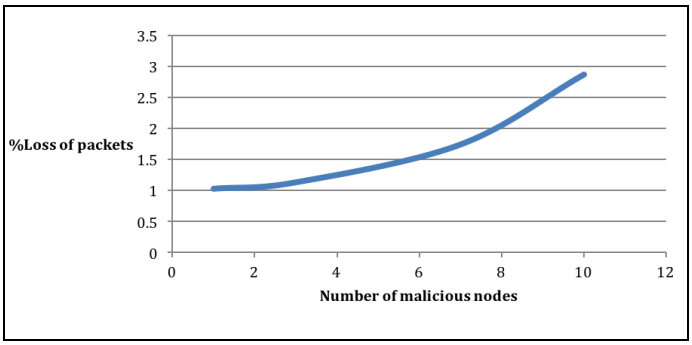

Figure 5: Packet Loss when area is 100*100.

The 4 cases are as shown. By observation, the packet loss gradually increases with the increase in flooding nodes. Max throughput dips down. Linear increase in graph of packet loss as expected. More flooding nodes result in more loss of data packets.

7.3.2 Area 500*500

(a) Throughput

Table 6: Packet Loss when area is 500*500.

Sr No	Total no. of nodes	Total no. of malicious nodes	Total Packets Sent	Total Packets Received	Max Throughput (kbps)
1	20	1	1000	996	60.416
2	20	3	1000	990	59.392
3	20	7	1000	978	58.368
4	20	10	1000	963	57.856

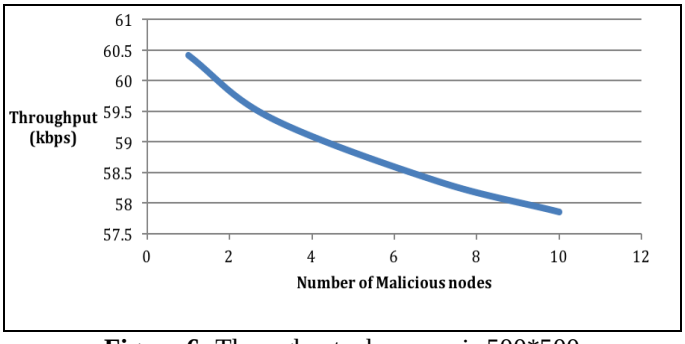

Figure 6: Throughput when area is 500*500

(b) Delay

Table 7: Delay when area is 500*500.

Sr No	Total no. of nodes	Total no. of malicious nodes	Max Delay in packet delivery (secs)
1	20	1	1.084563
2	20	3	1.26733
3	20	7	1.80122
4	20	10	2.56858

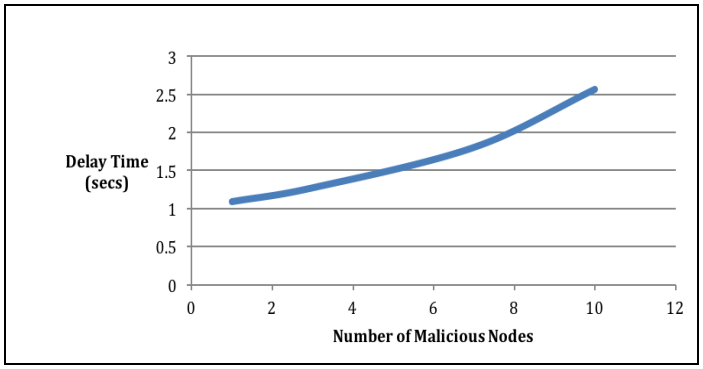

Figure 7: Delay when area is 500*500.

(c) Packet Loss

Table 8: Packet loss when area is 500*500.

Sr no	Total no. of nodes	Total no. of malicious nodes	Packets lost	% Loss of packets
1	20	1	4	0.4
2	20	3	10	1
3	20	7	22	2.2
4	20	10	37	3.7

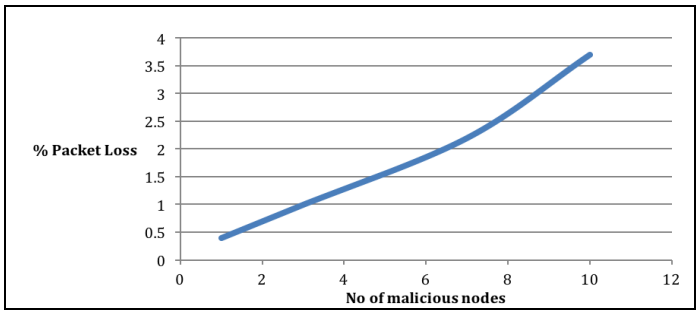

Figure 8: Packet Loss when area is 500*500.

Results are as expected. Larger network size has resulted in fewer throughputs and more packet loss. This is due to the large distance between the nodes. Graph is showing near to linear growth in packet loss. No variations are observed.

7.3.3 Area 1500*1500

(a) Throughput

Table 9: Throughput when area is 1500*1500.

Sr No	Total no. of nodes	Total no. of malicious nodes	Total Packets Sent	Total Packets Received	Max Throughput (kbps)
1	20	1	1000	847	51.2
2	20	3	1000	640	23.0
3	20	7	1000	519	20.1
4	20	10	1000	452	17.3

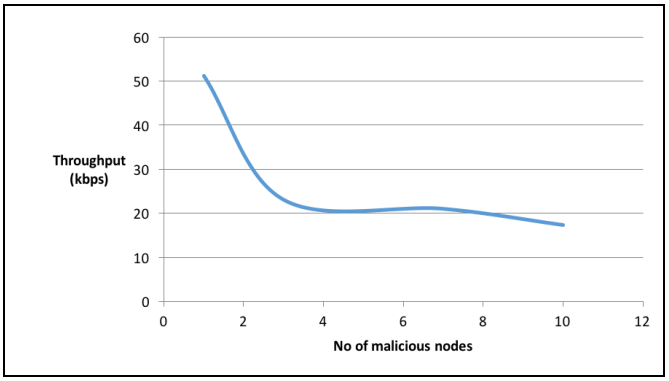

Figure 9: Throughput when area is 1500*1500.

(b) Delay

Table 10: Delay when area is 1500*1500.

Sr No	*Total no. of nodes*	*Total no. of malicious nodes*	*Max Delay in packet delivery (secs)*
1	20	1	2.01504
2	20	3	2.81038
3	20	7	2.85327
4	20	10	2.87869

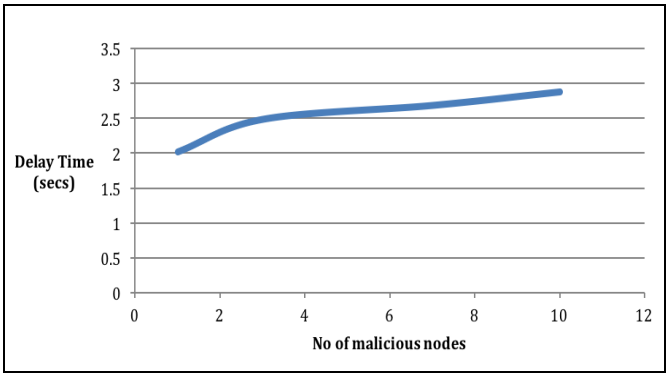

Figure 10: Delay when area is 1500*1500.

(c) Packet Loss

Table 11: Packet Loss when area is 1500*1500.

Sr No	*Total no. of nodes*	*Total no. of malicious nodes*	*Packets lost*	*% Loss of packets*
1	20	1	153	15.3
2	20	3	360	36
3	20	7	481	48.1
4	20	10	548	54.8

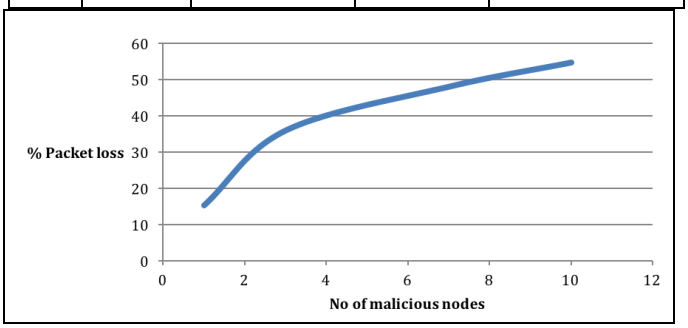

Figure 11: Packet Loss when area is 1500*1500.

There is a significant increase in packet loss in this scenario. Note that though the packet loss is the maximum, the rate at which the packet loss increases is less than the other two scenarios.

8. Conclusion

The flooding attack in AODV protocol was simulated using the NS-3 network simulator. It was noticed that the presence of malicious flooding nodes in MANET can affect the performance of the overall wireless network and can act as one of the major security threats. From the simulation, it can be concluded that due to the extensive flooding in the network, average percentage of packet loss and average time delay for delivery increases while throughput decreases, thus decreasing the overall network efficiency. The area of the network did not have a major effect on the performance, with minor decrease in packet loss observed in a very large network.

9. Acknowledgment

For this project, we would like to thank our mentor, Professor Shubha Puthran, who has guided and encouraged us to take this project up and has helped us overcome the difficulties that we faced during implementation. We would like to thank her for her positive and encouraging feedback. We would also like to thank our families for their continuous support and faith in us.

References

[1] S Corson and J. Macker, “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”. Internet Request for comment RFC 2501, Jan 1999.

[2] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz, “A review of routing protocols for mobile ad hoc networks”. Technical report, Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia, 2003.M. Clerc, “The Swarm and the Queen: Towards a Deterministic and Adaptive Particle Swarm Optimization,” In Proceedings of the IEEE Congress on Evolutionary Computation (CEC), pp. 1951-1957, 1999. (conference style)

[3] Muhammad O Pervaiz, Mihaela Cardei and Jei Wu, “Routing security in ad hoc wireless networks”, Department of Computer Science and Engg, Florida Atlantic University, Boca Raton, FL 33431.

[4] Krishna Gorantala, “Routing Protocols in Mobile Ad-hoc Networks”. June 15, 2006, Master’s Thesis in Computing Science, 10 credits; Supervisor at CS-UmU: Thomas Nilsson; Examiner: Per Lindstrom.

[5] P. Jaquest and T. Klausen "optimized Link State Routing Protocol"

[6] C.E. Perkins, E. Belding Royer, and S.R. Das, “Ad hoc On demand distance vector (AODV) routing”, IETF RFC 3561, July 2003.

[7] D.Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, 2007.

[8] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Proc. of Wireless Communications, IEEE, Oct 2007, Issue 5, pgs 85-91.

[9] "The NS-3 Network Simulator", http://www.nsnam.org/

[10] "The NS-2 Network Simulator", http://www.isi.edu/nsnam/ns

[11] G. Riley, "Large scale network simulations with GTNetS", in Proceedings of the 2003 Winter Simulation Conference, 2003.

[12] S. Sanyal, A. Abraham, D. Gada, R. Gogri, P. Rathod, Z. Dedhia, and N. Mody, "Security scheme for distributed DoS in mobile ad hoc networks", 6th International Workshop on Distributed Computing (IWDC'04), vol. 3326, LNCS, Springer, 2004, pp. 541.

[13] P. Yi, Z. Dai, Y. Zhong, S. Zhang, "Resisting Flooding Attacks in Ad Hoc Networks", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05), April 2005, pp. 657-662.

[14] Z. Eu and W. Seah, "Mitigating Route Request Flooding Attacks in Mobile Ad Hoc Networks", Proceedings of the International Conference on Information Networking (ICOIN'06), Sendai, Japan, January 2006.

[15] Perkins C.E., Terminology for Ad-Hoc Networking, Draft-IETFMANETterms-00.txt,November,1997.