Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol

Shruti Bhalodiya
PG Scholar
Computer Engineering
RK University
Rajkot, Gujarat, India

Krunal Vaghela
Dy. Director
School of Computer Science
RK University
Rajkot, Gujarat, India

ABSTRACT
Mobile ad-hoc network (MANET) is a self-deliberate data network, where all nodes behave like host or router. MANET is a collection of number of mobile nodes or devices that randomly generate a temporary network. Security is the fundamental requirement in MANET due to its behavior of changing topology, open medium and lack of centralized authentication. This leads to various security attacks in mobile ad hoc network and violate the criteria of routing mechanism. Mobile Ad-hoc network doesn't need backbone infrastructure support and it is very reliable and also contains the routable networking environment. In this paper, the effect of flooding attack in AODV based network is explained. The network parameters like Throughput, Packet Delivery Fraction (PDF) and End to End Delay are compared with normal network (without flooding attack) and a network with one or more flooder nodes. The performance of network parameters is compared in all the three scenarios. We have proposed a scheme which is finds single or number of malicious nodes in the network and drops fake packets.

Keywords
MANET, AODV routing protocol, Flooding attack, NS-2.35

1. INTRODUCTION
The mobile ad-hoc networks diverge from already present networks by the fact that they don't depend on fixed infrastructure [1]. MANETs contains nodes that are moving casually with some speed. In MANETs node work as a both router as well as host so it can be fixed or mobile. MANET network is a temporary network that can be ruined anytime [6]. This network designed dynamically and share common wireless link. As in ritual networks there is no basic fixed structure but in MANETs nodes are free to move randomly and can leave or join the network on the fly. In MANET every single node works as host and route. A mobile ad hoc network is a assembly of mobile nodes attached by wireless link without the necessity of stationary infrastructure in place like wireless access point or base station point.

MANETs are exposed to different threats due to not having any infrastructure and dynamic network topology, which leads to different types of security attacks.Wireless link in MANET create them more expected to attack. It is easy for hacker to attacks these networks easily and increase access to private information [5]. These violate the network goals such as accessibility, authenticity, authorization, reliability and confidentiality[2].

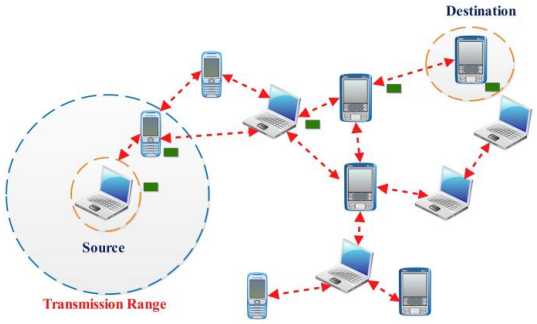

Fig 1: MANET Network

2. AODV ROUTING PROTOCOL
AODV routing protocol is a reactive routing protocol. In this routing protocol whenever the data transmission is needed at that time path is establish for transmission of the data over network, and also in AODV the routing table mechanism is auto update for particular time period and it is advance version of DSDV protocol for routing data over network. AODV routing protocol uses the table driven approach but it finds the paths only when it is needed. AODV is a combination of both protocol DSDV and DSR. It uses characteristics of a DSDV as well as DSR routing protocols.

AODV is used for both unicast routing as well as multicast routing. AODV uses a sequence number for finding the routing message which is fresh. It applies a destination sequence numbers for finding the fresher path. AODV has three main controls message called RouteRequest (RREQ), RouteReply (RREP) and RouteError (RERR).In an AODV, RREQ is used for the route broadcasting. Source node uses this route request packet for broadcast the route request.

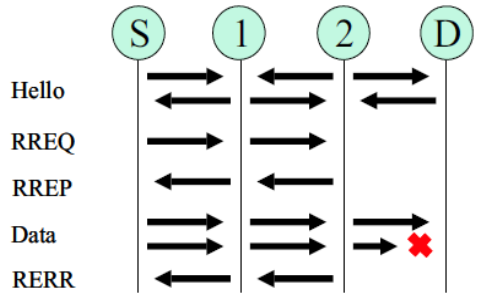

Fig 2: AODV Control Packets

3. FLOODING ATTACK

Flooding attack is type of Denial of Service (DoS) attack. The main issue regarding the flooding attack is that the flooder node floods the whole network. Flooder node receives the RREQ and it will generate the RREP with higher sequence number so source node assumes that it has the path for destination node. Flooding attacks main aim is to consume the power in terms of battery power and bandwidth. It will cause some issues regarding the network performance. Flooding attack leads to the degradation in terms of result of throughput, exhaustion of battery power and wastage of bandwidth. There are mainly three types of flooding attack.

3.1 RREQ Flooding [7]

In this type of attack, the flooder node broadcast several RREQ packets for the node which exist or not exist in the network. To complete RREQ flooding the attacker deactivate the RREQ rate so it will consumes network bandwidth.

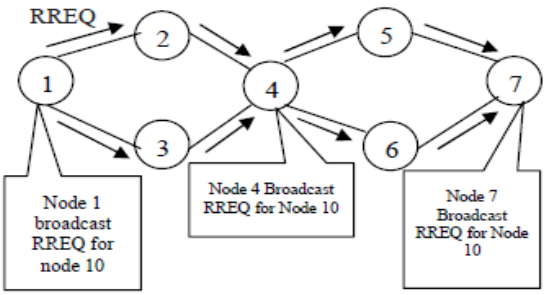

Fig 3: RREQ Flooding Attack

3.2 Data Flooding [7]

In this type of attack, data packets are used to flood the whole network. The attacker or flooder node, construct a route towards all the node then send the huge quantity of fake data packet and this bogus data packet fail the network resources so it will be hard to detect the flooder node.

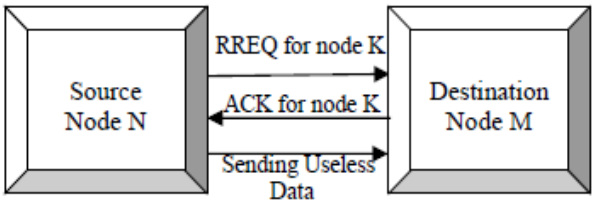

Fig 4: Data Flooding Attack

3.3 SYN Flooding

In syn flooding attack, attacker or flooder node sends the number of synchronization packet to the destination node. Hence the large amount of memory will be consumed through this attack.

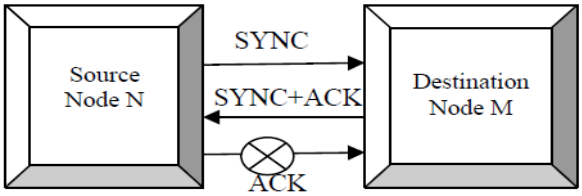

Fig 5: SYN Flooding Attack

4. RELATED WORK

In Fan Hong, Yu Zhang and Jian-Hua Song [8], the author planned the new methodology to conflict the flooding attack. In this technique they implementing two thresholds value namely, ratelimit and blacklistlimit. If no. of RREQ is less than ratelimit then the request succeeded else check it is less than blacklistlimit or not. If yes then make node black listed but if the no. of nodes greater than rreqlimit and less than blacklistlimit then place the RREQ in the delay queue. Then process after time out occurs. These techniques can handle the network with high mobility.

In Venkat Balakrishnan, Vijay Varadharajan and Uday Tupakula [9], they analyzed the flooding attack in unidentified communication. In this technique mainly three components are used: blacklist threshold, whitelisting threshold and transmission threshold. Efficiently recognize & reject the nodes which flood the network. In this unidentified network it's impossible to track back destination and source nodes.

In M. Pushpalatha, T. Rama Rao and Revathi Venkataraman, [10], they presented the extended AODV protocol based on the trust factor. In this technique, authors have categorized the nodes in three categories based on the trust value: Friends, acquaintance and stranger. Friends are trusted nodes, Stranger are non trusted nodes, and which has the trust factor less than the friends and greater than the stranger its called acquaintance. This technique does not work with higher node mobility.

In Komal Joshi and Veena Lomte [12], the author introduce a node-to-node verification technique using challenge-response protocol and MNT (Malicious Node Table). Challenge- response protocol(CRP) checks genuine node flooding from malicious node and MNT (Malicious Node Table) used for storage information about malicious node noticed by CRP. AODV routing protocol is used for packet forwarding and security will be maintained by MNT. The aim of this technique is to provide node accessibility and better security for packet transfer in MANET. It does not provide better packet delivery ratio, throughput and control overhead.

In Kashif Laeeq [13], author introduces RFAP technique for transforming the RREQ (route request) flooding attack on AODV protocol in MANET. The result analysis shows that, the RFAP technique can identify the malicious flooder node and protects the network properties from flooder or attacker node (flooding attack). At the time of flooding attack, original AODV protocol can create defective result compare to RFAP technique. RFAP technique can easily find the flooder or attacker node and defend the network from RREQ flooding attack. The RFAP technique cannot stop the illegal data packets.

5. PROPOSED SCHEME

In RREQ flooding attack AODV routing protocol is very weak due to route discovery scheme and its broadcast mechanism. There are many methods already implemented to reduce the congestion. In AODV it is compulsory to view that how many RREQ is originated by the single node. We assign the RREQ_RATELIMIT value as 10 which are proposed by (Request for Comments) RFC 3561.

Once RREQ is broadcasted to every node in the network it will wait for the RREP, if route request is not received by the node within time limit or within round-trip millisecond, a node will try again to determine the path and it try until it reaches the maximum TTL (Time To Leave) value. After

broadcasting route requests it will wait for the round-trip time of RREP. To congest the network, malicious node will generate more RREQ packets than the normal node. In this network topology data packet should have more priority than the RREQ packets, because node spent more time with RREQ packet and result service will be delayed. By increasing or disabling the RREQ_RATELIMIT we can restrict or override the malicious node. A node will choose the node in which the rate of limit RREQ_RATELIMIT is high and this is how it allows the network to be flooded and lead the fake RREQ in the network so it is a kind of DoS attack.

In DoS due to network load a normal node can't be fair to work with other node, as it is imposed by the fake RREQ. In result it will affect the bandwidth, throughput, processing time and many more parameters.

To detect and reduce the malicious node effect on network, the filter is used in proposed algorithm. To control the ratio of RREQ packets, we are using the filtering technique which maintains the threshold value of each node. Filter will check the threshold value of RREQ packets, if it is more than 10 then it will block the node otherwise it will be considered as a normal node.

The RREQ packet is processed as normal if the rate of RREQ originator is lower than the threshold. The threshold value helps to decide if a node is behaving maliciously or not. When the count of RREQs initiated by a node is larger than the value of threshold, then easily it can be assumed that the parallel node attempts to flood the network with possible false RREQs. When sender node is identified as a malicious, it will be entered in blacklist. Additional flooding of the false RREQs in the network can be prevented by this blacklisted entry. To support vibrant nature of MANETs, the blacklisted node is ignored for some specific time period. Later it is unblocked to allow participating in the network. Timeout will be increased, if blacklisted node again misbehaves. The neighbor nodes of the malicious node are capable to take interest to receive RREQs from remaining normal nodes in the network. In this way we can increase Throughput, End to End Delay and Packet Delivery Fraction (PDF) of AODV in MANET.

6. SIMULATION RESULTS

6.1 Performance Matrices

6.1.1 Throughput

The number of packets transmitted from sources to destination in given time slot.

6.1.2 Packet Delivery Ratio

It is the ratio between total numbers of received packet to the total number of packet sent by source node or sender node over a network.

6.1.1 End to End delay

Time require to transmit the data from source to destination.

6.2 Simulation Results

The simulations are carried out on NS-2 (Ver. 2.35) simulator installed in Ubuntu environment. We have implemented AODV with flooding attack and proposed AODV and compared all the results. Simulation parameters are presented in table 1.

Table 1: Simulation Parameters

Parameter	Value
Network Simulator	NS2.35
Simulation Time	100 s
No of Mobile Nodes	25, 50, 75, 100
No of Flooder Nodes	1 to 5
Topology (Area)	500 m x 500 m
Routing Protocol	AODV routing protocol
Traffic	CBR
Packet Size	512 Bytes/Packet
Pause Time	1.0 s
Maximum Speed	3.0 m/s
Mobility Model	Random Way Point
MAC Protocol	IEEE 802.11

6.3 Impact of Number of Nodes

6.3.1 Graph for Throughput v/s No. of Nodes

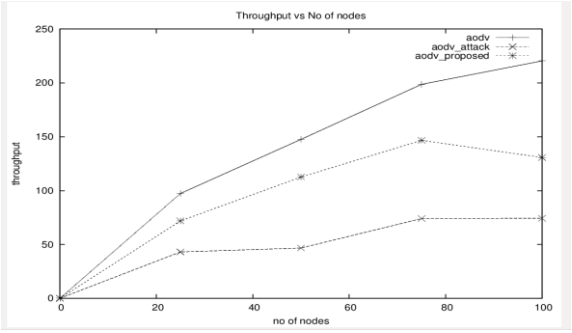

Fig. 6: Graph for throughput v/s no. of nodes

Figure 6 shows the impact of number of nodes on throughput. AODV protocol has a high throughput because it takes attack free path for data delivery. AODV with flooding attack suffers from attacking behaviour and down the throughput and proposed AODV gives improved performance compared to the flooding attack. The reason for the improvement is that our proposed solution strongly prevents flooder node as we have set the threshold value of RREQ as 10.

6.3.2 Graph for PDF v/s No. of Nodes

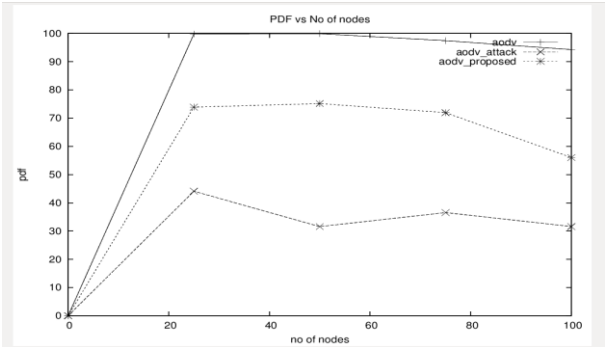

Fig. 7: Graph for PDF v/s no. of nodes

Figure 7 shows the impact of number of nodes on PDF. AODV protocol has a higher PDF compared to remaining both. AODV with flooding attack having very less PDF because it shows its attacking behaviour and decrease the performance of PDF as the attacker node congests the network. PDF is higher in our proposed scheme as compared to flooding attack even though the number of nodes is increasing because we are adding the node with more than 10 RREQ to the blacklist.

6.3.3 Graph for End-to-End Delay v/s No. of Nodes

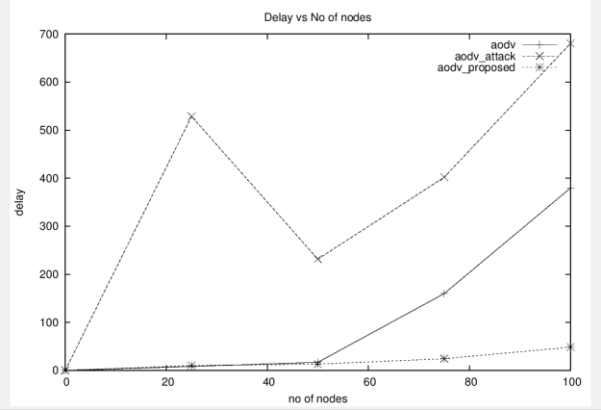

Fig. 8: Graph for end-to-end delay v/s no. of nodes

Figure 8 shows the impact of number of nodes on end-to-end delay. AODV protocol has a less delay compared to AODV with flooding attack protocol because it takes safe and attack free route. AODV with flooding attack has maximum delay compared to the reaming both because attacker node drops more packets which leads to delay. Proposed scheme give minimum delay compared to simple AODV protocol because it detect flooder node and eliminate it from the network.

6.4 Impact of Number of Malicious Nodes:

6.4.1 Graph for Throughput (flooder node) v/s No. of Malicious Nodes

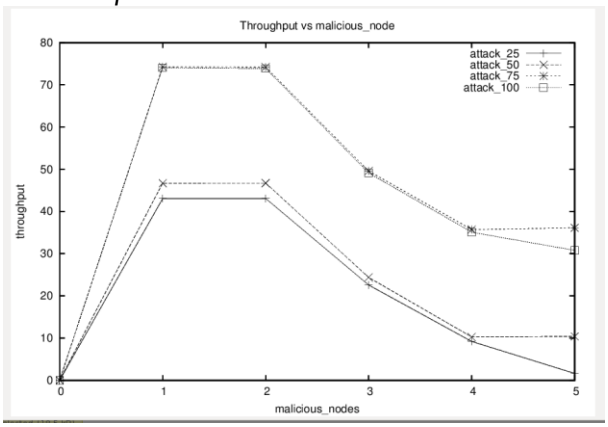

Fig. 9: Graph for throughput (flooder node) v/s no. of malicious nodes

Figure 9 shows the impact of number of malicious nodes on throughput. In AODV (with flooding attack) protocol when no. of malicious nodes increases, throughput decreases accordingly. But with various no. of attacker nodes the effect on the network of throughput remains same as we are increasing the number of nodes.

6.4.2 Graph for Throughput (proposed scheme) v/s No. of Malicious Nodes

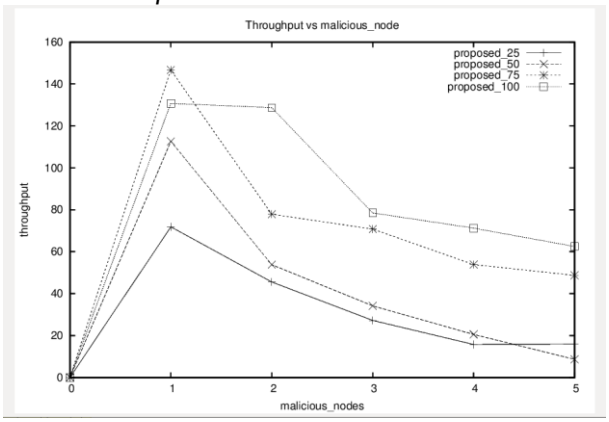

Fig. 10: Graph for throughput (proposed scheme) v/s no. of malicious nodes

Figure 10 shows the impact of number of malicious nodes on throughput. In our proposed solution effect of throughput on network remains same when no. of nodes increases. And if number of malicious nodes increases, throughput decreases. But for various number of nodes, throughput increases in our proposed scheme compared to AODV (with flooding attack) as the flooder node is blocked. Hence, normal nodes can transmit packets easily through the network.

6.4.3 Graph for PDF (flooder node) v/s No. of Malicious Nodes

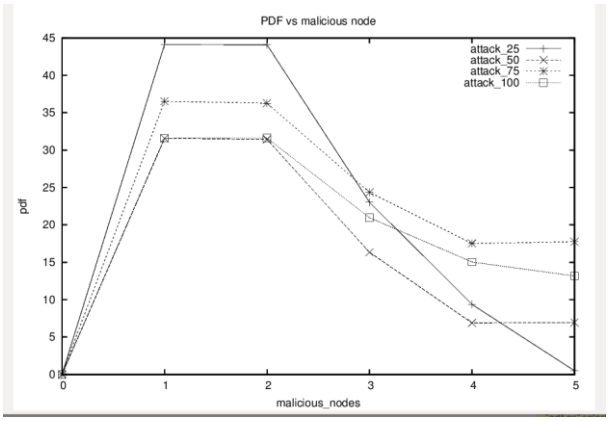

Fig. 11: Graph for PDF (flooder node) v/s no. of malicious nodes

Figure 11 shows the impact of number of malicious nodes on PDF. In AODV (with flooding attack) protocol when no. of malicious nodes increases, PDF decreases accordingly. But with various no. of attacker nodes, the effect on the network of PDF remains same as we are increasing the number of nodes. The reason behind this is the malicious behavior of attacker nodes strongly affects the network.

6.4.4 Graph for PDF (proposed scheme) v/s No. of Malicious Nodes

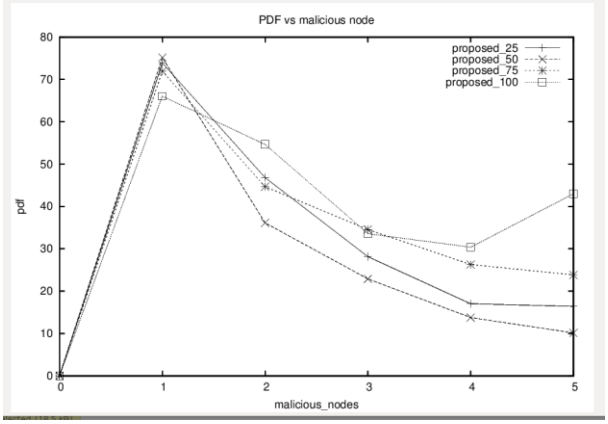

Fig. 12: Graph for PDF (proposed scheme) v/s no. of malicious nodes

Figure 12 shows the impact of number of malicious nodes on PDF. In our proposed solution effect of PDF on network remains same when no. of nodes increases. And if number of malicious nodes increases, PDF decreases. But for various numbers of nodes, PDF increases in our proposed scheme compared to AODV (with flooding attack) as threshold value 10 doesn't allow flooder node to congest the network.

6.4.5 Graph for End-to-End Delay (flooder node) v/s No. of Malicious Nodes

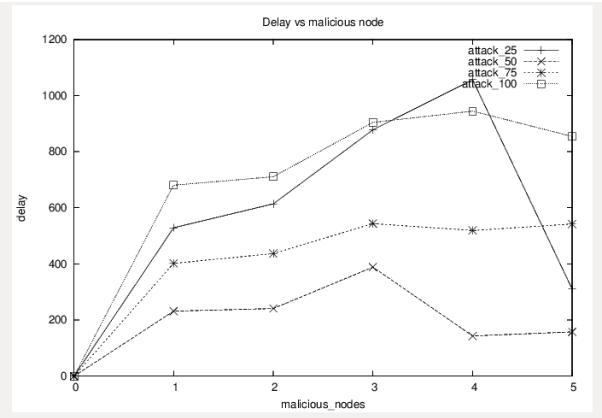

Fig. 13: Graph for end-to-end delay (flooder node) v/s no. of malicious nodes

Figure 13 shows the impact of number of malicious nodes on end-to-end delay. In AODV (with flooding attack) protocol when no. of malicious nodes increases, delay also increases accordingly. The effect on the network of delay remains same as we are increasing the number of nodes, when no. of attacker nodes is different. Because the malicious nodes drop more packets, the packets take more time to reach from source to destination which leads to delay.

6.4.6 Graph for End-to-End Delay (proposed scheme) v/s No. of Malicious Nodes

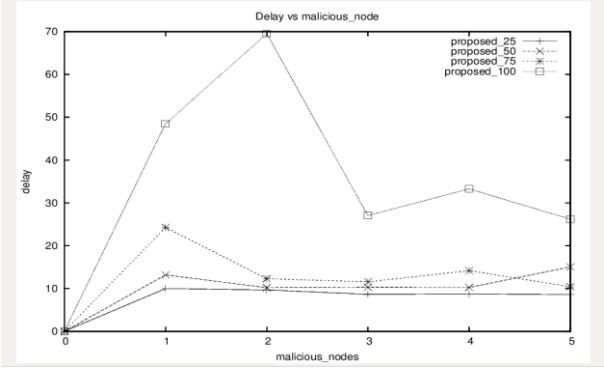

Fig. 14: Graph for end-to-end delay (proposed scheme) v/s no. of malicious nodes

Figure 14 shows the impact of number of malicious nodes on end-to-end delay. In our proposed solution, effect of delay remains same when no. of nodes increases. Also delay increases when no. of malicious nodes increases. In our proposed scheme delay decreases compared to the AODV protocol because threshold value 10 don't allow more than 10 RREQ so there is less possibility of flooding compared to AODV(with flooding attack) protocol.

7. CONCLUSION

Due to the absence of any centralized authority the mobile ad hoc network suffers from many security attacks as the wireless link is accessible to all. Flooding attack in MANET results in degradation of throughput, exhaustion of battery power, and wastage of bandwidth. In this paper we have proposed a solution for flooding attack using RREQ flooding attack. In our proposed solution threshold value set as 10. In the network if we found threshold value more than 10, then marked that node as malicious node. We can apply this solution to identify and remove any number of flooder nodes in MANET and discover a safe path from source to destination by diverting the malicious nodes. In future, focus will be to analyse flooding attack problem in other protocols. This proposed system can also be useful in other types of attacks to prevent it.

8. REFERENCES

[1] Pradip M. Jawandhiya and Mangesh M. Ghonge, "A Survey of Mobile Adhoc Network Attacks", *International Journal of Engineering Science and Technology*, Vol. 2(9), pp.- 4063-4071, 2010.

[2] A. Mishra and K..M.Nadkarni, *Security in Wireless Ad - hoc Network, in Book*. "The Hand Book of Ad Hoc Wireless Networks" (chapter 30) , 2003.

[3] Robinpreet Kaur & Mritunjay Kumar Rai, " A Novel Review on Routing Protocols in MANETs", *Undergraduate Academic Research Journal (UARJ)*, Volume-1, Issue-1, pp. 103-108, 2012

[4] Siva Ram Murthy and B.S.Manoj, "Ad hoc Wireless Networks"(Chapter 7),2014.

[5] E.M.Royer and C.E.Perkins "Adhoc On-Demand Distance Vector Routing", *IEEE*, February 1999.

[6] Datuk Prof Ir Ishak Ismail and Mohd Hairil Fitri Ja'afar," Mobile Ad Hoc Network Overview", *IEEE*, December 2007.

[7] Ruchita Meher and Seema Ladhe," Review Paper on Flooding Attack in MANET", *International Journal of Engineering Research and Applications*, pp. 39-46,January 2014.

[8] Jian-Hua Song, Fan Hong and Yu Zhang, "Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks", *IEEE*, 2006.

[9] Monu Singh,Ajay Singh,Rajesh Tanwar and Ritu Chauhan, "Security Attacks in Mobile Adhoc Networks",*International Journal of Computer Applications(IJCA)*, 2011.

[10] Venkat Balakrishnan, Vijay Varadharajan ,and Uday Tupakula" Mitigating Flooding attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications", *IEEE*, 2007.

[11] Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao, "Performance Analysis of Flooding Attack Prevention Algorithm in MANETs", *International Scholarly and Scientific Research and Innovation*, pp. 421-424, 2009.

[12] Ms. Neetu Singh Chouhan and Ms. Shweta Yadav, "Flooding Attacks Prevention in MANET", in *International Journal of Computer Technology and Electronics Engineering (IJCTEE)*, pp. 68-72, November 2011.

[13] Komal Joshi Veena Lomte, " Preventing Flooding Attack in MANET Using Node-to-Node Authentication", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 11, pp. 136-140, November 2013.

[14] Kashif Laeeq ,"RFAP, A Preventive Measure against Route Request Flooding Attack in MANETS", *IEEE*,2012.

[15] Neha K. Holey , Sonal S. Honale, "Various Methods for Preventing Flooding Attack in MANET –A Comparative Analysis", *International Journal of Computing and Technology*, Volume 1, Issue 3, pp. 120-122,April 2014.

[16] Teerawat Issariyakul and Ekram Hossain, "Introduction to Network Simulator NS2 manual", 2009 Edition.