iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** V **Month of publication:** May 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Prevention of DOS and Black Hole Attack in AODV

Sachin Gupta[1], Harsha Chawla [2]
[1]M. Tech Student, [2]Assistant Professor, Department of CSE & NGF College of Engineering & Technology Palwal, Haryana, India

Abstract: ***Mobile Ad Hoc Network (MANET) is a self-configuring, gathering of wireless devices and infrastructure-less network technology used to create a wireless network without wire using mobile nodes. In MANET all devices are free to move independently in any direction so they change their links to other devices frequently. Its performance is based on the services of the network; however MANET's are vulnerable to the attacks due to its dynamic topology, nomadic and open environment. However, network is vulnerable to the outside attacks by presence of malicious nodes. Therefore, MANET Networks are vulnerable because of its dynamic, nomadic and open operational environment. There are two security threats in an AODV such as DOS and Black Hole attacks. DOS attack is one of the server security scourges in an ad hoc networks aims to disrupt the services provided by network or the server by continuously sending unwanted packets using malicious node. The malicious nodes are the type of mobile nodes but it is different to normal mobile nodes as like change or removes routing information, send a fake route request to the server. The Black Hole attack captures the path and sends's fake route reply message and routing information.***

So to overcome from these consequences we are proposing an algorithm which introduces a mechanism of Dos and Black Hole Attacks (BHA) prevention and check network performance in the malicious environment. Throughput and end to end delay are also analyzed.

Keywords: -MANET, AODV Routing Protocol, DOS, Black Hole attack.

I. INTRODUCTION

Mobile Ad-hoc Networks is a collection of group of wireless mobile node, i.e wireless devices. The wireless nodes are connecting dynamically and sharing the information. Basically there are two types of mobile ad-hoc networks: Infrastructure based and networks with fixed and wired gateways. The bridges for wireless networks are known as base station [1].The personal computer make wireless node using the wireless LAN card, the PDA (Personal Digital Assistants) or Smartphone, the laptop or wireless devices.

Fig: 1 Mobile Ad-hoc Networks

Fig.1 is defining the mobile ad-hoc network and how to communicate one wireless device to another wireless device. A wireless node can be tackle of any employs, the air as the transmission medium. As shown, wireless node may be physically connected to a Laptop, a Mobile, or PDA, to enable wireless communication between them. MANET has following advantages:

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Ad hoc networks no more costly infrastructure such as copper wires or data cables is not required.
Ad hoc networks are very well-situated and simple to deploy, since there are no cables involved. So the deployment time can be reduced.
Ad hoc network configuration changes dynamically over the time in MANET's. While comparing to configurability of LANs, it is very easy to change the networks topology of a wireless mobile ad-hoc network.

There are some challenges in the MANET and these are as:

Nodes are mobile and connected dynamically in a random manner. Links of the network vary timely and are based on the closeness of one node to another.
No centralized administration node is available to handle the operation of the different mobile nodes.
Identifying relevant mobility in nodes and informing about their existence need movable updates, route selection to facilitate automatically.
The wired links have higher capacity then wireless links

A. Routing protocols in MANET

In Mobile ad hoc network Routing is primarily and most important concept for communication in the network. The aim of routing is to find out and select the best route between communicating node, when a communication take place between nodes in the network intermediate node play a important role because when source node send route request to destination node and destination node give reply of the route request to source node, In this intermediate node take a part in communication between source to destination, then create a route reply and sends the route reply to the source node through intermediate node. There are three types of routing protocols in Mobile ad-hoc networks.

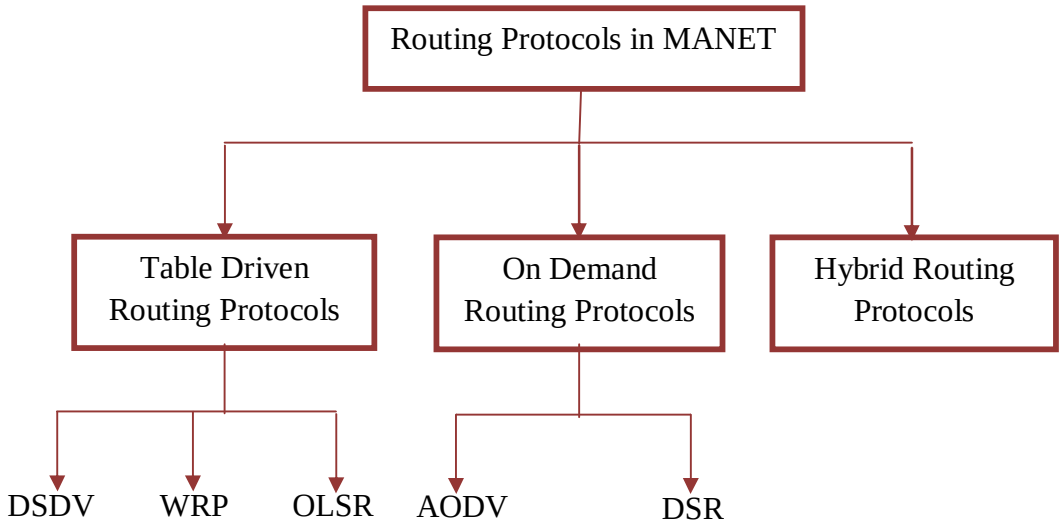


Fig. 2 Classification of Routing Protocol in MANET

1) *Table Driven Routing Protocols:* It is also called Proactive Routing Protocols. The Proactive means it works or maintains the routing information before the source node wants to send packet or information to the destination. The Table Driven Routing protocols maintain the updated path from each to every node available in the networks. In these protocols every node needs to maintain the routing table for storing the routing information. When network topology changes, then routing table also get updated and stores the fresh or up-to date information.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

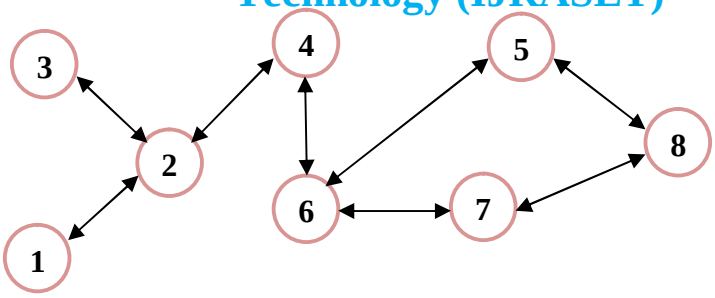


Fig 3 DSDV Route Establish: Networks

Table 1 DSDV Route Establish: Node 1 Routing

Destination	Next Hope	Distance	Destsequence
2	2	1	22
3	2	2	37
4	2	2	41
5	2	4	50
6	2	3	99
7	2	4	121
8	2	5	109

In Fig 3 and Table 1 Node 7 is disconnected from Node 6 and established connection with Node 8. So the routing table of Node 7 updated. Node 6 notices the link-break and sends the updates with new route information. Table Driven routing table updates are of two types: Full dumps and Incremental updates. If the routing table updating is full dump, then the whole routing table to be sends to the neighbor's node. It update incrementally, only position changed entries sent from the routing table since the final update and fit in a packet.

2) *On-Demand Routing Protocols:* An on-Demand routing strategy creates and maintains path between source and destination only when required and does not maintain a permanent routing entry in routing of each destination. It includes two processes. There are two types' reactive routing protocols.
AODV (Ad-hoc On Demand Distance Vector Routing Protocols)
DSR (Dynamic Source Routing Protocols)

a) *AODV (Ad-hoc On Demand Distance Vector Routing Protocols):* Ad-hoc On-Demand Distance Vector Routing Protocol is using a multi-hop technology based on distance vector routing protocol. The routes were created only when needed for communication between source and destination through intermediate mobile hosts. In AODV [3], Ad-hoc means node move or connected or disconnected with the networks any time, On Demand means when source wants to send data to the destination, Distance means find the distance between source to destination in terms of number of hope counts and Vector means list of information stored in the node's information list. Every transmission using Source Address, Destination Address, Source ID, Destination ID, Source Sequence Number, Time to Live (TTL) Destination Sequence Number. These protocols use the Open Shortest Path First (OSPF) method/Algorithm. AODV use some approaches for path or route establishment [13].

i) *Route Request (RREQ):* In Route Request source node broadcast/transmit the route request message for specific destination neighbor's node to pass the message to destination

ii) *Route Reply (RREP):* In Route Reply, destination uses the unicast route for reply message to source. The neighbor nodes make next hop entry for destination and forward the reply. If source receives multiple replies then it use the one with shortest hop count route/path. SSN (Source Sequence Number) and DSN (Destination Sequence Number): When source node sends the broadcast packet with sequence number and destination sequence number, then it is defining the fresh path.

iii) *Route Error (RERR):* When route error message are generated then there is a network link break between sources and

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

destination. AODV routing protocols detect the node and if possible do the local repairing. When link break occurred in optimum path then the neighboring node to sent previous request for sending the message to destination.

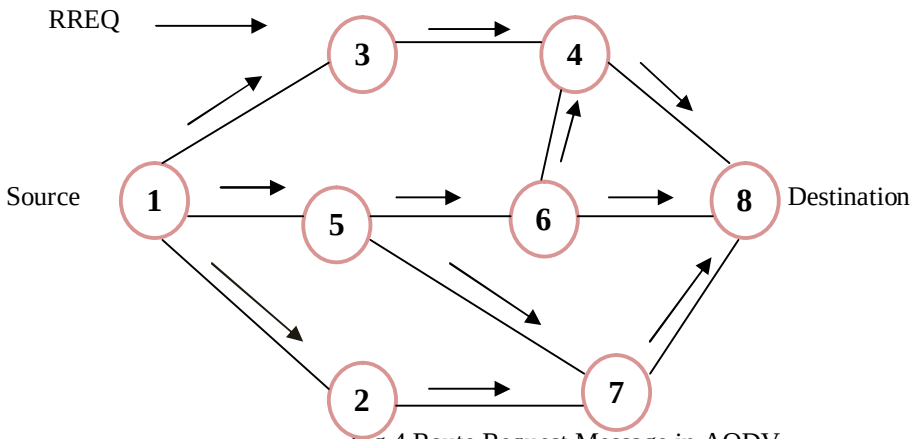


Fig 4 Route Request Message in AODV

Fig 4 is a mobile wireless network. Node 1 (Source) to Node 8 (Destination Node) flood the route request packets with a source sequence within the network. Node 1 send route request to all neighbors and neighbors through Destination.

In Fig 5 Destination uses the unicast path for the route reply. Destination is replying the route request on symmetric link. Destination Sequence number is defining the freshness of the route/path. In network source node counts the number of hop to reach the destination and find the route with minimum number of hopes. Source node selects this route for data transfer.

In AODV route maintenance happens when link break in the network, it broadcasts the route error (RERR) packet to its neighbors, which in reply propagates the RERR packet towards the node whose routes may be affected by the disconnected link. Then, the affected source node can re-initiate a route discovery process if the route is still needed. Neighbor node informs all other neighbors in the network that this link does not exist, so don't send any packet on that link.

3) *Hybrid Routing Protocols:* Hybrid routing protocols is combination of both reactive and proactive routing protocols. It was proposed to minimize the overhead of the proactive routing protocols and also to decrease the latency caused by route discovery within reactive routing protocols. Hybrid routing protocols are such as ZRP, IARP, IERP, BRP.

II. LITERATURE SURVEY

Prime Product Number approach to solve the malicious node problem [1] by prevention and removal. It proposed a scheme to mitigate the adverse effects of misbehaving node. Key contribution of this approach is, it assume that each node in the network has a specific prime number which belong to node unchanged identity. In this scheme MANET organized in to number of cluster in such a way that at least one cluster is a member of every node which is called cluster head. When destination node and intermediate node generate route reply message to the source node which is the product of prime number from destination node to source node and other information. If reply information is right and prime product number is fully divisible then node is trustworthy node otherwise call the removal process of the node. The main limitation of this approach is that first give the prime number to every node in MANET, cannot check the behavior of malicious node before assigned the prime number. if malicious node is cluster head how can find out. It is slow process. End to end delay, through put and packet delivery ratio is not improve.

In this approach [13] source node without altering intermediate nodes and destination nodes by using a Prior-Receive-Reply method. In this method, checking large difference between the sequence number of source node and destination node or intermediate node who has sent back RREP or not, compare the destination sequence number with source sequence number. If there is more difference between source and destination sequence number then destination node is malicious node. This method work only source node and destination node. No involvement of intermediate node. It is basis on specific attack black hole. Only sequence number checking technique used.

In this approach [8] it measure the performance of AODV routing protocol in the presence of malicious nodes evaluation has been considered as packet delivery ratio, through put, data packet sent/received and control packet droop. In this no prevention and avoidance technique used for malicious node. It only measures the performance of AODV. No technique is used for improved the performance in through put, end to end delay, packet delivery ratio.

In this article [11], investigate the security issues in MANET. Author examine attacks such as spoofing and colluding miserly attacks as well as counter measures against such attacks in existing MANET protocol. In this approach gives solution for only specific attack not all. No technique used for handling delivery ratio, end to end delay and throughput.

In this approach [14] algorithm is discussed for prevention of flooding attack. Node categorized as strangers and friends based on their relationships with their neighboring nodes. For evaluation of its neighbor node trust level a trust estimator is used. End-to-end delay packet delivery ratio is like a various parameter for trust level functioning

In this CORE mechanism approach [9] it is heighten watchdog for isolating and monitoring. Malicious node based on functional reputation, subjective and indirect various types of information on each entity's rate of collaboration is used for calculation of reputation. Since there is no inducement for spreading negative information maliciously about other nodes, the collaboration technique itself is prevented denial of service attack.

III. PROPOSED MODEL

Mobile ad- hoc network is wireless and dynamic and position of mobile node change continuously. These causes increase the presence of attacks in the ad- hoc network. The main focus on the work to prevention of Denial of Service (DoS) and Black Hole attacks (BHA) in Mobile Ad-hoc Network. In this research scheme detection of malicious node and change functioning of malicious node without involvement of middle node and destination node.

When any node get send route request if it is continuous route request then check the behavior of the node that it should not be intrusion node. For finding this malicious behavior we use the time limit and node counter which work as check the never receive how many route request in a given time limit, here time limit is set at 0.6 and 8 neighbor route request receive then node adding list of malicious behavior and declare malicious behavior node in last malicious behavior node.

In below figure 5 when source node want to send data to destination node, first select suitable path. In network any malicious node if present or enter its show their malicious property and start flooding the large amount of data packet to source by this cause congestion is increase over network and source node not able to send data to original destination. In last malicious node consume battery energy, consume the resources and drop the packet.

A black hole attack is another attack possible in MANET. It is defined for on-demand routing protocol. The aim of this attack is to absorb the routing packet or data packet during performing the operation. It is claiming that it has shortest path and fresh path with smaller number of hope count and large sequence number to destination even though it does not have a valid route to the destination node. Due to this claiming it attract all the packets and absorbed them without forwarding to destination node.Once it entered in the network, it drops forwarding data packet by making a black hole there. This node is called blackhole node or black node. In Blackhole attack it first respond to route request discovery instead first checking its routing table. It increase the congestion and traffic in the network, and therefore attacker can misuse the traffic.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

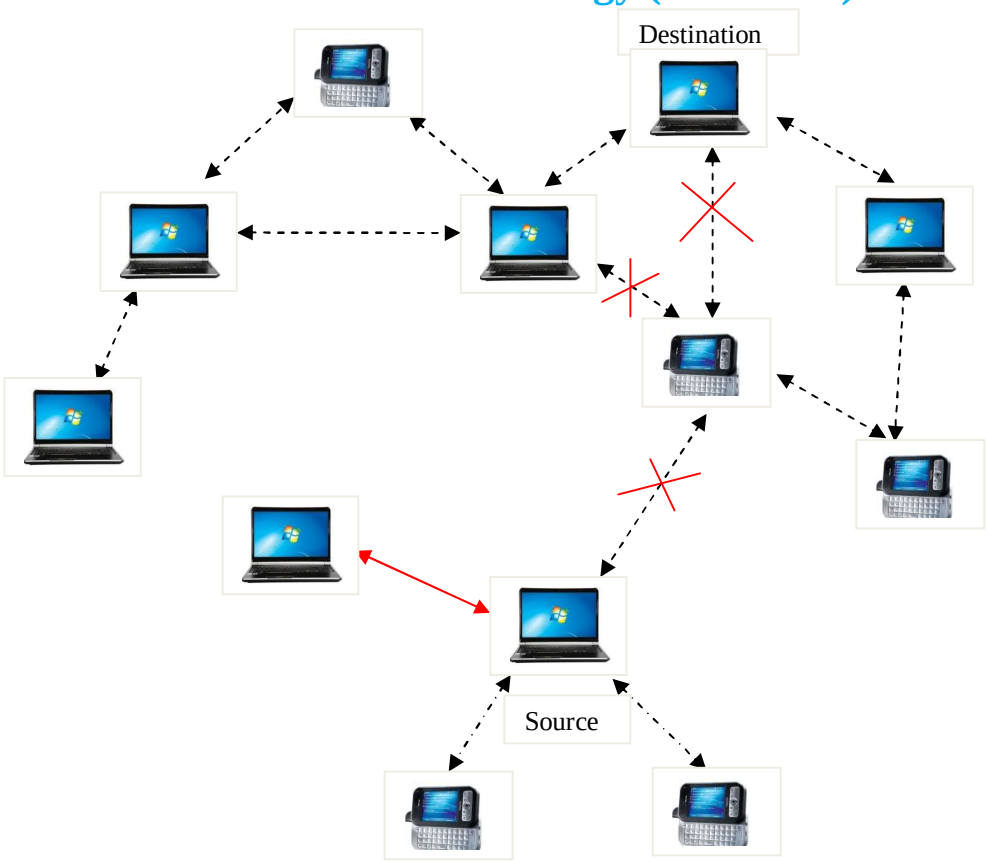


Fig 5 Basic DoS Scenario

Above Figure 5 show examples of Black hole attack, when source node(s) want to establish route for data sending between source to destination (D), source node broadcast the route request (RREQ). When black node or black hole node receive RREQ. It claiming with RREP and it has shortest path with minimum hop count and large sequence number. In last then source send the data to Black hole node and finally it observed the routing packet or drop the forwarding packet to actual destination. Malicious node abuses the relationship between nodes causing disruption in the operation of the network. Malicious (selfish) node intends to disrupt the ongoing proper operation of the routing protocols. Network battery power is limited. When node use the network battery power for its own purpose and node participate in network routing, this type of node is called malicious node.

Malicious nodes can also agree to forward packets but silently drop the packets. They are pretending to preserve energy and bandwidth. This causes defragmented networks, isolated nodes, and significantly reduced network performance. Launch all kinds of attacks by replaying, reordering or dropping packets from time to time, and even by sending fake routing messages [2]. Capture the network battery power, network resources, and increase the congestion in the network. In MANET network when multiple nodes behaves as selfish, then it belong to the resulting scheme in the form of degrading the routing information of other node and performance of other nodes and blocking the functioning of nodes in the network. Multiple nodes act maliciously, simultaneously, or alternately, resulting the schemes to be deal with them will become very slow at most nodes. If multiple nodes are malicious in same networks, then there will be the possibility of two more attacks. Network performance is depend on the network functioning and parameter like network load, throughput, performance of routing, end to end delay and packet delivery ratio but on the other hand malicious environment degrade the network performance.

IV. RESULTS & ANALYSIS

The Figure 6 is network scenario of DoS attacks. Here added the malicious node so malicious node constantly sends the fake route request in the networks. That time source node not able to send data to destination it is means disturb the whole networks. That is why decreased the routing performance. Figure 8 has presented the prevention of the DoS attack. After applying the proposed

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

solution of prevent the DoS attack malicious node are detect and prevents so source node again find the optimum path and start sending data to destination and increased the routing performance in malicious environments.

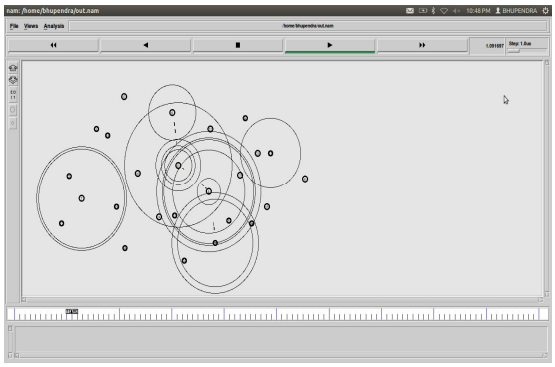


Fig. 6 DoS attack Prevention Scenario

Result 1

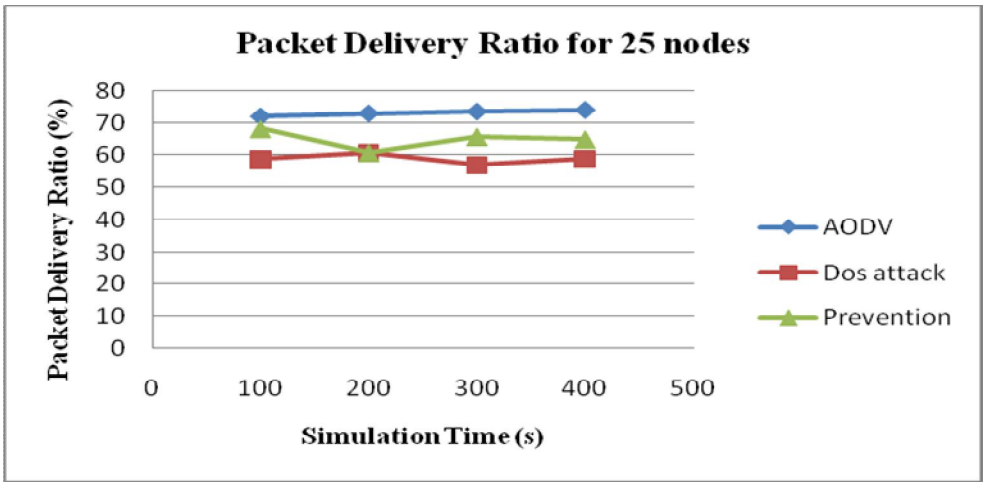


Fig. 7 Packet Delivery Ratio vs. Simulation Time (Sec.)

Result 2

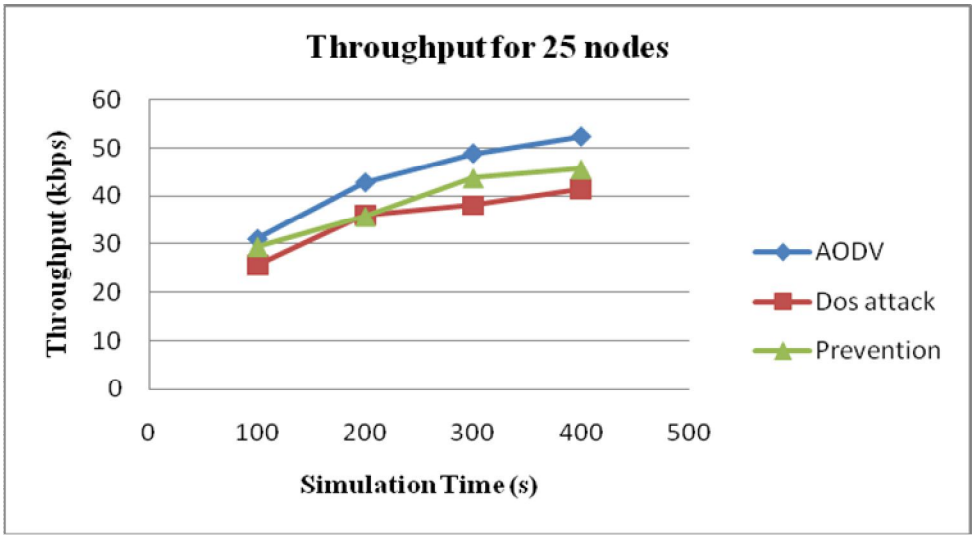


Fig. 8 Throughput vs. Simulation Time (Sec.)

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Result 3

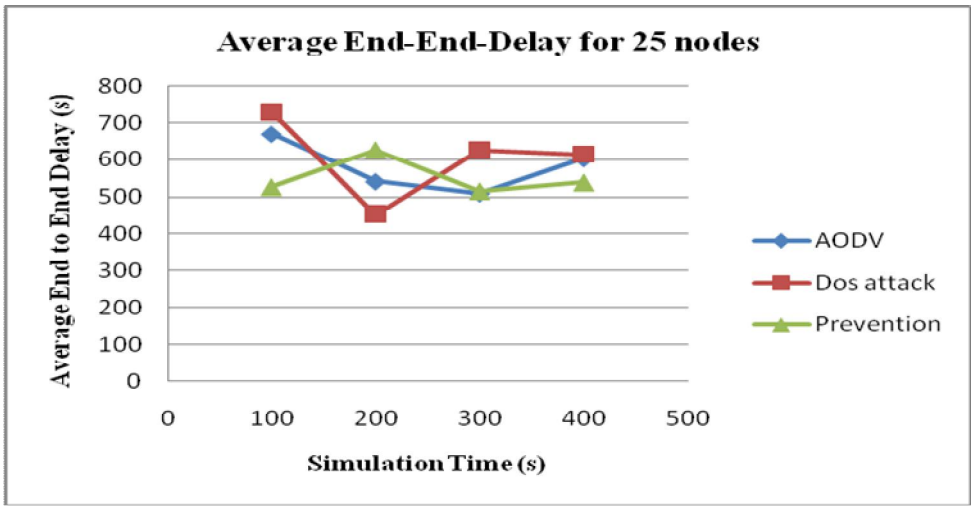
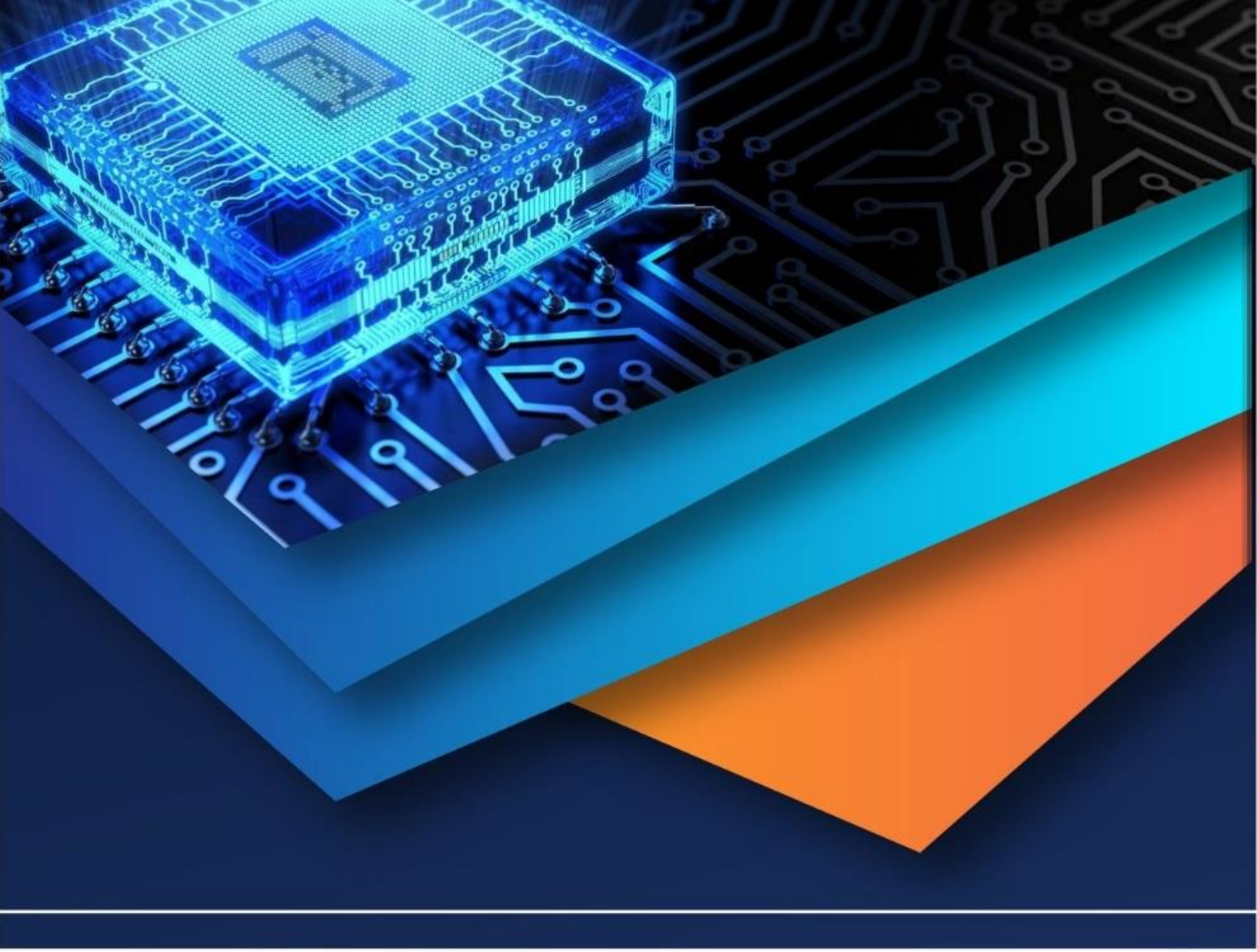


Fig. 9 Average End-to-end delay Vs. Simulation Time (Sec.)

Above Fig. 7, 8 and 9 they show the packet delivery ratio, average Throughput, End-to-End delay under Dos attack. It shows the prevention of our work for 25 nodes with simulation time 100 to 500 Seconds It shows that the throughput decreases with the existence of the attackers using Dos attack and in case of prevention throughput increase End-to End delay decrease.

REFERENCES

[1] Sapna Gambhir, Suarabh Sharma "PPN: Prime Prduct Number based Malicious Node Detection Scheme for Manets", 3rd IEEE(IACC) ,2013
[2] Seryvuth Tan, Keecheon Kim,"Secure Routing Discovery for preventing Black Hole Attack on AODV-based MANETs", IEEE, 2013.
[3] Rashid Sheikhl Mahakal Singh Chandee, Durgesh Kumar Mishra,"Security Issues in MANET: A Review"IEEE, 2010.
[4] Poussy A.Lotfy, Marianne A.Azer,"Performance evolutation of AODV",IEEE, 2013.
[5] Kritika Taneja, Dr.S.S Tyagi "Security Issue on AODV outing Protocol Suffering From Blackhole Attack" IJARCSEE, volume 1,Issue 7, September 2012.
[6] R.Gunasekaran, V.RHYmend Uthariaraj "Prevention of Denial of service attacks and performanceEnhancement in Mobile Ad Hoc Networks", IEEE, 2009
[7] Kavita Taneja and R. B. Patel, "Mobile Ad hoc Networks: Challenges and Future", Proceedings of National Conference on Challenges & Opportunities in Information Technology (COIT-2007) RIMT-IET, Mandi Gobindgarh. March 23, 2007
[8] Vijay Kumar,Rakesh Sharma,Ashwani Kush,"Effect of Malicious Nodes on AODV in Mobile Ad Hoc Networks",International Journal of Computer Science and Management research Vol 1 Issue 3 October 2012
[9] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Comm.and Multimedia Security, 2002.
[10] A.Rajaram, Dr. S. Palaniswami "Malicious Node Detection System for Mobile Ad hoc networks", International Journal of Computer Science and Information Technologies, Vol. 1 (2), 2010, 77-85
[11] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato," A Survey Of Routing Attacks In Mobile Ad Hoc Networks", IEEE, Wireless Communications, October 2007
[12] Teerawat Issariyakul, Ekram Hossain "Introduction to Network Simulator NS2" , @ copyright 2009 Springer Science+Business Media, LLC
[13] Dr.S.Tamilarasan," Securing and Preventing AODV Routing Protocol from Black Hole Attack using Counter Algorithm ", International Journal of Engineering Research & Technology IJERT) Vol. 1 Issue 5, July – 2012
[14] Ms. Neetu Singh Chouhan, Ms. Shweta Yadav ,"Flooding Attacks Prevention in MANET", IJCTEE
[15] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003
[16] Akanksha Saini, Harish Kumar,"Effect Of Black Hole Attack On AODV Routing Protocol In MANET",IJCST Vol. 1, Issue 2, December 2010
[17] The NS-2 Network Simulator : http://www.isi.edu/nsnam



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY