# An enhanced approach to secure manet against black hole attack

Yogita Sangwan and Dr. Binod

**ISSN Print:** 2394-7500
**ISSN Online:** 2394-5869
**Impact Factor:** 5.2
IJAR 2016; 2(2): 712-718
www.allresearchjournal.com
Received: 22-12-2015
Accepted: 25-01-2016

**Yogita Sangwan**
Research Scholar,
Deptt. of Computer Science,
Calorx Teachers' University,
Ahmadabad, Gujarat, India.

**Dr. Binod**
Professor, Deptt. of Computer
Science, Calorx Teachers'
University, Ahmadabad,
Gujarat, India.

**Correspondence**
**Yogita Sangwan**
Research Scholar,
Deptt. of Computer Science,
Calorx Teachers' University,
Ahmadabad, Gujarat, India.

## Abstract

The need of Wireless networks has grown to its peak today, as the users want to stay connected irrespective of their geographic position. Mobile Ad Hoc Network (MANET) is a is a system where of arbitrarily moving nodes are connected to form a network resulting in dynamic topology without any centralized control. As a result of this continuous mobility of nodes, interruptions in the ongoing communication are very common. Mobile Ad hoc Network (MANET) security is the key challenge because of its special features e.g. node to node communication, dynamic topology, and open network boundary. It has made it very difficult to control the attacker from disturbing the functions of network. One of the major attack faced by MANET is black hole attack which violates the integrity, confidentiality and functioning of the network by degrading its performance. This attack is very much common in case of AODV protocol which is a reactive (on demand) protocol. This paper explains an improved solution for default AODV protocol which in turn improves security as well as integrity against black hole attack. We have also compared the performances of black hole effected AODV, our proposed AODV and default AODV on the basis of various performance metrics. The metrics analyzed are system throughput, no. of packets send, received and dropped, packet delivery ratio and average end-to-end delay.

**Keywords:** Manet, Aodv, Rip, Rrep, Rreq, Rts, Cts

## Introduction

A mobile ad hoc network (MANET) is a collection of wireless nodes which are able to move freely without having fixed network infrastructure or any centralized control by any base station. Nodes in MANET can act like host as well as router. Host nodes are basically responsible for Processing, creating and maintaining the information while router nodes are multi-functional nodes which are able of searching optimal routes for communication.

Today, MANET is in great demand for applications like emergency, rescue (Where it is not possible to establish a fixed network), military due to its characteristics like self-organization., hop by-hop communications and mobile nodes. As a result of this MANET are highly susceptible to diverse challenges like routing, partitioning into clusters and providing security as per requirement. Among all of these

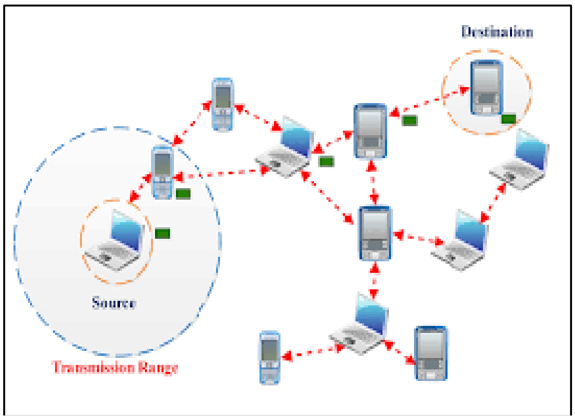

**Fig 1:** Structure of Manet

crucial challenges, security is the most critical one. MANETs are more vulnerable towards an attacker inside the network as due to mobility nodes enters and leaves the network at regular basis.

Among all the major assaults faced by MANET, Blackhole assault is the most acclaimed one. This assault is effective mostly in case of reactive routing protocols such as AODV.

In black hole attack, a malicious node attempts to advertise itself as important so that it has the shortest path to the destination node. This malicious node does not verify its routing table but claims to have the shortest path or fresh route to destination. Because of this attempt attacker node will always claim to have the fresh route and have the availability in replying to the sender for route request. As a result it intercept the data packet and retain it. When the route request is flooded into the network, the reply from the malicious node will be always received by source node before the actual node who is having the optimal path to destination. The route created because of this attempt is malicious and forged. After establishing the route, it is up to the node whether to drop all the packets or forward it to the unknown address. How malicious node fits in the data routes variesas per situation.

A Virtual Carrier Sense shows the concept of an exceptional handshake to "hold" the channel, called the Request To Send (RTS)/Clear To Send (CTS) mechanism.

In this research, our main objective is to improve AODV from blackhole assaults by introducing the concepts of dummy packets and virtual carrier sensing. This paper is divided into various sections that are started by this brief introduction section. in section 2, the concept of carrier sensing range is inroduced which is followed by section 3 consisting desciption about AODV protocol and black hole attack which is the most common attack in AODV protocols. The proposed strategy is given in Section 4. In Section 5, we discuss the proposed algorithm. Section 6 consists of various performance metrices which are used under results. It is fillowed by section 7 which shows simulation environment for analysis. Section 8 discusses the results of our proposed protocols as compared to black hole protocol by taking varying number of nodes. this followed by conclusion which gives the output of this paper.

### Carrier Sensing Range

Carrier sensing is the concept which can Carrier sense various passage by crash avoidance (CSMA/CA) traditions which has been used within the system. There are two segments named as RTS/CTS, which are used to hold virtual carrier sensing concepts. In this, the source at first forwards a RTS message (request to send) and destination response with a CTS. When this process is completed or After that DATA/ACK interchange, adjacent nodes which gets RTS or CTS, that nodes sets their Network Allocation Vector (NAV).This NAV is set in order to secure the channel for the coming DATA/ACK channel. As a result, whenever a node wants to transfer, it firstly ought to sense the channel before transmission for identifying the current status. If it detects a abnormal channel, it has to leave the communication so as to maintain a strategic distance from or diminish crash. An abnormal or bustling channel is identified when the detected energy of the flag overflows the a particular limit or Carrier Sense Threshold (CST). On the other hand if the flag power is appropriate to this limit, the channel is considered to be a sit still channel.

### Black hole attack in AODV Protocol

Adhoc networks are very much susceptible to attacks because of the number of distinct features they have. An ad-hoc routing protocol is a standard or a way of communication, which is having the responsibility of selecting particular route for sending the packets between computing devices. AODV is one of the common protocols which is used for mobile ad-hoc networks in order to communicate successfully. As the name suggests AODV is an on-demand routing protocol. It creates a route only when there is a demand from mobile nodes who wants to send some data to required destination in the network.

In this AODV approach, every mobile node maintains a routing table which keeps the information about the routes and neighbors with in the network. This routing table is used to find its Next Hop Node to the destination. Whenever any node wants to send some packets to a destination, it first check the entries in its routing table in order to confirm the route if exists. If this source node has a route which is the freshest, it will transmit packets through existing path. Otherwise, It finds a route by transmitting two types of control packets which are: Route Request (RREQ) and Route Reply (RREP).

Route Request (RREQ) ⟶

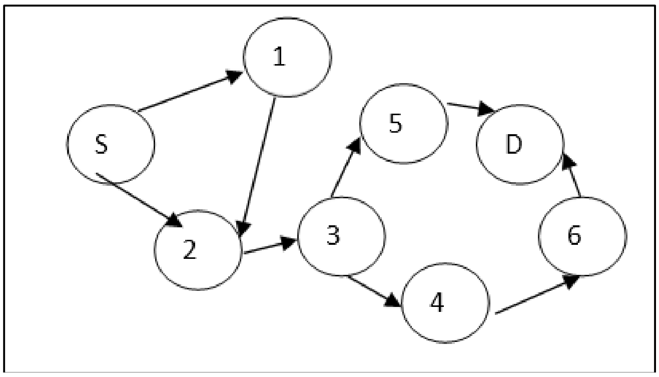

**Fig 3.1:** RREQ Packet Floods in Network

**Route Reply (RREP)** ◄┈┈┈┈┈┈◆

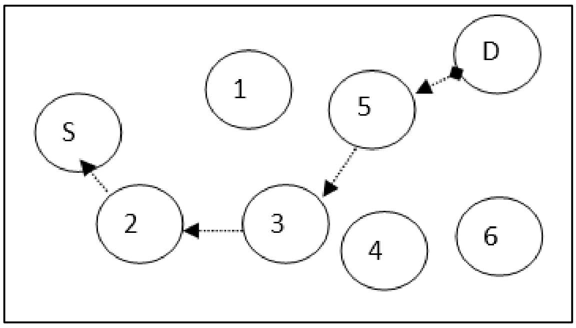

**Fig 3.2:** Unicasting of RREP Packet

Black hole attack is considered to be the crucial one and the most effective assault for AODV protocol as per its working. In black hole attack, a malicious node attempts to advertise itself as important so that it has the shortest path to the destination node. This malicious node does not verify its routing table but claims to have the shortest path or freshest route to destination. Because of this attempt attacker node will always claim to have the fresh route and have the availability in replying to the sender for route request. As a result it intercept the data packet and retain it. When the route request is flooded into the network, the reply from the malicious node will be always received by source node before the actual node who is having the optimal path to destination. The route created because of this attempt is malicious and forged. After establishing the route, it is up to the node whether to drop all the packets or forward it to the unknown address. How malicious node fits in the data routes variesas per situation.

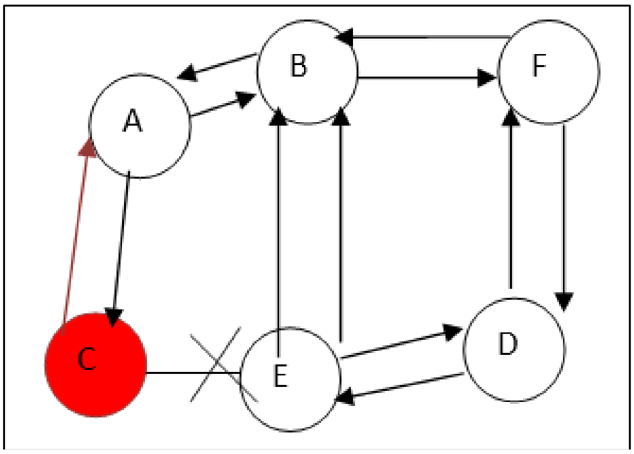

**Fig 3.3:** Black hole problem

Fig. 4.1 showsblack hole problem arised, node “A” is the source node which wants to send data transmission packets to node “D”(which is the destination node). Node “A” initiate the route discovery process in which route request packets are flooded. Node “C” is a malicious node then it will claim that it has an active route (which is the most fresh one) to the specified destination as it receives RREQ packets. It will then send the RREP (which is the reply massege) to node “A” before any other node. As a result of this node “A” assumes it is as an active route and think it as completion of route discovery process. Node “A” received the RREP from malicious node first so will ignore all other replies. It will start sending data packets to node “C”. In this way all the data packets will be lost, consumed or dropped.

## 4. Proposed Method

The transmission process starts as the source node wants to transmit an information to some destination. The source node at the first, requests for nearest Backbone node for a Requested IP (RIP). After accepting RIP from Backbone node, it responses to source node through any of the idle IP addresses and these idle IP addresses are chosen up hazardly. Along with this source node sends the Route Request (RREQ) for destination as well as for Requested IP (RIP) in order to proceed further.

If Source Node (SN) gets the Route Reply (RREP) for the destination node (this case is the typical case) and not for Requested IP (RIP), it is confirmed that the nearby system region is unaffected from black hole nodes. On the other hand if SN gets a RREP for the RIP, it states that there is a blackhole node in that course and it can harm the further transmission. For this type of condition, the SN is having responsibility of discovery for f blackhole nodes. The SN informs the adjacent of the same nodes from which it has received the RREP to RIP, to go into unbridled mode. Presently the SN broadcasts a false link information packets to the destination. This nearby nodes initiates by observing the packet stream and taking the decision of report. Additionally, these type of nearby nodes are responsible for transmitting the screen message to the next session for these fake information packet and so on. Whenever the checking nodes discovers the effect of presently active nodes, it informs the SN about this specific Intermediate Node (IN). This data is broadcasted all through the system prompting its posting as black hole. After getting the information routing tables are updated accordingly in order to avoid these misfortune nodes.

## 5. Aodv-P Algorithm

This Algorithm is explained in three phases as Source node activity, Intermediate node and Destination node activity and Blackhole removal process.

**5.1 Source Node (SN):** The first attempt of source node is to send a request to BBN (Backbone node) in order to get RIP (Restricted IP). When it gets response from BBN, it directs route request for RIP and destination. This is the time to await RREP so as to proceed further.

**5.2 Intermediate Node/Destination Node:** When this node gets route request, it creates an entry for path with in the routing table for the same node which has sent this request. If this node is the required destination or the path to the destination, it responds to RREQ by sending RREP. This RREP is the response to sender for informing the availability of path. If there is off chance then it just forward this request to the next node which is the neighbor og this node. As it gets RREP, it makes an entry in its routing table and send response in the opposite path. Whenever it gets a request to come in uninhibited mode, it just listen all packets that are concerned to specific IP address in the system and then manages its neighbors for the confirmation of fake or dummy information packets. If it determines false packet that is outstandingly more than typical information packet at a definite node, it educates back the IP of this node.

**5.3 SN on getting RREP (Blackholes Removal process**): If it confirmed, If RREP comes from goal node, the node does the usual working by conveying the information by the path. When RIP gets RREP from any node, it just starts the process of blackhole detection, by forwarding a demand. The input directed by the substitute ways are broken down in order to separate the dark gap. This data is transmitted to all nodes with in the system so as to prompt the renouncement of the Black Holes records and proceed further.

## 6. Parameters to Be Analysed

These are the basic parameters which are analysed in order to get network performance as per number of nodes.AODV-D (Default AODV),AODV-B (AODV with blackhole effect) and AODV-P (proposed AODV) are analysed on the basis of number of nodes**.**

**6.1 Total no. of Packets Send:** Total no. of sent packet is defined as it is one of the performance metrics which tells us the no. of packets that are sent while communicaton from source to destination.

**6.2 Total no. of Packets Received**: These are the packets received by the destination. It is very important performance metric.

**6.3 Total no. of Packets Dropped**: Dropped packets are the packets which are lost during communication. This parameter tells us about the number of packet lost. These packets can be lost in between the route by congestion, route failture and other reasons.

**6.3 Packet Delivery Ratio:** It is the measure of ratio between the aggregate number of data packets received by the destination nodes and the aggregate number of data packets generated by the source nodes. Higher the value of packet delivery ratio proportion higher would be protocol performance.

**6.5 Throughput of network:** It is the rate at which work is done or we can say rate of successful transmission from source to required destination with in the system.

**6.6 Average End to End Delay:** It is the time consumed between the moment of sending of a bit by source node and the moment of its reception by the destination node. It is the sum of all possible delays on the route taken by router to seek the path in the network such as buffering during route discovery latency, queuing at the interface queue, propagation, retransmission delays at the MAC and transfer times. The average end to end delay is measured in milliseconds. Simulation Model

**7. Simulation Environment:** This environment includes 100 nodes which are randomly scattered on 1000m x 1000m area. Simulation Parameters Setting Table shows the initial values of related parameters setting according to the simulation requirements.

**Table 7.1:** Simulation Parameters

| Parameter | Description/Value |
|---|---|
| Simulator | NS-2 |
| Number of nodes | 10,25,50,75,100,150,200 |
| Antenna Type | Omni directional |
| Coverage Area | 1000*1000 |
| Simulation Time | 700s |
| MAC Type | 802.11 Mac Layer |
| Traffic Type | UDP-CBR |
| Routing Protocol | AODV(Reactive) |
| No. of Black hole nodes | 7 |
| Channel | Wireless Channel |
| Max and Min Movement Speed | 1.5, 0.5 |

## 8. Simulation Ressults

### 8.1 Total no. of Packets Received

**AODV-D vs AODV-B**

As we compare the received packets of default AODV and AOBV-B,the graph shows considerable downfall. Due to presence of blackhole effect the number of packets at 10 nodes is nill in case of AODV-B, but it is maximum in case of AODV-D.As we go towards increasing the number of nodes,the packets received falls or we can say the network starts loosing some packets which is not so considerable but downfall happens. In case of AODV-B, no packet is received at nodes 10 and it is maximum at nodes 25 in this analysis. Various other factors are also responsible for this downfall and variations are fluctuated as per moibility. Blackhole nodes are responsible for degrading this parameter as per number of nodes within the network.

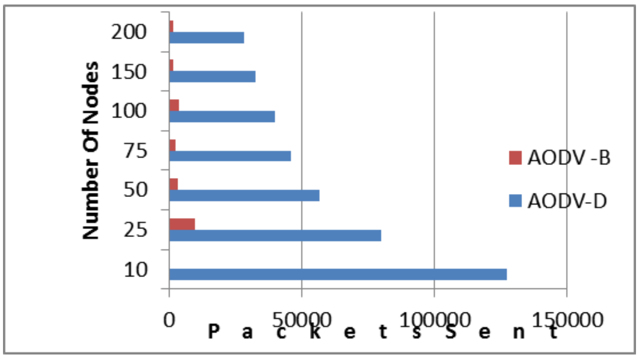

**Fig 8.1 1:** Results Analyses for Packets Received in AODV-D, AODV-B.

**AODV-D vs AODV-B**

The figure showing comparison of AODV-P which is our proposed protocol and AODV-B which is AODV with blackhole effect. AODV-P is having high performance at 10 nodes and as the number of nodes and packets are decreased the trend goes downward or it starts loosing packets. As we compare it with AODV-B, it has very high performance because with blackhole effect at load 10, AODV-B is unable to send anything while AODV-P sends maximum packets. At load 25 the trend shows AODV-P loses some of the packets but trend of AODV-B shows upward direction. This trend again falls till node 75 and increases again at 100 nodes to some extent.In case AODV-P, the graph shows constant downfall or we can say as the number of nodes are increased and packets are decreased, the packets received parameter shows constant downfall.

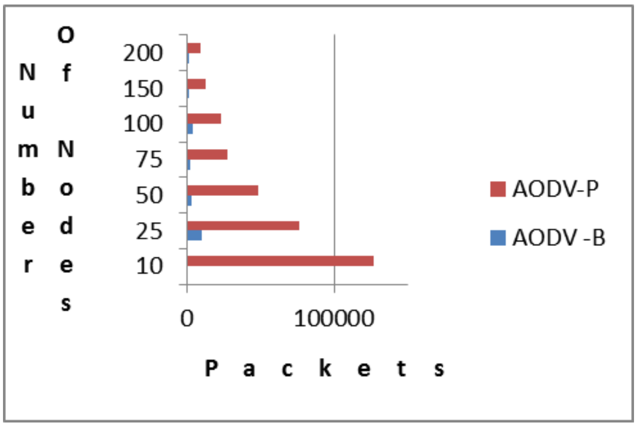

**Fig 8.1.2:** Results Analyses for Packets Received in AODV-P, AODV-B.

### 8.2 Total no. of Packets Dropped

**AODV-D vs AODV-B**

This graph shows the packet drop comparison of AODV-D and AODV-B with the simulation time of 700 and concept of dummy packets and virtual carrier sensing. The trends with in the graph shows AODV-D shows high performance by reflecting negligible packet drop at small number of nodes but as we increase the number of nodes and packets it starts dropping some packets which is maximum at load 200.In case of AODV-B, it drops all packets at load 10 and improves to very little extent as we increase the load. As the number of nodes are increased and packets to be sent decreased, it shows some transmission but very low as compared to AODV-D.

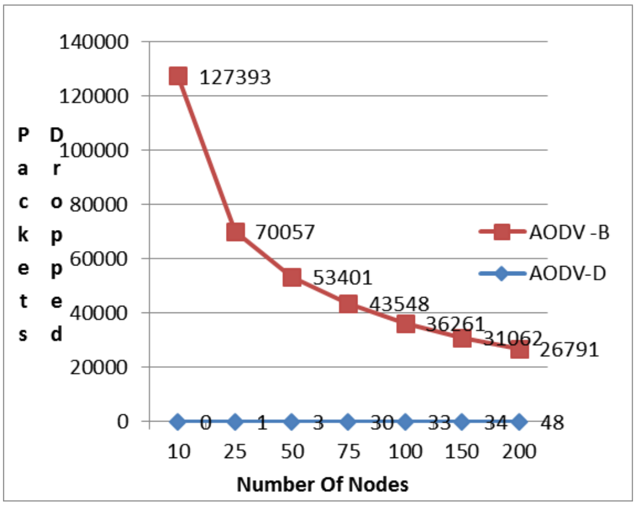

**Fig 8.2.1:** Results Analyses for Packets Drop in AODV-D, AODV-B

### AODV-P vs AODV-B

The figure shows the comparison of our proposed AODV and AODV-B. This analysis shows that packet drop in AODV-P is very small at low load or it is nill at load 10 and 25 nodes. As the number of nodes are increased it starts noticeable drop within the network. This packet drop is maximum at load 200.This type of trend shows that as we increase the number of nodes the performance of AODB-P starts degrading as compared to AODP-B, which shows opposite trend. AODV-B has maximum packet drop at small number of nodes and as the load is increased it starts increasing to some extent.

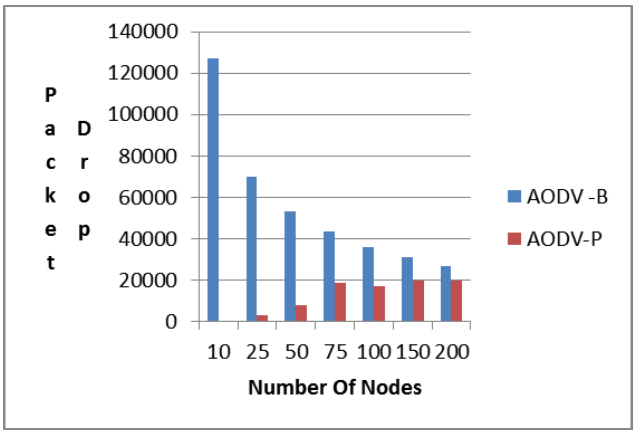

**Fig 8.2.2:** Results Analyses for Packets Drop in AODV-P, AODV-B.

### 8.3 Packet Delivery Ratio AODV-D vs AODV-P

The figure below shows the comparison of AODV-B and AODV-D while taking the concept of virtual carrier sensing and dummy packet. The trends shows constant PDR in AODV-D for small number of nodes and it goes little bit downward as we increase the number of nodes. When we analyse the trend of AODV-B, it shows opposite trend.it is nill at low load and increases to some extent with increase in number of nodes. After some increase, it shows fluctuating behaviour which may due to other factors with in the network.

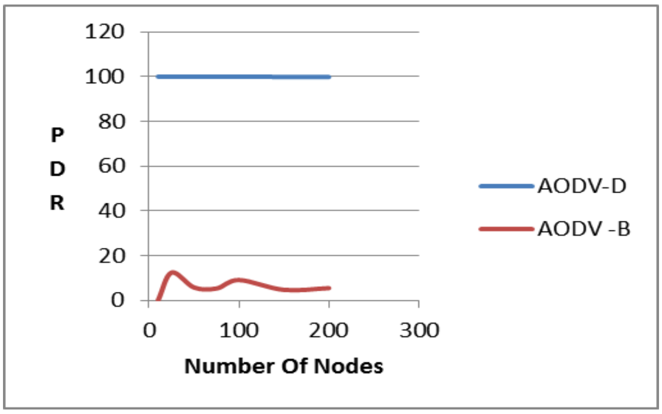

**Fig 8.3.1:** Results Analyses for PDR in AODV-D, AODV-B

### AODV-D vs AODV-P

The figure below shows the comparison of AODV-B and AODV-P while taking the concept of virtual carrier sensing and dummy packet. The trend shows AODV-P is having maximum value at 10 nodes and as the number of nodes increases, the PDR shows downward trend.

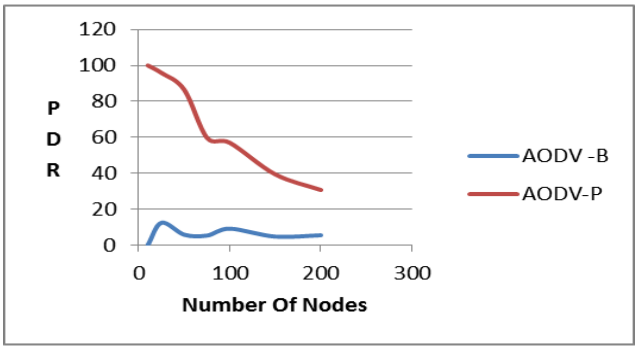

**Fig 8.3.2:** Results Analyses for PDR in AODV-D, AODV-P

This figure shows at load 200, PDR for AODV-P is minimum. When we analyse the trend of AODV-B, it shows opposite trend.it is nil at low load and increases to some extent with increase in number of nodes. After some increase, it shows fluctuating behaviour which may due to other factors with in the network.

### 8.4 Throughput of network

**AODV-D vs AODV-P** The figure below shows the comparison of AODV-B and AODV-D while taking the concept of virtual carrier sensing and dummy packet.

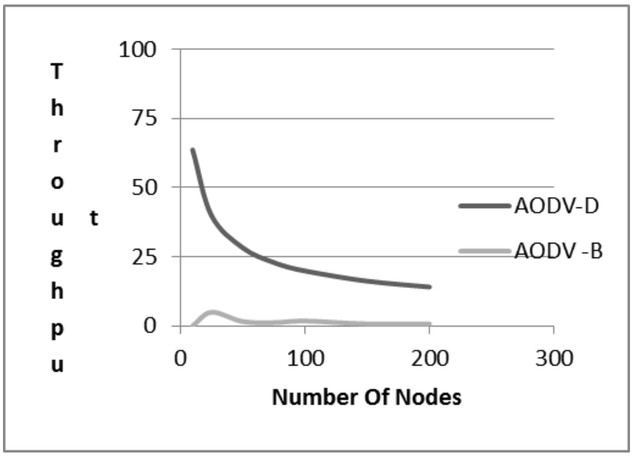

**Fig 8.4.1:** Results Analyses for throughput in AODV-D, AODV-B.

This figure shows throughput for AODV-D is maximum at 10 nodes and starts decreasing as the number of nodes within the system are increased. It is minimum at 200 nodes. As we talk about AODV-B, the throughput is very low at 10 nodes, it starts increasing to some extent in at starting and after 25 nodes it shows fluctuations which may be due to other factors like mobility, scalability and topology.

### AODV-B vs AODV-P

The figure below shows the throughput comparison of AODV-B and AODV-P while taking the concept of virtual carrier sensing and dummy packet. The trend shows maximum throughput for AODV-P at 10 nodes and it shows constant downfall as we increases the number of nodes within the system.

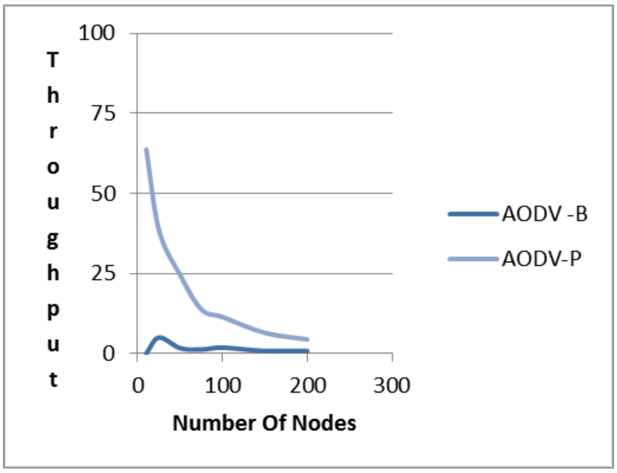

**Fig 8.4.2:** Results Analyses for throughput in AODV-B, AODV-P.

As we talk about AODV-B, the throughput is very low at 10 nodes, it starts increasing to some extent in at starting and after 25 nodes it shows fluctuations which may be due to other factors like mobility, scalability and topology.

### 8.5 Average End to End Delay

Figure 4.26 compares the Average End to End delay for AODV-D, AODV-B, and AODVP during the simulation time period of 700 seconds and the result is being compared during simulation.

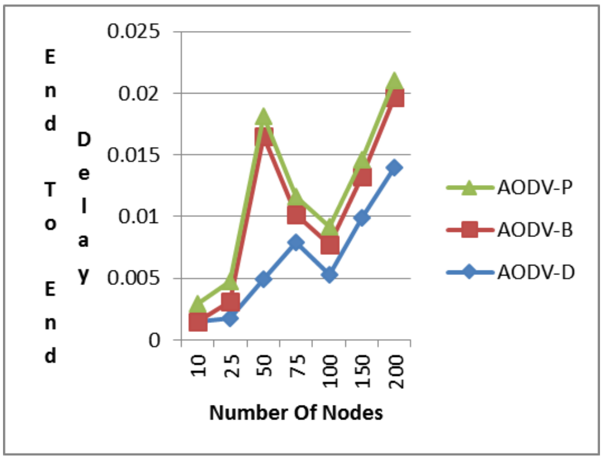

**Fig 4.34:** Results Analyses for average end to end delay in AODV-D, AODV-B,

### AODV-P

The above figure shows that average end to end delay is being increasing with increase in no. of nodes while forwarding data from source to destination but comparatively end to end delay in AODV-P is less than AODV-B. And there is a probability that results can fluctuate in case of AODV-D, AODV-B, and AODV-P with respect to above saying.

### Conclusion

As we know, due to the dynamic behaviour of Adhoc networks, these networks are highly susceptible to various assaults. Hence security has become the biggest challenge for these networks as with growing need. As the topology changes, routing is done on the basis of current status. AODV protocol is a on demand protocol which requests route whenever source wants to transmit data to some destination. This protocol suffers from a crucial attack named as Black hole attack of in which any malicious node diverts the traffic towards it by forwarding fake routing information to the source node. In this paper we have proposed s solution to avoid this blackhole effect on AODV along with selection of optimal path in order to prevent congestion in the system. As per analysis the results of simulations for the proposed AODV shows considerable improvements in packet delivery ratio (PDR) and throughput. The route discovery process is enhancedd by using the concepts of virtual carrier sensing on the AODV routing protocol and concepts of dummy packets. Subsequently, it is clear from the above discussion and analysis that AODV-P is a pure enhancement over AODV-B. It also shows improved performance as compared to AODV-B and control congestion with in the network.

### References

1. Ali Dorri, Alidorri. ce@gmail.com,Soroush Vaseghi Sorouush@gmail.com Department of Computer:" DEBH: Detecting and Eliminating Black Holes in Mobile Ad Hoc Network.
2. Antony Devassy, Jayanthi K. Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting. International Journal of Modern Engineering Research (IJMER) www.ijmer.com 2012 2(3):1017-1021 ISSN: 2249-6645
3. Perkins CE, Royer EM. Ad-Hoc On Demand Distance Vector Routing, Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applictions. 1999, 90-100,
4. David B, Johnson, David A Maltz, Josh Broch. DSR: The Dynamic Source Routing protocol for Multi-Hop wireless Ad Hocnetworks.
5. FIHRI Mohammed, OTMANI Mohamed, EZZATI Abdellah. The Impact of Black-Hole Attack on AODV Protocol: (IJACSA) International Journal of Advanced Computer Science and Applications, Special Issue on Advances in Vehicular Ad Hoc Networking and Applications
6. Aggelou G, Tafazolli, Rdmar. A bandwidth-efficient routing protocol for mobile ad hoc networks". In Proceedings of ACM Mobi-Com99/WoWMoM99, August Washington, USA, 1999.
7. Abusalah L, Khokhar A, Guizani M. A survey of secure mobile Ad Hoc routing protocols, Communications Surveys & Tutorials, IEEE, 2008; 10:78-93.

8. Mahsa Seyyedtaj, Mohammad Ali, Jabraeil Jamali. Different Types of Attacks and Detection Techniques in Mobile Ad Hoc Network. International Journal of Computer Applications Technology and Research 2014; 3(9)541-546, ISSN: 2319–8656.
9. Mohanapriya M, Krishnamurthi I. Modified DSR protocol for detection and removal of selective black hole attack in MANET, Computers & Electrical Engineering. 2014; 40(2):530-538.
10. Parsons M, Ebinger P. Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks
11. Corson MS, Macker J. Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations. RFC 501, 1999.
12. Vaidya N. On physical carrier sensing in wireless ad hoc networks, Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies. 4:2525-2535.
13. Jain S, Jain M, Kandwal H. Advanced Algorithm for Detection and Prevention of Cooperative Black and Grayhole Attacks in Mobile Ad Hoc Networks, Intl. Journal of Computer Applications Feb. Published by Foundation of Computer Science. 2010; 1(7):37-42.
14. Khatri S, Sharma P, Chaudhary P, Bijalwan A. A Taxonomy of Physical Layer Attacks in MANET. International Journal of Computer Applications, 2015; 117(22).
15. Al-Shurman M, Yoo SM, Park S. Black hole attack in mobile ad hoc networks. In Proceedings of the 42nd annual southeast regional conference (pp. 96-97). ACM.
16. Nurul I Sarkar, Wilford G Lol. “A Study of MANET Routing Protocols: Joint Node Density, Packet Length and Mobility 978-1-4244-7755-5/10/$26.00 © IEEE 2010, 515-520
17. Banerjee S, Sardar M, Majumder K. AODV Based Black-Hole Attack Mitigation in MANET, in Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013, 247.
18. Simanta Sarma, Binita Devi. 1(HOD & Asstt. Professor, Department of Computer Science, S.B.M.S College, Sualkuchi, Assam, India): “Security Attacks on Routing Protocols in Ad Hoc Wireless Networks, International Journal of Modern Engineering Research (IJMER) www.ijmer.com 2012; 2(6):4502-4509 ISSN: 2249-6645.
19. Kalwar S. Introduction to reactive protocol," Potentials, IEEE, 2010; 29:34-35,
20. Murthy S, Garcia-Luna-Aceves JJ. An efficient routing protocol for wireless networks, ACM Mobile Networks and Applications Journal, 1996, 183-197,
21. Zhu C Lee, Saadawi MJ. T: “RTT-Based Optimal Selection in Ad-Hoc Routing Protocols,” Conference, 2003; 2:1054-1059.