International Journal of Recent Trends in Engineering & Research
ISSN : 2455-1457 Impact Factor : 3.344

# Appraise of Mobile Coverage Problem and Black Hole Attack in MANET Using NS2

Samina Chikode[1], Sarita Molake[2], Swapnali kamble[3], Pradip chougule[4]
[123]*Computer Science and Engineering, Dr.J.J.Magdum College of Engineering, Jaysingpur-416101.*
[4]Assistant professor,Department of computer science and Engineering,Dr.J.J.Magdum College of Engineering,Jaysingpur.

**Abstract:** We examine a very common problem of mobile network that is out of coverage problem. To examine this problem we use common simulator NS2.A wireless Ad hoc network is a temporary network set up by wireless mobile nodes with less infrastructure. This leads MANETs are more vulnerable to various communication security attacks. One of the main active attacks is Black hole attack, it is a denial of service attack and it drops entire incoming packets between one source to destination. The attempt is to focus on analyzing and strengthening the security of routing protocol Ad hoc On Demand Distance Vector (AODV) for MANET.Our simulation result are end-to-end delay, packet dropping, throughput of packet dropping ratio are justify that black-hole attack are observed**.**

**Keywords**:AODV, Base station, Black hole attack, MANET, NS2, UDP, Mobile nodes.

## I. INTRODUCTION.

In this paper, we examine a very common problem of mobile network that is out of coverage problem. To examine this problem we use a very common simulator NS2 among various simulators. As we know that Mobile phones communicate through a system radio waves, antennas and towers. All mobile phone depend on radio waves and radio waves travel through air. In radio transmission mobile calls can be interrupted by various buildings, weather, mountain and other objects within your and nearest mobile tower. Various reason that disturb the completions of a call. Even when a carrier offers coverage in a certain geographical areas, we may not able to complete a call due to limitations in network architecture, capacity, and topography. A network that does not contain wire is known as wireless network. Mobile network problem i.e. out of coverage problem is occur because the mobile nodes are not present in the geographic area and packet send by one node other node through base station as intermediate are not get to the node these packets are dropped. Because the node is not present base station geographic area and how this happen in mobilenetwork we demonstrated by using wireless simulation model by using NS2 as tool[1].

On other hand there has been tremendous growth in the use of wireless communication over last decade. MANET is a collection of wireless mobile nodes that can communicate with each other by point to point transmission type. Due to the limited transmission range, multiple hops are essential for one node to communicate with faraway node in the network. In such a network each mobile node act as a host as well as a router, receiving and forwarding packets for other mobile node that may not be within transmission range of each other. MANET is an infrastructure less network, used in battlefields, military, emergency and disaster such as search and rescue .Mobile Ad-hoc networks are a collection of mobile hosts that communicate with each other without any infrastructure. Because of security vulnerabilities of the routing protocols, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. Absence of fixed base station in MANET makes many security issues thanconventional wireless network. Because of MANET uses open airmedium, continuously changing topology, absence of central administration, multi-hop routing and distributed cooperation, is vulnerable for several types of attacks. One of the main active attacks is Black hole attack which takes place in network layer. In Black hole attack, a malicious node or group of malicious node drop

the entire packets between sources to destination. In this attack a malicious node advertises itself as having the shortest path to specific node to absorb packet to it. In this attack, a malicious node sends a false RREP packet to a source node that initiated the route discovery, in order to pose itself as a destination node or an immediate neighbor to the actual destination node. In such a case, the source node would forward all of its data packets to the malicious node, which originally were intended for the genuine destination. The malicious node, eventually may never forward any of the data packets to the genuine destination. As a result, therefore, the source and the destination nodes became unable to communicate with each other.

In this paper, we attempt in analyzing and upgrading the security of the AODV routing protocol against Black-hole attack. AODV is an on demand, dynamic routing protocol and consumes less bandwidth than table driven protocol. Protecting against Black hole attack, additional commands are included in AODV. Our proposed method is a PL2 method is a combination of postlude and prelude control messages. Source based detection method is used to mitigate the Black hole attack is possible by customizing the original AODV. The simulation is done in ns2[2].

### 1.1 Mobile network

A network of two or more mobile devices with a single base station is known as mobile network. In this network, mobile can communicate each other if they are in the radio signal coverage area of the existing base station. The coverage area or boundaries of an access point or base station is known as a cell. A mobile network is also known as cellular network. A mobile network with one base station and two mobiles are illustrated in figure 1. Mobiles are communicate only when both in the coverage area of base-station. Otherwise they give coverage problem[1].

***Figure 1.Mobile network***

### 1.2 Wireless simulation model

A network of two or more mobile devices with a single base station is known as mobile network. In this network, mobile can communicate each other if they are in the radio signal coverage area of the existing base station. The coverage area or boundaries of an access point or base station is known as a cell. A mobile network is also known as cellular network a mobile network with one base station and two mobiles are illustrated in figure 1. Mobiles are communicate only when both in the coverage area of base-station. Otherwise they give coverage problem.

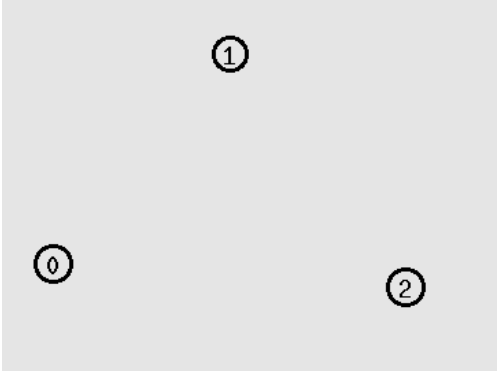


*Figure 2.Nam output window*

### 1.3 Ad hoc on demand distance vector routing protocol

As the name describes AODV forms the route from source to destination and between the intermediate nodes when there is demand for forwarding packets using MANETS. AODV (Ad-hoc On-demand Distance Vector) is a reactive routing protocol, yet it is fundamentally an improvement of DSDV routing protocol which is proactive protocol. Route discovery process takes place only when required. AODV can handle low, moderate, and relatively high mobile rates, together with a variety of data traffic loadings. However, it makes no provisions for security. In Route Discovery Process of AODV there are three types of messages: Route Request (RREQ), Route Reply (RREP), and Route Error (RERR) messages. RREQ-It is basically the broadcast request to find the route to a required destination node. Thus it helps to create a route discovery process by broadcasting Route Request message to its neighboring nodes. The neighboring nodes save the path where RREQ request is transmitted.After that it verifies the new or fresh route to the desired node in the routing table by the use of RREQ request .RREP- when the node finds a fresh path for destination then a route reply message is unicasted to the originator of the RREQ if the receiver is either the node using the requested address or is having a valid route to the requested address.RERR-it helps to keep eye on link status of the next hop in the appropriate route. RERR message is broadcasted to whole nodes whenever the breakage in the link is found. This is also called route maintenance.

| Source Address | Request ID | Source Sequence number | Destination Address | Destination Sequence Number | Hop count |
|---|---|---|---|---|---|
| | | | | | |

*Fig 3.RREQ format[2]*

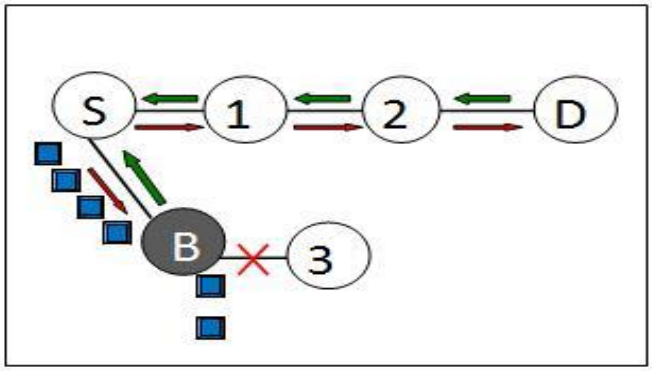
| Source Address | Destination Address | Destination Sequence Number | Hop Count | Life time |
|---|---|---|---|---|
| | | | | |

*Figure 4. RREP format[2]*

Each mobile node in the network can get to know its neighborhood by using periodic HELLO messages. HELLO messages are used to inform the neighboringnode that the link is still alive and never be forwarded [2].

### 1.4 Black-hole attack

The Black Hole attack is a powerful attack in MANET. In this Malicious Node attract all traffic by claiming the route to the destination which then absorbs the packets without forwarding them to the destination. Co-operative Black hole means the malicious nodes act in a group. The attacker injects falsified routing packets to attract traffic. The attacker intercepts or drops control as well as data packets to deny services to authentic nodes. This attack can be prevented by establishing routes free of such nodes or by removing them from existing routes



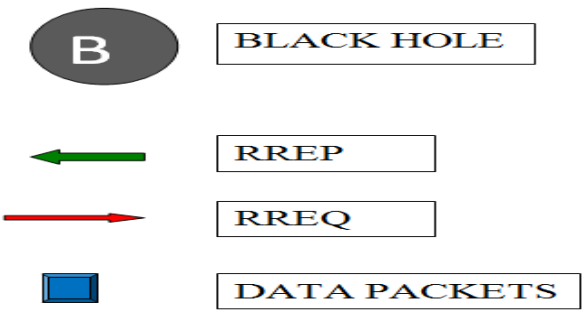



*Figure 5. Black hole attack [2].*

For example node S wants to send data packets to destination node D in Fig. 5 and initiates Route Discovery process. Malicious node B claims that it has shortest path to the destination, whenever it receives RREQ packets. So that Source node think that Route discovery process is completed and ignore all other RREP messages, begin to send packets over malicious node B.As a result all packets send through Black hole node B are simply lost or drop or send to unwanteddestination. Since our case of study is the AODV protocol, we will see how a malicious node can make a success of its attack in AODV.

Two kinds of black hole attack can be distinguished:

• Internal black hole attack: The malicious node is an internal node which does not seek to fit in an active route between a given source and destination, and if the chance would have it, this malicious becomes element of an active data route, it will be able to conduct its attack as the transmission of the data starts.

• External black hole attack: The malicious node is an external node which seeks to fit in an active route [2].

## II. PROPOSED METHOD.

### 2.1 Parameter require for simulation

| Parameter Name | Value |
|---|---|
| NS Version | NS2 |
| Channel | Wireless Channel |
| Propagation | TwoRayGround |
| Network Interface | WirelessPhy |
| Antenna | OmniAntenna |
| Interface Queue | DropTail |
| Routing Protocol | AODV |
| Transport Protocol | UDP |
| Packet Size | 1000byte |
| Transmission rate | 1Mbps |
| Mobile Speed | 150 m/s |
| Simulation Time | 20 sec |
| CBR start at node 0 | 0.0 sec |
| CBR stop at node 0 | 15.0 sec |
| Node 2 start move towards AP | 1.0 sec |
| Node 2 move away from AP | 2.5 sec |

*Table 1. Simulation parameters [1]*

### 2.2 Experimental analysis

Whenever we start simulation, CBR also start the transmission of data packets from the node 0 as a source node. Heredata packets of node 0 cannot send directly to the destination node 2 that can access the data packets or radio signal through access points i.e. node1. It means source and destination (i.e. node 0 and node 2) can communicate through access point (i.e. node 1).when node 2 move towards the base station we will find packet transmitted from source to destination node through base station or access point shown in figure 6 below. When after 2.5 seconds node 2 move away from access point and reach out of access point range allpackets are dropped at node 1 and base station/access point is not able to transmit packets that are coming from sourcenode to destination node. We can see these in figure 7.

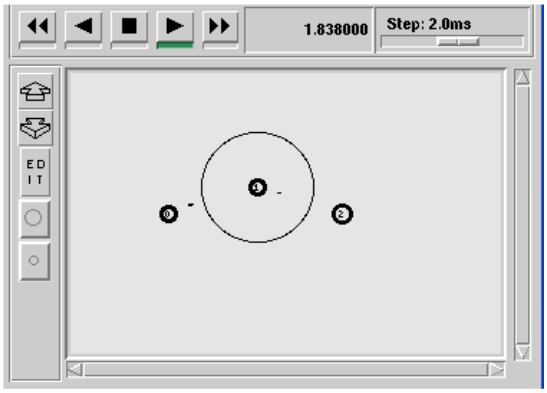



***Figure 6. Packet transmission***

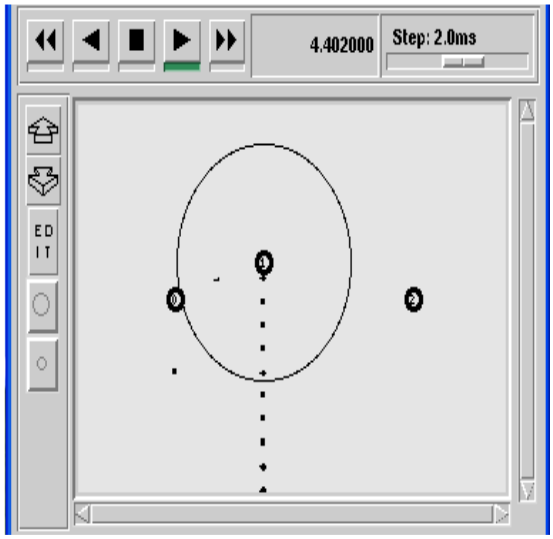



***Figure 7. Packet drop***

So from this wireless simulation model we know that packets send by source node are dropped because destination has reach out of access point range this is the one reason where source and destination cannot communicate with each other. Other reason is when malicious node is present in the mobile network that we have discussed below.

PL2 method is Prelude, Postlude method. The proposed solution is an enhancement of the original AODV routing protocol to find a secure routes and prevent Black hole attack on MANET. The Major concept is based on time and neighborhood parameters. Thismethod first check for malicious activity exists, and then starts detect and remove the Black hole nodes. Route discovery is same as original AODV, but when sending data packets, prelude and postlude messages are added[2].

### 2.3 Detection of black hole activity

Initially, data packets are divided into equal parts as Data (1… K) Where K=ceiling of (n/w).Where n is the number of data and w is the window size. Apart from the source, destination, some intermediate nodes are assigned as monitor nodes, given powers to overhear data packets and watching other intermediate nodes. After Route Discovery process, monitor(S, D, and NNR) nodes are broadcasted to all other NNR-Next Nodes in the Route. Source node sends prelude (S, D, ni) message with every equal block of data and waits for special type of acknowledgement as postlude (D, S, d_count) message from destination node after receiving data. ni is the number of data in particular block i and d_count is the number of data received by destination node. If source node not receive postlude message within timeout period TS, malicious activities are confirmed in the network. Windowing mechanism is used to reduce the end to end delay and data loss. Detailed processes are as shown in flowchart Fig.8 [2]

### 2.4 Black hole removal process

In Black hole removal process, source node sends query BQ (S, D, NRREP, ni) to monitor node to find out malicious node. NRREP is the ID of the node sending RREP to source. In response monitor nodes sends back result to source node. If source node receives result before a particular time TRES, predicted that the particular monitor node itself is a malicious node. So Source node depends on other monitor node's results to build a secured path. Based on monitor nodes result, source node starts votecount. Votecount is a count, for not forwarding the data packets of the particular node, when it receives from other node. Ifvotecount of the particular node is greater than the threshold value, the source node confirms that the node as a Black hole node and will be listed in Blacklist. Threshold value is a variable depends on the size of the network. As source node knows the location of the Black hole nodes, it ignores the RREPs from these nodes. The flow chart for detailed process is as shown in Fig.8

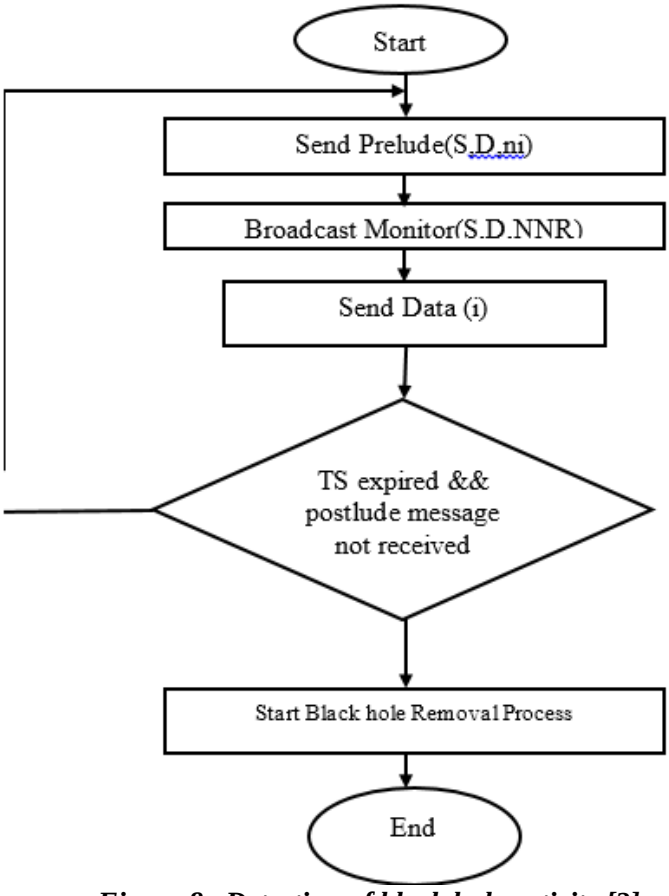



*Figure 8. Detection of black hole activity [2]*

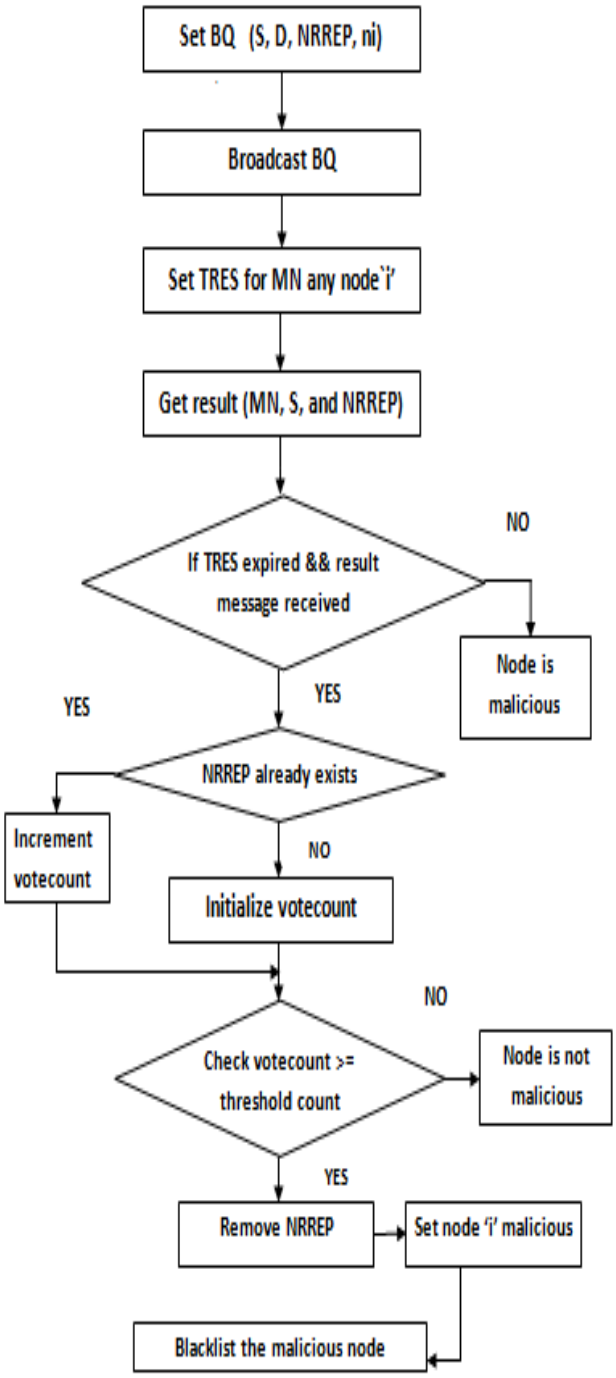



***Figure 9. Flow chart for black hole removal[2]***

## III. SIMULATION AND ANALYSIS.

The simulation has been carried out using NS-2.35. In ns2, two languages are used, tcl-tool command language as front end and c++ as back end .The user writes in tcl script, are interpreted by network simulator and givetwo output files. They are NAM andtr trace files.NAM is for visual animation of output and tr is the large text trace file consists of simulation Results. In this simulation 30 mobile are considered in the terrain area of 1000x1000. Malicious activity in the network is assumed as 10% i.e. 3 Black hole nodes are included in the simulation. Simulation parameters are

considered as shown in the Table.1 Performance of AODV can be analyzed by different simulation metrics such as end to end delay, packet delivery ratio,throughput and etc.

| Parameter Name | Value |
|---|---|
| AREA | 1000*1000 |
| Simulation Time | 50 S |
| Number of Nodes | 30 |
| Traffic Model | CBR |
| Protocol | AODV |
| Number of Attackers | 3 |
| Drop Rate | 2 Mbps |
| Packet Size | 512 bytes |

***Table 2 Simulation parameters [2]***

### 3.1 Packet delivery ratio

It is a ratio of total number of packets received by the destination node to the total number of packets sent by the source node. PDR simply describes the level of delivered data.

$$PDR = \frac{\Sigma \text{ Number of data packets received}}{\Sigma \text{ Number of data packets sent}}$$

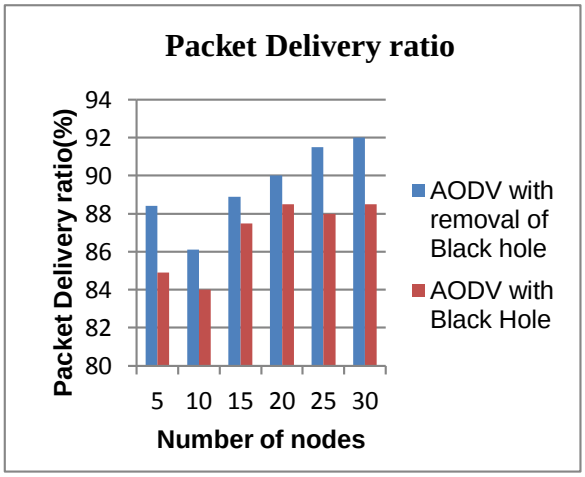



***Figure 10. Packet delivery ratio[2]***

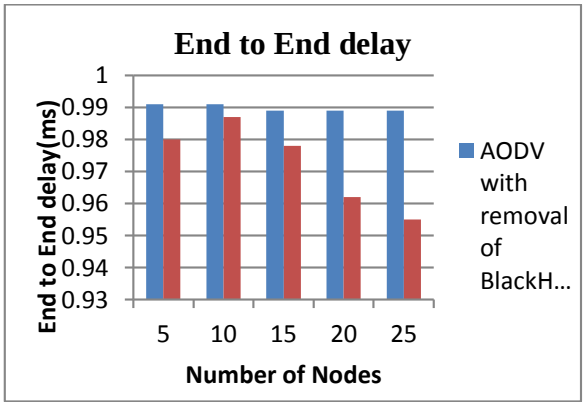



*Figure 11. End to end delay [2]*

In fig.10 shows that PDR of the proposed PL2 method is higher than AODV with Black holes. As Black holes induce packets drop, the PDR of original AODV decreases with increase in number of nodes.

### 3.2Average end to end delay

It is the average time taken by the data packets travel from source to destination. This includes all types of delay caused by buffering of data, Route Discovery latency, queuing, processing at intermediate nodes, retransmission delays, propagation time and etc .End to End Delay=Σ (arrival time - send time) End to End Delay must be low to get better performance of AODV.

### 3.3 Throughput

The number of bits received over the time difference between the first and the last received packets. Throughput graph is plotted by varying number of nodes. Presence of malicious node in MANET is degrading the performance of AODV.

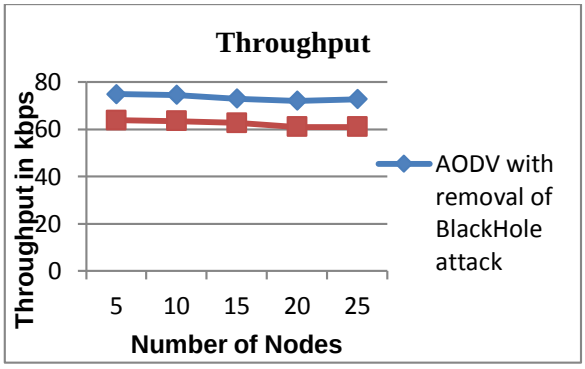



*Figure 12. Throughput [2]*

### 3.4 Drop rate

Total dropped packet for routing : total packet sent**.**

### 3.5 Routing Overhead

Total number of routing packet transmitted.

### 3.6 Normalized routing load

Total number of routing packet: total received data packet.

## IV. CONCLUSION

We summarizes the out coverage problem occur due to out of range of source and destination from base station or access point. An access point or base station sends or receives packets or signals only when they are available in their range otherwise all packets or signals are dropped. We have also analysed the Black hole attack with respect to different performance parameters such as end-to-end delay and packet delivery ratio. We proposed PL2 method.PL2 is a source, neighbour, and time based and modified AODV routing protocol to mitigate Black hole attack. We simulated our proposed solution using ns-2 and compared our modified AODV with original AODV in terms of packet delivery ratio, end to end delay and throughput. Simulation results show that theproposed method has good performance against Black hole attack and not much overhead. This solution holds good for grayhole attack also. In our future work, we may propose a feasible solution which will strengthen original AODV against cooperative Black hole attack.

## REFERENCES.

I. Ajay Singh and Dr.PankajDashore" Mobile Coverage Problem Analysis by using NS2"2013
II. Vasanthavalli.S, R.Bhargava Rama Gowd, Dr.S.Thenappan"Peruse Of Black Hole Attack and PreventionUsing AODV on MANET"2014.
III. AshikurRahman, PawelGburzynski, "Hidden Problems with the Hidden Node Problem", 23rd Biennial Symposium on Communications.
IV. Pommer, Hermann,"Roamingzwischen Wireless Local Area Networks", VDM Verlag, Saarbrücken 2008, ISBN 978-3-8364-8708-5.
V. C. Rama Krishna, "STTP on Wireless Communication ", 2009.
VI. Homgmei Deng, Wei Li and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Networks", IEEE communication Magazine, vol.40, no.10, pp.70 -75, October 2002.
VII. A. Baadache,andA.Belmehdi, "Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks", International Journal of Computer Science and Information Security,vol.7,no.1,2010.
VIII. Sun B, Guan Y, Chen J, Pooch UW, "Detecting Black-hole Attack in Mobile Ad Hoc Networks", 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, . 22-25 April 2003.