Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777698

SIMULATION AND ANALYSIS OF BLACK HOLE ATTACK IN MOBILE ADHOC NETWORK BASED AODV ROUTING PROTOCOL WITH VARYING NODE SPEEDS

Rupanshi Agarwal [1], Akash Sanghi[2]*, Gaurav Agarwal[3], Pragati Jain[4]
[1](Research Scholar (M.Tech.), Dept. of CSE, FOET, Invertis University, Bareilly, (U.P), India)
[2](Assistant Professor, Dept. of CSE, FOET, Invertis University, Bareilly, (U.P), India)
[3](Associate Professor, Dept. of CSE, FOET, Invertis University, Bareilly, (U.P), India)
[4](Research Scholar (Ph.D.), Dept. of CSE, FOET, Invertis University, Bareilly, (U.P), India)
rupanshi.a@invertis.org, akash.s@invertis.org*, gaurav.a1@invertis.org, pragatimpi6@gmail.com

Abstract: Mobile Ad Hoc Networks (MANET) has become an interesting technology due to the rapid development of wireless devices. The enormous growth and development accompanying the widespread use of the Internet has also raised concerns about the protection and transmission of digital data. Manets consists of endless list of mobile nodes. Dynamic topology and decentralized nodes are key features of MANETs. These features make MANETs vulnerable to several attacks. One of the important routing protocols used in ad hoc networks is the AODV (Adhoc on request Distance Vector) protocol. The security of the AODV protocol is compromised by a type of attack known as a "blackhole attack”. By sending a fake route in a blackhole attack malevolent nodes obstruct transfer of information.

This paper analyses the performance of AODV protocol with solo blackhole attack and co-operative blackhole attack. Different scenarios are framed with varying speed of nodes. The parameters for evaluation are packet delivery ratio, throughput and end to end delay. Tool used for simulation is Network Simulator (NS2).

Keywords— Ad Hoc Networks , AODV, Blackhole attack, PDR, Throughput, End to End delay

1. INTRODUCTION

The term 'ad hoc network' refers to autonomous nodes that are not structured and modify their own configuration [1, 2]. The mobile ad-hoc network is made up of independent movable nodes operating in a decentralized manner; and coordinate with each other to ensure communication between source node and target node [2, 3]. These networks can be readily and quickly set up at a cheap cost without the need for any form of fixed infrastructure such as a base station, which is required when establishing a cellular network [4], [5]. It enables multi-hop communication via the intermediary node, which is critical in establishing a communication link between the source and destination nodes as well as in forwarding data packets.

These are self-organizing, ad hoc and infrastructure-free networks [1]. MANET is a collection of mobile devices communicating with each other when inside wireless range directly from each other or through intermediaries [2]. The nodes in MANETs have limited processing power due to their small size, small memory and low computing power [4]. Each network node serves as both a host and a router. To connect with other nodes, network layer protocols such as AODV, DSR, and others are commonly used, which aid in determining the best path between the source and destination nodes. As a result, while discussing such networks, attacks such as blackhole, wormhole, sybil, and flooding attacks make mobile nodes vulnerable to them. A blackhole attack is one in which an existing renowned node seizes packets and drops them throughout the routing process, resulting in protocol performance degradation.

The rest of the paper is organized as follows: Section 2 describes the background of routing in manet and provide a thorough discussion about AODV. Section 3 gives brief introduction of blackhole attack in MANETs. Section 4 showcase the various parameters to be considered for analysis and evaluation of blackhole attack and also explain the random way point model using NS2. Section 5 presents the comparative simulation results of AODV protocol without blackhole attack, with solo blackhole attack and with co-operative blackhole attack based on the three parameters: PDR, throughput and end to end delay. Section 6 provides the conclusion and Section 7 describes the future scope.

2. BACKGROUND

This section gives an insight into the important factors which are required to be known for understanding the concept discussed.

2.1 MANET

The operation of a MANET typically begins with the source sending a request packet in search of the shortest path to the destination to be discovered [4]. The routing path contains all nodes that have a path to the destination and defines two parameters- hop count and destination sequence numbers which are included in route reply packets.

2.2. Categorization of Routing Protocols

Manet is divided into three main routing protocol categories [3] as shown in Fig.1.

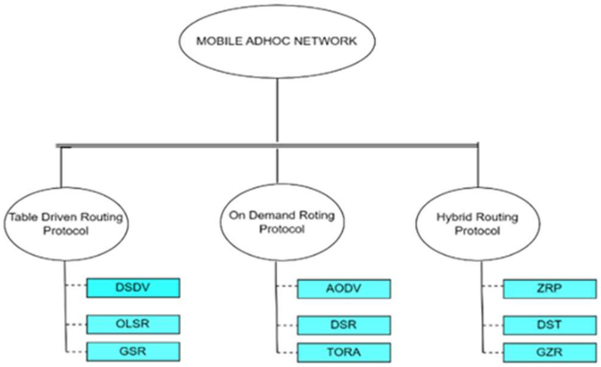


Fig. 1: Categorization of Routing Protocols

(i) Table Driven Routing Protocol

This protocol is also known as the proactive protocol since it requires all mobile nodes to update their routing tables whenever the topology changes [5]. This protocol needs regular maintenance of routing information but has the advantage of minimal latency and quick detection of black hole assaults. This type of approach is followed by protocols such as Optimized Link State Routing (OLSR), Destination Sequenced Distance Vector (DSDV), and others. These protocols are not suitable for storing full routing information in huge structures.

(ii) On Demand Routing Protocol

This protocol is also known as a reactive routing protocol since it only stores the routing table information when the path from the source node to the sink node is required [4], [5]. It surpasses proactive protocol because it is more scalable and has lower overhead, but it has a longer delay. This type of protocol includes AdHoc On-Demand Routing Protocol (AODV), Dynamic Source Routing (DSR), Temporally Ordered Routing (TORA), and others [6].

(iii) Hybrid Routing Protocol

This protocol combines aspects of both table-driven and on-demand protocols in that it initially stores routing table information and updates it if there is a change in network structure, thereby splitting the network into zones [5]. This method is followed by protocols such as Zone routing protocol (ZRP), BGR, ZHLS, DST, and others.

2.3 AODV Protocol

AODV is a reactive routing protocol that is commonly used in MANETs [7], [8]. It only establishes a path to the destination node when necessary, and no route is built until the node delivers the route discovery message as intended for data transmission [3]. Routing information is only saved in the routing tables of the active routing path's originating, destination, and intermediate nodes. The protocol's manner of operation saves network resources like memory overhead and works well with high mobility [9]. The discovery, establishment, and maintenance of routing paths are the three major processes involved in AODV. To conduct the algorithm, AODV comprises of three types of control messages [3], [10].

– Route Requests (RREQs)
– Route Replies (RREPs)
– Route Errors (RERRs)

One of the important elements of AODV is the serial number, which ensures the freshness of routing. To avoid routing loop formation, each node keeps its unique serial number. When the originating node wishes to communicate with the destination node, it starts the route discovery process.

The originating node's sequence number plus one for each route start step, and then the originating node broadcasts RREQ to all available neighbours [1]. The route request packet will be checked by the intermediate node that receives the RREQ. If the intermediate node is the destination node, it will update its own sequence number (intermediate node sequence number plus 1 and RREQ destination sequence number, whichever is greater) and then respond with an RREP [1], [4]. If the intermediate node is not a destination node but has a route to the destination node and the destination sequence number is greater than the destination node sequence number in RREQ, the intermediate node responds with an RREP. Otherwise, the originating node's RREQ will be transmitted to other neighbouring nodes. Each intermediary node will record the broadcast identification and the address of the node that delivered the RREQ before transmitting the RREQ in order to preserve the list of predecessor nodes.

When the intermediate node does not get an RREP for the preceding request for an extended length of time, it deletes the previously saved entry. If an RREP response is received, the intermediate node will store the broadcast identity as well as the next hop route. The broadcast identification and destination node IP address are used to determine whether the node has already received the RREQ, preventing the same node from getting redundant routing requests [4]. When the originating node receives multiple RREP responses, it chooses one depending on the number of hops and the sequence number. The RREP with the highest sequence number and fewest hops will be chosen. As shown in Fig. 2, the source node S receives the RREP send by all the other nodes to have the routing path i.e S-C-E-F. Some nodes will become unreachable if linkages collapse due to node movement. When their neighbour nodes identify interrupted nodes via the HELLO packet, an RRER is formed that store all of the missing destination addresses.

In order to retain route path information, these neighbour nodes send RRERs to the necessary nodes. If the originating node still needs to send a message to the interrupted node, the route discovery procedure will be restarted. Fig. 2 depicts the RERR transmission mechanism [3]. When node D's link fails, its neighbour node C will transmit an RERR to its upstream node.

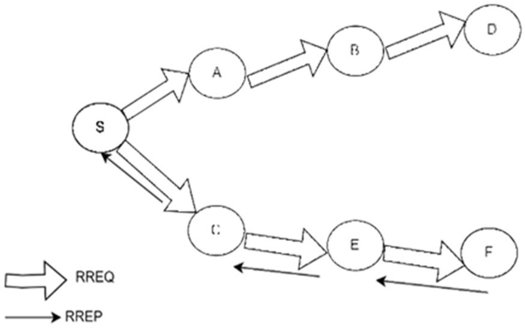


Fig. 2: Example of Route Discovery

A flowchart depicting the movement of control messages in AODV protocol is shown in Fig. 3.

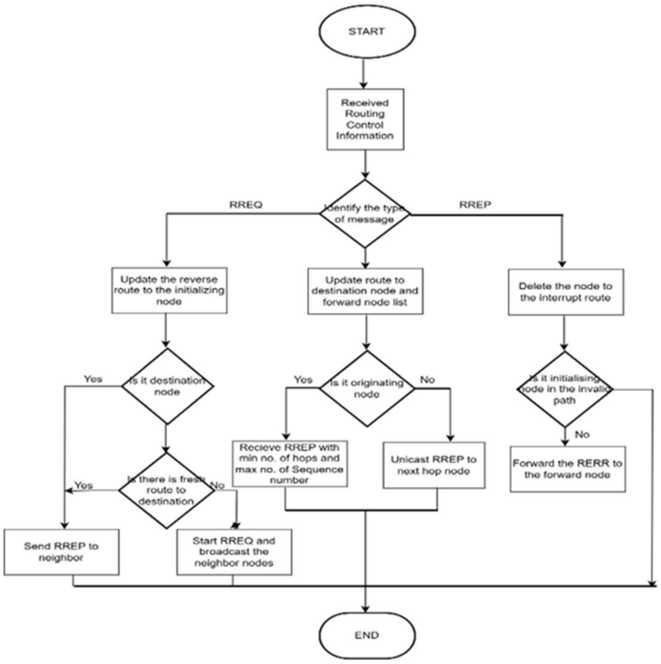
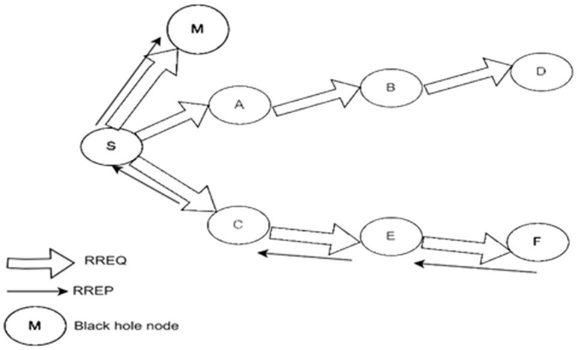

START
Received Routing Control Information
Identify the type of message
RREQ
RREP
Update the reverse route to the initializing node
Update route to destination node and forward node list
Delete the node to the interrupt route
Yes
Is it destination node
Yes
Is it originating node
No
Is it initialising node in the invalid path
No
Recieve RREP with min no. of hops and max no. of Sequence number
Unicast RREP to next hop node
Forward the RERR to the forward node
Yes
Is there is fresh route to destination
No
Send RREP to neighbor
Start RREQ and broadcast the neighbor nodes
END

Fig.3: Flowchart of control messages in AODV

3. BLACKHOLE ATTACK

The Blackhole Attack is one of the most serious routing attacks in MANET [11]. Upon receiving the RREQ, the blackhole node immediately sends a malicious RREP that sets the destination node serial number to a maximum and the number of hops to a minimum, claiming to have the latest and shortest path to the destination node [12], [13]. Because the blackhole node does not even query its routing table, it is usually the first node to respond to the RREQ. As a result, all packets sent to the blackhole node are absorbed by it without being forwarded to the destination node, acting as a blackhole in the network [10]. The Blackhole Attack disrupted network communication, resulting in a sharp decline in overall network performance [13], [15]. An example of a blackhole attack is shown in Fig. 4.



PDR= (Σ(Total packets received by all destination node))
(Σ (Total packets send by source node))

Fig. 4: Example of blackhole attack

The node S broadcasts the RREQs in order to locate the target node F. The RREQ is received and continually broadcast by the normal intermediate nodes A, B, C, D and E while the blackhole node M returns an RREP with the maximum sequence number and one hop to S. When the destination node F receives the RREQs from the normal nodes E and D, it will choose the shortest path S-C-E-F and return an RREP [3]. When S receives numerous RREPs, the AODV routing protocol mechanism selects the RREP with the most current and shortest path. As a result, the originating node S chooses the S-M route, which passes through the blackhole node M, and M discards all received data packets directly.

4. PARAMETERS AND METHODOLOGY

This section provides an insight into the parameters considered to analyse the impact of blackhole attack in AODV. Model used for simulation is also discussed along with the simulation environment fabricated to obtain the results required for analysis.

4.1. Parameters Considered

The performance of the protocol is determined by the simulation parameters. The primary characteristics include packet size, number of nodes, transmission range, and network structure. Following three factors are the key focus during simulation of various scenarios:

(i) Packet Delivery Ratio

The packet delivery ratio is a critical metric for assessing the performance of a routing system in any network[4]. The packet delivery ratio is calculated by dividing the total number of data packets received at destinations by the total number of data packets supplied from sources [4], [15]. When the packet delivery ratio is high, the performance is considered as better. Mathematically, it can be written as:

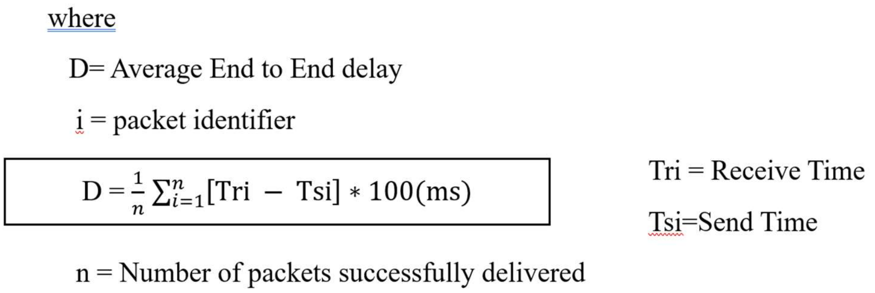
………(Eq. 1)

(ii) Average End-to-End Delay

The time it takes for a packet to travel from its origin to its destination is referred to as end-to-end delay [4]. The average end-to-end latency can be calculated by averaging the end-to-end delays of all successfully delivered messages. The probability of packet drop increases as the distance between the source and destination increases [1]. The average end-to-end delay incorporates all network delays, such as buffering, route finding latency, retransmission delays at the MAC, and propagation and transmission delay. It is measured in milliseconds (ms) and can be expressed mathematically as:

……… (Eq. 2)

where



where

D= Average End to End delay

i = packet identifier

$$\boxed{D = \frac{1}{n}\sum_{i=1}^{n}[\text{Tri} - \text{Tsi}] * 100(\text{ms})}$$

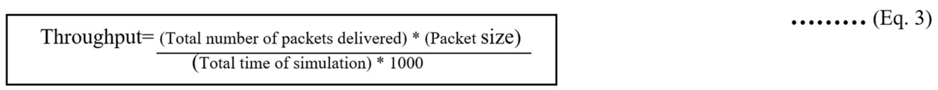
Tri = Receive Time

Tsi=Send Time

n = Number of packets successfully delivered

(iii) Average Throughput

Throughput is basically the rate of delivered packets to the destination [15]. It is measured in kilobits/sec (kbps). It can be represented mathematically as:



$$\boxed{\text{Throughput}= \frac{(\text{Total number of packets delivered}) * (\text{Packet size})}{(\text{Total time of simulation}) * 1000}}$$

……… (Eq. 3)

4.2. Random Way point Model

The most commonly used mobility model in wireless networks, particularly in Mobile Ad Hoc Networks, is the Random Way Point (RWP) model, which creates a more realistic mobility model in which each node moves to a random point within a specific network area, remains in that position for a set period of time known as the pause time, and then moves to the next random point, and so on. To generate mobility code setdest tool is used. Following are the steps to write mobility code:

(i) ns-allinone-2.35/ns-2.35/indep-utils/cmu-scen-gen/setdest

(ii) /setdest [-v version_number] [-n number_of_nodes] [-m min_speed] [-M maximum_speed] [-t simulation time] [-x grid_size] [-y grid_size].

(iii) Then redirect the whole output to the mob file.

4.3. Simulation Environment

For simulation and analysing the results of blackhole attack in AODV protocol NS-2.35 version of network simulator is used. NS-2.35 supports a wide range of network technologies, including wired and wireless networks, and can mimic a wide range of network protocols, including TCP, UDP, and IP [16]. It can also imitate routing algorithms like OSPF, BGP, and DSR, as well as wireless MAC protocols like IEEE 802.11 and Bluetooth.

NS-2.35 comes with a graphical user interface for creating network topologies and executing simulations [17]. It also includes a number of analysis tools for monitoring network performance indicators like throughput, latency, and packet loss [17].

To simulate the effect of black hole attack certain modifications in aodv.h and aodv.cc files are required. After modification there is a need to recompile the NS2. Therefore, to run the black hole attack simulation the NS2 is recompiled. Table 1 shows the various parameters used for simulation.

Table 1: Parameters used for Simulation

S.No.	Network Parameters	Value
1.	Simulator	NS-2.35
2.	Simulation time	1500sec
3.	Number of Nodes	10, 25, 35, 50, 75
4.	Black hole nodes	0,1,2,4
5.	Mobility Model	Random waypoint
6.	Routing Protocol	AODV
7.	Node speed	10m/s, 25m/s
8.	Mac protocol	802.11 Ext
9.	Traffic type	CBR
10.	Simulation area	1000m * 1000m

5. SIMULATION SCENARIOS AND RESULTS

This section presents the various scenarios used for simulation of AODV protocol, along with the results obtained after simulation. Scenario 1 is based on the node speed of 10m/s whereas scenario 2 considers the node speed as 25m/s. Both scenarios analyze the impact of solo as well as multi blackhole nodes on performance of AODV protocol based on the three parameters- throughput, e2e delay and packet delivery ratio. Comparative results of both scenarios are discussed in the end of this section.

5.1. SCENARIO 1 (Node speed is 10m/sec)

In this scenario, the node speed is 10m/sec and parameters simulated and analysed are throughput, E2E delay and packet delivery ratio. The results are based on the impact of blackhole attack on 0, 1, 2 and 4 nodes.

(i) Throughput vs Number of Nodes

It can be observed that on low node density throughput is low, it rises with increase in node density but again decreases at higher node density. Throughput values for AODV protocol without blackhole, solo blackhole and multi blackhole nodes are given in Table 2.

Table 2: Throughput vs Number of Nodes (Node Speed@10m/s)

S. No	No. of Nodes	Throughput (in kbps)			
		Without Blackhole	With 1 Blackhole	With 2 Blackhole	With 4 Blackhole
1.	10	78.82	62.71	34.58	28.88
2.	25	152.61	90.95	80.37	24.90
3.	35	157.78	80.53	63.75	40.98

4.	50	186.75	115.96	83.04	52.78
5.	75	148.60	79.61	53.98	59.56

Fig. 5 shows that throughput decreases as the number of blackhole attack increases. It can be noticed that when there is no blackhole node present in the network throughput is high but in the presence of blackhole attacks, where malicious nodes drop or selectively forward packets, the throughput of the network is negatively affected. The network's throughput gradually decreases due to increased packet loss, retransmissions, congestion, and wastage of time in route discovery.

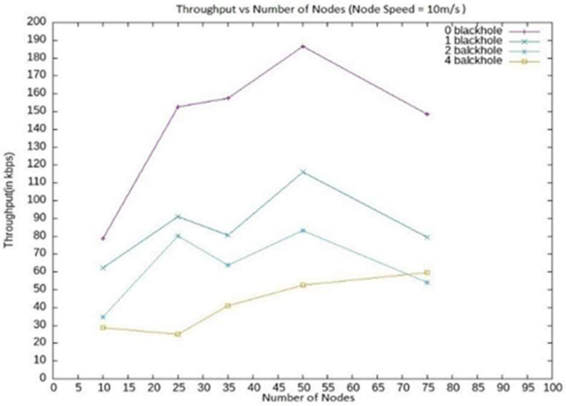


Fig. 5: Graph of Throughput vs Number. of Nodes

(ii) Packet Delivery Ratio vs Number of Nodes

It can be observed that on low node density packet delivery ratio is low due to the transmission load on fewer number of nodes. PDR increases with increase in node density but again falls on higher node densities due to increased packet flows between large number of nodes. PDR values for AODV protocol without blackhole, solo blackhole and multi blackhole nodes are given in Table 3.

Table 3: PDR vs Number of Nodes (Node Speed@10m/s)

S. No	No. of Nodes	End to End Delay (in ms)			
		Without Blackhole	With 1 Blackhole	With 2 Blackhole	With 4 Blackhole
1.	10	0.4	0.21	0.51	0.58
2.	25	0.23	0.5	0.47	0.19
3.	35	0.74	1.33	1.13	2.42
4.	50	1.01	1.65	1.7	2.20
5.	75	2.55	1.58	3.86	1.74

In absence of blackhole node in the network, the Packet Delivery Ratio (PDR) is at peak as per the expectations. In a normal network without any malicious nodes, packets are routed through reliable paths, and the PDR remains high. However, when blackhole nodes are introduced into the network, the PDR gradually decreases. This is because blackhole nodes selectively drop or discard packets, leading to a higher rate of packet loss. Legitimate nodes may route their packets through the blackhole nodes, believing that they are valid routes. But due to the malicious behaviour of the blackhole nodes, the packets are not delivered to their intended destinations, resulting in a lower PDR.

The extent to which the PDR decreases depends on factors such as the number of blackhole nodes, their strategic placement in the network, and the routing decisions made by legitimate nodes. It can be observed from Fig. 6 that as the number of blackhole nodes increases, the impact on the PDR becomes more significant, causing a decline in successful packet delivery.

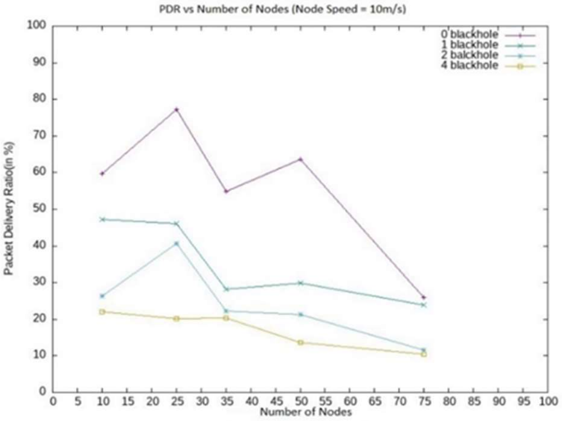


Fig. 6: Graph of PDR vs Number of Nodes

(iii) End to End delay vs Number of Nodes

End to end delay shows a general rise with increase in node density. Timing values for AODV protocol without blackhole, solo blackhole and multi blackhole nodes are given in Table 4.

Table 4: E2E delay vs Number of Nodes (Node Speed@10m/s)

S. No	No. of Nodes	Packet Delivery Ratio (in %)			
		Without Blackhole	With 1 Blackhole	With 2 Blackhole	With 4 Blackhole
1.	10	59.78%	47.14%	26.22%	21.94%
2.	25	77.27%	46.04%	40.63%	20.22%
3.	35	54.91%	28.11%	22.22%	18.37%
4.	50	63.69%	29.80%	21.53%	13.52%
5.	75	25.94%	23.87%	25.94%	10.53%

As depicted in Fig.7, with an increase in the number of blackhole nodes the end-to-end delay also tends to increase. Blackhole nodes interfere with the routing process by either dropping or selectively forwarding packets. Legitimate nodes may unknowingly route their packets through these malicious nodes, resulting in longer paths and increased routing delays. The routing interference caused by blackhole nodes contributes to the overall end-to-end delay.

Packet Loss and retransmissions is another reason of increase in e2e delay due to increase in blackhole nodes. Blackhole nodes selectively drop packets, leading to increased packet loss in the network. This loss requires retransmissions of the lost packets, resulting in additional delays. More the number of blackhole nodes, higher is the packet loss, and subsequently increased number of retransmissions, leading to longer end-to-end delays.

Blackhole nodes can cause congestion in the network by dropping or delaying packets. Congestion leads to increased queueing delay at intermediate nodes as they contend for limited network resources. As the number of blackhole nodes increases, the probability of encountering congestion and subsequent queueing delays rises, contributing to the overall end-to-end delay.

In the presence of blackhole nodes, the route discovery process may become longer and less efficient. Legitimate nodes may receive false or misleading route information from blackhole nodes, leading to prolonged route discovery attempts and increased recovery time for establishing valid routes. The extended route discovery and recovery time contribute to the overall end-to-end delay.

Overall, with an increase in number of blackhole nodes, the disruptions caused by their malicious behaviour result in longer routing paths, increased packet loss, additional retransmissions, congestion, and extended route discovery and recovery times. All these factors collectively contribute to an increase in the end-to-end delay in the network.

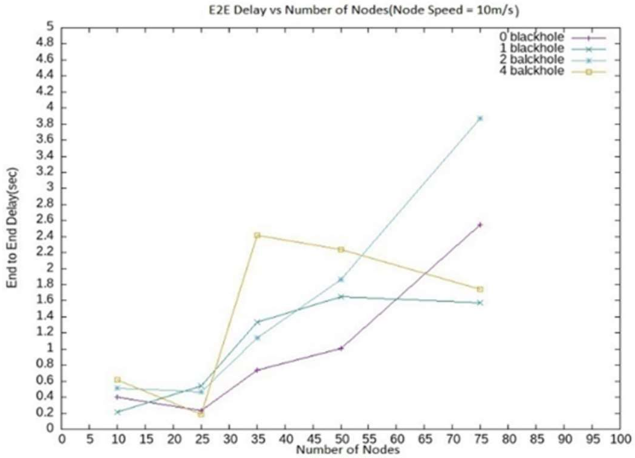


Fig.7: Graph of E2E delay vs Number of Nodes

5.2. SCENARIO 2 (Node speed is 25m/sec)

In this scenario, the node speed is 25m/sec and simulations are performed for the same parameters i.e., throughput, E2E delay and packet delivery ratio.

(i) Throughput vs Number of Nodes

It can be observed that when node speed is 25m/sec the throughput values decrease gradually in comparison to when the node speed is 10m/sec. Throughput values for AODV protocol without blackhole, solo blackhole and multi blackhole nodes at node speed of 25m/s are given in Table 5.

Table 5: Throughput vs Number of Nodes (Node Speed@25m/s)

S. No	No. of Nodes	Throughput (in Kbps)			
		Without Blackhole	With 1 Blackhole	With 2 Blackhole	With 4 Blackhole
1.	10	57.65	43.34	33.63	24.70
2.	25	164.13	100.64	73.54	60.76
3.	35	171.32	101.27	74.51	46.02
4.	50	137.88	102.68	78.37	52.98
5.	75	113.31	66.41	54.68	27.24

Fig.8 shows the change in throughput values for AODV protocol with increasing number of nodes. Obvious degradation is observed in throughput values with increase in blackhole nodes. On the other hand, with an increase in number of nodes, increase in throughput is observed at medium node density, which fades away at higher node density.

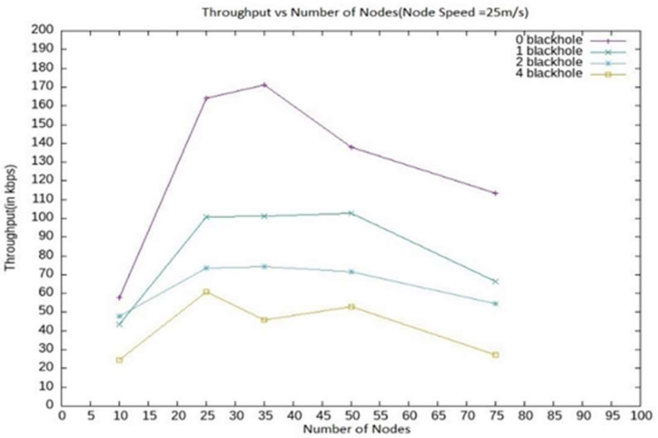


Fig. 8: Graph of Throughput vs Number of Nodes

(ii) Packet Delivery Ratio vs Number of Nodes:

There is expected degradation in PDR values in the presence of multi blackhole attacks. The PDR is likely to decrease due to increased packet loss, incomplete route establishment, routing instability, delays, and increased latency caused by the malicious behaviour of the blackhole nodes. Network security measures, such as intrusion detection systems or secure routing protocols, can be employed to mitigate the effects of blackhole attacks and enhance the overall network performance. Throughput values for AODV protocol without blackhole, solo blackhole and multi blackhole nodes are given in Table 6.

Table 6: PDR vs Number of Nodes (Node Speed@25m/s)

S. No	No. of Nodes	Packet Delivery Ratio (in %)			
		Without Blackhole	With 1 Blackhole	With 2 Blackhole	With 4 Blackhole
1.	10	48.68%	32.85%	25.53%	19.01%
2.	25	83.00%	50.80%	25.90%	29.54%
3.	35	59.72%	35.28%	37.23%	14.92%
4.	50	47.53%	25.86%	20.14%	12.47%
5.	75	20.04%	11.74%	9.72%	4.81%

The PDR is typically high when there are no blackhole attacks. AODV is designed to establish reliable routes between source and destination nodes, ensuring that a significant percentage of packets reach their intended destinations successfully. Without blackhole attacks, the PDR is generally close to optimal, assuming other network conditions are favourable. In the absence of blackhole attacks, AODV can efficiently discover and maintain routes in the network. Route discovery processes are usually successful, resulting in effective paths from source to destination. This contributes to efficient packet forwarding and reduced overhead. Fig. 9 shows the graph for PDR values at node speed of 25m/s.

On comparing the performance at node speed of 10m/sec and 25m/sec it can be observed that at higher node speed the packet delivery ratio decreases rapidly in case of co-operative black hole attacks.

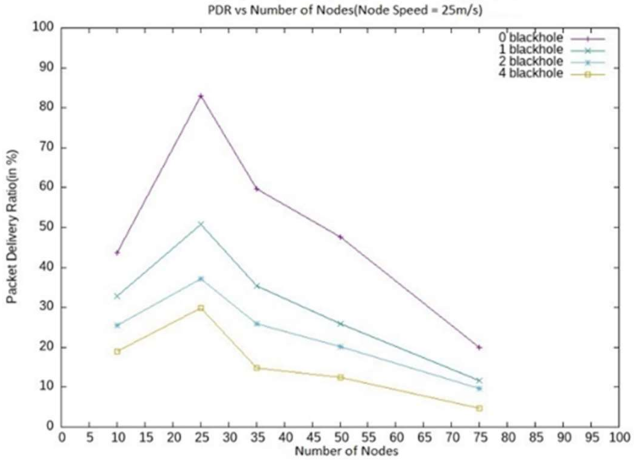


Fig. 9: Graph of PDR vs Number of Nodes

(iii) End to End delay vs Number of Nodes:

In the absence of blackhole attacks, AODV generally exhibits low latency and delay. Packets are forwarded along established routes, minimizing delays caused by rerouting or disruptions. This makes AODV suitable for real-time applications and sensitive data transfers, where low latency is crucial. Timing values for AODV protocol without blackhole, solo blackhole and multi blackhole nodes are given in Table 7.

Table 7: E2E delay vs Number of Nodes (Node Speed@25m/s)

S. No.	No. of Nodes	End to End Delay(in ms)			
		Without Blackhole	With 1 Blackhole	With 2 Blackhole	With 4 Blackhole
1.	10	1.69	1.35	1.03	0.75
2.	25	0.45	0.78	1.06	1.04
3.	35	0.74	1.08	0.96	1.48
4.	50	1.07	1.27	1.39	1.70
5.	75	2.01	1.82	1.37	2.25

Blackhole attacks can introduce additional delays and latency. Legitimate nodes that encounter a blackhole node may experience delays in packet delivery or have to re-establish new routes. These extra delays and latency can cause a decrease in the PDR, as the timely delivery of packets is compromised. As packets are dropped or delayed, the time taken for packets to traverse the network increases. The increased latency contributes to higher end-to-end delay and can impact the overall network performance. Fig. 10 displays the variation of e2e delay at node speed of 25m/s.

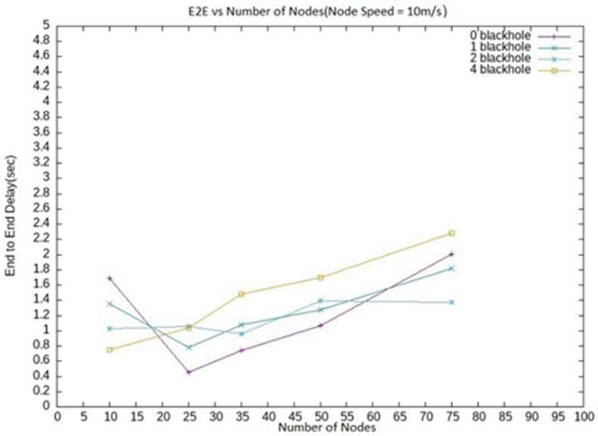


Fig. 10: Graph of E2E vs number of nodes

5.3. Comparative Performance @ Node speed (10m/sec vs 25m/sec):

To compare the performance of varying node speeds of blackhole attacks in AODV (Ad hoc On-Demand Distance Vector) routing protocol, we need to consider effect of movement and speed of the blackhole nodes on the network's overall performance. The node speed can have a significant impact on the routing process and the effectiveness of the blackhole attack. Here are some observations for solo and multi blackhole attacks for varying speed of nodes:

(i) Packet Delivery Ratio (PDR): The PDR is a crucial metric that indicates the percentage of packets successfully delivered to their intended destinations. As the speed of blackhole nodes increases, the probability of intercepting and dropping packets also increases. Therefore, higher node speeds of blackhole attackers generally lead to a lower PDR.

(ii) Routing Overhead: AODV relies on control packets, such as Route Request (RREQ) and Route Reply (RREP), for establishing and maintaining routes in the network. When blackhole nodes move at higher speeds, they may disrupt the route discovery process by dropping or delaying these control packets. This disruption increases the routing overhead, causing additional control packets to be transmitted and potentially affecting the network's overall performance.

(iii) Route Stability: The movement and speed of blackhole nodes can affect the stability of routes in AODV. When nodes change their positions rapidly, the routes established through the network may become invalid or unreliable. This instability can lead to frequent route discoveries and route repairs, increasing the latency and affecting the overall performance of the network.

(iv) Detection and Mitigation: Higher node speeds can make it more challenging to detect and mitigate blackhole attacks in real-time. Rapid movement may make it difficult for other nodes to observe the malicious behaviour consistently. This can delay the detection of the attack and hinder the deployment of countermeasures to mitigate its effects.

6. CONCLUSION

Overall, a blackhole attack in the AODV routing protocol has a detrimental impact on network performance, particularly in terms of throughput. Here's a summary of the observations regarding the impact of a blackhole attack on based on different parameters in AODV:

(i) Reduced Throughput: A blackhole attack leads to a significant reduction in throughput. The malicious node selectively drops or discards packets, preventing them from reaching their intended destinations. This loss of packets results in decreased throughput, as fewer packets are successfully delivered.

(ii) Disrupted Data Flow: The presence of a blackhole node disrupts the flow of data in the network. Legitimate nodes may route their packets through the blackhole node, only to have them dropped. This disruption creates interruptions and delays in the delivery of data, further lowering the overall throughput.

(iii) Increased Retransmissions: The dropped packets due to the blackhole attack necessitate retransmissions. Legitimate nodes need to detect the packet loss and resend the affected packets, consuming additional network resources and reducing the overall throughput.

(iv) Routing Inefficiency: Blackhole attacks disrupt the routing paths in the network, resulting in inefficient routing. Legitimate nodes may need to perform additional route discoveries and repairs to bypass the blackhole node and find alternative routes. These additional routing operations introduce delays and increase control packet overhead, negatively impacting the throughput.

(v) Packet Delivery Ratio (PDR) degradation: The PDR decreases as the blackhole node drops packets, leading to a reduced successful delivery of packets.

(vi) Delay and latency: Blackhole attacks introduce delays and increased latency in the network, affecting the timely delivery of packets and increasing end-to-end delay.

(vii) Network partitioning: In some cases, blackhole attacks can result in network partitioning, isolating a region of the network and disconnecting nodes from their intended destinations.

(viii) Reduced quality of service (QoS): The overall QoS parameters such as throughput, latency, and reliability are significantly degraded due to compromised routing paths and dropped packets.

7. SCOPE FOR FUTUTRE WORK

Mitigating black hole attacks and ensuring secure routing protocols can help maintain a higher throughput, higher packet delivery ratio and lower end to end delay by minimizing the impact of these malicious nodes and maintaining efficient data transmission in the network.

Mitigating black hole attacks in network communication involves implementing various security measures to detect and prevent such attacks. Some techniques to help mitigate black hole attacks can be implemented to improve the overall performance of routing protocols in presence of black hole nodes. Some of the domains to work further includes authentication and access control mechanisms, implementing secure routing protocols, employing various trust-based mechanisms, deploying intrusion detection system, etc.

8. REFERENCES

[1] S. S. Kariyannavar, S. Thakur, and A. Maheshwari, “Security in Mobile ADHOC Networks: Survey,” in Proceedings of the 6th International Conference on Inventive Computation Technologies, ICICT, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 135–143, 2021. doi: 10.1109/ICICT50816.2021.9358611.

[2] Pragati Jain, Akash Sanghi & Y.D.S. Arya. “Performance Analysis of QoS factors in Manet Protocols for Different Terrains” Journal of Optoelectronics Laser,41(8), pp.211–220, 2022. Retrieved from http://www.gdzjg.org/index.php /JOL /article/view/900

[3] A. S. Bhandare and S. B. Patil, “Securing MANET against co-operative black hole attack and its performance analysis - A case study,” in Proceedings - 1st International Conference on Computing, Communication, Control and Automation, ICCUBEA, Institute of Electrical and Electronics Engineers Inc., pp. 301–305, 2015 doi: 10.1109/ICCUBEA.2015.63

[4] G. li, Z. Yan, “Study and Simulation Research of Blackhole Attack on Mobile Adhoc Network”, 1st International Workshop on System Security and Vulnerability, IEEE CNS, 2018.

[5] S. Vemuri and S. Mirkar, "A Performance Comparison of MANET Routing Protocols," Innovations in Power and Advanced Computing Technologies (i-PACT)”, Kuala Lumpur, Malaysia, pp. 1-5, 2021. doi: 10.1109/i-PACT52855.2021. 9696785.

[6] Pragati Jain, Akash Sanghi, “Review of Various Routing Protocols in Mobile Ad-Hoc Networks (MANETs)” International Journal of Innovations & Advancement in Computer Science, (IJIACS), pp. 45-54, 2347-8616, 2018.

[7] A. U. Khan, R. Puree, B. K. Mohanta, and S. Chedup, “Detection and prevention of blackhole attack in AODV of MANET,” IEEE International IOT, Electronics and Mechatronics Conference, IEMTRONICS - Proceedings, Institute of Electrical and Electronics Engineers Inc., Apr. 2021. doi: 10.1109/IEMTRONICS52119.2021. 9422643.

[8] S. Praveen and V. Gupta, “Comparison of Performance of AODV Protocol under Black hole Attack on MANET”, International Journal of Engineering Research & Technology (IJERT), ISSN:2778-0181, Available: www.ijert.org, 2012.

[9] E. M. Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," IEEE Personal Communications, vol. 6, no. 2, pp. 46-55, April 1999.

[10] B. Clemence, Z. C. Xuan, and A. Younis, “A Blackhole Attack Mitigation Algorithm in MANET based on Standard Deviation Outlier Detection,” WSEAS Transactions On Computers, vol. 19, pp. 62–68, Apr., 2020 doi: 10.37394/23205.2020.19.9.

[11] E. Lema, E. G. -M. Desalegn, B. Tiwari and V. Tiwari, "Trust Embedded AODV for securing and Analyzing Blackhole attack in MANET," IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), Naya Raipur, India, pp. 362-367, 2022 doi:10.1109/WIECONECE57977.2022.1015 0765.

[12] C. N. Pushpatode and S. V. Sankpal, "Black Hole Attack Prevention in AODV Routing Protocol,"Asian Conference on Innovation in Technology (ASIANCON), PUNE, India, pp. 1-4, 2021 doi: 10.1109/ASIANCON51346.2021.9544 955.

[13] R. Kushwah, “Performance Analysis of Black-Hole Attack in MANET” in International Journal of Computer Science and Information Technologies, pp. 5225-5230, 2014.

[14] C. Brill and T. Nash, “A Comparative Analysis of MANET Routing Protocols through Simulation” in 12th International Conference for Internet Technology and Secured Transactions, pp. 244-247, 2017.

[15] 12 I. A. Shah and N. Kapoor, "To Detect and Prevent Black Hole Attack in Mobile Ad Hoc Network," 2nd Global Conference for Advancement in Technology (GCAT), Bangalore, India, pp. 1-4, 2021 doi: 10.1109/GCAT52182.2021.9587471.

[16] R. C. Jisha, J. Joseph and M. N. M. Basheer, "Comprehensive Study on Mobile Ad-hoc Routing Protocols: OLSR, AODV and DSDV," IEEE 3rd Global Conference for Advancement in Technology (GCAT), Bangalore, India, pp. 1-6, 2022 doi: 10.1109/GCAT55367.2022.9971899.

[17] Pragati Jain, Akash Sanghi, “Comparative Study of Various Network Simulators” in International Journal of Innovations and Advancement in Computer Science (IJIACS), pp 307-315, 2017.