Anti-Black Hole Attack Mechanism for Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol in Manets

Fawaz Mahiuob Mohammed Mokbal
MS (IT) Scholar, IBMS
The University Of Agriculture
Peshawar-Pakistan

Khalid Saeed
Lecturer Computer Sciences IBMS
The University Of Agriculture
Peshawar-Pakistan

ABSTRACT
Mobile Ad-hoc Networks (MANETs) can be set up dynamically anywhere and anytime without the need of infrastructure. MANETs consists of a set of wireless nodes. These nodes move randomly and communicate with each other via a wireless communication links. MANETs routing protocols are vulnerable to several types of attacks, the most famous and common is Black Hole attack .This research simulate the behavior of Black Hole attack on Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol using Network Simulator (NS2.35). Moreover, the black hole node(s) have been eliminated completely using the mechanism proposed in this research. The proposed approach is named as Anti-Black Hole Attack mechanism for AODV (ABHMAODV) Routing Protocol. The proposed mechanism maintains the performance of the protocol while handling Black Hole attacks.

Keywords
MANET, AODV, ABHMAODV, Black Hole Attack.

1. INTRODUCTION
A wireless ad-hoc network is also known as IBSS because the communication links are wireless. The network is ad-hoc because the connections between the stations are directly connected with each other and does not need access points [1]. Ad-hoc with mobility is commonly called MANETs (Mobile Ad-hoc Networks).

MANETs are autonomous systems in which mobile nodes are connected by wireless links and are free to move randomly. The nodes sometimes act as host and sometimes act as a router [2]. Moreover, the network topology is constantly changing and unexpectedly as well. These nodes cooperate with each other to do routine tasks in the network [3]. It is called infrastructure-less networks because it is temporary and short-range [1]. In most cases, the hardware components for MANETs have limited power, limited memory, and the processor capabilities are limited, as well as speed and data transfer rate are also limited. These limitations are called thin client [4]. Therefore, the range ultimately becomes less. The packets in MANETs are transmitted either directly from the source node to destination node or by passing through a series of intermediate nodes. However, the issue of security in MANETs is a challenging task such as establishing secure route between source node and destination node [3].

Figure 1 given below shows the diagrammatic representation of MANETs which consist of three nodes (n0, n1, n2).

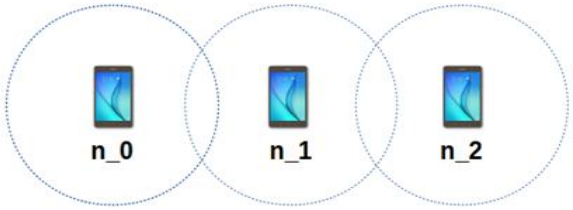

Fig. 1: MANETs Consist of Three Nodes.

MANETs are used in case of lack of specific infrastructure, or when there is little infrastructure to find due to many reasons including cost or non-consensual. In some cases MANETs are used in fire, safety, rescue and military operations in which the identified infrastructure or specific topology structure are not possible or have been destroyed [3]. Moreover, it can also be used in the classroom in a group which wants to communicate with each other, if any mobile device which has a wireless interface, the group of mobile devices can form MANETs. Protocols are needed to pass the packets in the network. There are many routing protocols in MANETs, and one of the most important among them is Ad-hoc On-demand Distance Vector (AODV) Routing Protocol.

2. AODV ROUTING PROTOCOL
The Ad hoc On-Demand Distance Vector (AODV) routing protocol intended for use by mobile nodes in ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network use, and determines unicast routes to destinations within the ad hoc network [5]. AODV is the reactive protocol which uses a table of routes and keeps information on recent routes that is used by the recent node. The protocol uses two functions such as route discovery and route maintenance.

2.1 Route Discovery
When a source node needs a new route to another node (destination node) and does not have a fresh-enough-route in its route table than the source node broadcasts the route request message (RREQ) to the rest of its neighbor nodes in the network. The source node waits to receive a route reply message (RREP) about desired node within a specific period of time from neighbor node or destination node itself. If the source node does not receive any response during that period, it either rebroadcasts route request again or assume that there is no known new route to the required destination node. When (RREQ) is received from the neighbor node than it will either send a reply (RREP) to the source node or forward the request based on the data in its own routing table. In addition, it establishes the opposite route on temporary basis using the IP address of the source node. The sequence number mechanism

in AODV is used to find the fresh-route and guarantee loop-free routes [5].

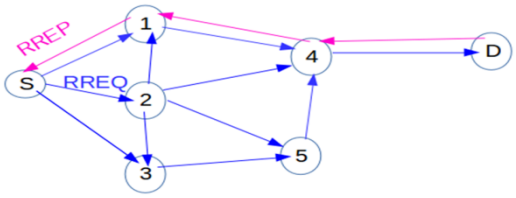

Fig. 2: AODV Route Discovery.

2.2 Route Maintenance

Route maintenance occurs when a node detects that the route to the neighbor node is no longer valid. It deletes the path of the route from its routing table and then broadcasts Route Error (RERR) message to each adjacent node. Each node, which receives Route Error message also re-transmit it to each neighbor nodes so that the message finally reaches the source node, and it either cancels or re-sent the route request data by sending a new route request message (RREQ). Hello messages in AODV are used to maintain the connectivity of neighbor nodes regularly [5].

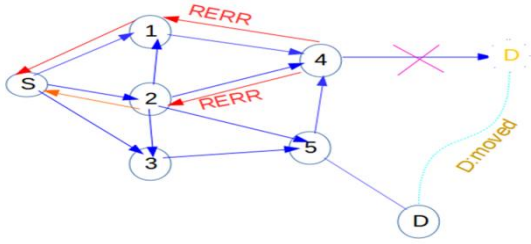

Fig. 3: AODV Route Maintenance.

3. ATTACKS IN MANETs

In MANETs, attacks can be divided into two categories such as passive attack and active attack. Passive Attack captures the data that is passing in the network, without affecting the contents of the data. While an active attack includes information drop, alteration, or deceit. Therefore, it interrupts the normal functionality of MANETs protocols. There are different attacks, which lies under either active attack or passive attack [6].

3.1 Eavesdropping Attack

This is a type of passive attack, in which an attacker can wiretap to any wireless network in order to capture the traffic within the network. It first captures the control messages to debrief the network topology to learn how nodes communicate with each other, and then abduct the information from the packets that are transmitted in the network by nodes. This type of attack is beneficial for gaining intelligence information about the data within the network [7].

3.2 Selfish Nodes (Selective Existence)

A selfish node can handily manipulate the protocol to cut its chance of starting an accepting a route, which exploits the network characteristic to keep its resources. It may fail or manipulates route request message to make sure that has no route through it [8]. Therefore, the selfish node behavior is known as selective existence attacks [9].

3.3 Gray Hole Attack

It is one of the active type of attack. Initially malicious node behaves correctly and replays true RREP messages to the nodes which started RREQ message. When the data packet arrives to a gray hole node, it is dropped and causes a denial of service. In addition, it may cause network resource consumption or battery consumption. In this case the malicious node goal has been achieved. Moreover, this attack is also known as routing misbehavior [10].

3.4 Modification Attack

This type of attack targets control messages (e.g. RREQ, RREP, and RERR). The control messages are used to set up the shortest and correct route and malicious node wants to forward the packet as it wants and it is done through modifying the contents of the control messages to mislead intermediate or victim node. Malicious node aim in this attack is to effect the network performance. This attack is also knows as detour attack [11].

3.5 Black Hole Attack

The primary difference between gray hole attack and black-hole attack is that in black hole attack the malicious node never initially send true control messages [12]. This attack exploits some properties of the protocol under attack when source node need to connect to the other destination node and does not have the known route, the source node broadcast RREQ message to its neighbor nodes. The attack exploits this mechanism to advertise itself as having the shortest path to the destination node. It is placed near the source node and receives RREQ, then without looking in its routing table, send faster RREP, this RREP has the highest sequence number and shortest hop count. The source node selects attacker node path and ignores another RREP coming from another node [13] as shown in figure 4.

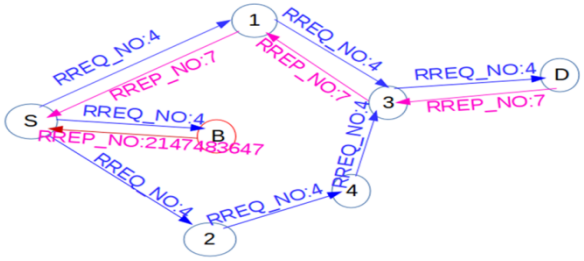

Fig. 4: AODV Black Hole Attack.

4. BLACK HOLE ATTACK IN AODV

This section explains how this attack effects the decision to choose a route, and how it deceives nodes in the AODV protocol and then the proposed mechanism to eliminate black hole attack in AODV Routing protocol.

4.1 AODV Routing Table

AODV Routing Protocol has a routing table at each node, which is used for maintaining the elements of important data in order to do routing discover, reply and maintenance route. The most important element is the sequence number that is updated at each node that is connected to the path in every discovery, reply or maintenance process of the route according to specific rules. In addition to the rest of the components of the table which is used by the protocol side by side to carry out its operations. Table 1 shows the components which are used in the AODV algorithm.

Table 1: AODV Routing Table Structure

ID_ Node	Current_Tim	Destination	Next_hop	Hops_No	Sequence_No	Time expire	Flag

4.2 AODV Sequence Number

The sequence number in AODV is 32 bit integer having range from -2147483647 to +2147483647, where the number 4294967295 is the highest value in 32-bit. To achieve sequence number rollover, the protocol starts operation by using the sequence number from zero, and then increases exponentially with positive signal until the highest number in the first 16-bit. Then it continue to increases in ascending with a negative signal until a higher value in the second 16-bit. therefore it returns to the value zero with a negative signal, then increases in ascending with negative sign, till up to the highest value in first 16-bit, then it increases in ascending with a positive signal until up to the highest value in the second 16-bit, then it goes back to zero value with a positive signal, and so on[5].

4.3 AODV Routing Table during RREQ/RREP Messages

In the normal case of AODV protocol operation when the source node wants to communicate with the destination node and does not have a fresh-route or does not have known route than the source node broadcast RREQ message to its neighbor nodes. Moreover, the process will continue until finding an intermediary node, which has a fresh-enough-route to the destination node or to find the same destination node. In order to avoid the same RREQ message forwarded from different neighbors, the node handling route request RREQ will accept the first one received, and ignore the other copies. As we can see in the figure 5 the nodes 1, 3 and 4 will ignore the other RREQ coming from 2 and 5 nodes. When the route request reaches to the neighbor node and has not enough fresh-route and true for the destination node specified in the RREQ than it forwards the request to the rest of its neighbor nodes through re-broadcast RREQ message. In addition, it establishes the opposite route and records it in a routing table [5]. The figure 6 shows how the RREP message is recorded in the routing table. In addition, it also shows how the routing table updates at each node and how the nodes establish the route.

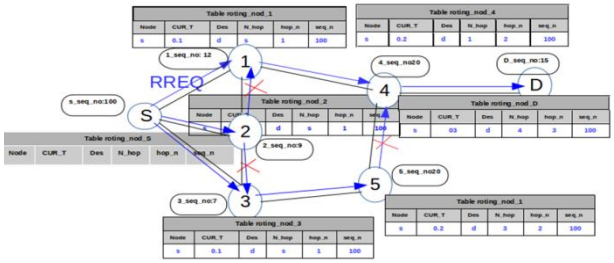

Fig. 5: AODV Routing Table during RREQ Message.

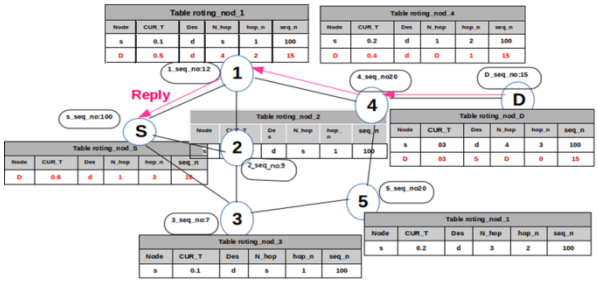

Fig. 6: AODV Routing Table during RREP Message

4.4 AODV Routing Table during Black Hole Attack

In case of black hole node, it is completely different, when a black hole node receives a RREQ message than it does not consult its own routing table for fresh-route, but it sends the RREP message back to the source node directly. This message contains the highest serial number and lowest hops count. Based on the rules to establish a route in AODV protocol, the source node upon receiving RREP message coming from black hole node, it establishes a path based on a fake message. When the original RREP comes from the normal nodes to source node, it discards these RREPs [13] as shown in Figure 7.

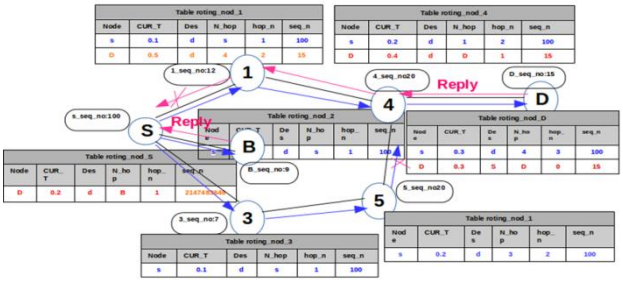

Fig. 7: AODV Routing Table during Black Hole Attack.

5. RELATED WORK

Zapata et al. [14] proposed Secure AODV Protocol (SAODV). The main task of SAODV protocol is to offer confidentiality relying on registration of most RREQ/RREP packet fields, which uses hash chain algorithm. The technique used in SAODV protocol verifies the signature of the previous nodes when each node sent the packet. The signing and signature verification in SAODV protocol operations exist in each node, which adds an extra burden, increases the cost of packet processing operations, and increases the energy consumption.

Yu and Xiao [15] suggested a method to detect selective forwarding attacks based on check-points. Using this technique first select some nodes along the route at random as the check-points node, then after receiving data packets, it will generate matching acknowledgments and then send them to the upper layer. However, an apparent problem exists in this process is that the nodes must send acknowledgments constantly, which will considerably raise the cost overhead of the network.

Kaplantzis et al. [16] proposed a scheme called centralized intrusion detection that uses two features to reveal selective forwarding and black hole based on SVMs "Support Vector Machines" and slipping windows. This intrusion detection work in the base station and hence the sensor nodes use no energy for backing this security added feature.

Jiang et al. [17] suggested a method in order to detect selective forwarding attack, which is based on the level of trust and loss of packets. The intermediate nodes discover and count the number of packets they received and sent. In addition, they report the statistical outcomes to the BS; the BS calculates the trust level of nodes and checks the packet loss.

Panaousis et al. [18] proposed AODV-WADR protocol, which works to supplement the work of the add Protocol, where nodes help to know whether the adjacent nodes channel has established a black hole-attack in MANETs or not, using two factors such as time and encryption.

Gandhewar and Patel [19] suggested a mechanism in order to detect and prevent a sinkhole attack, which contains four stages that are; Initialization stage for initialization its route

discovery RREP message, Storage stage for storing all the necessary information of all RREQ, Investigation stage, and Resumption stage for route establishment. This method is not so efficient in terms of End-to-End delay and energy conservation.

Rai et al. [20] proposed a method to detect multiple black hole attacks depended on "Trap RREQ". Before sending the real RREQ, the source node sends a fake RREQ to the Destination, which does not exist in the network and waits for all possible RREP during a specified period of time X, if any node replies RREP, than it is considered the black hole attack and block it by the source node. This method is not so efficient in terms of End-to-End delay and energy conservation.

Choudhary and Tharani [21] proposed a mechanism in order to prevent black hole attack in AODV based on "Timer Based Detection". Initially, each node in the network defines the max trust value to all its neighbor nodes and determines the min trust value allowable. If the trust value is less than min trust value, then it does not do any further communication with a neighbor whose trust value is less. This mechanism will prevent black hole attack after some time when network operation starts. Therefore, it is not so efficient in terms of packet delivery ratio (PDR).

6. PROPOSED MECHANISM

The mechanism proposed in this research uses the AODV protocol features, especially the sequence number stored in the routing table at each node with the addition of a mechanism for using the authentication and blocking the black hole attack, which contains the following:

- Detection method to check the RREP message.
- A blacklist for inserting the black hole nodes in it.
- Simple modifications in original receive reply (recvReply) function to implement the proposed mechanism.

When the neighbor node receives a RREQ message, the nodes that has fresh route will send RREP message to the node, which sent the RREQ message, otherwise the RREQ message will be forwarded till it reach to a node that has a fresh route to the destination or to the destination node itself. The black hole node will receive RREQ and will reply RREP message to the source node without looking in its routing table. The RREP message that is coming from black hole contained the highest sequence number and lowest hop count.

Here, at this point, the source node will receive RREP in order to check it. If the RREP is normal, then the node, which sent RREP will not be inserted in the black list otherwise looking in the black list, if the node that sent RREP exists in the list, then update the time for this node in the list, else insert the node that sent RREP in the black list. If the node, which sent a RREP message, is in the black list, then do not update routing tables otherwise, update routing tables.

6.1 Detection Method

A detection method, which has been proposed in this research is implemented at the source node and intermediate nodes, it will extract sequence number of the destination from the routing table, and then add to it the value of the gap, which we have pre-defined. Moreover, extracted sequence number of the destination from headers of the RREP messages which is send to the source node. If the sequence number of the destination at the head of the RREP messages is greater than the sequence number inside the routing table + gap, then the node, which sent RREP, is a black hole, black hole function is called and node is entered in it. The sequence number inside the routing table + gap together will not be static, it will dynamically change when the routing table updates.

6.2 Black-List Entry

In order to block the attacking nodes a black-list entry with its functions has been created in this research. These functions includes insert node to black-list, lookup for a node in black-list, update node existing in black-list and delete a node from black-list.

6.3 Simple Modifications in Original AODV Algorithm

A simple amendment in the protocol algorithm has been done to eliminate the black hole attack. When the RREP reaches the source node, it will call the detection method function to test the reply message, if it is dubious message, then the detection method calls black list function and insert a node in black list, which sent a reply.

In case of intermediate nodes, black-list function is not called, only detection method is called and the message is ignored if it is fake. The reason for this approach is to reduce end-to-end delay. In addition to the elimination of deceiving used by the black hole attack in some cases, the detection process at intermediate nodes aims to avoid deceiving the black hole attack, which seeks in some cases to pass the RREP fake messages to the source node via intermediate nodes. This trick can deceive the source node, but in the mechanism presented in this research, also has a solution to avoid such type of deceiving.

The pseudo simple algorithm modifications in ABHMAODV ::recvReply (Packet *p) as follows:

```
If (am source node)        {
 Get the des_Sq#_rt from my own routing table;
Get the des_Sq#_pck from header packet of RREP;
// call detection method
If ((node sent RREP not in black-list) and (des_Sq#_pck> des_Sq#_rt+gap))                    {
Attack= true;
Call black-list
Insert this node into black-list;
Do not update my routing table;
Drop route;  Packet free; Return;   }
Else If (node sent RREP is in black-list) {
Attack= true;
Update time for this node in black-list;
Do not update my routing table;
Drop route;  Packet free; Return;              }
If ((node sent RREP is not in black-list) or (des_Sq#_pck < des_Sq#_rt+gap))                    {
Attack= false;
Update my routing table; Return; }  }
If (am not source node "intermediate") {
 Get the des_Sq#_rt from my own routing table;
Get the des_Sq#_pck from header packet of RREP;
// detection method
If ((node sent RREP is not in black-list) and (des_Sq#_pck > des_Sq#_rt+gap))                    {
Attack= true;
Do not forward this packet;
Do not update my routing table;  }
Else If (node sent RREP is in black-list) {
Attack= true;
Do not forward this packet;
Do not update my routing table;          }
Else                                {
```

Attack= false;
Forward this packet;
Update my routing table; }

6.4 Simulation Methodology

To implement the proposed mechanism, two separate protocols have been created as follows:

- First, for the Black Hole Attack created protocol is named as AODVblackhole protocol.
- Second is named as Anti-Black Hole Attack Mechanism for AODV (ABMAODV) protocol.

All functions such as black list function, detection method and simple modifications in the original algorithm have been created inside the ABMAODV protocol, then three different scenarios have been implemented, each one has four cases (3x4=12). These are explained as follows:

- AODVblackhole protocol with AODV protocol for implementing black hole attack in original AODV protocol (attack case).
- AODVblackhole protocol with ABHMAODV protocol for implementing black hole attack in ABHMAODV protocol (attack case).
- Implement AODV without black hole attack (normal case).
- Implement ABHMAODV without black hole attack (normal case).

Table 2: Simulation Parameter

Operating System	Linux Mint Release 17.2
Network Simulator	NS2.35
Routing Protocols	AODV, ABHMAODV, and AODVblackhole
Type of Attack	Black Hole attack
Mobility Model	Random Waypoint
Simulation Time	500 seconds
Number of Scenarios	12 (3x4)
Number of Nodes	3,6,20
Number of Black Hole Attack Nodes	1,2
Simulation Area	1000 m x 1000 m
Transport Layer Protocol	UDP (User Datagram Protocol)
Traffic Model	CBR (Constant Bit Rate)
Packet Size	512 bytes
Link Capacity	1.0 Mbps
Connection Rate	5 packets/sec
Number of Connections	1,2
Node Speed	20 m/sec

6.5 Performance Parameter

1. Received Rate: the total number of data packets received by the destination node vs a total number of data packets sent by the source node.
2. Forward Rate: the total number of data packets forwarded successfully for routing vs total of data packets sent.
3. Drop Rate: total number dropped data packets for routing to total data packets sent.
4. Lost Rate: the total number of data packets sent by the source node and never received by the destination node.
5. Average End-to-End delay: the average time taken by a data packet to reach the destination. This includes all possible delays, only the data packets which are successfully delivered to destinations is counted.
6. Throughput Rate [bps]: Throughput is the number of packets successfully reached at destination per unit time (total size of packets received vs total time taken for transmission).
7. Packet Delivery Ratio: total packets received by destination vs total packets sent by the source.
8. Normalized Routing Load: the total number of routing packets transmitted at network layer vs total received data packets at the application layer.
9. Routing overhead: total number of routing packets transmitted at network layer including the packets forwarded.

6.6 Results

6.6.1 Scenarios of 3 Nodes:

The average received measurement in case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV protocols are same such as 99.96%, while in the case of AODV under attack is 0.0% due to the black hole attack.

The forward measurement is same in all cases, which is equal to 0.0%, the reason in the case of ABHMAODV under attack, normal case of ABHMAODV, and normal case of AODV protocols is the data transmission is directly between the source and the destination nodes and in the case of AODV under attack there was no transmission of data, so no forward.

The drop measurement in the case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV protocols are same 0.0% while in the case of AODV protocol under attack it is 100% due to the black hole attack.

The loss measurement in the case of ABHMAODV under attack, normal case of ABHMAODV and normal case of AODV protocols are same such as 0.04%, which is equal to one packet, while in case of AODV protocol under attack it is 100%, where the packets sent from the source node never reach the destination node due to the black hole attack.

The average delay measurement is approximately equal to 0.00579786 second (0.58%) in the case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV protocols while a delay of AODV protocol under attack does not exist due to lack of data transfer between the source and destination nodes. This is due to the black hole attack.

Packet delivery ratio in the case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV protocols are same such as 0.9996 (99.96%) while in case of AODV under attack it is 0.0%. It means that no packet was received by the destination node due to the black hole attack.

Average throughput [kbps] measurement in case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV protocols are same such as 20.49 while in case of AODV protocol under attack it is 0.0 due to the black hole attack.

Normalized routing load measurement is same, which is equal to 0.001202405 (0.12%) in the case of ABHMAODV under

attack, the normal case of ABHMAODV and a normal case of AODV protocols, while normalized routing load of AODV protocol under attack does not exist due to lack of data transfer between the source and destination nodes at the application layer. This is due to the black hole attack.
Routing table overhead measurement is same, which is equal to 3 packets at network layer in case of ABHMAODV under attack, normal case of ABHMAODV and normal case of AODV and AODV protocol under attack. It means that the black hole did not effect the network packets, but in case of AODV protocol under attack it is consider a waste of resources because the control packets were generated and there were no data packets translated.

6.6.2 Scenarios of 6 Nodes

The average received measurement in case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV protocols are same such as 99.96%, while in the case of AODV protocol under attack it is 0.0% due to the black hole attack.
The forward measurement is same in the case of ABHMAODV under attack, normal case of ABHMAODV and normal case of AODV protocols, which is equal to 100.00%. It means that all transmitted packets from the source node that has been received by the destination node were transmitted through intermediate nodes. However, in the case of AODV under attack there were 2 packets forwarded in the network but never received by destination which is equal to 0.08% which means that 99.96% packets were received by the black hole node were dropped and one packet (0.04%) was lost.
The drop measurement in the case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV are same such as 0.00% while in the case of AODV protocol under attack it was 100%. It means that all packets were received by the black hole node and were dropped.
The loss measurement in the case of ABHMAODV under attack, normal case of ABHMAODV and normal case of AODV protocols are same which is equal to one packet (0.04%). It means that all packets sent from the source node have reached the destination node except one, in fact, there is no lost, but the last packet was sent and the time of simulation was ended before this packet reached its destination or due to link failure or mobility. While in the case of AODV protocol under attack it is 100% lost due to the black hole attack, which means that all the packets sent from source node never received the destination node.
The average delay is same approximately 0.0179199 second (1.79%) in the case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV while a delay of AODV protocol under attack did not exist due to lack of data transfer between the source and destination nodes. It is due to the black hole attack.
Packet delivery ratio in the case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV protocols are same 0.9996 (99.96%) while in case of AODV under attack it is 0.0%. It means there were no packets received by destination node due to the black hole attack.
Average throughput [kbps] in the case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV protocols are same 20.49 while in the case of AODV protocol under attack it is 0.0 due to the black hole attack.
Normalized routing load measurement is approximately same, which is equal to 0.003206413 (0.32%) in the case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV protocols, while normalized routing load of AODV under attack do not exist due to lack of data transfer between the source and destination nodes at the application layer. It is due to the black hole attack.
Routing table overhead is same, which is equal to 8 packets at the network layer in the case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV and AODV protocol under attack. It means that the black hole did not effect the network packets, also, the packets at network layer increased as the node increases. However, in the case of AODV protocol under attack it is considered a waste of resources because the control packets were generated and there were no data packets translated.

6.6.3 Scenarios of 20 Nodes:

In these scenarios two traffic links have been used, one between node 0 and node 1 and the second between node 7 and node 2. In addition, two black hole nodes have been used in these scenarios so that traffic can be tested for packets between nodes with more than one traffic connection, in addition, to test the mechanism proposed in this research when there is more than one node for black hole attack. The results are as follows:
The average received measurement in the case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV protocols are same such as 99.96%, while in the case of AODV protocol under attack it is 0.0% due to the black hole attack.
The forward measurement is same in the case of ABHMAODV under attack, normal case of ABHMAODV and normal case of AODV protocols, which is equal to 100.00%. It means that all transmitted packets sent from the source node that has been received by the destination node were sent through intermediate nodes and all packets sent were forwarded. However, in the case of AODV under attack 2 packets were forwarded in the network but never received by destination which is equal to 0.08%. It means that one packet was received by the black hole node and was dropped and the other packet (0.04%) was lost.
The drop measurement in the case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV are same such as 0.00%. It means that the mechanism proposed in this research has eliminated the attack while in the case of AODV protocol under attack it is 100% due to the black hole attack.
The loss measurement in the case of ABHMAODV under attack, normal case of ABHMAODV and normal case of AODV protocols are same which is equal to one packet (0.04%). It means that all packets sent from the source node have reached the destination node except one, in fact, there were no lost, but the last packet was sent and the time of simulation was ended before that packet reached its destination or due to link failure or mobility. While in the case of AODV protocol under attack it is 100% lost due to the black hole attack, which means all the packets sent from source node never received by the destination node.
The average delay measurement is approximately same in the case of ABHMAODV under attack and in normal case of ABHMAODV with normal case of AODV which is equal to 0.0358146 (3.58%) second. It means that the mechanism proposed in this research did not cause any extra delay. While a delay of AODV protocol under attack does not exist due to lack of data transfer between the source and destination nodes. This is due to the black hole attack.
Packet delivery ratio in the case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV protocols are same such as 0.9996 (99.96%) while in the case of AODV protocol under attack it is 0.0%. It means

there was no packet received by destination node due to the black hole attack.

Average throughput [kbps] in the case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV protocols are same such as 40.97, the ratio increases because in this scenario there are two data link, each one has 20.49. While in the case of AODV protocol under attack it is 0.0, which means that no any data packet has been received by destination node due to the black hole attack.

Normalized routing load measurement is approximately same which is equal to 0.008817635 (0.88%) in the case of ABHMAODV under attack, the normal case of ABHMAODV and a normal case of AODV protocols, while normalized routing load of AODV under attack does not exist due to lack of data transfer between the source and destination nodes at the application layer. This is due to the black hole attack.

Routing table overhead measurement is same which is equal to 44 packets at network layer in the case of ABHMAODV under attack, normal case of ABHMAODV and normal case of AODV and AODV protocol under attack. It means that the black hole did not effect the generation or sending of network packets but it effected the established route, so only its packet were accepted at source node and other network layer messages were ignored, also, the packets at network layer are increased as the node increase. However, in the case of AODV protocol under attack, it is consider a waste of resources because the control packets generated and there is no data packet translated.

In addition to the results explained previously, the figure 8 given below shows the comparison between AODV and ABHMAODV at the received rate for all scenarios.

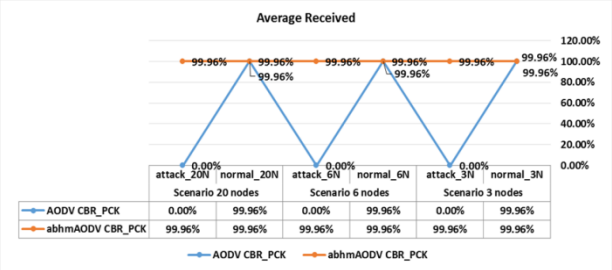

Fig. 8: Average Received

The figure 9 given below shows the comparison between AODV and ABHMAODV at forward rate for all scenarios.

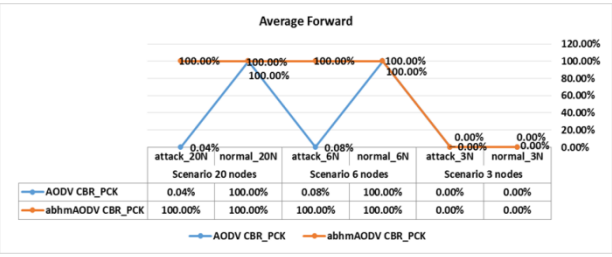

Fig. 9: Average Forward

The figure 10 given below shows the comparison between AODV and ABHMAODV at drop rate measurement for all scenarios. We can see clearly that the ABHMAODV has eliminated the black hole attack completely.

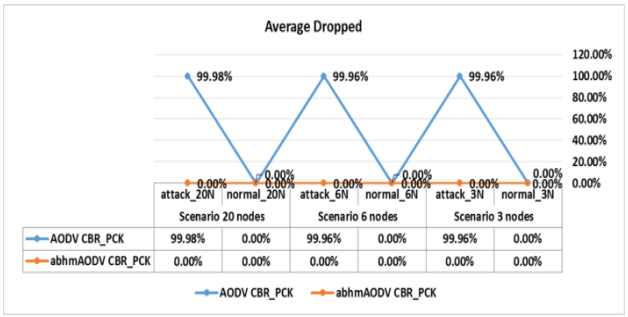

Fig. 10: Average Dropped

The figure 11 given below shows the comparison between AODV and ABHMAODV at loss rate for all scenarios.

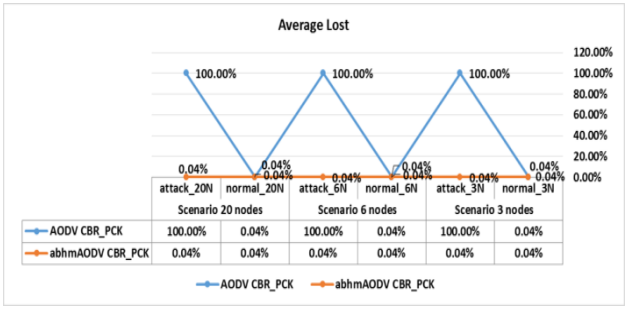

Fig. 11: Average Lost

Figure 12 given below shows the comparison between AODV and ABHMAODV at delay rate for all scenarios.

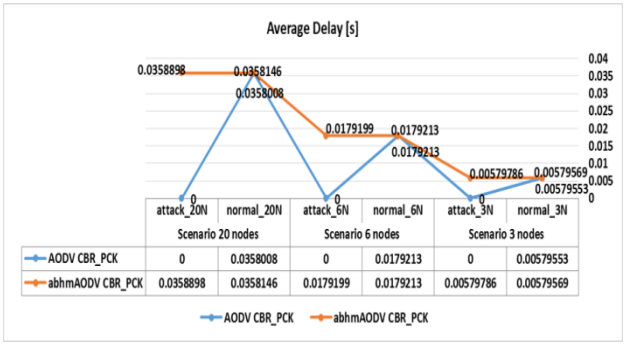

Fig. 12: Average Delay

Figure 13 given below shows the comparison between AODV and ABHMAODV at packet delivery ratio for all scenarios.

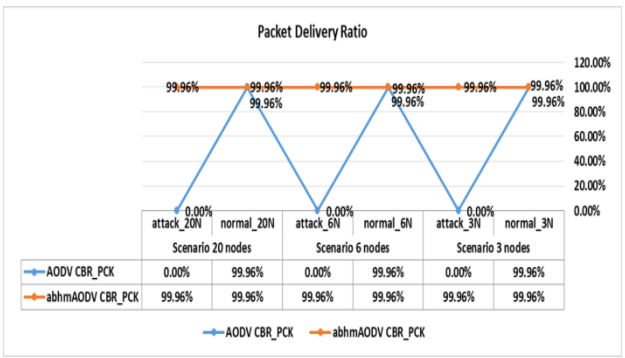

Fig. 13: Average Packet Delivery Ratio

Figure 14 given below shows the comparison between AODV and ABHMAODV at an average throughput in (kbps).

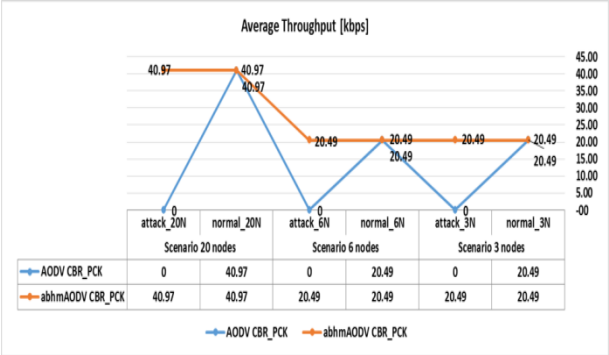

Fig. 14: Average Throughput (kbps)

Figure 15 given below shows the comparison between AODV and ABHMAODV at Normalized Routing Load measurement for all scenarios.

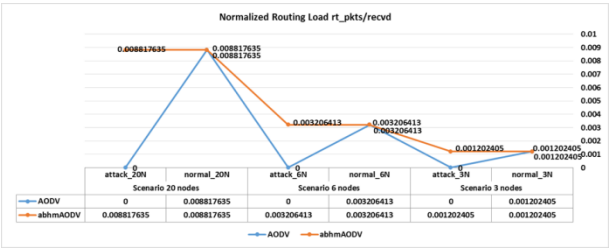

Fig. 15: Normalized Routing Load

Figure 16 given below shows the AODV and ABHMAODV at Routing Table Overhead measurement in different case.

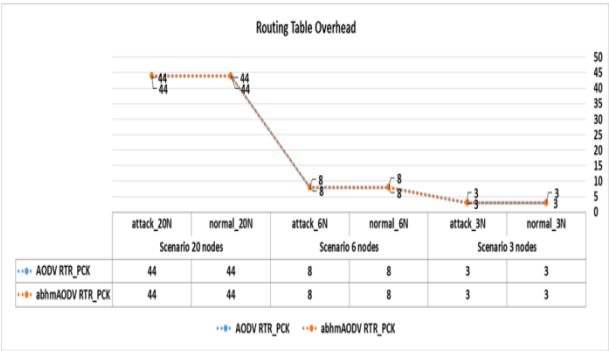

Fig. 16: Routing Table Overhead

7. CONCLUSION AND FUTURE WORK

7.1 Conclusions

Based on the results, the conclusions of this research are as follows:

1. ABHMAODV under attack, normal ABHMAODV, and normal AODV protocols were working at approximately the same level while the effect of black hole attack on original AODV protocol under attack is a considerable influence.
2. The mechanism proposed in this research has eliminated black hole attack completely.
3. The mechanism proposed in this research has maintained the performance of the original Protocol (best effort traffic and the efficiency of the routing protocol) under attack or without attack.

7.2 Future Work

This research proposed and implemented a mechanism to eliminate the black hole attack and tested it under different scenarios to obtain results in terms of best effort traffic and the efficiency of the routing protocol whereas in future this mechanism (ABHMAODV) can be simulated to test the energy efficiency at different stages (under attack scenarios/ and normal scenarios).

8. ACKNOWLEDGMENTS

We would like to thank ALLAH for helping us throughout our lives and gave us the ability and patience to carry out this research. Moreover, we are also thankful to our friends and families for their support.

9. REFERENCES

[1] Sreenath, N., Amuthan, A. and Selvigirija, P., 2012, January. Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs. In *Computer Communication and Informatics (ICCCI), 2012 International Conference on* (pp. 1-7). IEEE.

[2] Chlamtac, I., Conti, M. and Liu, J.J.N., 2003. Mobile ad hoc networking: imperatives and challenges. *Ad hoc networks*, *1*(1), pp.13-64.

[3] Macker, J., 1999. Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations.

[4] Satyanarayanan, M., 2001. Pervasive computing: Vision and challenges.*Personal Communications, IEEE*, *8*(4), pp.10-17.

[5] Perkins, C., Belding-Royer, E. and Das, S., 2003. *Ad hoc on-demand distance vector (AODV) routing* (No. RFC 3561).

[6] Rai, A.K., Tewari, R.R. and Upadhyay, S.K., 2010. Different types of attacks on integrated MANET-Internet communication. *International Journal of Computer Science and Security*, *4*(3), pp.265-274.

[7] Kanthe, A.M., Simunic, D. and Djurek, M., 2012, May. Denial of service (DoS) attacks in green mobile ad-hoc networks. In *MIPRO, 2012 Proceedings of the 35th International Convention* (pp. 675-680). IEEE.

[8] Sen, J. and Goswami, K., 2010. An algorithm for detection of selfish nodes in wireless mesh networks. *arXiv preprint arXiv:1011.1793*.

[9] Abdelhaq, M., Serhan, S., Alsaqour, R. and Hassan, R., 2011, July. A local intrusion detection routing security over MANET network. In *Electrical Engineering and Informatics (ICEEI), 2011 International Conference on* (pp. 1-6). IEEE.

[10] Marti, S., Giuli, T.J., Lai, K. and Baker, M., 2000, August. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 255-265). ACM.

[11] Vigna, G., Gwalan, S., Srinivasan, K., Belding-Royer, E.M. and Kemmerer, R.A., 2004, December. An intrusion detection tool for AODV-based ad hoc wireless networks. In *Computer Security Applications Conference, 2004. 20th Annual* (pp. 16-27). IEEE.

[12] Jathe, S.R. and Dakhane, D.M., 2012. A Review Paper on Black Hole Attack and Comparison of Different Black Hole Attack Techniques. *International Journal of Cryptography and Security ISSN*, pp.2249-7013.

[13] Kamal, A.R.M., 2004. Adaptive secure routing in ad hoc mobile network.*Master of Science Thesis, Department of Computer and Systems Science (DSV), Royal Institute of Technology (KTH), Stockholm, Sweden*.

[14] Zapata, M.G. and Asokan, N., 2002, September. Securing ad hoc routing protocols. In *Proceedings of the 1st ACM workshop on Wireless security*(pp. 1-10). ACM.

[15] Yu, B. and Xiao, B., 2006, April. Detecting selective forwarding attacks in wireless sensor networks. In *Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International* (pp. 8-pp). IEEE.

[16] Kaplantzis, S., Shilton, A., Mani, N. and Şekercioğlu, Y.A., 2007, December. Detecting selective forwarding attacks in wireless sensor networks using support vector machines. In *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on* (pp. 335-340). IEEE.

[17] JIANG, C.Y., ZHANG, J.M. and WANG, L.M., 2009. Selective Forwarding Attack Detection in Wireless Sensor Networks [J]. *Computer Engineering,21*, p.049.

[18] Panaousis, E.A., Nazaryan, L. and Politis, C., 2009, September. Securing AODV against wormhole attacks in emergency MANET multimedia communications. In *Proceedings of the 5th International ICST Mobile Multimedia Communications Conference* (p. 34). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[19] Gandhewar, N. and Patel, R., 2012, November. Detection and prevention of Sinkhole Attack on AODV protocol in Mobile Adhoc Network. In*Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on* (pp. 714-718). IEEE.

[20] Rai, A., Patel, R., Kapoor, R.K. and Karaulia, D.S., 2014, November. Enhancement in Security of AODV Protocol against Black-hole Attack in MANET. In *Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies* (p. 91). ACM.

[21] Choudhary, N. and Tharani, L., 2015, January. Preventing black hole attack in AODV using timer-based detection mechanism. In *Signal processing and communication engineering systems (SPACES), 2015 international conference on* (pp. 1-4). IEEE.