5.1 Introduction

MANETs usually suffer from security attacks for the reason that of their specification like lack of central monitoring and management, unclear defense mechanism, dynamic topology, cooperative algorithms, and open medium. The network layer protection systems for MANETs are involved with caring the network process to deliver data packets between mobile nodes during multi-hop ad hoc forwarding. Therefore, they look for to make sure that the routing message transferred between nodes is reliable with the protocol specification, and also the data packet forwarding behaviour of every node is reliable with its routing states [137].

Throughout the route discovery process of on-demand routing protocols, an assaulter can drop received routing messages, rather than relaying them because the protocol needs, so as reducing the amount of routing information obtainable to the another nodes, also known as black hole attack [138], and is a “reflexive” and easy way to achieve a Denial of Service. The attack may be done by selection (drop routing packets for a specified destination, a packet every n packets, a packet every t seconds) or drop all packets, and should have the result of creating the destination node unapproachable or lower communications in the network. The black hole attack is an essential issue which will occur in ad hoc networks particularly in well-liked on demand routing protocols like AODV [139].

5.2 AODV on MANETs

5.2.1 Protocol Operation

Being routing protocol, AODV involves route table management and is run based on the following route-request / route-reply cycle:
When source node transmits data to a node, the route of which is unknown, it broadcast a Route REQuest (RREQ) packet. This request packet will contain the last-known sequence number for that route and guarantee in loop-free networks.

Nodes that receive this packet update the Route Table (RT) for the source node address for a period of time: REV_ROUTE_TIMEOUT. This request can then be flooded throughout the network till it reaches the destination node or it reaches a neighbor node that contains a route to the destination node. Each node has backward pointers representing the reverse route back to the source node and maintains the received request.

The RREQ packet can contain the IP address of the source node, the broadcast ID, the IP address of the destination node, the destination sequence number, and the latest sequence number for the destination on the source node.

Once a node receives a RREQ message, check if the node either has route to the destination node with a sequence number is greater than or equal to the sequence number in the RREQ message or the node is that the destination itself, then a RREP message is created.

The RREP packet is sent a unicast transmission to the source. As the RREP traverses toward the source, the routing tables of all nodes will be updated for that destination IP address.

If the node that receives the RREQ message doesn’t have a route or is not the destination node, then it will broadcast the RREQ message to some other nodes.

Nodes maintain a observable table to maintain path of the RREQ’s received and their broadcast ID’s. If an already processed RREQ is received, then it will be dropped.

As before long because the source node receives the RREP message, it starts to transfer data packets to the destination.

AODV begins to use the route that is first available to the node. If an RREP message received by a node contains a larger sequence number or the same
sequence number with smaller number of hops then, the node can update its routing table therewith route.

- As long as a route is in use, it will remain active. A route is going to be thought of to move as long as there are information packets requesting the use of the route.

- If a link breaks while a route using that link is active, a Route ERRor (RERR) message will be generated by the node upstream. This message will propagate through until the source node and inform it of the now-unreachable destinations. Route discovery will be reinitiated for the destination for the nodes that require the use of that route.

- When a route is not used for a period of time, the route times out and is deleted from the route table. This time period is called the Route Expiry Time (RET) or the lifetime of the route.

According to the AODV request for comments [38], AODV uses the following fields with each route table entry:

- Destination IP address
- Destination sequence number
- Valid Destination sequence number flag
- Other state and routing flags (e.g. valid, invalid, repairable, being repaired)
- Network interface
- Hop count (number of hops needed to reach destination)
- Next hop
- List of precursors
- Lifetime (expiration and deletion time of the route)
ALGORITHM 1. AODV Routing Protocol [38]

// SN is the source node; DN is the destination node;
// RT = Routing Table; NN is the neighboring node
SN wants to communicate with DN
if RT of S contains a route to DN
    SN establishes communication with DN
else
    SN creates a RREQ packet and broadcasts it to its neighbors
    // RREQ contains the destination Address (DestAddr),
    // Sequence Number (Seq) and Broadcast ID (BID)
    for all nodes NN receiving RREQ
        if (RREQ was previously processed)
            Discard duplicate RREQ
        end if
        if (NN is DN)
            Send back a RREP packet to the node sending the RREQ
        else if (NN has a route to DN with SeqId >= RREQ.Seq)
            Send a RREP packet
        else
            The node recorded the received RREQ message
            Transmission the RREQ message
        end if
    end for
while (NN receives RREP message) and (N != SN)
    Store detail about the node
    Forward RREP on the reverse path
    Sending RREP in the RT
end while
SN receives RREP message
SN updates its RT depends on the node sending the RREP message
SN makes communication with DN
end if
The route table contains a field for the value of the lifetime of a route (i.e., RET value). ACTIVE_ROUTE_TIMEOUT value is predetermined and updated in this field or determined from the RREQ and RREP packets. Each time a node is receives a data packet or utilized to transfer a data packet, the lifetime field of the route value is updated to the current time plus ACTIVE_ROUTE_TIMEOUT.

5.2.2 Characteristics of AODV:

- Unicast, broadcast, and multicast communication.
- On-demand route formation with tiny delay.
- Multicast trees linking cluster members managing for lifetime of multicast cluster.
- Efficiently to repaired link breakages in active routes.
- Routers are loop-free in the network.
- Easily track accurate information using a sequence numbers.
- Route maintenance for always to keep track of next hop for a route.
- Sending HELLO messages easily to track neighbor nodes [40].

5.2.3 Interesting concepts of AODV:

The conceptions of AODV that build it advantageous for MANETs with restricted bandwidth include the following:

- **Minimal space complexity:**
  The algorithm makes certain that the nodes that don’t seem to be within the active path don’t keep information concerning this route. When a node receives the RREQ and determines a reverse path in its routing table and broadcasts the RREQ to its neighbor’s node, if it does not collect any RREP from its neighbor’s node for this request, it removes the routing information that it has documented.

- **Maximum utilization of the bandwidth:**
  This may be thought of the main success of the algorithm. Because the protocol does not need periodic universal advertisements, the demand on the obtainable information measure is a smaller amount. The sequence number counter is maintained by every node so as to follow any stale cached routes. All the intermediate nodes in a full life path change their routing tables conjointly
check that of most utilization of the information measure. Since, these routing
tables are going to be used frequently if that intermediate node receives any
RREQ from another source for same destination. Also, any RREPs that are
received by the nodes are compared with the RREP that was propagated last by
the destination sequence numbers and are discarded if they are not higher than the
already propagated RREPs.

– **Simple:**

  It is easy with every node behaving as a router, maintaining a routing
table, and the source node starting path discovery request, creating the network
self-beginning.

– **Most effective routing info:**

  When broadcasting an RREP message, if a node locates to receives an
RREP message with less significant hop-count, it changes its routing information
with this enhanced path and broadcast it.

– **Most current routing info:**

  The route information is retrieved on demand. Besides, after transmitting
an RREP message, if a node collects an RREP message with larger destination
sequence number, it changes its routing information with this latest path and
propagates it.

– **Loop-free routes:**

  It maintains loop-free routes by means of the easy logic of nodes
removing non better data packets for similar broadcast-id.

– **Coping up with dynamic topology and broken links:**

  Once the nodes are moving from their network and the network topology
is changed automatically or the communications in the dynamic path are
disconnect, the neighboring node that find out this link breakage transfer an
RERR packet. And also the source node recreated the path discovery if it still
wishes the route. It is guarantee for quick response to broken links.
– **Highly Scalable:**

It this algorithm, used minimum space complexity and broadcasts avoided once it compared with DSDV [40].

– **Security flaws in AODV:**

AODV avoids issues related to DSDV, DSR algorithm that store endlessly updated routes to any or all the destinations within the network. At the same time AODV has many security flaws. This leads to many attacks. In this thesis, addressing some of the attacks in AODV. The next section deals with the security issues connected with the networks.

5.3 **Black hole attack on AODV**

The black hole attack can be classified into many groups in terms of the approach accepted by the malicious node to initiate the attack. Particularly the malicious node will designedly drop all the forwarded data packets surfing it (black hole), or it will by selection drop the packets originated from or destined to sure nodes that it dislikes. Black hole attack in MANETs could be a serious security drawback to be solved [140].

So as to initiate a black hole attack, the first step for a malicious node is to find a way that allows it to get involved in the route forwarding path of data or control packets. To do so, it exploits the vulnerabilities of the underlying routing protocols which are generally designed with strong assumption of trustworthiness of all the nodes participating in the network.

Thus, any node will simply act and give a strict damage to the network by targeting both data and control packets. Dropping packets results in suspend the continue communication between the source and the destination node. Additional seriously, an attacker that captures the incoming control packets will stop the associated nodes from establishing routes between them.

In AODV, the originality of routing information determines by using the sequence number, and it contained within the message from the originating node. Once creating RREP message, a destination node compares its current sequence number, and
also the sequence number within the RREQ packet plus one, so selects the larger one as RREP’s sequence number. Upon receiving a number of RREP’s, the source node selects the one with the greatest sequence number so as to construct a route.

But, within the presence of black hole attack once a source node transmits the RREQ message for any destination node, it right away responds with an RREP message that has the best sequence number and this message is perceived as if it’s coming back from the destination or from a node that contains a recent enough route to the destination node. The source node takes for granted that the destination node is behind the black hole node and discards another RREP packets coming from another nodes. The source node immediately starts to send out its data packets to the black hole node trusting that these packets can reach the destination node. Thus the black hole node can be a focus for all the packets from the source node and rather than forwarding those packets to the destination it’ll merely discard them. So the packets concerned by the black hole node in no way reach the destination. Thus, the attack typically ends up in terribly low packet delivery ratio.

In AODV, the black hole attack takes place after the attacking node receives RREQ for the destination node that it is going to represent. To reach in the black hole attack, the attacker should generate its RREP message with sequence number greater than the sequence number of the destination node [141]. Upon receiving RREQ message, the attacker sets the sequence number of RREP as a very high number, in order that the attacker node will perpetually attract all the data packets from the source node, so drop the packets [142].

The implementation of black hole attack in AODV routing protocol consists of 2 steps. They are

Step 1: Causing false RREP message with highest sequence number and lowest hop count.

Step 2: Overwhelming its own packets however dropping different packets routed through black hole node.
5.4 Problem description

Security is one in every of the foremost primary issues in MANETs for the security of communication and data. For network process it's needed to carry out routing and packet forwarding. Thus more numbers of protection techniques has been build to counter live the malicious attacks. In this techniques used for the security of MANETs are unit referred to as protective and reactive mechanism. In protective mechanism, contains as access controls, secret writing techniques and authentications. In Reactive mechanism, completely various systems like Intrusion Detection Systems (IDS) and cooperation mechanisms are used. Just in case of MANETs intrusion is employed for detection of misuse. Black hole downside in MANETs [143] could be a serious security downside to be resolved.

The standard routing protocols face several issues owing to the dynamic behavior and resource constraints in MANETs. To beat this restriction, an approach to reach such quality is to use a biologically-inspired mechanism. Attack can occur when the malicious node present in the network is intended to attack directly the data traffic and intentionally drops, delay or alter the data traffic passing through it [144]. Black hole attack is incredibly dangerous active malicious node attacks on the MANETs. This problem arises at a malicious node joins during the week infrastructure network.

In black hole attack, a malicious node uses its routing protocol so as to announce itself for having the shortest path to the destination node or to the packet it wishes to interrupt. This hostile node advertises its availableness of contemporary routes regardless of checking its routing table. During this means offender node can continually have the supply in replying to the route request and so intercept the information packet and retain it [145]. It supported flooding, the requesting node is going to received the malicious node reply before the actual node response; hence a malicious and cast route is formed. Once this route is created, presently it’s up to the node whether or not to drop all the packets or forward it to the unknown address [146].

Figure 5.1 shows however malicious nodes occur in the network. The node ―S‖ is a source node and ―D‖ is the destination node. ―S‖ wants to send data packets to node ―D‖ and create the route using the route discovery process. So if node ―4‖ acts as a
malicious node then it will declare that it’s active route to the desired destination as soon as it receives RREQ packets. The malicious node immediately replies to the node “S” before some other node response. During this method, the node “S” can assume that this is often the active route and so active route discovery process is completed. Node “S” can ignore all other nodes replies and can begin sending data packets to node “4”. Finally, all the data packets will be lost.

![Figure 5.1: Black hole attack problem](image)

As an outcome, the source and the destination nodes cannot be communicate sufficiently with each other. While AODV treats RREP messages having higher sequence number to be fresher, the malicious node all the time send the RREP having higher sequence number [147]. So RREP message, once received by source node is treated anew, too. The result is that there is a high probability of a malicious node attempt to organize the black hole attack in AODV.

5.4.1 Black Hole Attack Caused By Route Request (RREQ)

An attacker will send imaginary RREQ messages to create black hole attack [148] with a non-existent node address. Every node can change their route to travel through the non-existent node to the destination node. As a result, the conventional route is going to be counteracted.

The attacker will generate black hole attack by faked RREQ message as follows:
1. Set the sort field to RREQ (1).
2. Set the conceiver address information to the originating node’s informatics address.
3. Set the destination informatics address to the destination node’s informatics address.
4. Set the source informatics address (in the informatics header) to a non-existent informatics address (black hole).
5. Increase the source sequence range by a minimum of 1, or reduce the hop count to 1.

The attacker creates a black hole attack between the source node and the destination node by faked RREQ message since it is shown in figure 5.2.

![Figure 5.2: Black hole node is formed by faked RREQ](image)

5.4.2 Black Hole Attack Caused By Route Reply (RREP)

The assaulter could generate a RREP message to create part as follows:
1. Set the sort field to RREP (2).
2. Locate the hop count field to one.
3. Set the conceiver informatics address because the originating node of the route and therefore the destination informatics address because the destination node of the route.
4. Increase the destination sequence range by a minimum of one.
5. Set the source informatics address (in the informatics header) to a non-existent informatics address (Black hole).
The attacker to transmission faked RREP message to the neighboring node. Once neighboring node receives the faked RREP message, it'll update its route to destination node through the non-existent node. Then RREP Black hole is made because it is shown in figure 5.3.

![Diagram showing Black hole node formation](image)

Figure 5.3: Black hole node is formed by faked RREP

The following pseudo code for attacker sending false RREP message with highest sequence number and lowest hop count:

```c
void BHA_AODV::recvRequest(Packet *p) {
    ---------------
    if (rq->rq_dn == index) {
        // The node is destination node
    ---------------
    } else {
        // The node is black hole node
        sendREP(
            rq->rq_sn,  // rt->rt_hops + 1,
            1,         // Lowest hop count
            rq->rq_dn,  // Original node
            rt->rt_sqno,  // Highest sequence number with 32 bit number
            4294967294,
        );  // else
    }
}
```

Figure 5.4 shows the output of highest sequence number from the malicious node. Here, the node 45, 46, 47, 48 and 49 are assigned as malicious node, it can be reply the faked RREP message to neighboring nodes.
5.4.3 Dropping Routed Packets

The attacker broadcast sequence number is higher than another nodes sequence numbers, so the source node 1 will select the route that sends all its data packets through node 3 and black hole node 5 to the destination node 6. Therefore, by sending false route reply, the malicious node attention all the data packets towards it. Once it receives packets, if the packets are set to it, then it simply drops the packets. Figure 5.5 shows the packet drop at the attacker node.

For the routine analysis of the network, a usual glowing performed AODV routing protocol is used as a suggestion. Then malicious nodes are established into the network. Simulations using NS-2 are carried out without black hole node and with black holes on the routing protocols AODV.
The following pseudo code for packets drop at black hole node is given below:

```c
void BHA_AODV::recv(Packet *pkt, Handler *)
{
    struct hdr_cmn *ch = HDR_CMN(pkt);
    struct hdr_ip *ih = HDR_IP(pkt);
    -----------------------
    if((u_int32_t)ih->daddr() == index)
    {
        // consuming its own packets
        ----------------------
    }
    else
    {
        // malicious node
        dropdata (pkt, DROP_RTR_ROUTE_LOOP);
        // Received all data packets are dropped
    }
} // end of BHA_AODV::recv
```

5.5 Simulation of black hole attack

Using Network Simulator tool under a various range of mobility and traffic scenarios used to evaluate the performances of the AODV routing protocols with and without black hole nodes. The entire simulations are carried out using NS 2.34 network simulator. It is fit for designing new protocols, comparing different protocols and traffic evaluations. NS2 is developed as a mutual environment and also distributed as open source software. In table 5.1 shows simulation parameters for evaluate performance of the routing protocols.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulator</td>
<td>NS 2 (version 2.34)</td>
</tr>
<tr>
<td>Simulation time</td>
<td>500 sec</td>
</tr>
<tr>
<td>Number of mobile nodes</td>
<td>100</td>
</tr>
<tr>
<td>Topology</td>
<td>1000 m X 1000 m</td>
</tr>
<tr>
<td>Transmission range</td>
<td>250 m</td>
</tr>
<tr>
<td>Routing protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Traffic model</td>
<td>CBR</td>
</tr>
<tr>
<td>Maximum speed</td>
<td>40 m/s</td>
</tr>
<tr>
<td>Packet size</td>
<td>512</td>
</tr>
<tr>
<td>Number of black hole nodes</td>
<td>2 nodes</td>
</tr>
<tr>
<td>Mobility model</td>
<td>Random way point</td>
</tr>
<tr>
<td>Data rate</td>
<td>10 mbps</td>
</tr>
</tbody>
</table>

Table 5.1: Simulation parameters

The figure 5.6 shows the result of the Packet Delivery Ratio (PDR) measured for the AODV protocol with malicious node and without malicious node when the node mobility is increased. The result shows both cases with and without the black hole attack. It is measured that the packet delivery ratio dramatically decreases when there is a malicious node in the network.

Figure 5.6: Packet delivery ratio of AODV without and with black hole attack
The PDR is 98.5% once there is no impact of malicious node and once the node is moving at the speed 10m/s, however due to the impact of the malicious node the PDR reduces to 89.6%, as result of a number of the data packets are dropped by the malicious node.

Figure 5.7: Throughput on AODV without and with black hole attack

Above figure 5.7 shows the network throughput and it is also decreases due to the malicious effect as compared to without malicious node.

Figure 5.8: Average end-to-end delay on AODV without and with black hole attack
From the figure 5.8 it is determined that, there is slight increase within the average end-to-end delay while not the impact of black hole, as compared to the impact of malicious node, this is often attributable to the immediate reply from the malicious node i.e., the character of malicious node here is that it might not check its routing table.

![Average Jitter in %](image)

Figure 5.9: Average jitter on AODV without and with black hole attack

It’s determined from the on top of figure 5.9 that, average jitter between the nodes is higher than without the malicious node, as compared to the average jitter between the nodes. This is due to the malicious nodes that provide the path with fewer numbers of nodes, or smaller path. Thus, average jitter between the nodes is reduces.

### 5.6 Summary

The results demonstrate that in presence of a black hole, packet loss in the network increases considerably. The network experienced 88.3% packet loss on an average due to the introduction of a single black hole node and 98.2% packet loss with two black hole nodes. This loss is partially due to packets dropped in the black hole node and partially due to congestion in the network over the paths towards the black hole node. Therefore, the best routing protocol for minimizing the black hole attack may be determined.