CHAPTER V

BLACKHOLE ATTACK IN MANET

5.1 Detection Techniques for Black hole Attack
5.2 Proposed Algorithm
5.3 Simulation and Results
5.4 Closing Remarks
CHAPTER-V
BLACK HOLE ATTACK IN MANET

In black hole attack, the malicious node promotes its availability to forward traffic. Depending on particular routing protocol, this can be done by either
- Broadcasting smallest path to destination through it or
- Claiming fresh routes to a destination in response to route requests.

A forged route is created and all traffic is moved to the malicious node. Packets are now at the discretion of the attacker who may wish to silently drop the incoming traffic.

In Black hole attack, malicious nodes attack while the route is being selected. One malicious node employs the routing protocol to choose the smallest path to the destination node, drops routing packets and does not forward packets to its nearby nodes in a Blackhole attack (Kumar et. al, 2014). Single Blackhole node can simply attack mobile Ad hoc networks (Mehta, et. al, 2013).

AODV is a reactive routing protocol which uses a broadcast route discovery mechanism (Sawant and Rawat, 2014). The protocol functions in two phases: route discovery and route maintenance. Route Discovery process is held whenever a source node wishes to talk with another node for which routing information is not present in its table. In Route Maintenance, symmetric links are assured by Periodic hello messages. AODV protocol is prone to many attacks such as black hole, warm hole and so on. Black hole attack is more adverse on AODV protocol as compared to other protocols. AODV stands for Ad-Hoc on Demand Distance Vector Routing algorithm. It is an algorithm which initiates route discovery only on demand, that is, a route is invented only when a route is needed for communication. In the process of route discovery, the following packets are used:

- RREQ: Route Request
- RREP: Route Reply
- RRER: Route Error
In Black hole attack, the malicious node awaits nearby nodes to send RREQ messages (Sawant and Rawat, 2014). When RREQ message is got by the malicious node, it sends a wrong RREP message without checking the routing table, and quickly gives a route to the destination, before other nodes send a real one. It assigns a high sequence number in order to get down in the routing table of the victim node. Therefore the process of route discovery is assumed to be completed by requesting nodes and ignore RREP messages of other nodes and by sending data packets to malicious node. All RREQ messages are now being attacked by the malicious node. When a link is not working and it is detected for the next hop of an active route, a RERR (Route Error) message is sent to its active neighbors that were using that particular route. (Soni and Nayak, 2013) The key vulnerabilities present in the basic AODV routing protocol are:

- Deceptive increment in Sequence Numbers
- Deceptive decrementing of Hop Count.

Blackhole attack is a main security threat in MANET. Assaulting node makes use of the protocols and misguides by revealing the smallest path to the desired node in a black hole attack. But rather than sending the packets to its neighboring node, the malicious node eventually drops routing packets (Perkins and Royer, 1999; Maan et.al, 2011)

A blackhole attack first attack into the multicast forwarding group by instigating a rushing attack by keeping in mind the end goal of capturing the information group of the multicast session. The aggressor drops a few or the majority of the packets that it gets as not in favor of sending the packets to the following nodes on the route. This type of assault frequently brings about low packet delivery ratio (Nguyen and Nguyen, 2008).

Ad hoc On-Demand Vector routing (AODV) protocol is the most famous MANET routing protocol. Many benefits are offered by this protocol such as dynamic, self-starting and multihop routing. Moreover, it is able to adapt changes of MANET topology and cannot accept the inactive routes automatically, (Perkins and Royer, 1999).
Blackhole Attack in Manet

Sadly, AODV is vulnerable to many routing assaults. (Maan et. al, 2011; Ramaswamy et. al, 2003).

Blackhole attack is one of the most dangerous attacks in AODV-based MANET, (Ramaswamy et. al, 2003). In this attack, false routing data is produced by the assailant and it is transmitted to the casualty nodes to cause false route entries in the routing tables of the nodes. Accordingly, numerous erroneous routing exist and bottleneck is caused in the communication channels. There are various types of directing conventions in MANET. In this segment, we will examine a part of the renowned steering conventions.

5.1 Detection Techniques for Blackhole Attack

In this section we have reviewed the different detection technique proposed by number of researchers all over the world in the last decades:

5.1.1 (Banerjee, 2008) proposed an approach to save the mobile ad-hoc network from the Gray Hole and Black Hole Attacks. They give us a technique which is efficient to discover cooperating malicious nodes, which drop a significant fraction of packets.

5.1.2 (Kurosawa et. al, 2007) have found an anomaly detection scheme. Source node receives more than one RREP after broadcasting RREQ, and calculates a threshold value which is the average of difference between vale of destination_seq no. of RREP Packet and the value stored in the list before the process. Further in this process this calculated value has the reference of the malicious node.

5.1.3 (Tamilselvan et. al, 2007) proposed a solution for detecting the black hole. They ensured the reliability of route before sending the data packets over it. AODV protocol has been modified in this solution. When source node receives RREP message it does not begin to send data packets immediately. It assures the safe route for sending data packets after waiting for receiving RREP messages from other neighboring nodes. The most reliable route is selected by the source node having more repeated common nodes. If there is no repeated common node and if the replying node provides information
about its next hop then the route is assumed reliable by the source node. The drawback of this solution is Processing delay.

5.1.4 (Su et. al, 2010) Anti-Blackhole Mechanism (ABM) was introduced as an Intrusion Detection System. When suspicious value goes beyond threshold (difference between RREQs and RREPs) a block message is broadcasted by nearby IDS. Three assumptions are made to use this method, i.e., two neighbor IDS should be within each other’s transmission range, an authentication mechanism to prevent block message and node id forging. Authentication mechanism adds overhead in processing.

5.1.5 (Vishnu et. al, 2010) Mechanism of detection and removal was proposed for black hole attack. This mechanism makes use of Backbone Nodes (BBNs). BBNs are used to provide Restricted IP (RIP). Source initially requests nearest BBN to allocate an RIP. After getting RIP, source broadcasts RREQ for RIP as well as destination. If source receives RREP for only destination, it means no malicious node is there. Else, a notification message is sent to all nodes by source node and source transmits dummy packets to destination.

5.1.6 (Sen et. al, 2011) postulated a solution to determine a Black Hole attack in standard AODV protocol. In the main advantages of proposed mechanism any cryptographic metrics is not applied. Instead, it protects the ad hoc network by determining and showing reactions to malicious activities of some intermediate nodes. Simulation results show us that this technique has a significantly higher detection rate along with the moderate Network Traffic Hidden Overhead and Computation Overhead.

5.1.7 (Jain et. al, 2010) proposed a technique which works on the concept of communication in which only limited size data packet should be transmitted from source to destination instead of sending huge amount of data packets. The information about malicious node is kept locally with each participation node so at any instant of time this information can be shared in the Network. So this information is kept away from malicious node which can be the cause of black hole attack into the system.

5.1.8 (Gupta, 2013) Modified Enhanced AODV (MEAODV) has been proposed which was the enhanced version of EAODV (Enhanced AODV). Route
discovery procedure is used to identify the impact of black hole attack by the MEAODV. MEAODV has various different and slightly improved calculations as compared to EAODV for examining RREP messages. Simulation results which stated high degree of performance by MEAODV as compared to EAODV in terms of better Performance Delivery Ratio (PDR) and less End-to-End Delay.

5.1.9 (Dhurandher et. al, 2013) With improved version of routing protocol, detection of collaborative black hole attack takes place having the control packets called CONFIRM, CHCKCNFRM and REPLYCONFIRM for checking traffic in effective manner. Simulation results also show that algorithm is packet traffic efficient as well as time efficient and greater than that of conventional AODV.

5.1.10 (Jhaveri, 2013) presented MRAODV which is the outcome with modification in R-AODV working towards overcoming the limitations in existing mechanisms. MR-AODV isolates Blackhole during route discovery phase instead of this previous algorithm R-AODV which worked upon providing novel secure path. So, from the above technique it works efficiently for normalized routing overhead in MRAODV. Simulation results prove that the MR-AODV is the reliable solution which works under various network parameters and traffic conditions.

5.1.11 (Arya et. al, 2014) have proposed the symmetric key based authentication security to secure the AODV routing protocol in MANET. Here, key pre distribution technique is used in which set of symmetric keys is assigned to each node at the time of deployment for the purpose of speeding up the algorithm.

5.1.12 (Jain and Khuteta, 2015) proposed mechanism that the security of modification on Ad-hoc On Demand Distance Vector (AODV) which acts like self-initiating routing protocol for MANETs, is degraded with an attack known as “Blackhole” attack. In the proposed plot it has been passed on that base node in the framework that constructs the probability of recognizing distinctive malevolent node in framework and further separates them from taking an interest in any correspondence.
5.1.13 (Siddiqua et al., 2015) Scheme proposed that every last node in the system condition engages its neighboring expectations indiscriminately. As indicated by us here, in unbridled mode, each node screens the bundle being sent by its neighbors keeping in mind the end node to watch the conduct of neighbor with respect to parcel activity. Each hub contrasts the close-by data and the data it stores in its information table. In the event that both are same the hub accepts that bundle which is sent further, generally hub sits tight for specific measure of time and checks the explanations behind parcel dropping. With a specific end goal, affirm bundles are sent to its neighbor, the hubs screens the control parcels and in addition information bundles to forestall particular dropping, as dark gap assault drops chosen parcels. Keeping in mind the end goal to screen the sent bundles, each hub needs to keep up learning tables with following passages: $F_m, r_m$ if the qualities vary, the hubs are dark opening hubs. A protected learning calculation for alleviating dark opening assault in AODV convention is suggested. The calculation directs the information bundles that are being sent in wanton mode to guarantee that the parcels are conveyed to final node.

5.1.14 (Abdelshafy and King, 2016) Self-Protocol Trustiness (SPT) an idea was proposed that a Blackhole Resisting Mechanism (BRM) which doesn’t require cryptography solutions or costly instruments. It simply works upon Timer concept which is used for finding threshold values for the accurate calculation of searching legitimate path or nodes.

5.1.15 (Pham and Yeo, 2016) For identifying malicious activity by any individual nodes they prove the check based on their performance metrics in which if any malicious node advertise wrong perception about their own self and involve in dropping data continuously it will be calculated by calculation on the malicious node by comparing the differences.

5.1.16 (Savner and Gupta, 2014) proposed a novel group arranged thought to enhance security and capability of the framework. As indicated by us, this methodology defends the perfect execution of MANET in closeness of dark opening assault. The re-enactment of the proposed procedure is finished
using NS2 arrange test framework and the reproduction comes about mirrors the execution of plan for location and prevention for the assaulted blackhole.

5.1.17 (Sharma and Bisen, 2016) For identification of the black-hole or malicious node a method is being proposed. In this procedure, a kind of trap strategy is incorporated into AODV convention for the acknowledgment of dangerous hubs. Right when the Black-gap hub is recognized after that an aggravating procedure is initiated to make distinctive hubs aware of noxious nodes.

5.1.18 (Sathish, 2016)To save the network from black hole attacks, it is necessary to discover malicious nodes during the process of route discovery, when they pass fabricated RREP imitating the source node. Our proposed methodology does almost the same. Based on next hop information and destination sequence number that can be extracted from RREPs, this scheme handles single and collaborative black hole attacks with extenuated computational, routing and storage overhead.

5.1.19 (Yadav et. al, 2017) Novel outlier detection scheme is proposed to make AODV routing protocol safe from black hole attack. The working process of our algorithm is as evident receiver node “R” receives the multiple copy of route request packet, i.e., RREQ from different paths. Route to hop count value is decreased by the malicious node “M (Black hole attack). On receiving multiple RREQ, it makes the sorted vector of received RREQ according to their hop count values. In general “R” selects the best and sorted route which has the least hop count value for sending the route reply packet. But in proposed scheme, “R” checks the validity and authenticity of the route. It calculates the median of the all received hop count values and calculates the absolute difference between median and coming hop count values for each and every route. If the difference is greater than threshold, i.e., threshold parameter decided from experiment. In this scheme its value is 10 and hop count value in their RREQ packet. Then corresponding route is discarded for transmitting the RREP and then next route is selected for their validity. In this way our proposed algorithm efficiently detects the black hole attack and makes the system more secured than the existing algorithm.
5.2 PROPOSED ALGORITHM

After reviewing all the detection techniques we have proposed an algorithm TBBM-AODV. In the proposed algorithm black hole nodes are identified which usually behave like normal nodes but pretend to have the highest sequence number or possess the shortest route path to the destination. Due to this behavior, the source node accepts the malicious node for sending data packets and the underlined node smartly absorbs all the data packets. Thus, the malicious node won't forward the data packets to the destination node for which they were expected and all the data will be lost or absorbed. The protocol in the proposed algorithm is a slightly modified version of AODV protocol that introduces the concept of timer.

In the underlying algorithm, source node sends the route request (RREQ), begins a timer to track the RREP packet, initializes a buffer to store the responses and waits for the route reply (RREP). The buffer will store RREP messages that come from the intermediate nodes or the destination node itself until the timer is expired, after then the source node does not accept any RREP response.

The proposed approach is different from the AODV protocol in the context of timer. Here, the source node is expected to send or transfer the data packets as soon as it receives the route reply (RREP) message. The timer and buffer mechanisms both are playing vital role in this algorithm. In our methodology, the time for which the timer is set for a period the buffer stores the RREP coming from the intermediate nodes or from the destination node itself. Synchronization is important in this approach.

Our algorithm ignores or discards the first RREP stored in the buffer as it has a higher probability of having a Blackhole, considering the fact that the malicious node fakes its identity and claims of having the shortest path to the destination. This is the modification proposed different from the AODV proto-col. Initially, the source node broadcasts a RREQ (Route Request) message to the destination and intermediate nodes and waits for the RREP (Route Reply) same as in the AODV protocol.
Then, the source node discards the first RREP message as discussed earlier. Then the source node sets a timer and initializes a buffer. All the RREP messages that are delivered to the source node before time out session are stored in the buffer.

5.2.1 Algorithm : Timer Based Buffer Management - AODV

1. procedure Send
2.   for each sender s ∈ S do
3.       s → RREQ;
4.       Timer_time = FT * (n - 1);
5.       Initializes Buffer;
6.       Buffer ← RREP ; Discard 1st RREP Since it contains high probability of blackhole
7.       s ← Buffer[RREP Timer]; RREP can be received via Intermediate Node (InN) or Destination Node (DN)
8.       if RREP ← DN then
9.          Compare SEQNO[RREP ] & SEQNO[Discarded RREP ]
10.         if Difference == Small then
11.             Path ← Legitimate
12.         else
13.             Discard RREP
14.       s ← Buffer[RREP + 1]
15.       end if
16.       else
17.         if RREP ← InN then
18.            s → RPLY → DN. To check suggested Route
19.            DN → ACK → s
20.            if s ← ACK then
21.                Path ← Legitimate
22.            else
23.                Discard RREP
24.            end if
25.        end if
26. end if
27. SN checks Timer of All RREP packets
28. if Any Condition == True then
29. Route Data
30. else
31. Discard RREP & Generate New RREP and begin again from Step 1.
32. end if
33. end for
34. end procedure

The time of the timer starts when the first RREP arrives at the source node. The time for the timer is set by the given equation.

\[
\text{Timer\_Time} = FT \times (n - 1)
\]  

(5.1)
here, \( FT = DT + PT \)

where \( FT \) is abbreviated as full time; \( DT = \) delay time and; \( PT = \) processing time.

Delay time is the time that a node takes in case of a low network problem and processing time is considered as the time taken by each node for receiving a RREQ message, reading, processing and queuing it. The sum of the delay time and processing time is here denoted by full time, i.e., \( FT \) and \( n \) is the total number of nodes present in the network (10 in this case). The product of full time and \( n-1 \) is considered as the Timers time. After timeout, source node selects the legitimate path to transfer data to the destination node.

5.2.2 Three Modes of Attack:

In our approach after the RREP messages are buffered, the source node decides which RREP is useful, legitimate and reliable. For this purpose three cases are tested in which a black hole node can attack in the network. Among the three cases: First checks whether RREP could show the highest destination sequence number, second inspects if it claims that it has the shortest path for the destination
and third tests if any malicious node can declare itself as a destination node just to get control over the data packets.

When all the RREP messages are checked for the mentioned cases, the source node finalizes the safe RREPs. If the conditions given in the algorithm are satisfied then only the source node is expected to route data otherwise the source node generates a new RREQ in the search of a legitimate path to the destination.

5.2.3 **Mechanism to check 3 Modes of Attack:**

After processing the first RREP, the source node processes the next RREP message stored in the buffer. It can either be received from an intermediate node or a destination node itself. If it is sent by a destination node then the source node compares its sequence number with the sequence number of the destination, if the difference is not large, then it is considered as a valid path otherwise it is treated as a blackhole which is masquerading itself as a destination node. In this condition the source node cancels this RREP and processes the next RREP stored in the buffer.

In the other case source node inspects if this RREP message is received from an intermediate node, which is declaring to have a path to the destination node. Then the source node sends a reply (RPLY) message to the destination node using the route provided by the intermediate node and waits for an acknowledgment. If the acknowledgment is not received then the node is considered as a BlackHole which was faking to have a fresh route to the destination and is discarded by the source node.

After rejecting this RREP the source node processes again the next RREP stored in the buffer. The source node again inspects all the above mentioned cases and if it finds the next RREP genuine then it is selected by the source node for sending the packets to the destination node. In the end, the source node will cross-check the buffer whether all the RREP messages stored are checked or not before the timeout. If the buffer is empty, and SN finds legitimate RREPs then the data is routed otherwise the source will generate another RREQ and begin new session.
In the figure 5.1 we have a network which is following the AODV protocol. In this figure 5.1 SN is behaving as a Source node which has a message to send to the DN node which is destination node.

Figure 5.1: Showing the blackhole attack and its detection using the proposed algorithm

It has 3 options for doing that as we can see in the diagram. For minimizing the effect of Blackhole we can use the following methods.

**Steps of the algorithm:**

**Initial Steps:-**

1. for each sender s Î S do
2. s → RREQ;
3. Timer_time = FT * (n - 1);
4. Initializes Buffer;
5. while timer > 0 & for each RREP do
6. Buffer ← RREP. It has 3 RREPs in this case as shown in above diagram
7. end while
8. Check each RREP. Whether it is legitimate or not.
9. end for
Phase 1: D is the malicious node
10: Received first RREP
11: if RREP ← D then Having highest Sequence Number
12: Discard RREP Since it contains high probability of Blackhole
13: end if

Phase 2: C is acting as a malicious node pretending to be the destination node
14: C masquerades to be DN
15: C Compares SEQNO[DN]
16: Compare SEQNO[RREP ] & SEQNO [Discarded_RREP ]
17: if Difference == Small then
Phase 3:- H is claiming that it has a fresh Root node to the destination node
(Acting as an Intermediate node)
23: \( s \rightarrow \text{RPLY [DN]} \) SN will send Reply message to the destination node DN following this path directed by H
24: \( s \) waits for ACK
25: if RREP \( \leftarrow \) InN then
26: \( \text{DN} \leftarrow \text{RPLY} \)
27: if \( s \leftarrow \text{ACK} \) then
28: \( \text{Path} \leftarrow \text{Legitimate} \)
29: else
30: Discard RREP
31: end if
32: end if

Final Steps:-
33: for each RREP do
34: Check Timer
Black Hole Attack in Manet

5.3 SIMULATION AND RESULTS

The Simulation is performed using Network Simulator 3 (NS-3). Mobility scenarios are generated using Random waypoint Model by varying 25 to 100 nodes and Attackers varying by 0 to 10 attackers’ node. The simulation parameter are summarized in table.1 the performance of the routing protocol is measured in varying: Increasing Network size and Increasing No. of attackers

5.3.1 Performance Metrics

The performance of this simulation is measured under the metrics like APDR, EED, Dtime, Drate.

5.3.2 Average packet delivery ratio (APDR)

The number of data packets actually received by the receiver over the number of data packets which a sender transmits is known as packet delivery ratio (PDR) of a receiver. Average PDR is average of PDR taken over all receivers is known as APDR.

\[ APDR = \frac{1}{n} \sum_{k=1}^{n} \frac{DPK_k}{SPK_k} \]

where \( DPK \) = Data Packet received by Destination \( SPK \) = Data Packet transmitted by Source \( k=\text{th} \) application

5.3.3 End-to-end delay (EED)

EED or end to end delay for a packet can be defined as time taken by a packet to travel from source node to destination node.
\[ EED = \sum_{k=1}^{n} \frac{DL_k}{DPK_k} \]

where, \( DPK = \) Data Packet received by Destination
\( DL = \) Delay at destination node
\( k = k^{th} \) application

5.3.4 Detection Time (Dtime)

The detection time is defined as the passage of time consumed by an algorithm for the detection of a malicious node. Measurement of Dtime is the difference between start time and attack detection time.

\[ Dtime = \sum_{k=1}^{n} ADT - ST \]

where \( ADT = \) Attack Detection time \( ST = \) Start Time
\( k = k^{th} \) application

5.3.5 Detection Rate (Drate)

\[ Drate = \sum_{k=1}^{n} \frac{DBH_k}{BH_k} \]

Drate is the ratio of the no of blackhole node detected to how many blackhole node present in the network via algorithm.

where \( DBH = \) Detected Blackhole Node, \( BH = \) Blackhole Node
\( k = k^{th} \) application

Table 5.1: Simulation Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulator</td>
<td>NS-3</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>1000 sec</td>
</tr>
<tr>
<td>Pause Time</td>
<td>10 sec.</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>25 to 100</td>
</tr>
<tr>
<td>Node Mobility</td>
<td>10m/sec</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Number of attackers</td>
<td>0 to 10</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>2mbps</td>
</tr>
<tr>
<td>Application data</td>
<td>CBR with one packet per second and each session has 200 sec to transmit data.</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Random waypoint</td>
</tr>
</tbody>
</table>
As shown in figure 5.5, the packet delivery ratio is high initially when the network is less dense or we can say that the number of nodes present is less. The packet delivery ratio is the ratio of the packets actually received by the receiver and the total number of packets sent by the source. Here, some packets are lost because of the presence of malicious nodes in the network. The reason why this graph has maximum value at initial is minimum number of nodes are present initially and thus, the probability of a malicious node or an attacker node targeting this network is less. Since the number of malicious node is less, fewer packets will be lost which implies to high packet delivery ratio. Thus, the graph is decreasing as the network becomes denser.
EED or End to End Delay is defined as the time taken by a packet to reach destination node from source node. Now the ratio of source-destination nodes is fixed thus only the effect of attackers on various network terms is enhanced due to the increasing number of attackers and increasing number of nodes. As shown in figure 5.6 the end-to-end network delay increases due to increasing number of attackers because the attackers will either drop the packets or move them in a loop before sending them to its destination. In both the conditions, it will result in delay and the packet will take more time in reaching to destination node. Thus, the end-to-end delay will increase.

The detection rate is less at first and increasing constantly with the number of attackers. Given algorithm is used to detect the malicious nodes and the illegitimate routes so that the data will not be directed through those paths.

![Detection Rate with increasing number of attackers](image)

**Figure 5.7: Detection Rate with increasing number of attackers**

This will increase the Packet Delivery Ratio (PDR) as well as the efficiency of the network. But, when the network is less dense and less number of nodes is present then the probability of a malicious node being a part of that network becomes less. When there is no malicious node present in the path, the detection rate will automatically decrease. With the increase in number of nodes present in the
network, the probability of an attacker node targeting that network will also increase and this will increase the rate of detection.

The detection time is defined as the passage of time consumed by an algorithm for the detection of a malicious node. Initially, the detection time is less since the number of nodes present in the network is less and the probability of a malicious node attacking that network is minimum.

![Detection Time with increasing number of attackers](image)

**Figure 5.8: Detection Time with increasing number of attackers**

Thus, detecting an illegitimate node in this network will consume less time. But, as the number of nodes present in the network will increase the number of malicious nodes will increase. Detection of all these nodes will take time thus; the graph is increasing with the increase in number of attackers to a peak point. After a point the detection time will start decreasing a little bit, since when the number of attackers is increased the detection of all these malicious nodes is practically not possible thus, it will detect as many as possible and will take a less time.

As shown in the figure 5.9, the packet delivery ratio is high initially when the number of nodes present is less. Here, some packets are lost because of the presence of malicious nodes in the network. By using this algorithm for detection of malicious nodes we can eventually increase the packet delivery ratio. The reason behind this is that with increasing number of nodes the number of attacker nodes
also increases and they result in reducing the value of average PDR. But when these malicious nodes will be detected by using this approach then the packet delivery ratio can be increased with a fair amount of value. Thus, the graph is increasing as the network becomes denser.

Figure 5.9: Average Packet delivery ratio with Increasing no of nodes

Figure 5.10: End to End Delay with increasing number of node

As shown in figure 5.10 the end-to-end network delay increases due to increasing number of attackers because the attacks will either drop the packets or
move them in a loop before sending them to its destination. In both the conditions, it will result in delay and the packet will take more time in reaching to destination node resulting in increased value of end-to-end delay. But if the given algorithm is used for the detection of black hole then the end to end delay value can be minimized a little as depicted in the graph by the second line.

The detection rate is high at first and decreasing constantly with the increasing number of nodes. With the increasing number of nodes the probability of attacker nodes increases simultaneously. Given algorithm is used to detect the malicious nodes and the illegitimate routes so that the data will not be directed through those paths.

![Detection Rate with increasing number of nodes](image)

**Figure 5.11: Detection Rate with increasing number of nodes**

This algorithm will work with maximum rate when the network is less dense as the number of attackers are less and can be caught easily. When the number of attackers increases detecting them becomes complex due to which the rate of detection decreases constantly.

Initially, the detection time is less since the number of nodes present in the network is less and the probability of a malicious node attacking that network is also minimum. Thus, detecting an illegitimate node in this network will consume less
time. But, as the number of nodes present in the network will increase the number of malicious nodes attacking the network will increase. Detection of all these nodes will take time thus; the graph is increasing with the increasing number of attackers.

![Detection Time with increasing number of nodes](image)

**Figure 5.12: Detection Time with increasing number of nodes**

### 5.4 CLOSING REMARKS

In this Chapter we have presented a survey on securing MANETs against a packet dropping attack BlackHole attack. We have presented an algorithm which deals specifically with the detection, prevention and reaction mechanisms of a BlackHole attack. This is a purely timer based algorithm whose time limit is also described. Another feature of this algorithm is buffer mechanism which is used here to store the data packets before they are transmitted. Further, we have categorized the detection of malicious node into three phases according to their occurrence in any network and the specific strategies they can encounter. A comparative study between attacking the network using which the minimum processing time will be consumed by the algorithm to detect illegitimate using which the minimum processing time will be less dense then this algorithm can be used to find the optimum path from all possible ways to route data.