CHAPTER VI

COLLUSION BWHOLE ATTACK IN MANET

CHAPTER-VI

COLLUSION BW HOLE ATTACK

This chapter proposes a new attack. It can not only decrease the network speed but can also end up in defaming as it is difficult to know who the actual intruder is. This attack is known as Collusion BW Hole Attack. In MANET, the communication begins when a data or a message packet is to be transmitted to any other node. For sending this packet, the source node selects a path which is secure as well as less time consuming. For selecting this path, routing tables are observed by the source node. The advantage of demand of source node is taken by intruder for hacking the network and eventually data is stolen or dropped in Collusion BW attack.

The intruder node will work with internal nodes. These nodes will form a tunnel and rather than sending the data to the desired node, they will simultaneously send it to the intruder node. The whole strategy and methodology of this new proposed attack is described further in the thesis. This thesis includes only the illustration of this attack, the approach that it may use and the weaknesses of network that can be pointed by this attack.

It is a cluster that can talk with each other without a predefined and specified topology or central administration. MANETs by nature are dynamic. It means that any node can leave or join the network.

It provides flexibility because centralized system is absent and a decentralized system is followed by them. It means that server and client are not present. Hence, any node can function as a host and router at one time. (Satav and Jawandhiya, 2016) A MANET network can be formed easily at low prices because it does not follow the predefined and centralized infrastructure. This property is the main reason why MANET is becoming so popular these days. But because of its flexible and dynamic nature, it is becoming prone to many dangerous attacks. The main purpose of these attacks is stealing of the information that is passed between communicating parties. (Bai *et. al*, 2017; Imran and Qadeer, 2016) In MANET, there is no restriction applied on the node. So, this can lead to dangerous consequences like eavesdropping, denial of services, stealing of information, response delay etc.

A MANET is more vulnerable to attacks because of the following factors:

- Security solutions that are difficult cannot be used in MANET because the Nodes have limited energy.
- Routing and transmission is done by using wireless medium. Wireless medium makes eavesdropping more likely. They are generally unreliable as they are a shared network.
- The communication might be unreliable even after making the channel reliable due to the broadcasting nature of MANETs.
- It is difficult to ensure that all the nodes that are taking part in the network are benign because MANET does not have any central management point or node.
- The network topology of network keeps on varying and the mobility of nodes plays a very important role in the network. Thus, routing is very challenging. (Sharma and Chauhan, 2015; Salehi and Samavati, 2011; Burmester and de Medeiros, 2009;)

6.1 AODV

This protocol aims to provide short processing time, memory consumption and network utilization as well as quick adaption to dynamic forming links. It gives loop freedom by working on destination sequence numbers. (Soni and Nayak, 2013; Shoja *et. al*, 2011, Vishnu and Paul,2010; Sharma and Sharma, 2012)

6.1.1 Security Flaws in AODV

Due to security features; some more secure protocols are designed to provide the authentication, confidentiality, integrity.

The misconduct of an inside attacking node is discussed. The actions performed by the inside attackers are:

1) It may modify or mould the RREQ or RREP packets.
2) It may spoof either the destination IP or the source IP and thus it is able to receive or drop data packets to work as a legitimate node.
3) It may generate a fake RERR packet to make a rise in the routing delay.
4) To cause a DoS attack, the attacker may send mock RREPs of highest sequence numbers (like Blackhole attack).
5) It may create the routing loops and launch sleep deprivation or resource consumption attacks to deplete the node batteries.
6) It replays old routing messages or form a tunnel/wormhole to interrupt the normal routing behavior.(Sharma *et. al*,2014; Revathi and Geetha,2012; Soni and Nayak,2013; Nikam and Raut, 2015; Kannhavong *et. al*, 2007; Gupta and Pathak, 2016; Shoja *et. al*, 2011)

6.2 COLLUSION BW HOLE ATTACK MODEL

When an RREQ is transmitted from a source node to other nodes for transferring of the package then MN1; the malicious node; may send Route Reply.

We know that the lower sequence number replaces the higher sequence number and permits the source node or other node to send the packet with the node with higher sequence number. Here, the source node transmits the packet from the malicious node. The malicious node MN1 again sends route request (RREQ) for the transmission of packet. After that, again a malicious node MN2 sends route reply with higher sequence number and the packet is again transferred through the malicious node MN2.

When a packet is sent to second malicious node MN2 in the network, it tunnels the packet to the other malicious node MN3. After the tunneling of packet to the malicious node MN3, usually RREQ broadcast takes place but here in the case of this attack unicast occurs and the packet is dropped. This attack satisfies the vulnerability present in AODV. So, detection of this attack is not possible easily manner isreasons for this are as follows:

1) To modify or mould RREQ or RREP packets.
2) Source IP address or Spoof destination pose as the authorized network node and thus drop or receive the data packets.
3) Make a tunnel/wormhole or replay old routing messages to interrupt the normal routing behavior.

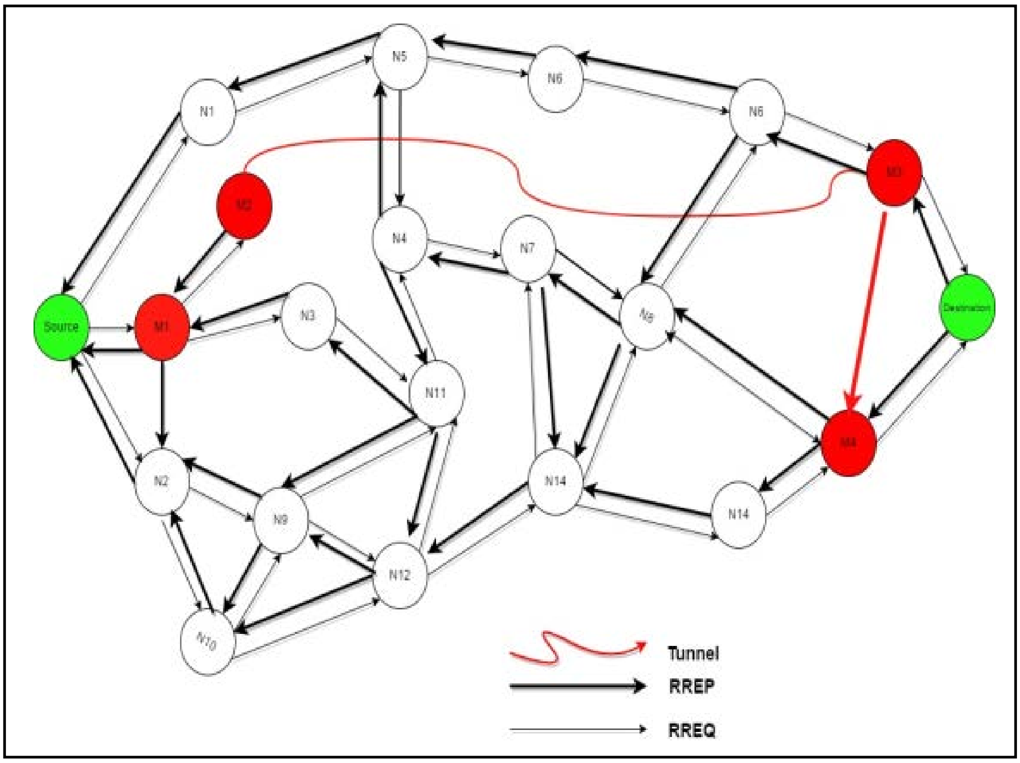

Figure 6.1: How a packet is dropped in Collusion BW Hole Attack

In wormhole attack, the attacking node captures the packet from one location and sends that to the other node which is located at a distance. A wormhole attack can be exploited very simply by the attacker without sacrificing with the legitimate node and without having its knowledge. On the other hand, in black hole attack, when the source node tries to transmit some data packets to a destination node, and begins the process of route discovery then a malicious node, MN1 shows that it has the route for the destination node every time it receives RREQ packets. Then the response is sent to source node at once. If the reply from a normal node for example (N1,N2,...,N14) etc. reaches the source node of the RREQ first, everything works well but when the packet is received by MN1 node then it makes the source node think that the routing discovery process is completed and ignores all other reply messages, and starts to send data packets. A forged routing is created. The outcome of which is that all the packets through MN1 are simply consumed or lost and never received by its desired destination. Collusion BW Hole Attack is not similar this attack as in this attack the packets are dropped once received by the malicious node. On the other hand, in Collusion BW Hole Attack there is no packet drop by first malicious node and in worm hole attack after tunneling the packet broadcast occurs while in Colliding Collusion BW hole attack unicast occurs and the packet is dropped by the malicious node. But at the same time, the RREP and RREQ route request and reply of the neighbour legitimate node are managed such a way that the dropped packet node (malicious node) can never be identified.

6.2.1 Symptoms of Attack

We can conclude that our attack Collusion BW Hole Attack is valid only when:

Case 1: The Malicious Node MN1 gets the packet from the source node by sending the higher sequence number of route reply RREP of the route request RREQ sent by the source node (Malicious Activity).

Case 2: After tunnelling when the malicious node MN3 receive the packet a unicast must occur instead of broadcast and the packet is dropped after the tunnelling. It means here is forge that MN1 is going to drop the packet but from MN1 to MN3 they keep transmitting the packets among themselves. This results in Spoofing of the destination and IP address to work as legitimate node.

6.2.2 Proposed Attack Model

N_L: Set of legitimate nodes.

N_M: Set of malicious nodes.

N: Total Number of nodes used i.e., NL ∪ N_M

B: Packet Drop By the Node

Collusion BW Hole Attack: An ordered set of attackers {MN1, MN2, MN3...}, MN is the malicious node. MN1 is first malicious node that receives packet from the source by sending route reply of high sequence number to the source node and works as legitimate node.

If A is any node such that A$\rightarrow$B then A$\rightarrow N_M$ must be true. As there can only be packet drop in the network only if that node is a malicious node which means A must belong to malicious node A$\rightarrow N_M$ (MN1, MN2, MN3...). Collusion BW Hole Attack is executed then N$\rightarrow N_M$ which means that all the nodes taking part must me malicious node, and also $N_M \rightarrow N_L$ this happens when a route request of high sequence number Seq_no. to the source node when it sends the route request to the neighbouring node.

6.2.3 How Is It More Dangerous Than Other Attacks

The Collusion BW Hole Attack defined in this Chapter can result in disastrous effects as it possess the pros of two types of attacks with diminished cons. The following key points describe its harmful consequences.

- In this attack two or more nodes will work in a collaboration to form a tunnel and the information they are stealing from the network will be sent to a node which is an intruder who wants to slow down the network. Now, identifying this third node which is not displaying any suspicious activity is a tough row to hoe.
- Secondly, the nodes which are working for the main intruder node will sometimes show their illegitimate nature and other times they will behave as normal genuine nodes. Thus, confusing the network handler and making it hard for it to be found at once.
- Third key factor in this attack is that even if the tunnel making nodes are identified by the network handler but still the identity of the main intruder node will be hidden as while being in the network the tunnel making node will never show any suspicious activity.
- The main intruder node is not bounded to be in the network, it may happen to be some external node which just wants to eavesdrop to the communication that is taking place between the nodes that are present in the network. Every algorithm can be applied to the nodes communicating in the network, but for outsiders it is impossible to predict which node is genuine.
- Also, if the main intruder node is disguising in the network, then it will properly hide its identity and won’t display any suspicious activity. It will be

completely dependent on the tunnel which is formed by the two disguised malicious nodes in the network.

Thus, these points sums up the whole idea of Collusion BW Hole Attack and how it can be more harmful to a network than other Denial of Service attacks in MANETs like Blackhole attack, Wormhole Attack, etc. The tunnel formed in this attack plays a vital role in hiding the identity of the main intruder node.

6.3 SIMULATION & RESULTS

Table 6.1: Simulation Parameters

Parameter	**Value**
Simulator	NS3
Area	1000 x1000
Simulation time	500 sec
MAC	802.11
Application traffic	CBR
Routing protocols	AODV
No. of S-D pairs	8
Pause time	10 sec
No. of malicious nodes	2 – 10
Bandwidth	2 Mbps
Data payload	512Bytes/Packet
Maximum speed	10 – 50 m/s
No. of nodes	100

6.3.1 Effect of number of attackers in network

Since the ratio of source-destination pair is fixed while the effect of attackers on various network parameters increases due to the ever increasing number of attackers. As shown in figure 6.4; the average End to End Delay increases as the number of attackers increase. This is because the attackers either drop the packet or keep on rotating the packet in a single loop. Here Collusion BW hole Attacks have the highest Average ETE Delay as in this case the packet is tunneled and rotated in its own loop for updating IP table so that it works as a legitimate node and cannot be identified. Average PDR increases with increasing number of attackers as the packet starts dropping with increase in attacker effect. The effect of NOR increases with increase in the attacker as it broadcasts the messages used for route discovery which will be large in number and since the number of attacker increases the route will include various attacker node for the destination but in Collusion BW hole attack it will be maximum as no broadcast occur, here unicast occur so very less chance that the broadcast message is received by any legitimate node.

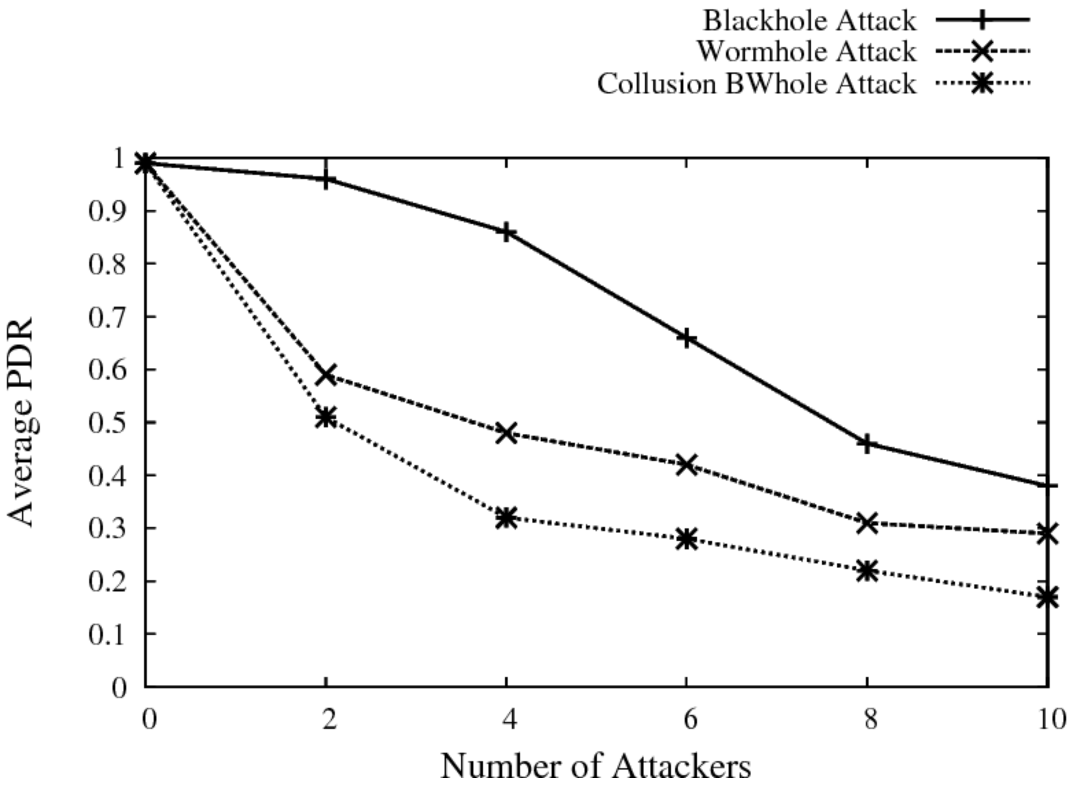

Figure 6.2: Average PDR with increasing number of attackers.

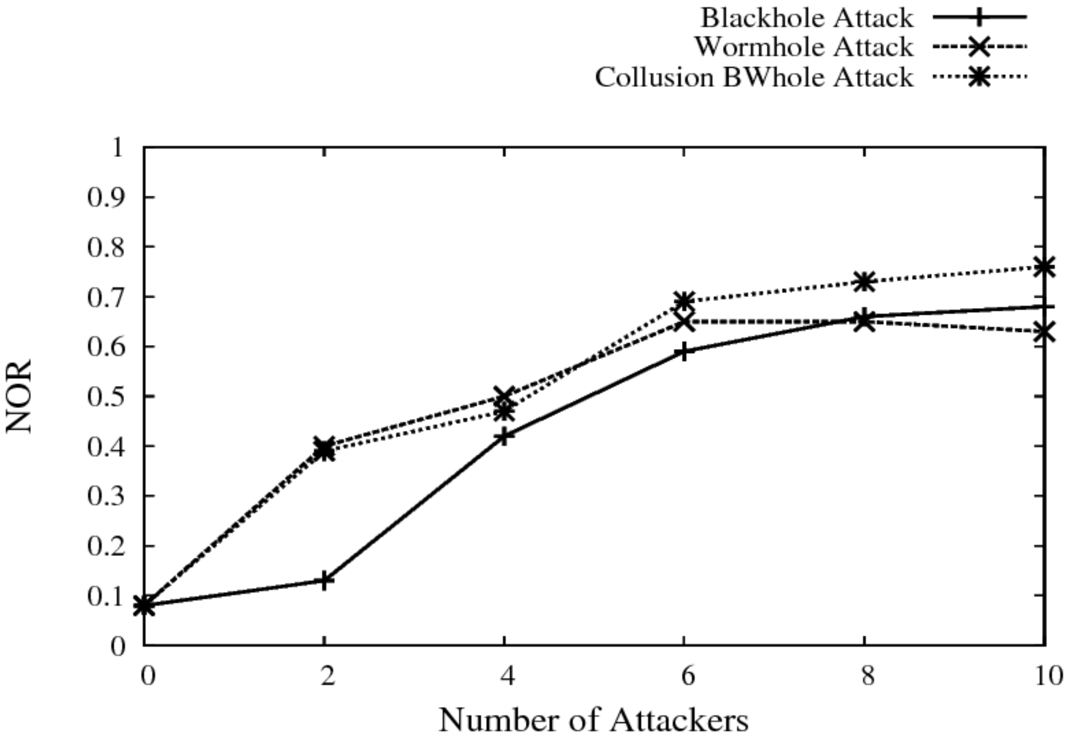

Figure 6.3: NOR with increasing number of attackers.

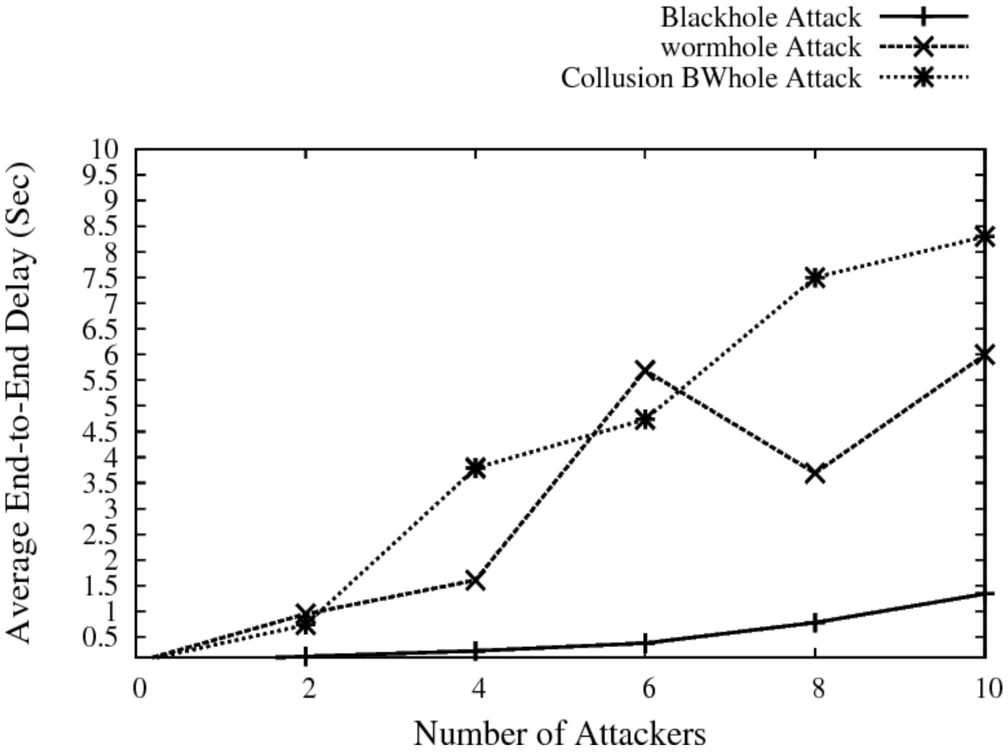

Figure 6.4: Average ETE Delay with increasing number of attackers.

6.3.2 Effect of Network Size

The effect of Attacker node is very less in low dense network and vice versa because of the lesser number of nodes, the probability that the attacker becomes a part of the discovery route is very less. The PDR decreases with an increase in the network size as the number of packets transmitted by the source will be always less than the packets that are received by the destination node. The packet drop increases as number of nodes increases so the PDR decreases. The Collusion BW Hole attack has the minimum PDR in this case. Normalize Routing Overhead increases if number of nodes increases as with an increasing number of nodes the broadcast messages which are used for the route discovery also increases gradually so average End to End Delay also increases if the network size increases.

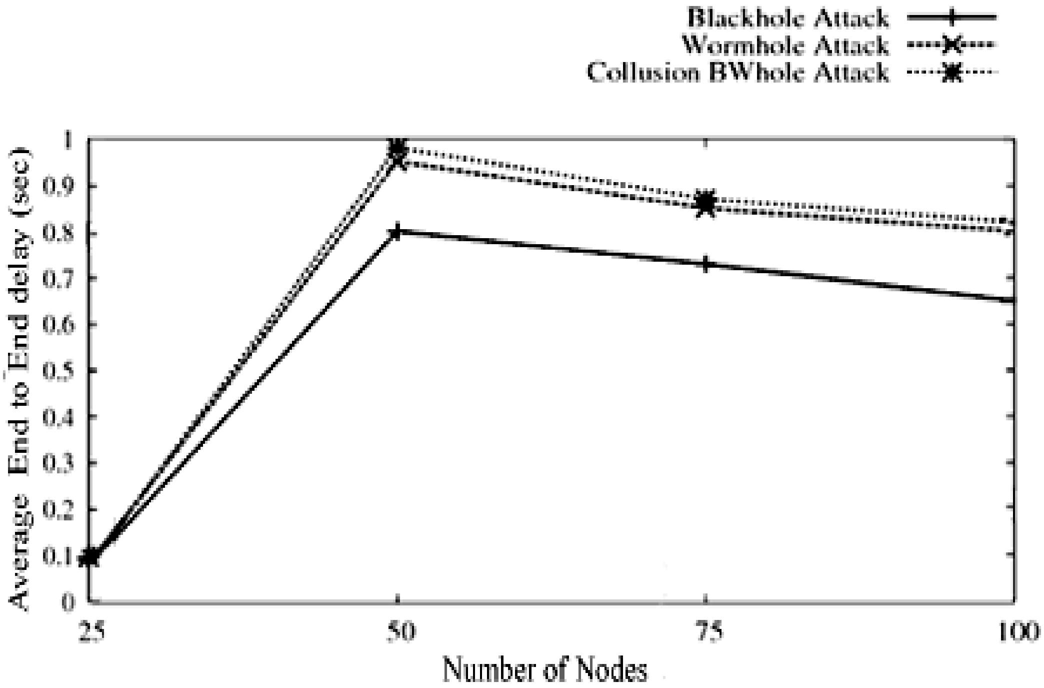

Figure 6.5: Average ETE Delay with increase in network size

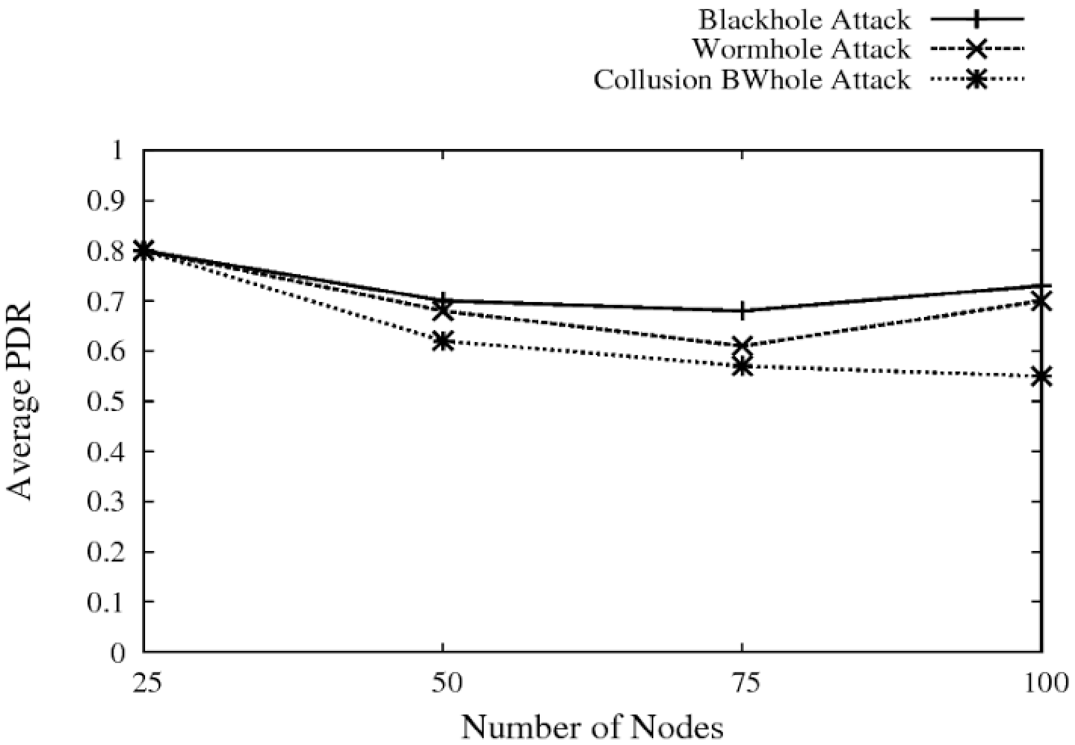

Figure 6.6: Average PDR with increase in network size

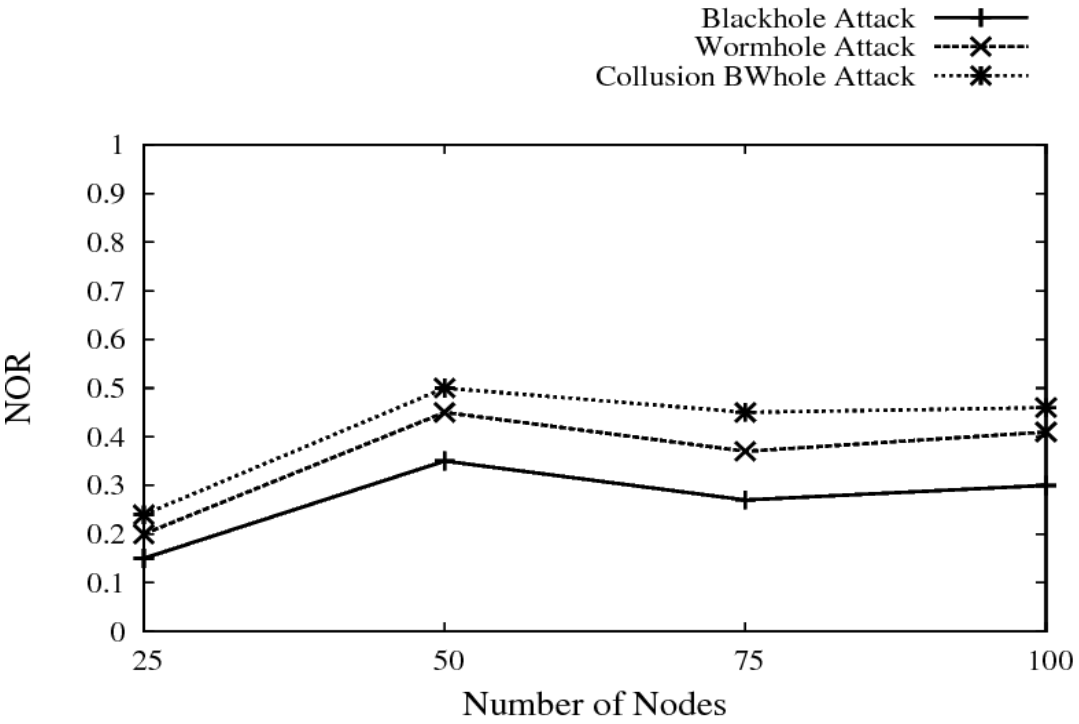

Figure 6.7: NOR with increase in network size

6.4 CLOSING REMARKS

As per the simulation result it can be concluded that in previously proposed attacks when a Malicious node receives a packet from the source node by generating the route reply of high sequence number and a large amount of route request is generated which increases the amount of traffic in the network which alarms the network that a packet has been hijacked by the attacker, also when a malicious node tunnel the packet to other malicious node then the broadcast occurs which helps in identification of the malicious node and the attack.

In our Collusion BW Hole Attack, as each node sends the route reply to the source node so there is very less time gap between the reply of the Malicious node and the legitimate node and also the packet is not dropped by the malicious node at the beginning, after tunneling of the packet to other malicious node the unicast occur which also keep the malicious node safe from being detected and the packet is dropped somewhere near the destination node which assures the network that the packet transmission was going in the legitimate route so no detection technique works to detect this attack.