Analysis of Black Hole Attack in MANET using AODV Routing Protocol

Sarita Badiwal
M. Tech, (CSE)
Rajasthan College of Engineering for Women,
Jaipur, Rajasthan, India

Aishwary Kulshrestha
Assistant Professor
Rajasthan College of Engineering for Women,
Jaipur, Rajasthan, India

Neeraj Garg
Assistant Professor
Deptt. CA and IT
JECRC University, Jaipur,
Rajasthan, India

ABSTRACT
Wireless networks have become so popular in recent years that now a day almost every electronic gadget can be operated in wireless. Wireless ad hoc network is more vulnerable to security threats than wired network due to inherent characteristics and system constraints. This paper mainly addresses attacks due to misbehaving or malicious nodes. We have examined the effect of Black Hole attack on AODV routing and its detection method. I have simulated this attack and determined effect of this attack on network performance by different network scenario. I have also implemented detection method that help to isolates the malicious node in the network.

General Terms
AODV routing protocol, Attacks, MANET.

Keywords
Sequence number, AODV Protocol, Black Hole Attack

1. INTRODUCTION
The wireless technology has been experiencing rapid exponential growth in past years. For better communication among the wireless devices some routing protocols are designed. A mobile ad hoc network is consist of self-configuring networking devices it means each device works as host and as a router in network. Each node helps to other nodes for conveying information. Routing is important task of MANET that provides better communication in MANET [11]. Wireless ad hoc network is more vulnerable to security threats than wired network due to inherent characteristics and system constraints. The nodes are free to join, move and leave the network making it susceptible to attacks both from inside or outside the network. The attacks can be launched by nodes within radio range or through compromised nodes. The frequent changes and unpredictability in network topologies due to the highly dynamic nature of mobile ad hoc networks, adds difficulty and complexity to routing among the mobile nodes in the network. These added challenges, together with the critical importance of routing protocols in communication establishment among mobile nodes, make the routing area one of the most active research area within the MANET domain. The main objective of an ad-hoc network routing protocol is the correct and efficient route establishment between two nodes so that messages may be delivered reliably on time [12].

1.1 Characteristics of MANET
1.1.1 Self Configuration
It is self configuring network that built automatically by a collection of mobile nodes without centralized management.

1.1.2 Limited computing and Energy resources
Mobile devices have limited computing power, disk size due to limited battery capacity.

1.1.3 Low bandwidth
Wireless devices have lower bandwidth comparative wired devices. These devices produce higher jitter, delay and longer connection setup time.

1.1.4 Dynamic Topology
Continues changing network topology due to mobility of nodes.

1.1.5 Open Medium
Generally ad hoc network are use in military operation or disaster so the medium is open.

1.1.6 Multi-hoping Environment
It is the distance between source node and destination node is very high then the connection between them take place with the cooperation of other node. This is known as multi-hoping connection.

1.2 MANET Application
Applications for AHNs is from small, static networks that are limited by power sources, to large-scale, highly dynamic networks. Main applications are those in which good efficient and dynamic communications must be established. Some examples are:

- Conferences and meetings of a group of people with laptops that may wish to exchange files and data without any additional infrastructure.
- Home environment for communication among the smart household appliances can be hold by an AHN between different devices, which may share their control information. For example in AHN formed by our electrical household appliances in the kitchen, the laptop computer.
- Emergency search and rescue operations require fast and dynamic communications, and with the help of AHNs they could be developed in remote areas.
- AHNs also satisfy military needs perfectly like battlefield survivability, operation without pre-placed infrastructure and connectivity beyond the LOS. The research on packet radio network started in a military context and the concept of Digital Battlefield is a burning topic nowadays.

2. RELATED WORK
The proposed system [1] starts route detection process of default AODV in the occurrence of an attacker. Source node S Wishes to send data to target D broadcast RREQ; A malicious node MN replies back with RREP enclosing abnormally high destination sequence number misleading

S as if it has a fresher route to D; another normal intermediate node IN sends RREP having acceptably higher sequence number. As RREP of the attacker holds higher destination sequence number of all received RREPs, source node unknowingly chooses path through MN to transfer data packets and therefore, (malicious node)MN intercepts and drops some or all of the received packets that causes denial-of-service in the network. This concern states the necessity of a variation of AODV protocol that proficiently discovers a secure route to the destination.

In [2] Geng Peng, Zou Chaanyun "Routing Attack and Solutions in Mobile ad hoc Network" IEEE-2006. A security routing mechanism based on common neighbor listening is proposed. In this mechanism, the trust_value and trust_threshold are defined to evaluate a node's credit standing and judge whether a node is a malicious node or not. The common neighbor which holds the biggest trust_value is chosen to listen to the network. The mechanism can react quickly and effectively protect the network from kinds of attacks when some malicious nodes occur in the Ad hoc network. Once the route is destroyed by malicious node, common neighbor will search another route to the destination during a route discovery phase. The mechanism can reinforce the security of on-demand protocols such as AODV (Ad hoc On-demand Distance Vector) and DSR (Dynamic Source Routing). The performance of common neighbor listening mechanism in AODV is justified by computer simulation. the performance of common neighbor listening mechanism is evaluated by computer simulation using ns-2. We use the mechanism in AODV and take the black hole attack.

In [3] and [4], the author's have introduced the route confirmation request (CREQ) and route confirmation reply (CREP) to avoid the black hole attack. In this approach, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has the route, it sends the CREP to the source node. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges that the route is correct. One drawback of this approach is that it cannot avoid the black hole attack in which two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker sending CREPs that support the incorrect path.

In [5], authors Satoshi Kurosawa et.al. have introduced an anomaly detection scheme to detect black hole attack using dynamic training method in which the training data is updated at regular time intervals to express the state of the network. In this scheme, the average of the difference between the Dst_Seq in RREQ packet and the one held in the list are calculated and this operation is executed for every received RREP packet. The average of this difference is finally calculated for each timeslot and it taken as the feature. Hence, it consumes considerable amount time to do calculations for every RREP packet.

3. AODV ROUTING PROTOCOL

It maintains routing information for only active routes. This protocol is based on two mechanisms (1) Route discovery (2) Route maintenance [13]. Each node has two counters 1. Sequence number which is used to find out the new route. 2. Broadcast ID. If sequence number of requested route packet is larger than the sequence number of destination node than this route is a fresh route otherwise intermediate nodes will reply to source node. There are four types of data packet message:

3.1 RREQ: When a packet is to be sent to the destination by a source node, than a message is broadcasted to the destination node through intermediate node. This message is known as Route Request (RREQ) message. RREQ packet consists of source and destination sequence number, broadcast ID, source address, and destination address. The Request id is increased by one every time when source node sends new RREQ. Thus it helps in identifying RREQ uniquely through the combination of source address and broadcast id. Each RREQ holds a value that indicates the number of times it can be re-broadcasted.

3.2 RREP : Destination node sends Route Reply (RREP) packet to the destination using reverse path as a reply to RREQ . RREP packet contains source address, destination sequence number, and destination address. The reason for unicasting RREP message is that every forwarding node caches the route back to the source.

3.3 RERR: Route Error Message is sent when there is a path failure or link breaks and when RREQ cannot be reached at destination. RERR packet includes unreachable destination sequence number, unreachable destination address and source address [6]. RERR Message is broadcasted in the following situations:

- A node identifies that a link with adjacent neighbor is broken and destination is no longer reachable.
- If it receives a data packet destined to a node for which an active route is absent and is not repairing.
- If it receives a RERR from a neighbor for single or multiple active routes.

3.4 HELLO: It needed for link status monitoring and for broadcasting connectivity information. A node should use this messages only if it is part of an active route.

3.5 AODV Working:

When source node have to send data to destination than AODV uses HELLO messages to discover path to destination through intermediate nodes. Each active mobile node transmits this messages in particular time interval to check if there is a path or not. If intermediate node does not receives multiple HELLO messages at regular interval from its neighbors than there is a no path. After path confirmation, source node floods RREQ packet towards destination. When an intermediate node receives RREQ packet, it checks its duplicity. If this RREQ packet is duplicate than it ignores it otherwise forward it towards destination. When reached to destination node, destination node will create a route reply (RREP) packet and send it back to the source node using reverse path. When source node receives RREP packet, it stores the path to the destination and will start the communication. When the source node receives multiple RREP packet, it selects the shortest path. In case of a link break towards the destination, intermediate node will generate Route Error (RERR) packet and sends it to source node. Source node

will delete that route and restart the route discovery process [9].

3.5.1 Concept of Sequence Number in AODV

Sequence number is very important parameter in AODV routing protocol.

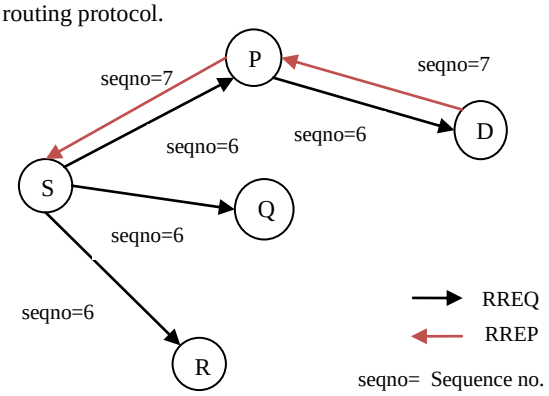

Fig.1 Use of Sequence Number in AODV Routing

Sequence number is monotonically increasing number that is maintained by originator node of RREP and RREQ message. Figure 1 shows how to use sequence number by source node and sink node. In figure 1 source node S sends message with sequence number 6 and when it reaches the destination node. The destination node increases sequence number by one and sends towards the source node. More greater sequence number signifies fresh information of the route in the network. So attacker node takes the advantage of sequence number and create the attack in the network and redirects the route [10].

4. ATTACKS IN WIRELESS NETWORK

Wireless ad hoc networks security is a highly challenging task. Security of communication in MANET is necessary for secure transmission of information. Absence of any central co-ordination mechanism for security on shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wire line network. Attacks can be classified into two types:

4.1 Passive Attacks

Passive attacks does not disrupt proper operation of network. Attackers snoop data exchanged in network without altering it. Confidentiality can be violated if an attacker is also able to interpret snooped data. This attack is difficult to be detected since the operation of network itself does not get affected.

4.2 Active Attacks

Active attacks are performed by the malicious nodes that carry some energy cost in order to perform the attacks. They involve some manipulation of data stream or creation of false stream.

4.2.1 Wormhole Attack

In wormhole attack an attacker receives packets at one point of the network, "tunnels" them to another point in the network, and then replays them into the network from that point. Routing is disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is called a Wormhole. In DSR, AODV Wormhole attack can prevent discovery of routes and may create a wormhole even for packet not addressed to itself due to broadcasting. Wormholes are hard to be detected as the path that they use to pass on information is usually not part of the same network. Wormholes are dangerous because they can cause damage without even knowing the network.

4.2.2 Byzantine attack

A set of compromised intermediate nodes that are working alone within a same network carry out attacks such as creating routing loops ,forwarding packets through false paths or selectively dropping packets which results in degradation of routing services within the network.

4.2.3 Rushing attack

Two colluded attackers use the tunnel method to form a wormhole. A fast transmission dedicated channel exists between the two ends of the wormhole that is shared by the attackers, the tunneled packets can propagate faster through these channels than those through a normal multi-hop route. This attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne [7].

4.2.4 Location disclosure attack

An attacker discover the Location of a node or structure of entire networks and disclose the privacy requirement of network through the use of traffic analysis techniques [8], or with simpler probing and monitoring approaches [7]. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security.

4.2.5 Flooding

Malicious nodes may also inject false packets into the network, or create ghost packets which loop around due to false routing information, effectively using up the bandwidth and processing resources along the way. This has especially serious effects on ad hoc networks, since the nodes of these usually possess only limited resources in terms of battery and computational power. Traffic may also be a monetary factor, depending on the services provided, so any flooding which blows up the traffic statistics of the network or a certain node can lead to considerable damage cost.

4.2.6 Sinkhole

In a sinkhole attack, a compromised node tries to attract the data to itself from all neighboring nodes. So, practically, the node eavesdrops on all the data that is being communicated between its neighboring nodes. Sinkhole attacks can also be implemented on Ad-hoc networks such as AODV by using flaws such as maximizing the sequence number or minimizing the hop count, so that the path presented through the malicious node appears to be the best available route for the nodes to communicate.

4.2.7 Denial of service attack

Denial of service attacks aimed at complete damaging of routing information and therefore the whole operation of ad hoc network.

4.2.8 Black Hole Attack

Black Hole Attack is a type of Denial-of-services (DOS) attack. This is also called Sequence Number Attack(SNA) because it is created by sequence number. Sequence number is monotonically increasing number and maintained by originator node of the RREQ and RREP message in the network [8]. AODV routing protocol includes key features such as RREQ and RREP (For route discovery), RERR and HELLO message (For route maintenance), sequence number and hop count. AODV routing protocol has every route entry is assigned by destination sequence number in the routing table. RREQ and RREP message contains several of fields. In Black Hole attack a malicious takes the advantage of sequence number and attacker node receiving the RREQ message from the neighboring node and more increase value of the destination sequence number and send reply message to the source node. Higher value of sequence number signifies the fresh information of the network. So source node accepts route reply message from the malicious node and ignores less destination sequence number route reply message. Network traffic redirect through the malicious node.

4.2.8.1 Black Hole Attack Methodology

When source node S wants to send data packet to destination node D. It creates route discovery process by using RREQ message having destination sequence number suppose 7 send to neighboring node A, B, C and F. When neighboring node receive RREQ message from source node S it updates routing table and further rebroadcast to their neighboring nodes. Each RREQ message is uniquely identified by using RREQ-Id and Source IP address that eliminate duplicates. Route reply message (RREP) is generated by either any intermediate node having fresh route information to the destination or destination node.

In figure 2 M is a malicious node, malicious node first listen the network. It means it received RREQ message from node C and change the value of destination sequence number and assigned higher sequence number value suppose 400 in RREP message and without checking own routing table immediately sends out to its neighboring node C towards the source node S. When destination node D generate RREP message it increases sequence number value by one and sends to neighboring node E towards the source node S. When source node S receives multiple RREP it accepts greater sequence number RREP and ignores less sequence number RREP. In AODV Routing protocol higher sequence number denotes the fresh information of the network. Finally network traffic is redirected through malicious node M generated by source node S. So route is established by source node S towards malicious node M and malicious node accepts the data packets and does not forward and performance of the network will be affected.

4.3 Detection Process for Black Hole Attack

Detection process is very difficult in Mobile Ad hoc network due to limited resources such as bandwidth, battery life and storage capacity. We should also concern minimum possible rise in routing overhead and delay to implement any detection process in MANETs. Here I have implemented detection process module which shown by dotted area in figure 3.

4.3.1 Algorithm and Flow diagram of Detection process

This Algorithm is designed to identify and isolate the Attacker nodes in the MANET. In this approach Source node identifies the Attacker nodes in the MANET with help of much more Differences of Sequence number of Source node and Destination nodes. The Algorithm is shown. Notations:

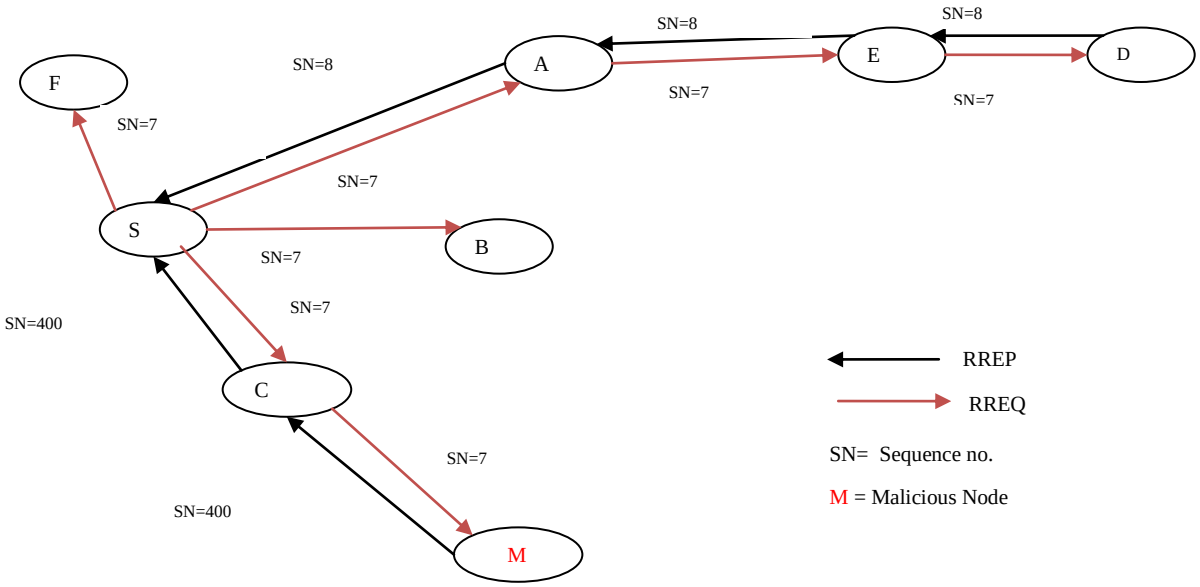

Fig.2 Black Hole Attack Model on AODV

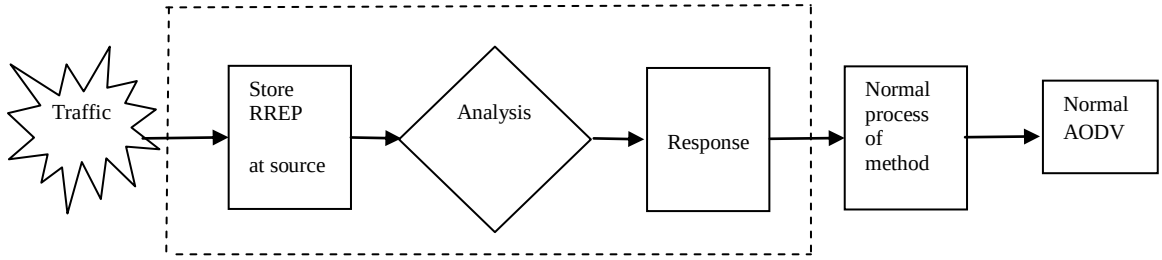

Fig.3 Block Diagram of Detection module

SN : Source Node Id
DN : Destination Node Id
RREQ : Route Request
RREP : Route Reply
DSN : Destination Sequence Number
SSN : Source Sequence Number
AN : Attacker Node
Step 1: Initialization process
Start the Route discovery process with SN and DN by using RREQ and RREP packets
Step 2:Storing process RREP packets
SN created a new routing table name as newm_routingTable to store all RREP packets for preprocessing of all RREP packets
Step 3: Identification and elimination of Attacker Nodes
While (newm_routingTable is not Empty)
{
Retrieve first entry from new routing table and determined which DSN is Much more difference with SSN then entry will be added in blacklist and discard them
}
Step 4: Route selection process
After step 3 a new route is selected from newm_routingTable by the DSN
Step 5: Calling normal process of Aodv routing
Called the RecvReply process of Aodv routing protocol
Step 6: Repeat step 3 to step 5 for each AN in network
Step 7: End

In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. The RREP packet is accepted if it has RREP_seq_no higher than the one in routing table. Our proposed solution provides an addition check to find whether the RREP_seq_no is higher than the much differences as threshold value. The threshold value is the average of the difference of dest_seq_no in each time slot between the sequence number in the routing table and the RREP packet.As the value of RREP_seq_no is found to be higher than the threshold value, the node is suspected to be attacker node and it adds the node to the black list. The source node shares this information with neighboring nodes by the attacker node identification. So that neighboring nodes know that RREP packet from the attacker node is to be discarded. Further, if any node receives
the RREP packet, it looks over the list, if the reply is from the blacklisted node; no processing is done for the same. It the RREP packet, it looks over the list, if the reply is from the blacklisted node; no processing is done for the same. It simply ignores the node and does not receive reply from that node again.

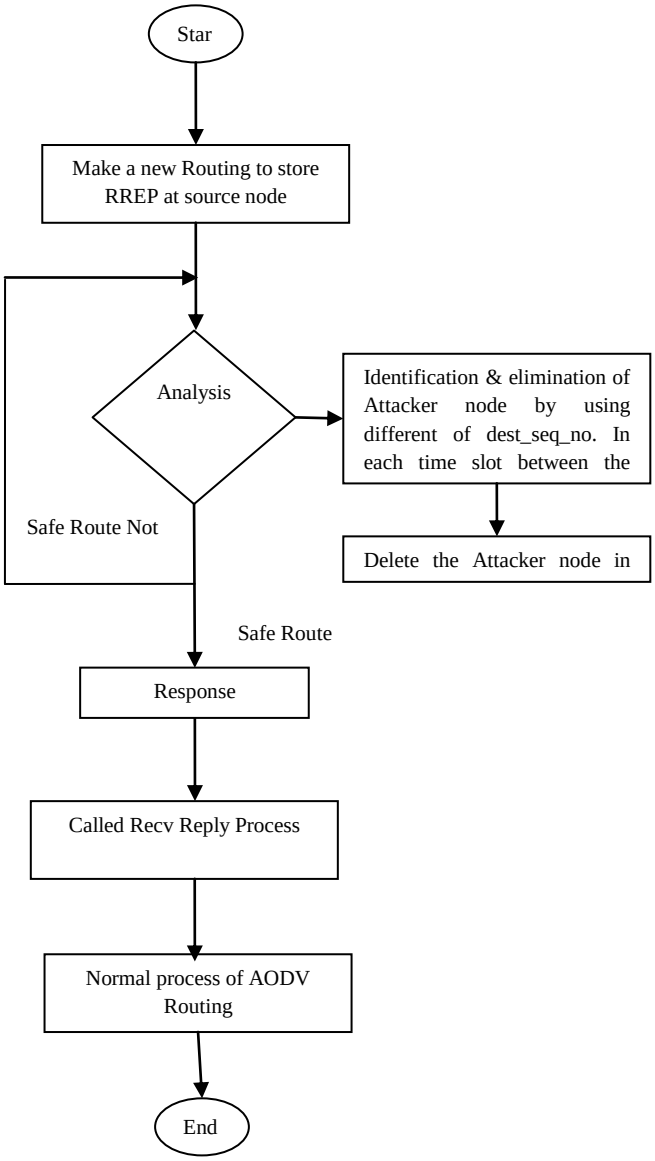

Fig.4 Flow diagram of detection process in AODV

4.4 Result and Analysis

4.4.1 Simulation Parameter

I have simulated Black Hole attack and determined effect of attack on AODV routing performance metrics such as Packet Delivery Ratio, Packet Loss by varying Node density number of nodes and mobility speed. Simulation parameter is shown in table 1.

Table 1 Simulation Setup parameter

Simulation Parameters	Value
Simulator	NS-3 (NS-3.11)
Number of Nodes	16
Simulation Times	100 secs
Traffic Type	CBR (Constant bit rate)
Network Structure	GridPositionAllocator
Packet Size	1000 bytes
Mobility Model	ConstantPositionMobility Model
Routing Protocol	AODV Routing
Channel	Wifi Helper
Application used	OnOff Helper
Malicious Nodes	2, 4, 6, 11, 13

4.4.2 Simulation Results

I have created a network by using simulation parameters shown in table 2. have run simulation four different seeds values and determined variation results shown in figure 5, figure 6 and figure 7. When we increase number of malicious node in the network then PDR (packet delivery ratio) decreases with respect to increase malicious nodes in the network. I have also added detection module in AODV routing protocol against Black hole attack with single and multiple malicious nodes in the network. and results are shown by figure 8 with different scenario normal AODV, AODV with attacker nodes and AODV with detection process.

Table 2 Effect of Black Hole Attack on PDR

Number of Malicious nodes	Packet Delivery ratio (%)	Packet Loss ratio (%)
1	64.86	35.14
2	59.35	40.65
3	39.93	60.07
4	24.22	75.78
5	18.12	81.88

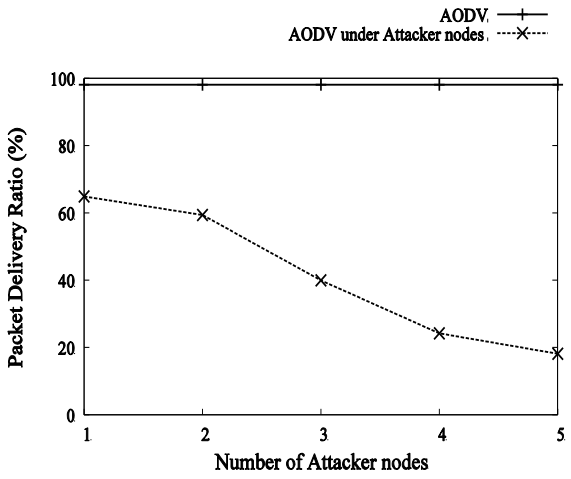

Fig.5 Number of attacker nodes v/s Packet Delivery Ratio

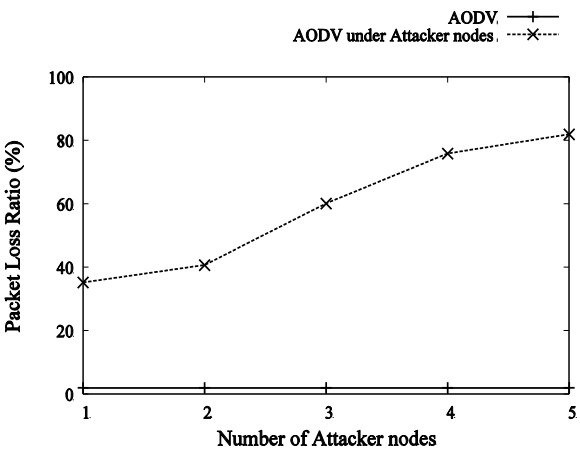

Fig.6 Number of attacker nodes v/s Packet Loss Ratio

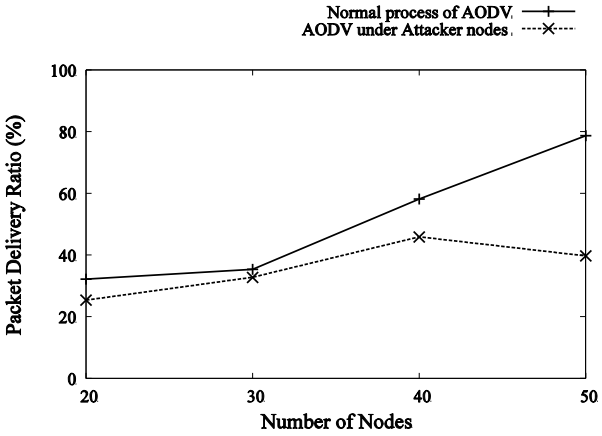

Fig.7 Number of nodes v/s Packet delivery ratio

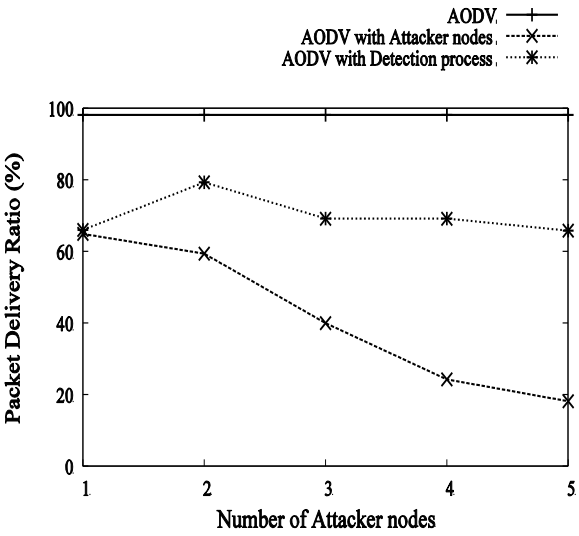

Fig.8 Number of attacker nodes v/s Packet delivery ratio

5. CONCLUSION AND FUTURE WORK

Black Hole attack is big serious problem in MANET. A malicious node degrades the performance of the network as we can see from the simulation results when we increased number of malicious nodes in the network then packet delivery ratio is decreased. I have analyzed the behavior of routing protocol and determined the effect of Black Hole attack on AODV routing and its detection method via simulation.

In future we will determine the effect of Black Hole attack on other routing protocol such as Dynamic source routing (DSR), Optimized Link State Routing (OLSR) and measure the performance of the network. To implement any detection techniques we need also consideration performance factor such as Average Delay and Routing Overhead.

6. ACKNOWLEDGEMENT

No volume of words is enough to express my gratitude towards my guide, Mr. Aishwary Kulshrestha, reader, Computer science and Engineering Department, Rajasthan College of Engineering for Women, who have been very concerned and have aided for all the material essential for the preparation of this paper. They helped me to explore this vast topic in an organized manner and provided me with all the ideas on how to work towards a research oriented venture.

I would also like to thank the staff members and my colleagues who were always there in the need of the hour and provided with all the help and facilities, which I required for the completion of my thesis.

7. REFERENCES

[1] Rutvij H. Jhaveri,Sankita J. Patel,Devesh C. Jinwala "Improving Route Discovery for AODV to Prevent Black hole and Grayhole Attacks in MANETs", INFOCOMP 2013.

[2] Geng Peng, Zou Chaanyun "Routing Attack and Solutions in Mobile ad hoc Network" IEEE-2006.

[3] Y.Zhang and W.Lee,"Intrusion detection in wireless ad-hoc networks", 6th annual international Mobile computing and networking conference proceedings, 2000.

[4] Seungjoon Lee, Bohyung Han, Minho Shin; "Robust Routing in Wireless Ad Hoc Networks" 2002, international Conference.

[5] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto; "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007, PP:338-346.

[6] C. Perkins, E. Belding-Royer, S. Das, "RFC-3561 Ad hoc On-Demand Distance Vector (AODV) Routing", pp. 1-32, July 2003.

[7] Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks", IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[8] Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection by Yibeltal Fantahum Alem & Zhao Hheng Xaun from Tainjin 300222, China 2010, IEEE.

[9] K. Natarajan and Dr. G. Mahadeven, "A Succinct Comparative Analysis and Performance Evaluation of MANET Routing Protocols", IEEE (ICCCI - 2013), Jan. 04 – 06, 2013, Coimbatore, INDIA.

[10] Michalis Papadopoulos, Constandinos X. Mavromoustakis and Georgios Skourletopoulos", Performance Analysis of Reactive Routing Protocols in Mobile Ad hoc Networks", 2014 International Conference on Telecommunications and Multimedia (TEMU),IEEE.

[11] Performance Measurement in MANET BY Sandeep Kumar Arora, Mubashir Yaqoob Mantoo Mahnaz Chishti and Neha Chaudhary, 2014 5th International Conference-IEEE.

[12] A Simulation Study of Malicious Activities under Various Scenarios in Mobile Ad hoc Networks (MANETs) by Akshai Aggarwal, Nirbhay Chaubey and Keyurbhai A Jani from Gujrat, India 2013, IEEE.

[13] A Performance Analysis and Comparison of various Routing Protocols in MANET by M. Shobana and Dr. S. Karthik from Coimbatore-641035, 2013, IEEE.