Detection of Multiple Black hole nodes attack in MANET by modifying AODV protocol

Nishu Kalia
Research Scholar, Lovely Professional University
Phagwara, Punjab
kalianish007@gmail.com

Harpreet Sharma
Research Scholar, Guru Nanak Dev Engineering College
Ludhiana, Punjab
harpreet3275@gmail.com

Abstract— ***Ad hoc Networks (MANET) is a self-configuring, infrastructure less network consists of independent mobile nodes that can communicate via wireless medium. Each mobile node can move freely in any direction, and changes their links to other devices frequently. Security is an essential part of ad hoc networks. Due to its dynamic topology, resource constraints, no centralized infrastructure and limited security, it is vulnerable to various attacks and black hole attack is one of them. In this attack, the malicious node advertises itself as having the shortest path to the destination and falsely replies to the route requests, and drops all receiving packets. There can be more than one black hole nodes present in the network which can work individually or in a group. In this thesis, the fake routing information is used by the source node in order to detect the multiple black hole nodes present in the wireless adhoc networks. The proposed mechanism is implemented in NS-2.34.***

Keywords- MANET, Throughput, Black hole, Blacklist.

I. INTRODUCTION

Wireless network has been gaining popularity due to the fact that the users can communicate with each other irrespective of their geographical position. A number of nodes can be connected via electromagnetic or radio waves. The wired network is used as the backbone of wireless network. When any computer device desires to communicate with other device, all the nodes should lie in between the radio range of each other. The wireless networks are getting popular due its ease of use. Wireless networks are easy to install as compared to the wired network. Based on coverage area, the wireless network can be divided into: Personal Area Network, Local Area Network and Wide Area Network. In the wireless network, the nodes can communicate directly or through a centralized medium such as base station or an access point. Cellular networks are basically considered as the infrastructure dependent networks where the communication as well as authentication between two nodes is done by using a base station.

Figure 1.1 A Cellular and Ad hoc Network.

Ad hoc networks are considered as infrastructure less wireless network in which there is multi hop radio communication between the nodes without any help of centralized infrastructure. Further, the ad hoc networks are classified in to static Ad Hoc network (SANET) and Mobile Ad hoc network (MANET). The lack of central administration or base station makes the routing process complex as compared to cellular networks**.** In static Ad hoc network, the mobility of host is not available. The geographical position of nodes is fixed. But in case of Mobile Ad hoc networks, there is dynamic topology that can change rapidly because the nodes move freely and can leave or join the network.

1.1 Mobile Ad hoc Networks (MANET)

Mobile Ad hoc Network (MANET) is a self organizing, self administrated and infrastructure less network where there is peer communication between the nodes communicated through radio waves. The various nodes which are within the same radio range can communicate directly and can relay the packets to other nodes. The intermediate nodes are responsible to forward the packets towards destination. So, each node in MANET can act as host as well as router. Each mobile node can move freely in any direction, and changes their links to other devices frequently. Due to its dynamic topology, the nodes can leave and join the network at any point of time. The protocols in MANET allow the nodes to discover the optimal route to transfer the data packets. It is one of the primary challenges in MANET to find out the optimal path in this dynamic multi-hop network. Also, the electromagnetic spectrum is shared between the nodes; it is difficult to provide fair bandwidth allocation to all the nodes. It allows the heterogeneous devices to communicate with each other like laptops, PDA, mobile phones, sensors, palm pilot etc. These devices vary in their size, computational power, memory, and battery capacity. As the nodes are performing the role of host and router, the battery consumption is one of the hindrances. So, before deploying the ad hoc network the various issues, like spectrum allocation and purchase, dynamic topology, efficient routing, battery consumption, bandwidth constraint, collisions, scalability, providing QOS, multicasting and security need to be addressed. The mobile nodes in MANET can be quickly deployed for various applications like in emergency and rescue operations when any natural calamity happens. In disasters like earthquakes and floods, it is difficult to deploy centralized infrastructure dependent network.

Figure 1.2 Mobile Ad hoc Networks.

But ad hoc network can be deployed easily and quickly. Security is an essential issue while deploying the ad hoc networks especially in a tactical environment. The military information is sensitive and needs to be prevented from security threats. Because of open wireless medium, dynamic topology, limited resources like bandwidth and power, there is more chances of security attacks in MANET. A lot research has been done in detecting and preventing the security threats in MANET.

1.2 Characteristics of MANET

a) Communication via wireless medium.
b) Nodes can perform both the roles of hosts and routers.
c) Dynamic network topology. Frequent Routing Updates.
d) Can be set up anywhere.
e) Autonomous.
f) Lack of centralized administration.
g) Energy Constraints.
h) Limited Security.
i) Limited Bandwidth

1.3 Applications of Ad hoc networks:

Due to cost-effectiveness of MANET, it is being used in vast application areas that includes military applications, rescue operations, wireless sensor networks, etc. These applications are described as:-

1. **Military applications:** As the ad hoc networks can be established or deployed quickly, it can be beneficial for providing quick communication between soldiers in the battlefield. There should be secure communication between the soldiers as it required privacy. The long life batteries should be equipped in nodes for long term communication.
2. **Emergency operations:** With the self-organization of the ad hoc network; there is minimal overhead to deploy it. Due to natural calamities like earthquakes, it is difficult to establish the fixed infrastructure wireless network quickly; the ad hoc network could be deployed immediately for the coordination in rescue operations. There should be minimum delay during communication in ad hoc network.
3. **Commercial Sector:** The ad hoc network is extensively used in collaborative and distributed computing applications. For the communication between groups of people in a business oriented conference, it will be efficient to establish ad hoc network instead of centralized network. The ad hoc network can be used in distributed file sharing applications also. It can be used in mobile offices, dynamic database access and also in electronic payments.
4. **Education & Entertainment Sector:** With the ad hoc networks, the interactive education can be provided by establishing the virtual classrooms in the schools and colleges. The ad hoc based network in a University or campus provides communication between students and teachers during the lectures and meetings as well. The ad hoc networks are also used for entertainment purposes like in multi user games, robotic pets, theme parks, outdoor internet access etc.
5. **Wireless Sensor network:** Wireless sensor network is a collection of spatially distributed autonomous sensors which works cooperatively to monitor the environmental or physical conditions like temperature, humidity, sound, pressure etc and pass their data to the main location. The application areas of sensor networks are environment monitoring, health care, home security, health care etc. The technical issues like mobility of nodes, size of network, power constraints, density of deployment and traffic distribution are need to be considered during its deployment.
6. **Wireless Mesh network:** The wireless mesh network provides the alternative paths to transfer the data between the nodes due to failure in existing paths which results in fast reconfiguration of the paths. With alternative paths, the data can be successfully transferred in case of damaged existing paths. The wireless mesh network can be considered as a special type of ad hoc networks. Basically, the ad hoc network is temporary network whereas the wireless mesh network has the planned configuration which is deployed for providing the cost effective dynamic topology over the certain geographic area.
7. **Hybrid wireless network**: In case of hybrid wireless network like multi-hop cellular network (MCN) and integrated cellular ad hoc relay (iCAR) network, there is combination of both cellular and ad hoc network. In MCN, the nodes within the same cell can communicate directly with each other via intermediate nodes in a multi hop environment. The base station may or may not participate in this multi-hop communication.

II. BLACK HOLE ATTACK IN MANET

In black hole attack, the malicious node exploits the routing protocol and advertises itself of having the shortest or valid path towards destination and drops all the received packets. In AODV, when a node requires a route to a destination node, it initiates the route discovery process. It broadcasts the Route Request (RREQ) packet towards its neighbors. If the neighbor does not have the fresh route to the destination node, it further broadcast the RREQ packet to other intermediate nodes. But if the intermediate node has the fresh enough route towards destination, it will send Route Reply (RREP) packet towards source node.

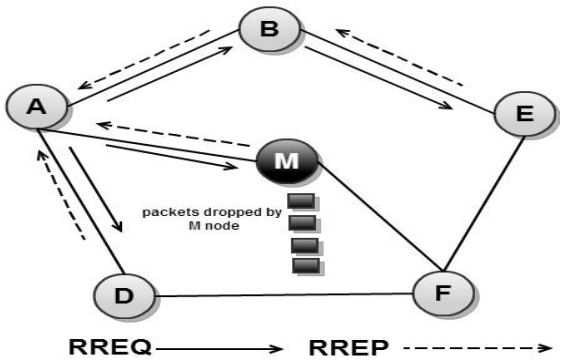

Figure 2.1: Black Hole Attack in AODV.

The fresh route means that the intermediate node must have the highest sequence number and minimum hop count as compared to one mentioned in the RREQ packet. The black hole node advertises itself of having shortest path by sending RREP packet with highest sequence number. Then, the source node will start sending the data packets towards the black hole node and the black hole node will drop all the data packets.
Imagine a malicious node 'M'. When node 'A' broadcasts a RREQ packet, the nodes 'B' 'D' and 'M' receive it. Node 'M', being a malicious node, does not check up with its routing table for the requested route to node 'E'. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node 'A' receives the RREP from 'M' ahead of the RREP from 'B' and 'D'. Node 'A' assumes that the route through 'M' is the shortest route and sends any packet to the destination through it. When the node 'A' sends data to 'M', it absorbs all the data and thus behaves like a 'Black hole'.

2.1. Types of Black hole attack in AODV

- **Internal black hole attack:** According to its name, the black hole node fits itself between the routes of source and destination. Due to its presence internally, it makes itself an active data route element. Now it is capable of conducting the packet drop attack when the data transmission is started. It is called an internal black hole attack because the malicious node belongs itself to the data route. It is more vulnerable to defend against it due to it is difficult to detect the internal misbehaving node.
- **External black hole attack:** The external black hole node stay outside the network but deny access to network traffic or disrupts the entire network or creates congestion in the network. It can become the internal attack when it takes the control of the any internal malicious node and attacks to other nodes in MANET. The external can explained as:
  a) The malicious node detects any active route and note down the destination id.
  b) The malicious node then sends the RREP packet that includes the destination id field which is spoofed to an unknown destination id. The value of the hop count is set to lowest and the value of sequence number is set to the highest one.
  c) The malicious node can send the RREP packet to the nearest available node that belongs to the active route or can send directly to the source node if the route is available.
  d) The nearest available node will relay the received RREP packet through the established reverse route towards source node.
  e) The source node will update its routing table with new information received from the RREP packet.
  f) The new route will be selected and source node will send the data via malicious node and the malicious node drops all the data packets that belong to that route.

2.2 Multiple Black Hole Attack in MANET

In multiple black hole attack, there are more than one black hole nodes that drop the data packets. In AODV, there is no direct path from source to destination; the nodes cooperate with each other for sending the data packets. The source node broadcasts RREQ packets to all the neighbor nodes for the establishment of routing path between source and destination. The intermediate nodes which have the shortest path towards destination sends RREP packet to the source. The sequence number is used to decide the freshness of the route. The highest sequence number refers to the fresh route. The black hole node advertises itself as it has the shortest path from source to destination. When black hole node receives RREQ packet, it sends RREP packet to the source with highest destination sequence number (e.g. 4294967295).

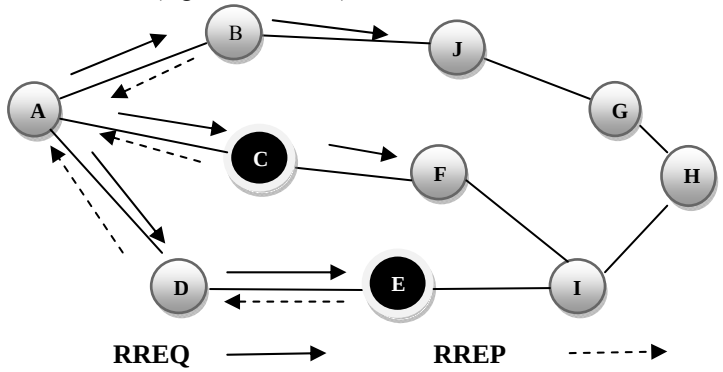

Figure 2.2 Multiple Black Hole Attack.

The source node then selects the black hole node as intermediate node through which the data packets will be sent. The Black hole nodes can work individually or in group. When black hole nodes work in a group, they are called as cooperative black hole nodes. The black hole node in case of cooperative black hole attack, the black hole nodes work in a group in order to drop the packets. . In the first phase, the black hole node exploits the routing protocol such as the AODV or DSR and advertises itself of having the shortest or valid path towards the destination with an intention to drop all the packets. In above figure, the nodes C and E are black hole nodes present in the network. Here, both the black hole nodes work individually in order the drop the data packets. If both black hole nodes work together then it is cooperative black hole attack. When the source chooses that spurious route, the black hole node starts to intercept the data packets in its second phase. In this paper, the detection mechanism is proposed for tackling the multiple black hole nodes problem by modifying the AODV protocol.

III. LITERATURE SURVEY

S.Marti et al., (2000) proposed the Watchdog/Pathrater as a solution to the problem of selfish (or "misbehaving") nodes in MANET using DSR protocol. The Watchdog method is used to detect misbehaving nodes and the Pathrater, to respond the intrusion by isolating the selfish node from the network operation. Watchdog runs on each node. When a node forwards a packet, the node's watchdog module verifies that the next node in the path also forwards the packet. The Watchdog does this by listening in promiscuous mode to the next node's transmissions. If the next node does not forward the packet, then it is considered to be misbehaving and is reported. The Path rater module uses the information generated by Watchdog to select a better route to deliver the packets, avoiding the selfish nodes.

Hongmei Deng et al., (2002) proposed the method for detecting the single black hole node in MANET. In this method, the intermediate nodes send RREP message along with the next hop information. After getting this information, the source node sends further request to next hop node to verify that it has the route to the intermediate node or not. If the route exists, the intermediate node is trusted and source node will send data packets via that trusted node. If not, the reply message from intermediate node will be discarded and alarm message is broadcasted and isolate the detected node from network. By using this method, the routing overhead and end to end delay will be increased. If the black hole nodes work as a group in an attempt to drop packets, then this method is not efficient.

Mohammad Al-Shurman et al., (2004) proposed the two methods to avoid the black hole attacks. According to the first solution, the source node verifies the validity of the route by finding more than one route to the destination. It waits for RREP packets to arrive from more than two nodes. When the source node receives RREP packets and the routes to destination have shared hops, the source node can then recognize the safe route. This method causes routing delay. The second solution is to store the last packet sent sequence number and the last packet received sequence number in a table. When node receives reply message from another node it checks the last sent and received sequence number. If there is any mismatch, then the ALARM packet is broadcasted which indicates the existence black hole node. Then the other nodes will come to know the existence of black hole nodes in the network. This mechanism is reliable and faster having less overhead.

Satoshi Kurosawa et al., (2007) proposed the solution based on dynamically conditions of MANET. It uses an anomaly detection scheme. The state of network at each node is expressed by multidimensional feature vector. Each dimension is counted on every time slot. The feature vector includes the number of sent out RREQ messages, number of received RREP messages, the number of received RREP messages, the average of the difference of destination sequence number in each time slot between sequence number of RREP message and the one held in the list. The mean vector is then calculated and they compare the distance between the mean vector and input data sample. If the distance is greater than some threshold value, then there is an attack. It uses dynamic training method in which the training data updated at regular intervals of time.

Chang Wu Yu et al., (2007) proposed the scheme in which the mobile nodes work collaboratively analyze and detect the multiple black hole attack. It is composed of four modules such as Local data collection, local detection, cooperative detection and global reaction. In local data collection phase, every node in the network evaluates the presence of suspicious node in its neighborhood by overhearing the information collected in an estimation table. Then in local detection phase, the detecting node would initiate the local detection to find out the possible black hole node. The local detection node sends the check packet to ask the cooperative node if it has successfully received the check packet or not directly. If the response is positive, then it is normal node. Otherwise, the cooperative detection method is activated. With this procedure, one-hop neighbors of suspicious node will be notified to participate cooperatively in making decision about black hole node. In the end, the

global reaction step will be followed for setting up the global notification in which warning messages are sent to the whole network.

Latha Tamilselvan et al., (2008) enhanced the AODV protocol by detecting the multiple black hole attacks working in a group. This approach uses the "Fidelity Table" where each node participating is assigned a fidelity level which acts as measurement for the reliability. If the level is 0, then that node is considered to be black hole node and is isolated from the network. The source node receives RREP packet along with fits fidelity level and the id of next hop node in the path. The node is considered to be reliable if the average of fidelity levels is above the threshold. Then, the source node selects the path with high fidelity level. The fidelity level of participating nodes is updated. After receiving the data packets, the destination node has to send the acknowledgement to the source. Then, the source node increments the fidelity level of intermediate nodes for their faithfully participation. But if the acknowledgment is not received in some given time, the fidelity level is decremented. All the nodes exchange the fidelity table periodically. As the fidelity level reaches to 0, the node is considered to be malicious one and other nodes will be informed about it.

P. Agrawal et al., (2008) proposed a mechanism for detecting the chain of multiple black and gray hole nodes working in a group. Here, the total traffic is divided into small set of data blocks. Initially, a backbone network of the strong nodes is deployed over the network. These strong nodes are assumed to be trusted with powerful computing power and radio range. The backbone nodes are used to detect the malicious nodes. With the help of these nodes, the end to end checking of data packets is carried out by source and destination to determine whether the data packets have reached to destination or not. If the result is negative, then the detection mechanism is initiated. For the detection of malicious node, the strong node which is associated with the source node broadcasts the find chain message which contains the id of the node that sent the RREP message. The strong node at the destination receives the chain message and instructs the neighbors of that node (who replied RREP to the source) to vote the next node to which they are forwarding the packets. If the next node id has null value, then it is black hole node and other nodes are alerted.

Latha Tamilselvan et al., (2008) proposed the solution in which the source node waits for the responses including the next hop details from other neighboring nodes for a predetermined time value. When the timeout value is over, it checks in the CRRT (Collect Route Reply Table) table firstly, if there is any repeated next-hop-node or not. If in the reply paths any repeated next-hop node is present, it assumes that the paths are correct or the chance of malicious paths is limited. This solution adds a delay and the process of finding repeated next hop is an additional overhead.

Payal N. Raj et al., (2009) proposed DPRAODV (detection, prevention and reactive AODV) to prevent the black hole attack by informing the other nodes about the malicious node. If the value of RREP sequence number is found to be higher than the threshold value, then the node is said to be malicious and it adds the node to the black list. As the node detected an anomaly, it broadcast a new control packet, named as ALARM to its neighbors. The ALARM packet contains the black list of malicious node as a parameter, so that the neighboring nodes come to know that RREP packet from the node is to be discarded. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The purposed solution not only detects the black hole attack, but also it tries to prevent it further, by updating the threshold which reflects the changing environment in real. The detected malicious node is then isolated from the network.

K. Lakshmi et al., (2010) enhances the AODV protocol. In AODV protocol, the destination sequence number is 32-bit integer associated with every route and is used to decide the freshness of a particular route. If the sequence number is largest, the route will be fresh enough. In this method, all the sequence numbers mentioned in RREP packet is stored along with the corresponding node ID in a RR-table (Route Request). Then, if the first destination sequence number in table is much greater than the sequence number of source node. That node will be identified as malicious node and the entry will be immediately removed from the table. The proposed solution also maintains the identity of the malicious node as MN-Id, so that the control messages from that node can be discarded. In addition, there is no need to forward the control messages from that malicious node. Moreover, in order to maintain freshness, the RR-Table is flushed once a route request is chosen from it.

Yiebeltal Fantahun Alem et al., (2010) proposed an Intrusion Detection using Anomaly Detection (IDAD) technique to prevent the black hole attack. IDAD assumes every activities of a user or a system can be monitored and anomaly activities of an intruder can be identified from normal activities. Hence, by identifying anomaly activities of an adversary, it is possible to detect a possible intrusion and isolate the adversary. To do so an IDAD needs to be provided with a pre-collected set of anomaly activities, called audit data. Once audit data

is collected and is given to the IDAD system, the IDAD system can compare the every activity of a host with the audit data on a fly. If any activity of a host (node) resembles the activities listed in the audit data, the IDAD system isolates the particular node by forbidding further interaction. It minimizes the extra routing packets which in turn minimizes the network overhead and facilitates faster communication.

Maha Abdelhaq et al., (2011) provide an improvement over the solution given in the paper [1] in which Source Intrusion Detection (SID) method is used. The SID mechanism is good for small scale MANET but when this mechanism is applied in a large scale MANET and the distance between the source node and the intermediate node is long, then the above solution is not sufficient. Secondly, if the distance between the source node and the intermediate node is long, the delay in the discovery period of the route will be high, which causes an overall network performance degradation. In order to mitigate the drawbacks in SID security routing mechanism, a new mechanism called Local Intrusion Detection (LID) security routing mechanism is proposed to allow the detection of the attacker to be locally; which means that when the suspected intermediate node unicast the RREP towards the source node, the previous node to the intermediate node performs the process of detection and not the source node.

Jaydip Sen et al., (2011) proposed DRI and Cross Checking Scheme which is used to identify the cooperative black hole nodes. Each node maintains the extra DRI table with two entries 'From' and 'Through', where 1 represents for true and 0 for false. These entries stand for the information on routing data packet from and through the node. In this solution, the Intermediate node replies the next hop information and DRI entry about next hop node along with RREP packet. The source node then checks the reliability of intermediate nodes by using cross checking scheme via alternate paths by using DRI table information. The detection mechanism used in this approach is time consuming. It provides 50 % throughput but increases end to end delay and routing overhead.

Jian-Ming Chang et al., (2011) Scheme detects and avoids the black hole attack based by combining the proactive and reactive defense architecture in MANET. In this proposed solution, before the route discovery process the source node sends the bait RREQ packet which contains the virtual and non-existent destination address. To avoid the traffic jam with bait RREQ packets, all the bait RREQ packets will survive for a period time. The malicious node will send back the bait RREP packet which advertises as the shortest path to the non-existent destination. The author adds the additional information in the bait RREP packet of having the record of generator of RREP. When source node receives the bait RREP packet, it can recognize the location of the attacker. After detecting the malicious node, a normal DSR route discovery process will be initiated. As compare to DSR and Watchdog method [14], the packet delivery ratio of this scheme is above 90%. Routing Overhead is more than DSR but lesser than Watchdog method.

Gurdeep Singh Bindra et al., (2012) proposed Extended Data Routing Information (ERDI) scheme that enhanced AODV to tackle the Cooperative black hole and gray hole attacks by maintaining the extended data routing table at each node along with the routing table. The ERDI table consists of fields for detecting the malicious node as well as also maintains the history of previous malicious behavior instances to accommodate the gray hole behavior. Refresh packet, BHID packet, further request and further reply packet in addition to the RREQ and RREP packets. The DRI table scheme (Jaydip Sen et al., 2011) was unable to find the gray hole behavior of the malicious nodes. In this scheme, when destination node is node able to receive the data packets due to malicious behavior of some node, it will send the NACK (Negative Acknowledgement) towards the source through other path. Then, the refresh packet is sent by both source and destination to intermediate nodes, to refresh the ERDI entries and delete the concerned path, through the same path from where NACK arrives. The normal Cross checking (Jaydip Sen et al., 2011) scheme will be then initiated to detect the cooperative black hole nodes. The BHID packet contains the id of black hole node detected and is broadcasted to all the nodes.

ketan S. Chavda, Ashish V.Nimavat(2014) proposed the mechanism in which black hole detection process is done which uses a preprocessor called as Pre_Process_RREP. In this process, when the RREP packets are accepted the process Compare_Pkts (packet p1, packet p2) is called where the destination sequence number of the two packets are compared and the packet which have the highest destination sequence number is selected only if the differences between the two destination sequence numbers is not much high. But if the difference between the two destination sequence numbers is exceptionally or significantly very high. Then, the packet with exceptionally high destination sequence number is considered as the black hole node and the other nodes are notified by an ALERT message which contains the id of the black hole node. This method causes delay in network and cannot be applicable for detection of cooperative black hole attack.

Siddiqua et al., (2015) proposed a secure knowledge based mechanism that detects and prevent the black hole attack in AODV by considering the reasons of packet dropping using promiscuous mode. Every node in the network listens the behavior of the neighbor nodes wirelessly. Each node compares the information of neighbor with the knowledge table information. Here, nodes monitor the neighbor nodes for the detection process. The modes monitor both the control packets and the data packets for the prevention of selective dropping. If the dropping of packets reached to a threshold value, it checks whether the suspected node is the destination node or not. Also, before declaring the suspected node as malicious node it also checks for the packet drop reasons like TTL (Time to live) and residual energy. After these considerations, if that suspected node is considered as black hole node, then its id is broadcasted to all the other nodes so that the other nodes avoid that node in the routing process. This mechanism brings better throughput and delay as compare to AODV protocol.

N. Chaudhary et al., (2015) proposed the Timer Based scheme in order to detect and isolate the black hole node in mobile adhoc network. This mechanism utilizes the trust value that is defined by each node on its neighbors. Initially, every neighbor node is assigned the maximum trust value and a timer is set with every data packet. The node does not communicate with those neighbor nodes whose trust value is less than the minimum value. A node checks by monitoring the wireless transmission whether have been received by the next hop before the timer is expired. If any node could not listen wireless transmission of the next hop, the trust value of the next hop will be reduced and the other nodes are notified so that they can update their routing tables. As the node's next hop continuously drop the data packets, its trust value is decreased and becomes less than the minimum trust value. The other nodes put such a malicious node id in their blacklist table. With this mechanism, the black hole nodes are removed from the network and packet delivery ratio is improved.

IV. PROPOSED METHODOLOGY

In this scheme, the source node broadcasts its own address and sequence number included into fake RREQ packet instead of destination address and destination sequence number. As the source node's sequence number is the most recent and fresh sequence number. The other nodes do not have the latest or fresh sequence number of the source node. When the intermediate nodes receive the fake RREQ packet, If the intermediate nodes have the source sequence number greater than the one received in fake RREQ packet, it will reply with RREP packet. But in our case, the legitimate intermediate node will have the small source sequence number than described in fake RREQ packet because only source node will have its latest or fresh enough sequence number. But if there exist any black hole nodes in the network, then they will reply with the RREP packet as it will advertise itself having the shortest path with the highest sequence number. So, the source node will detect the black hole nodes and will notify the other nodes about the black hole nodes so that the rest of the legitimate nodes will not communicate with black hole nodes. In previous papers, the destination sequence number[9] is used by the source node to compare the destination sequence number with the RREP packet's destination sequence number but in this case the source node may not have the fresh enough destination sequence number. As the source node had the old destination sequence number it used at the last time. In some papers, the RREP destination sequence number is compared with some threshold value but not given on which basis they calculated the threshold value. The parameters are not cleared while calculating the threshold value.

The proposed multiple black hole nodes detection mechanism algorithm:

a) The source node broadcasts the fake RREQ packet with its own source sequence number and address in the destination sequence number and destination address in the RREQ packet fields respectively.
b) When legitimate nodes receive the fake RREQ packet, it will compare the source sequence number in fake RREQ packet it received with the sequence number of the source described in the table.
c) As the source node sends its own sequence number, it will be more obvious that it will be the latest or fresh one. The intermediate node will have the source sequence less than the described in fake RREQ packet. So it will not reply with RREP packet.
d) But, if there exist any black hole node in the network then it will reply with the RREP packet and advertises itself as having the shortest path with highest source sequence number.
e) The source node will then detect the black hole nodes exist in the network. And then send the ALARM packet having the list of black hole nodes to the rest of the nodes.

Pseudo code of proposed method

```
// Data receiving routine
If(Data received on network layer && data->source == index )
{
if(detection mode == false)
Sendrequest(data->dest)
Else
```

```
Sendrequest(index)
}
// recv reply routine
Recvreply()
{
If(blacklist_nodeid ==reply->source)
{
Drop_reply();
}
If(detectionmode)
{
If(reply->dest_seqno> seqno)  // Comparison of sequence number
Blacklist(replysource)
Sendnotification(blacklisted_nodeid);
Detectionmode=false;
}
Else
//existing AODV code
}
//Recv notification routine
Recv_notification()
{
Deleteroute(notification->source)

Blacklist(notification->blacklisted_node)

}
```

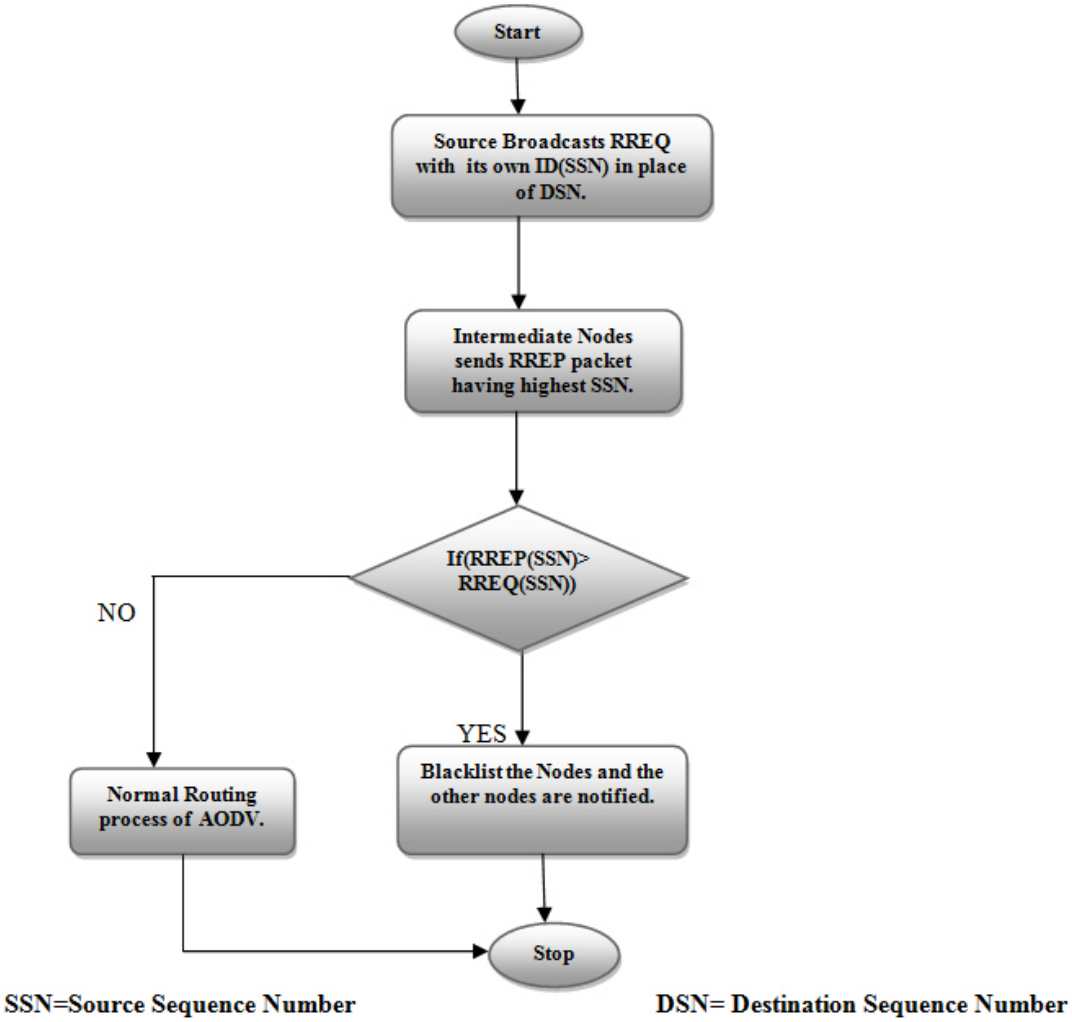

Figure 4.1 Flow chart of proposed method.

V. IMPLEMENTATION AND RESULTS

For implementing the proposed solution, I have used NS-2.34**.** A network simulator is a piece of software that predicts the behavior of a network, without an actual network being present. NS (version 2) is an object-oriented, discrete event driven network simulator developed at UC Berkely written in C++ and OTcl. While the C++ defines the internal mechanism or work as backend of the simulation, the OTcl sets up the simulation by assembling and configuring the objects as well as scheduling discrete events (i.e. a frontend). The C++ and the OTcl are linked together using TclCL. Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions can be done using NS2.

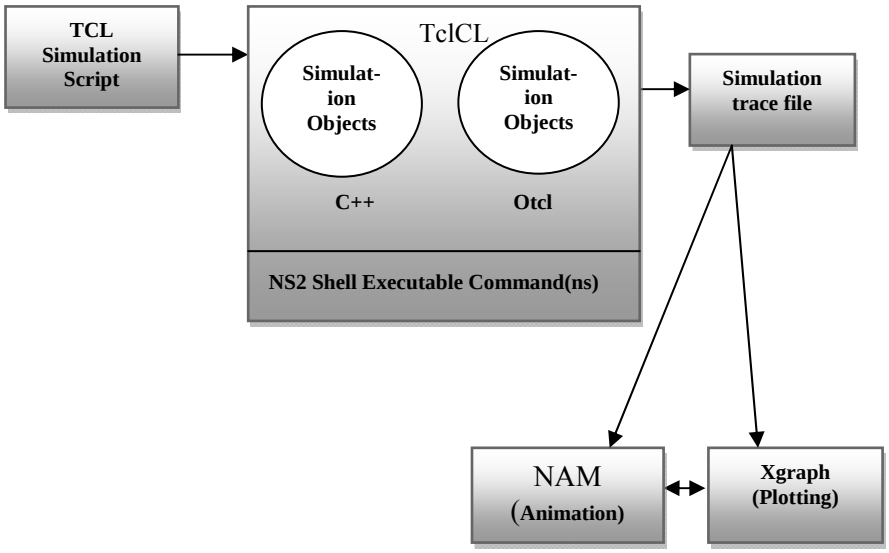

Figure 5.1 Architecture of Network Simulator.

In this thesis, the effect of multiple black hole nodes attack is evaluated by modifying the AODV protocol in the wireless ad-hoc networks. To implement it, the simulation of multiple black hole nodes attack in AODV is done by using Network Simulator (version 2.34). A new protocol is implemented after modifying AODV in which the data packets are dropped. For evaluating the performance of new protocol, the various simulation parameters are needed such as traffic, mobility model etc. The following parameters are used in performing simulation.

Table 5.1 Simulation Parameters

Simulation Parameter	Value
Simulator	Ns-2.34
Radio-propagation	Two ray Ground
Channel type	Wireless channel
MAC Type	802.11
Network interface type	Wireless Physical
Link layer	LL
Antenna	Omni Antenna
Mobility Model	Random Waypoint
Queue Length	50
Area	1000m*1000m
Number of Nodes vary	50
Mobility Speed	0-10m/s
Pause time (seconds)	1-2s
Traffic	CBR(Constant bit rate)
Transmission range	250
Carrier Sensing range	550
Data rate	10 packet/second
Packet size	512 byte
Simulation time	300s

First of all, the simulation of simple AODV protocol is done and performance of simple AODV is evaluated using network parameters packet delivery ratio, end to end delay and throughput. After that, the multiple black hole nodes behavior is implemented by modifying the AODV protocol and changed the name of the AODV protocol into BLACK.cc and make changes into it.

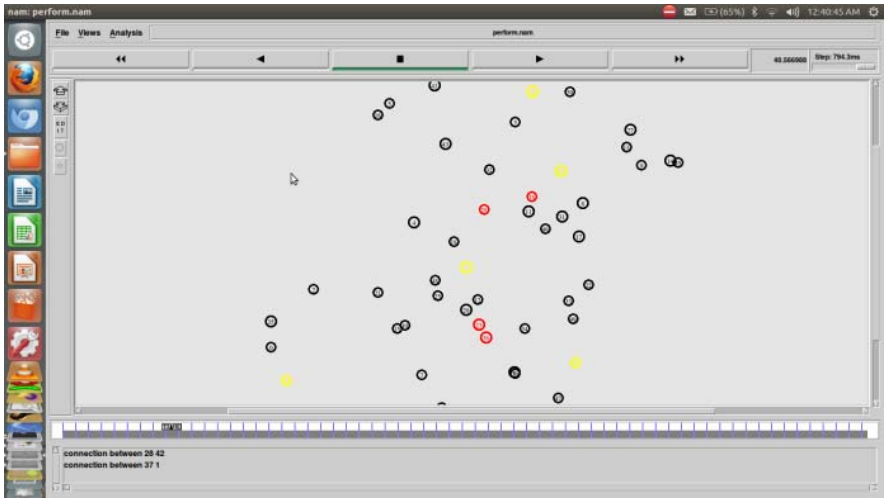

Figure 5.2 Mobile Nodes interacting with each other.

We need to change firstly the file "**\tcl\lib\ ns-lib.tcl**", the new procedure is added to create a node. We set a routing agent to the node as " **blackAODV**".

```
Simulator instproc create-black-agent { node } {
set ragent [new Agent/blackAODV [$node node-addr]]
$self at 0.0 "$ragent start"            # start BEACON/HELLO Messages
$node set ragent_ $ragent
return $ragent
```

If the implementations are ready, we need to compile the NS-2 again for creating the object files. In the root directory ns-2.34, the **/makefile/** is added with following lines.

```
black/black_logs.o black/black.o \
black/black_rtable.o black/black_rqueue.o \.
```

In this, the two nodes are taken as black hole nodes. When the packet is received using AODV protocol, the "**recv**" function is executed. It then processes that packet according to its type. If the packet belongs to routing management, the "**recvAODV**" handles that packet but if that packet is a data packet then it will be routed towards its destination but if there black hole nodes present in the network they will simply drop the data packets. After making the changes in the required files and adding the changed AODV protocol in the ns-allinone-2.34 directory, open the terminal and type:

```
$ cd ns-allinone-2.34
$ cd ns-2.34
$ make
```

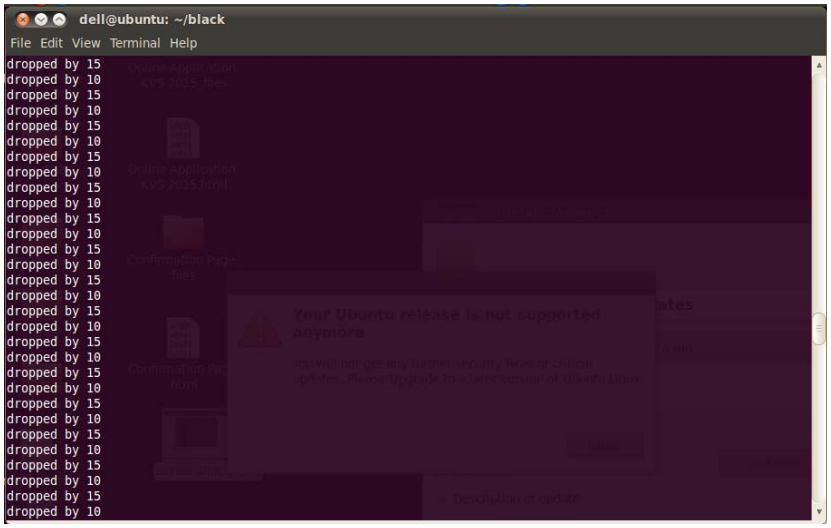

Figure 5.3 Black Hole nodes that drop data packets.

If no error comes, then our new AODV protocol with multiple black hole nodes attack is added successfully. Then, for running the new added protocol we need to make respective tcl file and run into the terminal. In the above figure, the nodes 10 and 15 are dropping the data packets which are the black hole nodes in the network. There can be more than two black hole nodes in the network. The tcl script file is used to simulate the newly protocol and generate the trace file so that the evaluation of protocol can be done. The above figure is the snapshot of black hole nodes that drop the data packets. We define all the required simulation parameters in the tcl file such as no. of nodes, mobility model, area etc. One can set the positions of nodes also. The nam file is created using tcl file to record the simulation traces.
The trace file is basically used to evaluate the performance of the newly added protocol by using awk file. The awk file uses the trace file data to generate the results.

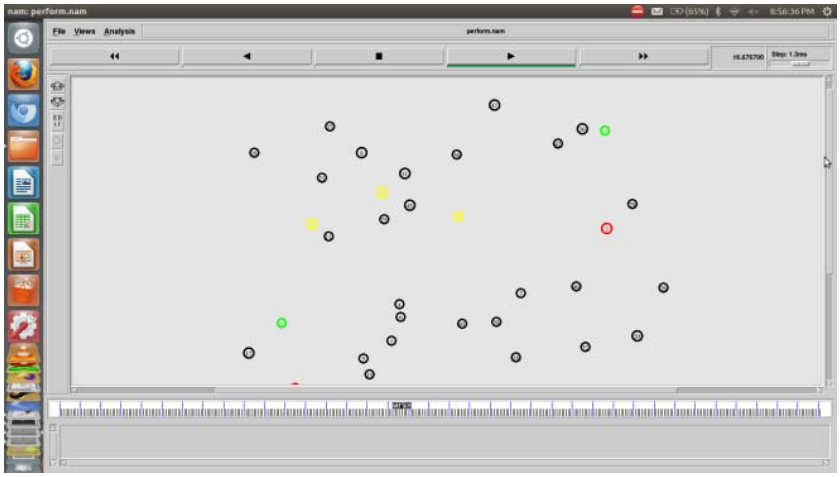

Figure 5.4 Snapshot of black hole nodes in AODV protocol.

For implementing the detection mechanism, the modifications are done in AODV protocol in order to detect the multiple black hole nodes. The proposed mechanism is implemented and the snapshot after implementing the detection mechanism is:

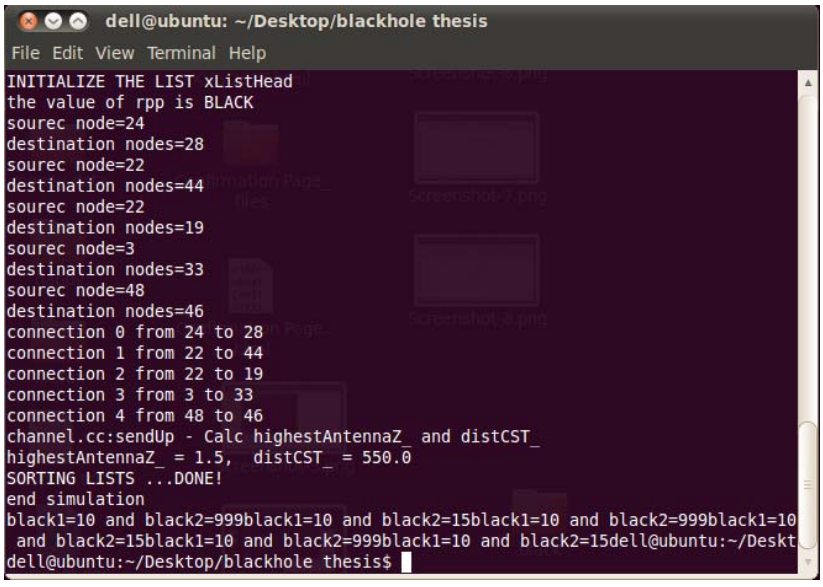

Figure 5.5 Detection of black hole nodes.

Here, we can see that the nodes 10 and 15 are detected as black hole nodes.
After implementing the detection mechanism, the results are evaluated by using the network parameters named as packet delivery ratio, end to end delay and throughput. On the basis of these parameters, the performance of simple AODV, Multiple Black hole nodes attack behavior and the detection mechanism for detecting the

multiple black hole nodes in AODV is evaluated. The evaluation is done on the basis of mobility. The various scenarios have been taken on the basis of the mobility of the nodes.

Packet Delivery Ratio: It is defined as the ratio of the number of packets received at the destination as compared to the number of packets sent by the source node. It is calculated on the basis of the data packets generated and received in trace files. The awk script is used to process the trace file ang the result is generated.

Packet Delivery Ratio= ∑ Number of packets received / ∑ Number of packets send

The comparison of AODV, Multiple Black hole Attack and Detection Mechanism is evaluated on the basis of Packet delivery ratio. In the following figure, the packet delivery ratio is evaluated on the basis of mobility. It means that as the nodes change their position what will be effect of the packet delivery ratio. The packet delivery ratio in case of black hole nodes attack drops as compare to the AODV protocol. But after detection, the Packet delivery ratio is improved.

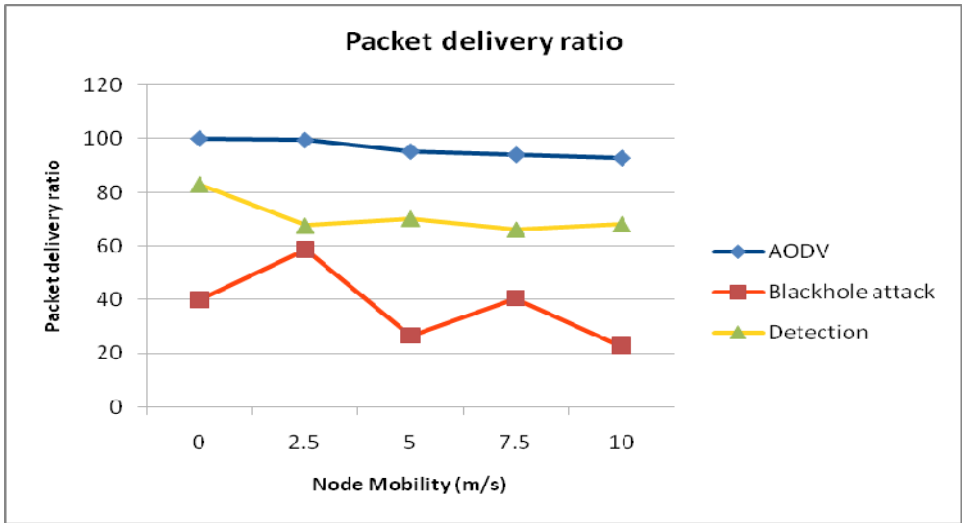

Figure 4.5 Packet Delivery ratio over Node Mobility

End to End delay : It is described as the average time taken by the data packet to be transmitted from source to destination. It means that how much time the data packet is needed to be transmitted between source and destination across the network. The end to end delay is calculated for the successfully received packets at the destination.

End to End Delay= ∑ (arrive time – send time) / ∑ Number of connections

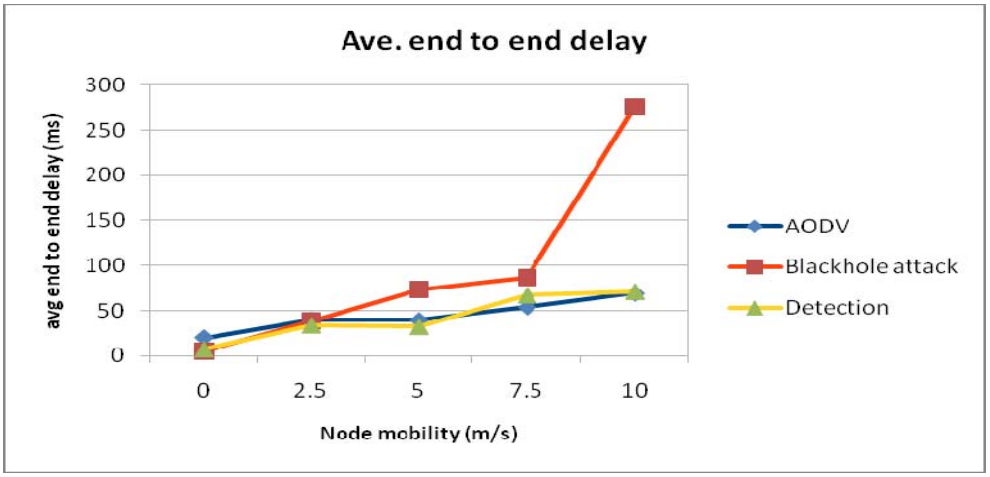

Figure 4.6 End to End Delay over Node Mobility

Throughput: Throughput means the amount of data packets transmitted across the network from one end to another end in a given amount of time. It is calculated as the time taken on the average of the number of bits that

are transmitted from the source to its destination. The throughput of detection mechanism is improved as compare to the black hole attack in AODV. The awk script is used to calculate the throughput using trace files.

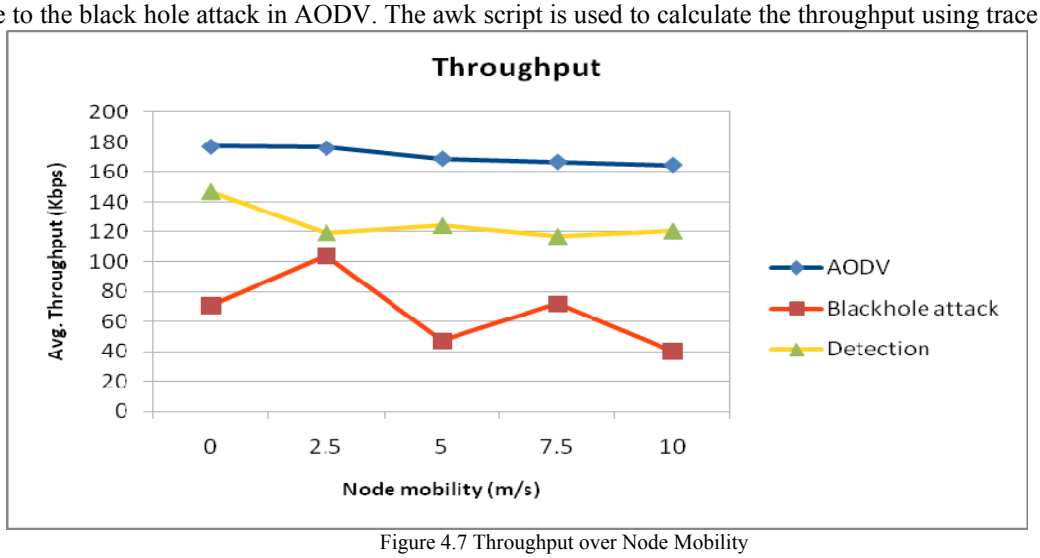

Figure 4.7 Throughput over Node Mobility

VI. CONCLUSION

Mobile Ad hoc Network is self configuring network where there are various constraints such as open shared wireless medium, limited resources like battery and bandwidth consumption, dynamic topology; it is vulnerable to variety of attacks. In this thesis, the proposed mechanism tackles with the multiple black hole nodes attack in MANET. To handle the multiple black hole nodes attack, we assume that the source node is an intelligent node which uses the sequence number concept to detect the multiple black hole nodes in MANET. In previous work, the destination sequence number was used by the source node to detect the black hole attack. But the source node might not know the fresh enough destination sequence number. But if the source node uses its own sequence number which will be the fresh enough for the detection purpose, the result will be more accurate. This detection mechanism is effectively implemented using NS 2.34. The drawback of proposed solution is that when the source node is busy in detecting the multiple black hole nodes, the data packets which are received at the source node from application layer can be delayed as we do not know how much time is needed to detect the multiple black hole nodes.

VII. FUTURE SCOPE

"Security issues in MANET" is still one of the hottest areas of research. A lot of research has been devoted to the detection and prevention of black hole attack in MANET. The intelligent source based detection mechanism is proposed here to detect the multiple black hole nodes in MANET. After the detection of black hole nodes, the notification of black listed nodes to other nodes increases the network overhead which should be reduced in future. Also, in future we will use a timer under which the detection will be done so that the delay of data packets can be decreased. In future, the focus of my research will be on detecting the cooperative black hole attack in MANET by using an intrusion detection system. In cooperative black hole, more than one black node can cooperate with each other in order to drop the data packets. It means black hole nodes work in a group to attack the ad hoc network. Also, there should be a generalized approach that can be nworked for other attacks like gray hole, warm hole etc.

REFERNCES

[1] Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng (2007) "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network". Paper presented at the PAKDD workshops, Nanjing, China, 22-25, pp. 538-549.

[2] E.A. Mary Anita, V. Vasudevan (2011), "Black Hole Prevention in Multicasting Routing Protocols for Mobile Ad hoc Networks using Certificate Chaining", International Journal of Computer Applications, Volume 1, pp. 21-28.

[3] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao (2011), "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", Human-centric Computing and Information Sciences, Springer, New York, pp. 1-16.

[4] Gurdeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal (2012), " Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs", 2012 International Conference on System Engineering and Technology, Bandung, Indonesia, pp. 1-5.

[5] Hesiri Weerasinghe (2008) "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking, Volume 2, pp. 362-367.

[6] Hemant Kumar, Dr. Ajit Singh (2012), "An Efficient Implementation of Digital Signature Algorithm with SRNN Public Key Cryptography", International Journal of Research Review in Engineering Science and Technology, Volume-1 Issue-1, June 2012, pp 54-57.
[7] Hongmei Deng, Wei Li, and Dharma P.Agarwal (2002), "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, pp. 70-75.
[8] J.Sen ,S.Koilakonda and A.Ukil (2011), "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks," Intelligent Systems, Modeling and Simulation (ISMS), 2011 Second International Conference on , 25-27 Jan. 2011, pp. 338-343.
[9] K. Lakshmi et al.(2010) "Modified AODV Protocol Against Black hole Attacks in MANET" International Journal of Engineering and Technology Vol.2 (6), pp. 444-449.
[10] L. Tamilselvan and V. Sankaranarayanan (2008), "Prevention of co-operative black hole attack in MANET," Journal of Networks, Vol. 3 Number 5, pp.13- 20.
[11] Latha Tamilselvan and V Sankarnarayana (2008), "Prevention of Black Hole Attack in MANET", Journal of Networks, Volume 3, Number 5, pp. 13-20.
[12] Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan (2011) "A local Intrusion Detection Routing Security over MANET Network", IEEE, July 2011, Bandung, Indonesia, pp. 1-6.
[13] Mohammad Al-Shurman, Seong-Moo Yoon and Seungjin park (2004), "Black Hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, Proceedings of the 42nd annual southeast regional conference , 2004, pp. 96-97.
[14] N.Mistry, D.C.Jinwala and M.Zaveri (2010), "Improving AODV protocol against black hole attacks", Proceedings of the International MultiConference of Engineers and Computer Scientists 2010, Volume 2, IMECS 2010, Hong Kong, pp. 1034-1039.
[15] P. Agrawal , R.K. Ghosh, and S.K. Das (2008), " Cooperative Black and Grayhole Attacks in Mobile Ad Hoc Networks", International Proceedings of 2nd international Conference on Ubiquitous Information Management and Communication, Suwon, Korea, ACM 2008, pp. 310-314.
[16] Payal N. Raj and Prashant B.Swadas (2009), "DPRAODV: A system against black hole attack in AODV based MANET", International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp. 54-59.
[17] P.C Tsou, J.M Chang, Y.H Lin, H.C Chao, J.L Chen (2011) "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs", 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 13-16 Feb. 2011, pp. 755-760.
[18] S. Banerjee (2008), "Detection/Removal of Cooperative Black and Grayhole Attack in Mobile Ad-Hoc Networks," In Proc. of WCECS 2008, San Fransisco, USA, 2008, pp. 337-342.
[19] S. Ramaswamy, H.Fu, M.Sreekantaradhya, J. Dixon, and K.Nygard (2003), "Prevention of Cooperative black hole attack in wireless ad hoc networks," International conference (ICWN˝03), Las Vegas, Nevada, USA, 2003, pp. 570-575.
[20] S.Marti, T.J.Giuli, K.lai and M.bakery (2000), "Mitigating Routing Misbehaviour in Mobile Ad hoc Networks", 6th MOBICOM, Boston, Massachusetts, August 2000, pp. 255-265.
[21] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto (2007), "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, Issue 3, Nov 2007, pp. 338–346.
[22] Sun B, Guan Y, Chen J, Pooch UW (2003) "Detecting Black-hole Attack in Mobile Ad Hoc Networks", 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003, pp 490-495.
[23] Yiebeltal Fantahun Alem, Zhao Chenh Xuan (2010), " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anamoly Detection",2nd International Conference on Future Computer and Communication, IEEE, Volume 3, 2010, pp V3-672,V3-676.
[24] Y. Zhang, W. Lee, "Intrusion detection in wireless ad-hoc networks," Proc. of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM'2000), pp. 275-283, Aug 6-11.