Identifying & Isolating Multiple Black Hole Attack on AODV protocol in MANET

A dissertation

submitted by

Aman Saurabh

Regd no:-11309398

To

Department of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab, India

In Partial fulfillment of the requirement for the

Award of the Degree

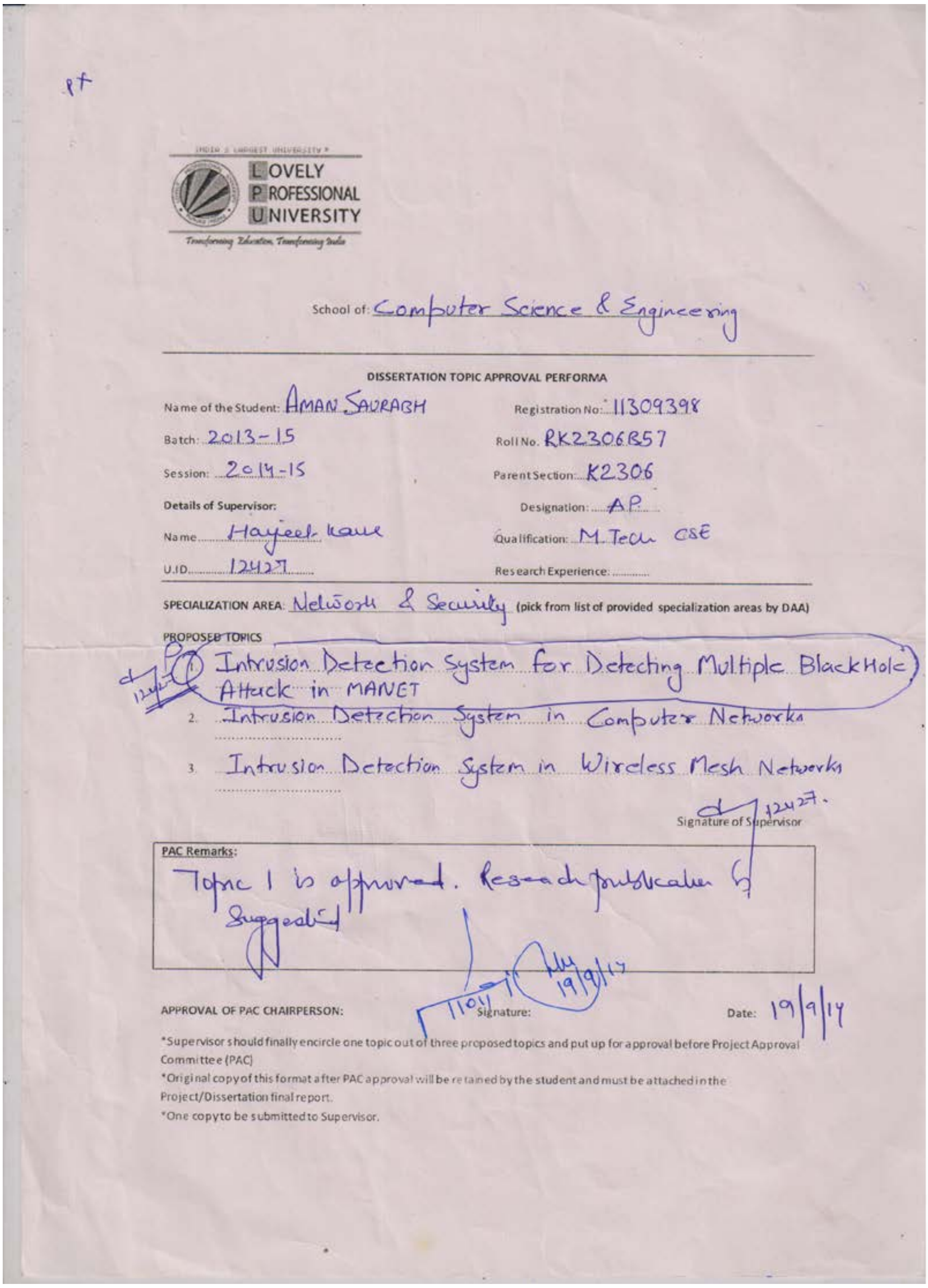
Master of Technology in Computer science

Under the guidance of

Mrs. Harjeet Kaur

(MAY 2015)

PAC FORM



pt

INDIA'S LARGEST UNIVERSITY

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education, Transforming India

School of: Computer Science & Engineering

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: AMAN SAURABH — Registration No: 11309398

Batch: 2013-15 — Roll No. RK2306B57

Session: 2014-15 — Parent Section: K2306

Details of Supervisor: — Designation: A.P.

Name: Harjeet kaur — Qualification: M.Tech CSE

U.ID: 12427 — Research Experience: ....

SPECIALIZATION AREA: Network & Security (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. Intrusion Detection System for Detecting Multiple BlackHole Attack in MANET
2. Intrusion Detection System in Computer Networks
3. Intrusion Detection System in Wireless Mesh Networks

12427.

Signature of Supervisor

PAC Remarks:

Topic 1 is approved. Research publication is Suggested

11014 19/9/14

APPROVAL OF PAC CHAIRPERSON: Signature: — Date: 19/9/14

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

ABSTRACT

A mobile ad hoc network can be described as a wireless network which is a collection of heterogeneous mobile devices and is self-organizing, self-configuring. The security in MANET is a highly preferred research area these days because it is susceptible to various attacks like collaborative black hole attack which we are discussing in this paper. A Multiple Black Hole Attack is a type of DOS attack which effects network load, packet end to end delay and network throughput. This paper investigates the study of AODV protocol under Multiple Black Hole Attack. This approach can be used to detect multiple black hole nodes present in an ad hoc network. The purpose of the designed algorithm is to avail stability in the network when it is under attack by multiple malicious nodes, maintaining a reasonable level of packet end to end delay, packet loss & throughput. It will also help in maintaining a secure passage to destination. In this algorithm we make use of the knowledge based learning & Bogus RREQ to validate each node in its path thereby providing a direct negotiation for secure route.

CERTIFICATE

This is to certify that **"AMAN SAURABH"** has completed M.Tech dissertation proposal titled **"Identifying & Isolating Multiple Black Hole Attack on AODV protocol in MANET"** under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation proposal is fit for the submission and the partial fulfillment of the conditions for the award of M.Tech Computer Science & Engineering.

Date: ________

Signature of Advisor

Name:

UID:

ACKNOWLEDGEMENT

I take this opportunity to express my profound gratitude and deep regards to my guide **Mrs. Harjeet Kaur** for her exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. The blessing, help and guidance given by her time to time shall carry me a long way in the journey of life on which I am about to embark.

I also take this opportunity to express a deep sense of gratitude to the teachers of Lovely Professional University for their cordial support, valuable information and guidance, which helped me in completing this task through various stages.

Lastly, I thank almighty, my grandparents, parents, siblings and friends for their constant encouragement without which this assignment would not be possible.

AMAN SAURABH

DECLARATION

I hereby declare that the dissertation proposal entitled, **“Identifying & Isolating Multiple Black Hole Attack on AODV protocol in MANET”** submitted for the M. Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: 5th May, 2015 **Investigator**

Aman Saurabh

Regd. No. 11309398

Contents

LIST OF FIGURES

LIST OF TABLES

Chapter 1
INTRODUCTION

A MANET can be described as a wireless network which is a collection of heterogeneous mobile devices and is self-organizing, self-configuring. In this type of network the devices communicate through a wireless medium with each other. It is necessary that the devices present in the network should cooperate with each other so the packets can be transmitted via intermediate devices when there is no direct path from source to destination. There is no concept of central controlling authority & a permanent network infrastructure in a mobile ad-hoc network. Transfer of packets is done with the help of routing protocols, which help in determining the suitable route from source to destination for initiating as well as maintaining a connection between the two. Network topologies are dynamic in nature, due to which there are link breakage and disruption in peer to peer connection. There is highly dynamic nature of wireless network imposes severe restrictions on routing protocols. Ad hoc network can be described as a wireless network which works without the existence of a centralized and fixed infrastructure as displayed in Figure 1. Without the presence of an infrastructure, there exist various issues & challenges in the working of these wireless ad hoc networks. Thus a wireless network consisting of mobile nodes which is ad hoc in nature can be called as MANET. The mobile nodes in the network are capable to acknowledge & course traffic via the intermediate nodes towards the destination, mobile nodes present in the network can act as a router as well as a host. The frequent fading of mobile nodes result in connection termination and re-association of nodes includes another variable to the characteristics of mobile nodes which is energy.

As MANETs are illustrated by limited bandwidth and node mobility, it is suggested to consider how much energy efficient a mobile node is and frequent changes in the topology and reliability of the communication in the scheme. There are many types of protocol are available in MANET. A routing protocol’s efficiency can be evaluated on the basis of battery power utilized by a mobile node participating in the communication in order to route the traffic in the network.

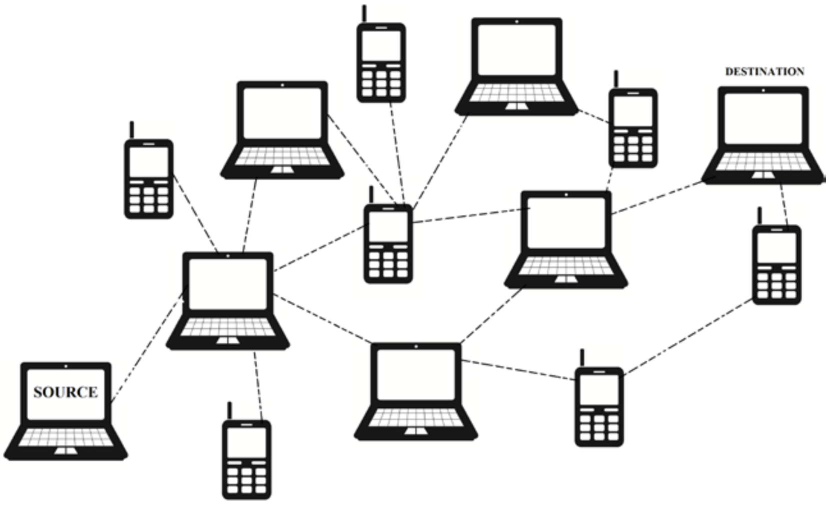


Figure 1: Mobile Ad-hoc Network

1.1 ROUTING PROTOCOL

The principle objective of routing protocols in ad-hoc network is to create optimal path i.e. having lesser intermediary nodes between source and destination with least overhead and least transfer speed utilization so that the data packets are passed on time. Protocols used in MANET should be able to perform in an effective & efficient manner over a variety of heterogeneous networking environment including small ad-hoc group as well as multi hop networks which are larger in size. Figure 2 displays the various categories of routing protocols available in ad hoc network. In reference to the routing topology of MANET, routing protocols in MANETs can be classified into proactive, reactive and hybrid. Proactive protocols constantly maintain the updated topology of the network and are typically table-driven. The Proactive routing protocols include DSDV. Reactive protocols are also known as source-initiated on-demand protocols, they do not periodically update the routing information. They initiate route discovery process only when they are requested to do so, source node wants to find a path to a desired a destination. AODV & DSR are some example of these types of protocols. Now coming to hybrid protocols, they utilize the functionality of both the protocols i.e., reactive and proactive approaches. Zone Routing Protocol is an example of hybrid routing protocol.

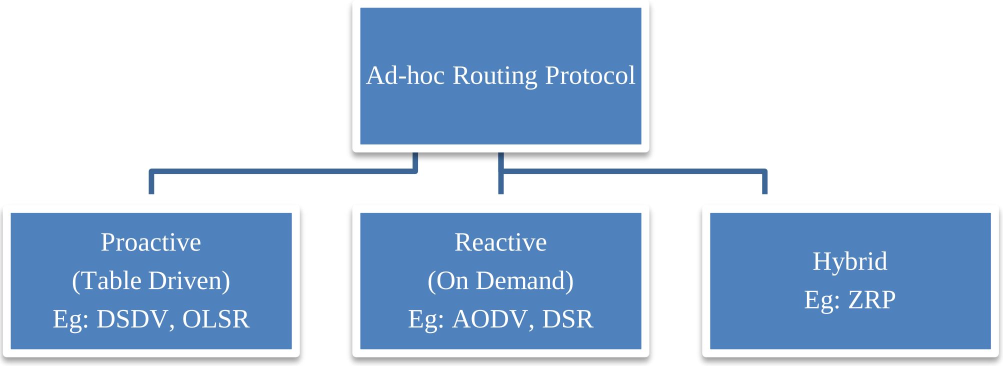


Figure 2: Routing Protocols

1.1.1 Proactive Routing Protocol

These protocols are likewise called as Table Driven protocols since they keep up the routing details even before it is required. Each node in the network keeps up routing details to each other node in the network, the routing details are stored in the routing tables which is updated regularly whenever there is a change in the network topology. The main drawback of these type of protocols is that, it maintains numerous number of tables. Thus they are not suitable for larger network due to their tendency of creating & maintaining node entries in the routing tables for each every node present in the network at every node. Due to this network overhead is increased which lead to the increase in the utilization of network bandwidth.

(a) Destination Sequenced Distance Vector Routing (DSDV) Protocol – It is one of the table driven routing protocol which is designed from the standard Bellman-Ford Routing algorithm. It integrates a novel attribute which is sequence number to each route's table entry of the typical RIP. Utilizing the newly integrated attribute, the wireless mobile nodes are now capable of distinguishing obsolete route information from the fresh one. Hence the formation of routing loops are avoided.

(b) Optimized Link State Routing (OLSR) Protocol - The Optimized Link State routing is defined in RFC3626. It is a proactive protocol which is basically table driven. As per the name implies, it utilizes the pure link state protocol in an optimized manner in order to spread network topology details. In a typical link state protocol, the information about the link's state is flooded all over the network. The OLSR makes use of this technique but the protocols in OLSR runs in multi hop scenario, therefore the flooding of the message in OLSR is optimized in order to retain the network bandwidth. The enhancement performed is centered on Multipoint Relaying method. OLSR being a table driven protocol performs these main operations consisting of updating and retaining info in a variety of tables. The data which is stored in the tables is based on received control traffic, and further control traffic is generated based on information which is obtained from these tables and route calculation is done with its help.

1.1.2 Reactive Routing Protocol

These type of protocols are also known as On Demand routing protocols or demand driven protocols because they are not into creating & maintaining routing details at each & every nodes at the network, when there is no active communication taking place in the network. In this protocol when a node desire to send a packet it initiates a route discovery process in order to determine optimal path to the intended receiver. The route discovery process includes flooding of route request packet throughout the network. Due to this type of packet flooding in the network, a substantial amount of control traffic is added to the network. The abundance of the control traffic in the network makes reactive routing protocols less suitable for real time traffic.

(a) Ad-hoc On-demand Distance Vector (AODV) - The Ad hoc On Demand Distance Vector (AODV) routing protocol is devised for the ad-hoc networks. AODV can adapt the single-cast and multiple-cast routing. It is on the basis of the on-demand mechanism to create the paths among the nodes by the desired source nodes. AODV manages the paths till it is required for the source nodes. It generates trees to associate with the multiple-cast category branches. The tree consists of the category branches and the nodes should integrate with its members. It is using the sequence number to preserve the originality of paths. AODV is a free of the loop, individual-origining, and calibrates with many nodes.

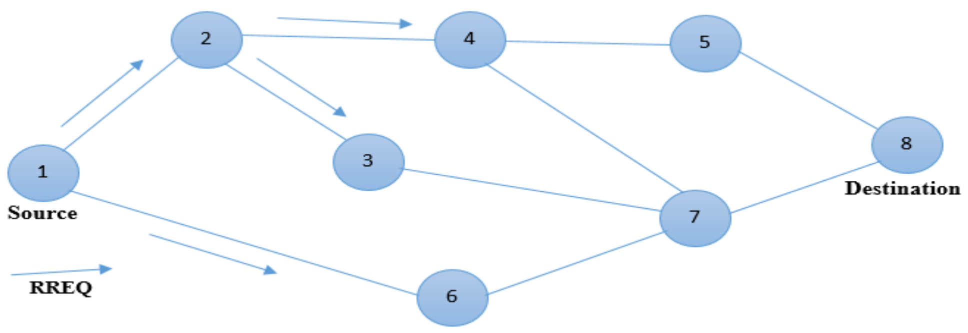


Figure 3: RREQ Broadcasted in the network.

It generates the paths with the RREQ / RREP mechanism as displayed in Figure 3. If the source node urges the path to the station node that didn't has a path, it transmits the RREQ message to the whole network. The nodes which receive the message refurbish the source node information. The information doesn't contain only source IP address, it also contains the generic sequence number, and transmission identification number, the route request message consists the sequence number to station node. The header format of a route request message is given in Figure 4. The node which receives the route request message transmits the RREP message, it can be the station node or the path to the station node includes the sequence number should be maximum than the route request message. It single-casts the route reply message to the origin node or else it retransmits the route request message. The nodes should manage the route request's origin location and the transmit identifier. When the node gets the route request message to be analysed, it abandon the rote request message.

Source Address	Request Id	Destination Address	Source Sequence	Destination Sequence	Hop Count

Figure 4: Header of a ROUTE REQUEST packet format.

As displayed in Figure 5, route request message transmits to the origin. It creates the set of nodes to the station node. When the origin node gets the route reply message, it starts to transmit the data messages to the station node. When the origin node gets the route reply packet consisting sequence number with the less distance between the nodes, it refurbishes the routing updates to the station node.

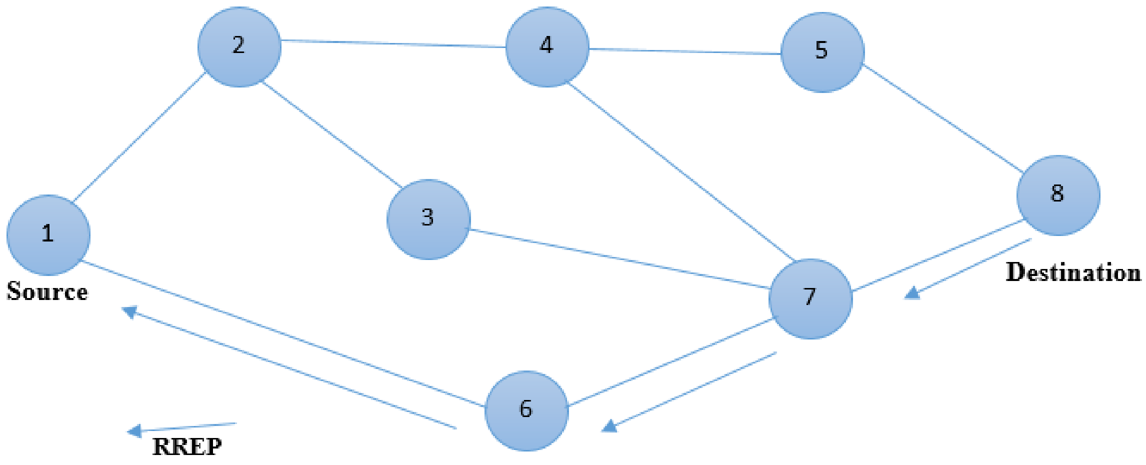


Figure 5: RREP propagates back to the source.

Source Address	Destination Address	Destination Sequence	Hop Count	Life Time

Figure 6: Header of a ROUTE REPLY packet format.

Figure 6 show header format of RREP packet. When the path is alive, it can be managed. The path is contemplated as alive when the data messages transmit from the origin node to the station node in the route. When the origin node does not transmitting the messages, the paths are discarded from the nodes. When the route is broken if the path is alive, the node generates the RERR packet to the origin to brief the unapproachable station nodes. When the origin receives the route error message, when the origin needs the path for the re launch the path construction.

Multiple-cast path can be created as the similar process. The node which wants to adhere the multiple-cast category transmits the route request message along the station node address for the multiple-cast category and set the join flag to express the likability to merge in the category. When a node receives the route request message which is the category of multiple-cast tree which have the sequence number of the multiple-cast group to transmit the routing reply message to the origin. When the origin node gets the routing reply messages it manages the path with the newest sequence number, and after the minimum distance to the later multiple-cast category. When the interval of time is completed, the origin node single-cast the Multiple-cast activation messages to the specified distance count. It acts as the scheme for switching on the path. The message is received by the specific nodes which has a multiple-cast path register would flush and discard the register. When the multiple-cast activation message is received by the node which is not branch of the multiple-cast tree, it is managing the optimal path in distinction to the received message of routing reply. Thus it should single-cast a multiple-cast activation message to the distance count, and till the node which were already the category of the multiple-cast tree is attained.

(b) Dynamic Source Routing (DSR) Protocol - It is a plain and competent routing protocol for the multiple-hop mobile ad-hoc networks. When the dynamic source routing protocol is used, it is a self-maintaining and self-configuring, which doesn't requires the already present infrastructure of the network. The nodes (computers) collaborate for the transmission of the messages to the nodes to permit transmission along the multi-hop among the nodes which are not in the vicinity of the communication field of the other nodes. In the network, when the nodes changes to merge or discard in the network, and the communication restraints are the changes in the intervention, the path is naturally identified and managed by the dynamic source routing protocol. When the sequence number of the transitional distance required to attain the station node can varies at period, the culminating terminology of the network can be of dynamic. The dynamic source routing protocol permits the node to identify the origin path among the multi-hop network to the specified station node in the mobile ad hoc network. The transmitted data message contains the completed header, list of ordered nodes for the message should ravine, permitting the transmitted message as paltry free of the loop and discarding the requirement for managing the information in the mediate nodes for the message is transmitted. With the inclusion of the header in the message for the origin path, the nodes transmitting the messages can stash the information of the routing or the paths.

1.1.3 Hybrid Routing Protocol

This type of protocols exploit the strengths of both reactive and proactive protocols, and combines the advantages of both together to obtain better results. In the initial stage of routing, the route is determined with the help of proactive method and after that the communication takes place by using reactive method from some additional active nodes. The basic idea is that each node has a pre-defined zone centred at itself in terms of number of hops and for the nodes which lie within the zone, the protocol used to maintain routing information in the network is proactive. The nodes which lie outside its zone, it does not maintain routing information in a permanent base. Instead, reactive routing strategy is adopted when inter- zone connections are required.

(a) Zone Routing Protocol (ZRP) – It make use of the mixed approach for routing. It utilizes the special features of both the routing protocols i.e. proactive & reactive. The main objective of ZRP is to resolve the excess use of network bandwidth & the delay which occurs in case of long route requests in proactive as well as reactive routing protocols. It breaks the network into various zones which are distinct in size. Each & every node which exist in the network is associated a particular zone, size of the zone does not depend on the amount of area it covers but the number of nodes which comes under the perimeter of that zone. The basic function of the ZRP is to provide a framework to other protocols i.e. it is not an independently operational protocol.

1.2 Advantages of Ad Hoc Networks:

Convenience: These networks being wireless in nature permits users to utilize network assets from approximately any suitable location inside their main networking environment which can be office or home.

Mobility: It is observed that with time there is significant evolution of public wireless networks, which now enable users to access the internet while they are outside their working environment like home or office.

Productivity: It describes that when users are connected to a wireless network, they can seamlessly go through their desired task online without any interruption even when they are on the go.

Deployment: The deployment of the infrastructure less ad hoc network is not much of a deal, it requires mobile nodes which can act as a host as well as a router.

Expandability: This type of network is scalable in nature, therefore it can handle the addition of new clients to the network. Whereas in case of a wired network, addition of new clients would be needing some extra wiring which will add to the cost.

Cost: The hardware required for wireless ad hoc network is quiet expensive on the basis of device configurations.

1.3 Applications of MANET

MANET is the self-configuring type of network in which the mobile nodes can leave or join the network when they want. MANET is decentralized type of network, no central controller is present. Due to their unique features mobile ad hoc networks can be deployed anywhere round the clock. Following are the various applications of MANET:

- Ad hoc networks do not pose the need for the deployment of a central controller and can be imbibed at anyplace, round the clock. In the infrastructure type of network if the central controller fails, whole network will be collapsed. Military applications take advantage of the unique features of MANET. In the battle fields, where it is difficult to manage and deploy infrastructure network we have got the option of Ad hoc networks at our stake.
- The Ad hoc networks are used for commercial purpose in the form of sensor networks. The sensor networks are deployed at far places like forests, deserts where these nodes can sense the conditions and pass the information to the base station.
- The mobile ad hoc networks can be used for the local communication e.g. Conferencing, Data exchange between mobile devices, Personal LAN gaming.
- Personal Area Network (PAN) is most common application of MANETs. PANs replace the traditional wired LANs for personal communication. They provide the solution to the communication between small areas. Bluetooth is the example of Personal area network.

1.4 Challenges of MANET

The various mobile nodes can form network at any place when required. In MANETs, no central controller is present; it is decentralized type of network. In such type of network following are the various key challenges:-

- MANET is the self-configuring type of network. Mobile nodes can move freely in the network. When the mobile node changes its position, network topology certainly changes with it. Designing an efficient routing protocol for such type of networks is a cumbersome task. The Multi cast routing is the key challenge in MANET.

- The security and reliability are the other major challenges of MANET. In this, certain types of internal and external attacks are possible. The attacker node can join the network at any time and trigger the attack. It have been a tedious task to design the key management and self-authentication mechanism for MANET
- The real time application like video conferencing requires fixed resource reservation to ensure quality of service. It is difficult to design such mechanism that guarantees Quality of service.
- The Mobile Ad hoc networks have been formed when nodes from various handheld devices or sensor nodes collocate. Power consumption is another major shortcoming of MANETs. The wireless sensor networks are deployed for sensing the environment conditions and generally deployed at far places. In such places, it is difficult to recharge or replace the battery of the sensor nodes. There have been inevitable requirements of efficient mechanism for power management.
- The mobile nodes can move freely in the network. In MANETs, it is very difficult to design a protocol which supports Location-aided Routing.
- There has been the existence of hidden terminal and exposed terminal problems in case of MANETs. There is an unavoidable need of a remedial mechanism to solve these problems.
- The mobile nodes can change its position at any time. This approach has led to the problem of link failure which degrades the network performance.

1.5 Classification of Attacks on MANET

The attacks on MANET can be categorized on the basis of the source and behaviour of the attacks. On the basis of the source the attacks can be internal or external and on the basis of behaviour the attacks can be either Passive or Active attack.

1.5.1 Attack on the basis of the source

The internal attack can be described as an attack on the network in which a malicious node is able get unauthorized access by masquerading itself. Clandestine nodes in the network are the reason behind internal attacks. These malicious node are able to sniff the network traffic and they can also take part in network activities. Figure 7(a) displays pictorial representation of the attack.

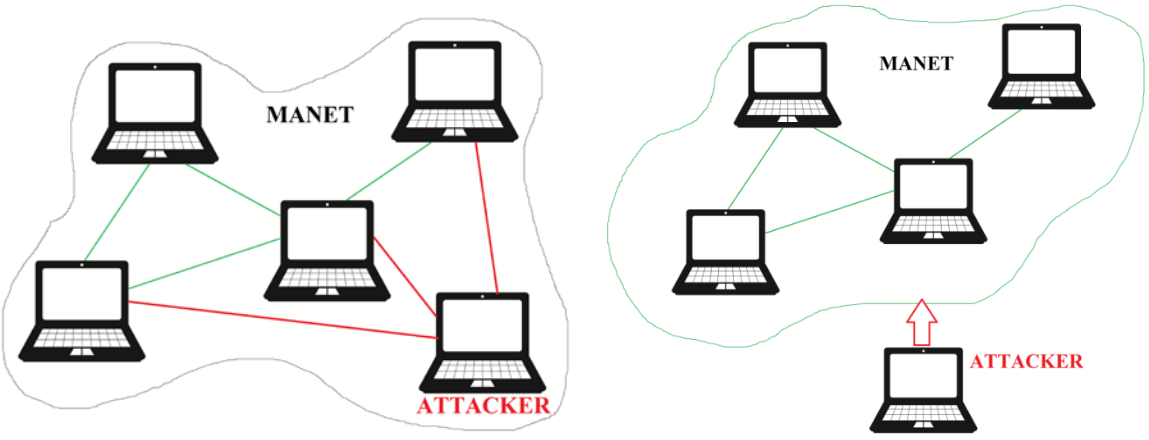


Figure 7: (a) Internal Attack (b) External Attack

The external attack can be described as an attack in which malicious node reside outside the network i.e. it does not belong to the network and wants to get access to the network. When these nodes are successful in accessing the network, they disrupt the performance of the whole network by flooding the network with bogus packets. Pictorial representation of the attack is displayed in Figure 7 (b).

1.5.2 Attack on the basis of the behaviour

A passive attack obtains data exchanged in the network without disturbing the communications operation. In this type of attack confidentiality of the network is compromised and these attacks are difficult to detect. Some examples of this type of attack are snooping and eavesdropping. Figure 8 (a) displays the passive attack.

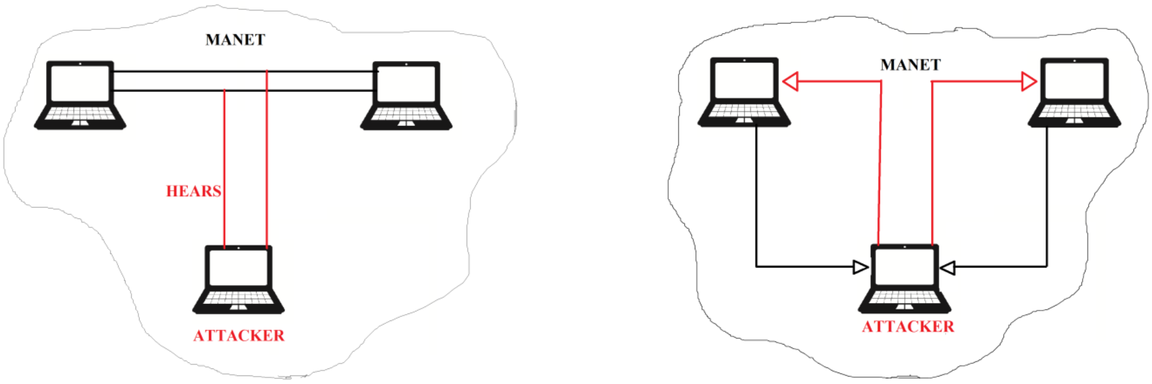


Figure 8: (a) PASSIVE ATTACK (b) ACTIVE ATTACK

An active attack can be described as an attack in which the information which is being sent on the network is altered or some new information is introduced in order to harm the receiver or participating entities. The integrity of the network is compromised in this type of attack. It comprises of information fabrication, modification and disruption to affect the network operation. Examples of these types of attacks include spoofing, masquerading. Figure 8 (b) displays active attack.

1.6 Attacks in MANET

1.6.1 Wormhole Attack

The worm hole attack is quite typical and merciless attacks, which can be executed in MANET. In this type of attack message is captured from the one region of network and replaying in other region. Attacker creates tunnel between two nodes which participate for communication. One attacker gather all message and other attacker replay to misinterpret to make destination unreachable from network.

1.6.2 Black hole Attack

In black-hole attack malicious node use its routing protocol to know other node that it has shortest path towards destination and attacker drop the packet to reduce the quantity of information is available to other node. This type of attack made intentionaly for deniall of service type attack. This make destination system unreachable or shutdown in network.

1.6.3 Denial of Service Attack

The main motive behind this attack is to make network resource unavailable to the nodes present in the network. On the successful execution of the attack, the network resources will be inaccessible. The techniques used by attacker to perform an successful DOS attack in MANET includes jamming of radio signal & making the mobile nodes run out of battery. It has further sub categories:

1. Smurf Attack
2. Distributed denial of services
3. SYN flood attack

1.6.4 Byzantine Attack

In this type of attack, there are multiple malicious node which works in collision to create routing loops, transmitting the packet through sub optimal routes as well as dropping of packets.

1.6.5 Man- in- the- middle attack

In this attack, an attacker sits between the sender and receiver and any information being sent between two nodes sniffs by him. In some cases, attacker may masquerade as the sender to communicate with receiver or masquerade as the receiver to reply to the sender. It starts when first attacker sniffs and eve dropped the packets.

1.6.6 Gray hole Attack

It is also is also known as selective packet drop attack because it drops the packet selectively with certain probability. The gray hole node works in such a way that for an instance it will act as malicious & then it will switch back to being a normal node.

1.7 Black Hole attack

In MANET, when a source node broadcast requests for route discovery it is eavesdrop by an attacker which was originally for the routers present in the network. When a RREQ for a path to desired destination node is received by the malicious node, it creates a bogus RREP response consisting of shortest path and highest sequence number. The main aim of malicious node is to get into the path of data transmission and drop the packets which pass through it. When the source node receives the RREP from the malicious node, it thinks that malicious node has the shortest path to the desired destination node, therefore it rejects all the RREP sent to it by the other nodes. By now the source has selected the path consisting of a black hole node, it will start transmitting data packets on that path thinking that it will reach the destination through that optimal path. But when all the packets sent by the source node on the selected path reaches the black hole node, they all will be dropped by it. Hence the packets transmitted by the source node will not reach the destination.

1.7.1 Multiple Black Hole attack

In this type of attack there are more than one malicious node in the network or we can say black hole node in the network. These nodes can either work in cooperation or individually.

1.8 Black Hole Problem in Routing Protocol (AODV)

It is a demand driven protocol in which path creation is only performed when it is required by the source node. Whenever the source needs a path to the destination, it begins a route discovery process inside the network. It floods a RREQ packet containing source address & destination address to its neighbors, who receive the packet & check for the destination address, increase the hop count & forward it to their neighbors and further. This procedure is done repetitively until the packet has reached the destination or it has reached an intermediate node which has fresh route to the destination. The intermediate node having fresh enough route to the destination will only reply to the RREQ packet. The node having path to destination responds by unicasting a RREP packet back to the neighbor from which it first received the RREQ.

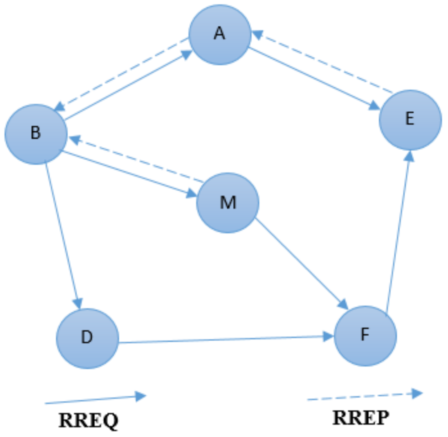


Figure 9: Routing Discovery Process in AODV protocol

A black hole problem can be defined as mischievous node introducing itself as an intermediary node having shortest path to the destination, instead of forwarding packets to its neighbors it drops the routing packets. Figure 9 consist of six nodes A, B, D, E, F and M respectively, in which M is a malicious node. Whenever node A floods an RREQ packet in the network, it will be received by nodes B, D and M. It is known that Node M is a misbehaving node, therefore it sends back a RREP packet instantly on receiving the request and advertising itself having the shortest path to the destination without even consulting its routing tables for the requested route to node *E*. The node A will receive reply from M earlier than any other node in the network. Hence it will assume that M holds the shortest path to the destination & will start transmitting packets to it. Node M will behave like a black hole by absorbing all the packets sent to it.

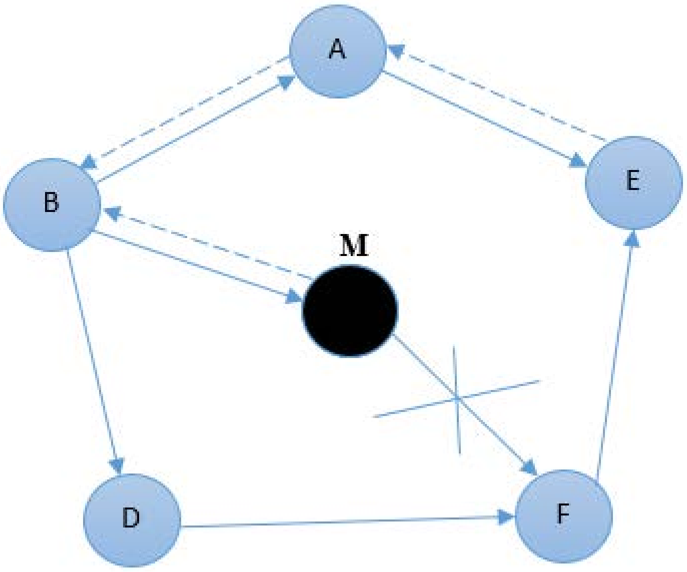


Figure 10: Black Hole problems in AODV

In AODV, the freshness of the routing information obtained from the sequence number present in the routing packets. When a source node broadcasts the RREQ message for desired destination node, if there exist a black hole node in the network then the black hole node as shown in Figure 10 will instantly send a RREP as a response of the RREQ having the higher value of sequence number and it will be sent in such a manner that the source will think thank it is coming from the original destination node or from a genuine intermediate node which has fresh enough route to the destination. Source will start transmitting the packets which will be absorb by the malicious node. Hence making destination unreachable.

1.8.1 Multiple Black Hole Problem in AODV

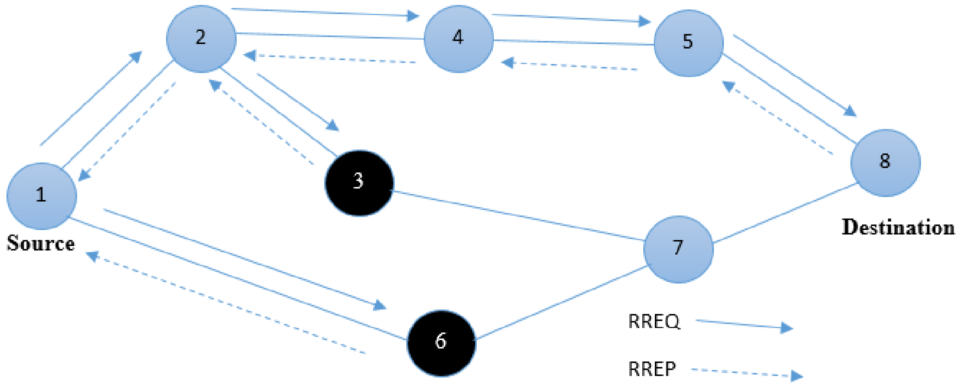


Figure 11: Multiple Black Hole Node

AODV works on the basis of the on-demand mechanism to create the paths among the nodes by the desired source nodes. AODV manages the paths till it is required for the source nodes. It generates trees to associate with the multiple-cast category branches. The tree consists of the category branches and the nodes should integrate with its members. It is using the sequence number to preserve the originality of paths. In the presence of multiple black hole as displayed in Figure 11, the misbehaving nodes will fabricate a RREP consisting of highest sequence number value, in order to introduce itself having a shortest path to the intended destination. The source node will rely on the information obtained from the RREP and it will start sending packets to that malicious node. A malicious node can be present at any place in the network. In the above figure there are more than one adversary nodes in the network which in our case are node 3 & node 6.

Chapter 2
LITERATURE REVIEW

A mobile ad hoc network (MANET) is a self-constructing network that is designed instinctively by a set of mobile devices via wireless communication channels. Nodes in such a network work together by forwarding packets for each other. MANETs do not have centralized administration or fixed network infrastructure. In MANET most of the routing protocols were developed without any security measures and are thus susceptible to a number of attacks. One of the popular routing protocols in MANET is Ad hoc on-demand distance vector routing (AODV). Though, it is susceptible to the well-known black hole attack, where a misbehaving node deceptively advertises itself having shortest optimal paths to a destination node at the time when route discovery process is initiated by source node.

Sanjay Ramaswamy, et al were the first who proposed a solution for identifying multiple black hole nodes working in cooperation [6]. They somewhat modified AODV protocol by presenting cross checking and data routing information table (DRI). In which the table maintained every single entry of the node. For the transfer of the packets the authors relied on the trusted nodes.

The black hole issue is a security attacks that occur in mobile ad hoc networks (MANETs). There are two possible solutions presented by Mohammad Al-Shurman et al. The first solution is to determine multiple routes to reach the destination [2]. Whereas the second solution is the exploitation of the sequence number present in the header of routing packets. On simulating the solutions it is observed that compared to the typical AODV routing scheme; the second solution can verify 75% to 98% of the route to the destination depending on the pause times at a minimum cost of the delay in the networks.

Some enhancement in the existing AODV protocol is introduced by Latha Tamilselvan et al [1] which are able to avoid multiple black holes. In order to identify multiple black holes cooperating with each other technique is given to discover the safe route by avoiding the attacks. An assumption was made by the researchers while giving the solution for the concerned issue is that nodes are authenticated in advance and therefore they are allowed to participate in the communication passage. It uses Fidelity table where every node that is participating is given a loyalty level that will provide trustworthiness of that node. In the fidelity table, nodes which are having 0 values is are considered as adversary nodes and is thus eliminated.

An IDAD is introduced by Yibeltal Fantahun Alem et al to prevent both single as well as multiple black hole nodes [7]. It works on the principle that the mobile nodes present in the network do not trust on the other nodes to avoid intrusion. IDAD consists of audit data which is the pre-collected set of anomaly actions. If the action (activity) of a node is identical to the actions then the system forbids the particular node. On simulating the proposed system, it is observed that it maximizes the network performance by decreasing the control packet generation.

The advanced routing methods are discussed by Fan-Hsun et al. They not only categorize these proposals into single black hole attack and collaborative black hole attack but also analyzed the classes of these solutions and provided a comparison table. They presented summary of the pros and cons with popular routing protocol in wireless mobile ad hoc networks [9]. Then, the routing methods of existing solutions are categorized and discussed. In this work it is observed that there are specialized skills in both proactive routing and reactive routing. The proactive detection method has the superior detection probability & packet delivery ratio, but the major drawback in it is the higher routing overhead because the broadcast packets is done periodically. The routing overhead problem was removed by reactive detection method, but in the beginning of routing procedure it suffered from some packet loss.

A defence mechanism for a synchronised attack by multiple black hole nodes in a MANET is proposed by Jaydip Sen et al. The defence mechanism works by making some modification in the typical AODV protocol and it makes use of data routing information (DRI) table along with the stored and current routing table [8]. In the DRI table, the bit 1 represents true and the bit 0 represents false. From field in the DRI table is for routing data packets from the node and through field is for routing data packets through the node. For a node 3 if the entry is 1 0 that means the node 4 has routed packets from node 3 but not routed packets through node 3. Cross checking relies on trustworthy nodes and it will send packets to the trustworthy nodes only. Trustworthy nodes are the nodes through which the data packets have routed previously. If the data packet is not routed previously to the node that will become the suspicious node and the packets will not be routed to the suspicious nodes. On the basis of simulation carried out it is observed that on applying this proposed mechanism a reasonable level of throughput in the network is maintained.

An algorithmic approach for improving the security of AODV protocol is introduced by Rajib Das et al with the ability to detect and remove the black hole nodes in MANET [5]. An additional route is proposed to the intermediate node that send RREP message to source node for identifying the route to destination node is exists or not. The proposed approach cannot be applied to identify a multiple black hole attack consists of multiple nodes. Along with the routing table there is a data routing information (DRI) table which can be used for identifying multiple black hole nodes. On simulating the proposed algorithm, it is observed that there is reduction in network throughput and packet delivery ratio.

Durgesh Wadbude et al [4] discussed that network topology changes frequently, therefore AODV, DSR are used for being efficient adaptive routing protocols. Security becomes the major issue in Mobile Ad hoc Networks because the network is wireless. Some of the attacks due to misbehavior of malicious nodes include modification, fabrication, masquerade and denial of service attacks, which interrupts the transmission. An efficient secure AODV routing protocol is proposed in this paper. Simulation results indicates that suggested routing algorithm delivers a superior level of security and performance than present works. The results obtained from the simulation shows the enhancement in the network performance, with respect to overhead, and end to end delay to the secure AODV routing protocol.

Chapter 3
Present Work

3.1 Problem Formulation

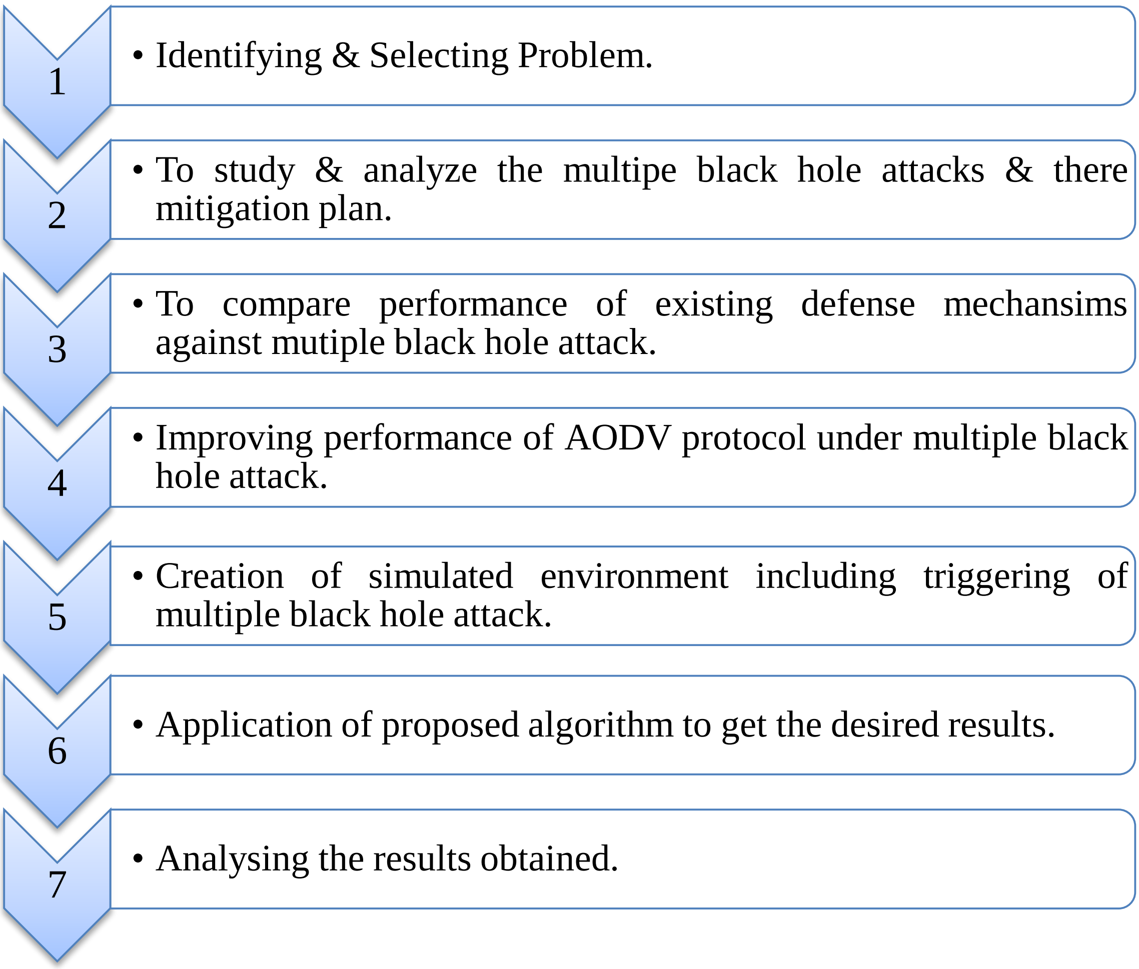
In MANET inside and outside attacks are possible, which degrade the performance of the network. In Inside attacks a node within the network become malicious node and it launched attacks on network. In outside attacks a malicious node which is outside the network, it become the member of the networks and then launched the attack on network. A passive outsider eavesdrops on all communication and aims to compromise privacy.

Among all the attacks discussed previous black hole attack is the most common active type of attacks. Black hole attack is the denial of service attacks which is triggered by the malicious nodes in the network. In the previous times, many techniques have been proposed to isolate black hole attacks from the network. When black hole attack is triggered in the network, throughput of the network reduced and delay increase as steady rate. The black hole attack is even worse if the multiple black hole nodes exist in the network. When multiple black hole nodes exist in the network, all the malicious nodes are responsible for triggering the black hole attack. This type of attack is called multiple black hole attack. In our work, we work on to detect and isolate multiple black hole attack in mobile Ad hoc network.

A significant amount of research has been devoted to study security issues as well as countermeasures to various attacks in MANET. However, there is still much research work needed to be done in the area. The purpose of this thesis is to identify the Black Hole attack using AODV protocol in MANET. This thesis work focuses on finding a secure route for communication by identifying and isolating all the malicious nodes present in mobile Ad hoc network to provide enhanced security and stability to MANET.

3.2 Research Methodology

Research methodology is a way to systematically solve the research problem. It can also be understood as a science of studying how research is done scientifically. It is a tool that is used to investigate the desired area thoroughly, collect & analyse data and on its basis conclusions are drawn. The approach towards research includes quantitative, qualitative and mixed approach. In our research the approach used is quantitative. This approach begins by studying the existing literature regarding our selected problem multiple/multiple black hole attacks in MANET, followed by comparison of existing defence mechanisms and introducing some enhancement in the existing protocol to strengthen the security. A simulated environment is created to test the performance of the algorithm & the analysis of the result is done. In Figure 12, research design is displayed.



1
- Identifying & Selecting Problem.

2
- To study & analyze the multipe black hole attacks & there mitigation plan.

3
- To compare performance of existing defense mechansims against mutiple black hole attack.

4
- Improving performance of AODV protocol under multiple black hole attack.

5
- Creation of simulated environment including triggering of multiple black hole attack.

6
- Application of proposed algorithm to get the desired results.

7
- Analysing the results obtained.

Figure 12: Research Methodology

3.3 Objectives

Following are the various objectives of this research work

- To focus on analysis of black hole attack in MANET and its consequences by reviewing the previously proposed plans suggested for counter measurement of Black Hole attack.
- To analyze the effects of black hole attack in the light of Network throughput, load, and end-to-end delay in MANET.
- To design an effective algorithm for detecting the Multiple Black hole Node in MANET using AODV protocol.
- To simulate the proposed algorithm and review the results

3.4 Simulation Tool

NS2 Overview: The network simulator (NS), a simulated program developed by VINT (Virtual Internetwork Test-bed) project group, is a discrete event simulator for networks.. It assists simulations of various network activities like simulation of UDP and TCP, some of MAC layer protocols, various routing and multicast protocols over both wired and wireless network etc.

Trace files are used to store the simulations, depending on user’s requirement and can be fed as input for analysis by different component:

- A NAM trace file (.nam) is used for the ns animator to produce the simulated environment.
- A trace file (.tr) is used to generate the graphical results with the help of a component called X Graph.

Chapter 4
Results & Discussion

4.1 Research Design

Network Simulator is used for simulating the environment in which at first a tcl file is created in which we fix the co-ordinate of simulation area i.e. terrain for displaying the simulation is specified, in our case it is 800 x 800 (x, y). NS instance is created, other parameters like channel type, antenna type, network interface, MAC type, number of mobile nodes, routing protocol are defined. Nodes are configured, network animator (nam) file is created and all the events & configuration are traced by generating a trace file on successful execution of the tcl file. All the necessary parameters are summarized in Table 1.

Table 1: Simulation Parameters

Parameter	Value
Terrain Area	800 m x 800 m
Simulation Time	50 s
Number of Sources	1
Number of Nodes	15
Routing Protocol	AODV
Data Payload	512 Bytes/Packet
Pause Time	2.0 s
Number of Adversaries	1 to 3
MAC type	802.11
Application Traffic	CBR

Number of nodes: This parameter in the above table is used to represent number of nodes that are used for conducting the simulation.

Pause time: this parameter represents the time interval for which the nodes can be paused in the network during simulation.

Traffic type: Network traffic can be of two type's viz. Variable Bit Rate (VBR) and Constant Bit Rate (CBR). In current simulation CBR type traffic is used.

Simulation time: Simulation time is the duration of time for which the simulation is carried out.

4.1.1 Wireless Mobile Node Architecture

The architecture of a Mobile Node is explained in the figure 13. Simply, it is enhanced version of regular node. The enhanced part of regular node is shown below the dotted lines. There are number of blocks in the mobile extension part. Mobile's node network consist of link layer (LL) connected to ARP module. Link layer is connected an interface priority queue (IFq), and Medium Access Control (MAC). Radio Propagation Model is connected with network interface which is further connected to the MAC and Channel. Each component briefly describe here:

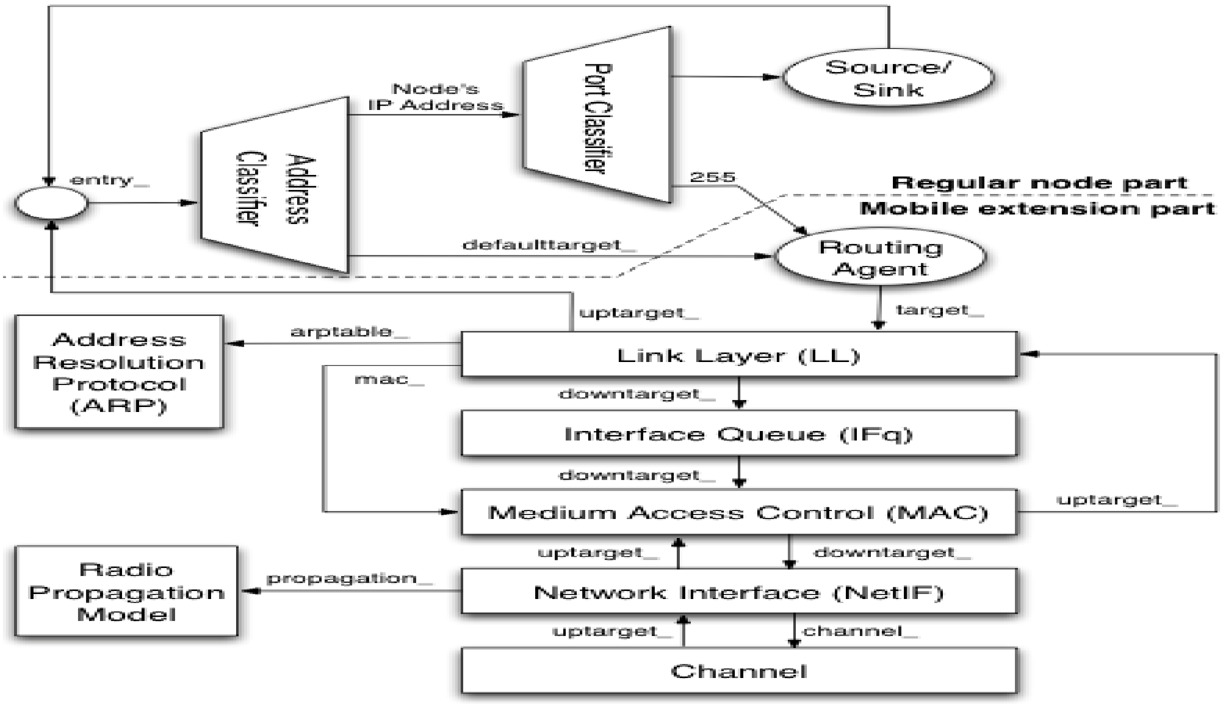


Figure 13: Mobile Node Architecture

1) Routing agent: A routing agent is responsible for transmitting packets from the node. Routing protocol works along with routing agent which uses networks for propagating routing information.

2) Link Layer: Link layer provides bandwidth, packet transmission time and propagation delay. For mobile node ARP module is attached with link layer which resolves issues of all IP to hardware (Mac) address conversions. Basically all packets transmitted between sender and receiver are functioned by LL by the routing agent. The LL hands down packets to the interface queue. Mac layer handles all the incoming packets to the LL till the node entry _point and these incoming packets are hands down in the interface queue by LL.

3) Interface Queue: This module models buffer management. The priority is given to the routing protocol packets by the PRIQueue class of queue and inserting routing protocols at the beginning of the queue. In queue filter runs over packets and removes destination address.

4) Medium Access Control (MAC): Ns-2 has been used for MAC layer in implementation of IEEE 802.11 Distributed Coordination Function (DCF) from CMU.

5) Network Interfaces: This is the module where the real transmission takes place. The radio propagation model works in the network interfaces to control packet transmission error. The Network Interphase layer act as a hardware interface through which channel is accessed by the mobile node. The shared wireless media interface is implemented called class Phy/WirelessPhy. Collision occurs in this type of interface and packets transmitted by other node interface to channel are received by the radio propagation. Meta-data is linked with each transmitted packet act like the transmission power, wavelength etc. In packet header meta-data is used for receiving interwork interface for propagation model to analyse minimum power received by each packet at receiving node.

6) Channel: This module is in fact not a part of a mobile node. It is the part which is shared among all neighbouring mobile nodes. A mobile node puts the packet being transmitted on this module. The destination node reads the channel and picks up the packet belonging to itself from this channel.

7) Address Resolution Protocol (ARP): This module translates hardware addresses into network (i.e., IP) addresses The Address Resolution Protocol (implemented in BSD style) module receives queries from Link layer. If ARP has the hardware address for destination, it writes it into the mac header of the packet. Otherwise it broadcasts an ARP query, and caches the packet temporarily. For each unknown destination hardware address, there is a buffer for a single packet. In case additional packets to the same destination are sent to ARP, the earlier buffered packet is dropped. Once the hardware address of a packet's next hop is known, the packet is inserted into the interface queue.

8) Tap Agents: Protocol Entity. Agents that subclass themselves as class Tap defined in mac.h can register themselves with the mac object using method installTap(). If the particular Mac protocol permits it, the tap will promiscuously be given all packets received by the mac layer, before address filtering is done.

9) Radio Propagation Model- It uses Friss-space attenuation (1/r2) at near distances and an approximation to two ray Ground (1/r4) at far distances. The approximation assumes specular reflection off a flat ground plane.

10) Antenna- An Omni-directional antenna having unity gain is used by mobile nodes.

4.1.2 Quantitative Metrics

There are a number of quantitative metrics that can be used for evaluating the performance of a routing protocol for mobile wireless ad-hoc networks. In current study, the general ideas described in RFC 2501 is followed, and four quantitative metrics are used. The packet delivery ratio and average end-to-end delay are most important for best-effort traffic. The other two qualitative metrics used in this thesis are and throughput.

(i) Packet Delivery Ratio

The packet delivery ratio is defined as the fraction of all the received data packets at the destinations over the number of data packets sent by the sources. This is an important metric in networks.

$$\text{packet delivery ratio} = \frac{\text{received packets}}{\text{generated packets}}\ \text{x}\ 100$$

(ii) End-to-End Delay

End-to-end delay includes all possible delays in the network caused by route discovery latency, retransmission by the intermediate nodes, processing delay, queuing delay, and propagation delay.

$$\text{end to end delay} = \frac{\sum(\text{time received} - \text{time sent})}{\text{total data packets received}}$$

(iii) Throughput

Ad hoc networks are designed to be scalable. As the network grows, various routing protocols perform differently. The amount of routing traffic increases as the network grows & network throughput is affected.

$$\text{throughput} = \frac{\text{received data}}{\text{data transmission period}} \text{ x } 8$$

(iv) Packet Loss

Packet Loss helps in determining the number of packets received by the receiver in reference to the number of packets transmitted by the sender.

$$\text{Packet Loss} = \text{GeneratedPackets} - \text{ReceivedPackets}$$

4.2 Implementation

At first the network is deployed with finite number of mobile nodes. Source and Destination are assigned in the network after that the source node broadcast a Fake Route Request containing a bogus destination address in the network. In this scenario if there is any black hole node present in the network then it will reply to source’s request with a Route Reply Packet (RREP) , on receiving that packet source will add the responding node to its black list & then knowledge based learning will be applied for confirmation of the malicious node if the node is confirmed being malicious then blacklist will be updated & an alarm message will be broadcasted in the network containing the id of the malicious node in order to isolate the malicious node and to inform all the nodes present in the network about the existence of the malicious node. After the malicious node is isolated, shortest path will be created with the help of AODV protocol & communication will take place. If the malicious node is not confirmed by applying knowledge based learning then step 3 will be repeated i.e. source ill again broadcast a fake route request packet if it doesn't receive a reply then the normal route discovery process using AODV protocol will take place & shortest path will established to the destination. The communication will take place on the established path.

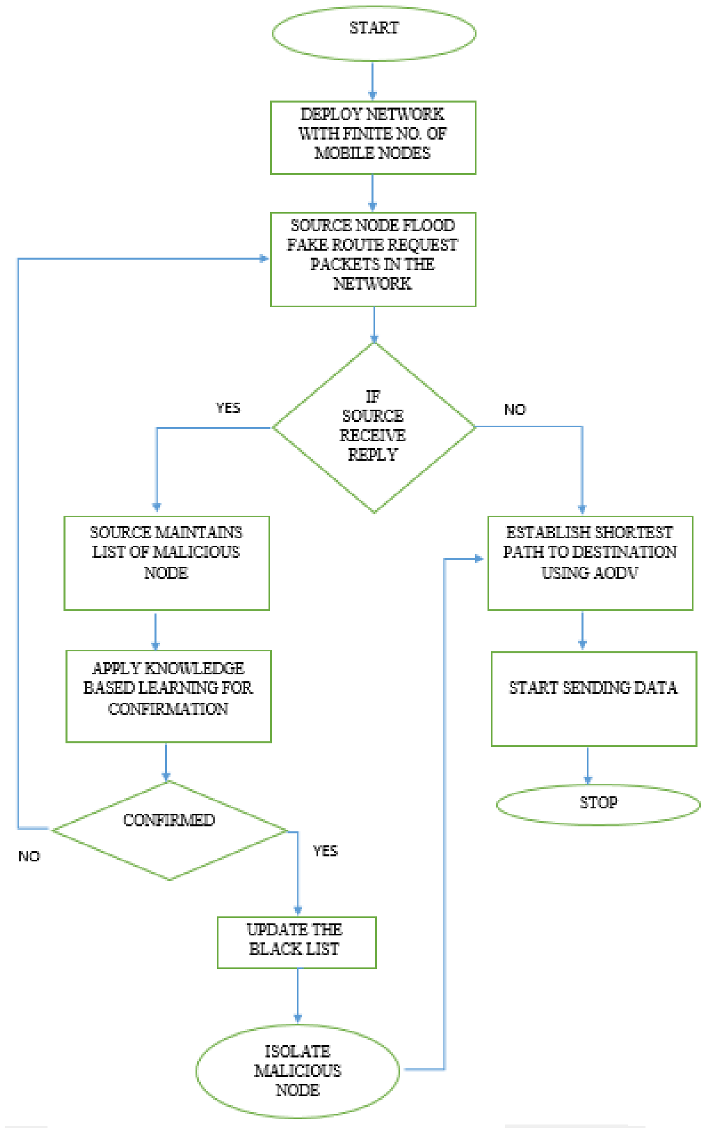

START
DEPLOY NETWORK WITH FINITE NO. OF MOBILE NODES
SOURCE NODE FLOOD FAKE ROUTE REQUEST PACKETS IN THE NETWORK
IF SOURCE RECEIVE REPLY
YES
NO
SOURCE MAINTAINS LIST OF MALICIOUS NODE
ESTABLISH SHORTEST PATH TO DESTINATION USING AODV
APPLY KNOWLEDGE BASED LEARNING FOR CONFIRMATION
START SENDING DATA
STOP
CONFIRMED
NO
YES
UPDATE THE BLACK LIST
ISOLATE MALICIOUS NODE

Figure 14: Flowchart of our proposed algorithm

PSEUDO CODE

S: Source Node D: Destination Node

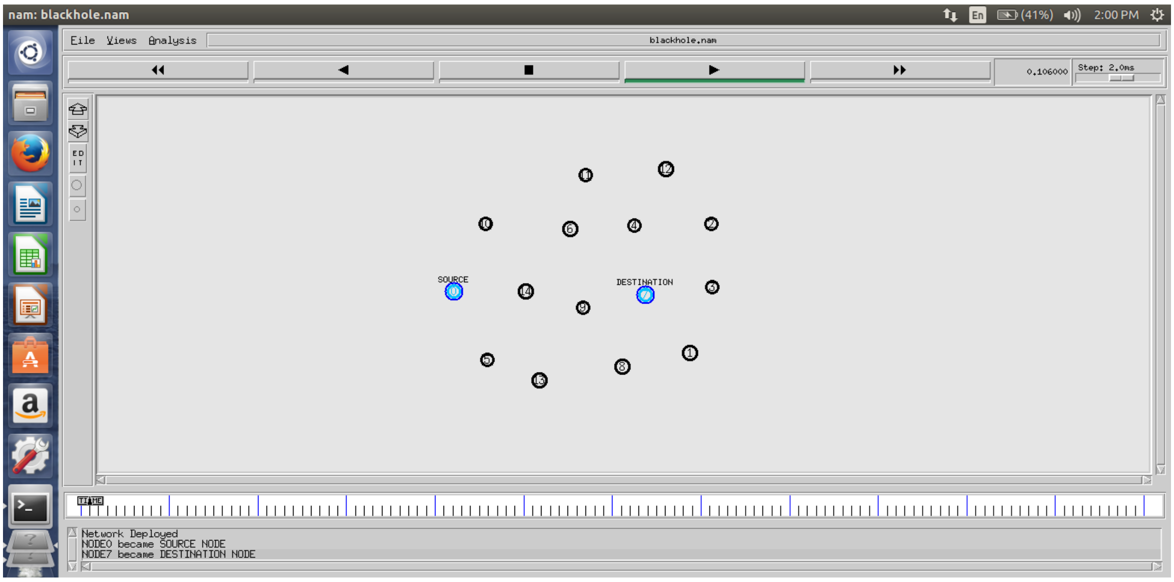
N: Network n: Nodes in the network

F_RREQ: Fake Route Request

```
1. Init (N:n)-> Initialize network N with n nodes.
2. valid_path (S->D in N)
3. S:Flood(F_RREQ(N))
4. for all reply {
5. if (reply){
6. test(reply)
7. black hole node detection & confirmation
8. update(black_list)} else
9. goto step 3, else
10. path (S->D, aodv)
11. exit
```

4.2.1 Network Deployment

The simulation for the proposed method has been carried using network simulator 2 & is graphical interface is created using network animator and the operating system used is Ubuntu 14.0.4. The network animator shows the positions of various nodes. The operating system used is installed on Virtual box which is allocated 4 GB RAM, 30 GB HDD and Intel 2.2 GHz processor Quad core Processor.

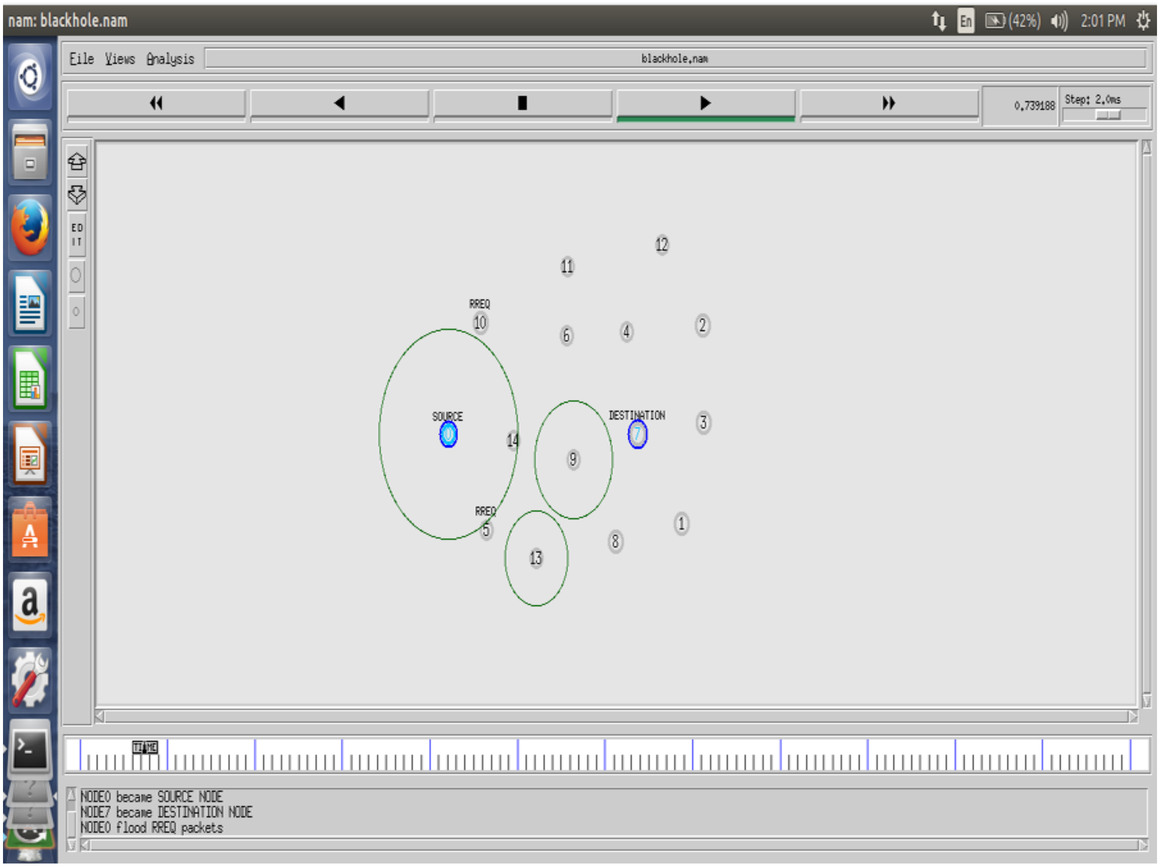


```
Network Deployed
NODE0 became SOURCE NODE
NODE7 became DESTINATION NODE
```

Figure 15: Network Deployment

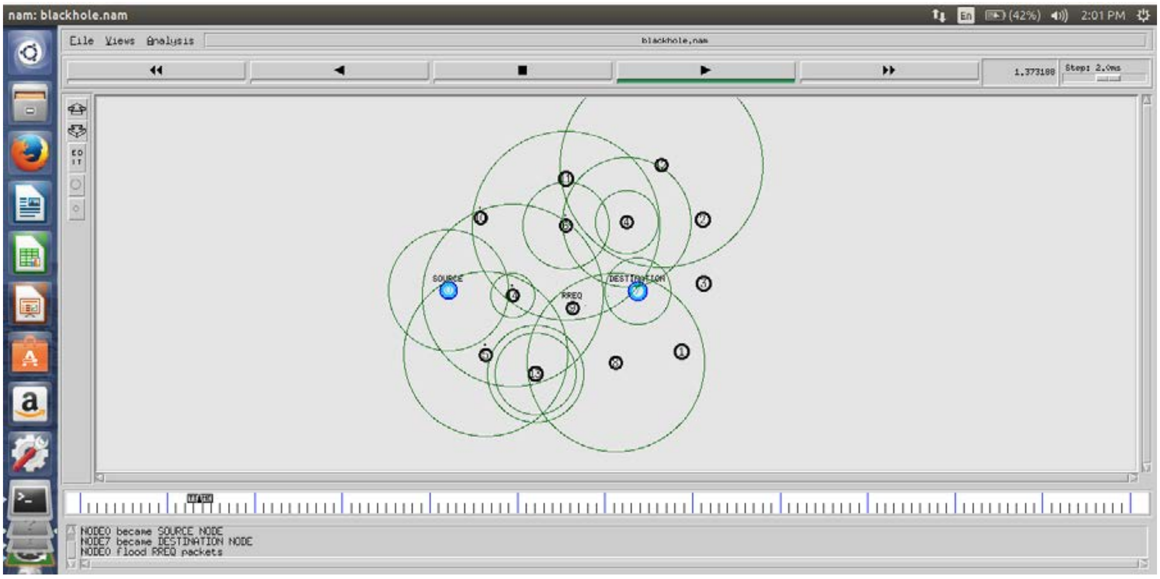
The figure 15 displays nodes in the network arranged arbitrarily and having numbers to distinguish each other. The two nodes designated as source and destination are demonstrated in blue colour. This animation has a start, stop, forward, and rewind, previous and next button. Additionally there is a zoom button to zoom in and out to see the nodes of the network. The speed of the animation can be adjusted on the basis of the requirement. The position of the node can be changed according to our requirement using the edit button. Thus the network animator offers a set of buttons that can be used to control the communication between the nodes in the network at any time.

Figure 16 and 17 shows the Source node broadcasting route request (RREQ) packets to its neighbouring nodes so that a route to destination could be found. The neighbouring nodes further broadcast this RREQ packets until it reaches the intended node i.e. destination node. At a certain point, node 0 becomes the source node whereas node 7 becomes the destination node and node 0 starts flooding the network with RREQ packets.



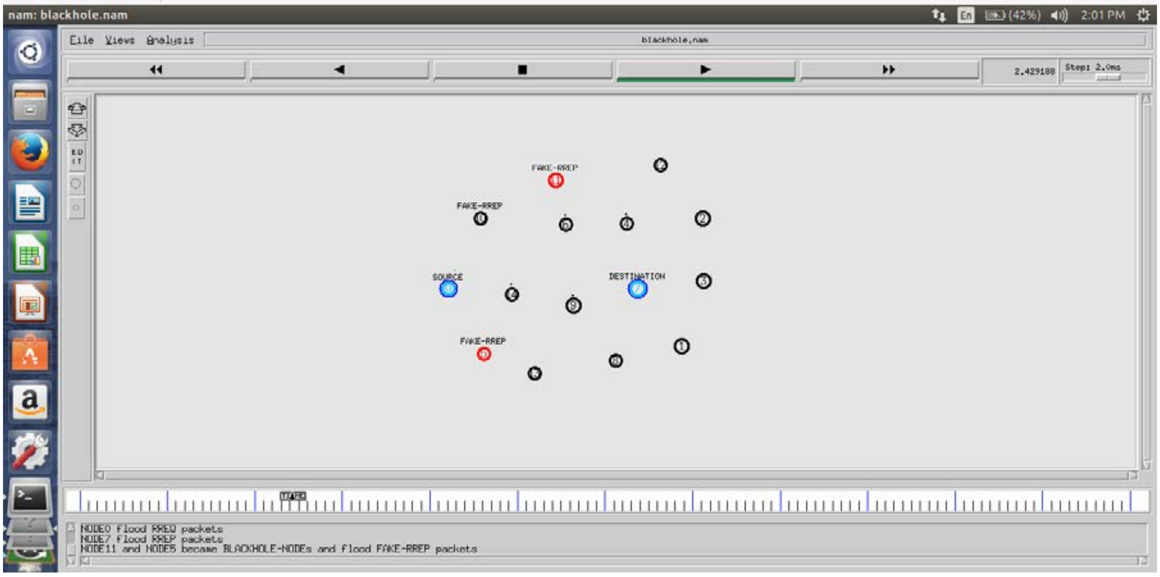
```
NODE0 became SOURCE NODE
NODE7 became DESTINATION NODE
NODE0 flood RREQ packets
```

Figure 16: Source Node Broadcasting RREQ packet



```
NODE0 became SOURCE NODE
NODE7 became DESTINATION NODE
NODE0 flood RREQ packets
```

Figure 17: Neighbouring nodes of the source receiving & further broadcasting RREQ

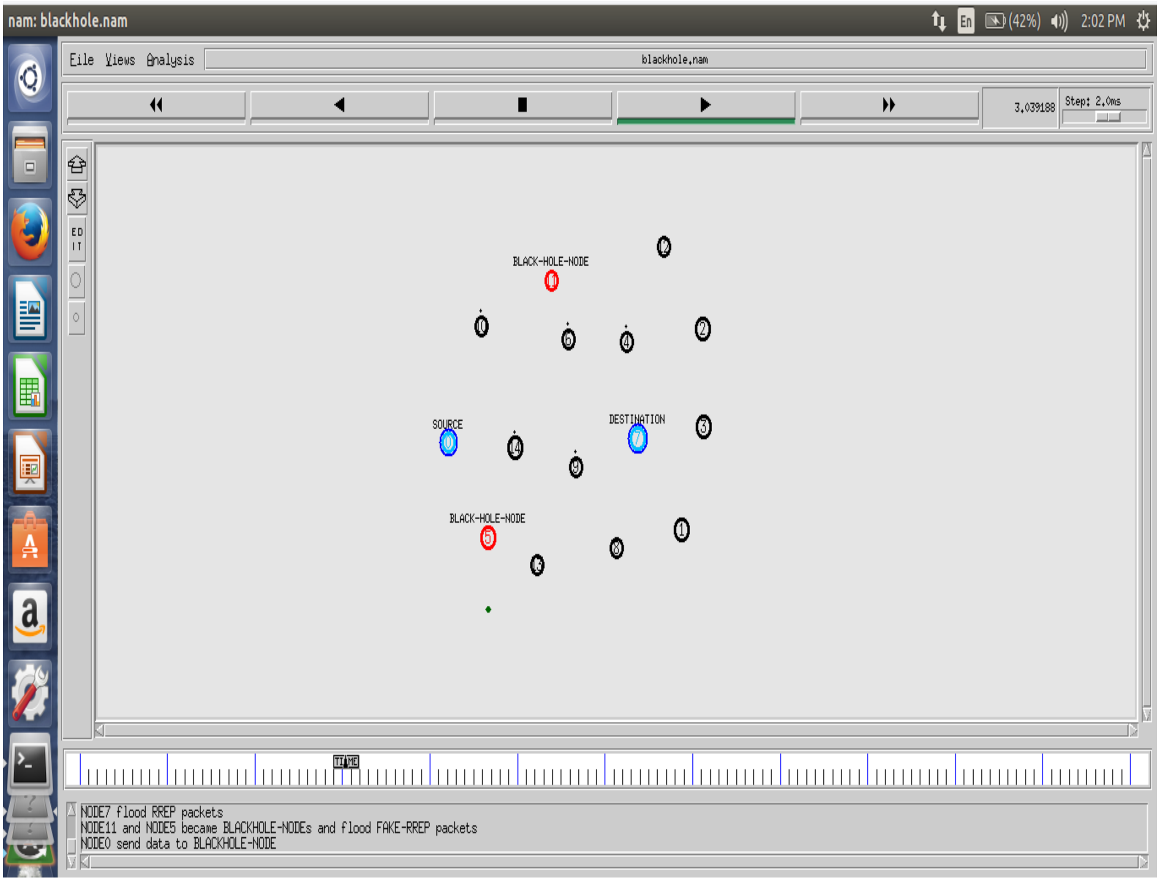


```
NODE0 flood RREQ packets
NODE7 flood RREP packets
NODE11 and NODE5 became BLACKHOLE-NODEs and flood FAKE-RREP packets
```

Figure 18: Malicious nodes replying with fake route reply packets

Figure 18 shows that the black hole nodes upon receiving the RREQ packets, start sending the RREP (Route Reply) packets to the source which initiated the route request. Now the point here is that the black hole nodes present in the network do not bother about whether the node to which a route is being requested even exists. It simply starts replying as soon as it receives the request packet with a higher sequence number. While the legitimate nodes check of they have any route to the requested node and only then reply. Thus during this whole procedure the black hole nodes are easily isolated and the whole network can be warned about their existence. The figure shows malicious nodes in red colour and they are sending fake RREP (Route Reply) packets to the source while the other nodes simply discard the route request packet received to find route to a non-existent node in the network.

Figure 19 shows that the source selects the route with the shortest path i.e. the route through which the route reply was received the earliest. Now this route has a black hole node and upon receiving data, it starts dumping all the packets thus resulting in loss of packets and increase in end-to-end delay.

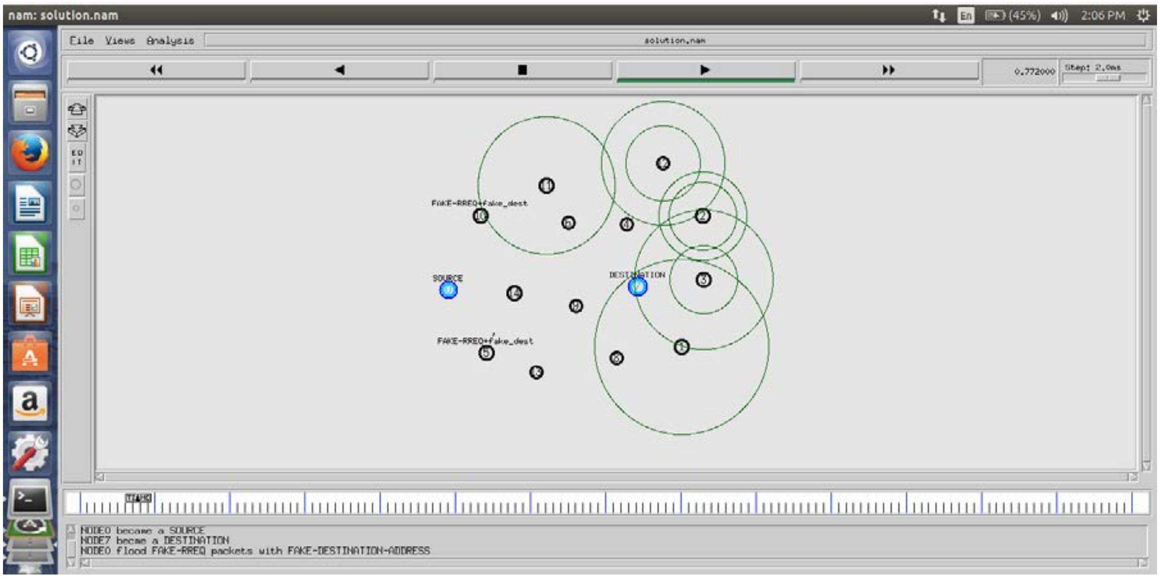


```
NODE7 flood RREP packets
NODE11 and NODE5 became BLACKHOLE-NODEs and flood FAKE-RREP packets
NODE0 send data to BLACKHOLE-NODE
```

Figure 19: Malicious Node 5 dumping the packets.

4.2.2 Solution Implementation

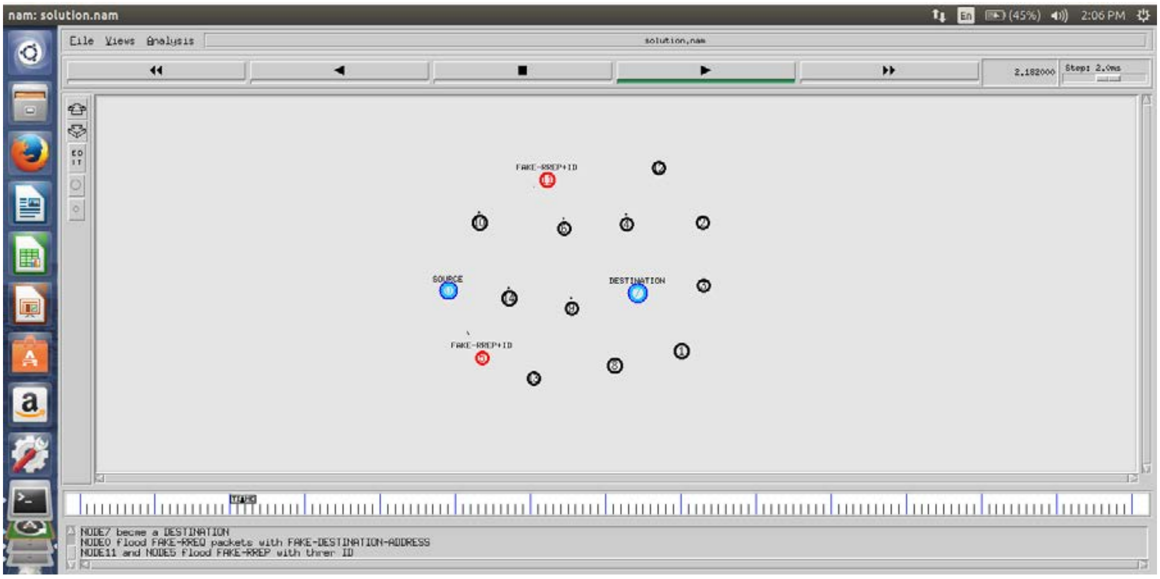
The solution for the black hole attack is implemented using a fake route request packets being broadcasted in the network and application of knowledge based learning.



```
NODE0 became a SOURCE
NODE7 becme a DESTINATION
NODE0 flood FAKE-RREQ packets with FAKE-DESTINATION-ADDRESS
```

Figure 20: Fake RREQ packets are broadcasted by the source node

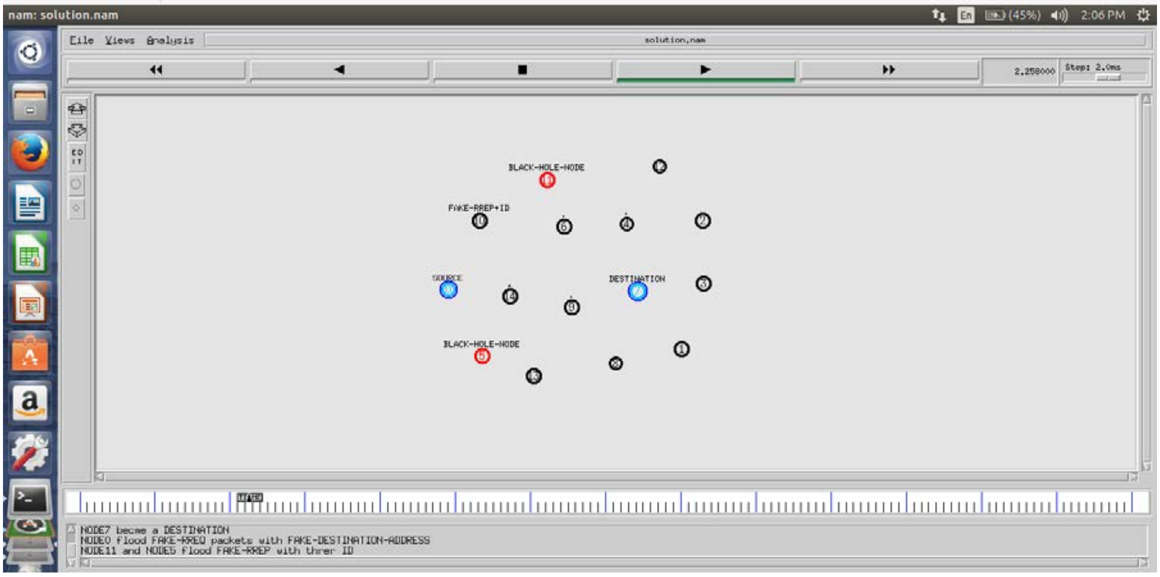
Figure 20 shows the fake route request packets being broadcast in the network for the identification of the malicious black hole nodes. The network is flooded with a request of route to a destination node which is non-existent in the network and this broadcasting continues until it reaches every node in the network.



```
NODE7 becme a DESTINATION
NODE0 flood FAKE-RREQ packets with FAKE-DESTINATION-ADDRESS
NODE11 and NODE5 flood FAKE-RREP with threr ID
```

Figure 21: Malicious node replying with Fake RREP

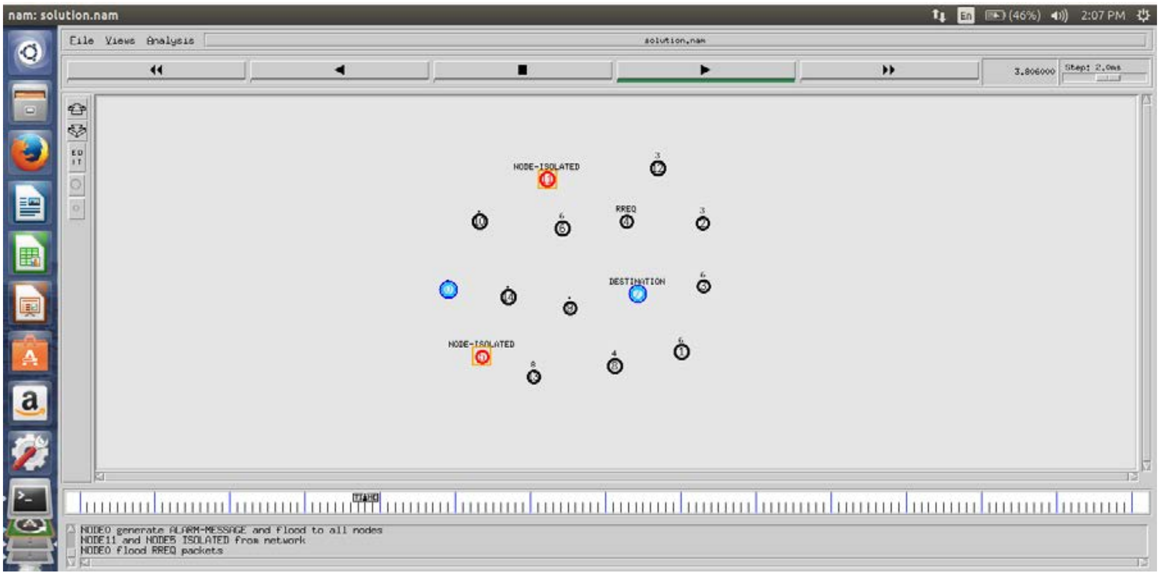
Figure 21 shows that upon receiving the route request packet, the black hole nodes are the one which immediately reply with a route reply packet having minimum number of hop counts and higher sequence number. Therefore making it a considerable path for the transmission of data. But the catch here is that the destination asked for in the route request packet does not even exists in the network, then how some of the nodes are able to provide a route to the non-existent node. Therefore these nodes which reply with a route reply packet are considered to be malicious nodes.



```
NODE7 becme a DESTINATION
NODE0 flood FAKE-RREQ packets with FAKE-DESTINATION-ADDRESS
NODE11 and NODE5 flood FAKE-RREP with threr ID
```

Figure 22: Malicious node broadcasting Fake RREP

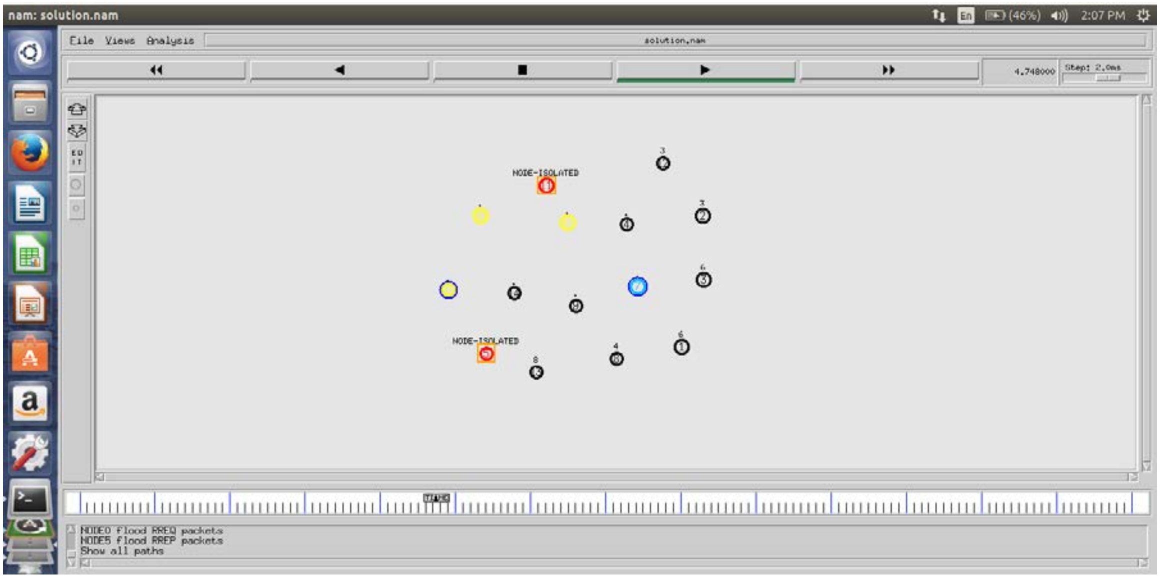
On receiving the reply from the malicious node, source node applies knowledge based learning & nodes are given rating. The node with highest number of rating is considered malicious and is then added to the black list. Figure 23 shows that black hole nodes are isolated after the successful detection and these nodes will not be considered for data transmission or participate in any activity being performed in the network.



```
NODE0 generate ALARM-MESSAGE and flood to all nodes
NODE11 and NODE5 ISOLATED from network
NODE0 flood RREQ packets
```

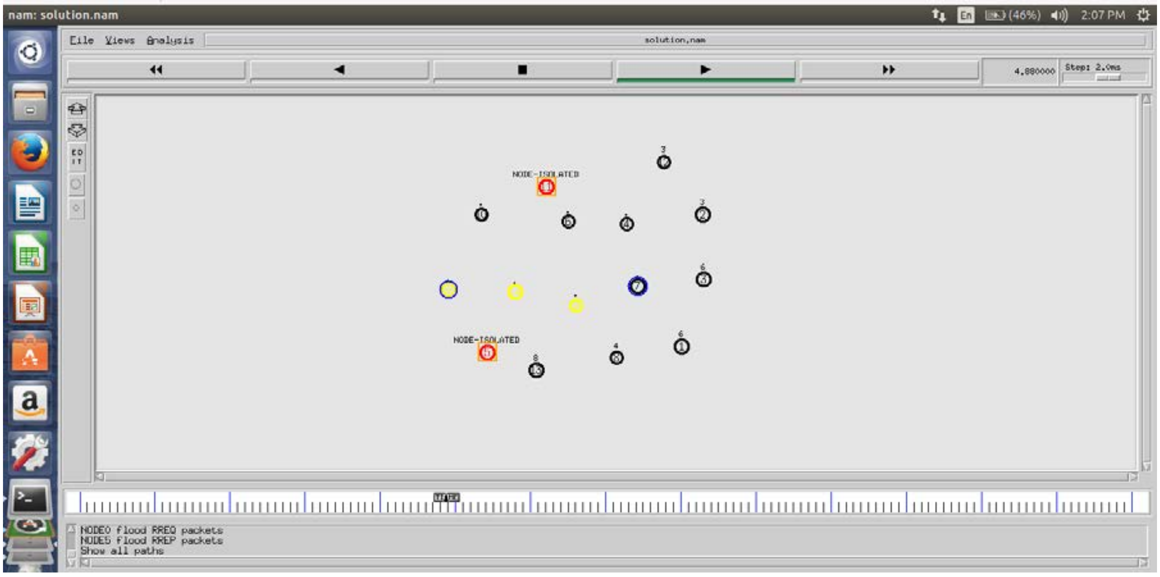
Figure 23: Malicious nodes isolated

Figure 24 shows the normal route discovery process initiated by the source node. The source nodes sends route request packets to its neighbouring nodes which further broadcast these to their neighbours and continues until it reaches all the nodes in the network or intermediate nodes which has a route to the requested destination.



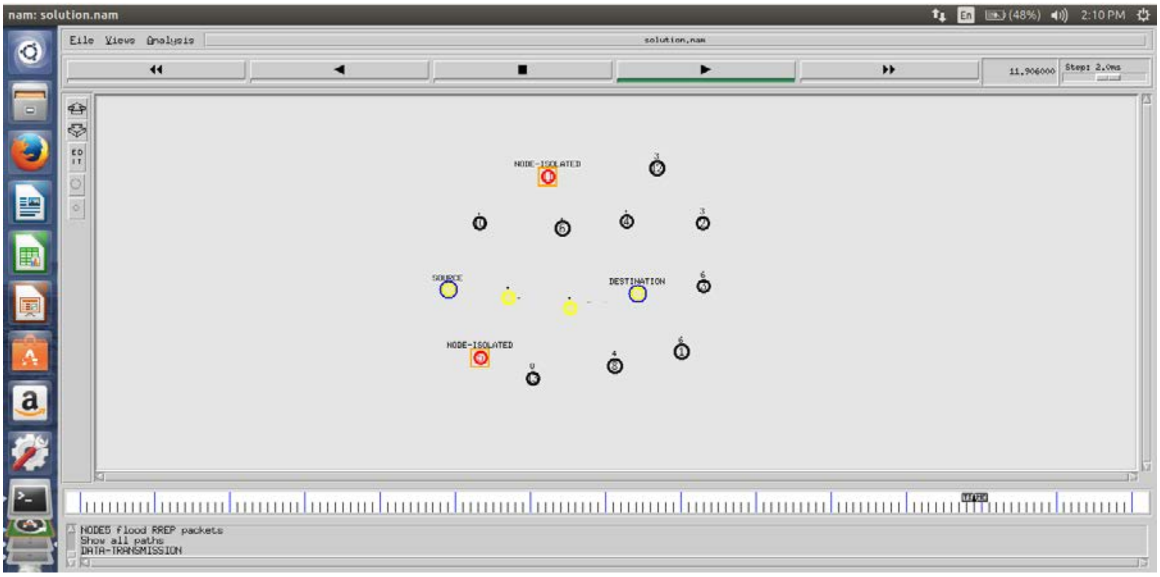
```
NODE0 flood RREQ packets
NODE5 flood RREP packets
Show all paths
```

Figure 24: Source node start normal route discovery process



```
NODE0 flood RREQ packets
NODE5 flood RREP packets
Show all paths
```

Figure 25: Nodes having route to destination sends RREP packet



```
NODE5 flood RREP packets
Show all paths
DATA-TRANSMISSION
```

Figure 26: Shortest path is selected to transmit data

Figure 26 shows that upon receiving the route request packet, all the immediate nodes having route to the destination send route reply packet to the source which initiated the route request. The source node upon receiving these route reply packets calculates the hop count, sequence number and select the best path to the destination.

4.3 Result Analysis

The graphs are used to signify the variation in throughput, packet loss and end-to-end delay using the proposed method. Green line characterizes the change in case of the new scenario and red colour represents the conventional method. These two parameters are a widely used for validating and confirming the use of particular methods. Throughput can be defined as the number of packet data received per unit time whereas end-to-end delay defined as the time taken between sending of a packet and it's receiving on the destination. Figure 27 shows the change in end-to end delay after deployment of the proposed method. It shows that the proposed method reduces end-to-end delay while packet is going to transmit from source to destination. In the previous schema, the delay starts linearly increasing when there is presence of malicious node in the path mark as red line whereas in absence of malicious node delay first decrease but the new path deploy because of malicious activity it will be not as much shortest then previous so at some point of time the peak of the graph increase and decrease because of delay which mark as green line in graph.

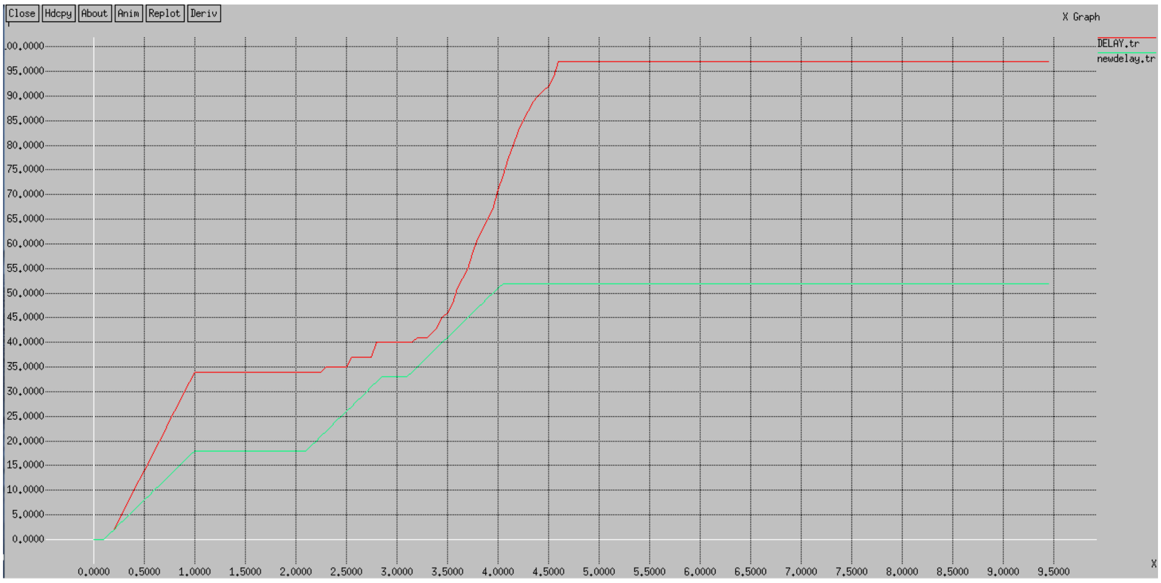


Figure 27: End to End delay graph

Figure 28 represents the network throughput after applying proposed method. As delay in the network is minimum because of isolation of malicious node, so throughput of the network is linearly increased after some pint of time. From graph we can see that when number of packet increase throughput is gradually increase with time in our proposed schema shown by green line. While red line represents previous schema when the malicious node present in the network at that time packet continuous drop so the line is constant for some period of time.

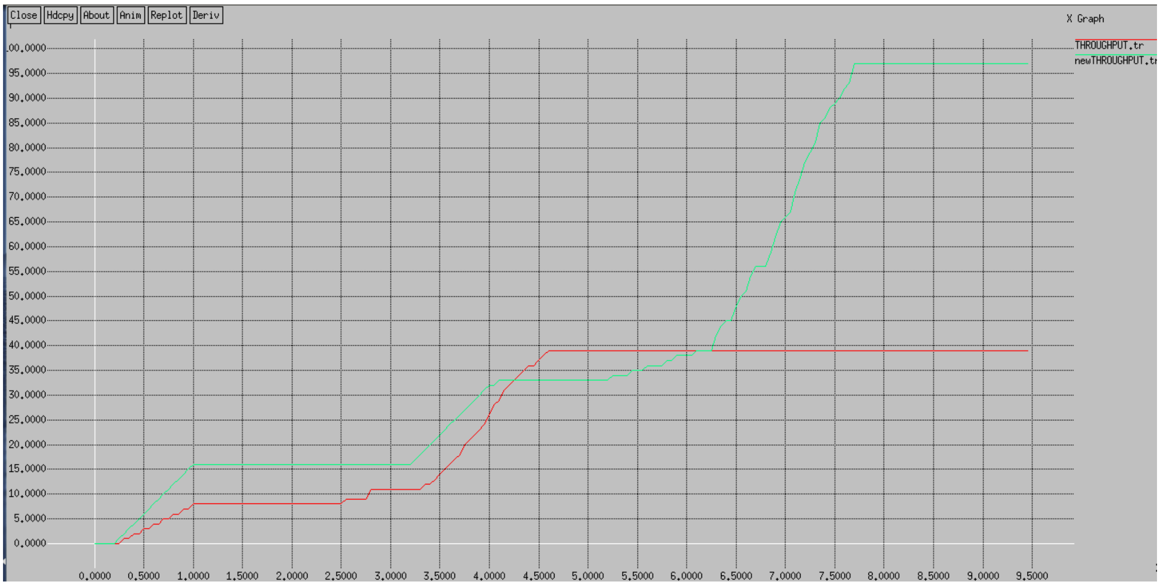


Figure 28: Throughput Graph

As we have applied the proposed algorithm for setting up the path then packet loss is less as compared to the previous scenario. We make the channel secure so final result comes is maximization of throughput and minimization of packet loss. In previous schema malicious node continuously dropping the packet so final output is major loss of packet. In Figure 29 we see that the red line is continuously increase because of dropping of the packet and green line constant after some time because of securing of channel.

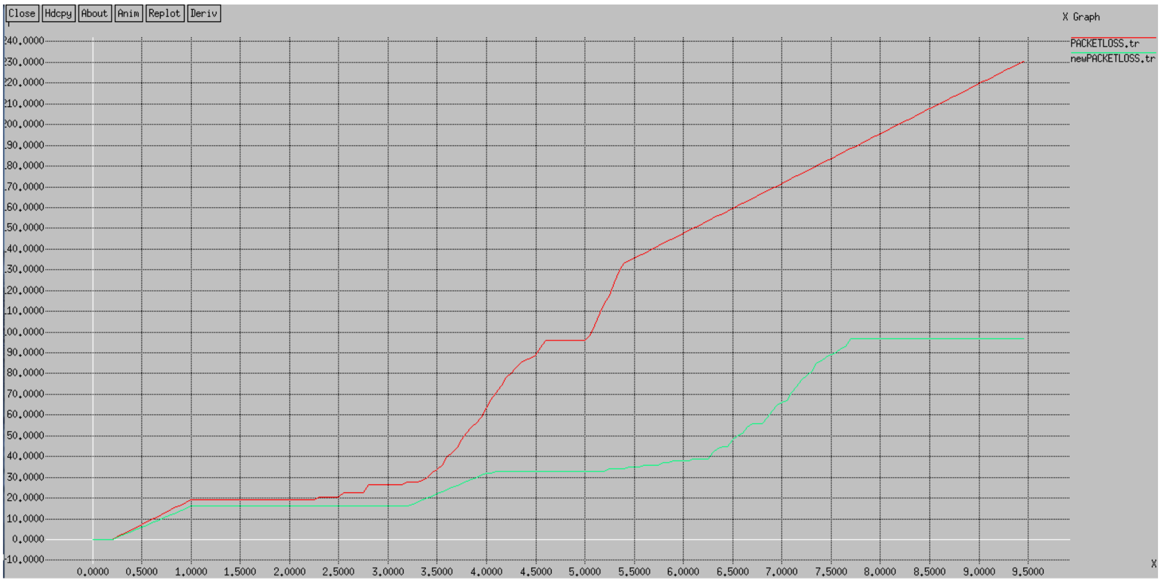


Figure 29: Packet Loss Graph

Chapter 5
Conclusion & Future Scope

As MANET being infrastructure less it can be deployed with fewer efforts as compared with the traditional network infrastructure environment. It has a lot of potential but still there are some issues to overcome. One of the popular research areas nowadays is security in MANET and in our thesis we are addressing security issues in one of the reactive routing protocol (AODV) in MANET.

In earlier research conducted, solutions introduced are lacking in terms of effectiveness or efficiency. If any proposed algorithm works in presence of a black hole attack then there are chances that it will not work under multiple black hole attack. The algorithm proposed by us can work effectively & efficiently in both the scenarios of a single as well as multiple black hole attack. Our future task will be to develop an algorithm which is capable in detecting the above mentioned attacks as well as collaborative black hole attacks in which nodes act in coordination with each other and are successful in evading detection.

Chapter 6
REFERENCES

Research Papers

[1] Latha Tamilselvan and V Sankaranarayanan "Prevention of Co-operative Black Hole Attack in MANET", JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008.

[2] Mohammad Al-Shurman and Seong-Moo Yoo "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE'04, April 2-3, 2004.

[3] Priyanka Goyal, Vinti Parmar and Rahul Rishi3 "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[4] Durgesh Wadbude and Vineet Richariya "An Efficient Secure AODV Routing Protocol in MANET", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012

[5] Rajib Das, Bipul Syam Purkayastha and Prodipto Das "Security Measures for Black Hole Attack in MANET: An Approach".

[6] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".

[7] Yibeltal Fantahun Alem and Zhao Cheng Xuan "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", 2010 2nd International Conference on Future Computer and Communication.

[8] Jaydip Sen, Sripad Koilakonda and Arijit Ukil "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks"

[9] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao "A survey of black hole attacks in wireless mobile ad hoc networks", Computing and Information Sciences 2011.

[10] Kitisak Osathanunkul and Ning Zhang "A Countermeasure to Black Hole Attacks in Mobile Ad hoc Networks", 2011 International Conference on Networking, Sensing and Control Delft, the Netherlands, 11-13 April 2011

[11] Songbai Lu, Longxuan Li, Kwok-Yan Lam and Lingyan Jia "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", 2009 International Conference on Computational Intelligence and Security.

[12] Sheenu Sharma, Roopam Gupta "SIMULATION STUDY OF BLACKHOLE ATTACK IN THE MOBILE AD HOC NETWORKS", Journal of Engineering Science and Technology Vol. 4, No. 2 (2009) 243 – 250

[13] S.Sankara Narayanan and S.Radhakrishnan , "Secure AODV to Combat Black Hole Attack in MANET" , 2013 International Conference on Recent Trends in Information Technology (ICRTIT)

Chapter 7
APPENDIX

MANET	Mobile Ad-hoc Network
AODV	Ad-hoc On Demand Distance Vector
RREQ	Route Request
RREP	Route Reply
DRI	Data Routing Information
DOS	Denial of Service
DSDV	Destination Sequence Distance Vector
OLSR	Optimized Link State Routing
DSR	Dynamic Source Routing
ZRP	Zone Routing Protocol
RERR	Route Error
FRq	Forward Route Request
FRp	Forward Route Reply
FRREQ	Fake Route Request
FRREP	Fake Route Reply
MAC	Media Access Control
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
CBR	Constant Bit Rate