# ENERGY EFFICIENT STEP VERIFICATION FOR DETECTION OF BLACK HOLE ATTACK IN MANET

*Dissertation submitted in fulfilment of the requirements for the Degree of*

**MASTER OF TECHNOLOGY**

**in**

**COMPUTER SCIENCE AND ENGINEERING**


By

**BALJINDER SINGH**

**11402722**

Supervisor

**MR. MANMOHAN SHARMA**




**School of Computer Science and Engineering**

Lovely Professional University

Phagwara, Punjab (India)


December 2016

December 2016

# PAC FORM

LOVELY PROFESSIONAL UNIVERSITY
Transforming Education, Transforming India

**TOPIC APPROVAL PERFORMA**

School of Computer Science and Engineering

**Program :** 1703::M. Tech - IT (Information Technology) (Full Time)

**COURSE CODE :** INT546 **REGULAR/BACKLOG :** Backlog **GROUP NUMBER :** CSEBGD0333

**Supervisor Name :** Manmohan Sharma **UID :** 16073 **Designation :** Assistant Professor

**Qualification :** M.Tech (CSE) **Research Experience :** 9 YEARS

| SR.NO. | NAME OF STUDENT | REGISTRATION NO | BATCH | SECTION | CONTACT NUMBER |
|---|---|---|---|---|---|
| 1 | Baljinder Singh | 11402722 | 2014 | BLI87 | 09872205068 |

**SPECIALIZATION AREA :** Networking and Security **Supervisor Signature:**

**PROPOSED TOPIC :** Energy Efficient algorithm for Detection of Black hole attack in MANET

| Qualitative Assessment of Proposed Topic by PAC | | |
|---|---|---|
| **Sr.No.** | **Parameter** | **Rating (out of 10)** |
| 1 | Project Novelty: Potential of the project to create new knowledge | 6.25 |
| 2 | Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students. | 7.00 |
| 3 | Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program. | 6.75 |
| 4 | Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills. | 7.00 |
| 5 | Social Applicability: Project work intends to solve a practical problem. | 6.25 |
| 6 | Future Scope: Project has potential to become basis of future research work, publication or patent. | 6.50 |

| *PAC Committee Members* | | |
|---|---|---|
| PAC Member 1 Name: Prateek Agrawal | UID: 13714 | Recommended (Y/N): Yes |
| PAC Member 2 Name: Pushpendra Kumar Pateriya | UID: 14623 | Recommended (Y/N): Yes |
| PAC Member 3 Name: Deepak Prashar | UID: 13897 | Recommended (Y/N): Yes |
| PAC Member 4 Name: Kewal Krishan | UID: 11179 | Recommended (Y/N): Yes |
| PAC Member 5 Name: Dr. Ashish Kumar | UID: 19584 | Recommended (Y/N): NA |
| DAA Nominee Name: Kanwar Preet Singh | UID: 15367 | Recommended (Y/N): NA |

**Final Topic Approved by PAC:** **Energy Efficient algorithm for Detection of Black hole attack in MANET( Remarks: There are four *students who have listed the same topic. So be particular while pursuing the same.)***

**Overall Remarks:** Approved (with minor changes)

**PAC CHAIRPERSON Name:** 11011::Rajeev Sobti **Approval Date:** 26 Oct 2016

11/25/2016 1:07:24 PM

# ABSTRACT

MANET is a one of the most promising and rapidly growing field for research and development of wireless network which is based on a self organized and rapidly deployed network. As the mobile devices and wireless networks significantly becoming more popular and increase over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. In this dissertation report discuss about the Mobile ad hoc network (MANET), challenges facing, and communication of types, communication types, mobile movement, routing protocols, and attacks in MANET. Study various research papers and from that find out the problem which is related to security and energy efficiency in MANET. Due to characteristics of MANET like dynamic network topology and mobility in nodes various attacks are possible. Black hole attack is most occurring attack in MANET, in this a malicious node act as good node show having shortest path to the destination and when route is defined than it starts dropping the packets. So we overcome this attack using an enhanced security algorithm using the Step Verification of Detection Black Hole attack with energy efficiency in MANET.

# DECLARATION STATEMENT

I hereby declare that the research work reported in the dissertation entitled **"ENERGY EFFICIENT STEP VERIFICATION FOR DETECTION OF BLACK HOLE ATTACK IN MANET"** in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor **Mr. Manmohan Sharma**. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

*Signature of Candidate*

**Baljinder Singh**

**11402722**

# SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation entitled "**Energy Efficient Step Verification For Detection of Black Hole Attack In MANET"**, submitted by **Baljinder Singh** at **Lovely Professional University, Phagwara, India** is a bonafide record of his original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor

Manmohan Sharma

**Date:**

**Counter Signed by:**

1) **HoD's Signature:** _____

   HoD Name: _____

   Date: _____

2) **Neutral Examiners:**

   **(i) Examiner 1**

   Signature: _____

   Name: _____

   Date: _____

   **(ii) Examiner 2**

   Signature: _____

   Name: _____

   Date: _____

# ACKNOWLEDGEMENT

I would like to express my deepest gratitude towards my mentor **Mr. Manmohan Sharma** for providing excellent guidance, advice, encouragement, supervision and inspiration throughout the development of this dissertation study. I would like to thank to the **Project Approval Committee members** for their valuable comments and discussions. I would also like to thank to **Lovely Professional University** for the support on academic studies and letting me involve in this study.

And last but not least, I find no words to acknowledge the moral support rendered by my parents and friends. All this has become reality because of their blessings and above all by the grace of **GOD.**

**BALJINDER SINGH**

**(11402722)**

# TABLE OF CONTENTS

# LIST OF FIGURES

**FIGURE NO. FIGURE DESCRIPTION PAGE NO.**

# LIST OF TABLES

**TABLE NO.** **TABLE DESCRIPTION** **PAGE NO.**

# CHAPTER 1
# INTRODUCTION

Wireless network invoke to the type of networks in which the communication between devices is implemented without use of wires. Radio wave and microwaves are used for communication in the wireless network and it eliminates the cost of wires. It is necessary that, both devices/mobile nodes that are communicating to each other, they remain within the radio range of each other. The IEEE standard 802.11 [1][2] is used for wireless network. Wireless networks have many characteristics like easy setup, mobility, productivity, security and economic and cost saving installation. Wireless networks can be classifies into two types:

- Infrastructure network
- Ad-hoc network

**Infrastructure network:** Infrastructure network has center administrator which is known as Access Point (AP). All the wireless devices such as laptops, mobile phones are connected with each other through Access point.

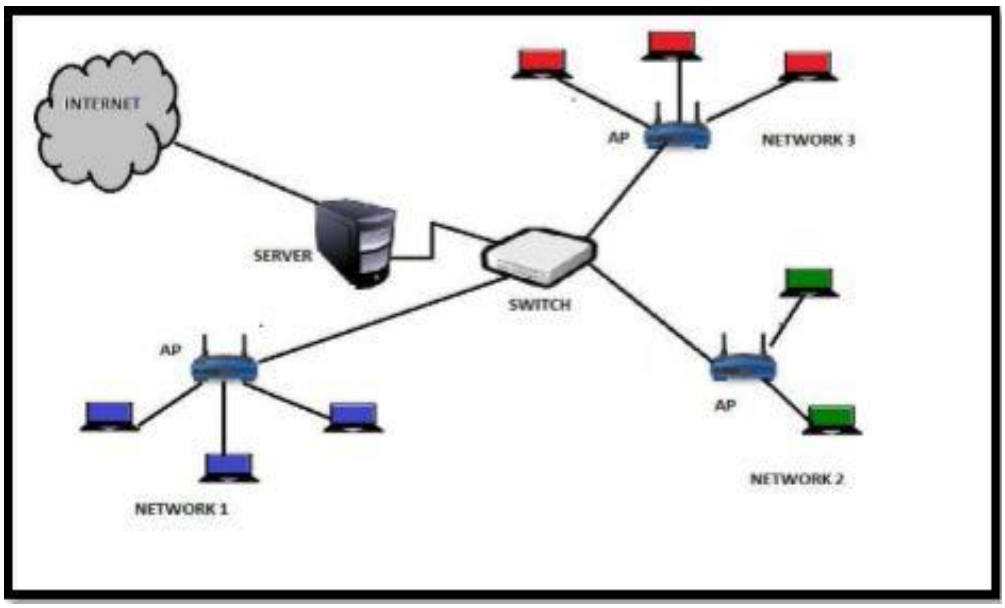


**Figure 1.1**- Infrastructure network

Access point is also responsible for data routing means if one node wants to send the data to other node, that information is routed through the access points. In infrastructure network, fixed base station is there which is called access points and all wireless devices that are communicating with other wireless devices are connected to access point. In figure 1.1 shows the three access points are used and wireless devices are connected to that access points and these devices are communicating to each other by using Access point.

**Ad hoc networks: [1][2]** Ad-hoc network is also known as infrastructure less network, in this type of networks, there is no central coordinator means no Access point. When node is entered in the ad-hoc network to forwarding the data to the destination, and then the decision of the nodes to forwarding the data is made at run time execution is completely based upon the network connectivity. It is a network which is used for emergency purpose. In ad hoc wireless network there is no fixed infrastructure or base station. When the mobile nodes in the range of each other then nodes can communicate directly on the other side nodes when the nodes are not in the range of each other then nodes can communicate indirectly means with the help of intermediate nodes. Figure 1.2 shows the example of ad hoc wireless networks. In this various nodes are communicating with each other directly without any Access points.

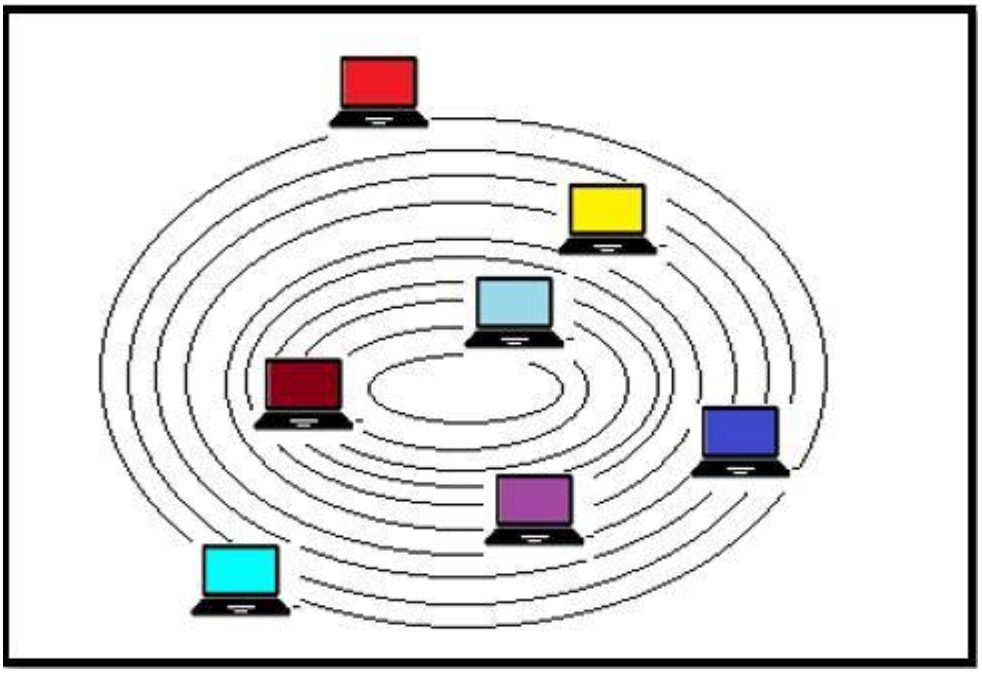

**Figure 1.2-** Ad-hoc network

## 1.1 MOBILE AD HOC NETWORK (MANET)

A Mobile Ad hoc Network (MANET) [1][2][3][4[5][11] is a collection of wireless mobile nodes which make a temporary network without the usage of an established infrastructure or centralized administration. In this type of network, every device actively participates in data forwarding and work like a router. Communication between two nodes performed via radio links. It can be performed directly if the destination is within the sender's transmission range, or through intermediate nodes acting as routers (multi-hop transmission) if the destination is outside sender's transmission range.

There may be several areas where users of a network cannot rely on an infrastructure, it is too expensive, or infrastructure may not be present in a disaster area or war zone, in these situations mobile ad-hoc networks are the only choice. The ad-hoc setting up of a connection with an infrastructure is not the main issue here. These networks should be mobile and -use wireless communications.

MANET is basically a continuously self-configuring, infrastructure-less network of mobile devices connected with each through wireless system. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently.

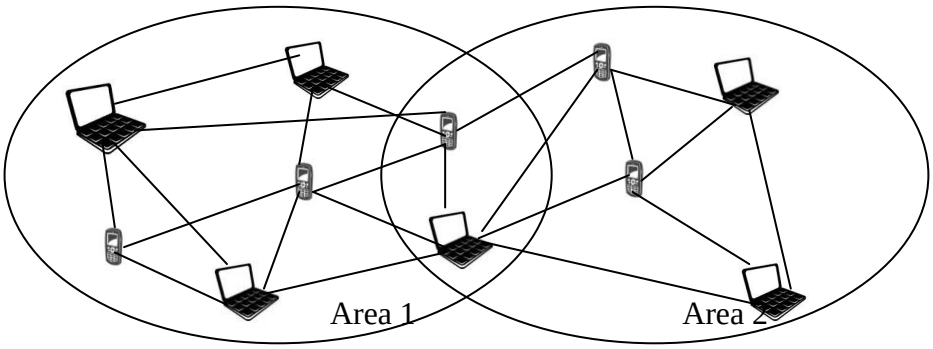


**Figure 1.3-** Mobile ad-hoc network

Each must forward traffic unrelated to its own use, and therefore be a router. The main challenge in building a MANET is each device easily equips the changes which continuously maintain the information required to properly route traffic. Such kind of networks may operate by themselves which means transmission of the information within that private network or may be connected to the larger Internet. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network in contrast to a mesh network has a central controller to determine, optimize, and distribute the routing table.

## 1.2 HISTORY OF AD-HOC NETWORK [1][2][3]

The process of Ad-hoc network is mainly divided into three generations first, second and third generation. Third generation is used by most peoples in present time. In 1970, the first generation, PARNET (Packet Radio Network) was used in the battle environment on a test basis for providing the different network functions. In 1980, the second generation of ad-hoc network is come forward, implements the network system as a part of SURAN (Survivable Adaptive Radio Network) program and further enhancements by using packet switched network to the mobile battlefields. In 1993, the third generation of ad-hoc network is based on the radio waves concept. Bluetooth and ad-hoc sensor are the main examples of third generation ad-hoc network. The network is mainly divided into two categories- infrastructure based and infrastructure less network, in the infrastructure based the fixed and wired gateways and routers and in case of infrastructure less networks does not exist any type of fixed and wired gateways.

## 1.3 TYPES OF MANET [3][5]

- **Vehicular Ad-hoc Network (VANET).** VANET is referring as a type of mobile ad-hoc system, in this network vehicles are provided with wireless equipments and infrastructure less structure of the system. The implementation of hardware in vehicles for finding the position of vehicles and giving the access to other vehicles to communicate with that system.
- **Intelligent Vehicular Ad-hoc Network (InVANET).** InVANET is use the IEEE 802.11 and WiMax IEEE 802.16 for the communication. The main goal of

implementation of InVANET is to evade vehicle crash and safe the peoples. It also helpful for the drivers, they know about the speed of other vehicles by using InVANET.

- **Internet Based Mobile Ad-hoc Network (IMANET).** In IMANET the mobile phones are connected with the internet to provide the universal data.

## 1.4 FEATURES OF MANET [3][5][7][8]

- **Autonomous terminal**: In the MANET every mobile node is an autonomous node means that any node in network behaves like a host and router. The node which is part of the network sends the requests to other nodes and receives the request and transfer that requests.

- **Distributed operation:** There is no device for the central control the operations of the network, the control and management of the network is distributed among the terminals. The nodes present in a MANET should collaborate to perform the security and routing.

- **Dynamic network topology**: The topology of the network may change time to time and the connectivity among the nodes may be lost. The nodes in the MANET dynamically establish routing among themselves as they move. A user in the MANET may not only operate within the ad hoc network, but may require access to a public fixed network.

- **Multi-hop routing:** Routing algorithms in ad-hoc network can be classified as single-hop and multi-hop. Single-hop routing is easy than multi hopped routing in terms of implementation and the structure of the network. The cost of working and applicability of the services is less as compared to multi-hop. When data is delivering from a source to destination out of the direct wireless transmission range, the packets should have been forwarded via one or more intermediate nodes.

- **Fluctuating link capacity:** The link between source and destination can be shared by other nodes so over the channel fading, interference and noise are occurred. The path between any two users can traverse multiple wireless links and the link themselves can be heterogeneous.

- **Limited physical security**: MANETs are generally more easy to physical security attacks than are fixed cable networks. The increased possibility of attacks likes eavesdropping, and denial-of-service attacks and spoofing should be carefully considered.

- **Energy-constrained operation:** The mobile nodes in a MANET may rely on batteries or other means for their energy. The devices in the MANET need mechanisms and optimized algorithms that implement the communicating functions.

## 1.5 MANET CHALLENGES [3][5][7][8]

- **Limited bandwidth:** Wireless link continue to have significantly lower capacity than infrastructure networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.
- **Dynamic topology:** Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.
- **Routing Overhead:** In wireless ad hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.
- **Hidden terminal problem:** The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.
- **Packet losses due to transmission errors:** Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, unidirectional links, and frequent path breaks due to mobility of nodes.
- **Mobility-induced route changes**: The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going

session suffers frequent path breaks. This situation often leads to frequent route changes.

- **Battery constraints:** Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.
- **Security threats**: The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.

## 1.6 MANET APPLICATIONS [1][2][3][5][8]

- **Military battlefield:** Ad-Hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information head quarter.
- **Collaborative work:** For some business environments, the need for collaborative computing might be more important outside office environments than inside and where people do need to have outside meetings to cooperate and exchange information on a given project.
- **Local level:** Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at a e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.
- **Personal area network and Bluetooth:** A personal area network is a short range, localized network where nodes are usually associated with a given person. Short-range MANET such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop, and a mobile phone.
- **Commercial Sector:** Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed.

## 1.7 MANET VULNERABILITIES [1][2][3][5][7]

Vulnerability means weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:

- **Lack of centralized management:** MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad hoc network.
- **No predefined Boundary:** In MANET we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node.
- **Cooperativeness:** Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation.
- **Limited power supply:** The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.
- **Adversary inside the Network:** The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the external attack.

## 1.8 SECURITY GOALS [1][2][4]

- **Availability:** Availability means the resources or data are accessible to authorized parties at that times when they need. Availability ensure the survivability of the network against the DOS attack, it applies both to data and to services.
- **Confidentiality:** Confidentiality ensures that information or computer-related assets are accessed only by authorized parties. The information which is

exchanging over the MANET should be protected from the any disclosure attack like eavesdropping and unauthorized reading of messages.

- **Integrity:** Integrity ensures that data can be modified only by authorized parties or only in authorized way. Integrity means that a message which is transferred should not be corrupted.
- **Authentication:** Authentication means that participants in the network or communication are authenticated. There are no impersonators are present in the network who can change our data using authenticate person's identity.
- **Authorization**: Authorization means assigns the different access rights to the different types of users. For e.g. a network management can be performed by network administrator only.

## 1.9 ADVANTAGES AND DISADVANTAGES OF MANET [1][2]

### 1.9.1 ADVANTAGES

1. In emergency situations like earthquake area, disaster area mobile ad-hoc network is very useful.
2. MANET is very useful to provide the real time information to the mobile users.
3. MANET has various applications in education, entertainment and other fields like battlefield etc.
4. MANET has less cost as compared to wireless network or wired network.

### 1.9.2 DISADVANTAGES

1. Mobile nodes in the MANET have very less energy resources like battery power.
2. Mobile nodes change its positions time to time so the communication between them is interrupted.

## 1.10 ATTACKS ON MANET [1][2][4][9][10]

MANET is an open network, which is easy to attack as compared to wireless or wired network. Securing the MANET is not easy task, firstly to develop the solution for attack we need to discuss the types of attacks in MANET.

### 1.10.1 Attacks on the Basis of behavior: [7][8]

- **Active attack:** Active attacks are those attacks in which attacker or intruder do some modification or alter or change the original data or information flows between the nodes. Figure 1.4 shows that when one is send the data to other node then attacker steal that information and change it then send to the other node.

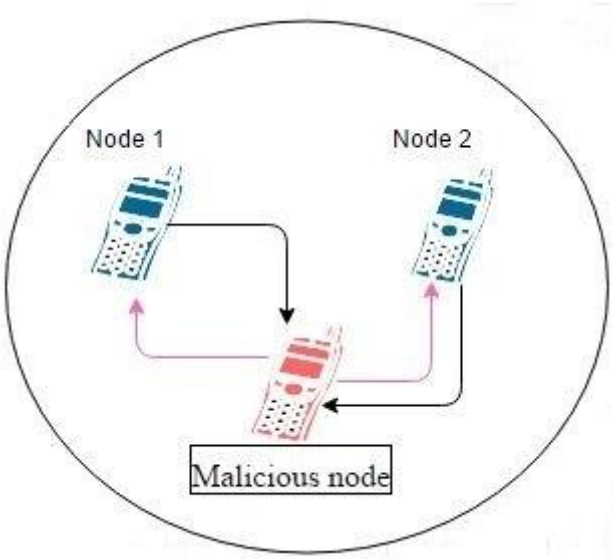


**Figure 1.4-** Active attack

- **Passive attack:** Passive attacks are those attacks in which attacker or intruder can only listen the communication without doing any type of modification. A passive attacker does not affect the operations of routing protocol in MANET. Figure 1.5 shows that a malicious node just analyzes the traffic between nodes.

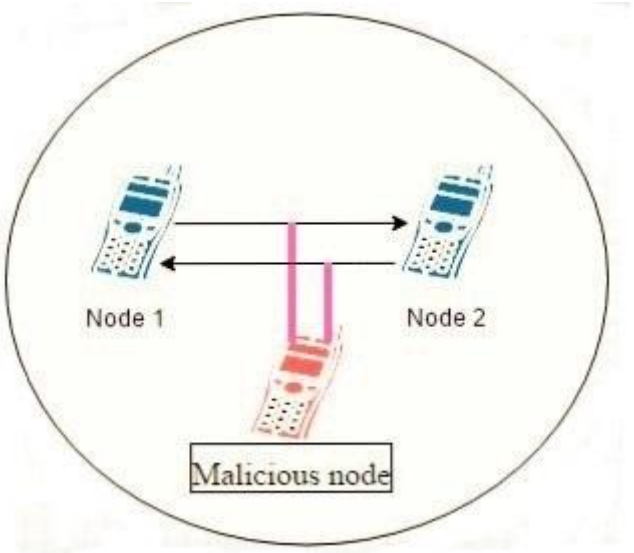


**Figure 1.5-** Passive attack

### 1.10.2 Attacks on the basis of source: [7][8]

- **Internal attack:** When the active attack is done by attacker from the same network is called internal attack. Attacker can be a malicious node which is the part of the network.

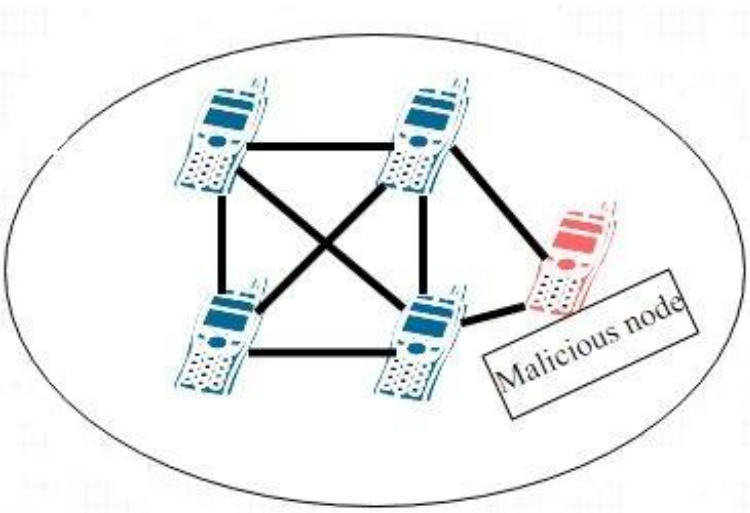


**Figure 1.6-** Internal attack

- **External attack:** In external attack, attack is performed by attacker for outside the network. The attack cannot be a part of the network but tries to access the information or data.

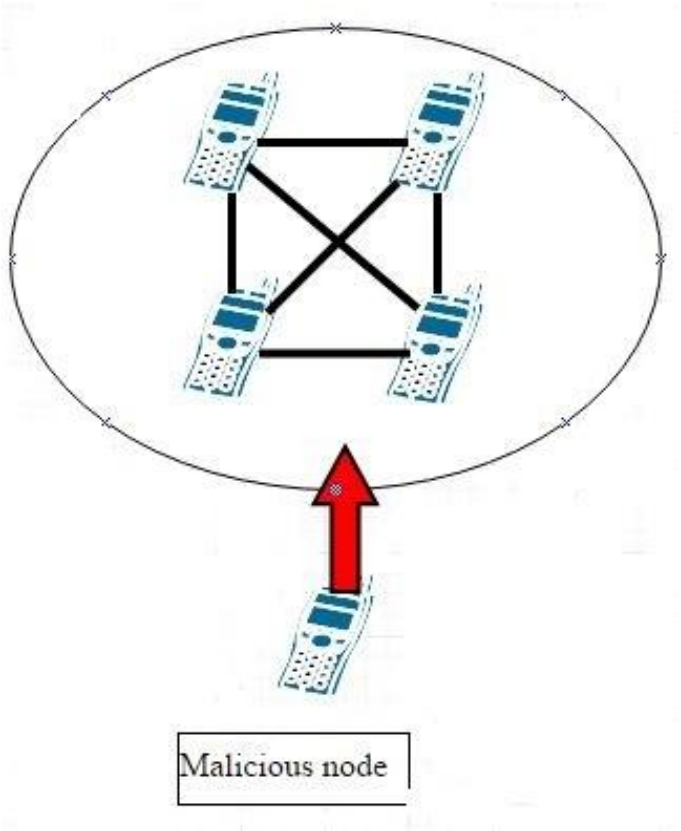


**Figure 1.7-** External attack

## 1.11 BLACK HOLE ATTACK [1][2][9][10][11]

Black hole is one major security attack in MANET in which a malicious node or group of malicious nodes behaves like a node which has shortest path to reach the destination. In MANET, when sender wants to send the data to receiver then sender node sends the RREQ to the neighbors. The neighbor node which has a path to reach the destination sends the RREP back to the sender. This node can be a malicious node, after receiving the data packets that node drops all the packets.

Types of black hole attack:

1. Single black hole attack and Cooperative black hole attack.
2. Internal black hole attack and external black hole attack.

### 1.11.1 Single black hole attack and Cooperative black hole attack:

- **Single black hole attack:** When one attack act as malicious node in the whole network is called single black hole attack. The complete scenario of black hole attack is shown in figure 1.8.

Here node A is sender node and node G is a receiver node. Node A wishes to send the data to node G. Firstly node A will send the route request to all the neighbors means node B, M, D and wait for the reply. Now neighbor nodes of A broadcast the route request message to all the neighbors and by doing this route request reach to destination node G. One node M is a malicious node and reply back to the sender node with route reply message. In that message node M tells the sender that has a shortest path to reach the destination and sender node A trust that node. Now sender node sends all the packets or data to node M and M just all the packets.

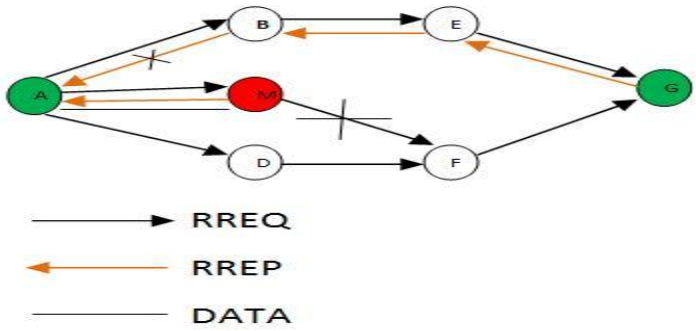


**Figure 1.8-** Single black hole attack

- **Cooperative black hole attack:** In cooperative black hole two or more nodes from the network act as malicious nodes and with the help of each other perform the black hole attack. In figure 1.9 when node M receives the route request and reply back to the sender node A with route reply message. Now sender node doing the confirmation forms the next node after the node M and node D reply with yes. Now sender sends the packets to node M and that will drop all the packets.

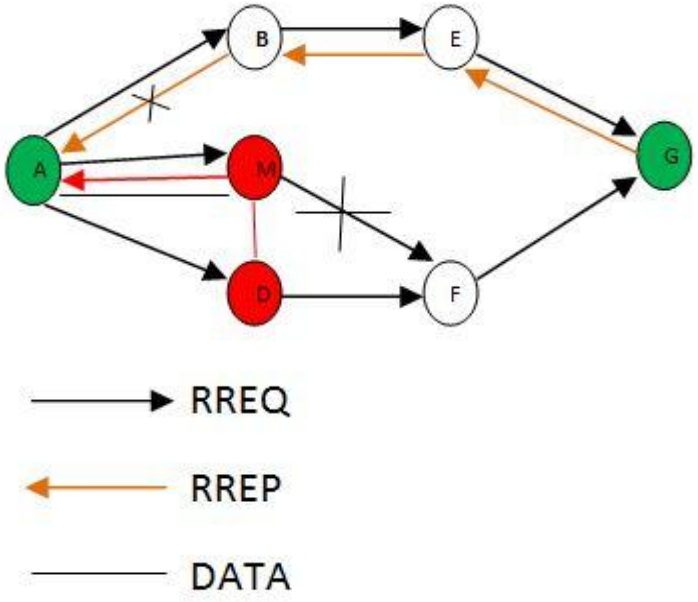


**Figure 1.9-** Cooperative black hole attack

### 1.11.2 Internal black hole attack and external black hole attack:

- **Internal black hole attack:** This is a type of attack in which malicious node is present in the network and perform the attack. When the packets are transmitted through it then it decides that whether to drop or send the packets. It is not easy to detect as compared to external black hole attack.
- **External black hole attack:** When the malicious node is present outside the network is called external black hole attack. The malicious node is not a part of the network it just creates the disturbance in the network.

## 1.12 Others types of attacks: [1][2][7][8][10]

### 1.12.1 GREY HOLE ATTACK

Grey hole attack is a type of active attack in MANET in which a malicious node misguide the sender node by accepting the request to send the message in the network. In the starting, an attacker sends the RREQ to the sender node but the moment the malicious node receives that message and implement the DOS attack.

### 1.12.2 FLOODING ATTACK

In the flooding attack network is flooded with the packets. These packets can be data packet or RREQ packets. In RREQ packet flooding, an attacker filled the network with RREQ packets by choosing an IP address which has no existence in the network and in data packet flooding, an attacker enters the network and establish path with all other nodes within the network.

### 1.12.3 DOS ATTACK

In DOS attack, an attacker sends the excessive messages to the server or in the network to reject authenticate user's access from the resources or server.

### 1.12.4 IMPERSONATION ATTACK

Impersonation attack is another major attack in MANET in which attacker node use the identity of authenticate node and send the data to all other nodes.

## 1.13 ROUTING IN MANET [1][2][4][9]

Routing in MANET is very different from other networks like wireless network. Routing in the MANET is depends on some factors like route request, route reply and topology. In MANET every node act like router, every node can send the data or receive the data without using of any router. Multi-hop routing is used in MANET for communication between nodes which are not in direct transmission range. If the nodes are in direst transmission range, then no need of multi-hop routing. All the routing protocol must be in such a way that the path from source to destination found.

**Table 1.1-** Comparison between various ad-hoc routing protocols

| Parameters | AODV | DSR | DSDV | TORA | ZRP | CBRP |
|---|---|---|---|---|---|---|
| Loop free | Yes | Yes | Yes | No | Yes | Yes |
| Reactive | Yes | Yes | No | Yes | Partially | Yes |
| Proactive | No | No | Yes | No | No | No |
| Multiple-routes | No | Yes | No | Yes | No | Yes |
| Distributed | Yes | Yes | Yes | Yes | Yes | Yes |
| Unidirectional link support | No | Yes | No | No | No | Yes |
| QOS support | No | No | No | No | No | No |
| Multicast | Yes | No | No | No | No | No |
| Security | No | No | No | No | No | No |
| Power conservation | No | No | No | No | No | No |
| Periodic broadcast | Yes | No | Yes | Yes | Yes | Yes |
| Require rel. & seq. data | No | No | No | Yes | No | No |

### 1.13.1 Properties of ad-hoc routing protocols: [1][2][12]

- **Distributed operation:** Ad-hoc routing protocols should be distributed means it should not be dependent on ant centralized controller device. The dissimilarity is that in ad-hoc network a node can leave or join the network at any time.
- **Loop free:** Ad-hoc routing protocols should be loop free in order to improve the overall performance of the network.
- **Demand based operation:** Demand based means protocol should be used only when it needed to decrease the control overhead means protocol should be reactive in a nature.

- **Security:** In ad-hoc network communication is happen with the help of radio waves, so it is more vulnerable to attacks as compared to others. So we want the well secured routing protocols to secure the communication.
- **Multiple routes:** In order to decrease the congestion and number of reaction to topological changes multiple routes can be used. If one route is invalid then another route is present for the communication.
- **Power conservation:** The device or node in the ad-hoc network can be a laptop or mobile phone which has a smallest energy as compared to other devices. It is very important the routing protocols should use less energy for the communication.
- **QOS support:** Some types of quality of service is necessary to add into the routing protocols.

## 1.14 CLASSIFICATION OF ROUTING PROTOCOLS IN MANET [1][2][6][12]

Ad-hoc routing protocols can be classified in three types:

### 1.14.1 PROACTIVE ROUTING PROTOCOLS [1][2][4]

Proactive routing protocols are known as table driven protocols; these types of protocols are based on the periodic exchange of control messages and update routing tables. Every node in the network maintained some routing tables before starting the communication with other nodes. There are so many number of messages exchanged so that overhead in the network is increased. Some examples of proactive routing protocols are: DSDV, WRP, and CGSR.

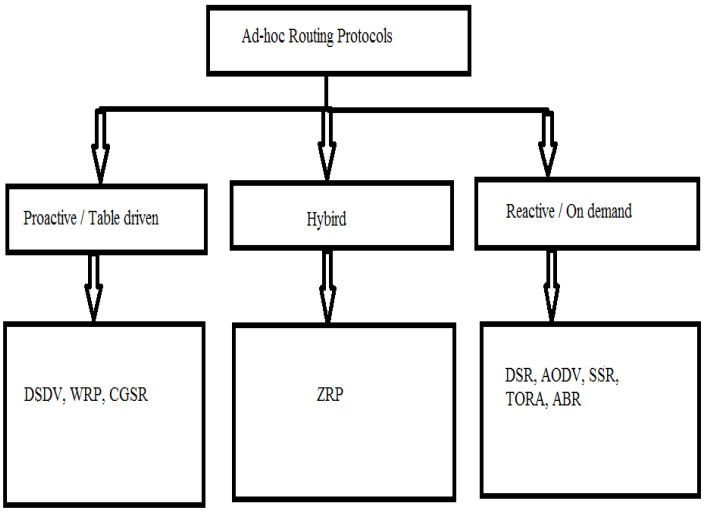


**Figure 1.10-** Ad-hoc routing protocols

- **DSDV:** DSDV is a proactive routing protocol which is completely loop free. In DSDV only single path is present for the destination, which is selected by using the distance vector shortest path routing protocol. Two types of update packets are used: full dump and incremental.
- **WRP:** WRP is another proactive routing protocol which is also loop free with the help of predecessor information. In WRP, each node needs to keep four routing tables and due to this overhead will increase.
- **CGSR:** In CGSR, nodes are collected into some particular area which is called cluster. In each cluster, there is one cluster head which is responsible for the communication.

### 1.14.2 REACTIVE ROUTING PROTOCOLS [1][2][4]

Reactive routing protocols are also known as on demand routing protocols. In the reactive protocols the route between sources to destination is established on the basis of on demand. The routes are created only when the sender sends the route request to the neighbors. The reactive routing protocols are source initiated protocol. Some examples of on demand routing protocols are: DSR, AODV, TORA and ABR.

- **DSR:** Dynamic Source Routing is a reactive routing protocol; in this each packet needs to carry the full address from source to receiver. For large network DSR is not good protocol because of overhead.

- **AODV: [9]** AODV is an on demand routing protocol formed by the combination of DSDV and DSR. From DSDV, it picks the concept of peer to peer routing and sequence number while from DSR its uses the process of route discovery and route maintenance. In contrast to proactive protocols, it creates the route only when required instead of creating a route table beforehand as in DSDV. The whole transmission process in AODV is divided into two stages:
  1. Finding and maintaining the routes
  2. Forwarding data through discovered routes.

To find routes in AODV [13], there are three messages named below which are used.

**i. Route Request Message (RREQ)**

**ii. Route Reply Message (RREP)**

**iii. Route Error Message (RERR)**

**1. RREQ**

Whenever a source node wants to send data, it sends a RREQ message to its neighbors and neighboring nodes further transmit that message to their nodes. This process is carried till the destination replies or any intermediate with path towards destination replies. Every RREQ message has fields like hop count, broadcast ID, sequence number, IP address of both destination and source.

**2. RREP**

RREP message is generated when RREQ message reaches destination or any node which is having path to destination. It is replied back to source from same path from which request message reached the node generating RREP, since the nodes receiving request message stores path.

**3. RERR**

Each node in the network keeps a check whether the connection between it and its neighbors is fine or not. If the link is found to broken, then an error message (RERR) is generated to make other nodes know about it.

**Route Discovery Process:**

The process of route discovery starts with the generation of RREQ. As in Figure 1.11, when node 1 wants to communicate with node 7, it will generate a RREQ message and will transmit it to its neighboring nodes: 2 and 4 which will further transmit it to their neighbor and process continues until it reaches destination. Once

RREQ message reaches destination, node 7 will generate RREP and will send it to source and the route between node1 and node 7 will be established.

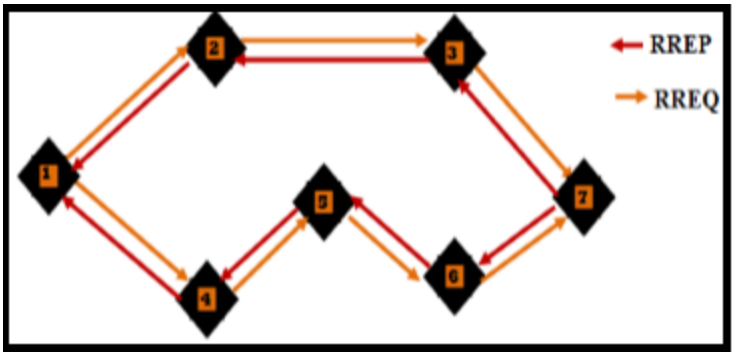


**Figure 1.11-** Route discovery in AODV

If the link between any two nodes which connects node 1 to node 7 breaks, an error message will be generated and sent to node 1 informing that path towards destination no longer exists and new path need to be established

- **TORA:** It is based on LMR protocol which uses the route repair procedure and similar link reversal as in LMR and it also creates the DAG's. TORA reduces the far reaching control message to a set of neighbor nodes.
- **ABR:** Associated based routing protocol uses the query reply scheme to find routes to require destination. In ABR, to select stable route each node has to maintain associativity with their neighbors.

### 1.14.3 HYBRID ROUTING PROTOCOLS [1][2][4]

Hybrid routing protocols in MANET are both the reactive and proactive routing protocols features. The route setup is based on the reactive protocols and overcome the limitations of reactive and proactive routing protocols. ZRP is the example of hybrid routing protocol.

- **ZRP:** Zone Routing Protocol is a hybrid routing protocol, in this each node has to maintain network connectivity. Nodes which are present in routing zone, routes are available for those nodes only. By using ZRP, we decrease the overhead of the network.

# CHAPTER 2
# REVIEW OF LITERATURE

Neha and Manmohan Sharma [13] proposed an algorithm to detect the black hole attack from the mobile ad-hoc network. Black hole attack is done by malicious node or group of nodes, when the malicious node enter into network and fake itself as node had a shortest path to send the data from source to destination. Firstly sender node send the route request to its neighbors and wait for the reply within some time period, if reply back to the sender reached then the two step verification if performed to check that whether the reply from malicious node or not. In the first step check the malicious table and match the id of node which is send the route replies with the malicious table, if it matched then route replies message is discarded. In the second step of the verification sender node ask the next node about the true path to the destination, if the next node verified the path then the sequence number and node id is stored in the RREP table else if node does not verified the path the id and sequence number of that node is stored in malicious table. If the running time is greater than waiting time then select the sequence number from the RREP table. Select the one sequence number from the RREP table and compare with all other. The packet drop value was checked with its limit if it crossed then stored in the malicious table else if select the highest sequence of route reply message for the communication. The performance was increased in terms of less overhead with compare to normal AODV, less end-to-end delay and high packet delivery ration in the proposed technique.

Abbas Afsharfarni and Abbas Karimi [14] described a clustering algorithm using link's weight in order to decrease the energy consumption in MANET. The main aim of this paper is to provide one weight based algorithm; in this algorithm weight is calculated of each node by not only that particular node but also by using neighboring nodes information. The link weight has been defined as connection between two nodes. The proposed algorithm has been divided into three steps. In first step, determines the weight of link between two nodes with the help of neighborhood share, speed of link, energy of link and the number of nodes connected. In the second

step, each node node's weight has been calculated from the link weight. In the third step, cluster head is selected with highest node weight. The result of this algorithm, lifetime of the network has been increased, less energy consumption, reduce the re-formation of clustering and it also compare with LEACH and WCA.

Alka Adlakha, Vasudha Arora [15] described the performance of two reactive protocols, AODV (Ad-hoc On Demand Vector Routing) and DSR (Dynamic Source Routing) on the basis of different parameters like packet delivery ratio, end to end delay, throughput, routing overhead etc. They use the GloMoSim (Global Mobile Information system simulator) for check the performance of these two routing protocols. In the packet delivery ratio, AODV is better than DSR by 5% more. In the end to end delay is very high in DSR almost twice than AODV, in case of throughput, it is better in AODV rather than DSR and in case of routing overhead is less in AODV as compared to DSR.

Alfy Augustine and Manju [16] James described the technique which is very helpful to detect the black hole attack in MANET. The name of technique was watchdog, which was based on the IDS (Intrusion Detection System). Black hole is Denial of service type of attack, in which the malicious node absorbed all the packets which are sent from the sender. In this paper the concept of alarm is used, it means when the malicious node is find then a alarm is generate to the sender node with the help of AODV routing protocol. In this technique detection of misbehavior nodes by monitoring the next neighbor hop's transmission. In this the overhead produced by the packets was compared with the buffer and packet has been removed if packet was matched. When the receiver receives the packet it sends the acknowledgment to the sender. When the black hole attack is performed by any malicious node then throughput, packet delivery was decreased and end-to-end delay was increased. According to the author this technique is very helpful to detect the black hole attack.

Rajib Das, Dr. Bipul Syam Purkayastha and Dr. Prodipto Das [17] proposed an algorithmic approach to focus on analyzing and improving the security of AODV, which is one of the popular routing protocols for MANET. In this research paper the proposed solution is capable for detecting and removing the black hole nodes at the beginning. AODV (Ad Hoc On-Demand Vector Routing) routing protocol is a reactive routing protocol for ad hoc and mobile networks that maintain routes only

between nodes which need to communicate. In this paper, propose an additional route to the intermediate node that replies the RREQ message to check whether the route from the intermediate node to the destination node exists or not. When the source node receives the Further Replay from the next hop, it extracts the check result from the reply packets. If the result is yes, we establish a route to the destination and begin to send out data packets. If the next hop has no route to the inquired intermediate node, but has a route to the destination node, we discard the reply packets from the inquired intermediate node, and use the new route through the next hop to the destination. By applying this solution for black hole attack we are able to identify signals and multiple black hole nodes cooperating with each other and discover secure path from source to destination.

Yonghui Chen, chunfeng zhang, zhiqin liu [18] described the protocol which is helps us in the saving of energy in case of AODV routing protocol. In this paper, firstly consider the density of nodes which are impact the energy consumption and it is not only reduce the energy as well as check the alternative paths and second is effective flooding mechanism which is associated with node stability and residual energy of nodes. They defined that when the intermediate node receive the RREQ (Router Request) and it compare destination address, if it is matched then send RREP (Route Reply), otherwise send RREQ to the neighbors and it also compare the rate of change of neighbors with the threshold value. In this algorithm only those nodes are chosen which are having sufficient energy and good mobility for establishing a path. The performance of this algorithm is better than the AODV and AOMDV in terms of packet delivery ratio, end to end delivery, throughput etc.

Deepika Patil, Nitika Vats Doohan [19] described the novel threshold alarm based preemptive route repair algorithm (TAB-PRRA) for multi-hop local repair in AODV. The problem arises when the communication is going on between two nodes via so many intermediate nodes, if one link is breakdown by any reason then the data will lose. In this algorithm firstly send the hello packet to measure the current status of nodes which are in the specific range of the sender, it contains battery life, TTL value, node mobility field and number of packets relayed all this called strength of a node then define the link broken part. Transmission range of every node was based on four quadrant clock techniques. In this algorithm the strength of node is check alter

every 10 sec, then compare its threshold value with the minimum threshold value means strength, if its greater then it allows for communication otherwise issue the alarm and update the routing table of the nodes. This algorithm was capable to detect pre-emptive link failure and reduce the battery usage

Hwan-Seok Yang, Seung-Jae Yoo [20] proposed an authentication technique which will provide the secure communication between the nodes and increase the reliability of the nodes. Clustering is used in this technique. In which a cluster head is chosen by the confidence level of the nodes available in the network and that cluster head is having certificates and acts as a certificate authority to manage authentication information between the nodes. Multi step authentication technique is used to provide authentication. CA (cluster authority) issues a authentication key to nodes for authentication between them by measuring reliability of the nodes.

Mandeep Singh, Mr.Gagangeet Singh [21] described the study of different cluster head algorithms for MANET which is reduced the energy consumption, increase the security of network and increase the lifetime of the network. Clustering is a method in which we divide the whole network into some parts and maintains the transmission of data among the interacting nodes. All the cluster head is connected to each other for better communication. The selection of cluster head is divided into two methods first is distance constrained selection and second is size constrained selection. Cluster head, cluster gateway and cluster member are the three types of nodes present in the cluster. We select the cluster head on the basis of maximum energy level. In this paper threshold signature is describes in order to secure the cluster based network. They describes the LIC (Lowest ID cluster), in this lowest ID node is select as a cluster head and in the Power awareness load balancing cluster (LBC) algorithm give the variable virtual ID to the nodes. Least cluster change (LCC) algorithm select the cluster node which is having less mobility. Highest connectivity cluster node algorithm select the node which is having more number of nodes connected to it.

Shelbala Solanki, Anand Gadwal [22] described the hybrid security mechanism for MANET using digital signature and RSA. The each node is require to verify its identity for participate in the communication because manet is a infrastructure less network so DOS attack, impersonation and man in the middle

attack can be performed by the attackers. In this algorithm the starting from the route discovery process, sender sends the RREQ to its neighbors and they check for destination id then it segregate into two parts mutable information has information about the intermediate nodes and non mutable information is related with source and data. When the path is found then sender sends the packet along with signature to the destination and encrypts the packet with the help of RSA algorithm. Receiver compare signature if it is matched then accepts the packet otherwise drop the packet. This algorithm maintains the authentication and confidentiality of the packet. Performance was evaluated in terms of packet delivery ratio, throughput and the average latency.

T. Kiran, T. P. Anish [23] described the secure hidden routing in the MANET. They proposed algorithm which is having two phases, in the first phase build the point to point traffic matrices using time slices techniques and derive the end to end matrices with the help of traffic filtering rules. Algorithm always uses the minimum hop count path, and check for the optimal path. Routing algorithm changes the route after some time which is hidden for the attacker. Less delay, hidden traffic pattern, traffic delay less are the basic advantages of this algorithm. They use data communication, attacker model, star, AOMDV, optimum route selection modules for the implementation of this algorithm.

P.SRINIVASAN and K.KAMALAKKANNAN [24] described the method which directly incorporates signal strength and residual battery capacity of nodes into route selection using cross layer approach is called signal strength and energy-aware routing protocol (SEA-DSR). It uses the reliability factor for route selection among the all routes. In this paper, they use signal strength of the nodes and residual energy of the intermediate nodes and also protect from the link breakage. First phase is route discovery for the destination using RREQ and add the reliability count (RELCOUNT). Second phase is route discovery at the intermediate nodes; here we check the threshold value. Third phase is route selection at the destination node, we use more reliable path, and last phase is route maintenance. This method reduce the link breakage, reduce the path setup time and better perform in terms of packet delivery ratio, average end to end delay and control overhead.

Yunjung Yi, Mario Gerla and Kwon [25] has been described On-Demand Passive cluster based flooding to reduce the flooding overhead without decreasing the performance of the network. In this, network is portioned into on demand clusters interconnected through gateways as shown in Figure 2.2. In this, there was no transmission of cluster related information. In this, data packet was sent an extra field was attached containing cluster state of node, cluster id and cluster head address. This technique leads to significant decrease in power consumption and overhead and use the topology information to overcome the loss of data and energy in flooding the route requests.

HARPREET KAUR, GURBINDER SINGH BRAR, Dr. Rahul Malhotra [26] described the method which helps us to reduce link failure problem in MANET. Link failure degrades our network performance. This method works on three assumptions, first is we should select the path which is having highest signal strength and second is based upon the hop count like AODV, and the last assumption is based on sequence number. In this protocol firstly mutual authentication is required between the nodes to prevent inside and outside attacks. We add another field which is known as header field with the RREQ. The selection of route is mainly based on the fresh sequence number. It provides the minimum packet loss and highest throughput in the network.

Jhunu Debbarma, Mrinal Kanti Debbarma, Sudipta Roy Nikhil Debbarma and Rajat K. Pal [27] described energy efficient protocol for power conservation in MANET to reduce end-to-end delay, increase the packet delivery rate and also increase throughput. The proposed algorithm is based on IEEE 802.11 power saving techniques which means reduce the power consumption and reduce transmission latency on useless packets. If the density of nodes is higher, then better performance of the network.

Manali Singh, Prof. Jitendra kumar Gupta [28] proposed the noval approach for routing establishment that work according to the threshold value and energy level of the nodes. This method provides more reliable communication, increase the route life time, packet delivery ratio and throughput. In this model, we use set the energy module, set transmission power, idle power, receive power and sleep power required by each nodes. We compare the threshold value with the energy of the node if it is equal or less than we do not choose that path. In this method, they use energy

deterioration and management routing schemes. RSSI (Received signal strength indicator) value used by a node along with an active route to guess a link breakage in its link with its next hop to the source node of this active route. DSR is used as routing protocol for increasing the performance of the network.

Shandilya and Sahu [29] has been described a scheme which was based on trust to secure our network from RREQ flooding attack. In this paper, when sender nodes sends the route request to all the neighbors by using DSR routing protocol then calculate the trust level of each neighboring nodes. In this, nodes are divided into acquaintance, stranger and friend. If the node is stranger then add that node into blacklist. If node is acquaintance, it means trust level between friend and stranger and if node is friend then trust level is full. But it had limitation that delay queue may delayed detection of malicious node till delay time out occurs, till then nodes flood network with packets and hence it fails.

P. P. Khatri, Dr. R. V. Dharaskar, Dr. V. M. Thakare proposed [30] the new DSR protocol with some changes for better performance in high mobility and less usage of energy. In this paper, firstly describes about the DSR protocol and then new propose a new protocol which is based o two main routing objectives. First is for minimum total transmission energy and second is total operational life of the network. The main aim of this protocol is route is selected by sender having higher energy nodes. Once the intermediate nodes receive the RREQ start the timer, then add its own cost and send to the neighbors**.** If the timer of the REQ is not expired then intermediate node re-broadcast the RREQ with the maximum level of energy nodes. Destination nodes also wait for timer and send the RREP with maximum energy path to the sender. In the last with the maximum energy level path should be selected.

Anil Jaswal, Anil Sagar [31] described the Enhance energy efficient position based DSR routing protocol which is deals with the residual energy, bandwidth, load and hop count in terms of route discovery. By using this method, we select maximum residual energy nodes so that energy usage among all the nodes can be balanced. In this protocol, RREQ is same as DSR and intermediate node check route cache for destination. If node has same address then it send RREP to the sender node, otherwise broadcast the RREQ. Some important points like, if energy level is same of two paths

then the selection is based on the bandwidth. If energy, bandwidth is same then based on hop count, if these three are same within two paths then check the minimum load.

Uma Rathore Bhatt, Neelesh Nema and Raksha Upadhyay [32] proposed the enhanced DSR to reduce the flooding of RREQ packets in the network with the less usage of energy and less congestion. In this method, when node receive a RREQ packet it check its own residual energy, received signal strength and speed. If the pre-defined threshold value is higher than packet will be discarded. In this method when a packet is received by any node it checks destination id if it is matched then send the RREP packet to the sender, otherwise check the packet id if it is same as previous then discard it. If all of this is right then compare the threshold value.

Ruchi Gupta [33] describes the trustful location based energy deterioration method based on the on demand routing. The main problem in MANET is that the mobility of nodes means the location of the nodes; in the previous work we use the GPS to find the location of the mobile node. It provides the better throughput, packet delivery ratio and increase the lifetime of the network. We use on demand routing protocols on the basis of sending control messages, size of control headers and efficient route reconfiguration. It combines the neighbor discovery and location based routing for enhance the lifetime of the network. We use the sensor node to minimize the state of information to be maintained and delivery of the data is based on the link quality.

# CHAPTER 3
# PRESENT WORK

**Problem Formulation-**

Mobile Ad Hoc Network is an infrastructure-less temporary network, in which number of nodes are there which can move anywhere in the network. Due to MANET characteristics like dynamic network topology, mobility of nodes there are lots of security challenges occur in the MANET which may cause different kind of attacks. In this work Detection of black hole attack is done.

Node in MANET can simply leave or join the network any time. In every year there are tons of researches completed to provide security to black hole attack in MANET. Various solutions are provide by researchers for securing network from malicious node but still security mechanisms are not this much of sufficient only due to MANET challenges and its characteristics. As security increases attackers also become smarter and intelligent they found new ways or technique for doing attack.

In existing technology it detects single black hole attack for which a step verification method is used to detect black hole so attackers start doing attack with the help of each other by using more than two nodes they start doing black hole attack. So enhancement is done to provide more security to the network from single black hole attack with energy efficiency. In proposed work, we add one distance_time_value field for verification about true path from the reply node. Problem in this system is there energy usage of mobile nodes and neighbor node is also malicious one and it simply verifies that node is having true path and path is selected which causes black hole attack in the network

## 3.1 PROPOSED WORK

In our proposed work, we detect the black hole attack from MANET with energy efficiency. In the previous work, we understand that in the MANET problem of energy efficiency is still there and the security of our data packets is big issue. Here are several techniques which are used in detection the black hole attack and to save

the energy of network but our algorithm is able to detect the malicious at various levels with the usage of energy efficiency by using clustering model.

We want to start the communication in MANET with the help of AODV protocol. In this, firstly sender node sends the RREQ to the neighbor nodes to communicate with the destination node. I will set the waiting time limit for the RREP packet from the neighbor nodes, and then compare it with running time. Running time is the time when the RREP packet is reached to the source, if running time is less than or equal to waiting time then proceed further otherwise it goes to next factor which is known as distance factor to check the distance between them in terms of time otherwise drop the RREP. In distance factor, I set the threshold value and check the result if distance is satisfies the threshold value then no need to check the malicious table for the malicious node and store the distance in dt_table. If distance time not satisfy the threshold value then check for malicious node id in the MAL_table, if it is present in MAL_table then discard the RREP otherwise it goes to next verification step which means ask the next hop about the true path to the destination. If next tells that he has a true path then store the node_id and sequence number in RREP_table otherwise store in MAL_table. Now from the RREP table, node select highest destination seq_no and compare it with other destination seq_no from the RREP table if it greater than check for packet drop value. If it satisfies the condition of packet drop then store in MAL_table otherwise keep in the RREP_table. Now nodes select the next highest destination seq_no and find the parameters to calculate the node_value. It calculates from the battery power, buffer length, serve time and number of device connected with that node and link weight which is calculated from parameters like percentage of neighborhood sharing, speed of the link, energy of that link and from the distance factor and then find the total weight of the node. The node_value is further store in node_value_table and then make the clusters based on the areas. Now select the highest node_value as a cluster head and start the communication.

## 3.2 OBJECTIVE OF THE STUDY

The main objectives of study are:

- To propose a method that can save the energy of mobile nodes in mobile ad-hoc network.
- To evaluate the efficiency of proposed method in detecting the black hole attack with energy efficiency.

## 3.3 RESEARCH METHODOLOGY

**Nomenclature:**

- **Mal_Table:** In which malicious nodes are stored.
- **Seq_No:** Specific Number which source receive from destination for a path.
- **Node_ID:** MAC Address of the node.
- **Mal_ID:** Malicious node ID stored in malicious table.
- **RREP_Table:** Stores Seq_No and Node_ID of all RREP.
- **Distance_time_value table-** In which distance_time_value is stored

.

**Tables:**

- **Mal_Table**

**Table 3.1-** Mal_table

| Mal_ID |
|---|

- **Distance_time_value_table**

**Table 3.2-** Distance_time_value_table

| Node_ID | Distance_time_value | Sequence no. |
|---|---|---|

- **RREP_table**

**Table 3.3-** RREP_table

| Seq_No | Node_ID |
|---|---|

- **Node_value_table**

**Table 3.4-** Node_value_table

| Seq_No | Node value |
|---|---|

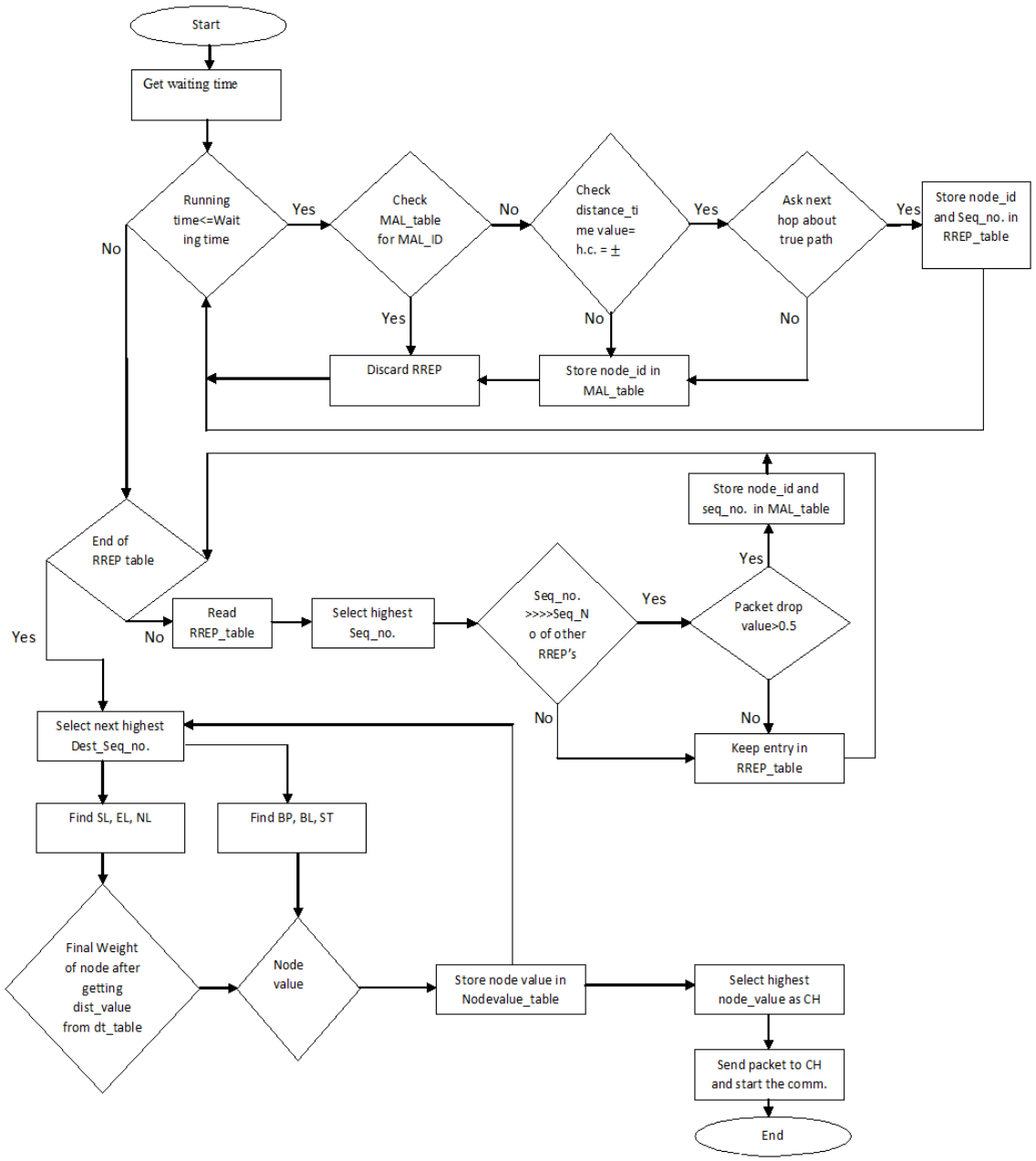


**Figure 3.1-** Flow chart of proposed algorithm

**Algorithm-**

**Step 1:** Get current time (Time at which route request message is sent)

**Step 2:** Get waiting time (WT).

**Step 3:** While (RT<=WT).

Verification of route reply messages are done by various step verifications on the basis of traffic.

**Step 4:** Check for malicious node.

**4a.** After getting route replies from intermediate nodes, check the malicious_table for malicious node_id which is formed on the basis of previous traffic.

**4b.** If node_id is matched with the malicious_table, then discard the route reply.

**4c.** If node_id is not found in the malicious_table, then go to step ii.

**Step 5:** Check the distance_time value.

**5a.** If distance_time value matches with expected hop count value, then store that value in dt_table and go to step C.

**5b.** Else discard the route reply.

**Step 6:** In this sender node ask the next hop that node replied for the route request message has a path to destination or not.

**6a.** If next hop confirms that replying node has path, then node_id and seq_no. is stored in RREP_table.

**6b.** Else node_id and seq_no. is stored in malicious_table.

**Step 7:** Once the running time (RT) is greater than waiting time (WT) all verifications are done of route reply messages.

Now select one seq_no. from the RREP_table.

While (End of RREP_table is not reached) do two step verification.

**7a.** Compare the selected seq_no. with all other seq_no. which are present on the RREP_table, if seq_no. is exceptionally high than do next step verification and go to step D (ii).

**7b.** In this, the value of packet drop is checked here, if it is greater than 0.5 then store that node_id in malicious_table otherwise node_id keep in RREP_table and go to step E.

**Step 8:** Once the all seq_no. are verified then select one highest seq_no. from the RREP_table.

While (End of RREP_table is not reached), find the cluster head.

**8a.** Find the final weight of node using speed of link (SL), energy of link (EL) and neighborhood links (NL) and distance_time value which is getting from dt_table.

Final weight of node = (F1 * SL) + (F2 * EL) + (F3 * NL) + distance_time value.

$$SL = \frac{S_a + S_b}{2}, \quad EL = \frac{E_a + E_b}{2}$$

a and b are two connected nodes. $S_a$ and $S_b$ are their speed.

$E_a$ And $E_b$ is the consumed energy by two nodes.

EA is the energy of node A and EB is the energy of node B.

F1, F2, F3 are weight factors.

F1 + F2 + F3 = 1.

**8b.** Then find the battery power (BP), buffer length (BL) and serve time (ST) and go to step F.

**Step 9:** Find the node value by adding the final weight of node and all the components of step E (ii).

Node value = Final weight of node + BP + BL + ST.

And store the node value in node_value_table.

**Step 10:** Select one highest node value from the node_value_table and make that node cluster head then send the packets to that cluster head. Cluster head will select from neighbor nodes of the sender.

**Step 11:** Delete all other seq_no. from RREP_table.

# CHAPTER 4
# RESULT AND DISCISSION

## 4.1 Simulation Set-up

Ns-2 is used for simulation and it is an IEEE 802.1 standard which is used at data link layer and physical layer. AODV routing protocol is used at network layer and TCP protocol is used at transport layer. Radio propagation and wireless channel is used in an area of 800m * 800m. Constant Bit Rate (CBR) packets are used for sending packets. Simulation parameters are shown in **Error! Reference source not found.**.

**Table 4.1-** Simulation parameters

| PARAMETER | VALUE |
|---|---|
| Simulation Area | 800m * 800m |
| Routing protocol | AODV |
| Simulator | NS 2 |
| No. of Malicious Nodes | 2 |
| Traffic Type | CBR |
| Number of Nodes | 15 |
| Transmission Range | 100m |

In fig. 4.1 show the placement of nodes in the network. We assume the scenario that source node will send the route request message and other neighbor nodes reply back. In route reply packet node id and other attributes are present.

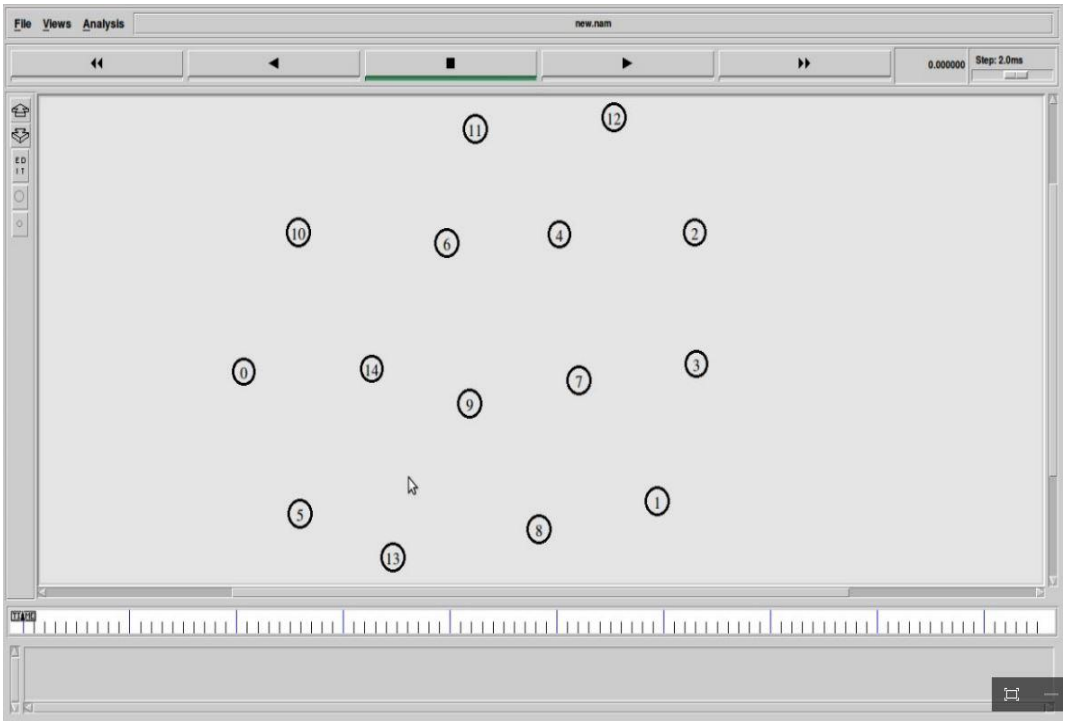


**Figure 4.1-** Node placement in the network

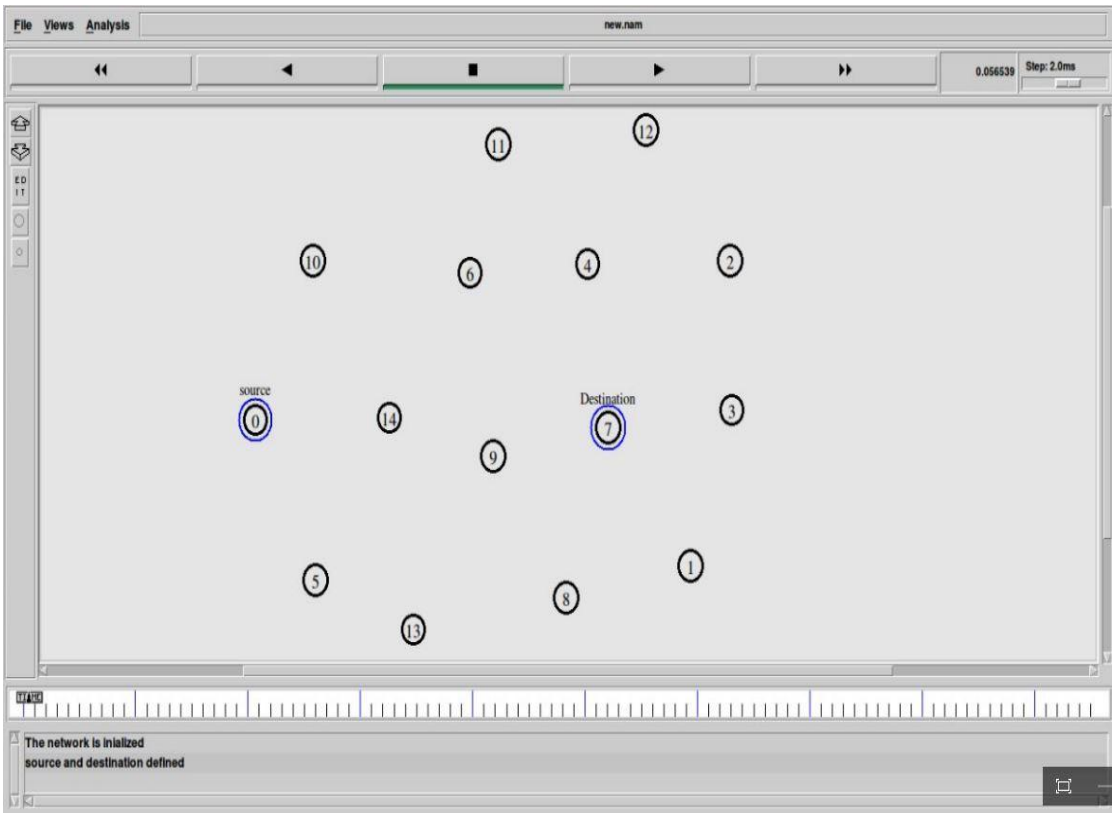


**Figure 4.2-** Source and destination nodes

In Fig. 4.2 source and destination nodes are shown. Node 0 is source node which is connected to multiple other nodes and node 7 is destination node.

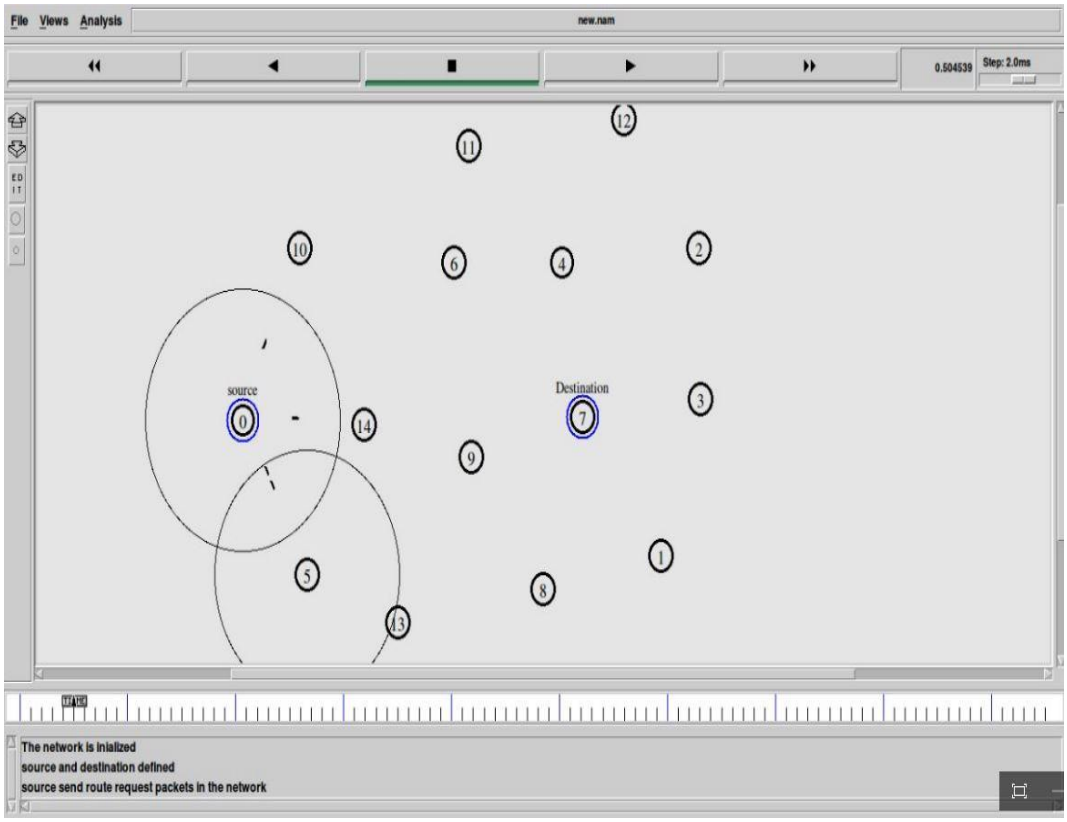


**Figure 4.3-** Route request packet forward

In Fig 4.3 source node (node 0) send the route request message to reach up to destination node (node 7). Source node will send route request message to all its neighbors.

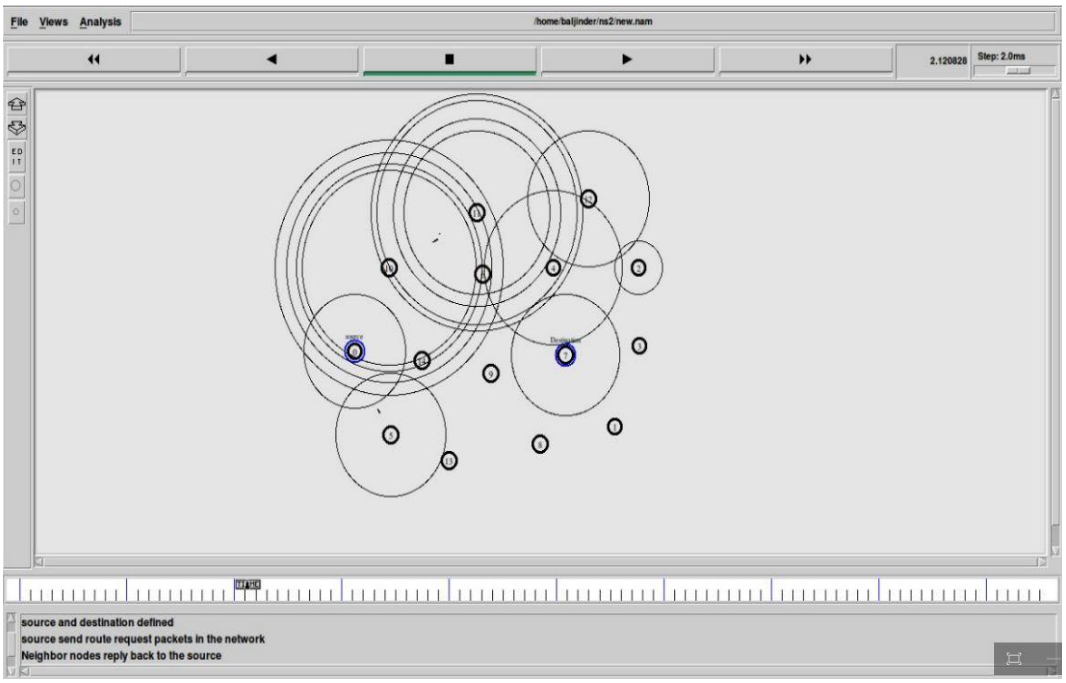


**Figure 4.4-** Route reply backward

In Fig. 4.4, all the neighbor nodes send the route reply message back to the source with path to the destination.

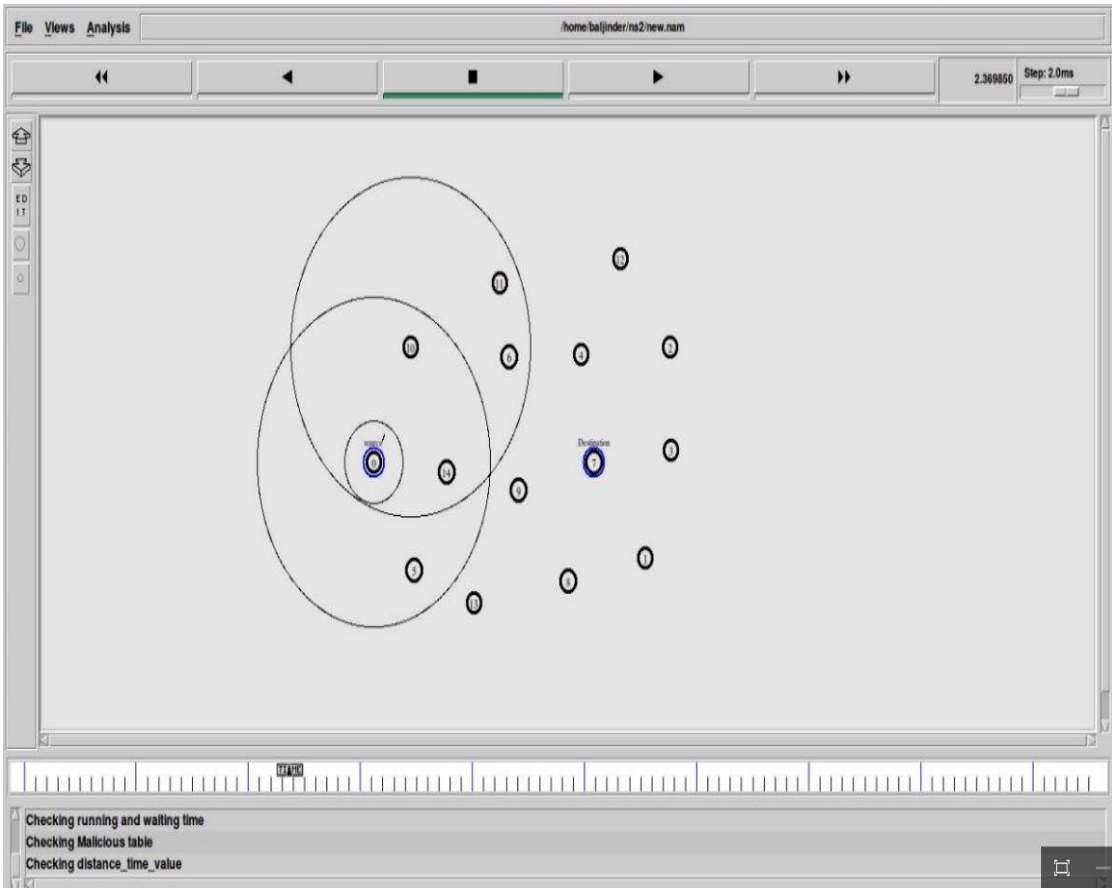


**Figure 4.5-** Verification steps

In Fig. 4.5 After checking the running and waiting time of route reply messages, various steps are performed for verification like checking the previous malicious table, check distance time value etc. If node are verified then it's ok otherwise discard the route reply message.

In Fig 4.6, now source node will ask from the next nodes about true path is performed and then isolate the malicious nodes in the network. Node 11 and node 5 are malicious nodes in this network.

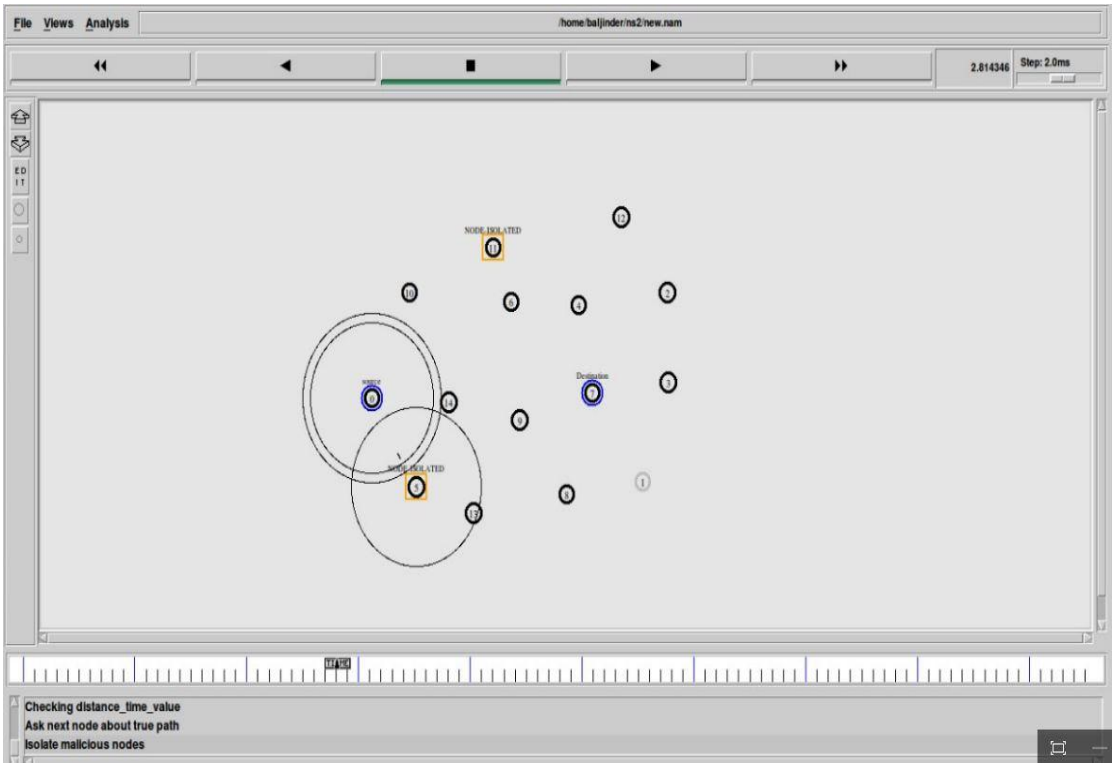


**Figure 4.6-** Isolates malicious nodes

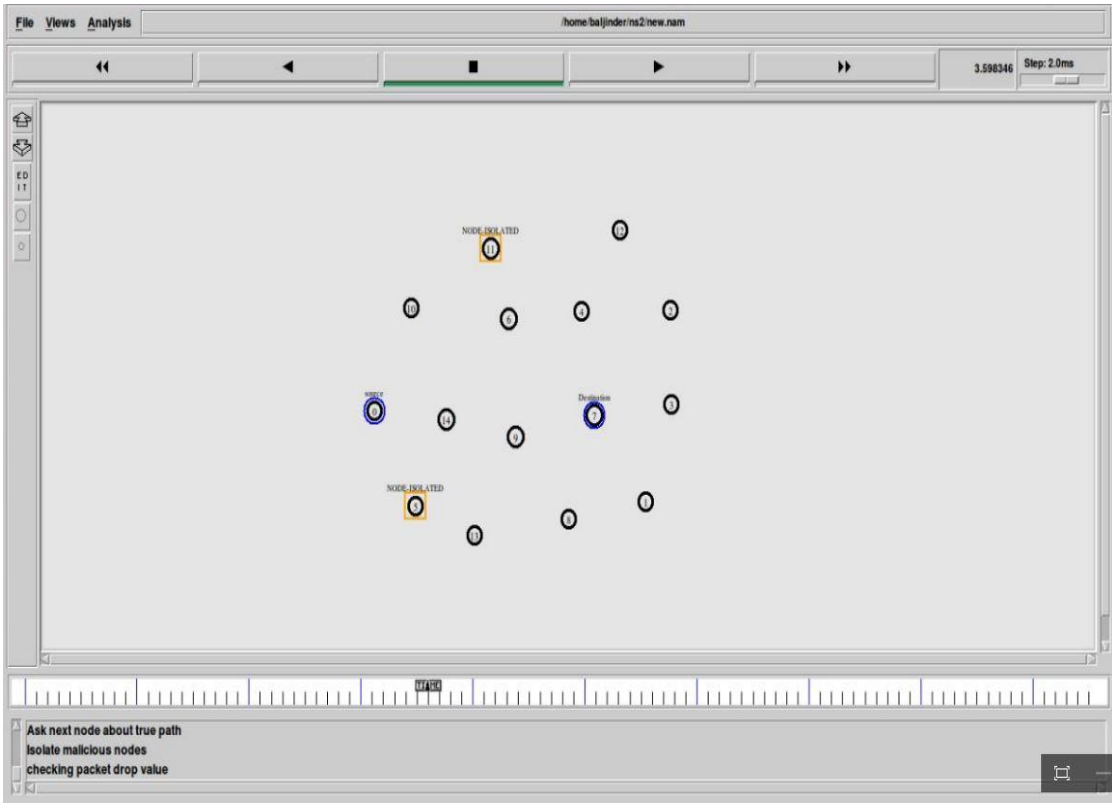


**Figure 4.7-** Checking packet drop value

In Fig 4.7, packet drop value is checking from the route reply table, if the packet drop value is greater than 0.5 then it means that node is malicious node.

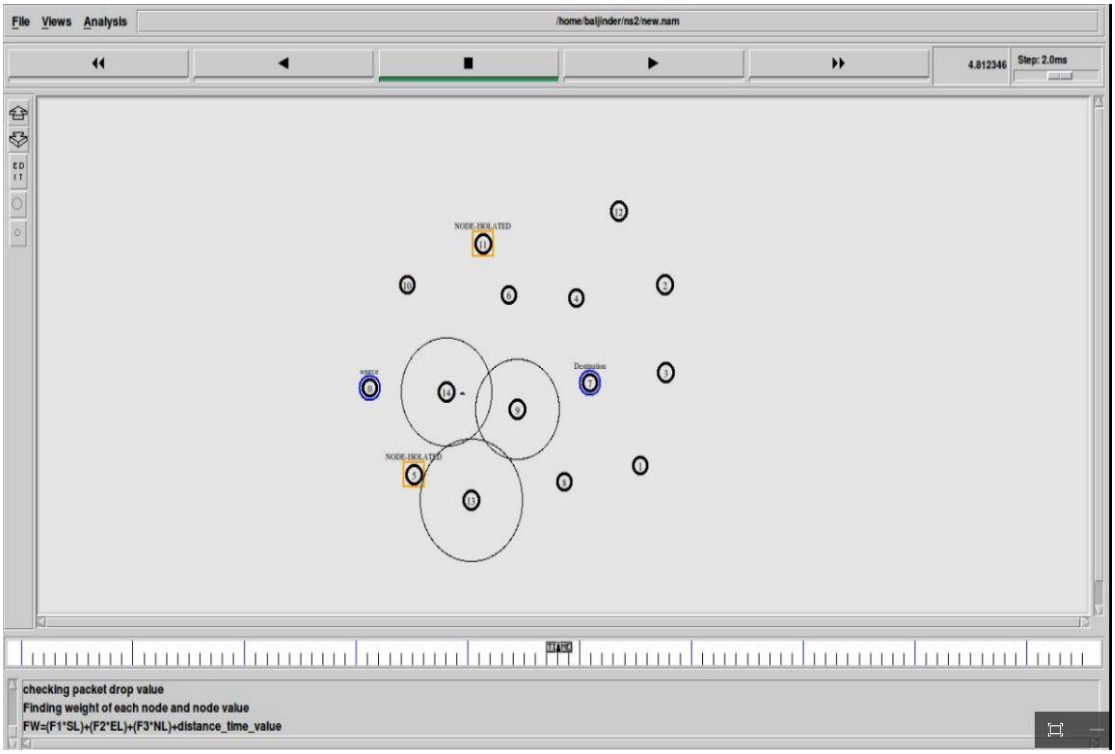


**Figure 4.8**- Final weight of each node

In Fig. 4.8, Select one by one all the sequence number from the route reply table and then find the final weight of each node means speed of the link, energy of the link etc.

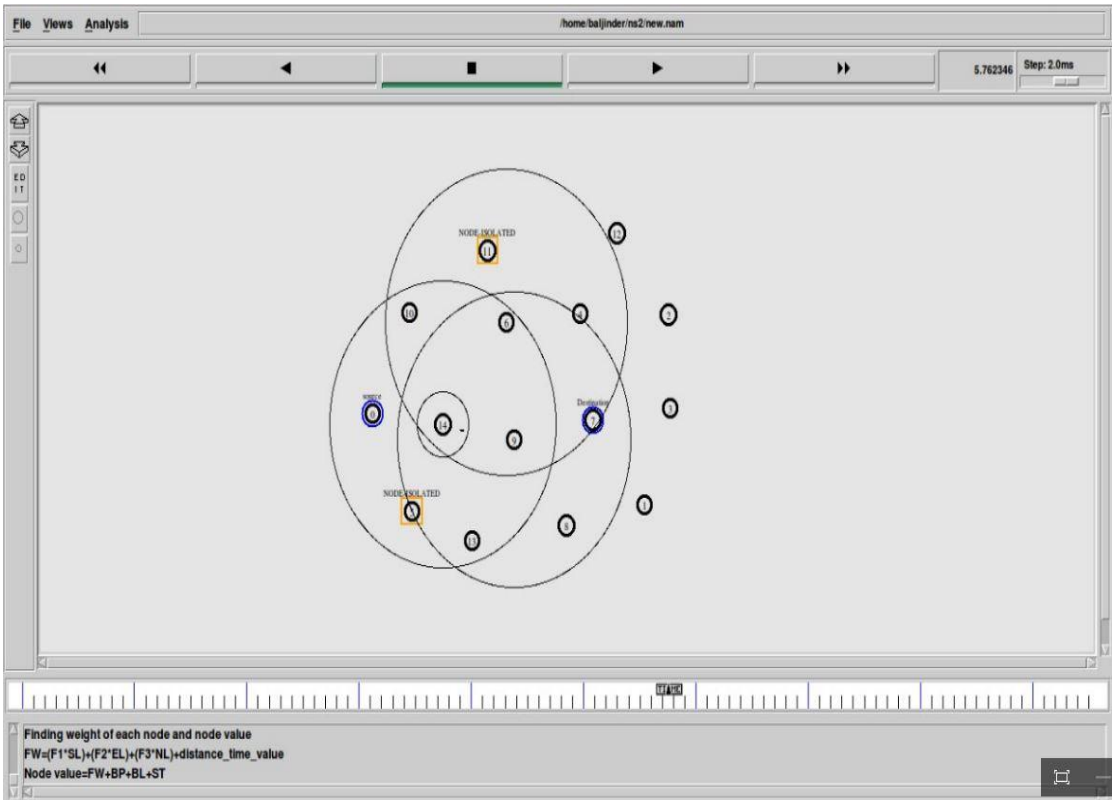


**Figure 4.9**- Final node value

In Fig. 4.9 Simply add the final weight of each node with battery power, buffer length and serve time. Then we have node value and store it into node_value table.

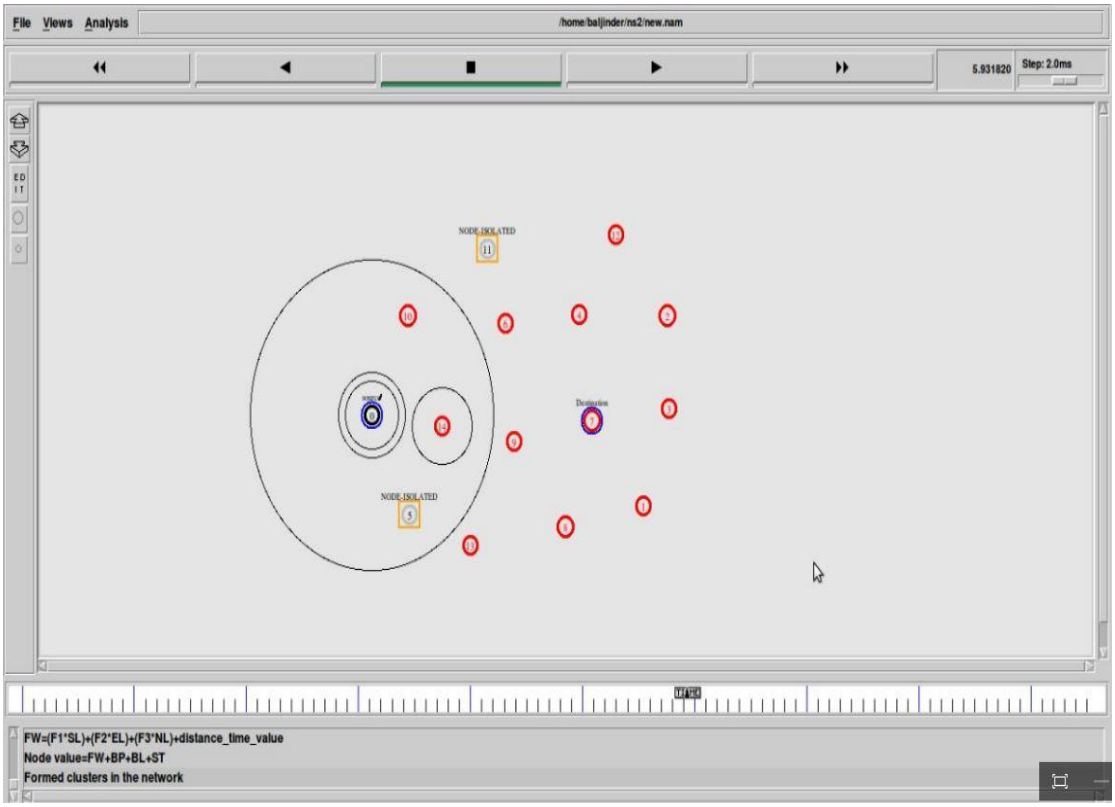


**Figure 4.10**- Cluster formation

In Fig. 4.10, the process of cluster formation is going to start on the basis of area.

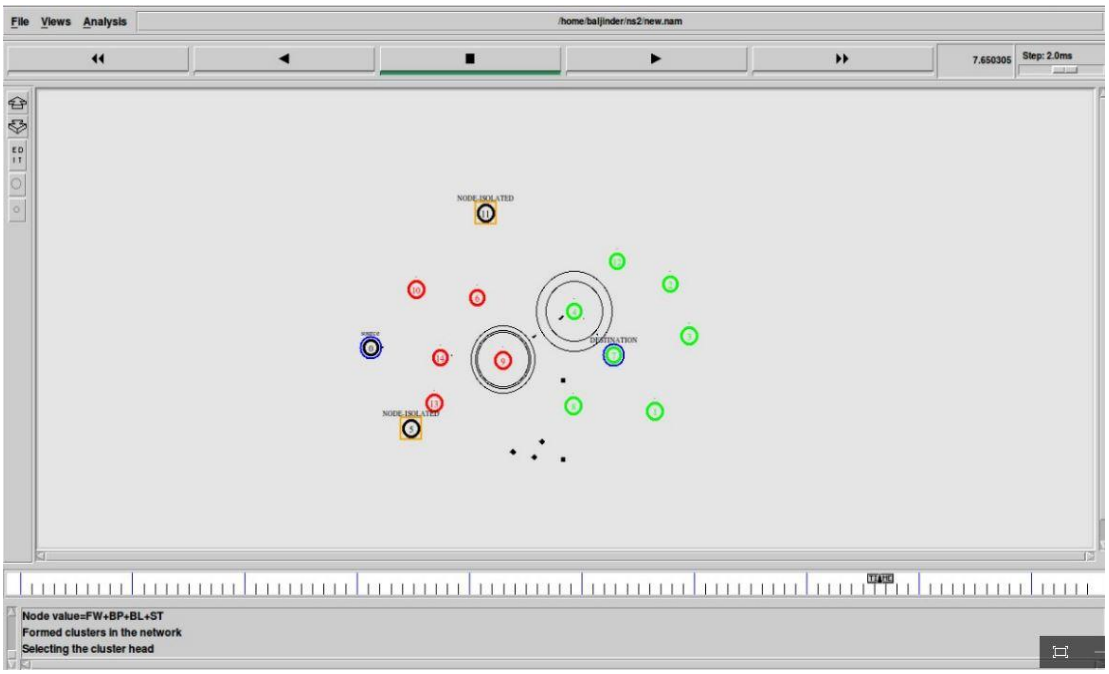


**Figure 4.11**- Selecting cluster head

In Fig. 4.11, from the node value table, select node as cluster head which have highest node value. Node 9 and node 4 select as a cluster head.

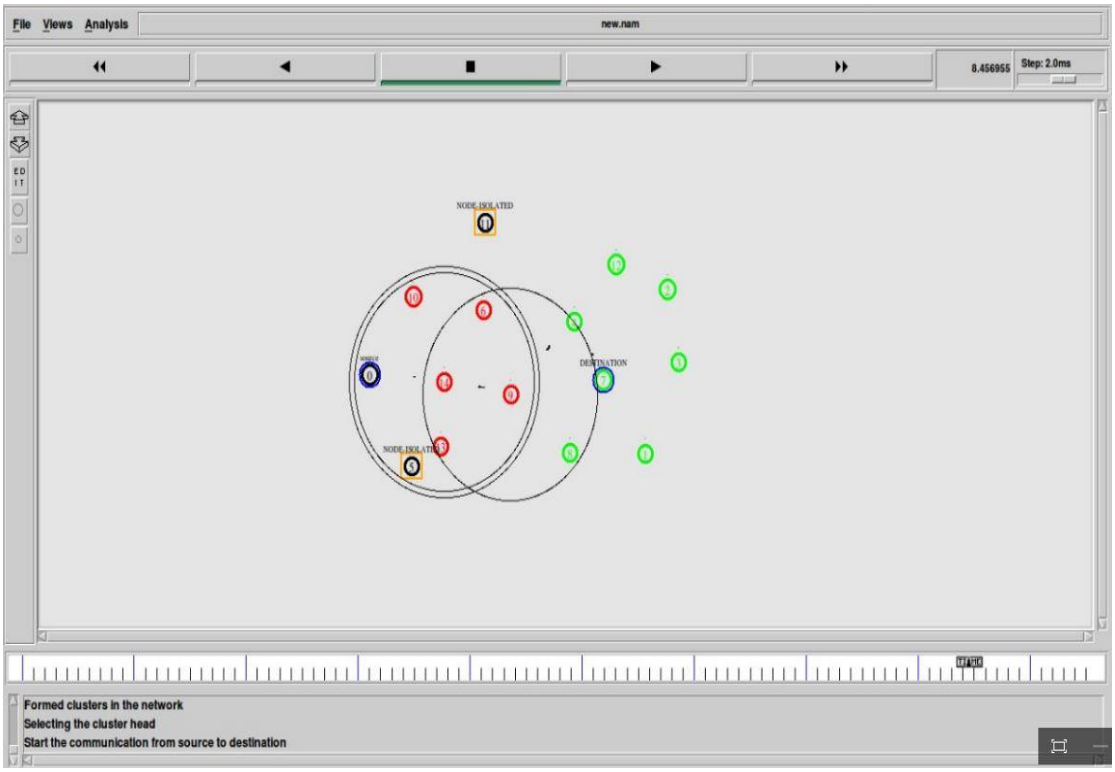


**Figure 4.12-** Transmission start between source and destination

In Fig. 4.12, show the transmission between source and destination. There are two clusters and two cluster head (node 9 and node 4). Source node sends the data to cluster head then it pass the data to next cluster head.

## 4.2 Experimental result-

To check the performance of proposed technique, simulation of AODV in the under black hole attack and under proposed algorithm is done. The parameters for evaluating the performance are throughput, energy and packet delivery ratio (PDR).

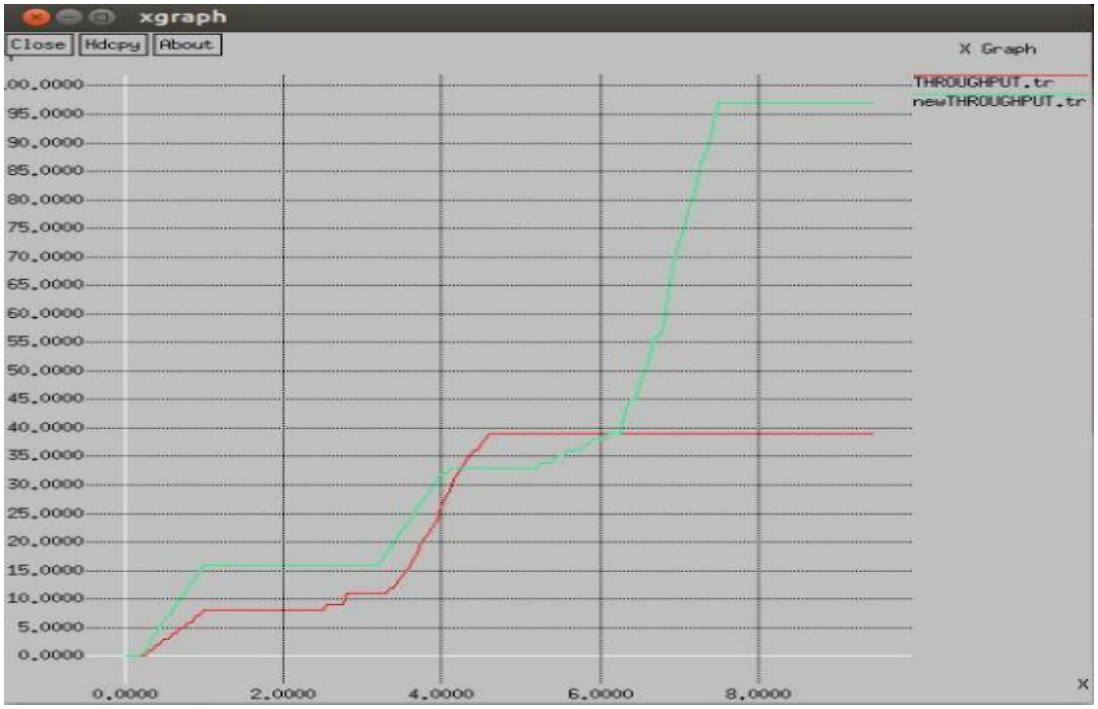


**Figure 4.13-** Throughput comparison

In Fig. 4.13, the Comparsion of throughput is done. The simulation of this graph is based on under black hole attack and with proposed method. Throughput means number of successful packets transfer over the communication channel. So from the slope in the graph we can simply compare the obtained throughput value in which red line is under black hole attack and green is proposed method.


**Figure 4.14-** Packet loss rate comparison

In Fig. 4.14, Packet loss ration comparison is done between under black hole attack and proposed method. Packet loss ration means, how many packets are loss in one unit time or in one transmission. Red line in the graph shows the under black hole attack and green line show the proposed method packet loss ratio.


**Figure 4.15-** Energy comparison

In Fig. 4.15, Energy comparison is done between under black hole attack (red line) and proposed method (green line). Energy means battery of the mobile nodes, we use the word efficiency it means use the energy of mobile nodes in efficient way, so we can increase the lifetime of the network.

# CHAPTER 5
# SUMMARY AND CONCLUSION

This research report provides the introduction of MANET (Mobile ad-hoc network along with its challenges, applications, advantages, disadvantages and various security attacks mainly black hole attack. It discusses the research work done by different researchers in different areas of MANET like improving routing protocols, flooding techniques, energy efficiency techniques, clustering formation techniques, security attacks specially black hole attack.

The main focus is on black hole attack which is one of the securities attack. In black hole attack, attacker publicize itself as a node which have shortest path to destination node from sender and when attacker or malicious node receives the packet, it decides whether to packet or drop it. The black hole attack reduces the performance of network. Literature review shows that with time lots of changes have been proposed in AODV and DSR for detecting and preventing black hole attack. Each method has its own advantages and disadvantages.

In the proposed algorithm various terms are used to detect black hole attack from MANET with energy efficiency which means saving the energy of mobile nodes. Previous step verification algorithm is only for detection of black hole attack without energy efficiency. In our proposed algorithm we use cluster head concept which is used for communication. The node selected as cluster head which has highest node value means highest battery power, buffer length, serve time etc. In this algorithm we use the concept of distance time value, packet drop value which helps in order to increase the PDR and throughput of the network. It uses the least energy for communication.

**Future Scope**

So the scope of this work is to study the effects of Black Hole Attack on MANET and to find methods for detecting black hole node and possibility of occurrence of black hole attack on MANET with less usage of resources with an increase in performance.

Further the methods for detecting and preventing cooperative black hole attack, security measures for transmitting data from source node to destination node once route has been established can be found.

# REFERENCES


[1]. C.K Toh, (2002), “Ad Hoc Mobile Wireless Networks Protocols and Systems”, Pearson Education, Inc., p. 27, 32 – 37.

[2] C. Siva Ram Murthy, B. S. Manoj, (2004), “Ad Hoc Wireless Networks: Architecture and Protocols”, Pearson Education, Inc., p. 283 – 284, 431 – 436.

[3]. Mohit Kumar and Rashmi Mishra, “An Overview of MANET: History, Challenges and Applications” Indian Journal of Computer Science and Engineering (IJCSE), Vol. 3 No. 1 Feb-Mar 2012.

[4]. H. Deng, W. Li, D.P. Agrawal, “Routing Security in Wireless Ad Hoc Network”, IEEE Communications Magazines, vol. 40, no. 10, October 2002.

[5]. Jeroen, H.; Ingrid M.; Bart, D.; and Piet D.; “An Overview of Mobile Ad hoc Networks: Applications and Challenges”, Journal of the Communications Network, Vol. 3 (July 2004), pp. 60-66.

[6]. Giannoulis, Antonopoulos, Topalis, Koubias, "ZRP versus DSR and TORA: a comprehensive survey on ZRP performance," Emerging Technologies and Factory Automation, 2005, 10th IEEE Conference on, vol.1, pp.8 pp., 1024, 19-22 Sept. 2005.

[7]. Priyanka Goyal, Vinti Parmar, Rahul Rish, “MANET: Vulnerabilities, Challenges, Attacks, Application”, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[8] Nawneet Raj, Priyanka Bharti, Sanjeev Thakur, “Vulnerabilities, Challenges and Threats in Securing Mobile Ad-hoc Network”, Fifth International Conference on Communication Systems and Network Technologies, © 2015 IEEE DOI 10.1109/CSNT.2015.101.

[9] S.Sankara Narayanan and Dr.S.Radhakrishnan, “Secure AODV to Combat Black Hole Attack in MANET”, International Conference on Recent Trends in Information Technology (ICRTIT), ©2013 IEEE.

[10] Ms.Nidhi Sharma Mr.Alok Sharma, “The Black-hole node attack in MANET”, Second International Conference on Advanced Computing & Communication Technologies, © 2012 IEEE DOI 10.1109/ACCT.2012.112.

[11]. J. Luo, M. Fan, and D. Ye, "Black Hole Attack Prevention Based on Authentication Mechanism", 2008 IEEE, 173 ICCS 2008, p: 173-177.

[12]. S.K. Doshi, T.X. Brown, "Minimum Energy Routing Schemes for a Wireless Ad Hoc Network", IEEE INFOCOM 2002

[13]. Neha and Manmohan Sharma, “Step Verification for Detection of Black Hole Attack in MANET”, International Journal of Applied Engineering Research (IJAER), vol. 3 number 55 (2015), pp. 2887-2891.

[14]. Abbas Afsharfarnia and Abbas Karimi, “A New Clustering Algorithm Using Links' Weight to Decrease Consumed Energy in MANETs”, TELKOMNIKA, Vol.12, No.2, June 2014, pp. 411~418, DOI: 10.12928/TELKOMNIKA.v12i2.1949.

[15]. Alka Adlakha, Vasudha Arora, “Performance Evaluation of AODV and DSR Routing Protocols under Constrained Situation**”,** International Journal of Advanced Research in Computer and Communication Engineering**,** Vol. 4, Issue 7, July 2015.

[16]. Alfy Augustine and Manju James, “Black Hole Detection using Watchdog”, International Journal of Current Engineering and Technology, Vol. 5, No. 4 (Aug, 2015).

[17]. Rajib Das, Dr. Bipul Syam Purkayastha, Dr. Prodipto Das, “Security Measures for Black Hole Attack in MANET: An Approach”, International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 4 Apr 2011, pp. 2832-2838.

[18]. Yonghui chen, chunfeng zhang, zhiqin liu, “Energy Efficient Routing Protocol Based on energy of node and Stability of Topology”, Third International Conference on Information and Computing, 2010.

[19]. Deepika Patil, Nitika Vats Doohan, “A Novel TAB Based Preemptive Multi-Hop Local Repair Algorithm for AODV in MANET**”,** International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.

[20]. Hwan-Seok Yang,Seung-Jae Yoo, “Authentication Techniques for Improving the Reliability of the Nodes in the MANET”, International Conference on IT Convergence and Sercurity (ICITCS), IEEE, Oct 2014, pp. 1 – 3.

[21]. Mandeep Singh, Mr.Gagangeet Singh, “Secure and Efficient Cluster Head Selection Algorithm for MANET”, Journal of Network Communications and Emerging Technologies (JNCET), Vol. 2, Issue 2, June (2015).

[22]. Shelbala Solanki, Anand Gadwal, “Hybrid Security Using Digital Signature & RSA Encryption for AODV in MANET**”,** International Journal of Computer Science and Information Technologies, Vol. 6 (3), 2015, pp.- 2630-2635.

[23]. T. Kiran, T. P. Anish, “Secure Hidden Routing in Mobile Ad Hoc Networks”, International Journal of Advanced Research in Computer Science and Software Engineering**,** Vol. 5, Issue 4, April 2015.

[24]. P.SRINIVASAN and K.KAMALAKKANNAN, “SIGNAL STRENGTH AND ENERGY AWARE RELIABLE ROUTE DISCOVERY IN MANET**”,** International Journal of Communication Network Security ISSN: 2231 – 1882, Vol. 1, Issue-4, 2012.

[25] Y. Yi, M. Gerla, T.J. Kwon, “Efficient flooding in ad hoc networks using on-demand (passive) cluster formation”, ONR ”MINUTEMAN” project under contract N00014 - 01 - C – 0016.

[26]. Harpreet kaur, Gurbinder singh brar, Dr. Rahul Malhotra, “TO PROPOSE A NOVEL TECHNIQUE TO REDUCE LINK FAILURE PROBLEM IN MANET”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Vol. 3, Issue 10, October 2014.

[27] Jhunu Debbarma, Mrinal Kanti Debbarma, Sudipta Roy Nikhil Debbarma and Rajat K. Pal, “An Energy-Efficient Protocol for Power Conservation in Mobile Ad-hoc Networks”, 2013 International Symposium on Computational and Business Intelligence, 2013 IEEE, DOI 10.1109/ISCBI.2013.28.

[28]. Manali Singh, Prof. Jitendra kumar Gupta, “Energy Saving Technique in Wireless Mobile Ad-hoc Network for Reliable Communication”, International Journal of Computer Trends and Technology (IJCTT), vol. 7, No. 2– Jan 2014.

[29]. S.K. Shandilya, S. Sahu, "A Trust Based Security Scheme for RREQ Flooding Attack in MANET", International Journal of Computer Applications (0975–8887) Volume 5– No.12, August 2010.

[30]. P. P. Khatri, Dr. R. V. Dharaskar, Dr. V. M. Thakare, “Designing an efficient power aware routing algorithm based on existing Dynamic Source Routing (DSR) Protocol”, International Journal of Electronics, Communication & Soft Computing Science and Engineering, page no. -316-319, ISSN: 2277-9477.

[31]. Anil Jaswal, Anil Sagar, “An Approach to Enhance Energy Efficient Position Based DSR Routing Protocol”, International Journal of Computer Science and Mobile Computing, Vol. 4, Issue.2, February 2015, pg.395 – 401.

[32]. Uma Rathore Bhatt, Neelesh Nema, Raksha Upadhyay, “Enhanced DSR: An Efficient Routing Protocol for MANET”, International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), ©2014 IEEE.

[33]. Ruchi Gupta, “Trustful Location based Energy Deterioration on Demand Multipath Routing in Mobile Ad hoc Networks”, Fourth International Conference on Advanced Computing & Communication Technologies, © 2014 IEEE.

# APPENDIX

| | |
|---|---|
| AODV | Ad hoc On Demand Distance Vector |
| CBRP | Cluster Based Routing Protocol |
| DSDV | Destination Sequenced Distance Vector |
| DSR | Dynamic Source Routing |
| IEEE | Institute of Electrical and Electronics Engineers |
| MANET | Mobile Ad-hoc Network |
| NS | Network Simulator |
| PDR | Packet Delivery Ratio |
| RREQ | Route Request |
| RERR | Route Error |
| RREP | Route Reply |
| Seq. no. | Sequence Number |
| TORA | Temporally Ordered Routing Algorithm |
| TTL | Time To Live |

# LIST OF PUBLICATIONS

**Published Papers**

[1] Manmohan Sharma, Baljinder singh, "Energy Efficient algorithm for Detection of Black hole attack in MANET", *Shannon 100, 3rd International Conference on Computing Sciences (ICCS), April 2016.*