Simulation and Analysis of Performance Parameters for Black Hole and Flooding Attack in MANET using AODV protocol

A

Dissertation

submitted

in partial fulfillment

for the award of the Degree of

Master of Technology

In Department of Computer Science & Engineering

(With specialization in Computer Science & Engineering)

Supervisor Name
Dr Naveen Hemrajani
Professor

Submitted By
Swati Jain
SGVU111605991

Department of Computer Science & Engineering

Suresh Gyan Vihar University
Mahal, Jagatpura, Jaipur

MAY 2013

Candidate's Declaration

I hereby that the work, which is being presented in the Dissertation, entitled "**Simulation and Analysis of Performance Parameters for Black Hole and Flooding Attack in MANET using AODV protocol**" in partial fulfillment for the award of Degree of "**Master of Technology**" in Deptt. of **Computer Science & Engineering** with specialization in **Computer Science & Engineering** and submitted to the **Department of Computer Science & Engineering,** Suresh Gyan Vihar University is a record of my own investigations carried under the Guidance of **Dr Naveen Hemrajani** Department of **Computer Science & Engineering**.

I have not submitted the matter presented in this Dissertation anywhere for the award of any other Degree.

…………………………

(SWATI JAIN)

Enrolment No.: SGVU111605991

M Tech Scholar,

Dept. of Computer Science & Engg.

Suresh Gyan Vihar University

Mahal, Jagatpura, Jaipur

Counter Singed by

…………………………

(Dr Naveen Hemrajani)

Professor

Dept. of Computer Science & Engg.

Suresh Gyan Vihar University

Mahal, Jagatpura, Jaipur

DETAILS OF CANDIDATE, SUPERVISOR (S) AND EXAMINER

Name of Candidate: Swati Jain

Dept. of Study: Computer Science & Engineering

Enrolment No. : SGVU111605991

Thesis Title: Simulation and Analysis of Performance Parameters for Black Hole and Flooding Attack in MANET using AODV protocol

<table>
<tr><th colspan="6">Supervisor (s) and Examiners Recommended
(with Office Address including Contact Numbers, email ID)</th></tr>
<tr><th colspan="3">Supervisor</th><th colspan="3">Co-Superviosr</th></tr>
<tr><td colspan="3">Dr. Naveen Hemrajani (Prof.)
Suresh Gyan Vihar University,
Mahal, Jagatpura, Jaipur
Rajasthan
Contact No.9829032657
E- mail ID: naven_h@yahoo.com</td><td colspan="3"></td></tr>
<tr><th colspan="6">Internal Examiner</th></tr>
<tr><th colspan="2">1</th><th colspan="2">2</th><th colspan="2">3</th></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
</table>

Signature with Date

Programme Coordinator Dean / Principal

Abstract

As the increase of wireless networks, use of mobile phones, smart devices are gaining popularity so the adhoc network is also a uprising field. Mobile Ad-hoc Network is a collection of the mobile nodes that is formed without the support of any existing network infrastructure. The MANET is self configurable network, in which nodes connect and disconnect from the other nodes in the network automatically at any point of time. The characteristics of the MANETs are flexibility, distributed operation, addressing mobility, node to node connectivity, etc. Each device in a MANET is free to move independently in any direction, linking to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router .the node receive the data and forwards it to neighboring node in the path for the further transmission so that it can be reached to the particular destination. Its routing protocol has to be able to cope with the new challenges that a MANET creates such as nodes mobility, security maintenance, and quality of service, limited bandwidth and limited power supply etc. The work describe here is the simulation of flooding and black hole attack in the MANET using AODV protocol. The simulation work is carried out in Network Simulator (NS2.34). Three network scenarios are simulated and the performance parameters like average delay, routing overhead, packet drop rate and packet delivery rate are analyzed and compared By the simulation it has been evaluated that in flooding attack the routing overhead(21.87%) is more as compared to the black hole attack(18.05%). This show that the flooding attack can also make system more vulnerable as this causes more consumption of bandwidth, unnecessary battery utilization of devices, clogs the network. The packet delivery ratio in scenario when black node attacked is 10.52% and in flooded situation it is 15.59% which shows that more packets are correctly received by the destination in flooding attack as compared to black hole attack.

Keywords: MANET, Wireless Networks, Ad hoc Networking, Routing Protocol, Performance Parameters, Flooding

Acknowledgment

Acknowledgement is not only a ritual, but also an expression of indebtedness to all those who have helped in the completion process of the project.

I take this opportunity to express my profound gratitude and deep regards to Dr. Naveen Hemrajani (Prof.) Suresh Gyan Vihar University for exemplary guidance, monitoring and assistance in completion of the project. The blessing, help and guidance I have received by him will be earnestly cherished throughout my life.

I owe my deepest gratitude and profound indebtedness to Dr. Sumit Srivastava (Assoc. Prof.), Manipal University, Jaipur for invaluable guidance and encouragement to carry out the project.

I also extend my wholehearted thanks to Suresh Gyan Vihar University, Mr. Dinesh Goyal (Head Computer Science & Engg.) Ms. Savita Shiwani (Program Cordinator, M.Tech (CS/SE/IC)) and all other staff members for the valuable information provided by them and their cooperation during project work.

Table of contents

List of Tables

List of Figures

List of Abbreviations

IEEE :	Institute of Electrical and Electronics Engineers
WLAN :	Wireless Local Area Network
PAN :	Personal Area Networks
WPAN :	Wireless Personal Area Networks
LAN :	Local Area Networks
WAN :	Wide Area Networks
Wi-Fi :	Wireless Fidelity
MANET :	Mobile Ad-Hoc Network
DoS :	Denial of Services
AODV :	Ad-Hoc On-demand Distance Vector Routing
TORA :	Temporally Ordered Routing Algorithm
DSR :	Dynamic Source Routing
MPR:	Multipoint Relay
RREQ :	Route Request
RREP :	Route Replay
RERR :	Route Error
TC :	Topology Control
UDP :	User Datagram Protocol
TCP :	Transmission Control Protocol
ACK :	Acknowledgement
CBR :	Constant Bit Rate
TCL :	Tool Command Language
OTCL :	Object Oriented Tool Command Language

1. INTRODUCTION

Mobile Ad-hoc Network is a collection of the mobile nodes that is formed without the support of any existing network infrastructure. The MANET is self configurable network, in which nodes connect and disconnect from the other nodes in the network automatically at any point of time. The characteristics of the MANETs are flexibility, distributed operation, addressing mobility, node to node connectivity, etc. Routing of the data in the MANETs are done on the basis of the node discovery and then transmission i.e. the node receive the request message and forwards it to neighboring node in the path for the further transmission so that it can be reached to the particular destination and with help of route reply message the communication takes place. Each node work as a relay agent to route the data traffic. As MANET is dynamic in nature so it is accessible to all the users it may be a legitimate user or the malicious node which reproduce the data or attack in the network. For the connection between the nodes the routing protocols are required .In MANET these are such as AODV (Ad-hoc On Demand Routing protocol), OLSR (Optimized Link State Routing), DSDV (Destination-Sequenced Distance-Vector) etc.

MANET suffer from security attacks because of its features like open medium, dynamic change in topology, lack of central authority for the management and monitoring, distributed operation , lack of infrastructure. So MANET is susceptible to various attacks. In black hole attack, a malicious node uses its routing protocol to advertise itself for having the shortest path to the destination node it wants to intercept. The malicious node advertises availability of fresh routes to the other nodes irrespective of checking its routing table. In this way attacker node indicate the route availability as reply to the route request messages and thus capture the data packet and retain it.

In the work done the black hole attack is simulated using the Network Simulator NS2.34. The black node is inserted into the network and the performance is evaluated for AODV protocol.

1.1. Problem Statement

The black hole attack is simulated under the reactive routing protocol, AODV (Ad-hoc On Demand Routing) protocol. The behavior of the network is to be analyzed how it works in normal, when a large number of packets are flooded in the network and when malicious node is inserted into the network. A comparison is also done to analyze the vulnerable behavior of the study the impact of the black hole.

1.2. Objectives

- To simulate the black hole attack using the Ad- doc On Demand Distance Vector routing protocol.
- To study various attacks in MANET
- To analyze the performance of the network on factors like routing overhead, packet delivery rate, packet dropped rate.
- Analysis of network in normal behavior and when a number of packets are flooded in the network.
- Comparing the simulated results on various factors for the different scenarios.

In the thesis, the Black hole attack is simulated in wireless ad-hoc network and it is evaluated. The simulation is done in NS2.34 which contains the network protocols for the simulation of different number of network nodes. For the evaluation of the network in the existence of a malicious node, the black hole node is created with the help of an agent. A tcl script is created for the implementation ,which consist of the creation of the nodes, connection between the nodes, setting the topography area in which the nodes are located according to the x axis and y axis. The simulation is run for 150 seconds. During the simulation the network is analyzed to study behavior with three, five and ten nodes. The three different scenarios are considered first one is in which the protocol works normally, then large number of packets are flooded and in last malicious node behavior is observed.

In chapter 2 of the thesis overview of wireless network, adhoc network, characteristics of ad-hoc network is illustrated. The security issues are also explained in the chapter. Chapter 3 describes the network simulator (NS2.34) ,its use in the implementation .Chapter 4 presents the simulation of the black hole attack, result analysis of simulated network performance on different parameters. The values are compared for normal behavior and attacked network. The thesis end at conclusion part which state the overall analysis overview and further study.

When the AODV works normally the delay is 383.42 millisecond, when packets are flooded the delay is increased by 0.77 ms, this delay increases more by 133.92 ms when black node is injected into the network. The routing overhead is the number of control messages that are forwarded in the network to manage the network functioning. This value is 21.87% when number of nodes is five in flooded network which is an increase of 21.75%fromthe normal behavior.

2. NETWORK (MANET) DETAILS

The entity network is a collection of computers which are connected together with the help of wired cables or wireless media and allows transmission of data between the systems. The computers, laptops other smart devices are called nodes which initiate the connection, transfer information and terminate connection. The network possess following properties [1]:

A. Sharing of data and information
B. Sharing of resources
C. Distributed computing
D. Complex Structure
E. Scalable

The network can be classified into two types

A. Wired Network

In this type of network the devices are connected to each other with the help of coaxial cable, twisted pair or optical fiber cable. In short there must be a physical channel for communication to take place. The data transmission between the communicating entities is done over the wire.

B. Wireless Network

A network in which the communicating devices exchange information without the use of wire. These devices must lie in the radio range during the communication. The electromagnetic waves are used for the transmission of the data. The wireless networks are becoming more accepted due to its mobility nature, easy to use and less costly. The wireless communication can be possible with the help of Earth-based transmitters and receivers, Communications satellites or IEEE 802.11standards.

Characteristics of Wireless Network

Easy to use and install – The devices in the wireless network can be configured easily with other devices to remain connected to the network. The user need not to connect the device with the wires, which are costly and the setup is complex.

Mobility- The users can remain connected with the network while moving freely. As there is no infrastructure required for the connection establishment .The devices can be configured easily with the access point, which is within the range of the device.

Scalability - The number of users can be increased, they can range from small number of users to thousands.

2.1. Types of Wireless Network

According to the coverage area, it can be classified as follows [2]:

2.1.1. Wireless Personal Area Network

The devices are connected within a small area i.e. within range of few meters or kilometers. The examples are Bluetooth, Zigbee and sensor network. Bluetooth uses short-range radio waves over distances up to approximately 10 metres. For example, Bluetooth devices such as keyboards, pointing devices, audio head sets, printers may connect to personal digital assistants (PDAs), cell phones, or computers wirelessly. The ZigBee devices pass data over longer distance, and the data is relayed through middle nodes which lie in the path ,so to reach to the destination node .

2.1.2. Wireless Local Area Network

WLAN is a network which associate two or more devices using the access point, i.e. without any wired connection the communicating ends can remain connected with the network through an access point. If the user has portable devices like smart phones, tablets, iphones, laptops etc. on which 2G, 3G or 4G networks are enable then he can access information from the internet anywhere at WLAN hotspots. This facility benefits user as he can move around anywhere within the local coverage area and remain connected with the internet. WLANs are based on IEEE802.11 standard which is commonly called as Wireless Fidelity (Wi-Fi). The wireless lan products are based on IEEE 802.11 standards. The standards include 802.11a, 802.11b, and 802.11g. The802.11a provides bandwidth up to 54mega bits per second (Mbps) and the frequency spectrum around 5GHz regulated signals. The 802.11a cost higher so only used for the business purposes 802.11b supports bandwidth which ranges to 11 Mbps. The 802.11g supports bandwidth up to 54 mbps and for higher range it uses 2.4 GHz.

2.1.3. Wireless Wide Area Network

These are the networks that cover a large area such as the neighboring cities or towns. The access points are usually parabolic dishes, microwave links. A system contains base station gateways, access points and wireless bridging relays.

2.1.4. Wireless Mesh Network

The radio nodes are arranged in a mesh topology and provide cost effective connectivity over certain coverage area. It is a special type of wireless ad-hoc network in which each node work also as a relay agent to forward the messages to other nodes. It can be implemented with various wireless technology including 802.11, 802.15, 802.16.

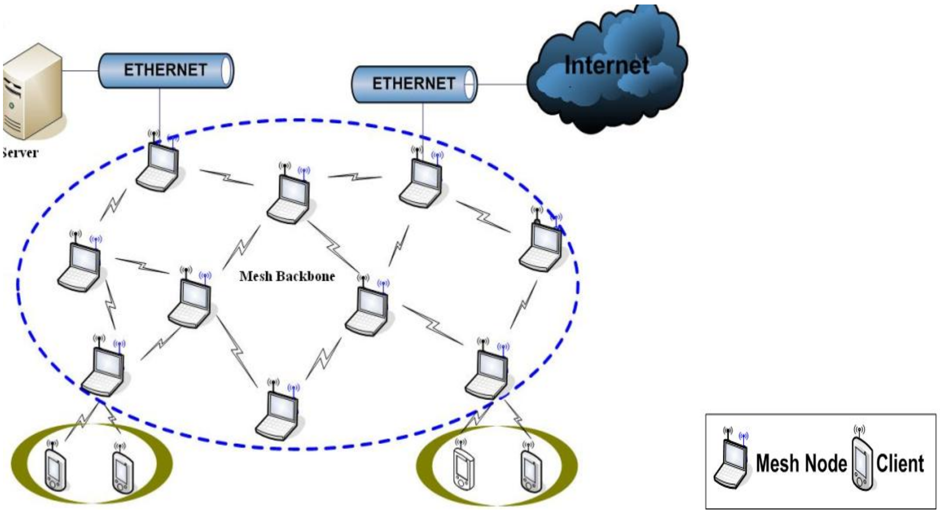


Fig.1 Wireless Mesh Network

2.2. Ad-Hoc Network

It is an infrastructure less network i.e. doesn’t depend on a preexisting infrastructure setup. A node serve as a routing agent to forward the data packets to the neighboring node, which further transmit the packet to reach the destined node. The nodes can join or leave the network at any point of time as there is no centralized administration. The nodes which forward data are selected dynamically based on the network connectivity. Ad-hoc network works on the flooding technique for forwarding the data.

Advantages of Ad-hoc network

A. No centralized administration

B. Self –organizing and adaptive

C. No Infrastructure required so cost less

D. Easy to deploy

2.2.1. Mobile Ad hoc network (MANET)

Mobile Ad-hoc Network is a collection of the mobile nodes that is formed without the support of any existing network infrastructure. The MANET is self configurable network, in which nodes connect and disconnect from the other nodes in the network automatically at any point of time. The characteristics of the MANETs are flexibility, distributed operation, addressing mobility, node to node connectivity, etc. Routing of the data in the MANETs are done on the basis of the node discovery i.e. the node receive the data and forwards it to neighboring node in the path for the further transmission so that it can be reached to the particular destination. Each node work as a relay agent to route the data traffic. As MANET is dynamic in nature so it is accessible to all the users it may be a legitimate user or the malicious node which reproduce the data or attack in the network. [3]

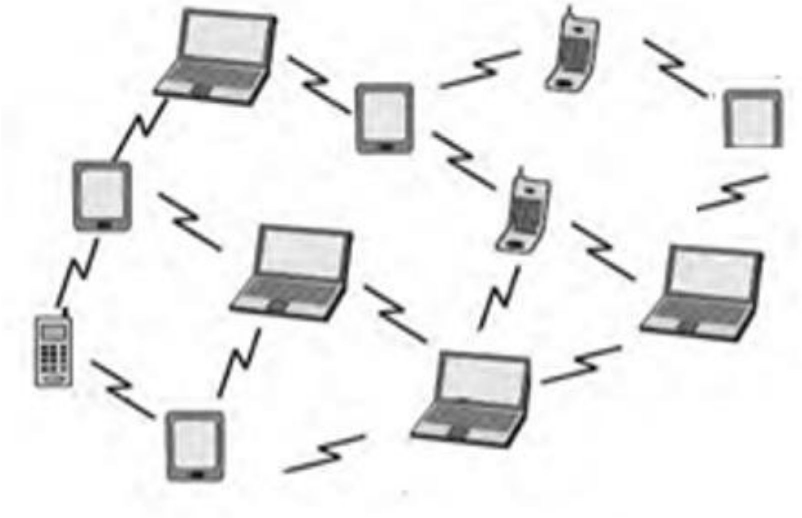


Fig.2 Mobile Ad-hoc Network

2.2.2. Characteristics of MANET

The mobile adhoc network are self organizing, any can join or leave network at any point of time. The communication is carried out by relaying the packets to the neighboring nodes. The characteristics are classified as follows:

A. No Centralized Administration – Each node in the MANET has its own communication capabilities for forwarding the data traffic over the network and adjusts according the topology.

B. Flexibility- MANET enables fast organization of the ad hoc network. When a node is to be associated with the network it should have the limited wireless communication range i.e. such node which can be available nearby.

C. Peer to peer connectivity of the nodes- In MANET the nodes neighbor to each other forms a set for communication to which request response messages are flooded.

D. Resource constraints- The node may have limited energy so this may limit the functionality of the network.

E. Dynamic Network topology-Nodes move freely in the network .A node discovers the service of a nearby node using the service discovery protocol. They may have unidirectional or bidirectional links.

F. Heterogeneous Nodes – In the MANET architecture any node can participate in forwarding thee data packets, the node can be PCs, smart phones, tablets, embedded systems.

2.2.3. Challenges in MANET

A. **Change in Network Topology –** Since the network is self organizing and nodes move freely in the network so the topology changes very frequently and randomly at any point of time. This cause problem in routing the packet to the intended recipient. The position of the node is dynamic so once the route is known it can’t be said that whether the node will still remain for the couple of minute. [4]

B. Limited Power Capacity- As nodes are mobile they are not fixed with any hardware, they are available in different types and many of the nodes rely on the battery. The transmission, reception, routing, retransmission all these functioning consume power. So this is a drawback in MANETs as if in between the relay of packet the node lost its battery then it will be of no use and the packet transmission may be suffered.

C. **Limited Wireless Bandwidth -** Wireless links have low capacity as compared to the hardwired links.

D. **Detection of Devices –** The detection of the nodes is monotonous in the distributed environment where movement of the nodes is random. Their identification and existence in the network needs dynamic updates to make possible the selection of optimal route

E. **Limited physical security –** The wireless network is more prone to attacks as compared to the wired network because of its wireless medium, which is accessed by both the legitimate users and malicious attackers. There are possibility of the spoofing, denial of service attacks, black hole attack, grey hole etc.

F. **Scalability-** It is defined as do the mobile adhoc network work at satisfactory level and achieve the quality of service parameters in the case when the number of the nodes increases in the network.

2.2.4. Applications

As Mobile adhoc network is infrastructure less and dynamic network so it is gaining popularity. Adhoc networks can be established anywhere where the nodes have connectivity with other nodes and can join and leave the network at any point of time. The applications of the MANET are as followed:

A. Military- Using the adhoc network the communication among the soldiers, vehicles, and headquarters of military can be possible as this area do not have the proper establishment of the base station for the communication.

B. Emergency Services- Ad hoc can be used in emergency operations such as, search and rescue, recovery from disasters like fire, flood, volcano eruption, earthquake, etc. Information is relayed from one rescue team member to another over a small portable device.

C. Commercial environment- Ad hoc networks can autonomously link an instant in business so as to share the daily updates of office, in vehicular management to manage road traffic and accidents, inter-vehicle communication.

2.2.5. Classification of Routing Algorithms

The mobile adhoc networks are based on dynamic topology that changes randomly due to the mobile nature of the nodes. The node behaves like the router and does the task of node discovery, routing of the packet, maintenance of the information to relay the packets. This overall functioning in MANET is to be performed by the node itself only so the routing protocol in MANET is different from the conventional protocols of the wired network. So the new node broadcast message to its neighbor and make them aware about its presence in the network. The node also listens for the broadcast messages from its neighbor. When every node in the network participates in this way, the nodes can be selected to route the packet to destination. The routing protocols in MANET are categorized as:

1. On Demand Routing or Reactive Routing algorithm
2. Table Driven or Proactive Routing algorithm
3. Hybrid Routing Algorithm

2.2.5.1. On Demand Routing or Reactive Routing algorithm

These protocols do not maintain the routing information at the nodes if they are not the communicating entities. The route calculation is done only when the node wants to connect to the destination node, for this it broadcasts route request packet to the neighboring node in the network which further broadcast packet. When the destination is found it sends route reply message via the shortest path. The algorithms under this category are Ad-hoc On demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR), and Temporally Ordered Routing (TORA)

2.2.5.1.1. Ad-hoc On Demand Distance Vector Routing

This MANET routing protocol is based on the distance vector algorithm, in which each node knows about its neighboring node and maintains its own routing table. Every node exchanges its routing table with the neighboring node periodically so that every node may know the useful route.

AODV is capable of unicasting and multicasting. It is based on demand algorithm i.e. the routes are maintained as long they are needed by the communicating nodes.
The terms [5] which are commonly used with respect to the AODV protocol are defined as:

A. Active Route- A routing table contains entries with a finite metric called as hop count which is used for route establishment. The route is said as inactive if it has infinite value in its hop count field. So in table only active route entries are maintained.

B. Broadcast - It means the packet is forwarded to all the nodes in the network and enables flooding of packet in the entire network.

C. Forwarding node - A node which agrees to forward packets destined for another destination node, by retransmitting them to a next hop which is closer to the unicast destination along a path which has been set up using routing control messages.

D. Forward route - A route set up to send data packets from a source to a destination. The RREQ route request message is used for forwarding the packet

E. Originating node - A node which initiates an AODV message which is the processed and possibly retransmitted by other nodes in the ad hoc network. For instance, the node initiating a Route Discovery process and flooding the RREQ message is called the originating node of the RREQ message.

F. Reverse route- A route set up to forward a reply (RREP) packet back to the source from the destination or from an intermediate node having a route to the destination.

The AODV uses control messages for the route discovery and maintenance which are exchanged between the communicating entities. These messages are described as follows:

A. **Route Request Message (RREQ) -** Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.[6]

B. **Route Reply Message (RREP) -** A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

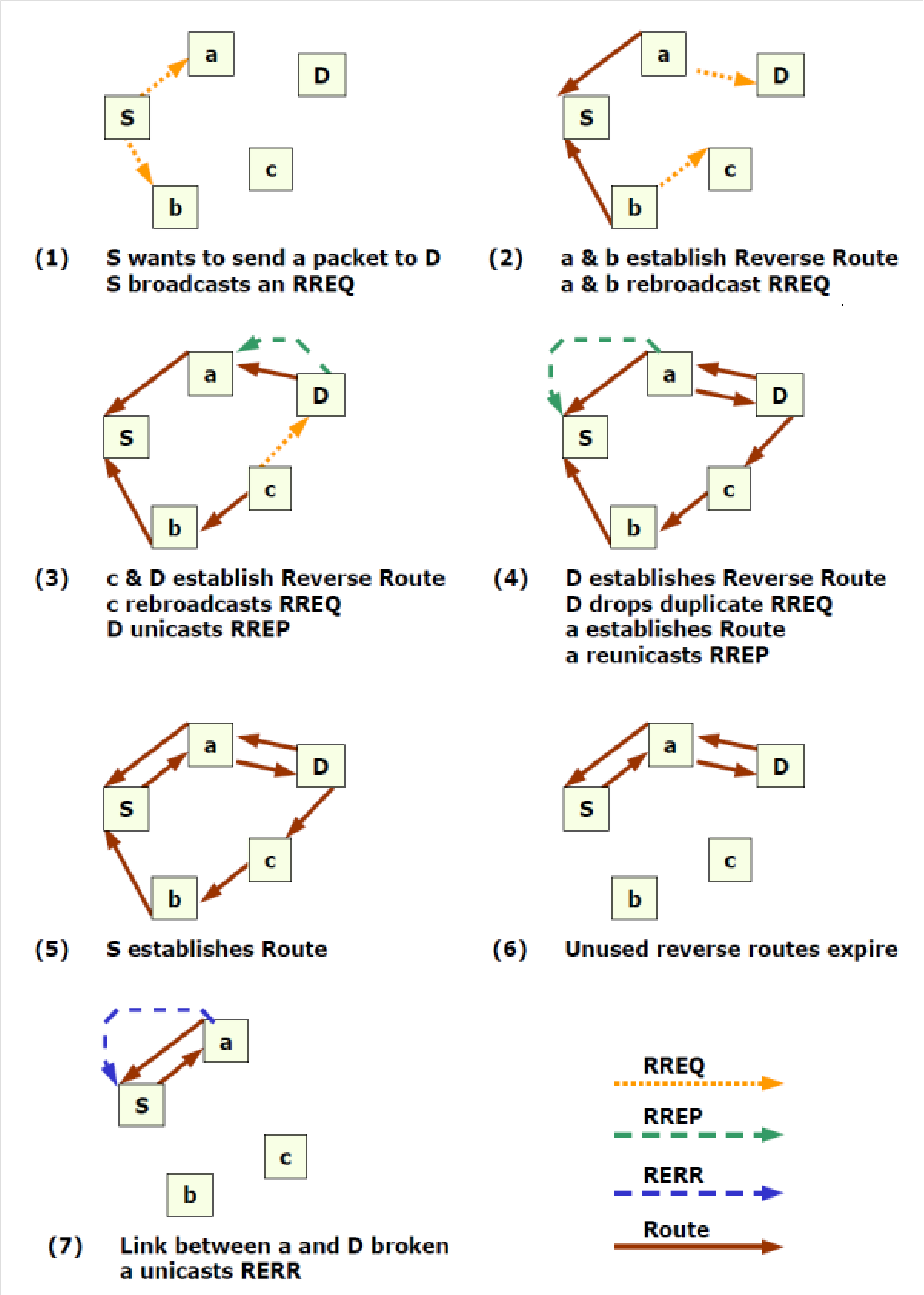
C. **Route Error Message (RERR) -** Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down.

Route Establishment in AODV

The path in AODV protocol is build using the route request /route reply message exchange. When a source node desires to route message to the destination but it doesn't have route to reach to the nodes. It broadcast the route request (RREQ) packet in the network. The neighboring node receives the packet and set up backward pointers to the source node in the routing table. A node receiving the RREQ may send the route reply (RREP) back to the source node if it has a path to the destination node or itself is a destination node. The node keep track of the RREQ's source IP address and broadcast ID. If the node receives a RREQ message which it had already processed then RREQ message is simply discarded and not further propagated.

As the RREP message is received by the source node, it starts forwarding the packets to the destination on the route with smaller hop count. As long as the data packets are transmitted by source to the destination the route remains active. Once the source stops transmission of data packet, the link will terminate and entries are also deleted from the routing table of intermediate nodes. In case of link break a route error (RERR) message to source node informing the unavailability of destination. After receiving this message if source still wants to set up the route, it can reinitiate route discovery.

The figure 2 explains the route establishment [7] in AODV protocol in this the source node S wants to send data packet to the destination D. Each diagram describes the steps of forwarding the packets from source 'S' to destination 'D'.



(1) S wants to send a packet to D
S broadcasts an RREQ

(2) a & b establish Reverse Route
a & b rebroadcast RREQ

(3) c & D establish Reverse Route
c rebroadcasts RREQ
D unicasts RREP

(4) D establishes Reverse Route
D drops duplicate RREQ
a establishes Route
a reunicasts RREP

(5) S establishes Route

(6) Unused reverse routes expire

(7) Link between a and D broken
a unicasts RERR

Fig 3 Route Establishment in AODV protocol

2.2.5.1.2. Dynamic Source Routing Protocol

DSR is similar to the AODV protocol, it also establishes the route on demand when required. It uses source routing instead of relying on routing tables at each intermediate node. In the source routing, source node itself have to specify the path to reach to the destination node. All the routing information is maintained at mobile nodes. It performs route discovery and route maintenance. The route is established by flooding the route request packets in the network, when the destination receives this packet, it response back to source by sending the route reply message. This reply message consists the route traversed by route request message.

2.2.5.2. Table driven or Proactive Routing Algorithm

These protocols regularly maintain the updated information about the nodes in the network. Every node knows about the other nodes in advance and thus the view of whole network is within the reach of each and every node. The routing information is maintained in the routing tables. Whenever the network topology changes, these tables are updated. The example of protocols under this category is:

1. Optimized Link State Routing Protocols (OLSR)
2. Destination Sequenced Distance vector routing (DSDV)
3. Cluster Gateway switch Routing Protocols (CGSR)
4. Fish eye State Routing Protocol (FSR)
5. Wireless Routing Protocol (WRP)

2.2.5.2.1. Optimized Link State Routing Protocols (OLSR)

This protocol inherits the property of link state routing algorithm. The routes information is exchanged periodically to maintain the topology information at each node. OLSR is an optimization on link state routing algorithm, it reduces the size of the information sent in the control messages and also the number of retransmission to flood these packets are also decreased with the use of multipoint relays in the network.[8] OLSR uses two types of messages HELLO message and topology control(TC) message to search node and then to distribute the link information to all the nodes in the network The node use this topology information to calculate next hop destinations for all other nodes in the network based on the optimal shortest path route.

The OLSR protocol uses Hello message to discover 2-hop neighbor information and elect the set of multipoint relays (MPRs). The MPR are selected such that there exists a path to each of its two hop neighbors. These MPR nodes then forward the TC messages.

OLSR Working

OLSR disseminate the network topology information by flooding the packets all the way through the network. The received packets are flooded in such a way that each node retransmits the packet. These packets contain a sequence number so as to avoid loops. This sequence number is registered with the receiver node in its table to avoid further retransmission of packet and this also ensures that packet is retransmitted only once. In this way the duplication or loops of retransmissions of the packets are reduced. Only MPR nodes broadcast route packets. The nodes within the network maintain information of MPR nodes. MPR nodes are selected with in the vicinity of the source node. The selection of MPR is based on HELLO message sent between the neighbor nodes. Routes are established, once it is done the source node that wants to initiate transmission can start sending data.

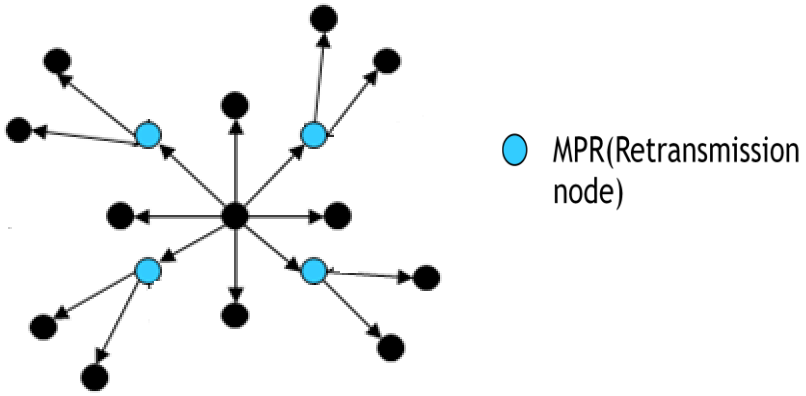


Fig. 4 Multipoint Relays in OLSR

2.2.5.2.2. Destination Sequenced Distance vector routing

The Destination Sequenced Distance Vector Routing (DSDV**)** is adapted from RIP, routing information protocol. In this, each mobile node of an ad hoc network maintains a routing table, listing all available destinations, the metric and next hop to each destination and a sequence number generated by the destination node. These tables are stored in each mobile node and using the routing table, the packets are transmitted between the nodes of an ad hoc network. Each node periodically updates its table or whenever new information is available so to keep the data consistency. When change in network topology is detected, each mobile node advertises routing information using broadcasting a routing table update packet. The update packet starts out with a metric of one to direct connected nodes. This indicates that each receiving neighbor is one metric (hop) away from the node. [9] After getting the update packet, the neighbors update their routing table, increment the hop count by one and retransmit update packet to the neighbors of each of them. This process is repeated until all the nodes in the network received the update packet with the corresponding metric. When the routing tables are updated the data packets are forwarded to the intended recipient

2.2.5.3. Hybrid Routing Protocol

These protocols are based on both the reactive and proactive protocols. The routes are established initially proactively and then serve the data to other nodes that are activated, through reactive flooding. The Zone Routing Protocol is based on this type of protocol in which the network is divided into zones and uses different protocols in different zones i.e. two different protocols are used in between inter and intra zone. The proactive protocols are used for route establishment within the intrazone and for information exchange among zones reactive protocols are used. The source node forwards a route request message to the border nodes of its zone, containing its address and sequence number. A Border node checks its zone for the destination. If the destination is not within its boundary, it attaches its own address and forwards the route request packet to its own border nodes. When destination node is found it sends back the route reply packet on reverse path back to source. The source then uses the saved path in reply packet to send packets to the destination.

2.2.6. Security Issues in MANET

Security is the adoption of such policies to prevent unauthorized access, misuse of information, attacks from malicious users or denial of network resources. A secure network is that which possess the following attribute:-

1. Confidentiality- To keep the information secret from the unwanted access. It is necessary to maintain the information safe and secure from the attacks.

2. Integrity of Message – To keep the accuracy and consistency of the data during its transit from node to node. So that the data is not modified by the unwanted access.

3. Authorization –it specify the privileges and the permissions of the entity participating in the communication over network.

A mobile adhoc network consists of a set of mobile nodes which move around in the network area. These nodes rely on each other for forwarding the packet, routing of control packets, maintenance of the links etc. In the wired network these functions are carried out by the dedicated nodes only but in the MANET the available nodes are responsible to perform these tasks. This causes more concern on the security issues in ad hoc network to achieve confidentiality, integrity and availability of data in the network. MANET suffer from security attacks because of its features like open medium, dynamic change in topology, lack of central authority for the management and monitoring, distributed operation , lack of infrastructure. Due to various factors the routing protocols in MANET are susceptible to various attacks. The network consists of heterogeneous nodes which can be a malicious node, whose intention is to attack the network and reproduce the false information. The attack can be classified as an active attack or passive attack.

2.2.7. Limitations of MANET

In MANET the nodes are free to move randomly in the network area. The MANET is self configurable network, open medium and there are other limitations which make MANET open to various attacks. The reasons are stated below:

2.2.7.1. No Central Authority Control

As MANET is self configured network, nodes join and leave the network when desired. Each node works as a relay agent in forwarding the packets and the exchange of message is done without any centralized control. This causes MANET more susceptible to attacks. The node in the network can be malicious node which is connected to other node as a legitimate user, because there is no mechanism to take care of the system. Without central administration any node can join the network and thus attack in the system. In this case the detection and monitoring of the traffic becomes difficult when the adhoc network is large and topology is dynamic.

2.2.7.2. Availability of Nodes

As in MANET for communication the nodes are needed to be available all the time so that the information can be relayed over such path. As nodes are mobile they are not fixed with any hardware, they are available in different types and many of the nodes rely on the battery. The transmission, reception, routing, retransmission all these functioning consume power. So this is a drawback in MANETs as if in between the relay of packet the node lost its battery then it will be of no use and the packet transmission may be suffered.

2.2.7.3. Less Secure Boundaries

MANET network is vulnerable to passive, active attacks and data integrity may loss. As the links are open to various attacks. Attacks on the link interface, information exchange between the nodes and the link termination between the nodes. The spoofing of the one’s identity, data tampering, leakage of confidential information, impersonation attacks etc. are some of the harm that is caused by the malicious node.

2.2.7.4. Problem of Scalability

In the fixed network the number of the nodes is known already and the network topology is designed in the beginning phase of establishing the network. While in the MANET architecture is not fixed, the nodes are mobile and topology changes. The number of nodes is unpredictable so adhoc network must be scalable and adaptable to all the changes occurred due to its mobile feature.

2.2.8. Classification of attacks in MANET

Due to various factors the routing protocols in MANET are susceptible to various attacks. The network consists of heterogeneous nodes which can be a malicious node, whose intention is to attack the network and reproduce the false information. The attack can be classified as an active attack or passive attack.

The figure shown below lists all types of attacks at each layer in MANET[10] These attacks at each layer are discussed as follows.

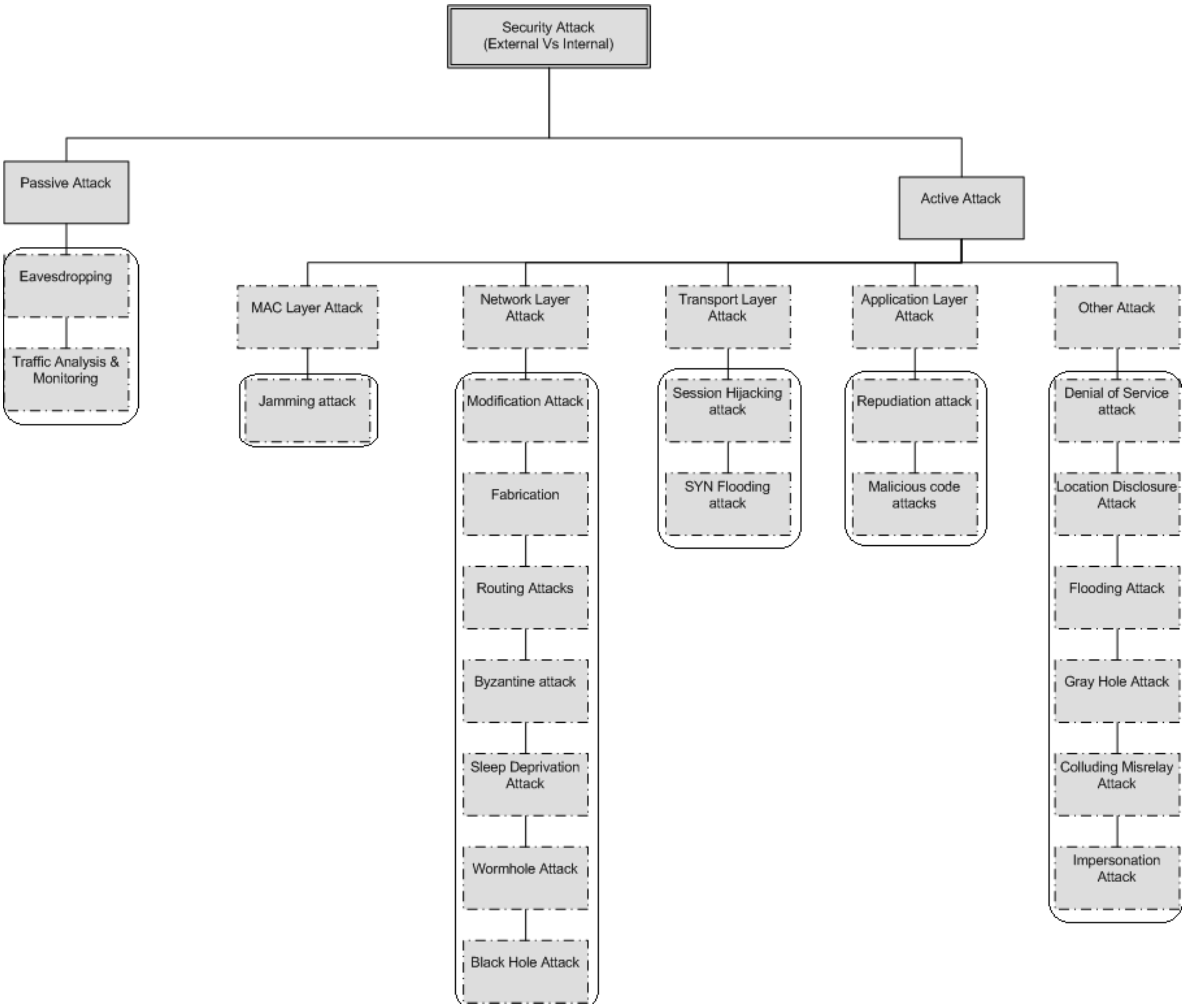


Fig. 5 Classification of Attacks in MANET

2.2.8.1. Passive attack

It analyze network traffic i.e. identify the communicating entities, monitors message exchange between them ,decrypt weakly encrypted data, capture authentic data such as passwords, public key ,private key, that is exchanged over the link. From these messages, the inferences are drawn by the attackers regarding the messages and thus steal the information without the client or user information

Eavesdropping

It means to listen the confidential information without the one’s consent. The attackers in the network do sense the network when any secret data is shared between two communicating entities.

The information can be passwords, encrypted keys, public and private keys. These data are to be kept secret from the unauthorized access.

Traffic Analysis & Monitoring

In this type of attack the susceptible node monitors the packet transmission information as source and destination addresses. The messages which are exchanged between the nodes are traced by the malicious node and the data can be replicated, saved, or misuse. The messages are intercepted and useful and secret information is deduced from the patterns. The frequency and timing of the network packets are monitored regularly by the attacker node and in this way secret data is accessed.

2.2.8.2. Active Attack

In this the intruder attempts to break into the system, insert infected code, or steal information, destroy or reproduce it, thus disrupting the normal functionality of the network. It is classified into external attack and internal attack. The nodes which are not the part of network and attack on the data such type of attack is categorized as external attack while in the internal attack, the malicious node is an entity of internal network that propagates the false information.

2.2.8.2.1. MAC Layer Attack

Jamming attack

The attack lies in category of Denial of service attacks. In mobile ad hoc networks the mobile nodes communicates via wireless medium. So the radio signal can be blocked or interfered by an attacker node, which may result in corruption of message or data loss. The jammer can prevent a real traffic source from sending the packets or it may block the destination node to receive the packet. The jammer can interfere with other wireless communication in various strategies [11]. These can be constant, deceptive, random or reactive jammer. In all these line of attack the motive is to block the transmission of packets and thus to make system vulnerable.

2.2.8.2.2. Network Layer Attacks

Modification Attack

The malicious node in the network modifies the content of the control messages. The control messages mainly like RREQ, RREP and RERR use for establishing the shortest and optimal path between the node and reporting the error if the error occurs during the transmission of the packets. The route information like sequence numbers, hop count, life of a packet, source and destination address etc. are carried out by the control packets. The attacker simply modify these information and make the system infected, misleading the intermediate node. The malicious node changes the route information in RREQ message i.e. when the packet contain the route request , the node can take it to such nodes which do not exist in the network. The route reply message is also generated from such nodes and once the route is established with such malicious node the data packets are drained out from the system and thus affecting the system. Malicious node intends to perform this attack to affect the network performance, or its intension may be selfish, it does not want to route the packet. This attack can be performed by adding a number of virtual nodes and decreasing hop count field of the RREP messages.

Fabrication

The modification attack modifies the content of the packet while in the fabrication attack the attackers introduce their own packets to mismanage the functionality of the network operations. They inject huge packets in the networks which do not contain the relevant information .These attacks are against the authentication, access control and authorization ability .The examples of the fabrication attacks are inserting messages into the network, replay the messages, spoofing the network services, taking the identity of another host and producing the false information

Routing Attacks

The Manet routing protocols are vulnerable to the routing attacks. In this type attack the working of protocol is affected by the malicious node. New false routes are created by the attacker due to which the original correct route working is prevented and false information is propagated in the network. In reactive protocols the routes are created when required, while in proactive the routes are discovered and maintained in the routing tables. As routing tables are to be maintained for storing the route information so the attacker can simply attack on the stored information and corrupt it. The various attacks on the tables can be from the following listed:

a. Routing Table Poisoning - in such type of attack the genuine route update packet are poisoned. Then routing is performed using this false information which may result in the congestion and falsified information exchange.

b. Routing Table Overflow - A malicious node advertises routes to nonexistent node. The attacker tries to create enough routes to prevent new routes from being created. An attacker floods excessive route information to overflow victim’s routing table

c. Route Cache Poisoning- A node can overhear any packet, may add the routing information contained in that packet header to its own route cache, even if that node is not on path.

d. Packet Replication – The node replicate the packets which are old and forward such packets unnecessary in the network causing the congestion , consuming the bandwidth , producing fake information and make network malfunction.

Byzantine attack

A attack in which the set of nodes are compromised in such a way that the malicious and false node cannot be directly detected as the compromised nodes cooperate among themselves and perform the malicious activities in the network.[12] The compromised nodes act as legitimate node and destroy the network untraceably, generate and advertise false information about the network links which does not exists, dropping the packets, forwarding packets to the unintended recipient, flood false routing updates. This results in distraction and deprivation of the routing services.

Sleep Deprivation Attack

Sleep Deprivation attack is one of the type of Denial of Service Attacks, which affects only nodes, especially the handheld devices that have limited resources, as they are battery operated. Mobile nodes prefer to stay at the sleep mode, when they are not used. In a period time, attacker can propagate some control messages through the network, in which other nodes are interested. Other nodes pass to the operation mode from the sleep mode and start processing these unnecessary packets until their batteries completely run out. [13]

Wormhole Attack

In wormhole attack an attacker records packets at one location in the network and tunnels them to another location from where these packets are retransmitted into the network. The routing is interrupted when routing control messages are tunneled. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multihop route, for example through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to it, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole.

Black Hole Attack

In black hole attack, a malicious node uses its routing protocol to advertise itself for having the shortest path to the destination node it wants to intercept. The malicious node advertises availability of fresh routes to the other nodes irrespective of checking its routing table. In this way attacker node indicate the route availability as reply to the route request messages and thus capture the data packet and retain it. In protocol which is based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it’s up to the node whether to drop all the packets or forward it to the unknown address

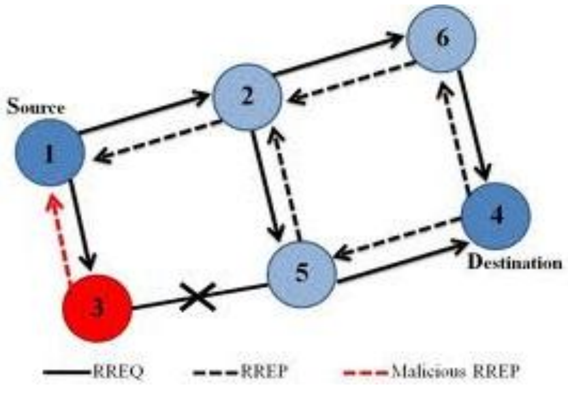


Fig 6 Black hole attack

2.2.8.2.3. Transport Layer Attacks

Session Hijacking attack

With the session hijacking the spoofer gain access to information and services illegally. At the transport layer when TCP sessions are established, the attacker spoofs the IP address of the victim, determine the information which is expected by the destination and then performs the attack on the victim. Thus the attacker pretends to be the victim node and continues session with the targeted node. [14] The attacker sends infected session data, and node A acknowledges the receipt of the data by sending an ACK to node B. The node B is expecting ACK packet with different sequence number so now it tries to resynchronize with node A. Thus the cycle goes on and on and ACK packets pass to and fro between the nodes, thus causing ACK storm.

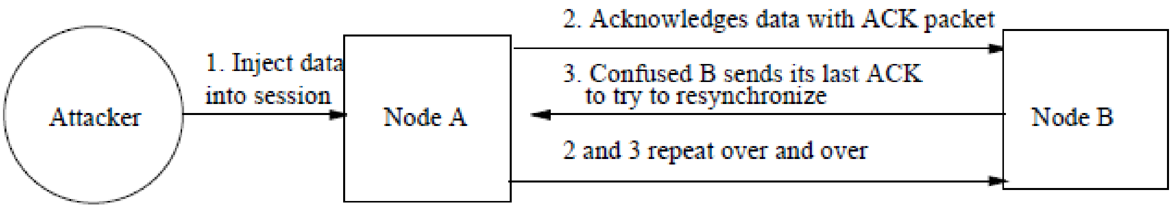

Attacker
1. Inject data into session
Node A
2. Acknowledges data with ACK packet
3. Confused B sends its last ACK to try to resynchronize
2 and 3 repeat over and over
Node B

Fig. 7 Session Hijack attack

SYN flooding attack

The attacker creates a number of half opened connection with the victims node, but never completes the handshaking process to open the connection. The three way handshake allows the communicating entities to establish the connection. During the attack the malicious node sends the SYN packets to victim node and spoofs the addresses from SYN messages which are returned back. Then the victim sent SYN –ACK packets as it receives the SYN packet. Now the victim waits for the response i.e. ACK from the node and thus the attacker left the victim in an half open connection state.

2.2.8.2.4. Application Layer Attacks

Repudiation attack

To keep information secure the techniques are to be used at each and every layer in the network. The repudiation attack refers to a denial of participation in all or the part of communication. For example a selfish person could deny conducting an operation on some services provided by the credit card system in bank or the user decline any on –line transaction in bank.

Malicious code attacks

Malicious code, such as viruses, worms, spywares, and Trojan Horses, can attack both operating systems and user applications. This malicious code generally can spread them in the entire network and cause the user machines or devices and networks to slow down or even break down the functioning of the system. In MANET, an attacker can produce similar attacks to the mobile system of the ad hoc network. The control packets may carry sensitive data which can be garbled by the attacker.

2.2.8.2.5. Other Attacks

Denial of Service attack

A DoS means making the network or the machine, device inaccessible to its intended users.DoS attack is achieved by attacker by flooding the targeted node with traffic or sending such malicious information which triggers into a crash. Thus the legitimate user is deprived from the services or resources they expected. The attacker injects a number of the junk packets into the network resources and these packets overspend a significant portion of network resources and bring in the wireless channel contention and network contention in MANET. The attacks which fall in this category are sleep deprivation and routing table overflow. The overflow causes attacks on the routing table which leads to the creation of the routes to the nonexistent nodes. The examples of DoS attacks are flooding the network and preventing the intended users from receiving the network traffic, disrupt the connection between two devices thus the service access is prevented.

Location Disclosure Attack

The location information such as a route map, topology are gathered by the node. The information related with the location of nodes or network architecture is disclosed by the attacker. The leaked information is then accessed by the malicious nodes for the further attacks.

Flooding Attack

The attacker drain the network resources as bandwidth and consumes the node‘s resources like battery power or to disrupt the routing operation to degrade the network performance. The route request messages, hello messages are forwarded by the malicious node to all the nodes in the network. So when the route reply messages are generated by these nodes in reply to route request message with no one to receive the message.

Gray Hole Attack

This attack leads to the packet drop, the node first agree to forward the packets and then fails to forward it. This attack occurs in two phases .First the attacking node behaves properly as a legitimate node and replays true RREP messages to nodes that sends RREQ messages. In this way the node agree to send over the packet to the recipient. [13]After agreeing on this the attacker node just drops the packets to launch a Denial of Service attack. Again the neighbor node wants to establish the connection through the attacker node. The attacking node establishes a route, sending RREP messages. This process goes on until the malicious node succeeds in attacking the node. This attack is also called as routing misbehavior attack. As the node misbehaves with other nodes by dropping the packets, overloading the nodes, consumption of battery, network resources. A gray hole attack may exhibit different behavior it may drop selective packets and forward other packets.

Colluding Misrelay Attack

The packets are modified or dropped by a multiple number of attackers who work in collusion to disrupt the routing operation in MANET. The first attacker forwards the routing packets as usual to avoid detection by the node. The second attacker drops or modifies these routing packets

Impersonation Attack

The attacker does the address spoofing, device cloning, and unauthorized access and replay attack. The device cloning is the reprogramming of a device with the hardware address of the device. This can be done for the duration of one frame, which is termed as spoofing. [10]The attacker thus gains the identity of another node and produce packets using its identity.

3. NETWORK SIMULATOR DETAILS

3.1. Network Simulator (NS) Introduction

NS is an event driven simulator developed at the University of California Berkley, which consist of many network objects such as application, protocols, and traffic source behavior. The NS is a part of software of the VINT project [15] that is supported by DARPA since 1996.This simulator provides study of the dynamic nature of communication network in wired as well as wireless network .NS2 support many protocols and user can also specify the protocols due to which it is flexible and modular in nature.

NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism (i.e., a backend) of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a frontend). The C++ and the OTcl are linked together and formed TclCL.Like in the C++ there are objects, in OTcl the variables are referred as handle. In the OTcl a handle works at front end which interacts with the users and other OTcl objects. A large number of C++ of objects are predefined in NS2. These C++ objects are used to set up a simulation using a script written in TCL.

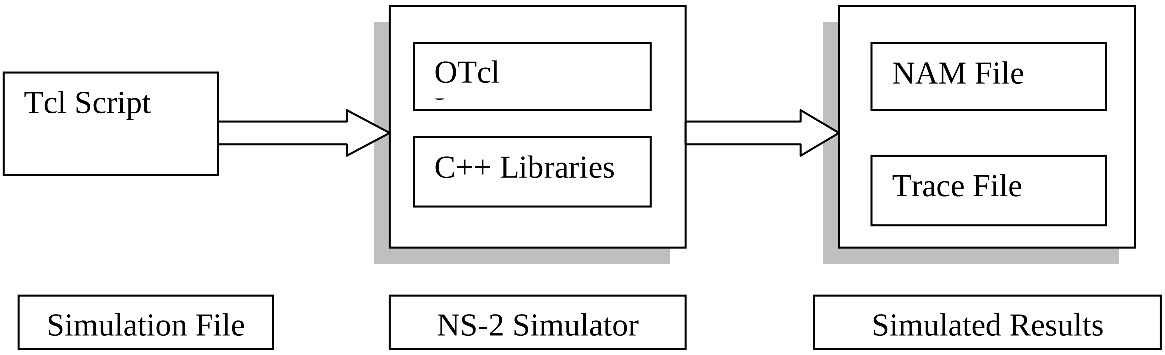


Fig. 8 Network Simulator Architecture

As shown in figure 8, a Tcl script written by a user is interpreted by simulator. After simulation NS creates two analysis reports simultaneously. The output can be either text based or animation based simulation. The interpretations of these results are done with the help of the tools. One of which is Network Animator (NAM) file which display the visual animation of the simulation. The other is the trace file that consists of the behavior of all objects in the simulation. The trace file displays the output in a text format, in which each label has a meaning. Both of these files are created as output of the simulated work. For the analysis of a particular behavior of the network, user can extract the relevant information from these files and transform it to more conceivable presentation. [16]

3.2. Tcl Language in NS

Short for Tool Command Language, TCL is an interpreted programming language developed by John Ousterhout at the University of California, Berkeley. It is a dynamic programming language and has a wide range of usage, which mainly includes web applications, networking, administration, testing etc. Tcl is easy to deploy and can be extended easily with any of the platform. Thes language is fully compatible with programming language like C which makes it significant from the other. Also the Tcl libraries can be interoperated directly into C programs. The Tcl is used in designing the structure and topology for the network simulation. The designed architecture is easy to configure with the network parameters.

To simulate in NS2, a user needs to define a network scenario in the simulation script of TCL. This simulation script is an input to executable file ns. During the simulation the trace file is generated which provide the text based tracing or an animated tracing; both of these provide the packet flow information. For the analysis of the text based trace file an AWK program is used. NAM program is used for the animated trace file to by which the user can view the simulation using the animation program.

Need of two language- NS2 uses Tcl to create and configure a network and uses C++ for the execution of the simulation All C++ codes are compiled and linked together for the creation of an executable file. Tcl is an interpreter not a compiler. To make any changes in the tcl file is easy and can be done quick as compared to the file of C++. So by making Tcl script change the user can simulate and test as many as changes as he want. The NS2 thus comprises of both language and makes it significant.

In the simulation work the Network Simulator version 2.34 is used. The simulation is carried out for three different scenarios. First one is to analyze normal behavior of the working of ad hoc on-demand distance vector protocol. Second scenario is for the flooding attack in this a malicious node is inserted into the network which floods a large number of packets. In the third scenario a black node is inserted into the network which forwards the false packet and drops the packet. The methodology used for the simulation work is first to design the assumptions of the simulation. Second to implement, configure and run the simulation concepts. In the final step results are collected and analyzed various performance parameters for the simulated work.

4. SIMULATION OF BLACK HOLE ATTACK

4.1. Black hole Attack in AODV

The black hole attack is simulated in the AODV routing protocol is based on the reactive approach, the route between the nodes for the communication is established on demand i.e. whenever the node requires the route it broadcast a route request message in the network. In response to the route request a route reply message is forwarded by the intermediate node .This intermediate node work as a relay agent in forwarding the packet to reach to the destination and when this intermediate node work against the forwarding rules in the network which in turn causes performance degradation over the network.

When AODV protocol is used in MANET for the communication three types of control messages are used RREQ, RREP and RERR (Already explained in section 2). In general when the nodes communicate they are classified as source node, which want to send the data to the other node i.e. the receiver or destination node. [17]In between the source and destination there lies the intermediate node. To discover the path in MANET all the nodes work in cooperation with the help of these control messages. The AODV protocol uses the destination sequence number for each route entry, this sequence number provide loop free connection and is the shortest path. AODV also has feature of less bandwidth utilization, low processing, less memory overhead. The source node broadcast the RREQ message in the network .This RREQ message is propagated from the source and forwarded by the other intermediate nodes. The intermediate node then further broadcast this message to its neighboring node. This process continues until the packet is received by the destination or intermediate node. The route entry in the routing table must be a valid entry; means the entry stated in table must form below a threshold value. As the RREQ packet travels through the network, the hop count is increased by one at the intermediate node. If a RREQ message with same ID is received by the node then that packet is discarded.

When intermediate node or destination receive the RREQ message and has a fresh valid route to the destination, they create RREP route reply message and send it as a reply to that RREQ message. The node also saves the entry of hops count, source address and sequence number of the destination node. Afterwards the RREP messages are forwarded by intermediate node, these nodes update their routing tables, which is ACTIVE_ROUTE_TIMEOUT constant value of the protocol. With the help of the unicasted RREP message the route is chosen by the second packet to reach to destination.

The black hole attack in AODV protocol absorbs the network load and drops the packets. When a malicious node is added in the network scenario the node act as legitimate user and participate in the network where the packets are dropped or corrupted by this node. In the black hole attack the malicious node wait for the neighbors to broadcast route request control message .As it receive the RREQ message it send a false RREP packet with the modified sequence number. After receiving the RREP message the source assumes that node is having the fresh route for the destination node. [18]The source node discards the packets from the other nodes and start forwarding the packets to the malicious node. In this way the malicious node succeeded in taking all the routes towards it. It does not allow forwarding the packet anywhere. This is how the black hole attack is introduced in the AODV protocol.

4.2. Simulation of Black Hole Attack in AODV

The simulation is done using Network Simulator version 2.34.in the work done the black hole behavior in wireless adhoc network that uses AODV protocol is implemented. All the routing protocols in NS are installed in the directory. The changes are done in the source file named as aodv.cc and aodv.h. The simulated work shows the functioning of AODV protocol when works normally the implementation is done for 3, 5 and 10 nodes. The flooding is also performed on the protocol. A comparative study at different parameters like delay, routing overhead, dropped packet ratio is done when the AODV protocol function in a normal behavior and when the black hole node is introduced

For the simulation the network scenario is designed for the small number of nodes i.e. up to 10 nodes. The UDP connection is established between the nodes. UDP is chosen as no acknowledgement overhead is there in the network. The TCP requires the connection to be established with the help of three way handshaking and for each message sent there must be acknowledgment. CBR application is attached with the connection which generates the packets at the constant bit rate. The duration of the simulation is 150 seconds.

For the simulation following three scenarios are considered

A. In the **first scenario** the functioning of AODV w.r.t. simply routing protocol is considered. The numbers of the nodes on which the simulation is done and is tested are three, five and ten nodes. The positions of the nodes are defined manually in the scenario.

B. In **second scenario** the packets are flooded in the network on the nodes and the performance parameters are evaluated.

C. In the **third scenario** the black hole node is introduced in the network .This node drops the packet and make the network malfunction which in turn degrades the performance of the network. This black hole node also corrupts the packets which are passed on to the destination node from the source node.

The **TCL script** code snippet for the **simulation of MANET in NS2** is mentioned below

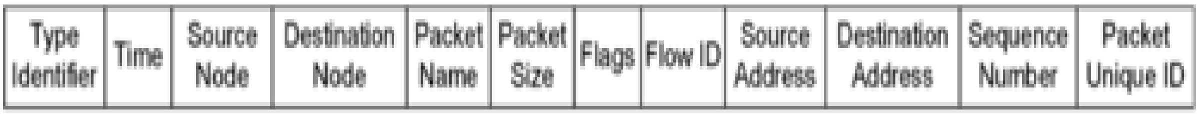
```
# Define options

set val(chan)          Channel/WirelessChannel    ;# channel type

set val(prop)          Propagation/TwoRayGround   ;# radio-propagation model

set val(netif)         Phy/WirelessPhy            ;# network interface type

set val(mac)           Mac/802_11                 ;# MAC type

set val(ifq)           Queue/DropTail/PriQueue    ;# interface queue type

set val(nn)            5                          ;# number of mobilenodes

set val(rp)            AODV                       ;# routing protocol

set val(x)             500                        ;# X dimension of topography

set val(y)             400                        ;# Y dimension of topography

set val(stop)          150                        ;# time of simulation end
```

```
# Provide initial location of mobilenodes

$node_(0) set X_ 5.0

$node_(0) set Y_ 5.0

$node_(0) set Z_ 0.0


$node_(1) set X_ 490.0

$node_(1) set Y_ 285.0

$node_(1) set Z_ 0.0

$node_(2) set X_ 150.0

$node_(2) set Y_ 240.0

$node_(2) set Z_ 0.0


$node_(3) set X_ 250.0

$node_(3) set Y_ 240.0

$node_(3) set Z_ 0.0


$node_(4) set X_ 100.0

$node_(4) set Y_ 70.0
```

```
$node_(4) set Z_ 0.0
```

This TCl script code snippet specifies the various parameters for the scenario. Various values are set for replicating the identified scenario like the channel type, propagation model, network interface, topography area, end of simulation time etc. The positions of all the five nodes are set manually at the design time of the simulation.

As the black hole node is inserted in the code and the scenarios are executed the trace file and network animator file are generated. [19]The general format of the trace string in the trace file is shown below:



Type Identifier	Time	Source Node	Destination Node	Packet Name	Packet Size	Flags	Flow ID	Source Address	Destination Address	Sequence Number	Packet Unique ID

Fig. 9 Trace String Format

Characteristics of all 12 fields of the trace string are as explained below :

1. **Type Identifier**:

- "+": a packet enque event
- "-": a packet deque event
- "r": a packet reception event
- "d": a packet drop (e.g., sent to dropHead_) event
- "c": a packet collision at the MAC level

2. **Time**: at which the packet tracing string is created.

3-4. **Source Node and Destination Node**: specify the source and destination ID of the object.

5. **Packet Name**: Name of the packet type

6. **Packet Size**: Size of the packet in bytes.

7. **Flags**: A 7-digit flag string which denote various values like congestion notification, priority, congestion action etc.

8. **Flow ID**: mention the type of flow

9-10. **Source Address and Destination Address**: the format of these two fields is “a.b”, where “a” is the address and “b” is the port.

11. **Sequence Number**

12. **Packet Unique ID**

This trace format is in general, the value in trace varies according to the type of the application used for the network and the trace level used, which can be IP trace, ARP trace, TCP, CBR, AODV trace. According to that the other values in the trace file are displayed, the trace file named as wireless trace is generated for the three nodes. The trace file snippet for the scenario is illustrated below:-

```
s -t 5.000000000 -Hs 0 -Hd -2 -Ni 0 -Nx 50.00 -Ny 50.00 -Nz 0.00 -
Ne -1.000000 -Nl AGT -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 0.0 -Id
2.0 -It cbr -Il 210 -If 0 -Ii 0 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0

r -t 5.000000000 -Hs 0 -Hd -2 -Ni 0 -Nx 50.00 -Ny 50.00 -Nz 0.00 -
Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 0.0 -Id
2.0 -It cbr -Il 210 -If 0 -Ii 0 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0

s -t 5.000000000 -Hs 0 -Hd -2 -Ni 0 -Nx 50.00 -Ny 50.00 -Nz 0.00 -
Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 0.255 -Id
-1.255 -It AODV -Il 48 -If 0 -Ii 0 -Iv 30 -P aodv -Pt 0x2 -Ph 1 -
Pb 1 -Pd 2 -Pds 0 -Ps 0 -Pss 4 -Pc REQUEST

s -t 5.000535000 -Hs 0 -Hd -2 -Ni 0 -Nx 50.00 -Ny 50.00 -Nz 0.00 -Ne -1.000000
-Nl MAC -Nw --- -Ma 0 -Md ffffffff -Ms 0 -Mt 800 -Is 0.255 -Id -1.255 -It AODV
-Il 106 -If 0 -Ii 0 -Iv 30 -P aodv -Pt 0x2 -Ph 1 -Pb 1 -Pd 2 -Pds 0 -Ps 0 -Pss
4 -Pc REQUEST
```

These lines of the trace file specify that the packets are send by the node0 as the value of –Hs is 0 (hop source).

The value –**Hd** = -2 denotes that the packet is broadcasted to all other neighboring node in the network. The value of node ID is shown by –Ni.

The parameters **- Nx**= 50.00,-Ny = 50.00 and –Nz = 0.00specify the location of the node 0 in the simulated area i.e. on x axis, y axis and on z axis. The value in field –Nl specify the layer at which the agent works.

The value of **–Nw** shows the reason of packet drop. In the above mention string it is blank as this is the start of the simulation process. When the simulation ends then the value “END” is mentioned in this field.

The values **–Ma,-Md, -Ms, - Mt** shows MAC level packet information like duration, source and destination Ethernet address and

Information at the IP trace level are denoted by the fields **–Is**(source address. Port number), **-Id** (Destination address. Port number), **-It**(packet type),**-Il**(packet size), **-If**(flow ID) **–Ii** (unique ID)

-P denotes packet specific information.

Using the network animator the simulation can be visualized. The simulation results in network animator for the 50 nodes are shown in figure 10. Here the node 1 is source node the location of the node is fixed .This node produces the flooding attack in the network. Initially the node is broadcasting the request message to all the nodes in the network.

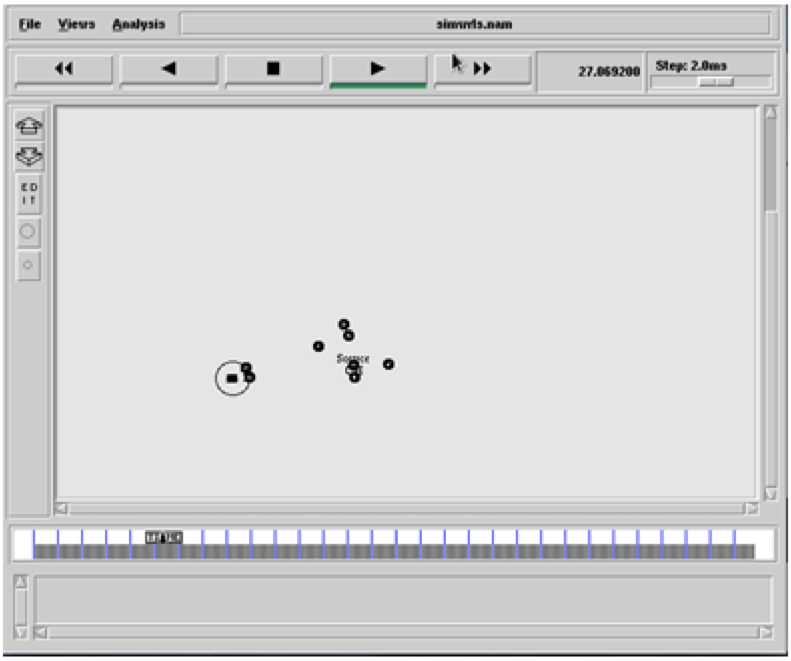


Fig. 10 Malicious Node is sending the request message

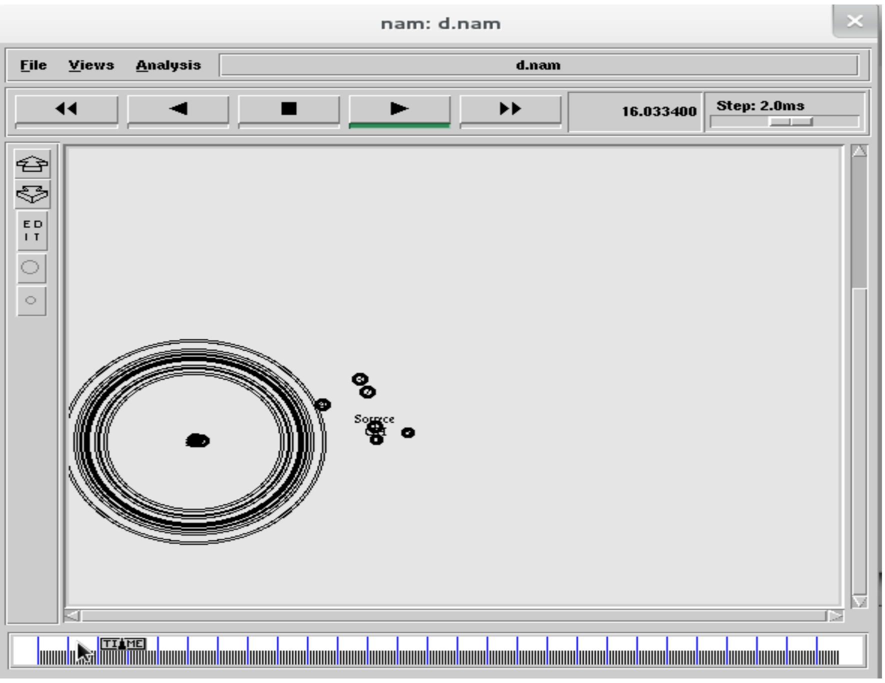


Fig.11 Malicious Node is flooding the message.

In the third scenario the black node is inserted in the network. The figure12 file shows the flow of message from the source node 1 to the destination node 3 via intermediate node2. In this node 0 is a malicious node which inserts false packet and drops the packet which are forwarded by intermediate node. The simulation is run for 5 seconds. After 1 second the malicious node gets active and start the transfer of the false packet in between the communication. The figure 13 and Fig 14 shows this mechanism where the malicious node inserting false data

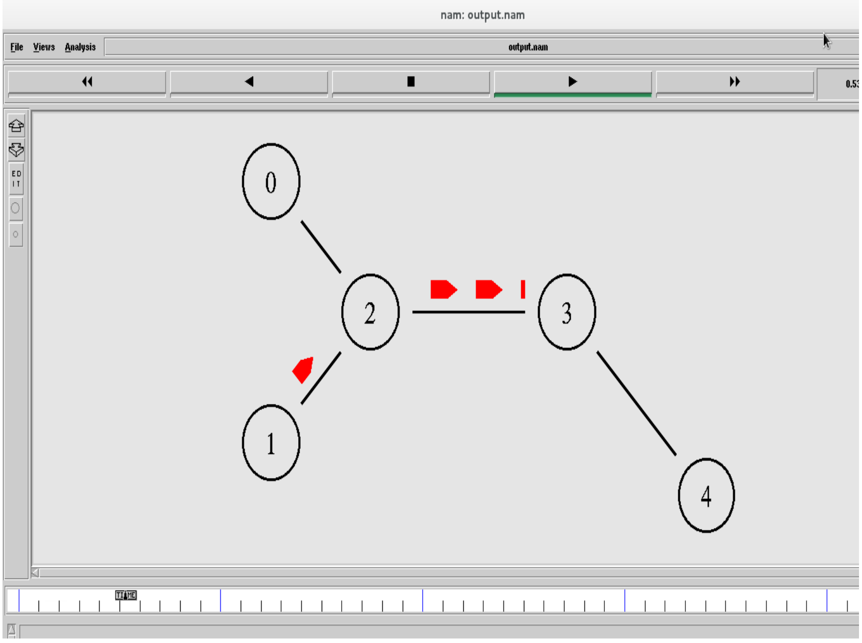


Fig.12 Node 1 sends data to Node 3

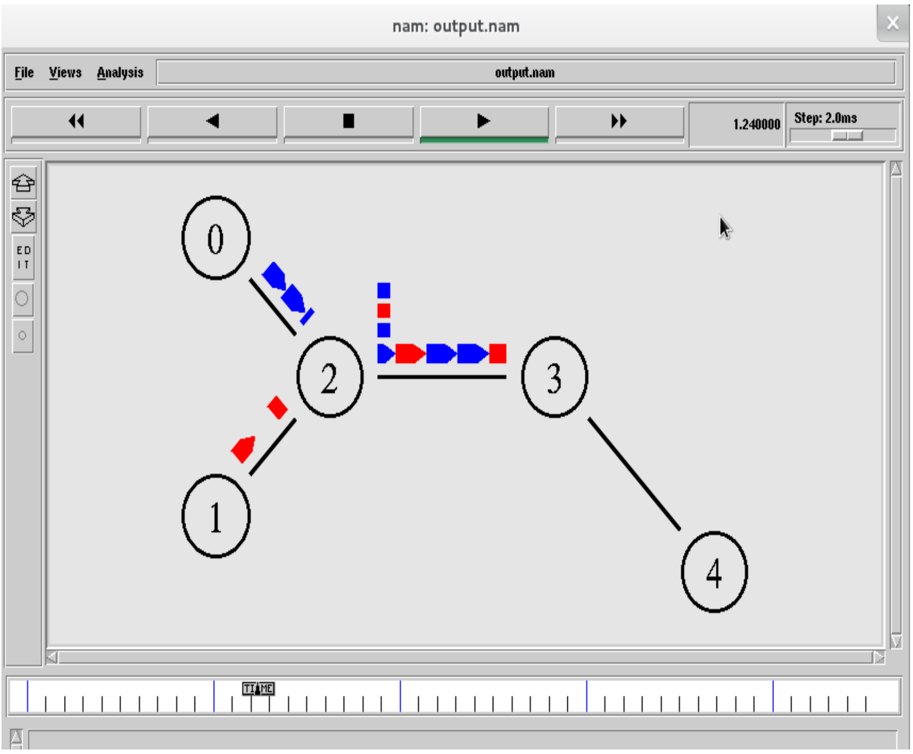


Fig.13 Node 0 inserting false data packets

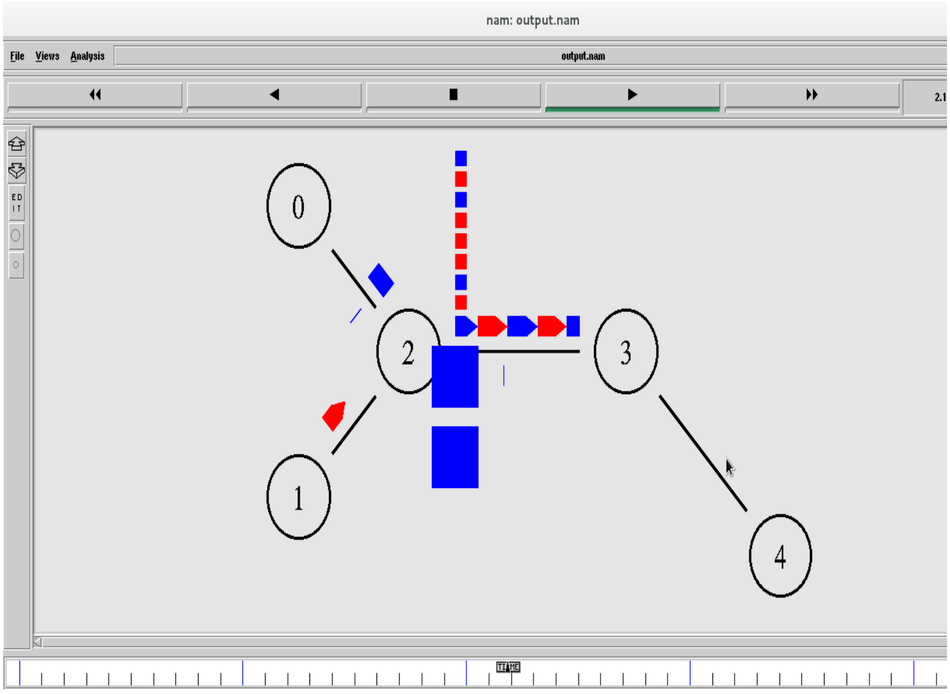


Fig.14 Node 0 inserts false packet and drop packets

4.3. Performance Analysis on Various parameters

The network is simulated in NS2 for the three scenarios. With first scenario the normal functioning of the AODV protocol is studied. In second scenario the network is flooded by a large number of packets and in the last (third) scenario a node which behaves as a black hole is inserted in the network. For the performance evaluation in the AODV protocol the simulation is performed in NS2. The work is carried out for three, five and ten nodes. The comparative study has been done based on the values of parameters (Packet Delivery Rate, Average Delay, Routing overhead and Dropped packet Ratio etc) which are calculated during the simulation. The characteristics of those parameters are mentioned below:

- Average Delay (in ms) it is measured as the time the packet is received minus the time the packet is sent.

- Packet Delivery Rate is the rate the packets are successfully received. This is equals to the total packets successfully received on the total number of packets sent. This performance metric gives an idea of the protocol performance of in terms of packet delivery.

- Routing overhead this means the total routing control packets are transmitted during the simulation time.

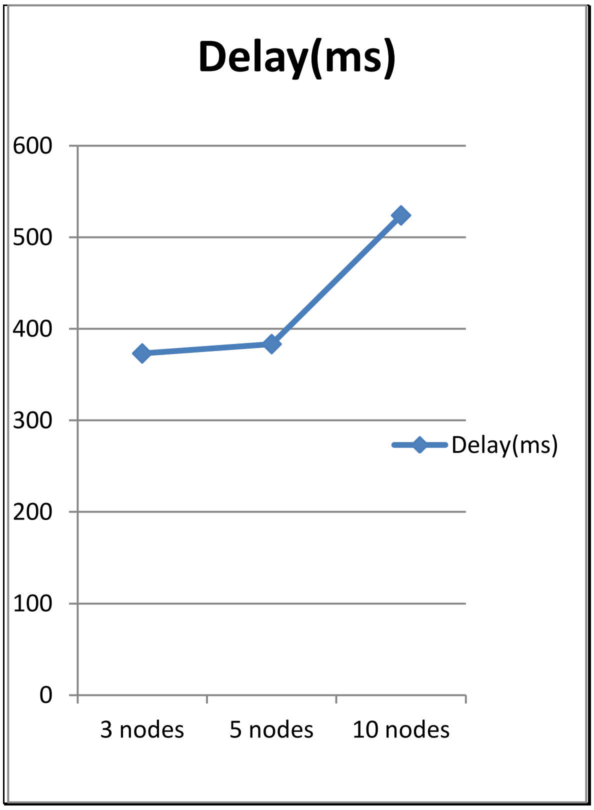
- Dropped packet ratio is the ratio of such packets that doesn’t reach the destination and dropped in the network during transmission.

These values are evaluated and thus the performance is analyzed in all these three scenarios. The value of delay is calculated in milliseconds, when there are 3 nodes, 5 nodes and 10 nodes in the network. The figure displays as the number of nodes are increased the delay in network also increases. The routing overhead specify the transmission of control packets i.e. route request, route reply messages in the network

Scenario I: Below tabular/graphical representation shows the comparative study for three, five and ten nodes for the above parameters w.r.t defined **scenario (A)** in the (section 4.2)**.**

Parameters/ Nodes	3 nodes	5 nodes	10 nodes
Delay(ms)	373.25	383.42	524.00
Routing Overhead (%)	0.03	0.12	3.97
Packet Delivery Rate (%)	50.90	41.24	16.12
Dropped Packet Ratio (%)	49.10	58.76	83.89

Table 1. Values when AODV works normally



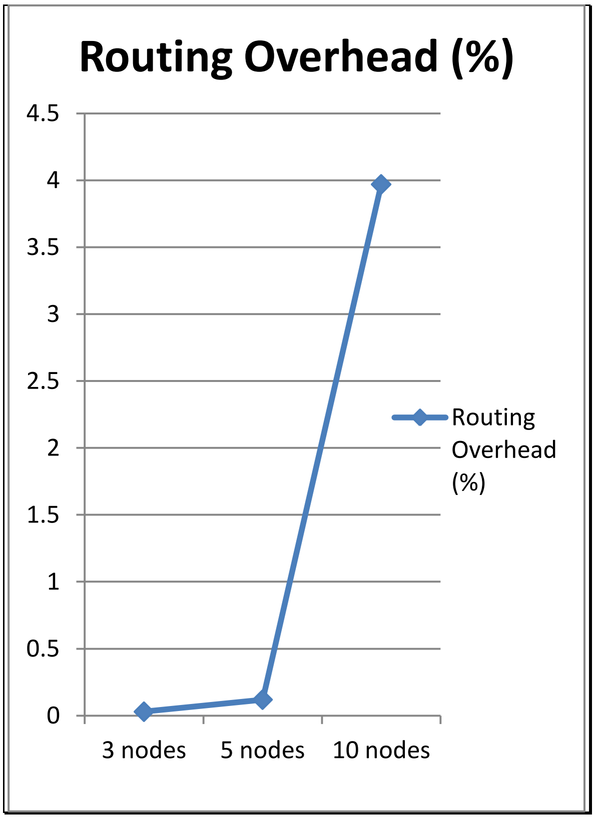
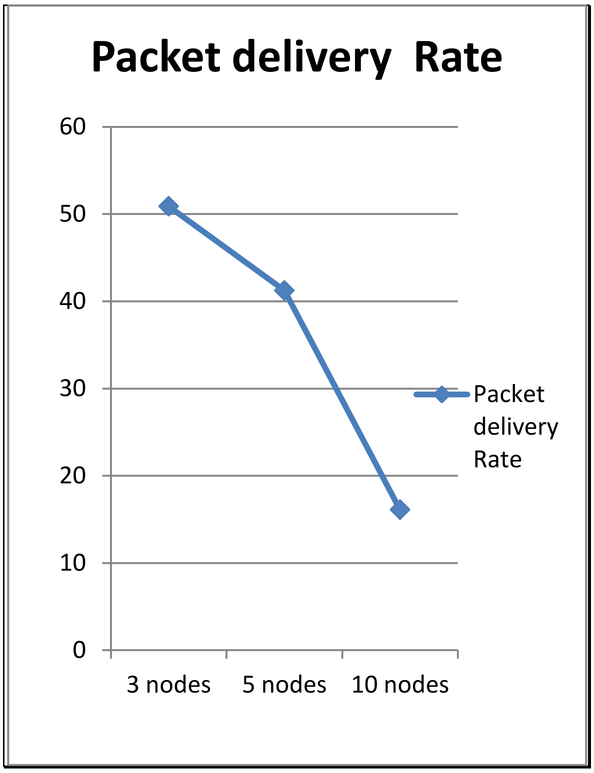


Fig. 15 Normal Delay Pattern

Fig. 16 Normal Routing Overhead Pattern



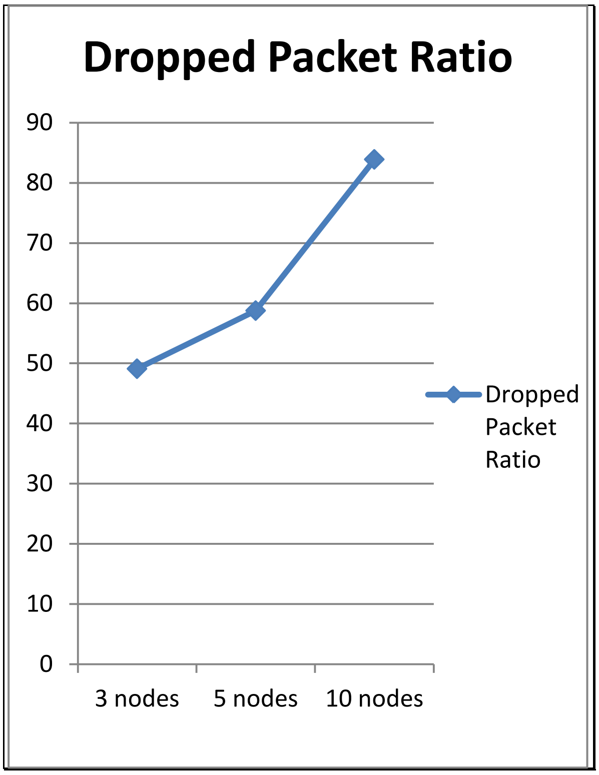
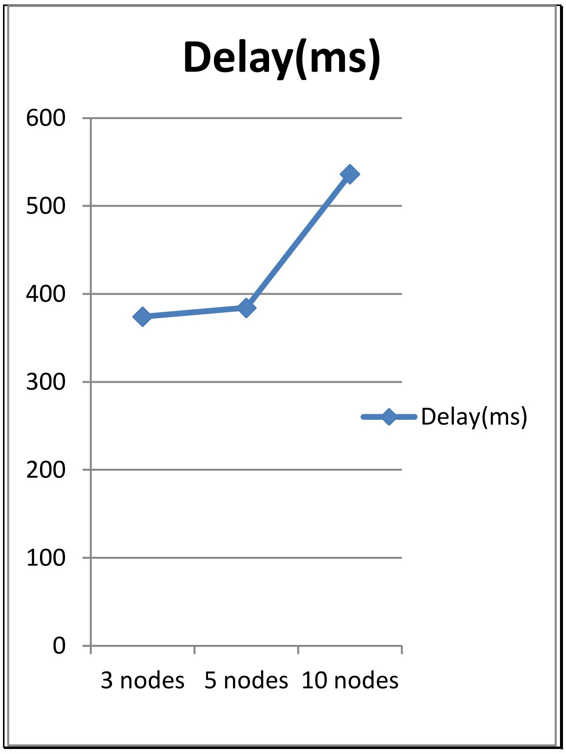


Fig. 17 Normal Packet Delivery Rate Pattern **Fig. 18 Normal Dropped Packet Pattern**

Scenario II: In which the packets are flooded throughout the network Below tabular/graphical representation shows the comparative study for three, five and ten nodes for the above parameters w.r.t defined **scenario (B)** in the (section 4.2)**.**

Parameters/ Nodes	**3 nodes**	**5 nodes**	**10 nodes**
Delay(ms)	374.18	384.19	536.27
Routing Overhead (%)	2.39	21.87	30.08
Packet delivery rate	50.73	10.07	15.59
Dropped Packet Ratio	49.26	89.69	84.44

Table 2 Parameters when Flooding



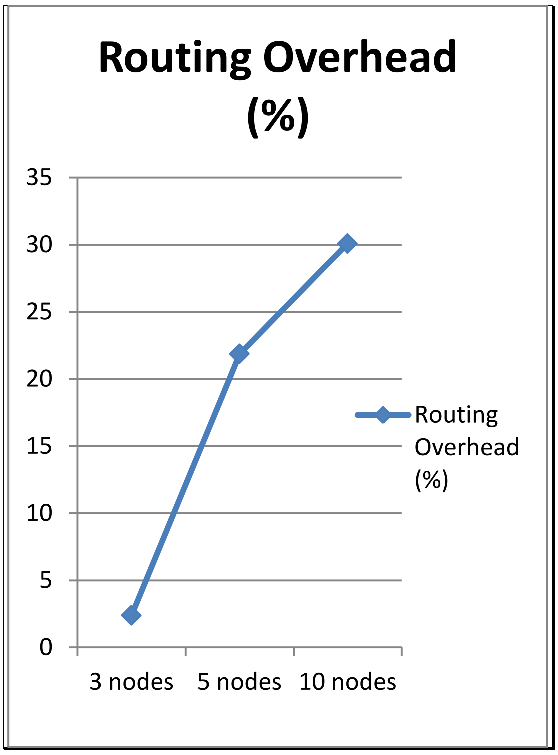
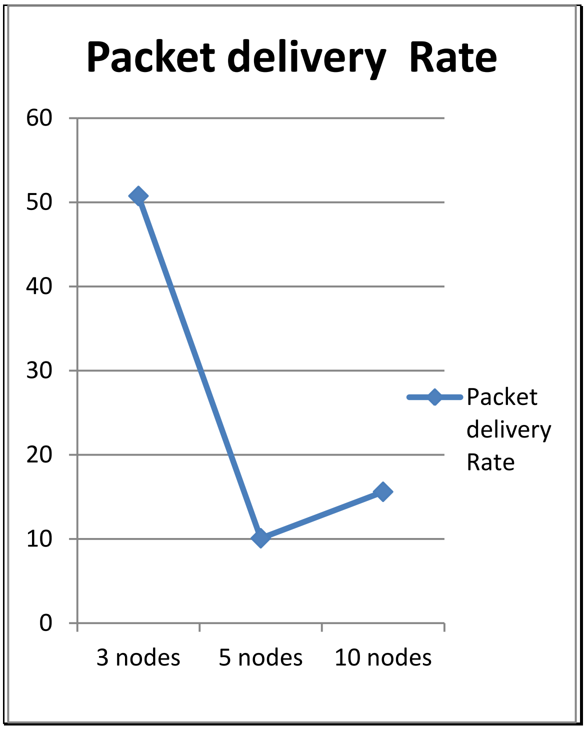


Fig. 19 Flooding Delay Pattern

Fig. 20 Flooding Routing Overhead Pattern



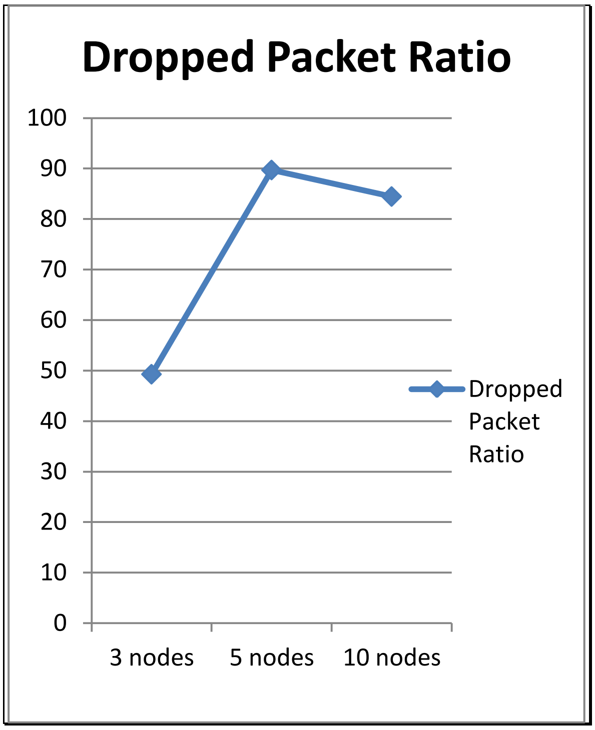


Fig. 21 Flooding Packet Delivery Rate Pattern

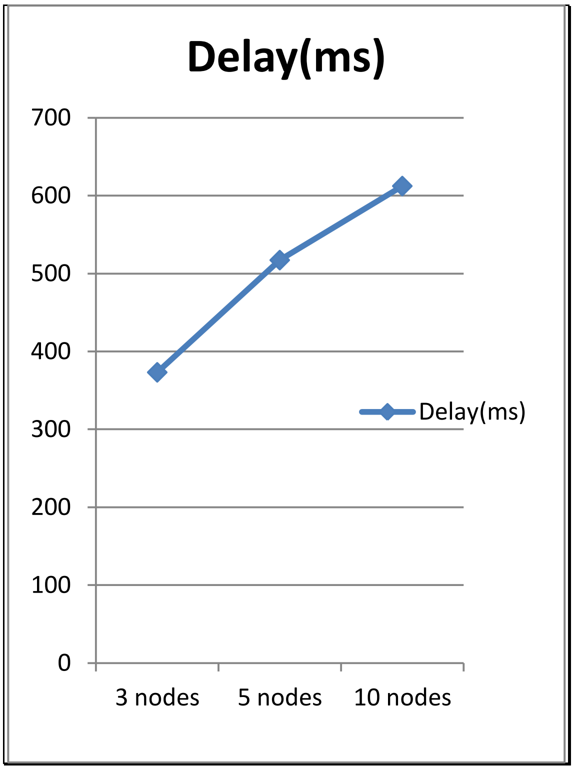
Fig. 22 Flooding Dropped Packet Pattern

Scenario III: The node that exhibit the malicious behaviour is introduced in the network.With such node the performance of network is studied and it is analyzed that the network performance degrade when there is black hole node in the network and the number of nodes are high. When the number of nodes are less then it works accepatable.

Below tabular/graphical representation shows the comparative study for three, five and ten nodes for the above parameters w.r.t defined **scenario (C)** in the (section 4.2)**.**

Parameters/ Nodes	3 nodes	5 nodes	10 nodes
Delay(ms)	373.25	517.34	612.39
Routing Overhead (%)	0.03	18.05	24.03
Packet delivery Rate(%)	50.9	4.11	10.52
Dropped Packet Ratio	49.1	95.91	97.89

Table 3 Parameters when Black hole is introduced



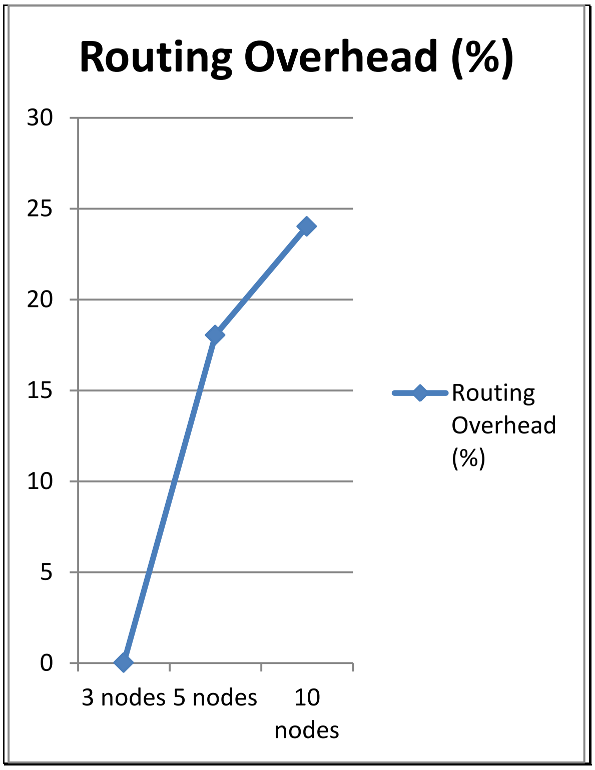
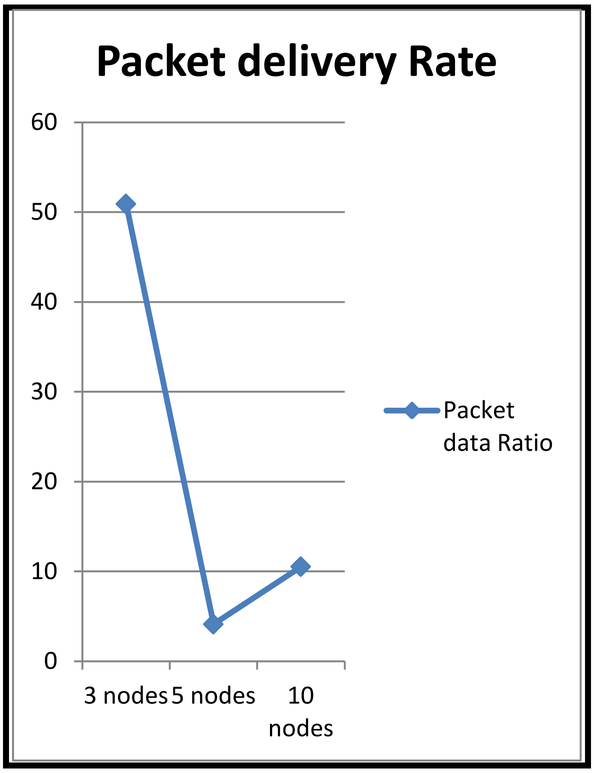


Fig. 23 Black Hole Delay Pattern

Fig. 24 Black Hole Routing Overhead Pattern



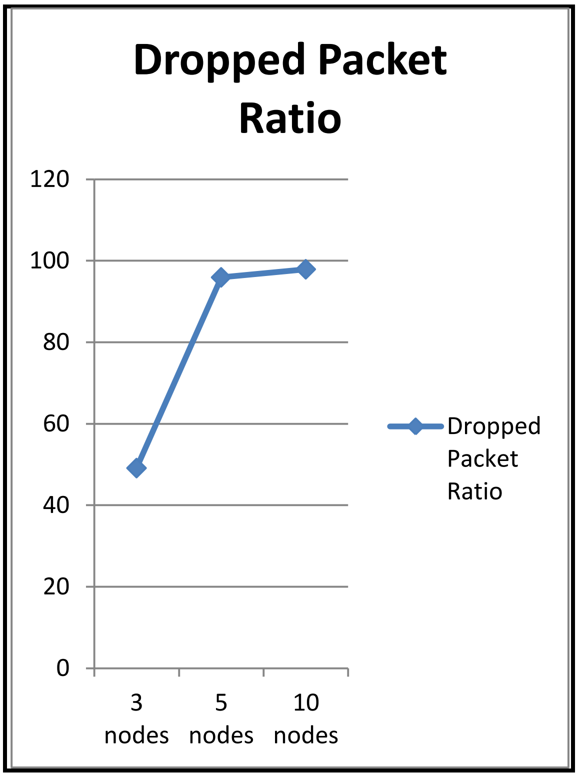


Fig. 25 Black Hole Packet Delivery Pattern

Fig. 26 Black Hole Dropped Packet Pattern

A comparative study is done for the simulated work . The delay patern is compared for the normal working of AODV protocol, flooding attack and black hole attack. It is evaluated that the delay is more in presence of black hole node as compared to malicious node which produce flooding attack.

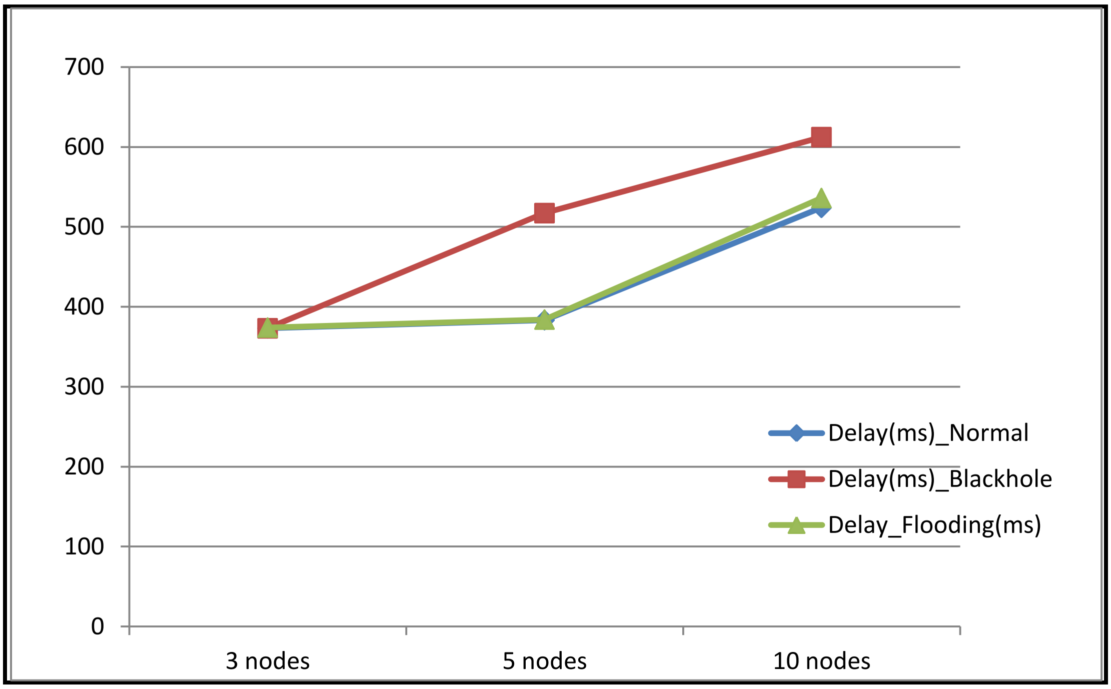


Fig. 27 Comparative Delay Pattern

When the simulated results are compared for the routing overhead it has been observed that as the malicious node in floodind scenario, broadcast a large number of request message in the network this causes increase in the overhead as compared to the overhead produced by the black node. So it has been analyzed that flooding attack is more vulernable than black hole attack in this case. The flooding attack in turn affect bandwidth consumption.Figure 28 shows the comparative study for routing overhead in the three cases. The Figure 29 compares the result for the packet delivery ratio for the small number of nodes the packets are deliverd correctly .The evaluation of packet drop rate is shown in the figure30.

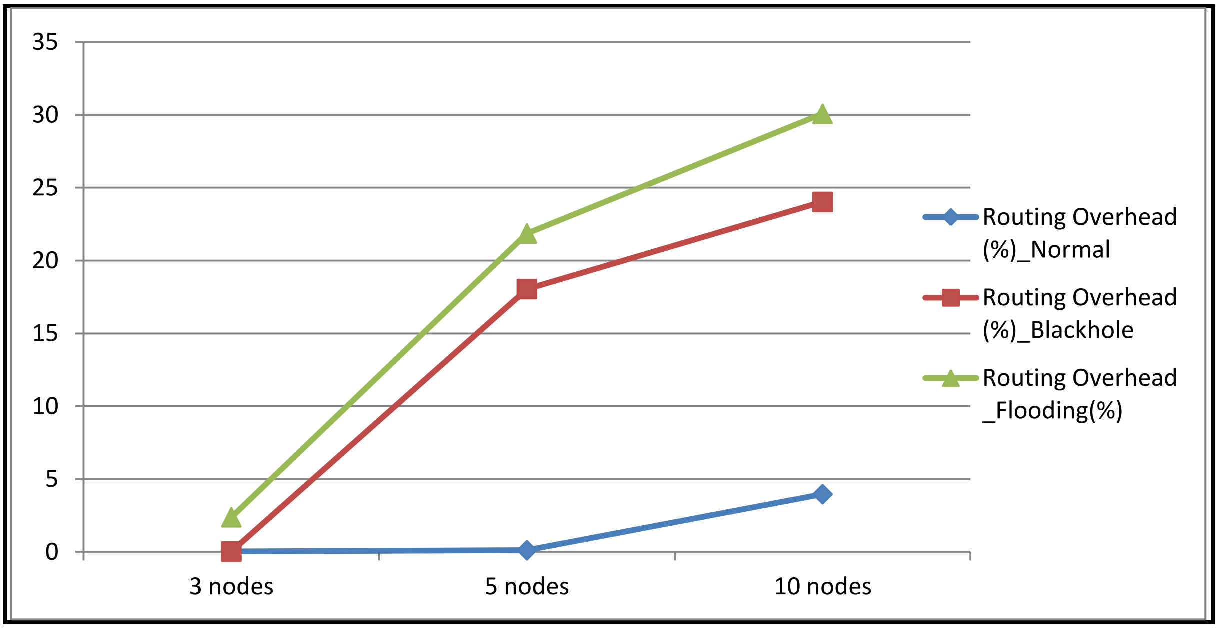


Fig. 28 Comparative Routing Overhead Pattern

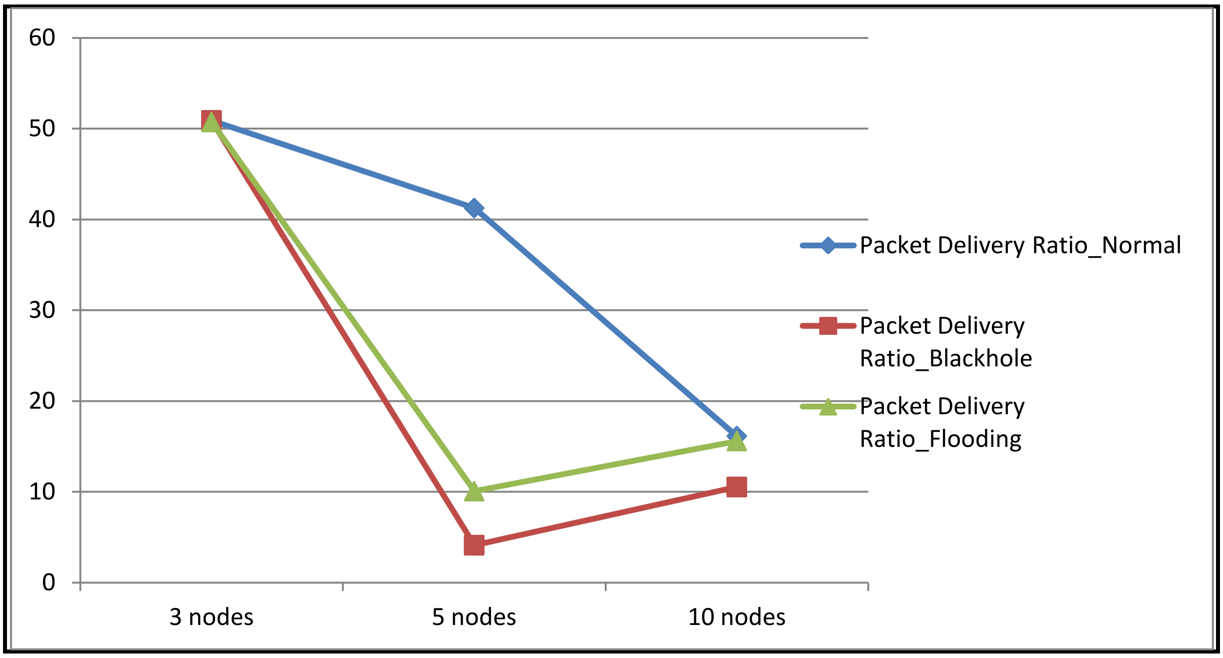


Fig. 29 Comparative Packet Delivery Pattern

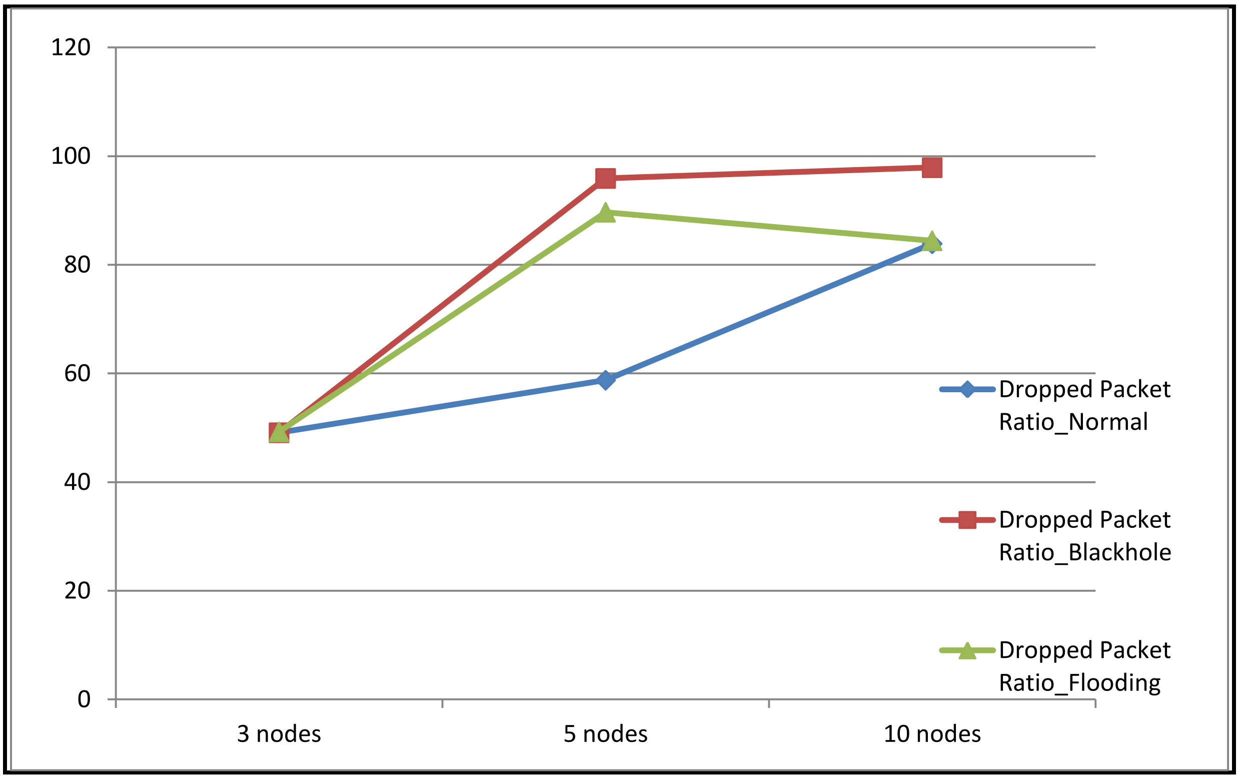


Fig. 30 Comparative Dropped Packet Ratio Pattern

5. CONCLUSION

The Black hole attack and flooding attack are simulated and performance of the different scenario is analyzed on factors like routing overhead, packet drop ratio, packet delivery rate and routing overhead. The tool used in the project is Network Simulator version 2.34 .The simulations is carried out using AODV protocol, for different scenario and is compared for different number of nodes. By the simulation it has been evaluated that in flooding attack the routing overhead (21.87%) is more as compared to the black hole attack (18.05%). The observation shows that the malicious node without intruding in packet transfer can also degrade network performance. This is possible by flooding a large number of false packet in the system which make network vulnerable as this in turn causes more consumption of bandwidth, unnecessary battery utilization of devices, clogs the network.

The packet delivery ratio in scenario when black node attacked is 10.52% and in flooded situation it is 15.59% which shows that more packets are correctly received by the destination in flooding attack as compared to black hole attack. Delay in normal working of protocol is 524.00 ms, in flooded scenario it is 536.27ms and in presence of Black node it is 612.39 ms. The packet drop ratio specifies the number of packets dropped by the node on the total number of packets which are transmitted. In normal working it is 58.76%, in presence of flooding attack this reaches to 89.69% and for black hole attack it is 95.91%.

6. LIST OF REFERENCES

[1] http://en.wikipedia.org/wiki/Computer_network

[2] http://en.wikipedia.org/wiki/Wireless_network

[3] http://www.ietf.org/rfc/rfc2501.txt

[4] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu "Mobile ad hoc networking: imperatives and challenges" Elsevier, 2003

[5] https://tools.ietf.org/html/draft-ietf-manet-aodv-09

[6] IRSHAD ULLAH ,SHOAIB UR REHMAN " Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols " June 2010

[7] http://baumann.infopublicqec.pdf

[8] Jacquet, P.Hipercorn Project,Inst.Nat.deRecherche en Inf.et Autom., Le Chesnay, France, Muhlethaler,P.Clausen,T.Laouiti." Optimized link state routing protocol for ad hoc networks" Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International

[9] Guoyou He "Destination-Sequenced Distance Vector (DSDV) Protocol"

[10] Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S.Ali "A Survey of Mobile Ad Hoc Network Attacks"

[11] Ali Hamieh, Jalel Ben-Othman "Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution"

[12] Shabir Sofi, Eshan Malik, Rayees Baba, Hilal Baba, Roohie Mir "Analysis of Byzantine Attacks in Adhoc Networks and Their Mitigation "

[13] Sem_H Dokurer "Simulation Of Black Hole Attack In Wireless Ad-Hoc Networks"

[14] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei "A Survey of Attacks and Countermeasures inMobile Ad Hoc Networks "

[15] http://www.isi.edu/nsnam/vint

[16] Teerawat Issariyakul ,Ekram Hossain "Introduction to Network Simulator NS2"

[17] Nital Mistry, Devesh C Jinwala, Member, IAENG, Mukesh Zaveri "Improving AODV Protocol against Blackhole Attacks"

[18] Mangesh Ghonge, Prof. S. U. Nimbhorkar"Simulation of AODV under Blackhole Attack in MANET"

[19] http://www.ns2ultimate.com

7. APPENDICES

Appendix A Thesis Review Paper

Review paper entitled “**Detection and Mitigation Techniques of Black Hole Attack in MANET: An Overview** ” has been published in “**Volume 2, Issue 4, May 2013**” of the “**International Journal of Science and Research, India , ISSN 2319-7064”**.Here is the corresponding web link.

Web Link: http://ijsr.net/archive/v2i5/IJSRON2013943.pdf

Corresponding review paper is attached here for your reference as well.

Appendix B Thesis Research Paper

Research paper entitled **“Simulation and Analysis of Performance Parameters for Black Hole and Flooding Attack in MANET using AODV protocol “** is under review process.