CHAPTER 4

ALGORITHM DESIGN AND IMPLEMENTATION

In the previous chapter, the methodology used for the research was discussed. Three algorithms are defined to identify the failure node, intruder node and both Victim and intruder node with directional antenna transmission. Divide and Conquer Methodology used for achieving this algorithm implementation. These algorithms areextension toAd-hoc On-Demand Distance Vector protocol.

This chapter deals with algorithm design and implementation scenarios and it is based on the publications on Hemalatha & Paul Rodrigues 2014, Advanced AODV Protocol for Identify the Victim node using Divide And Conquer strategy – In a MANET, Research Journal Of Applied Sciences, Engineering And Technology, Maxwell Publication.

Hemalatha & Paul Rodrigues, ‘Identifying Intruder In Mobile Ad-Hoc Network Using AIHAODV Protocol’, Research Journal Of Applied Science MedwellPublication (Accepted Yet To Be Published).

Hemalatha& Paul Rodrigues2015, ‘Directional Advanced Intruder Handling Ad-Hoc On-Demand Distance Vector Protocol Using Divide And Conquer Strategy – Implementation’, Research Journal Of Applied Sciences Engineering And Technology, Maxwell Publication.

4.1 ADVANCED AD-HOC ON-DEMAND DISTANCE VECTOR (AAODV) ALGORTIHM FOR IDENTIFYING A VICTIM NODE IN MANET

From the literature survey of chapter 2 it is evident that Victim node identification mechanisms and MAC link failure detection techniques used basically some additional computation like link congestion monitoring, residual battery power, reliability, bandwidth, availability and service traffic type, signal strength and flow capacity, energy based node selection and alternate path identification etc. Above proposed technique from the literature does not pin point the victim node and link failure node. In this research work Victim node identification algorithm is developed by extending Ad-hoc On-Demand Distance Vector which is named as Advanced Ad-hoc On-Demand Distance Vector (AAODV) algorithm.

AdvancedAd-hoc On-Demand Distance Vector algorithm details are explained in the following section.

4.1.1 AAODV Algorithm Design

Design Stages: Design Stages involved in Advanced Ad-hoc On-Demand Distance Vector algorithm(AAODV) for identifying a Victim node are as follows:

A. Decide the path using AODV protocol.

B. Transmit packet.

C. Apply AAODV algorithm on packets.

D. Identify the victim node.

E. Redirect to the new route.

F. Sending alert message.

The above design steps of AAODV algorithm are implementedby extending AODV protocol.AAODV algorithm is simulated using Network simulator, assigned parameter for simulation is shown in the below Table 4.1.

Table 4.1 Parameter of the simulation

Channel Type	Wireless Channel
Radio Propagation Model	Two Ray Ground
Antenna type	Omni Antenna
Interface queue type	Drop Tail /Pri Queue
Maximum Packet in Queue	50 packets
Network interface type	Phy/Wireless Phy
MAC type	802_11
Topographical Area	500 X 300 sq.m
TxPower	0.5W
Rx Power	0.1W
Idle Power	0.01W
Initial energy of a Node	1000.0 Joules
Routing protocol	AODV
Number of mobile nodes	10, 20,30,40,50,60,70,80,100
Mobility	0 or 20m/s

4.1.1.1 Decide the path using AODV protocol

In this stage, existing Ad-hoc On-Demand Distance Vector (AODV) protocol is used to identify routes between the source node and the destination node. The Ad hoc On-Demand Distance Vector (AODV) routing protocol is designed for mobile ad hoc networks. AODV is capable of both unicast and multicast routing. It is an On-Demandalgorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. AODV builds routes using a route request / route reply query cycle. Simulation in the NS2 scenario of router request is shown in the below Figure 4.1.

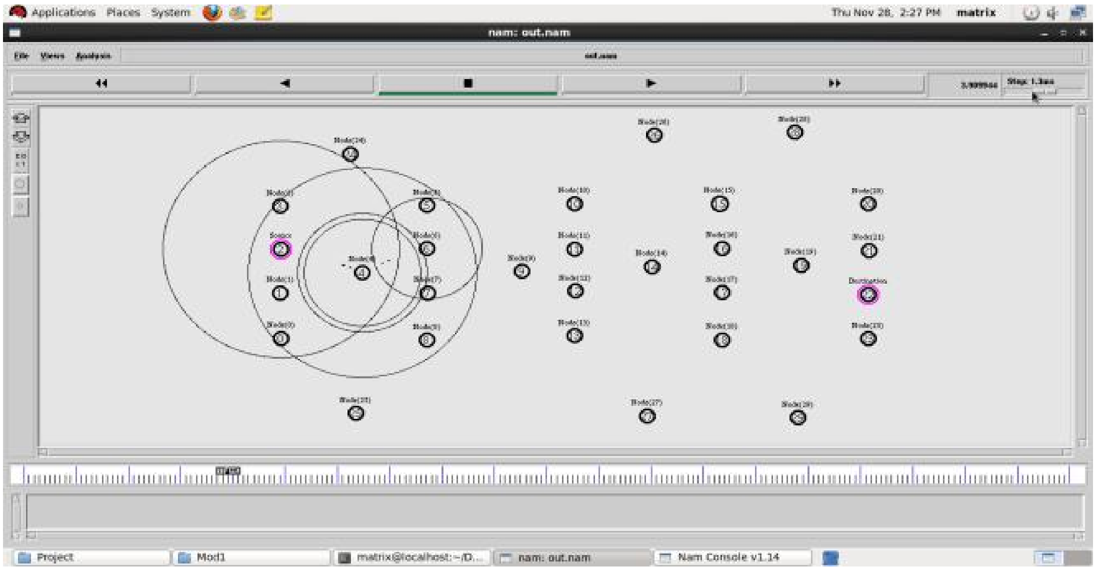

Figure 4.1 Decide the path between source to destination

4.1.1.2 Transmit packet

Once the path is identified between source to destination using AODV protocol, source node starts sending packets to the destination node through the identified path. Sender broadcasts a control packet to all its neighbors. Each node receiving the packet and forwards to its neighbors, sequence numbers help to avoid the possibility of forwarding the same packet more than once, Packet reachesdestination provided that destination is reachable from sender node,the destination does not forward the packet. The simulation snapshot shows the packet transmit in the Figure 4.2.

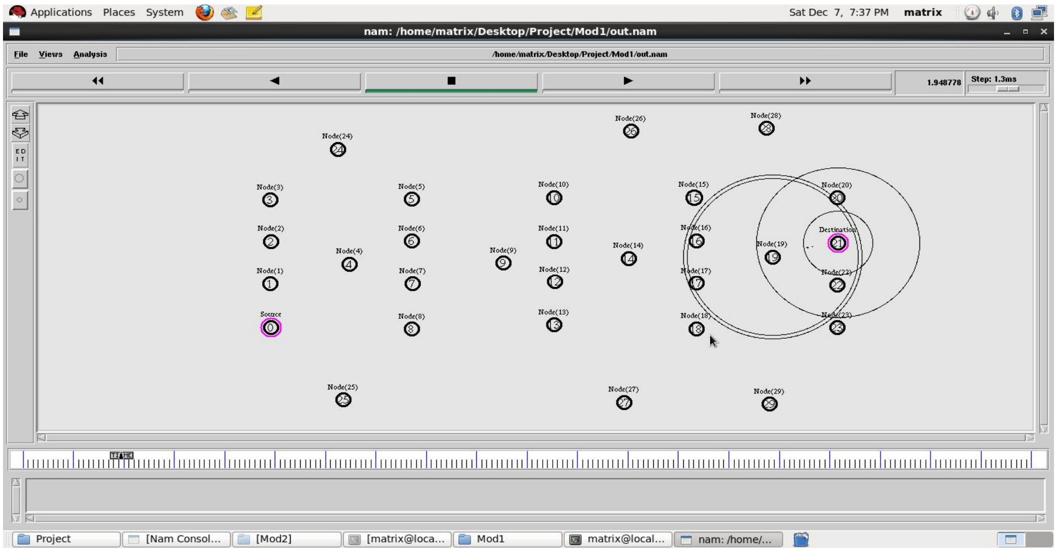

Figure 4.2 Packet transmits

4.1.1.3 Apply AAODV algorithm packets

Procedure(Source, Dest, G) - Divide and Conquer strategy

Consider the ordered Set G={1……..N} .

Step 1: Initialize source = 1, dest = N .

Step 2: Calculate middle = No of hops (source to dest)/2 .

Step 3: (i) Check whether the packet passes through the middle node.

If (yes)

Calculate the new middle node from the middle node to the destination then go to step 2.

Else

Calculate the middle node from source node to middle node, then

go to step 2.

Repeat the process.

If there is no flow of data, then the node may be a Victim or failure node.

Process whether the middle node is victim node

If True Set Victim = Middle and initiates route discovery process.

Step 4: Process to confirm Victim node

Send route request to the Victim node.

If there is no reply, then confirm Victim node.

Step 5: Process to retransmit the data through stage 1.

Step 6: Send alert message about the Victim node or failure node.

Step 7: Stop.

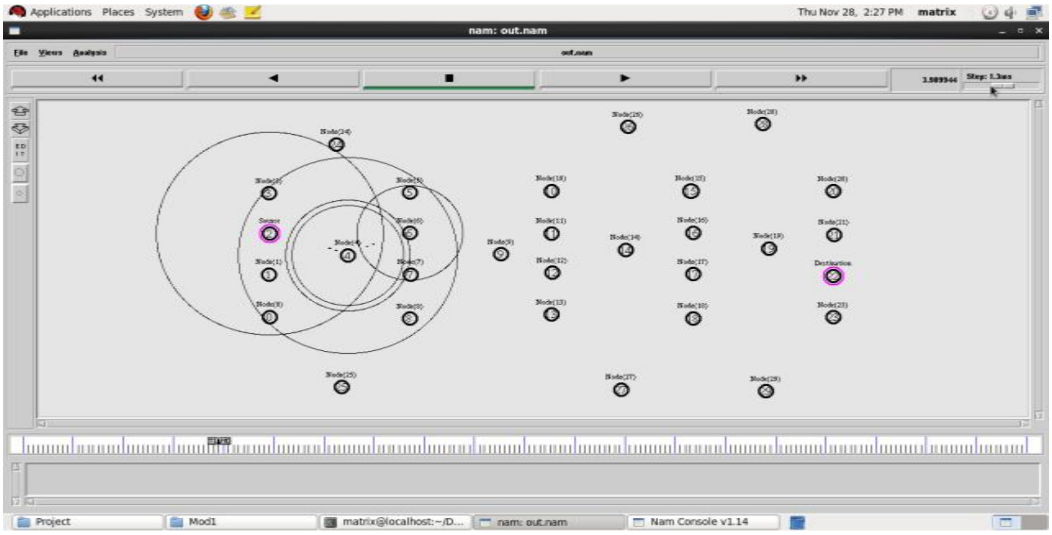

Figure 4.3 Apply divide and conquer strategy

4.1.1.4 Identify victim node

In this stage, the victim node is identified when the node is not forwarding the packet to the next node. Victim node is confirmed based on the identification stage as well as the suspect stage. It includes the phenomenon that source node sends a packet to the suspect node for the confirmation process. At that time suspect node repliesappropriately to the sender within the time period as well as in the appropriate sequence, then that suspected node is considered as healthy node, else that node will be considered as the failure (victim) node. This particular node in turnsenses and collects information from other neighboring nodes. Neighboring node will give the message to the sender node to the suspect node reply message is in appropriate time period.

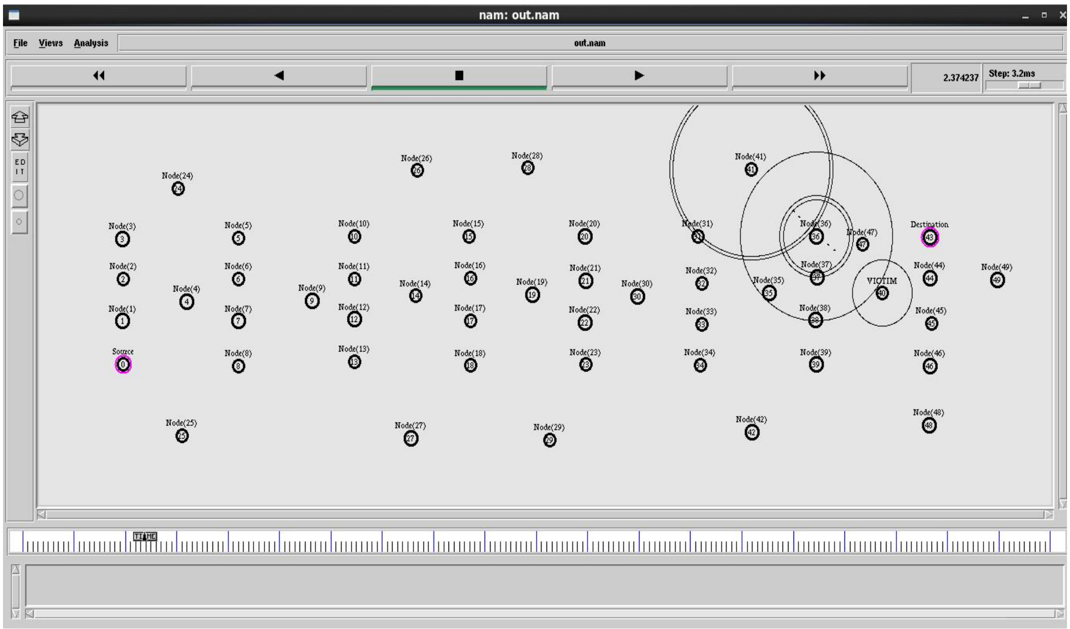

Figure 4.4 Identify victim node

4.1.1.5 Route redirection

The source node discovers new routes to retransmit the packets when the node is identified as Victim node. Afteridentification of victim node, the alert message sends to all the nodes to ensure that packets are not transmitted via victim node. Further the same process is applied if any nodes are suspected of any of the newly established routes. The new path is identified with the help of AODV protocol. Fundamentally AODV protocol focuses on non repetition and shortest path. Route direction in simulation is shown in Figure 4.5.

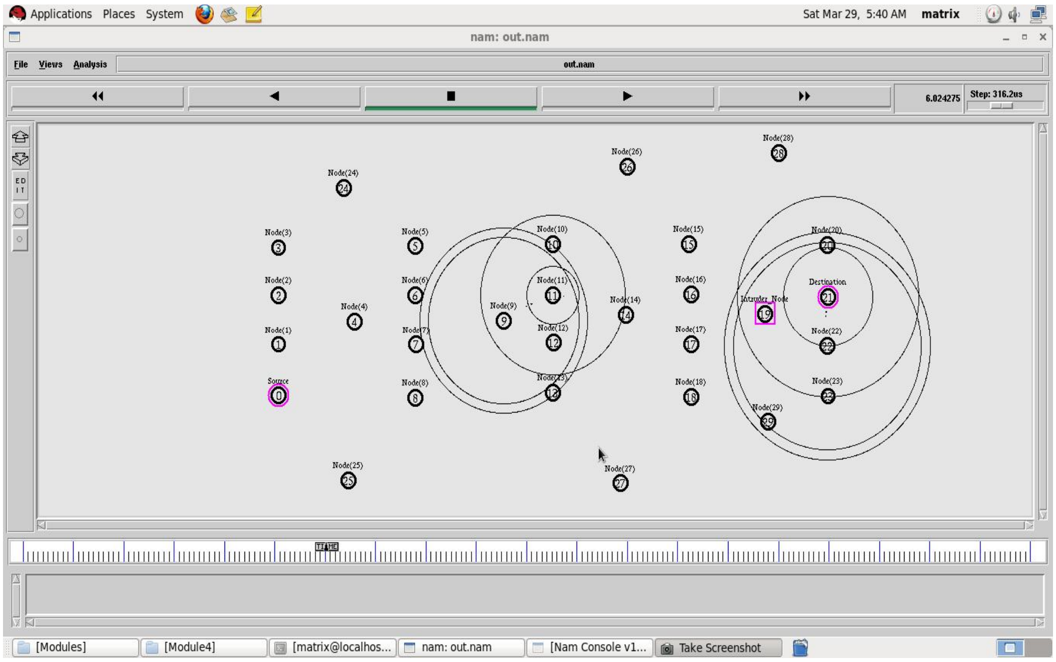

Figure 4.5 Route redirection

4.1.1.6 Send alert message

This stage is focused for sending alert message to remaining all nodes and isolating the victim node in the network to avoid further packet transmission through the victim node. When the node is confirmedas victim node, then the node will give the message to the entire node in the network. The entire node should be prepared with that system and alert with that victim node. Every node should contain the routing table, that routing table contains the source IP address, destination IP address, broadcast id, number of hops, and total number of hops. The network will send a message with data packet that data packet contains the routing table. The routing table contains a victim node id and IP address and all the details of that node, also mentioned in that data packet. Sending an alert message about the victim node is shown in the Figure 4.6.

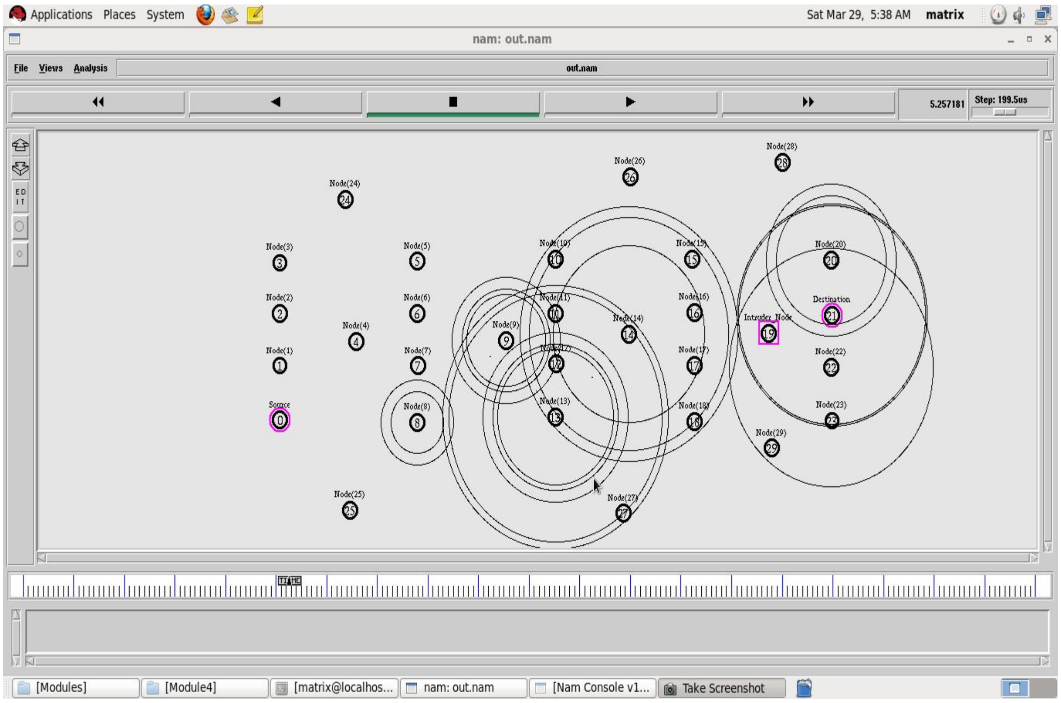

Figure 4.6 Send alert message

In this chapter design and implementation of Advanced Ad-hoc On-Demand Distance Vector algorithm is explained. In the next section Advanced Intruder Handling Ad-hoc On-Demand Distance Vector algorithm design and implementation is dealt with.

4.2 ADVANCED INTRUDER HANDLING AD-HOC ON-DEMAND DISTANCE VECTOR (AIHAODV) ALGORITHM FOR IDENTIFYING AN INTRUDER NODE IN MANET

From the literature review in chapter 2, the Intruder node identification mechanisms are working based on signature, anomaly detection, data mining techniques, reliability, bandwidth, availability and service traffic type, etc. In this research work AAODV algorithm is extended to identify an intruder in MANET which does not need any additional mechanism as described above. This proposed algorithm is implemented using Ad-hoc On-Demand Distance Vector and is named Advanced Intruder Handling Ad-hoc On-Demand Distance Vector algorithm.

4.2.1 AIHAODV Algorithm Design

Design Stages involved in the Advanced Intruder Handling Ad-hoc On-Demand Distance Vector algorithm (AIHAODV) implementation for identifying an intruder are as follows:

A. Decide the path using AODV protocol.

B. Transmit packet.

C. Apply AIHAODV algorithm on packets.

D. Identify the intruder

  (i) Suspect intruder.

  (ii) Confirm intruder

E. Redirect to the new route.

F. Sending alert message.

Above design stages of AIHAODV algorithm are implementedby existing AODV protocol, exclusive of AODV properties. NS2 is selected as a simulation tool, assigned parameter for simulation is shown in the below Table 4.2.

Table 4.2 Parameter of The Simulation

Channel Type	Wireless Channel
Radio Propagation Model	Two Ray Ground
Antenna type	Omni Antenna
Interface queue type	Drop Tail /Pri Queue
Maximum Packet in Queue	50
Network interface type	Phy/Wireless Phy
MAC type	802_11
Topographical Area	500 X 300 sq.m
TxPower	0.5W
Rx Power	0.1W
Idle Power	0.01W
Initial energy of a Node	1000.0 Joules
Routing protocol	AODV
Number of mobile nodes	10, 20,30,40,50,60,70,80,100
Mobility	0 or 20m/s

4.2.1.1 Decide the path is using AODV protocol

The Ad hoc On-Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for mobile ad-hoc networks. AODV is capable of both unicast and multicast routing. It is an On-Demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources.

AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Simulation in NS2 for deciding a path between source to destination is shown in the Figure 4.7.

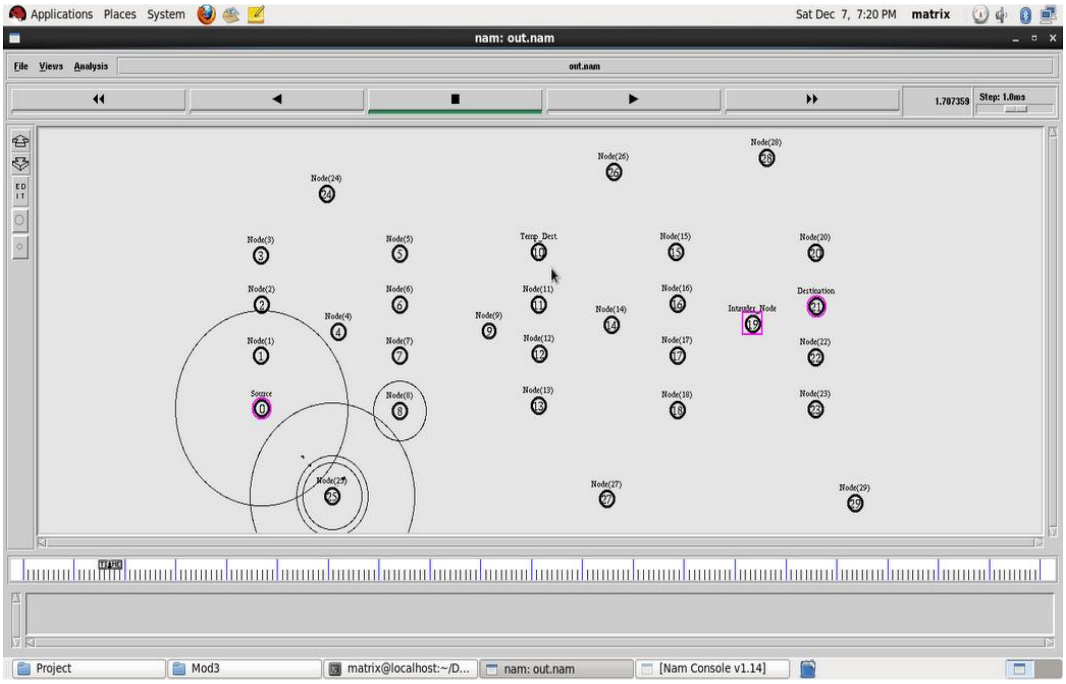

Figure 4.7 Decide the path using AODV protocol

4.2.1.2 Packet transmit

Sender broadcasts a control packet to all its neighbors. Each node receives Packets and forwards it to its neighbors, sequence numbers help to avoid the possibility of forwarding the same packet more than once, Packet reaches destination provided that destination is reachable from the sender, then destination Node does not forward the packet. Simulation of packet transmit is shown in the Figure 4.8 below.

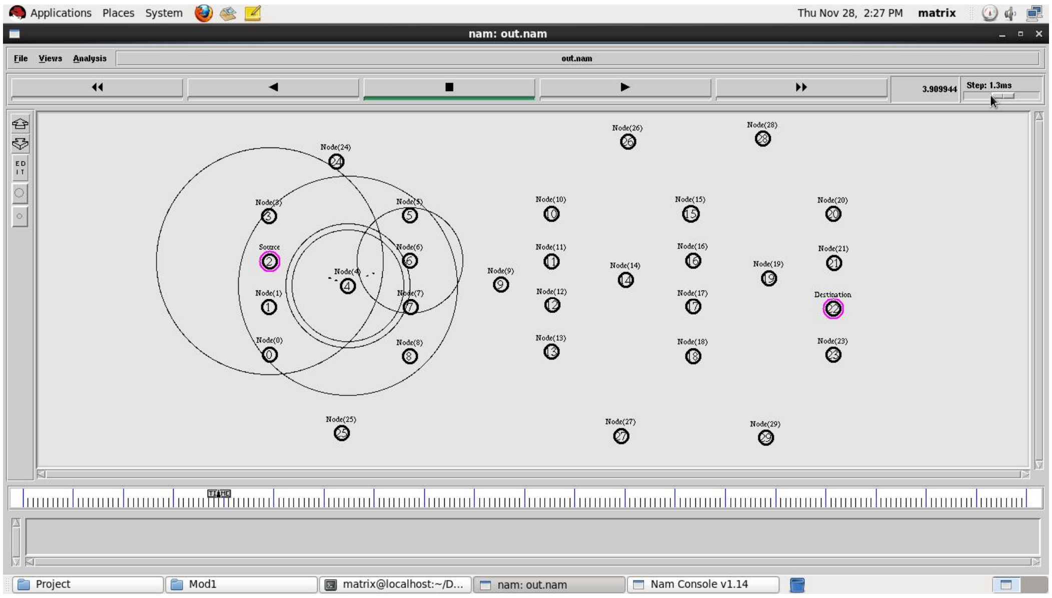

Figure 4.8 Packet transmits

4.2.1.3 Apply AIHAODV algorithm on packets

In this stage, AIHAODV algorithm starts working to find out if any node is not forwarding the packet to the next hop.

The AIHAODV algorithm

```
Procedure (Source, Dest, G)
Consider the ordered Set G={1……..N}
Step 1:   Initialize source = 1, dest = N.
Step 2:   Calculate middle = No of hops (source to dest)/2.
Step 3:   Check whether the packet passes through the middle node
          If (yes)
          Calculate the new middle node from the middle node to the
          destinationthen Goto step 2
          Else
          Calculate the middle node from source node to middle node,
          then go to step 2
          If there is no flow of data, then the node may be the intruder node.
          Process whether the middle node is intrusive.
          If True Set intruder = Middle and initiate route discovery process.
Step 4:   Process to confirm Intruder node.
          Send route request to the Intruder node.
          If there is a reply, then confirm as an intruder node
          Otherwise node may be the failure node.
Step 5:   Process to retransmit the data through stage 1.
Step 6:   Send alert message about the Intruder node.
Step 7:   Stop.
```

4.2.1.4 Identify the intruder

An Intruder can be identified using the AIHAODV algorithm, which can be used to propose a strategy of Divide and Conquer .The node which is not forwarding the packet to the next hop is taken into consideration in identifying an intruder, by passing into two sub stages are suspect and conformation.

(i) Suspect the Intruder

According to the intruder identification process, ifa node is identified as not forwarding the packet to the next hop, the node is making it as a suspected node. Suspecting or doubtful about the node and that node will get a special caution. That node will be under surveillance. All the activity about that node will be noted and recorded. This process must be confidential.

This module will have the important role in this research work. Because it will not only consider that reason while suspecting because of an intruder, but also if that node does have enough power to enable then also it will suspect from the network. That is the reason nodes are gone to the confirmation phase.

(ii) Intruder Confirmation

In this stage, intruder node is confirmed based on the identification stage as well as the suspect stage. It includes the phenomenon that source node sends a router request packet to the suspect node for the confirmation process. The time suspected node responds appropriate router reply to the sender withinthe time period as well as in the original reply, then that suspected node is considered as good node, else that node will consider as the intruder node. This strategy will process with the help of a neighbor node. Neighbor node will give the message to the sender node that the suspect node is giving the reply message in proper time period.

In this research work, AODV protocol is extended for intruder identification introducing two new stages to the AAODV algorithm and named as AIHAODV algorithm. The AIHAODV algorithm can perform divide and conquer strategy used to identify the intruder. The scenario of Intruder confirmation is shown in Figure 4.9 and the algorithm for confirming intruder is shown below. Simulation snap shot about intruder highlighting is shown in the Figure 4.10.

```
        Procedure(Source, H, Intruder)

        Consider the ordered Set H= {1…….. M }

Step 1: Initialize source = 1, Intruder = M

Step 2: Send router Request to the M .
```

Step 3: If there is a RREP from the M to source and confirm M is an intruder

Else if there is False RREP from the intruder to source and confirm M is intruder

Step 4: Otherwise the Node M is not an intruder node

Step 5: Stop

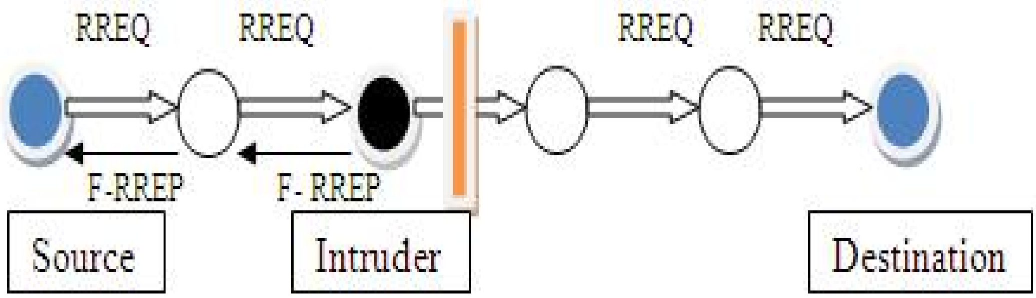

Figure 4.9 Intruder confirmation scenario

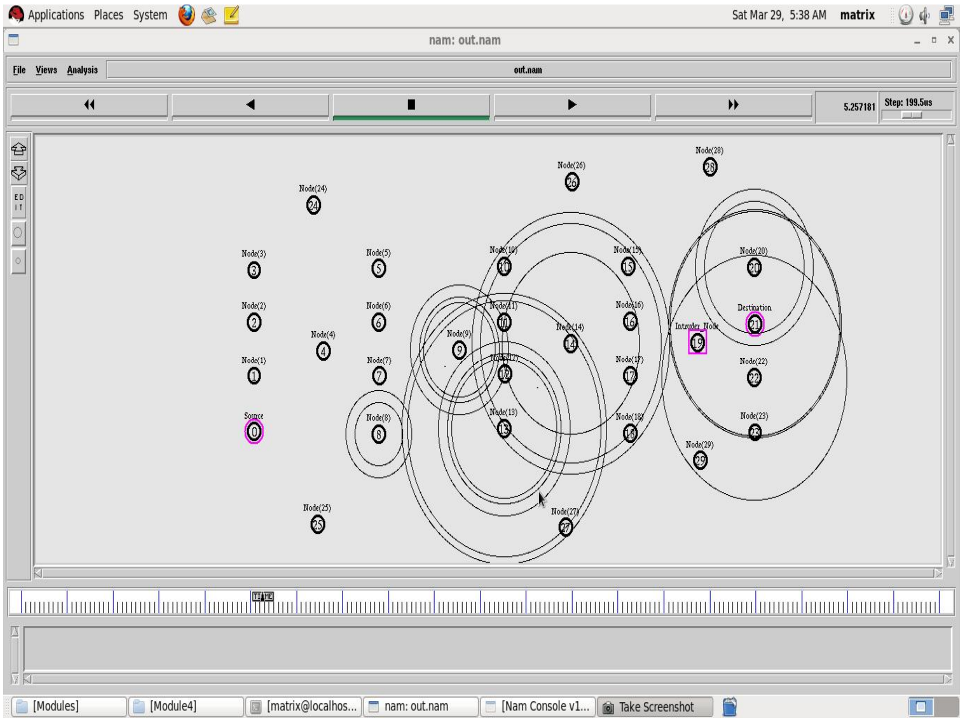

Figure 4.10Intruder confirmed

4.2.1.5 Route redirection

Once the alert message is sent to the entire node, the new route will make from on to source to the destination is shown in Figure 4.11.

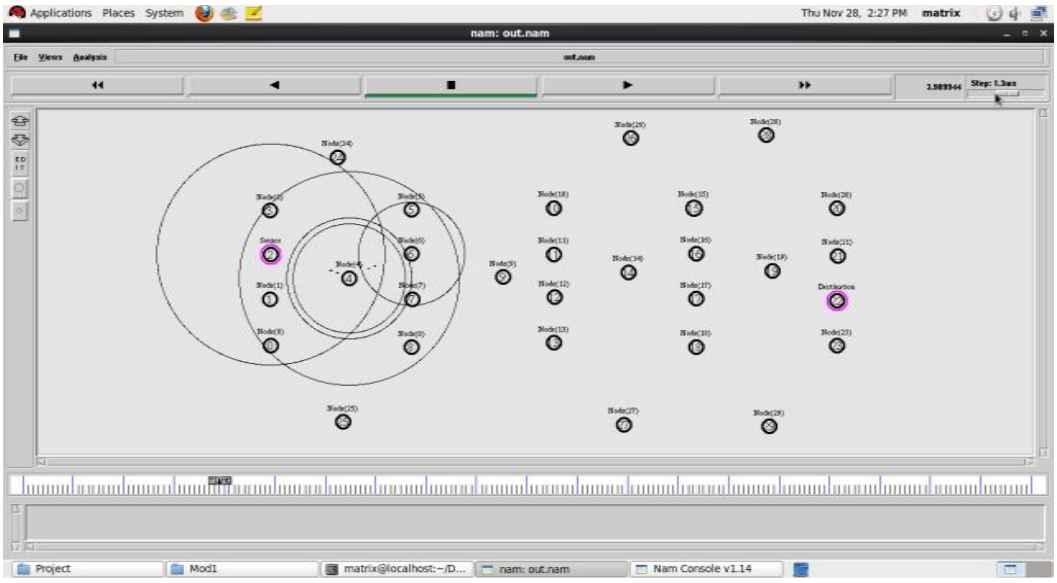

Figure 4.11 Route redirection

4.2.1.6 Send alert message

Once the Suspected node was confirmed as an intruder, then the source node will give alert message to the entire node in the network. Then the entire node should be prepared with that system and alert with that intruder node activity. Every node should contain the routing table, that routing table contains the source IP address, destination IP address, broadcast id, number of hops, and total number of hops. Source node alerts all the nodes about intruder by sending the intruder node id and IP address. Other nodes omit the deciding of packet transmit via intruder node. Simulation snap shot, sending alert about the intruder is shown in the Figure 4.12.

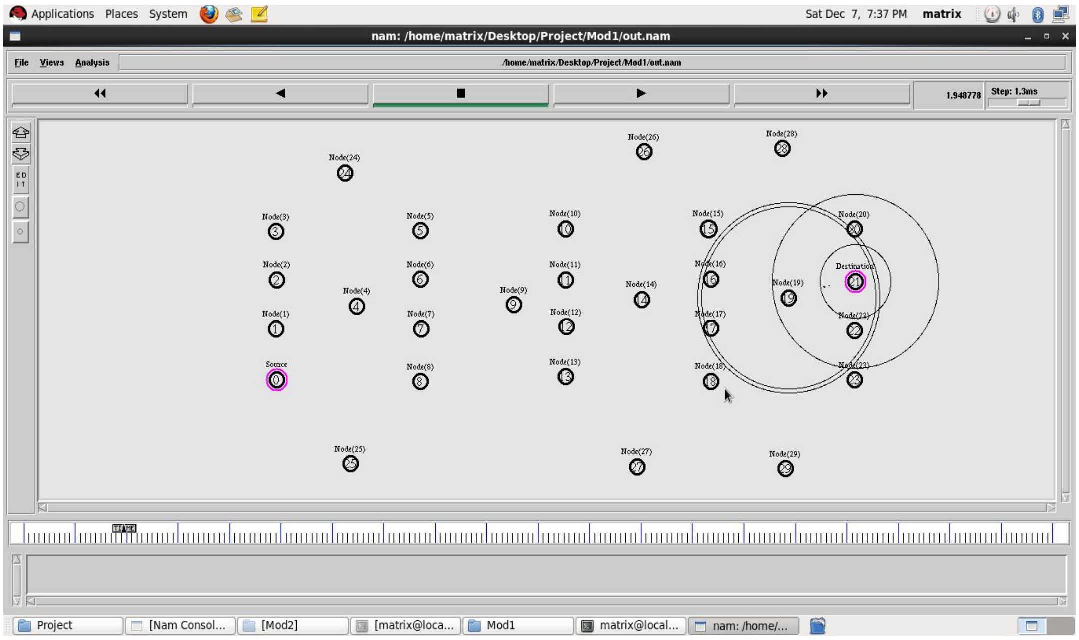

Figure4.12 Send alert message

In this section design stages of AIHAODV algorithm were implemented in the AODV protocol for identifying an intruder node in NS2 simulator, Omni directional antenna transmission. The next section, the DAIHAODV algorithm was enhanced to identify the victim and the intruder node in the MANET with directional antenna transmission.

4.3 DAIHAODV ALGORTIHM FOR IDENTIFYING A VICTIM AND INTRUDER NODE WITH POWER OPTIMIZATION

In the last two sections, Advanced Ad-hoc On-Demand Distance Vector (AAODV) algorithm was designed for identifying failure node in the MANET and Advanced Intruder Handling Ad-hoc On-Demand Distance Vector (AIHAODV) algorithm was designed for identifying Intruder nodes in MANET using the NS2 simulator. These two algorithms are providing solution for reliable packet delivery without any security threat. In MANET battery power (Adamou&Sarkar 2003) is another limitation factor, to overcome this limitation Directional Advanced Intruder Handling Ad-hoc On-Demand Distance Vector (DAIHAODV)(Asis Nasipuri et al 2000) algorithm was designed for identifying victim and Intruder node with directional transmission. This DAIHAODV algorithm combines the features of AAODV and AIHAODV algorithm, and implemented in the AODV protocol by adding the additional features of Directional antenna transmission to transmit the packets.This chapter deals with algorithm design and Implementation scenarios.

4.3.1 DAIHAODV Algorithm Design

The design stages of DAIHAODV algorithm are as follows,

A. Decide the path using AODV protocol.

B. Transmit Packet using directional antennas.

C. Apply DAIHAODV algorithm.

D. Identify the Intruder Or Victim node

   a. Suspect an Intruder or Victim node.

   b. Confirm an Intruder or Victim node.

E. Redirect to the new route

F. Sending alert message.

G. Power Identification

These design stages are implemented in the AODV protocol without changing the properties of AODV protocol. The Network Simulator was used for simulating the design stages in AODV protocol.DAIHAODV algorithm identifies victim node and an intruder node along with (Choudhury& Vaidya 2002)directional transmission. In this algorithm, each node should know in advance about the next hope direction, so that the packets focus on that direction to reach destination. Energy computing is an important role in this algorithm. Residual energy takes into account before transmitting and after transmitting by packets of every node. Simulation screenshot shown in the yellow and red color about the energy in each node. Simulation Parameter is taken is shown in the below Table 4.3.

Table 4.3 DAIHAODV Simulation Parameters

Channel Type	Wireless Channel
Radio Propagation Model	Two Ray Ground
Antenna type	Directional Antenna
Interface queue type	Drop Tail /Pri Queue
Maximum Packet in Queue	50Packets
Network interface type	Phy/Wireless Phy
MAC type	802_11
Topographical Area	500 X 300 sq.m
TxPower	0.5W
Rx Power	0.1W
Idle Power	0.01W
Initial energy of a Node	1000.0 Joules
Routing protocol	AODV
Number of mobile nodes	10, 20,30,40,50,80,100
Mobility	0 or 20m/s

4.3.1.1 Decide the path using AODV protocol

At this stage, source nodes establish a path to the destination through generating Router Request and receiving Router Response from the Destination as in the AODV protocol path establishment, which is shown in the Figure 4.13 in NS2 simulation.

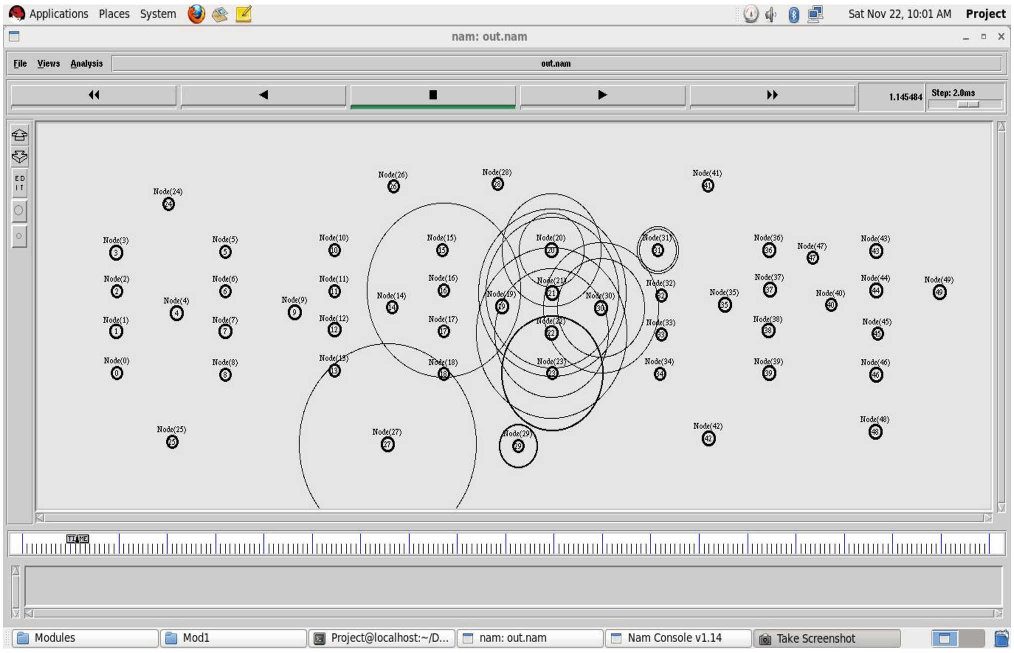

Figure 4.13 Decide the path between source to destination

4.3.1.2 Transmit packet using directional antennas

This stage is processed with packet transmission; the packet can be transmitted via the route which is discovered by the AODV protocol as in Figure 4.13. Packet transmitted is shown in Figure 4.14. If the packet is reached properly to the destination, then the route is perfect and the route does not have any failure in packet and intruder. If any packet loss or any delay happened,means it considers that the route may have any suspected node.

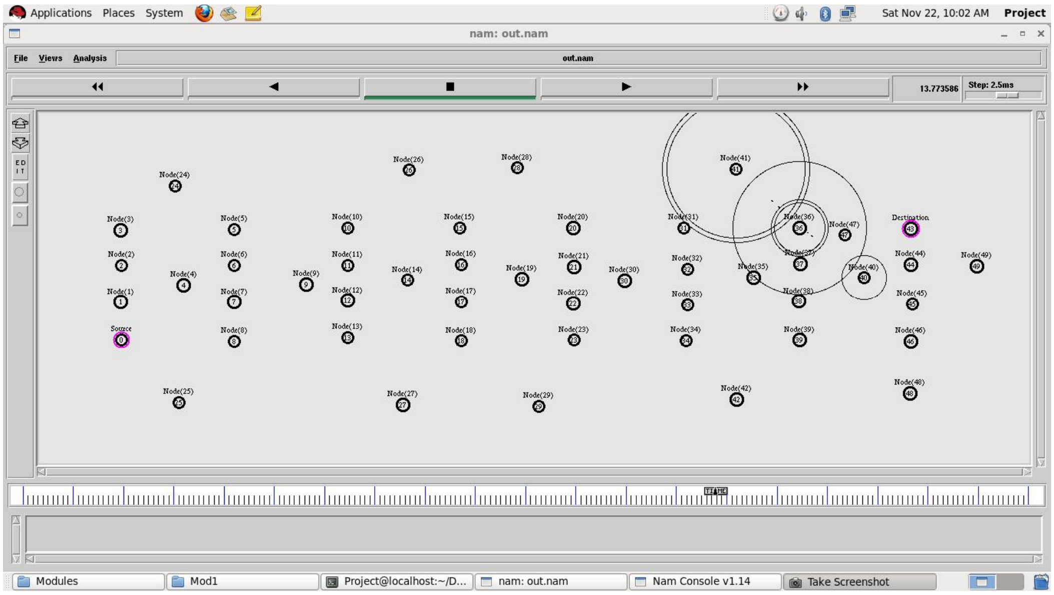

Figure 4.14 Packet transmits

4.3.1.3 Apply DAIHAODV algorithm

This stage is processed with the strategy of divide and conquer, the packet can be transmitted via the route which is discovered by the AODV protocol as in Figure 4.13. It can calculate the number of nodes in the route as in Figure 4.15and identifying any node is not forwarding the packet to the next hop.

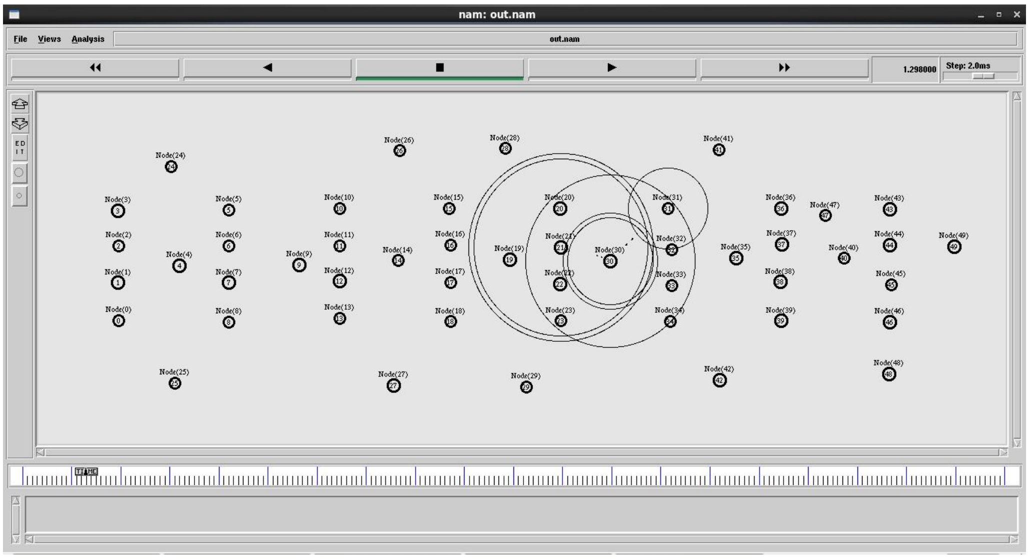

Figure 4.15 Number of node calculation

```
        Procedure (Source, Dest, G)

        Consider the ordered Set G={1……..N}

Step 1: Initialize source = 1, dest = N.

Step 2: Calculate middle = No of hops (source to dest)/2.

Step 3: Check whether the packet passes through the middle node

        If (yes)

        Calculate the new middle node from the middle node to the destination,

        ThenGoto step 2

        else

        Calculate the middle node from source node to middle node

        then Goto step 2

        If there is no flow of data, then the node may be the Victim node (power failure or link failure) or intruder node.

        Process whether the middle node is intrusive.

        If True Set intruder = Middle and initiate route discovery process.

Step 4: Process to confirm Victim node.

        Send route request to the Victim node.

        If there is a router reply, then node may be the link failure node or intruder node.

        Otherwise node is a power failure node.

Step 5: Process to the node is an intruder node
```

Transmit the Route request to the suspected node using the recent path from node to intruder node

If it is Router reply received conform the node is an intruder otherwise node is a link failure node.

Then retransmit data through stage 1.

Step 6: Send alert message about the intruder, link failure node and Intruder node.

Step 7: Stop.

4.3.4 Identify the Intruder or Victim Node

This stage is focused in identifying whether any node is not forwarding the packet to the nexthop.

(i) Suspect node as a victim or an Intruder

If any node is violating the MANET packet transmitting principles, respective node will be marked as a suspected node. Suspected node is processed in the classification of either victim node or Intruder node. Suspected node is forwarded into the next stage for confirming whether it is a failure node, link failure node, or an intruder.

(ii) Confirm suspected node as a victim or an Intruder

Suspected node is taken for processing of confirming victim node or intruder node. The source node generates a router request to the suspected node. If there is no Router reply received from the suspected node, then the node is confirmed as a Victim node. Otherwise, node is taken the processing on whether it is a link failure node or intruder node. To make Confirmed node as a link failure or an intruder node does the dummy packet generation. The source node generates a dummy packet and makes a route to the suspected node. The dummy packet acknowledgement is reached by source, and then confirmedit as an Intruder node, otherwise confirmed as a link failure node. Intruder or victim node identification is shown in the following Figure 4.16 and 4.17.

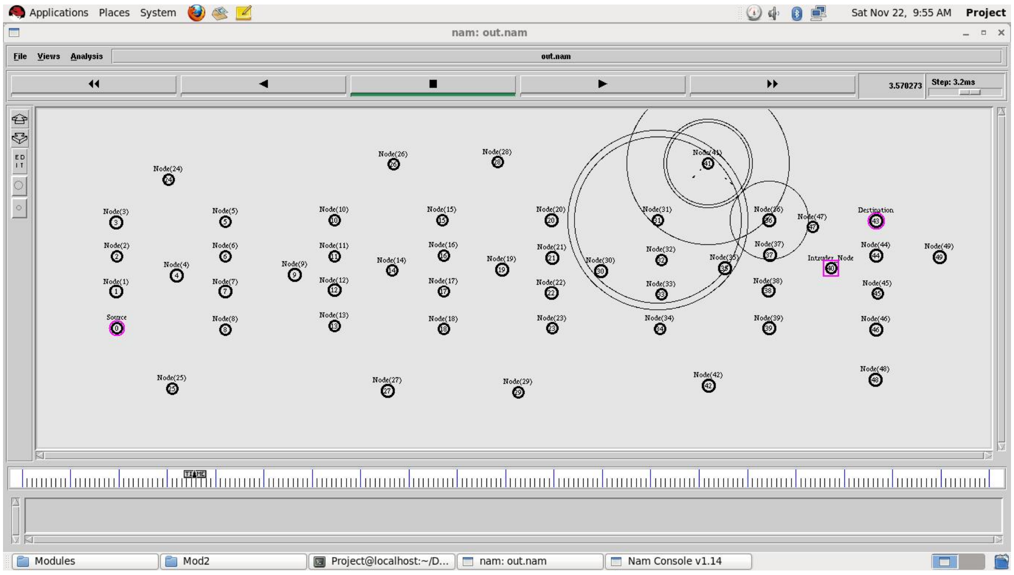

Figure 4.16 Intruder is identified

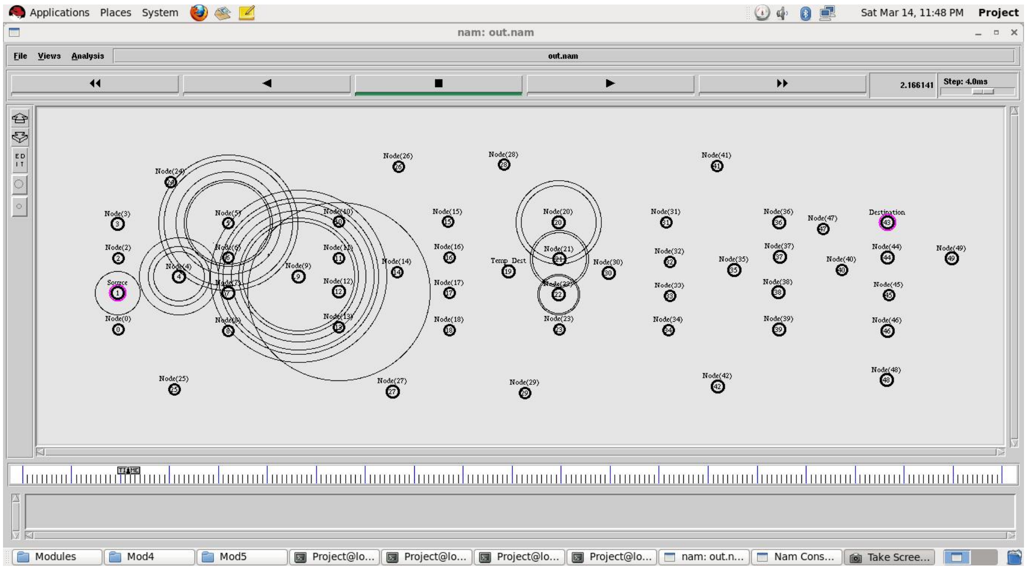

Figure 4.17 Victim node identification

4.3.1.5 Route redirection

In this stage, a new route is identified for transmitting the packet without affecting of security disturbances. New route selection is confirmed that the route is not confirmed victim and intruder node. Sending new router request for retransmitting the packets is shown in Figure 4.18.

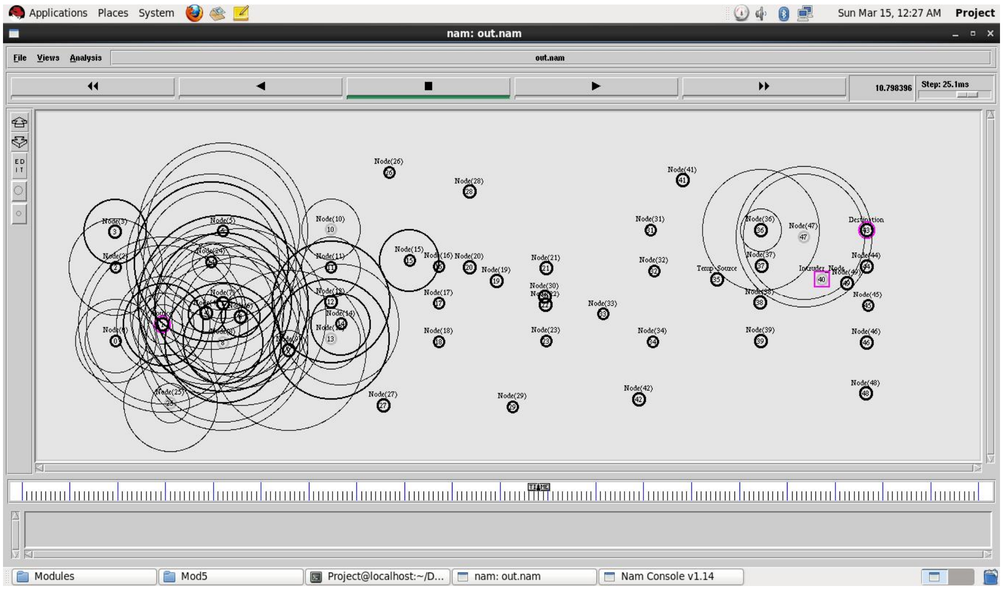

Figure4.18 Route redirection

4.3.1.6 Send alert message

In this stage, once the victim node or intruder node was identified, then the source node givesan alert message to all other nodes in the network.The alert message is consists the details of the victim node or Intruder node. This information is communicated to all the other nodes, In future other nodes will not accept the router request that comes through Victim or Intruder node. Transmitting of alert message is shown in the Figure 4.19.

4.3.1.7 Power identification

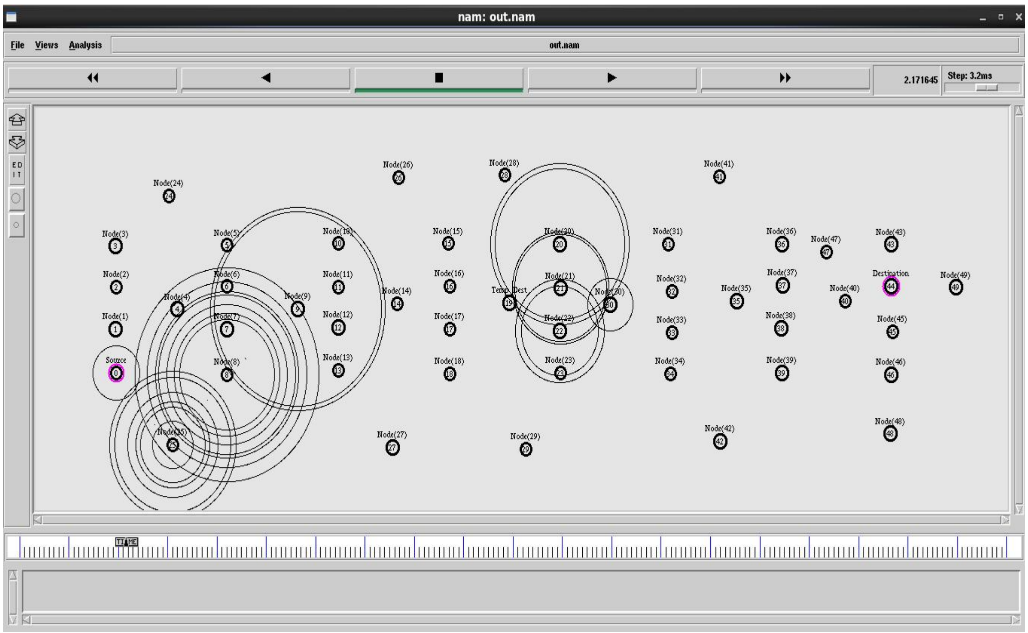

Figure 4.19 Send alert message

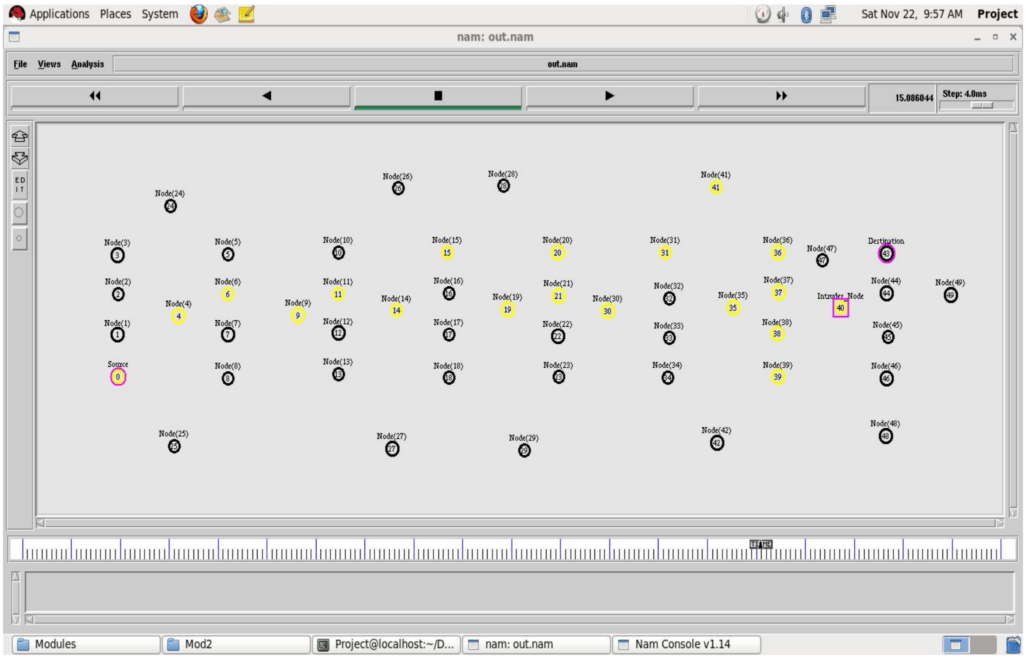

Figure 4.20 Power identification

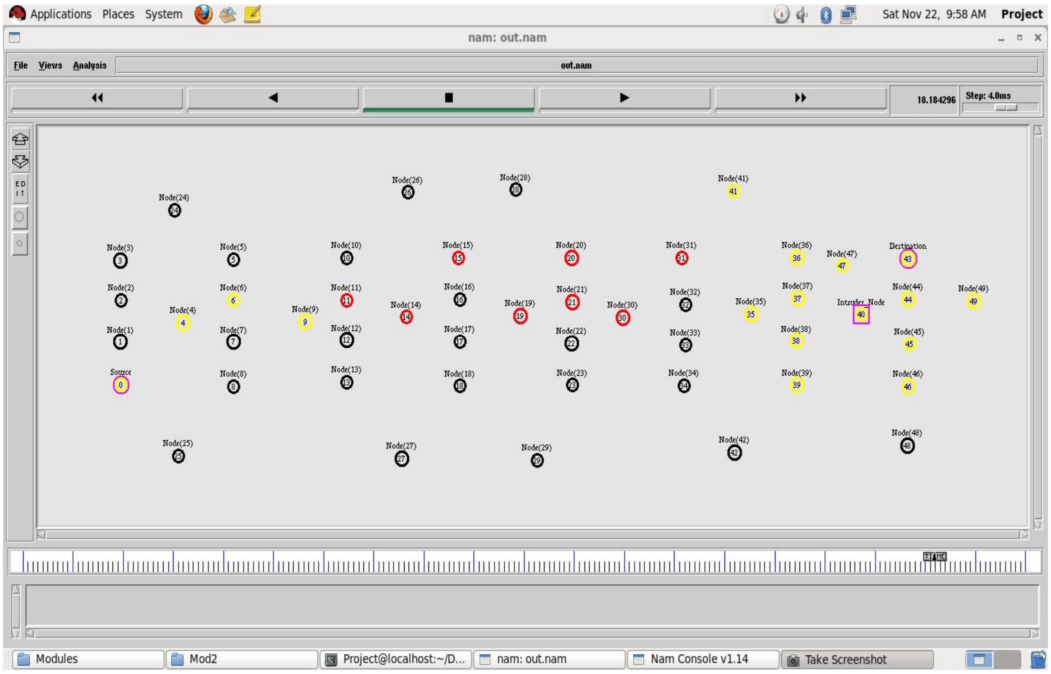

Figure 4.21Power status

From the above output screen from the Figure4.20 and 4.21 the yellow circled nodes are having residual power after transmission of packets and the transmission is based on the Directional Antenna (Alawiehet et al 2009) (Kawadia & Kumar 2003).The Red circled nodes are having no power after transmission of packets. Additional process of power identification before and after transmission will use to avoid the node becomes a failure due to power dry out. So the nodes involved inthe transmission of packets only when it poses a sufficient energy to transmit the packets(Alawieh et al 2009,) (Fang Xie et al 2007) (Firdhous & Suhaidi Hassan 2011**)**.

In this part Directional Advanced Intruder Handling Ad-hoc On-Demand Distance Vector Algorithm was designed in different stages using Network simulator and shown snap shoot of each designed stage in Network simulator.

The next chapter, technical analysis of strength of character converse the Result analysis of Advanced Ad-hoc On-Demand Distance Vector (AAODV), Advanced Intruder Handling Ad-hoc On-Demand Distance Vector (AIHAODV), Directional Advanced Intruder Handling Ad-hoc On-Demand Distance Vector (DAIHAODV) algorithms are discussed in details.