Optimizing Energy Consumption and Providing Security Using Hybrid Approach in MANET

A Dissertation Proposal submitted

By

Pooja Chahal

(11003396)

To

Department of Computer Science and Engineering

In partial fulfillment of the Requirement for the Award of the Degree of

Master of Technology in Computer Science and Engineering

Under the guidance of

Mr. Gaurav Kumar Tak

(April 2015)

INDIA'S LARGEST UNIVERSITY

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education, Transforming India

School of: Computer Science and Engineering

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Pooja Chahal — Registration No: 11003396

Batch: 2010-2015 — Roll No. A09

Session:2014-15 — Parent Section: K2006

Details of Supervisor: — Designation: Assistant Professor

Name: Gaurav Kumar Tak — Qualification: M.Tech

U.ID 15746 — Research Experience: ----

SPECIALIZATION AREA: *Networking and Security* **(pick from list of provided specialization areas by DAA)**

PROPOSED TOPICS

1. Efficient security mechanism for wireless networks.
2. Cloud Computing
3. Phishing Attacks detection with artificial neural networks

G Gaurav K. Tak 15746

Signature of Supervisor

PAC Remarks:

Topic 01 is approved.

APPROVAL OF PAC CHAIRPERSON: **Signature:** **Date:** 20/9/14

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

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

*One copy to be submitted to Supervisor.

ABSTRACT

In recent years wireless communication become common. Wireless networks can be in infrastructure or infrastructure less. Mobile Ad hoc Network (MANET) is special type of infrastructure less network. All nodes are connected with each other using wireless connection and they are allowed to move from one place to another without any restriction. Since MANET is infrastructure less so nodes does not form any topology. Each and every node acts as routers and takes part in the communication. The communication is done with the help of routing protocols. Due to high mobility and multipath propagation network is vulnerable to attacks. There are various attacks that can be possible on MANET like Denial of Service attack, Black hole attack, Wormhole attack, Sybil attack etc which can disturb the communication between the nodes. There are many techniques to prevent or control this attack. But each technique may slow down the process of data transfer. So there is need for some improvement in routing protocol to transfer the data at high speed. The aim of the thesis is to combine two protocols (DSR and AOMDV) and make a hybrid protocol using hybrid approach and then apply SBPGP on it. In this work an attempt is made to enhance security using SBPGP security model, minimizing the energy consumption, time complexity and increasing the network lifetime. Simulation is done on MATLAB and compared with the original protocols.

CERTIFICATE

This is to certify that Pooja Chahal has completed M.Tech dissertation proposal title **"OPTIMIZING ENERGY CONSUMPTION AND PROVIDING SECURITY USING HYBRID APPROACH IN MANET"** under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

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

Date:

Signature of Advisor

Name: Mr. Gaurav Kumar Tak

UID: 15746

ACKNOWLEGMENT

The report has been written with the kind guidance and support of my mentor. The satisfaction and happiness that accompanies the successful completion of any task would be incomplete without mentioning the names of people who made it possible, whose constant guidance and encouragement crowns all efforts with our success.

I would like to express my deep gratitude and thanks to my mentor, **MR. GAURAV KUMAR TAK,** for his help and guidance throughout my dissertation work. I have received an enormous amount of valuable advice and knowledge from him that helps me a lot in my work. Thank you, **MR. GAURAV KUMAR TAK,** sir for giving me motivation and support in my research work.

DECLARATION

I Pooja Chahal hereby declare that the dissertation proposal entitled, **OPTIMIZING ENERGY CONSUMPTION AND PROVIDING SECURITY USING HYBRID APPROACH IN MANET** submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: **Investigator**

Regn. No 11003396

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 WIRELESS NETWORK

Wireless communications have become pervasive. A wireless network is a network that does not require any wires for communication. All the nodes or hosts in a network are wirelessly connected with each other. It does not require any set of cables so it is a cheap process as compared to wired connection. Generally homes, enterprises, telecommunication networks prefer wireless communication over wired. Wireless Telecommunication networks are implemented using radio communication and the implementation takes place at 1^{st} layer of OSI model i.e., physical layer. Wireless networks consist of local, metropolitan, wide and global areas. Examples of this type of networks are Wi-Fi local networks, cell phones and terrestrial microwave networks.

1.2 ADHOC WIRELESS NETWORKS

An ad hoc network is a network that is formed by collection of two or more nodes (devices) that moves in an unpredictable manner. One node can communicate that is within its radio range or outside their radio range. The data is forwarded from one to another node with the help of intermediate nodes. An ad hoc network is infrastructure less, self organizing, adaptive. It follows an infrastructure less architecture yet has a potential of service discovery, routing and packet forwarding. These networks are autonomous and decentralized in nature. The nodes present in network can anytime join or leave the network. All nodes should be able to find the presence of other nodes so that further communication and sharing of data can take place. Examples of ad hoc network are palmtop, laptop, Internet mobile phones etc. Ad hoc wireless devices can take any form so the computation, storage communication capabilities are also different. As there is diversity in the wireless devices so the battery capacity also varies tremendously from one device to another device. There are no routers or access points in wireless network so nodes themselves act as router. These nodes can make different topologies based on the connectivity with each other in the network.

1.2.1 TYPES OF ADHOC NETWORK

There are two types of Ad hoc network

1.2.1.1 SANET (STATIC ADHOC NETWORK)

In Static ad hoc network the geographic conditions and stations are fixed. As soon as nodes are deployed they are fixed. There is no mobility and that's why this type of networks is termed as SANET.

1.2.1.2 MANET (MOBILE ADHOC NETWORK)

MANET is a part of wireless networks. No wires and fixed routers are used in this type of network. It is not everlasting network; it is the short term network. Nodes has the capability to self organize themselves and it follows infrastructure less architecture. Network is formed by number of nodes moving in an inconsistent manner. They do not form any topology. And every nodes further acts as routers which transfers packet from one node to another node. There are many types of MANET like VANET, SPANs, iMANET, Tactical MANET.

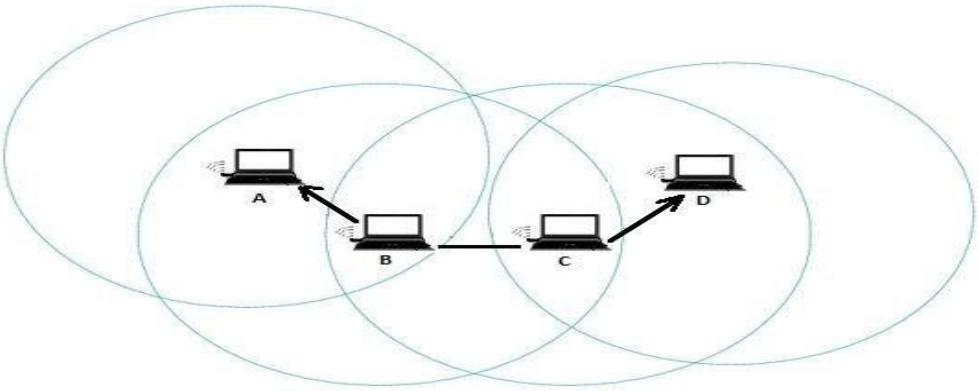

Figure 1.1: Mobile ad hoc network

1.2.1.3 CHARACTERSTICS OF MOBILE ADHOC NETWORK

Ad hoc network is formed by the nodes moving in arbitrary manner. They are self- organizing in nature and hence they can join or leave the network anytime. No routers are used in ad hoc networks nodes itself plays routers and host at the same time. When communication takes place between two nodes then the node which wants to transfer the packet should be in the radio range of source node. The network is self organized and can be setup anywhere without any need of infrastructure. Topology is dynamic, which is a consequence of node mobility. The communication is done with the help of routing protocols like AODV, WRP, and ZRP etc. As these networks are decentralized so the communication is done by mutual trust between the nodes. If any node comes out to be malicious then it hampers the communication so trust plays an important role in the communication. There is no geographical restriction they can be setup anywhere.

Types of Mobile Ad hoc Network:

1) Vehicular Ad hoc Networks (VANET's)
2) Intelligent Vehicular Ad hoc Networks (InVANET's)
3) Internet based Mobile Ad hoc Networks (iMANET's)
4) Smart Phones Ad hoc Networks (SPAN's)

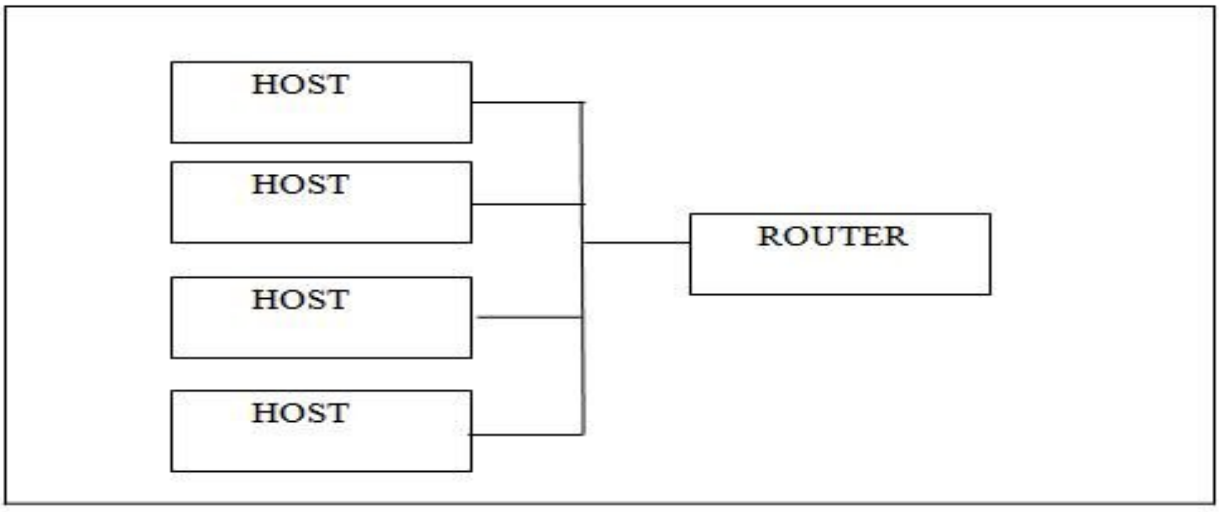

Figure 1.2: Mobile node acting as host and router

1.2.1.4 APPLICATIONS OF MANET

1) Tactical Networks
   a) Military communication
   b) Automated battlefields
2) Sensor Networks
   a) Wireless sensor networks
3) Emergency services
   a) Rescue operations
   b) In hospitals
   c) Disaster recovery
   d) In case of earthquakes, tsunami replacement of fixed infrastructure
4) Commercial environments
   a) Ecommerce
   b) Vehicular services
   c) Shopping malls, sports stadium
   d) Business
5) Home and enterprise networking
   a) Conferences, meeting rooms
   b) Personal Area Network (PAN)
   c) Home/offices wireless networking

1.2.1.5 ADVANTAGES OF MANET

1) Router free : No need of router
2) Fault tolerance: It supports connection failures
3) Mobility: Nodes can easily move from one place to another
4) Connectivity: As nodes are cooperative no need of gateways and central system
5) Fast installation: Flexibility of setting MANET is high

1.2.1.6 DISADVANTAGES OF MANET

1) Lack of secure boundaries
2) Lack of centralized management
3) Restricted power supply
4) Scalability
5) Random topology
6) Memory and computation power limitations
7) High latency

1.3 SECURITY

Security is one of the major issues in wireless network. These networks are vulnerable to attacks. Securing ad hoc network form attacks is very challenging. Once the unauthorized person gets access to the network then he can misuse it. Attacks can be categorizes into two type active attack and passive attack. In passive attack the intruder only keep tracks of data that is being transfer between the hosts. There is no modification or fabrication of data. Eavesdropping and traffic analysis are examples of passive attacks. In active attack intruder modify the data. Examples of active attacks are modification, replay, and denial of services. There are some more attacks like black hole, wormhole, grey hole, Sybil, sleep deprivation attacks that has great impact on ad hoc networks. As soon as a node becomes malicious node it hampers the communication. So there is need of secure routing and secure routing protocol that can provide security against the malicious behavior of nodes.

There are many attacks or security problems in MANET:

- Dos attacks: It is an attempt to make the network unavailable to the users
- Resource consumption: An attacker wants to consume all the resource like power or battery. Example of resource consumption attack is sleep deprivation attack.

- Host impersonation: A node impersonate legitimate node and misuse the network. It is also known as spoofing attack. In this attack attacker wants to get the secret information like public key, passwords etc that should be disclosed in the communication.
- Information disclosure: In this attack an attacker obtains all the information and discloses this information to the third party.
- Interference: Whenever any interference occurs in the network it reduces network performance such as delay, throughput, data loses etc.

1.4 SECURITY MODEL

In this work to issue PGP type certificate we have applied SB model. Suppose a MANET is established in an area where many people are communicating with each other and the wireless channel over which they are communicating is not secure. Let us consider there are N nodes and they are randomly moving from one place to another and any mobile node if free to join or leave the network at any time. In this scenario the mobile nodes that joined the network at the beginning are said to be senior nodes and the nodes that joined the network later on that are said to junior nodes.

For the construction of model some assumptions are there:

- Every node has a nonzero ID and it should be unique
- Every node that is present in the network has a mechanism to recognize the senior nodes in that particular network
- Communication in the is consistently good and authentic with senior nodes rather than junior nodes
- Every senior node has some local detection method by which they can easily detect the malicious nodes or misbehaving nodes among its surrounding nodes.

In this model two or more senior nodes collectively form a Certifying Authority (CA). Whenever a new node comes in the network these senior nodes will check all the information about that new node and if they are satisfied with the information then only they collectively sign on the certificate of new node.

$$SN = \text{ceiling } (N \times M\ \%) + 1$$

$$SCA = \text{ceiling } (SN \times K\ \%) + 1$$

$$JN = N - SN$$

where

SN is senior nodes

JN is junior nodes

N is total number of node in the network

SCA is set of nodes required for CA functionality S

M is variable %

K is variable % (depends on M)

1.5 ROUTING PROTOCOLS

As MANET is infrastructure less, node frequently moves from one place to another and so secure routing is required and it is done with the help of routing protocols. The main aim of routing protocols is to dynamically exchange information of networks paths from source to destination and select the best path to reach the destination.

Classification of routing protocols:

- Table Driven or Reactive
- On Demand or Proactive
- Hybrid

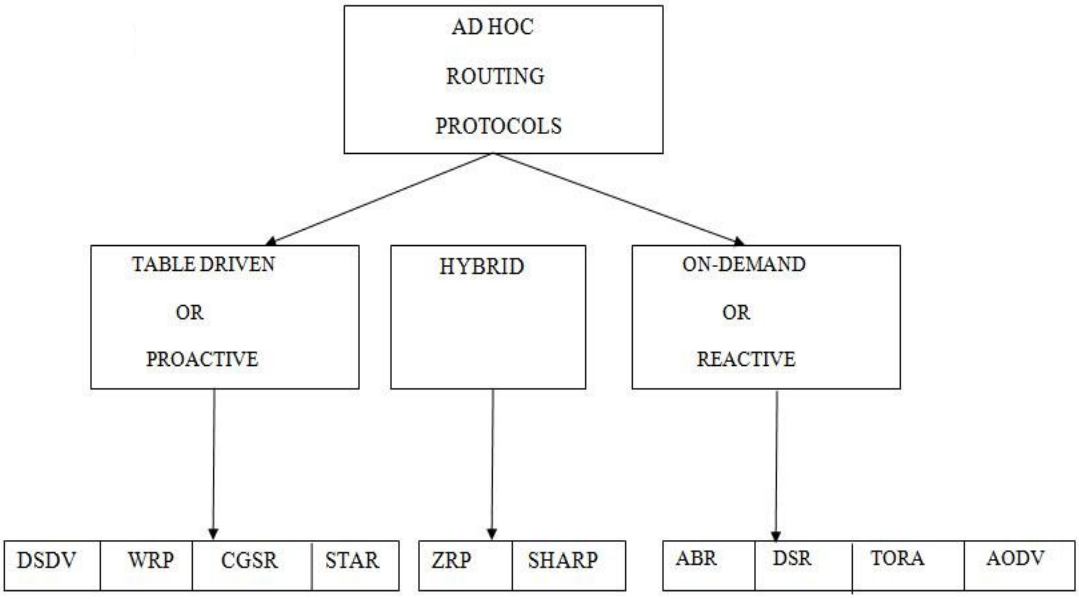

Figure 1.3: Classification of Routing Protocols

1.5.1 TABLE DRIVEN OR PROACTIVE ROUTING PROTOCOL

The main aim of table driven routing protocol is to maintain up-to-date routing information from each and every node present in the network. Every node has to maintain one or two routing table to store all the information of nodes and whenever nodes moves from one place to another place, this route update should be in the node routing table to maintain a consistent network.

1.5.1.1 DISTANCE SEQUENCED DISTANCE VECTOR (DSDV)

DSDV is table driven routing protocol and it is based on distributed Bellman-Ford routing algorithm with some modification. Every node has to maintain the routing table which contains the destination host and number of next hops and each entry in table is assigned with the sequence number. Whenever there is change in the topology routes should be updated. In this each node should advertise its routing information with neighbors. Advertisement can be multicast or broadcast. Hence every node has the information of other nodes present in the node and efficient communication is possible.

1.5.1.2 CLUSTER SWITCH GATEWAY ROUTING (CGSR)

CGSR is table driven protocol. In this nodes are grouped together in the clusters and each cluster has one cluster head. Distributed cluster head selection algorithm is used to elect the cluster head. When one cluster head moves away from the particular cluster then new cluster head must be selected. And it creates a lot of problem as nodes are mobile and if cluster moves frequently it consumes a lot of time to reselect the cluster. To deal with this problem LCC algorithm is used in which cluster head changes only when two cluster head comes in contact.

1.5.2 ON-DEMAND OR REACTIVE ROUTING PROTOCOL

In this route is discovered only when it is required .When node wants to start the communication then it will check its route cache if it exists then the communication will take place and if route is not there then it demands form route discovery process and as soon as it will finds the route it starts its process. There are mainly two processes in on demand routing protocol.

Route discovery When node wants to communicate with another node and if the route is not present in its cache it will initiates route discovery process. The source node then contains the destination address and the addresses of intermediate nodes.

Route maintenance As the topology is dynamic each node is free to move so there are link breakage which can hamper the network so it is very important to maintain the route and it is done by route maintenance process.

1.5.2.1 AD HOC ON-DEMAND ROUTING PROTOCOL (AODV)

AODV is reactive routing protocol and it is an improvement of DSDV protocol. In this whenever a nodes wants to communicate it will broadcast RREQ packet to the neighboring nodes and the neighboring nodes further broadcast this packet until the destination path is discovered. And when a node finds the next route it will reply with route RREP. The reply is sent by using reverse path.

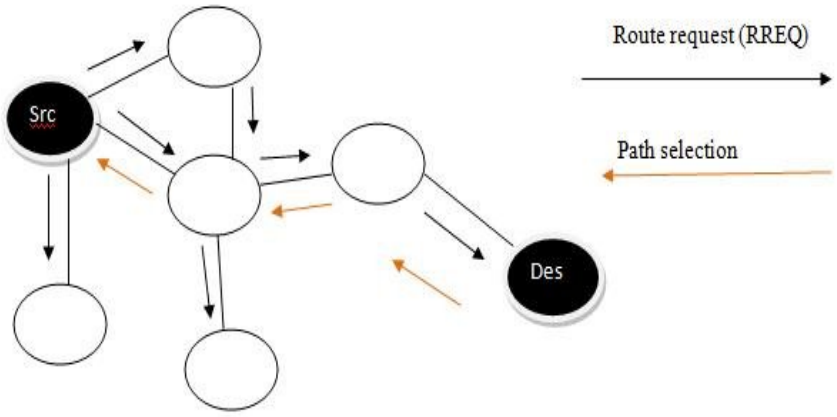

Figure 1.4: AODV Route discovery

1.5.2.2 ADHOC ON DEMAND MULTIPATH ROUTING PROTOCOL

It is the advance version of Ad hoc on demand distance vector (AODV) routing protocol. In this for every route discovery process multiple paths is discovered. It keeps the information of hop counts and next hops and assigns the same sequence number to next hops. When RREQ message is reached to destination then RREP is traversed back through multiple paths. If any route failure is there then alternate route is selected. New route discovery is needed when all routes fails. AOMDV is used to compute multiple loops free and link disjoint paths

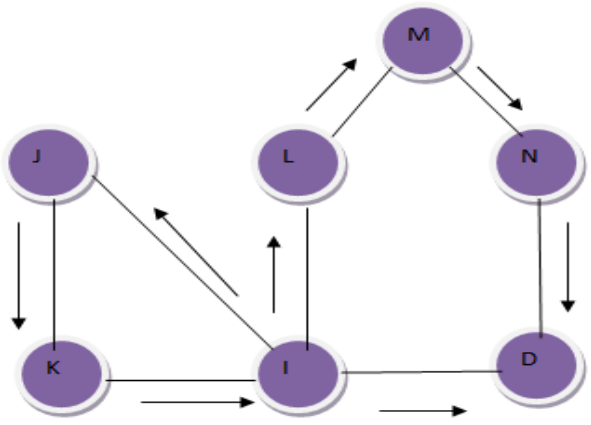

Figure 1.5: Routing loop with multipath computation

1.5.2.3 DYNAMIC SOURCE ROUTING

DSR is reactive routing protocol and it uses source routing process. This protocol uses Link state routing algorithm in which source initiates the route discovery process only on demand basis. In this no HELLO packets are exchanged between nodes. In this protocol Route Request (RREQ) is send to all the neighbors of the node. And then these nodes will further send RREQ message to their neighbors and this process will go on until destination source is found out. Each node contains a sequence number and the path it has traversed.

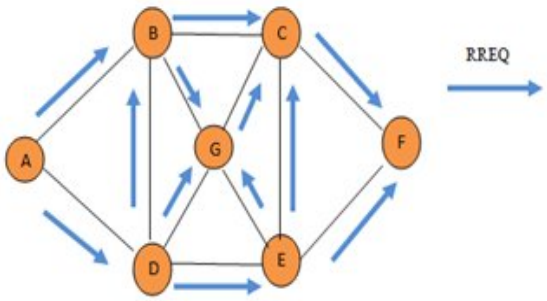

Figure 1.6: Dynamic Source Routing

1.5.3 HYBRID ROUTING PROTOCOL

It is a combination of proactive routing protocol and reactive routing protocol. It deals with the shortcomings of both table driven and on demand routing protocols. It uses route maintenance process of table driven protocol and route discovery process of on- demand routing protocol. Hybrid protocol is used in large networks.

1.5.3.1 Zone Routing Protocol (ZRP)

Zone Routing Protocol is hybrid protocol. In this protocol there is one zone known as routing zone which is similar to cluster (in CGSR) but here every node acts as cluster and members of clusters. Zone can overlap. Whenever a node wants to communicate then it should first discover the neighbors. When a query packet is forwarded it will check whether it is coming from the neighbor or not, if it is coming from the neighbor then it will mark his entry in the same zone as covered. Then query is forwarded in the same manner until it reaches to the destination. At last destination will reply using the reverse path and creates a path.

CHAPTER 2
LITERATURE REVIEW

(Boundpadith Kannhavong, 2007) had discussed all the attacks possible on the MANET. Attacks are black hole, colluding misrelay attack, link spoofing attack, wormhole attack, replay attack, message withholding attack, flooding attack. Author also discussed about the advantage, disadvantages and countermeasures of each attack.

(Moukhtar A. Ali, 2007) classified multicast routing protocols according to different parameters like multicast topology, topology maintenance, topology initialization, core or coreless approach. The author also focuses on the concept of how to apply multicast routing in MANET's and the considerations that each protocol should achieve robustness, efficiency, scalability, security and quality of service (QOS).

(Quamar, 2008) had proposed a security model for small networks using Seniority based trust model and PGP type authentication service. Author also explained some of the related algorithm such as mechanism of certification authentication and certificate revocation mechanism. Then the performance is estimated and author concluded that the particular model is easy, reliable, efficient and easy to deploy.

(Sran, 2012) described about the security with the help of Public Key Infrastructure (PKI), Pretty Good Privacy (PGP), and Seniority Based Pretty Good Privacy (SBPGP). There are many models that provide security to small networks using PGP so the author focused on providing security to large networks. Her paper describes the concept of PKI, technologies related to PKI and comparison of PKI based model. And the results show that SBPGP gives better result as compared to other PKI techniques.

(V.Seethalakshmi, 2012) had estimated the performance of routing protocols in MANET like DSDV, AODV, DSR, TORA and AOMDV. He also introduces new protocol that is a modification in AOMDV and it is known as modified AOMDV (Energy_AOMDV). This protocol improves the battery power of individual node. Author concluded that AOMDV is best protocol among AODV, DSR, TORA and DSDV but when he compared AOMDV and Energy_AMODV, the result shows that Energy_AOMDV is better that AOMDV.

(P.Kanungo, 2012) discussed about the performance of four routing protocols that is AODV, DSR, OLSR and DSDV. Performance analysis was done by considering four parameters that includes end to end delay, throughput, control overhead and packet delivery ratio. And result shows that DSR gives better result in Packet Delivery Ration as compared to other protocols.

(A.Parvathavarthini, 2013) had discussed about types of routing protocol. Routing protocols are mainly categorized into three types proactive, reactive and hybrid. The protocols that are discussed in this paper are DSDV, WRP, CGSR, DSR, AODV, ABR, TORA, ZRP and SHARP

(D.Sharmila, 2013) proposed a new energy efficient mechanism known as Modified Progressive Energy Efficient Routing (MPEER) with scheduling mechanism. In this method threshold value is set for all the nodes and shortest path will be selected between source and destination. If there are many shortest paths between source and destination then the efficient one and the foremost one will be selected.

If energy of source node > Link cost +energy of neighbor nodes, then nodes will be discarded

If energy of source node < Link cost +energy of neighbor nodes, then nodes will be considered as intermediate nodes.

This procedure will go on and choose all the intermediate nodes between source and destination. Once the destination will be found the RREP message will be sent back using these intermediate nodes. Once the path is selected then for each node transmission power will be checked and store in RREQ message with its ID. At last priority based packet

scheduling is applied on it. Result shows that less energy is consumed for path setup and delay is also minimized.

(Rizvi, 2013) discussed about the problem of packets dropped and provided a solution for the same and it also increases Packet Delivery Ratio using Dijkstra's algorithm. Dijkstra algorithm is used find out the shortest distance between source and destination. This algorithm has great significance in routing. Basically Dijsktra's algorithm was first used to find out the shortest distance between one city to another city. In this paper author used Euclidean distance to find out the distance between nodes and it can be calculated by using a formula:

$\sqrt{(X_n^2 - X_m^2)} - (Y_n^2 - X_m^2)$

Where M (X_m, Y_m) are the coordinates of node M

N (X_n, Y_n) are the coordinates of node N

If distance $\leq$ Transmission Range then nodes are said to be neighbors

If distance $\geq$ Transmission Range then nodes are not considered to be neighbors

Then the shortest distance will be selected and message will be transmitted through this route only. By using this technique author solved the problem of packet dropped, link breakage, mobility and scalability. This method also increases the packet Delivery ratio.

(Janish, 2013) had focused on providing security with Public Key Infrastructure (PKI) and its various types in MANET. The Seniority based pretty good privacy (SBPGP) technique is applied on two routing protocols AODV and DSDV protocol. Result shows that end to end delay and throughput of AODV is better that DSDV but delivery packet fraction of AODV is low.

(Arri, 2013) discussed about the multicast routing protocol IODMRP and AAMRP. A security model known as SBPGP applied on these protocols to provide some set of security. Performance is analyzed by observing various parameters like Packet Delivery Ratio, throughput and end to end delay. Result shows that AAMRP proved to show better Quality

of Services parameters and IODMRP shows better result in end to end delay as compared to AAMPRP.

(Kumar, 2014) discussed about a method that will minimize the Route Rediscovery Process. Author used two schemes to do so. First one will minimize the Route Discovery process by applying flooding process optimization algorithm which uses TTL (Time to Live) value to find out the stable route between sender and receiver. Second scheme will minimize the link failure by using Received Signal Strength (RSS) value. With these methods author improved the performance of AODV protocol by minimizing route request message during route discovery process. Also this method has very effective result as compared to original AODV.

(Sharma, 2014) reviewed various methods of location based routing like Location Aided routing (LAR), Location Area Based Ad hoc Routing (LABAR) protocol, ALARM, Distance Routing Effect Algorithm for Mobility (DREAM), Greedy Perimeter Stateless Routing (GPSR), Local Area based Routing protocol called Location Aided (LARDAR), Energy efficient Location Aided Routing, A Location based Routing scheme for opportunistic networks. Each method has common aim to reduce overhead, minimizing the energy and end to end delay

(Indrani Das, 2014) discussed about the effect of node mobility on AOMDV. Three models have been discussed in this paper. First one is Random Waypoint model, in this model movement of node depends on mobility speed and pause time. Second one is Probabilistic Random Walk mobility model, in this movement of nodes depend on probability defined in probability matrix. 3 states were defined in this model 0 represents current state, 1 represents previous state and 2 represents next state. P (a, b) means probability that a node P moves from position a to position b. Third model is Random direction model, in this node can only move up to the boundary of simulation area and after reaching to boundary it will pause for some time. Then it will choose random direction from 0 to 180 degree. Result shows that random direction proves better than other model.

CHAPTER 3

PRESENT WORK

3.1 PROBLEM FORMULATION

MANET has an infrastructure less architecture all nodes are free to move from one place to another without any restrictions. Nodes communicate with each other through routing protocols. MANET is vulnerable to many types of attacks so there is an urgent requirement of sending data packets at higher rates. Previously in DSR and AOMDV whenever communication takes place RREQ message is send to all the nodes present in the network and hence energy consumption is more because every node has to participate in the communication. So in this current work an attempt is made to optimize energy and provide some security to the network and this is done by combining these two protocols and then applying Seniority based pretty good privacy.

3.2 OBJECTIVES

The objectives of this work are

1. The given study focuses on analysis of various routing protocols in MANET.
2. Analyzing the effect of Dynamic Source Routing (DSR) protocol and Ad hoc on demand Multipath Distance Vector (AOMDV) Routing protocol on the network.
3. Implementing these two protocols as a hybrid protocol.
4. Apply Seniority Based Pretty Good Privacy (SBPGP) on hybrid protocol.
5. Minimizing Route Discovery Process
6. Minimizing the energy consumption.
7. Improve efficiency

3.3 RESEARCH METHODOLOGY

Research methodology defines the way in which the research work is carried out. It act as a tool to investigate a particular area in which firstly data is collected, analyzed and conclusion is drawn from the analysis. There are basically three approaches of research methodology i.e. quantitative approach, qualitative approach and mixed approach.

QUANTITATIVE APPROACH

In this approach firstly data is collected by means of experiments, deep study about the topic, simulation. Then the results that we get are analyzed and decisions are made. This approach is generally used by the researcher who wants to verify their proposed method or observe method in greater detail.

QUALITATIVE APPROACH

This approach requires knowledge claims. It includes strategies like ethnographies, phenomenology and grounded theories. When researcher focuses on single phenomenon or concept then this approach is used.

MIXED APPROACH

It is a combination of both quantitative and qualitative approach.

PROPOSED APPROACH

My approach is quantitative. It started with the literature survey of networking, wireless network, MANET, security issues in MANET, solutions, protocols etc. At last to narrow down all the things I came to a conclusion to design a hybrid protocol for handling security using Seniority based pretty good privacy (SB P.G.P).

RESEARCH DESIGN

There are four stages of research design:

1) Problem Identification and selection

2) Literature review

3) Implementation

4) Result analysis

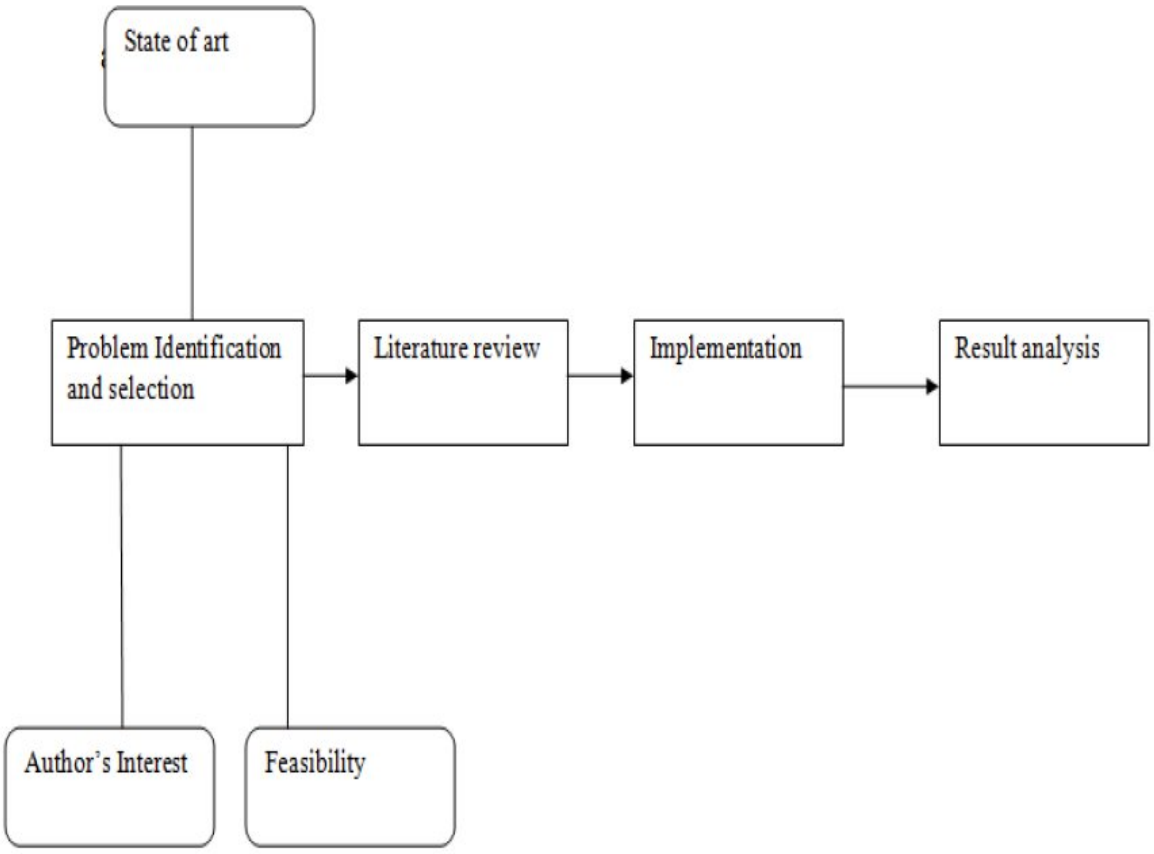

Figure 3.1: Block diagram of Research Methodology

Proposed Methodology

Step 1) Combine two protocols to make a hybrid protocol using this algorithm

Algorithm 1 send data

If route exist && energy> threshold

Then send (packet DATA)

Else

For each NODE

If co-ordinates of node are in between sender and destination

Then send (packet RREQ)

Endif

endfor

i=0

repeat

if NTT is elapsed **then** NTT=NTT*2 **endif**

i=i+1

until i>=3 **and** no RREP is received

if RREP is received **then**

update the routing table

send DATA to destination

else cannot reach the destination

endif

endif

endif

Algorithm 2 receive_RREQ

If source.RREQ_ID< node.RREQ_ID **then** drop the packet RREQ

Else

update the reverse route to the source if necessary

if node know a path to destination **then** send the packet RREP

else

save the Previous_IP into RREQ_LIST

if source.RREQ_ID>node.RREQ_ID **then** update RREQ

update node.RREQ_ID

For each NODE
If node's co-ordinate is in between sender and destination
Then send packet RREQ
Endif
endfor
endif
endif

endif

Algorithm 3 receive_RREP
Delete from the RREQ_LIST the node whose address is equal to RREP_PREVIOUS_IP
Send the packet RREP only to the nodes whose addresses are stored in RREQ_LIST.

Step 2) Create a wireless ad hoc network with multiple nodes that are connected wirelessly with each other.

Step 3) Select the source and destination (node from which the data has to be send)

Step 4) Both the protocols that are used in this work are on demand routing protocols so the resulting hybrid protocol is also on demand routing protocol. On demand routing protocol initiate the route discovery process only when it is demanded.

Step 5) Start the route discovery process

Step 6) Initially all the nodes were idle. As soon as route discovery process starts Route Request (RREQ) message is send to only those nodes whose coordinates fall in between the

source and destination and the nodes which is in the range of source and destination. And all other nodes will remain idle. But when comparison is done with the original method then in that case RREQ message is send to all the neighboring nodes then these neighboring nodes will further send RREQ message to their nodes and so on until destination is found. In this no node will remain idle. Every node has to take part in the route discovery process no matter if in future they are used or not in the communication. As all the nodes are used so energy consumption is more in this case but in our method the nodes which are idle does not consume any energy and hence energy consumption is less.

Also previous method (DSR and AOMDV) is time consuming as compared to new method because RREQ message is send to all nodes present in the network.

Step 7) Once the RREQ message is received by the destination through intermediate nodes then RREP will be sent back to source by selecting the shortest and most stable path. It is done by using Dijkstra's algorithm. It is used to find the shortest distance between source and destination.

Step 8) When the path is selected then Route Reply (RREP) message is send from destination to source through the shortest path which is accompanied by certification number which is unique for every route and it will provide security to the network.

CHAPTER 4

RESULTS AND DISCUSSIONS

Implementation of the proposed techniques has been done on MATLAB and it is showing good results in terms of energy, security and time. Two cases has been taken in this work one is non failure case it means data packet generated at source node will be successfully transmitted to destination node without any failure. But in other case there is a link failure. Any intermediate node can cause link failure and hence new path should be selected to transfer the data packet. Comparison is being done between new method (hybrid approach) and previous method (DSR and AOMDV). And hybrid approach proves beneficial for the network as compared to previous method.

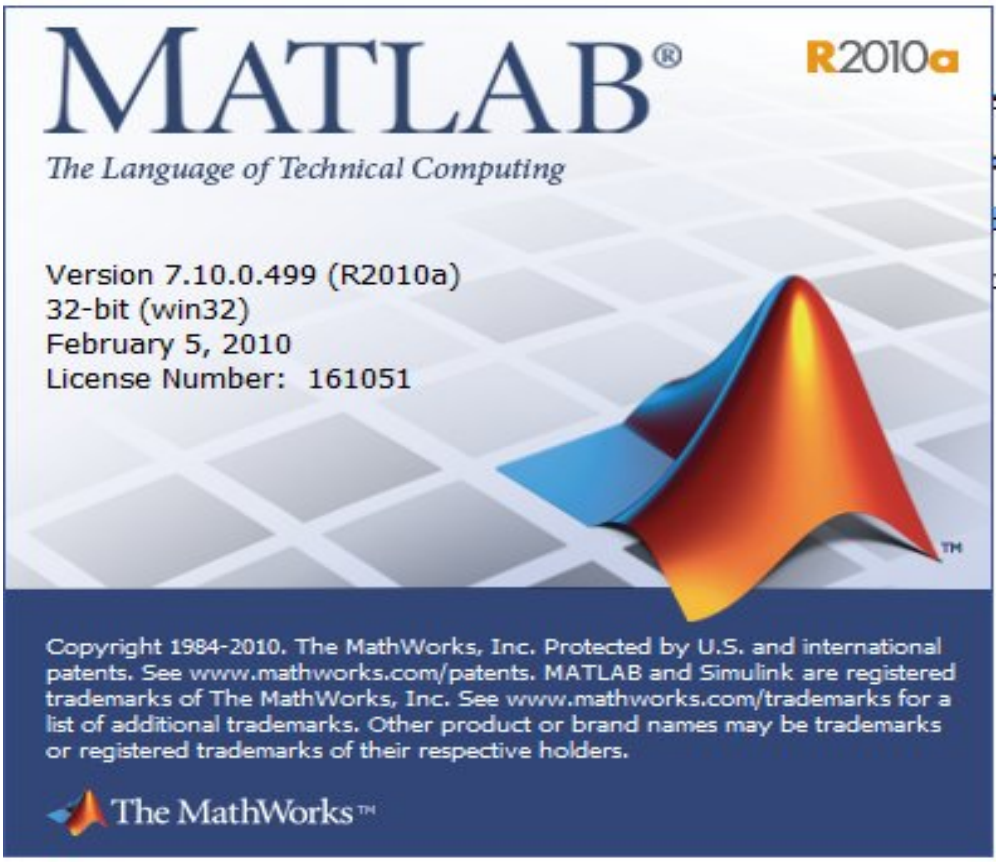

Figure 5.1: MATLAB

CASE 1: NON FAILURE

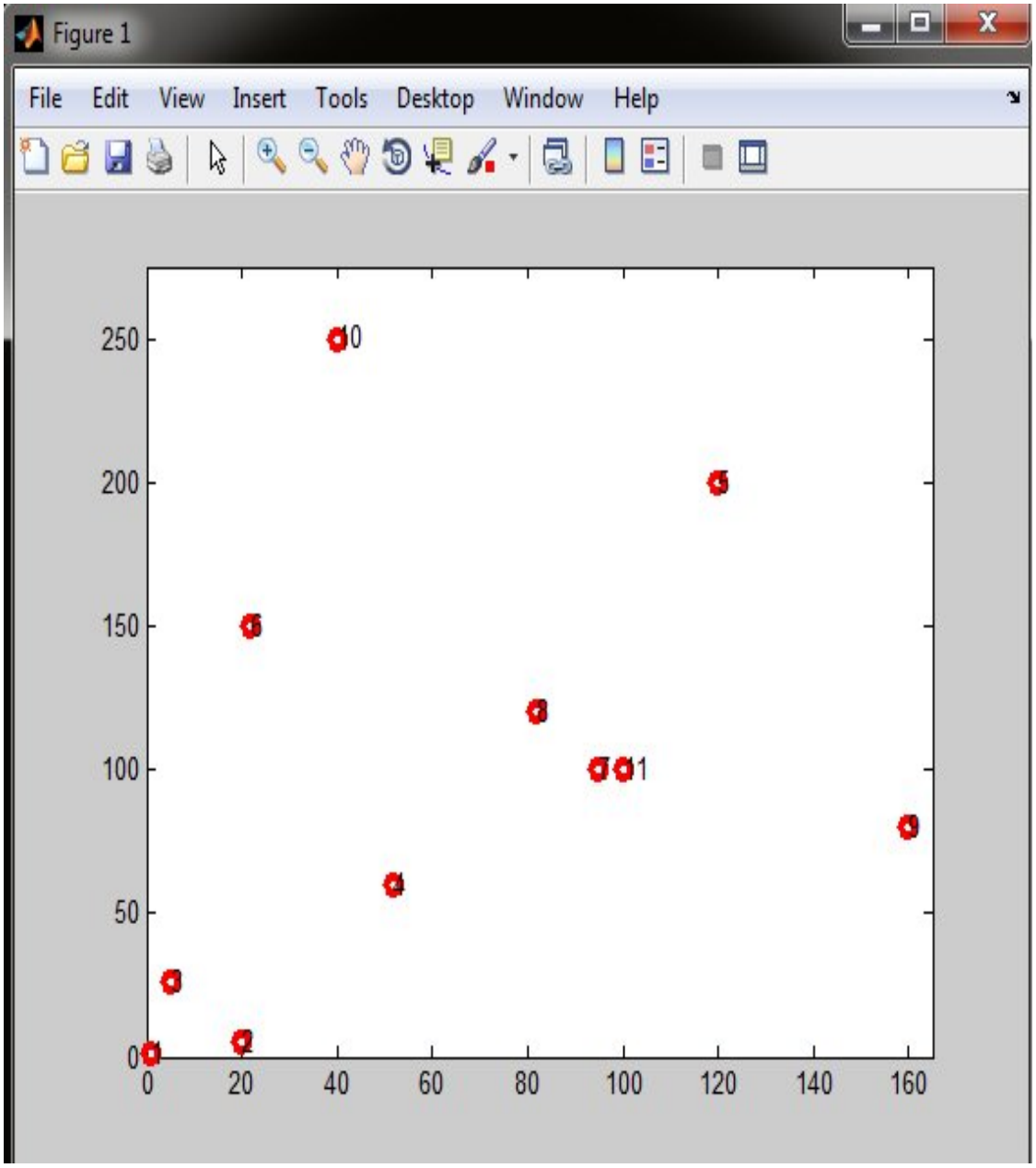

Figure 5.2: MANET

Above figure is showing a Mobile Ad hoc Network and 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 represent nodes present in the network.

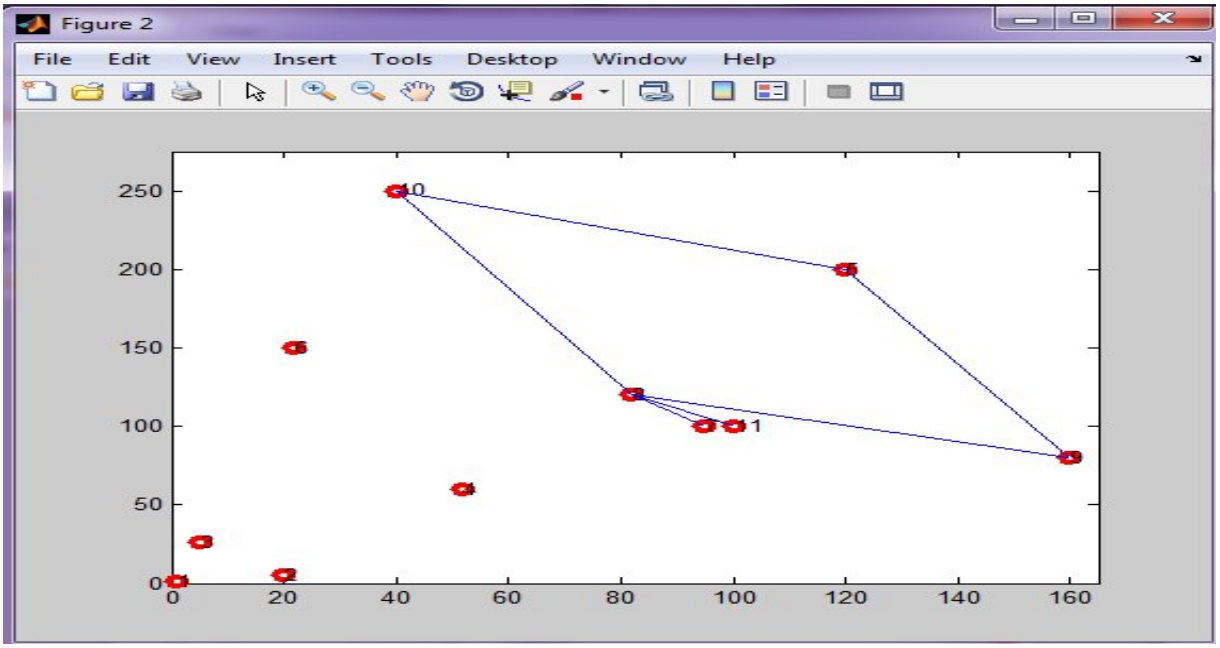

Figure 5.3: Source and destination

In Figure 5.3 Source is 10 and destination is 9. RREQ is send to only those nodes whose coordinates fall in between source and destination and that are within its range no other nodes will get RREQ message from source. Here source is 10 and destination is 9. So RREQ will be send to node 5, 8, 7, 11 and 9.

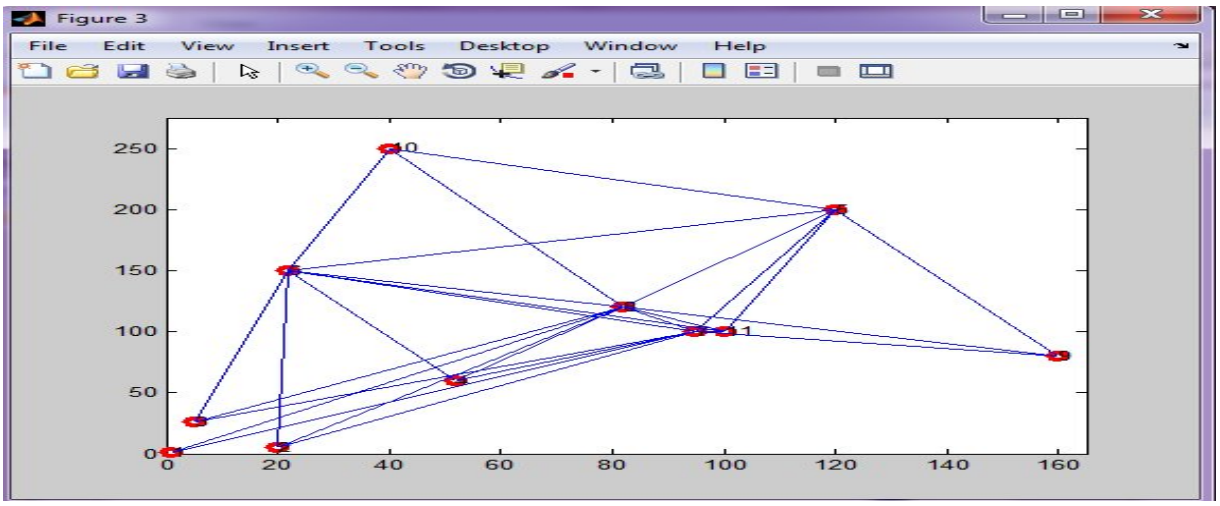

Figure 5.4: Path selected in original DSR and AOMDV

In figure 5.4 RREQ is sent to all nodes that are present in the network.

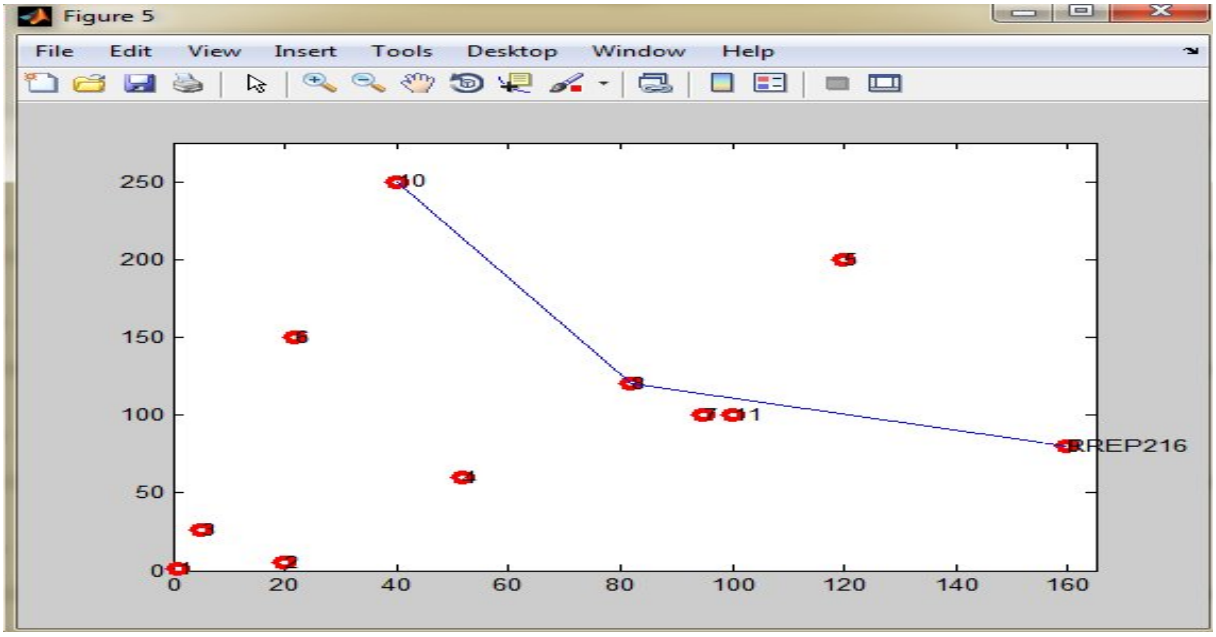

Figure 5.5: Route Reply

In above figure RREP is generated at node 9 with certification number 216 which is unique for each path

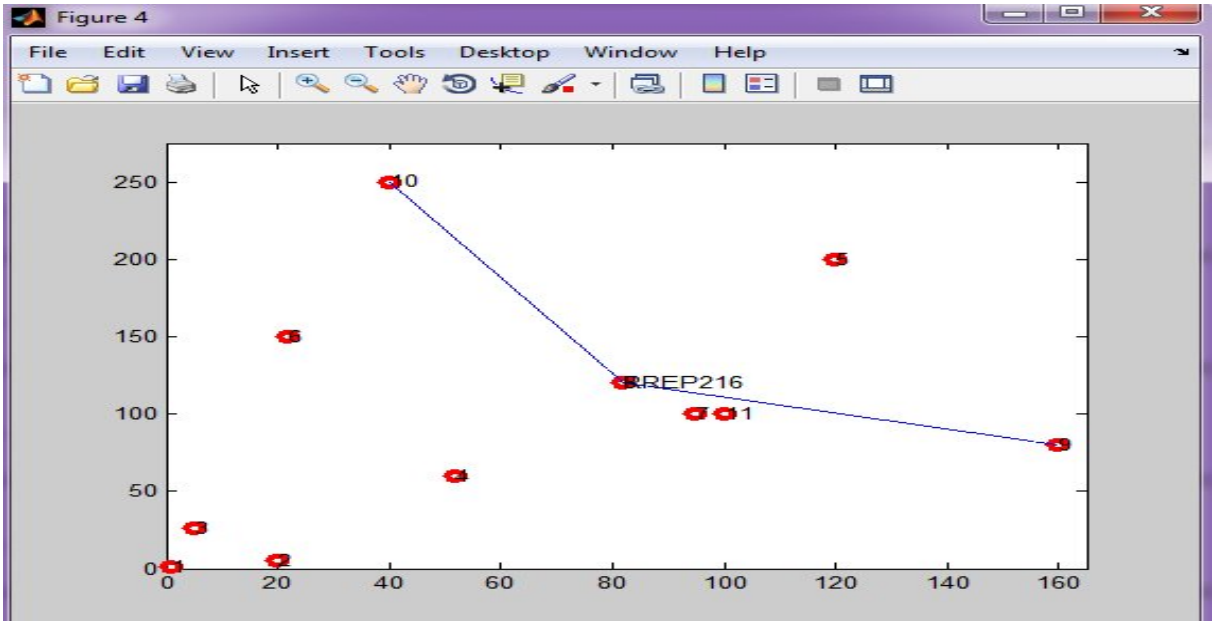

Figure 5.6: Route Reply

In figure 5.6 RREP is send from node 9 (destination) to node 8 (intermediate)

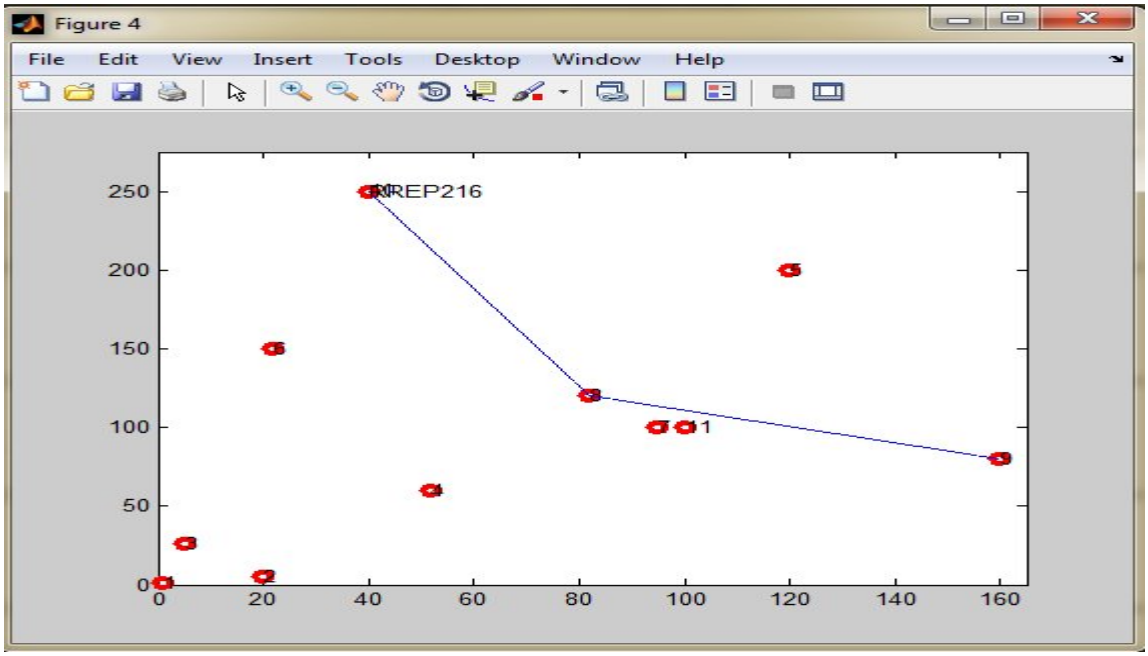

Figure 5.7: Route Reply

In figure 5.7 RREP is send from intermediate node (node 8) to source node (node 10)

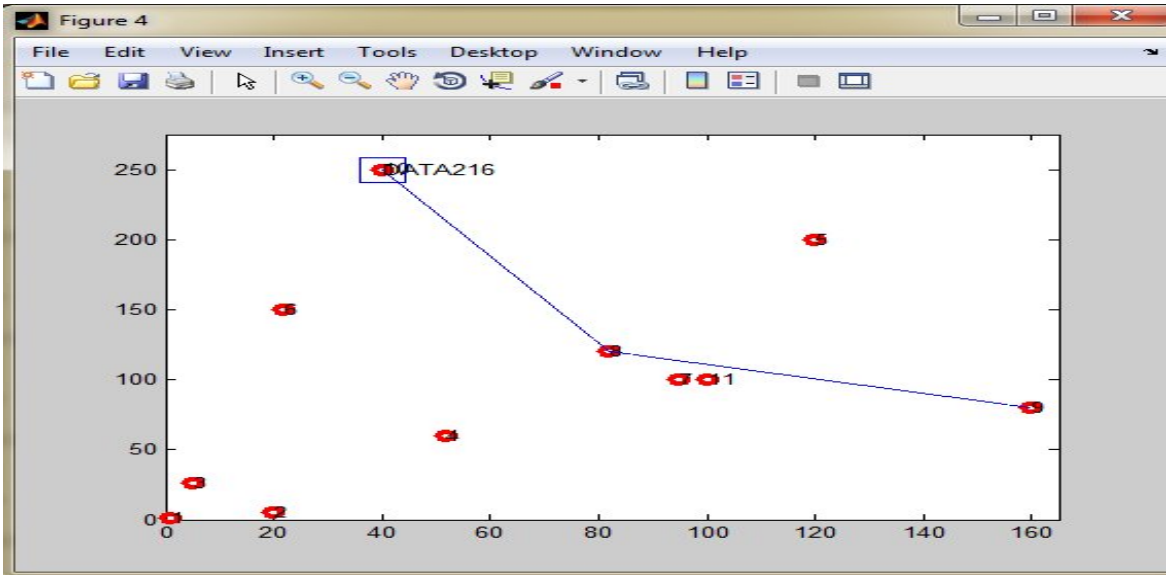

Figure 5.8: Data

In figure 5.8 data packet is generated at node 10 (source) which is to be send to destination

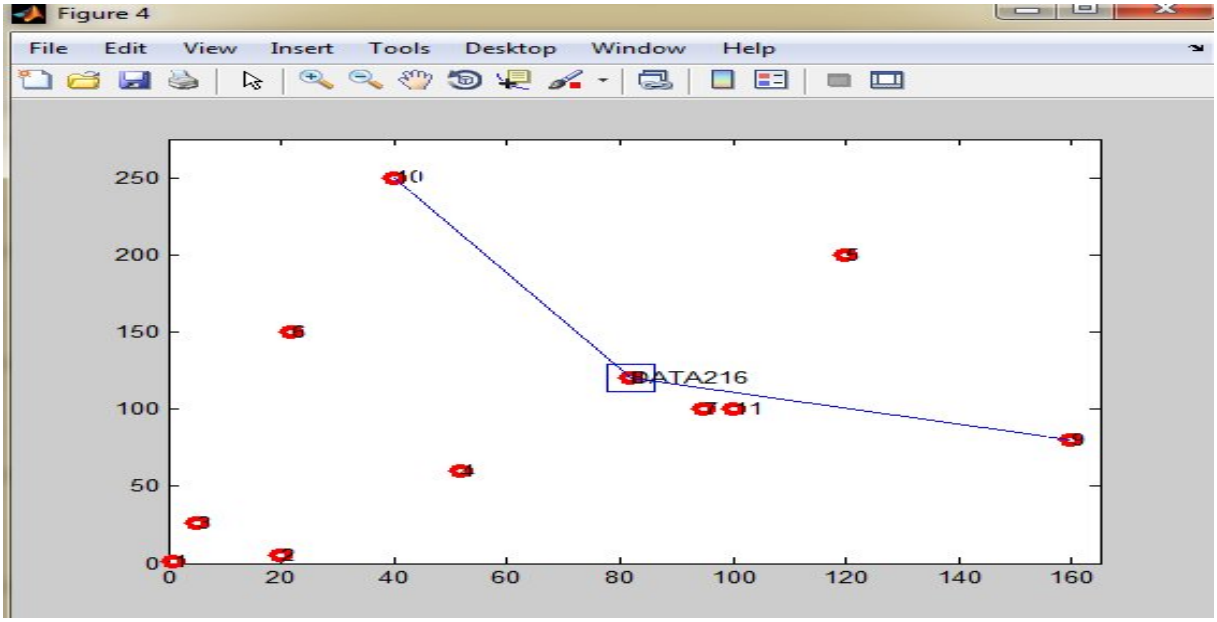

Figure 5.9: Data

In figure 5.9 data is send from node 10 (source node) to node 8 (intermediate node).

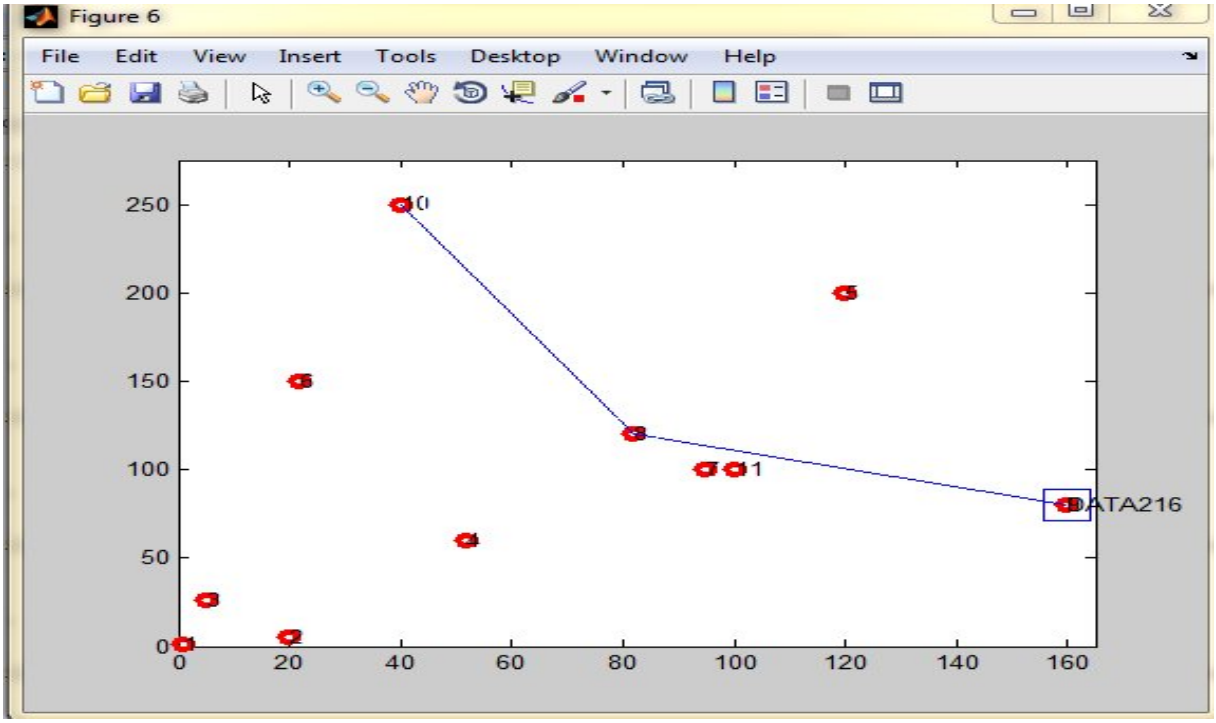

Figure 5.10: Data

In figure 5.10 data is send from node 8 (intermediate node) to node 9 (destination node)

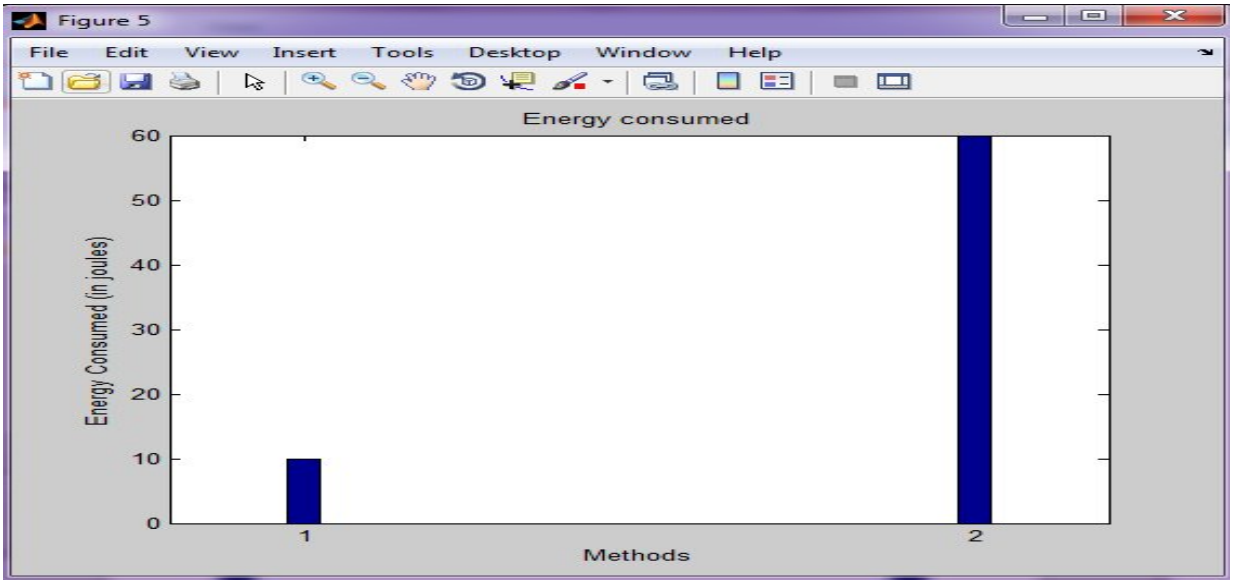

Figure 5.11: Energy consumed

Above figure represents total energy consumed in new method and previous method. And it is shown that new method consumes less energy as compared to previous method and this is because in new method RREQ is sent to only few nodes but in previous method RREQ is sent to all the nodes present in the network.

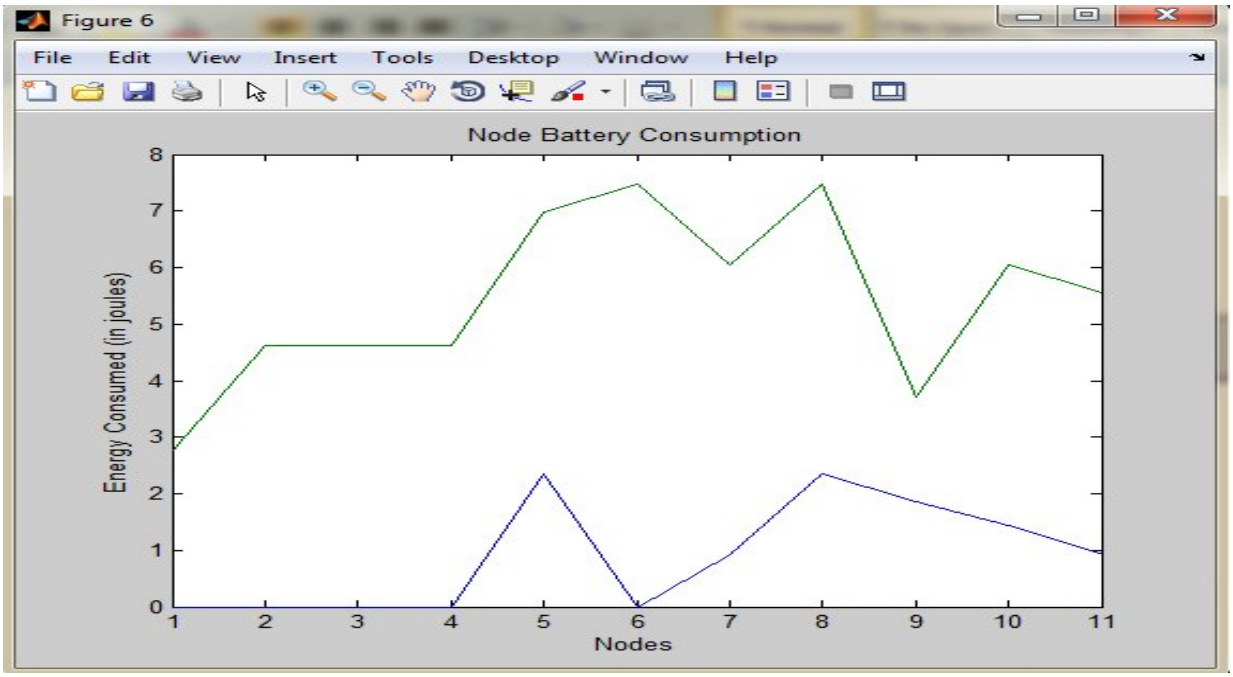

Figure 5.12: Node battery consumption

Figure 5.12 shows node battery consumption and it is clear that all nodes are consuming energy because in DSR and AOMDV as RREQ are sent to all the nodes. Hence energy consumption in this case is more as compared to new method as only node 5, 7, 8, 9, 10 and 11 are involved in the communication.

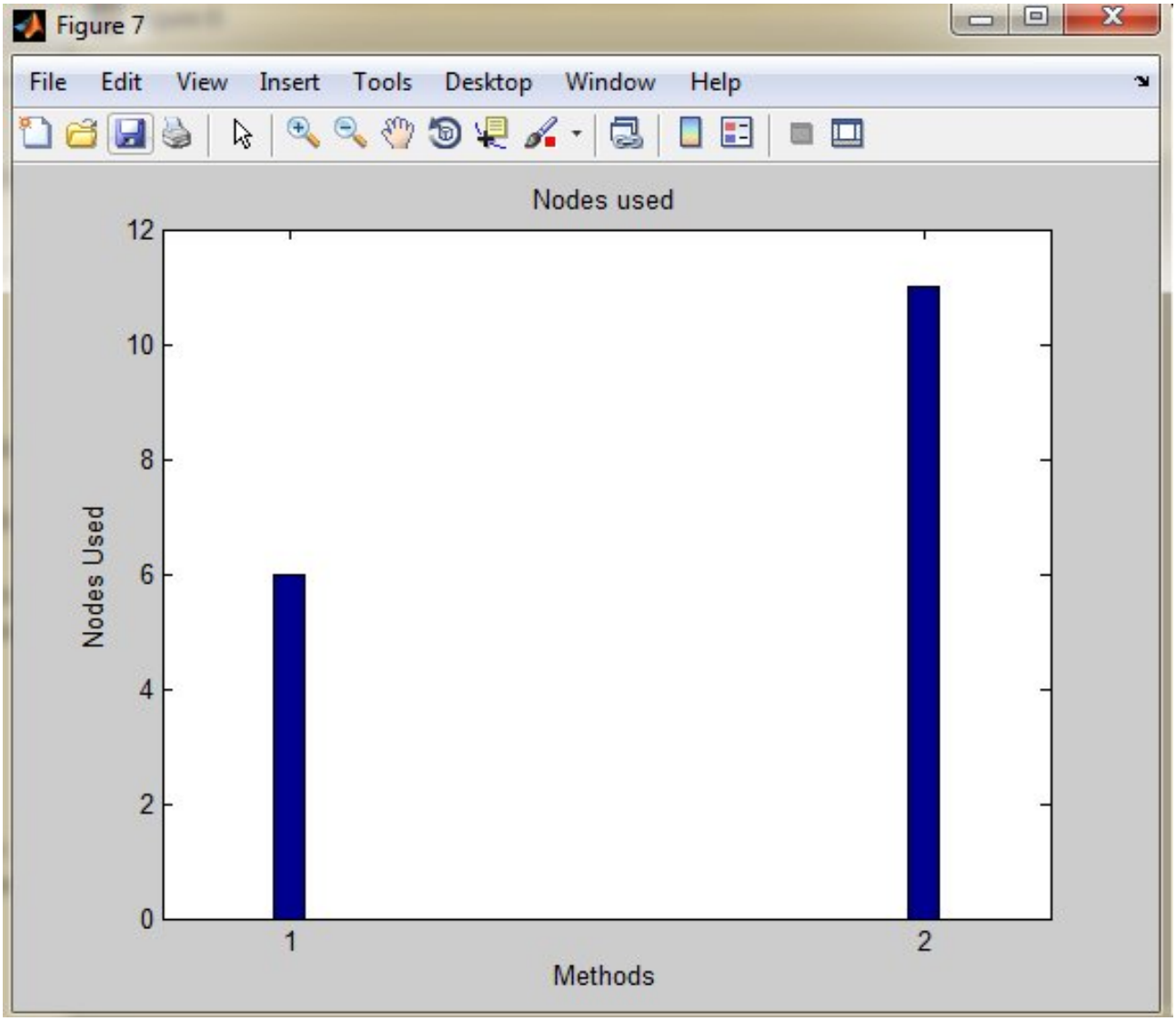

Figure 5.13: Nodes used

Figure 5.13 shows number of nodes used in new method (method 1) and previous method (method 2). Method 1 used 6 nodes for communication and method 2 used 11 nodes.

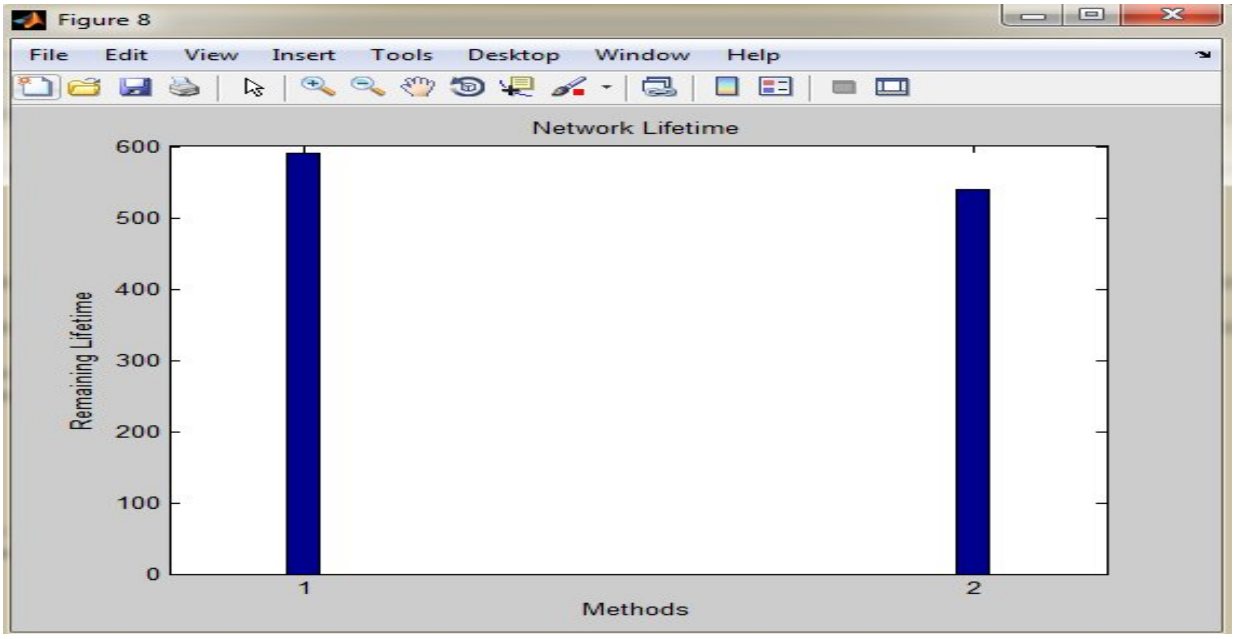

Figure 5.14: Remaining lifetime

Above figure represents how much lifetime is remaining and it shows method 1 have more remaining lifetime than method 2.

End- to – End delay: Average time taken by data packet to travel from source to destination.

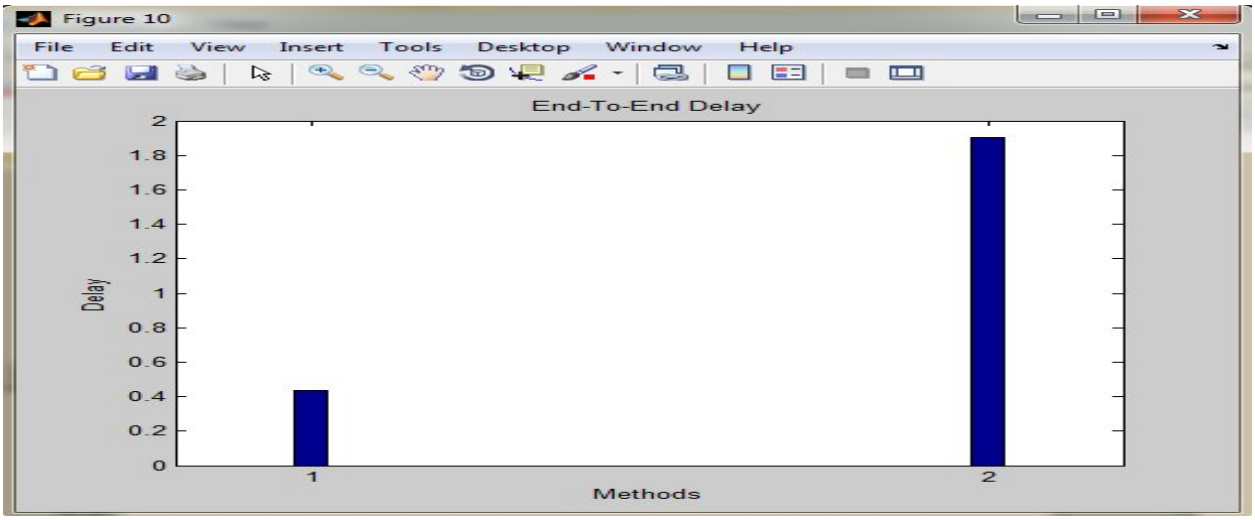

Figure 5.15: End -to-End delay

Figure 5.15 clearly shows that end-to-end delay in method 1(new) is less than method 2 (previous).

```
failure occur at:
No failure

New
path:
    10     8     9

duration:
  3.6667e-004


All
path:
    10     8     9

duration:
  4.0000e-004

efficiency in %=
    8.3533
```

Figure 5.16: Duration and Efficiency

Figure 5.16 shows the duration or total time taken to send data from source and destination. Here new path represents path selected in new method and all path represents path selected in previous method. And efficiency is also shown in this figure which is approx 8% more than previous method.

CASE 2: FAILURE

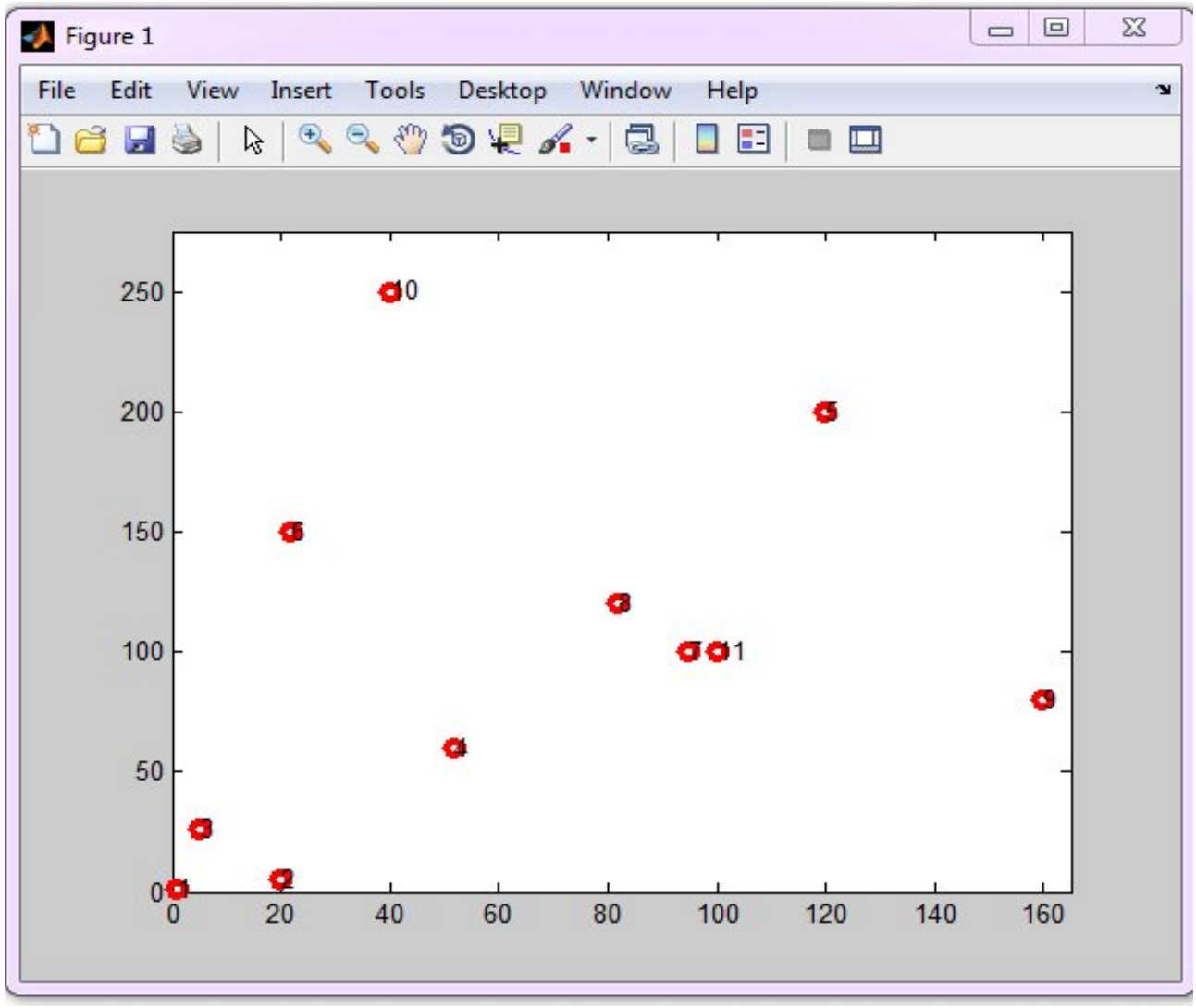

Figure 5.17: MANET

Above figure is showing a Mobile Adhoc Network and 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 represents nodes present in the network.

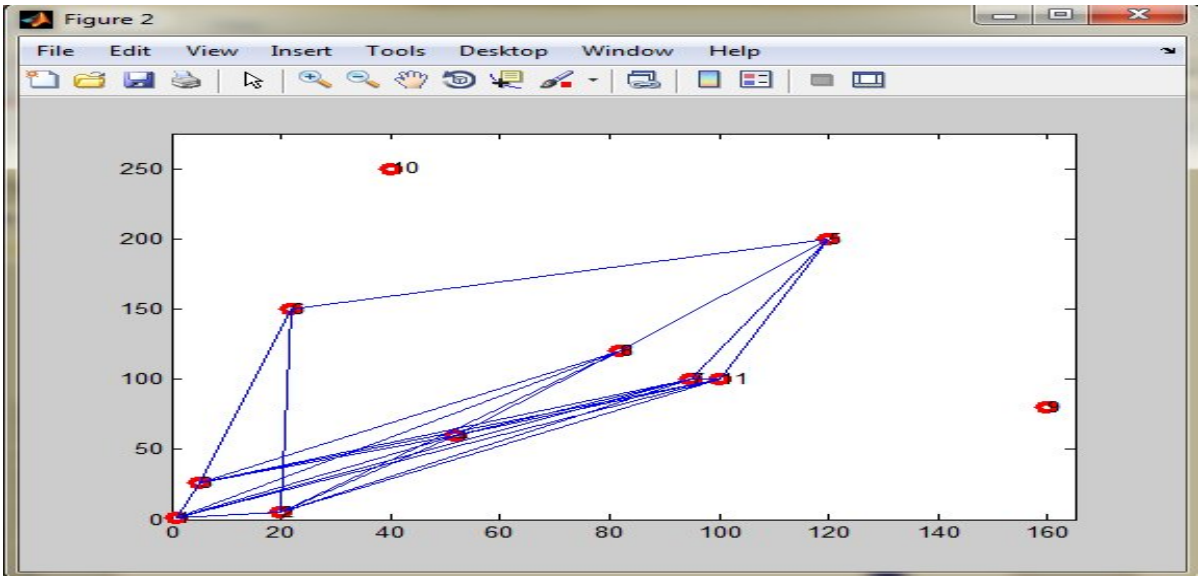

Figure 5.18: Source and destination

In Figure 5.18, source is 1 and destination is 5. RREQ is send to only those nodes whose coordinates fall in between source and destination and that are within its range no other nodes will get RREQ message from source. Here source is 10 and destination is 9. So RREQ will be send to node 1, 2, 3, 4, 5, 6, 7 and 8

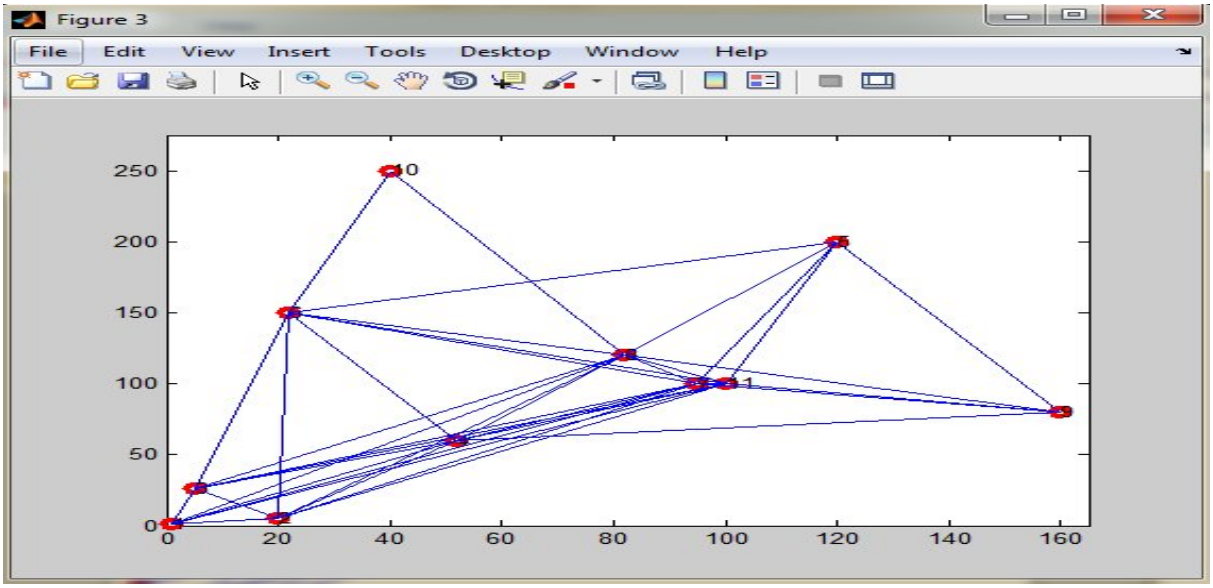

Figure 5.19: Path selected in original DSR and AOMDV

In figure 5.19 RREQ is sent to all nodes that are present in the network.

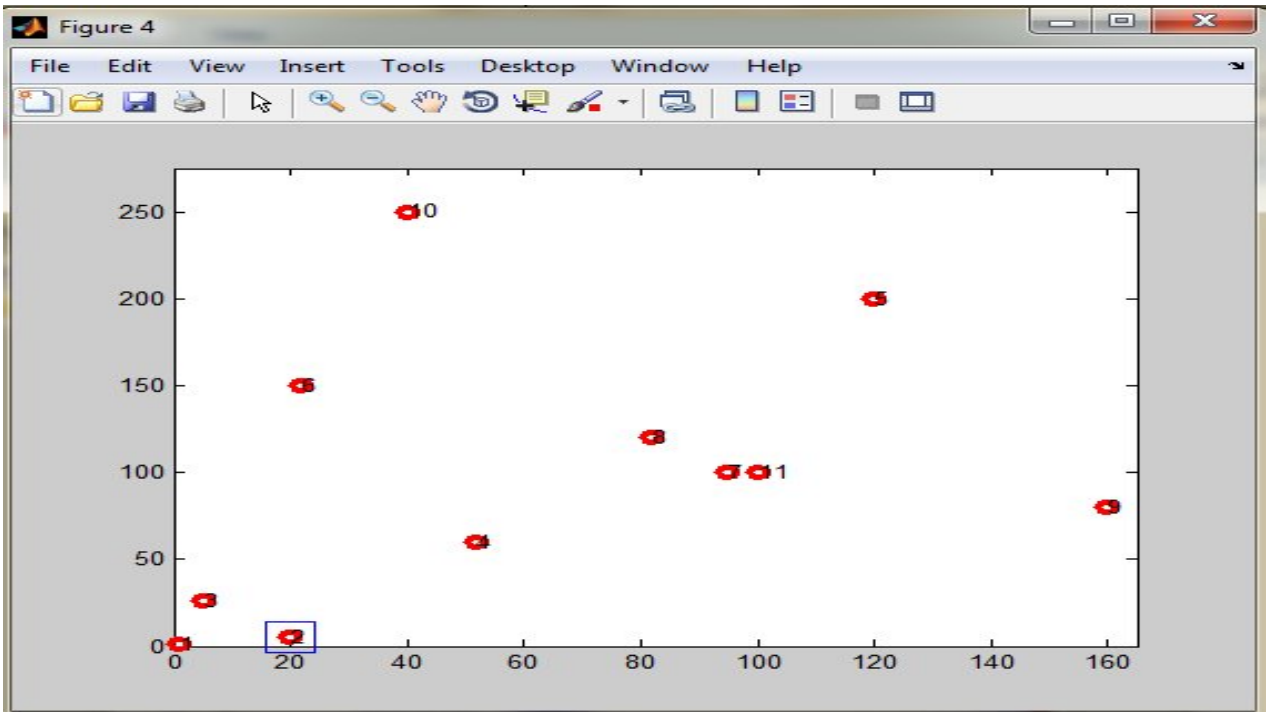

Figure 5.20: Link failure

Figure 5.20 show that there is link failure at node 2 so no path will be selected using node 2.

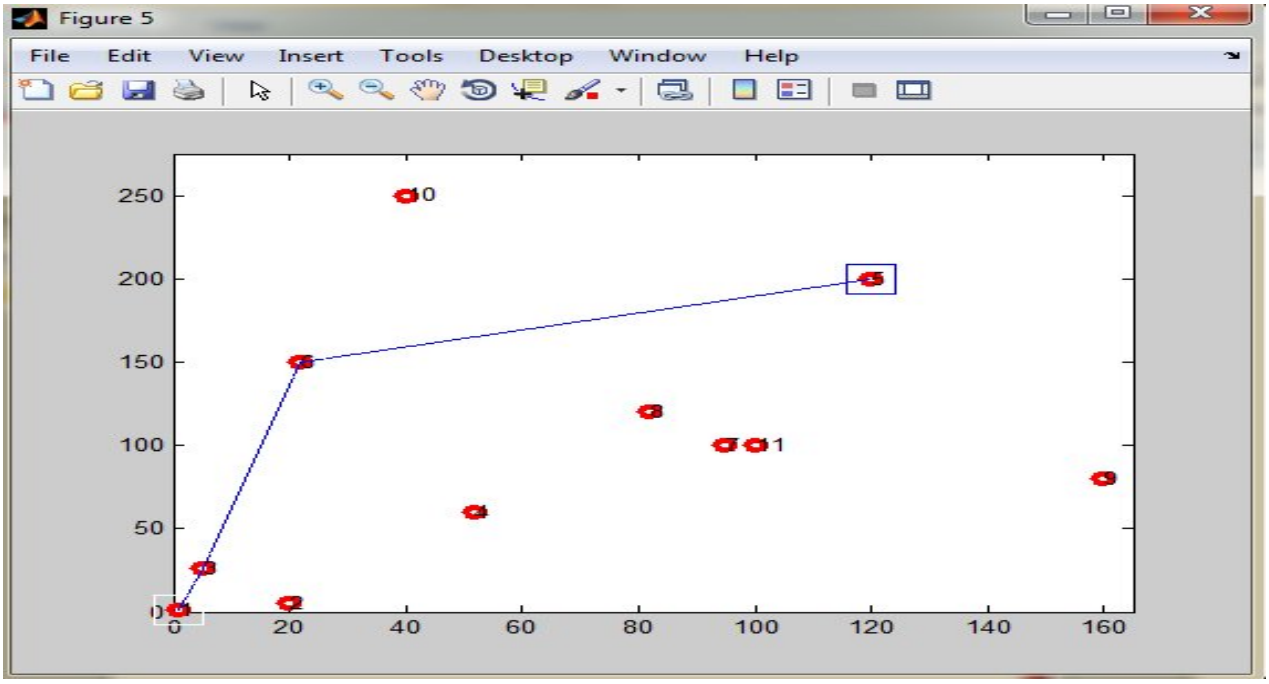

Figure 5.21: Path selected

This figure shows path selected to send the data

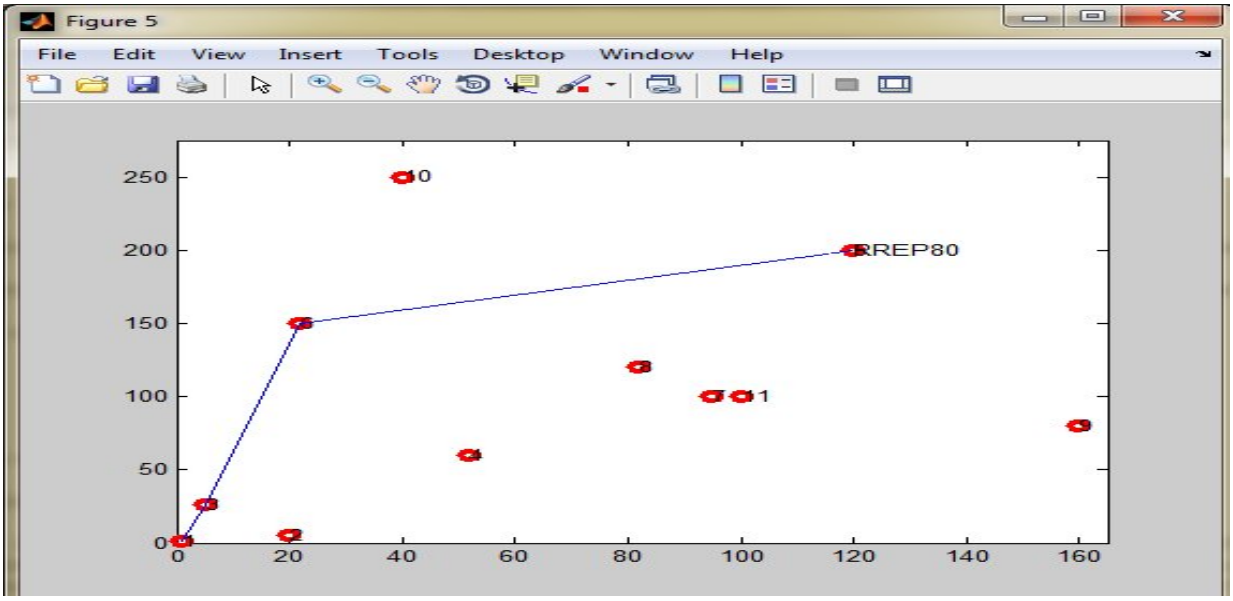

Figure 5.22: Route Reply

In above figure RREP is generated at node 5 (destination) with certification number 80 which is unique for each path

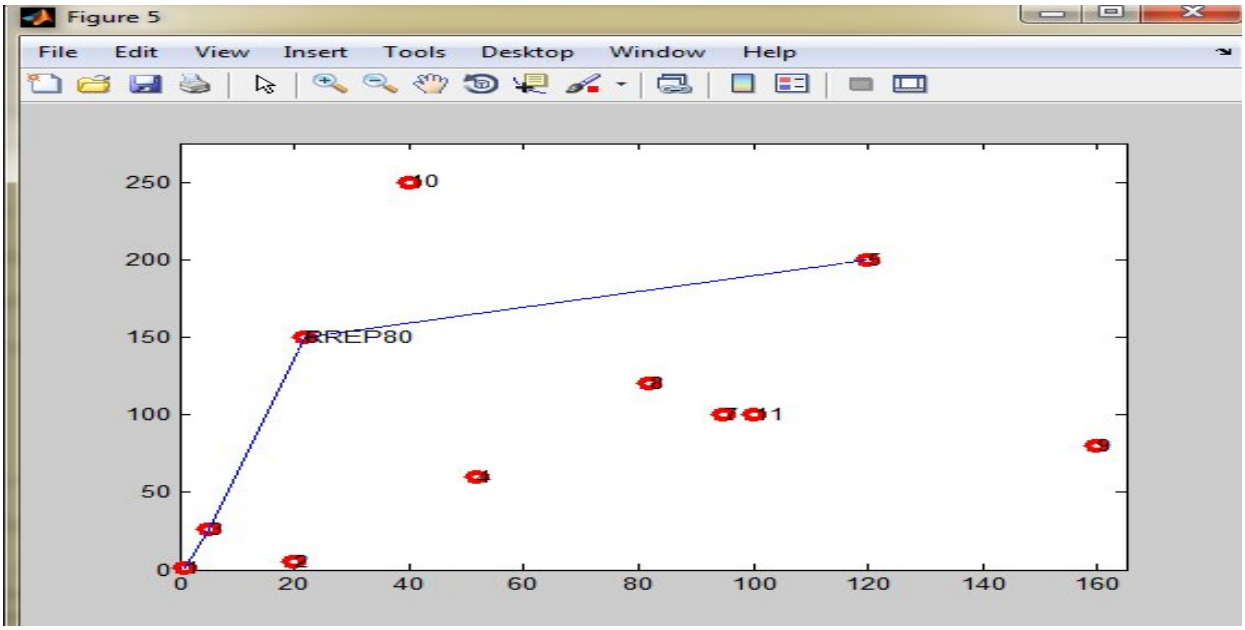

Figure 5.23: Route Reply

In figure 5.23 RREP is send from node 5 (destination) to node 6 (intermediate)

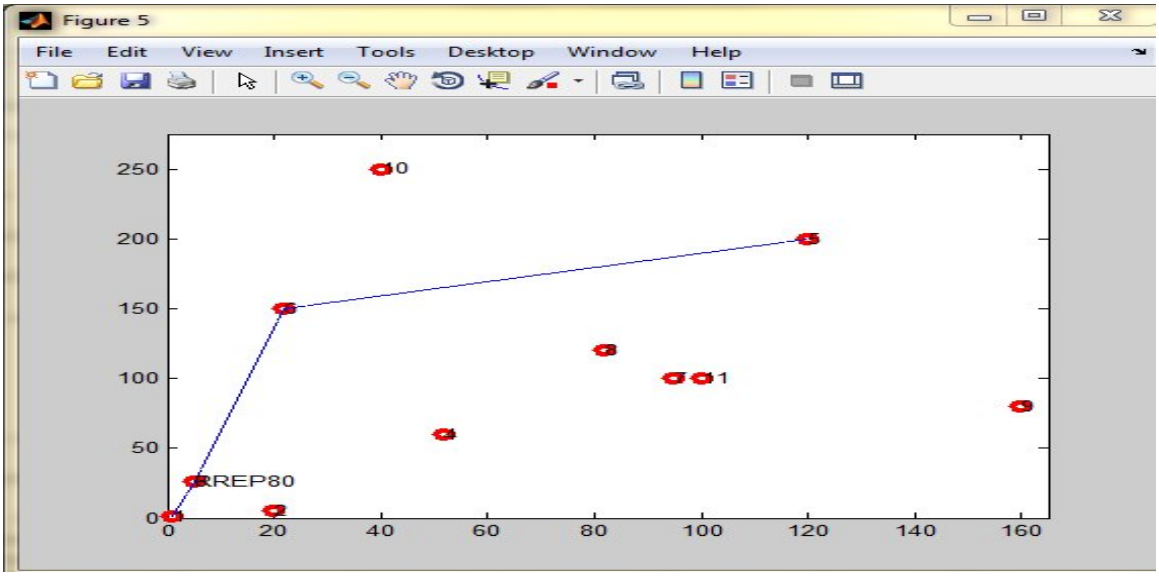

Figure 5.24: Route Reply

In figure 5.24 RREP is send from node 6 (intermediate) to node 3 (intermediate)

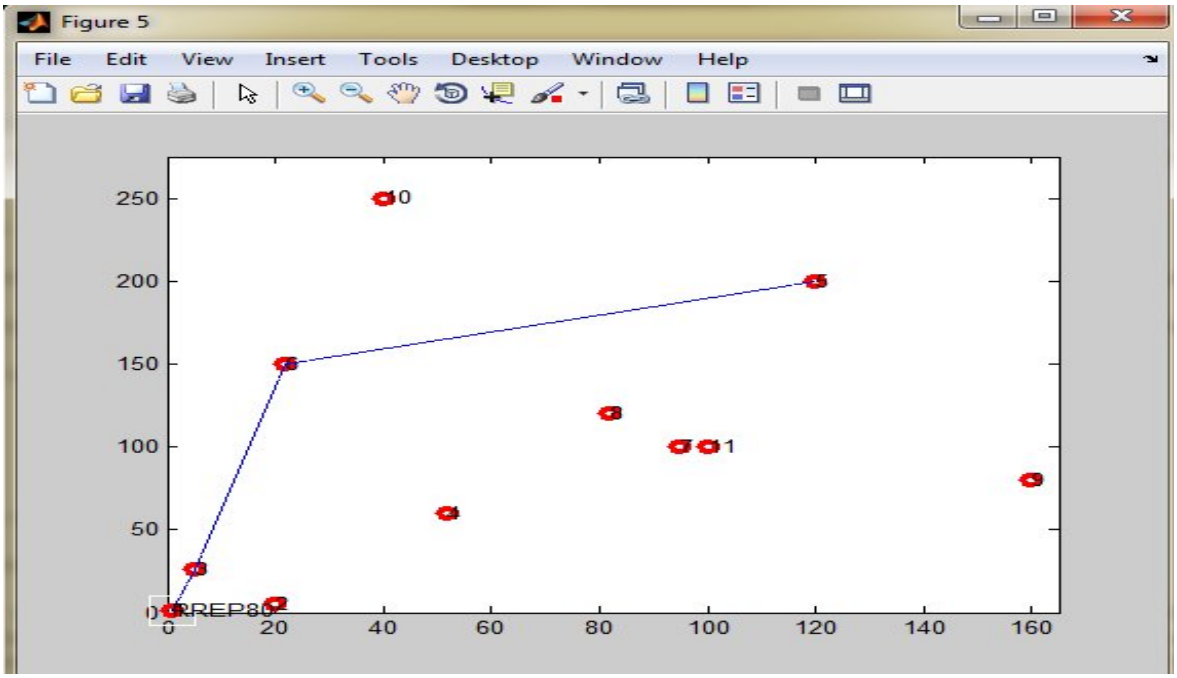

Figure 5.25: Route Reply

In figure 5.25 RREP is send from node 3 (intermediate) to node 1 (destination)

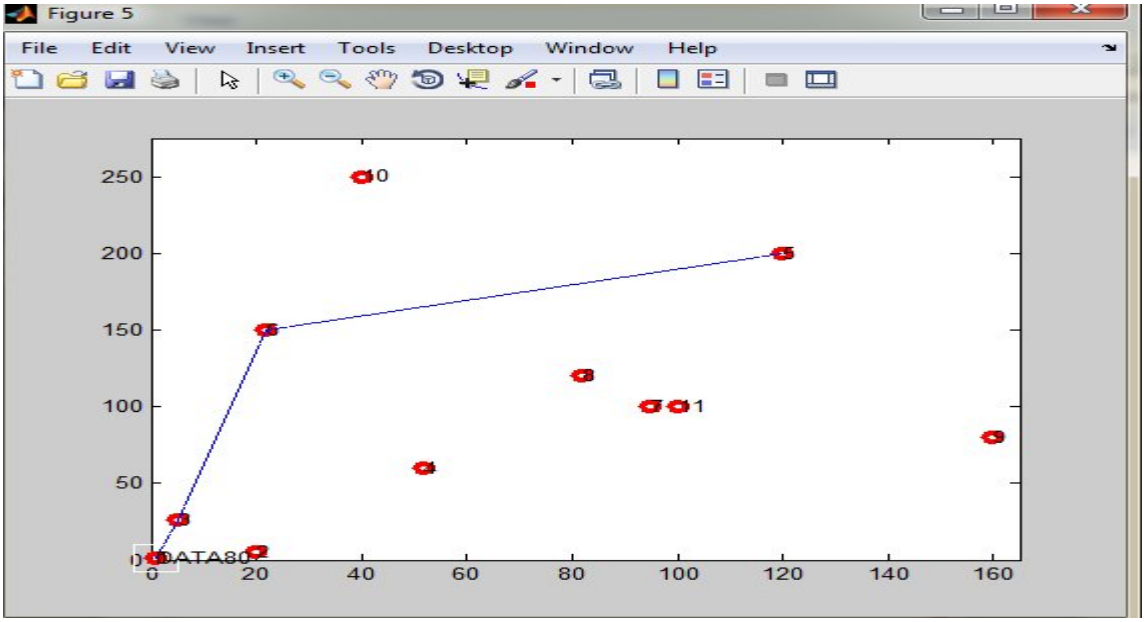

Figure 5.26: Data

In figure 5.26 data packet is generated at node 1 (source) which is to be sent to destination

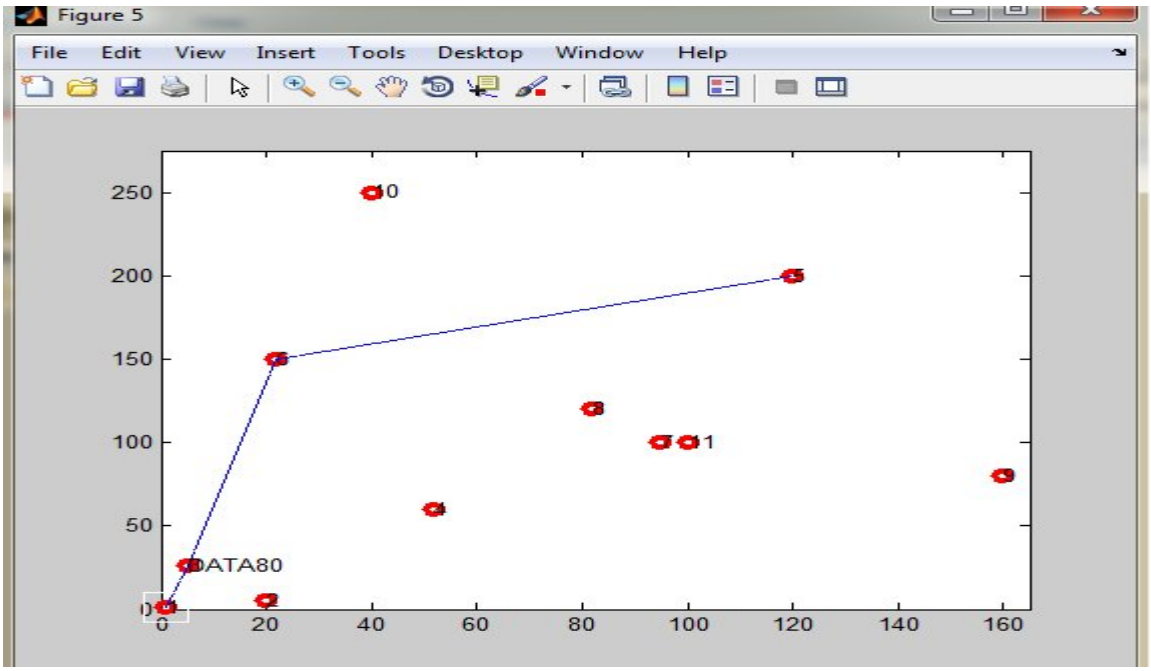

Figure 5.27: Data

In figure 5.27 data is send from node 1 (source node) to node 3 (intermediate node).

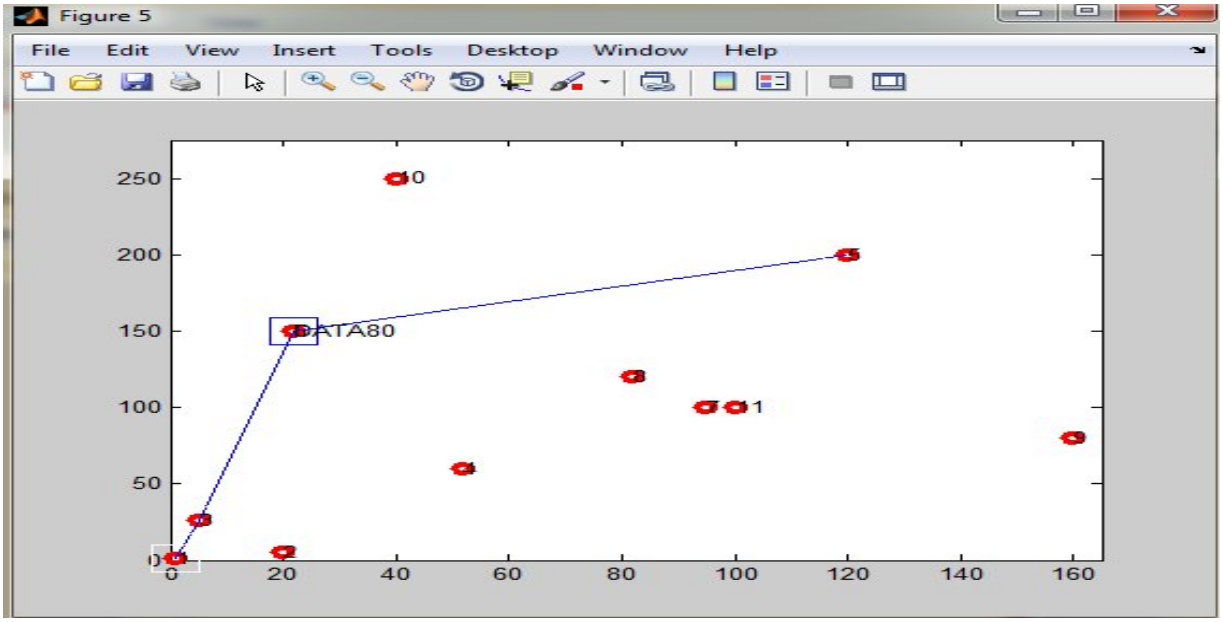

Figure 5.28: Data

In figure 5.28 data is send from node 3 (intermediate node) to node 6 (intermediate node).

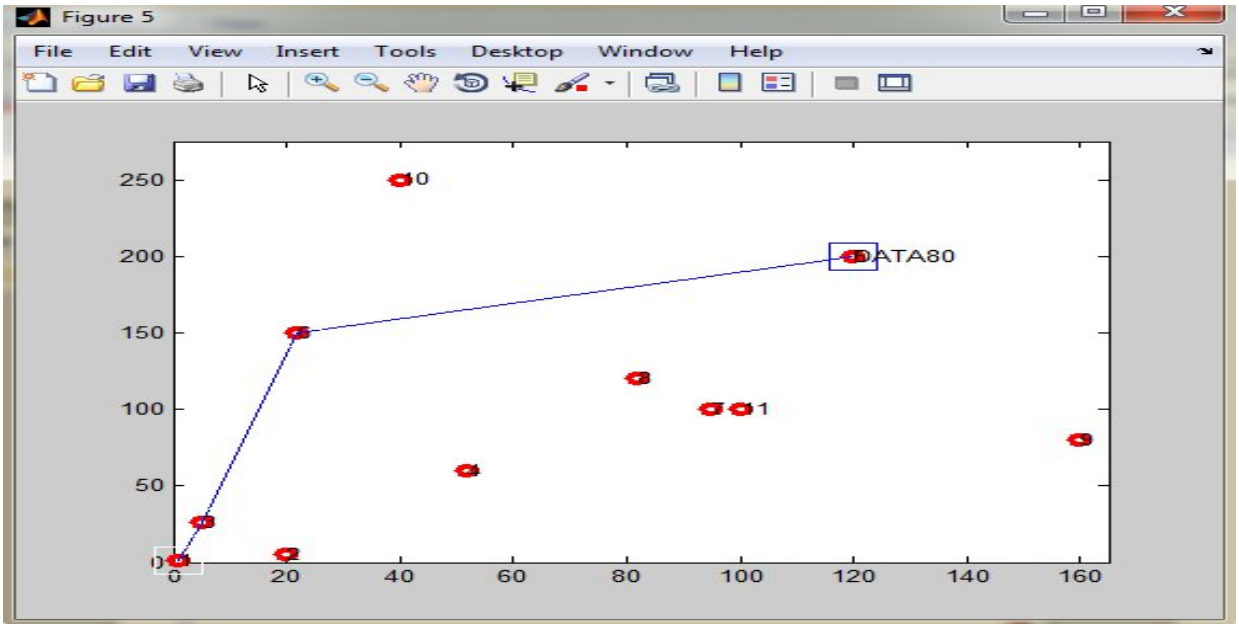

Figure 5.29: Data

In figure 5.29 data is send from node 6 (intermediate node) to node 5 (destination).

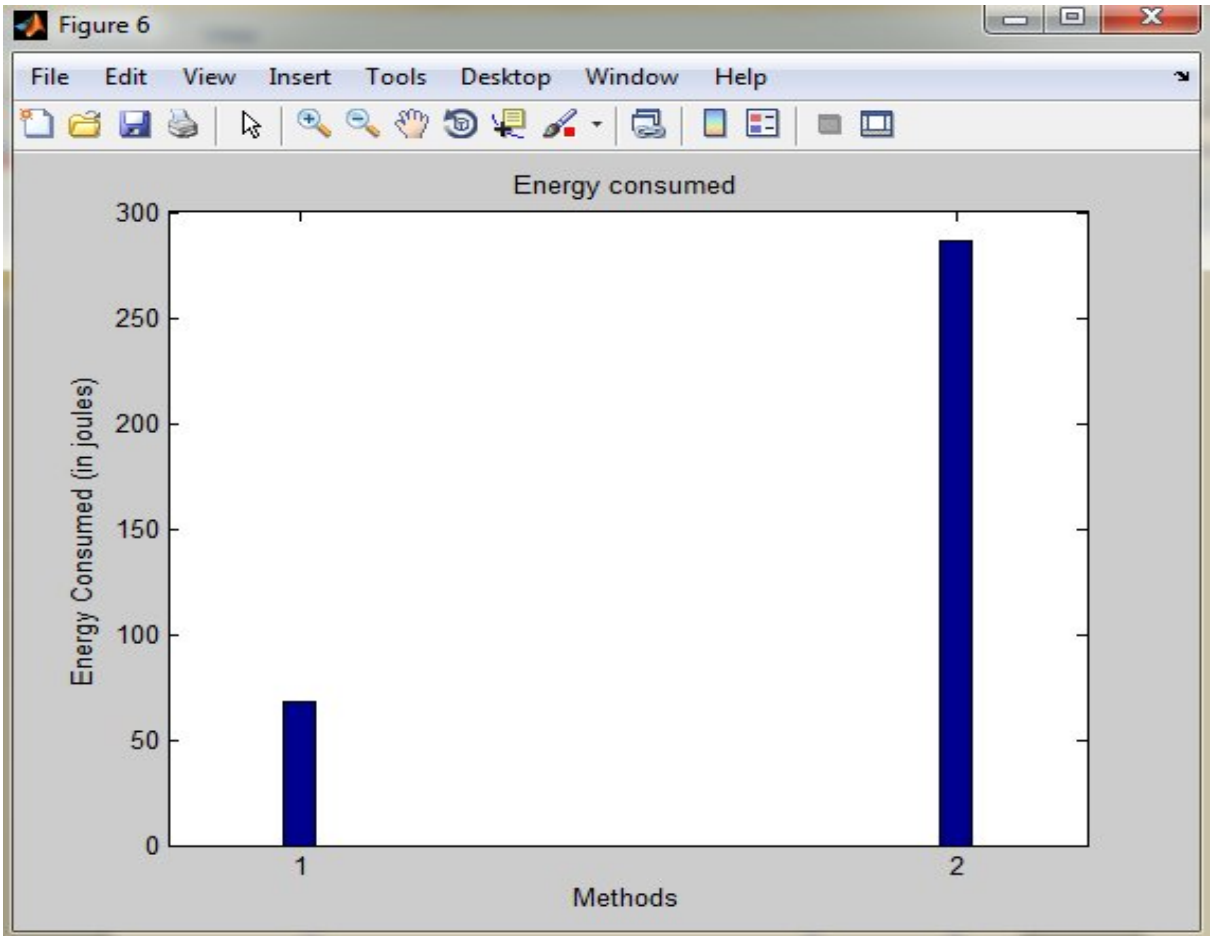

Figure 5.30: Energy consumed

Above figure represents total energy consumed in new method and previous method. And it is shown that new method consumes less energy as compared to previous method and this is because in new method RREQ is sent to only few nodes but in previous method RREQ is sent to all the nodes present in the network

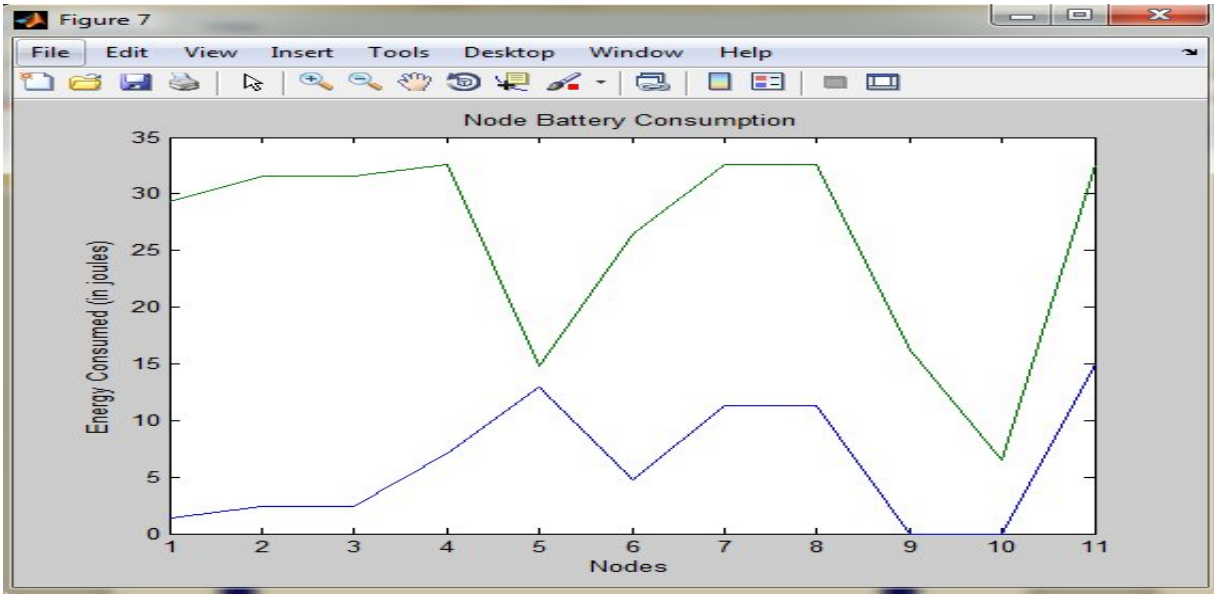

Figure 5.31: Node battery consumption

Figure 5.31 shows node battery consumption and it is clear that all nodes are consuming energy because in DSR and AOMDV as RREQ are sent to all the nodes. Hence energy consumption in this case is more as compared to new method as node 1, 2, 3, 4, 5, 6, 7 and 8 are involved in the communication.

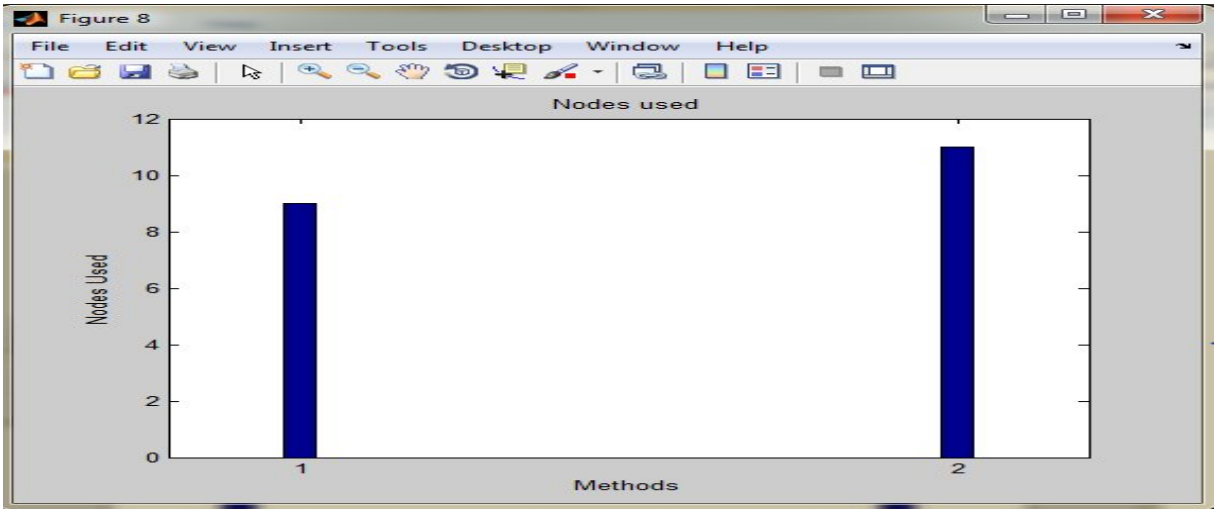

Figure 5.32: Nodes used

Figure 5.32 shows number of nodes used in new method (method 1) and previous method (method 2). Method 1 used 9 nodes for communication and method 2 used 11 nodes.

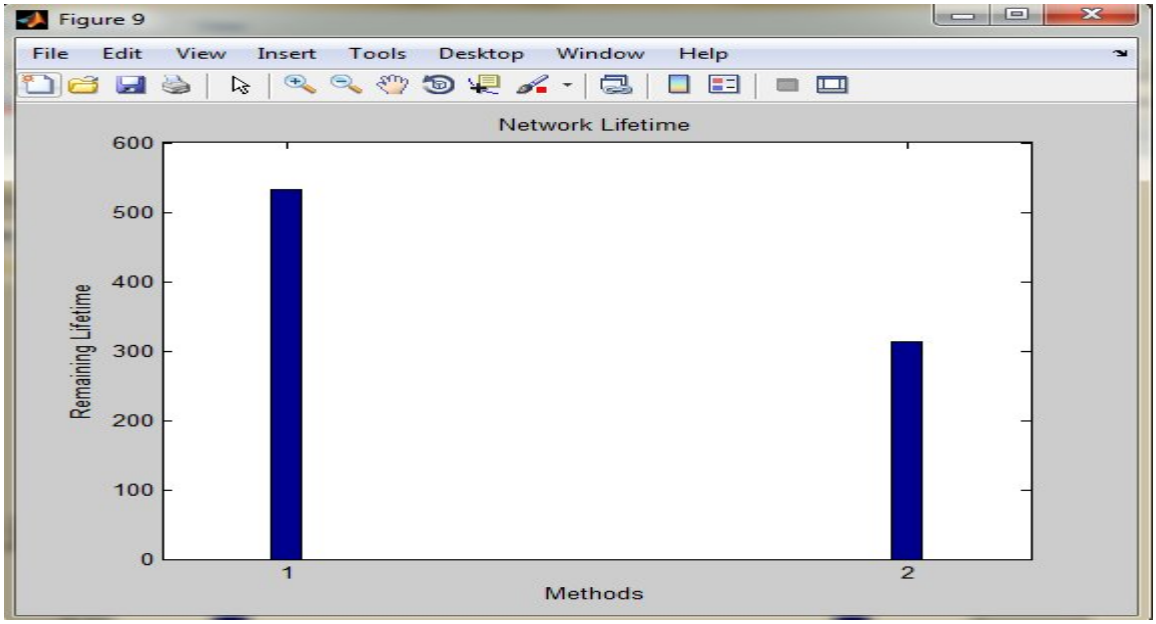

Figure 5.33: Remaining lifetime

Above figure represents how much lifetime is remaining and it shows method 1 have more remaining lifetime than method 2.

Throughput : It is the rate of successful data delivery over the communication channel

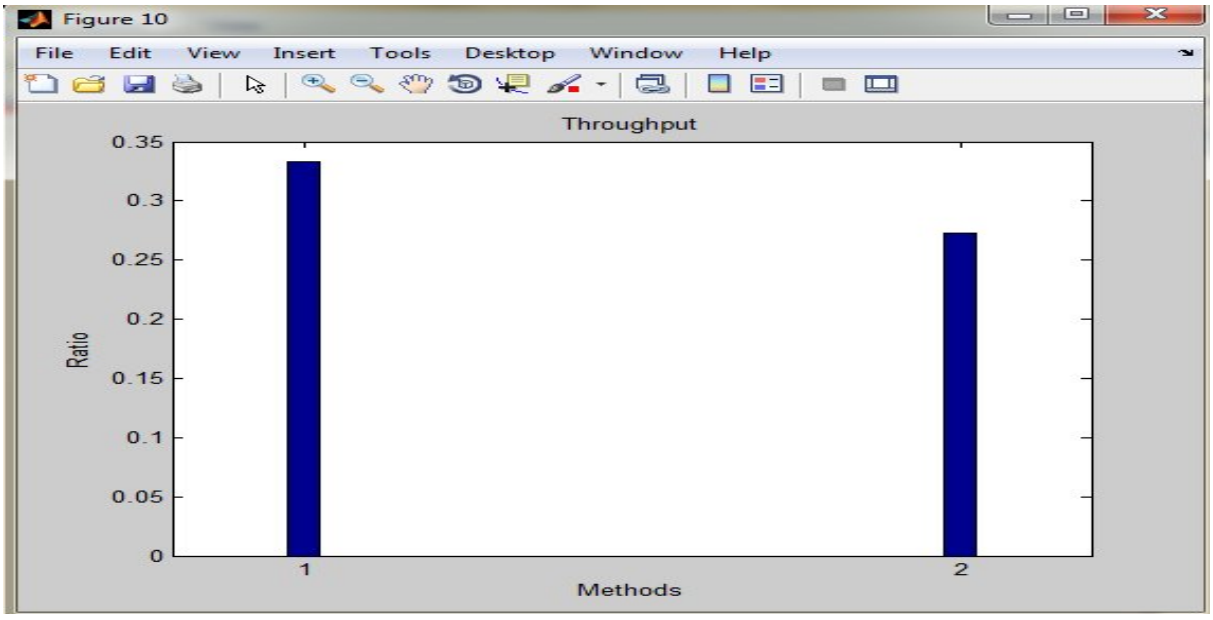

Figure 5.34: Throughput

Figure 5.34 shows throughput new method (method 1) is higher than previous method (method 2)

End-to- End delay: Average time taken by data packet to travel from source to destination.

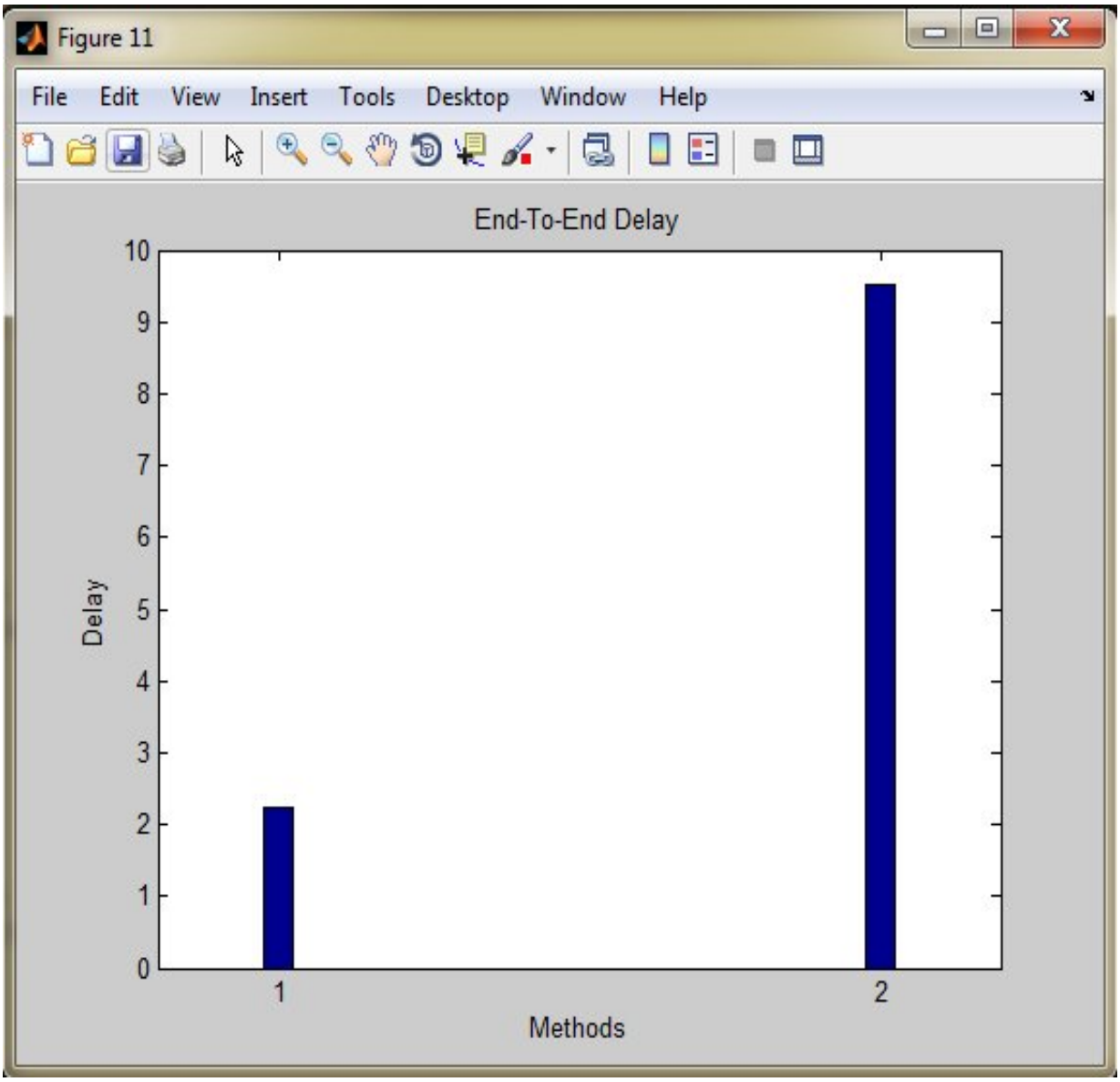

Figure 5.35: End-to-End delay

Figure 5.35 clearly shows that end-to-end delay in method 1(new) is less than method 2 (previous).

```
failure occur at:
    2


    1    2    6    5
```

Figure 5.36: Link Failure

Figure 5.36 shows link failure that occurs at node 2. Hence the path 1, 2, 6, 5 that is previously selected will be discarded and new path will be selected.

```
New
path:
     1     3     6     5

duration:
    0.0015


All
path:
     1     3     6     5

duration:
    0.0024

efficiency in %=
   36.3983
```

Figure 5.37: Duration and efficiency

Figure 5.37 shows the duration or total time taken to send data from source and destination. Here new path represents path selected in new method and all path represents path selected in previous method. And efficiency is also shown in this figure which is approx 36% more than previous method.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

MANET is self organizing, adaptive, infrastructure less so each and every node has the capability to move from one destination to another destination and due to this random mobility, routing becomes an issue. Every node acts as both host and router at the same time and transfer of packet from one node to another node is done by the help of routing protocols. If the node is frequently moving then it becomes an issue for providing secure routing. There are many routing protocols and each having unique features. Selecting a routing protocol is based on the network environment. Basically there are three types of routing protocols proactive, reactive and hybrid protocol. MANET is vulnerable to security attacks which when comes into play can decrease the performance of communication protocol. There are many protocols which have the capability to handle it at some extent but when the network is complex and have multipath then performance degradation occurs. So there is an urgent requirement to transfer data at higher rates. Hence successful implementation of a hybrid approach in MANET has been done in this thesis and it is giving good result in terms of energy, time, security and efficiency. Minimization of energy is there which is done by using a technique in which RREQ is only send to those nodes whose coordinates come in between source and destination. And if nodes coordinates are not in between source and destination then that node will be discarded. Then RREP is sent back from destination to source using the shortest path .This technique proves to be advantageous as rest of the nodes present in the network will not lose their energy and they will remain idle. Time complexity is also reduced. And security is provided by using SBPGP security model. When RREP message is sent back it is attached with certification ID (which is unique for every path). And when any other node try to send packet then it is not possible because of this certification ID. Hence by applying all these techniques efficiency of the network is also improved. In future this technique can be applied to various multicast routing protocols like Distance Vector Multicast routing protocols (DVMRP) and Multicast Open Shortest Path First (MOSPF).

CHAPTER 6

REFERENCES

JOURNALS

A.Parvathavarthini, D. S. (2013). An overview of Routing Protocols in Mobile Adhoc Network. *International Journal of Advanced Research in Computer Science and Software Engineering* .

Arri, R. S. (2013). Analysis of QOS parameters of AAMRP and IODMRP using SBPGP security model. *International Journal of Computer Application* .

Boundpadith Kannhavong, H. N. (2007). A survey on routing attacks in mobile adhoc network. *Wireless Communication, IEEE* , 7.

D.Sharmila, J. N. (2013). Power Aware Progressive Energy Routing Protocol for MANET. *International Journal of Computer Application* .

Indrani Das, D. L. (2014). Effect of mobility on AOMDV protocol in MANET. *International Journal of Wireless and Mobile Networks* .

Janish, N. M. (2013). Performance Evaluation of AODV and DSDV under Seniority Based Pretty Good Privacy Model (SBPGP). *International Journal of Scientific and Engineering Research* .

Kumar, R. K. (2014). Minimizing the Route Rediscovery Process in MANET. *Journal of Theoretical and Applied Information Technology* .

Moukhtar A. Ali, A. E.-S. (2007). A survey of multicast routing protocols for ad-hoc wireless networks. *Minufiya Journal of Electronics Engineering Research (MJEER)* .

P.Kanungo, S. a. (2012). Performance analysis of AODV, DSR, OLSR and DSDV Routing protocols using NS2 Simulator. *Elsevier* .

Quamar, M. R. (2008). A Hybrid Cryptography Model for managing Security in Dynamic Topology of MANET. *Internation Symposium on IEEE* , 1-7.

Rizvi, M. S. (2013). A proficient approach to amplify packet delivery ratio adapting shortest path algorithm. *International Journal of Computer Application* .

Sharma, A. G. (2014). A survey on Location Based Routing protocol in MANET. *International Journal of Computer Science and Information Technology* .

Sran, J. K. (2012). SBPGP Security based model in Large scale MANETs. *Internation Journal of Wireless Networks and Communications* , 1-10.

V.Seethalakshmi, J. J. (2012). Performance analysis and enhancement of routing protocol in MANET. *Internation Journal of Modern Engineering Research* , 323-328.

WEBSITES

techterms.com/definition/manet

www.antd.nist.gov/wahn_mahn.shtml

webcache.googleusercontent.com/search?q=cache:OqAKaViq57IJ:https://www.ietf.org/rfc/rfc2501.txt+&cd=10&hl=en&ct=clnk&gl=in

perso.crans.org/raffo/papers/phdthesis/thesisch3.html

BOOKS

Mobile Ad Hoc Networking by Stefano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic John Wiley & Sons, 07-Oct-2004

Secure Routing in Wireless Mobile Ad Hoc Network by Mishra Manuj (Author), Sharma Govind (Author), Pathak Ram (Author) 28 Apr 2014

CHAPTER 7
APPENDIX

7.1 ABBREVIATIONS

AODV	Ad hoc On Demand Vector
AOMDV	Ad hoc On demand Multipath Distance Vector
AAMRP	Ant Based Multipath Routing Protocol
CA	Certifying Authority
CGSR	Cluster Gateway Switch Routing
DOS	Denial of Service
DSDV	Distance –Sequence and Distance-Vector
DSR	Distance Source Routing
IODMRP	Improved On demand Multipath Routing Protocol
IMANET	Internet based Mobile Ad hoc Network
JN	Junior Node
MANET	Mobile Ad hoc Network
OSI	Open System Interconnections
PAN	Personal Access Network
PDR	Packet Delivery Ratio
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure

SANET	Static Ad hoc Network
SB	Seniority Based
SN	Senior Node
SCA	Set of nodes required for Certifying Authority
SBPGP	Seniority Based Pretty Good Privacy
SHARP	Sharp Hybrid Adaptive Routing Protocol
SPAN	Smart Phone Ad hoc Network
TORA	Temporarily Ordered Routing Algorithm
VANET	Vehicle Ad hoc network
WRP	Wireless Routing Protocol
ZRP	Zone Routing Protocol

7.2 GLOSSARY TERMS

MANET- A mobile ad hoc network is a network formed by number of nodes moving in an arbitrary manner.

Open System Interconnection (OSI) model- A model of communications between cooperating devices. It defines seven- layer architecture of communication functions

Protocol- A set of rules that govern the operation of functional units to achieve communication

QOS- It refers to the properties of a network that contribute to the degree of satisfaction that users perceive, relative to the network's performance. Four service categories are typically included under this term: data rate, delay, traffic loss.

Router- An internetworking device that connects two computer networks. It makes use of an internet protocol and assumes that all of the attached devices on the networks use the same communications architecture and protocols. A router operates at OSI layer 3.

Routing protocols- Communication between the two nodes or hosts is done with the help of routing protocols.

7.3 LIST OF PUBLICATIONS

1) A paper entitled "Comparative Analysis of various attacks on MANET" has been published in *International Journal of Computer Application,* Volume 111 – No 12, February 2015.

2) A paper entitled "Hybrid protocol for handling security using SBPGP" has been published in *International Journal of Computer Application,* Volume 115 – No 22, April 2015

3) A paper entitled "Minimizing energy and providing security using hybrid approach in MANET" has been accepted in *International Journal of Applied Engineering Research* (IJAER) in April 2015 which has **SCOPUS** indexing. (Paper code :35207)

4) A paper entitled "Minimizing energy and providing security using hybrid approach in MANET" has been accepted in *International Conference on Advances in Applied Engineering and Technology (ICAAET)-2015.*Conference Proceeding will be published in **SCOPUS** indexed Journal *International Journal of Applied Engineering Research* (IJAER)