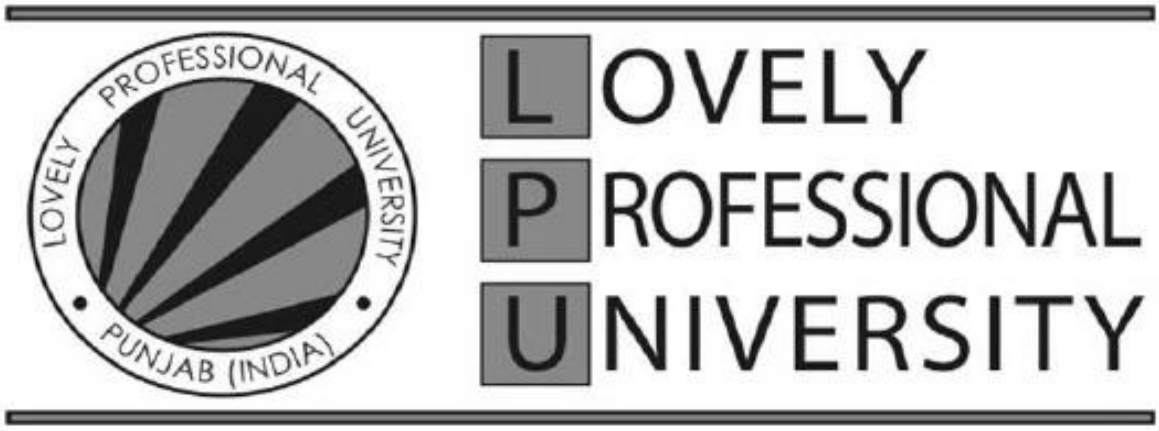


MOBILE AD-HOC NETWORK

Performance Evaluation in Energy consumption to increase the Network Life time

Dissertation Proposal

Submitted

By

Rupinder Kaur

11310514

Department of Computer Science and Engineering

In partial fulfillment of the Requirement for the

Award of the Degree of

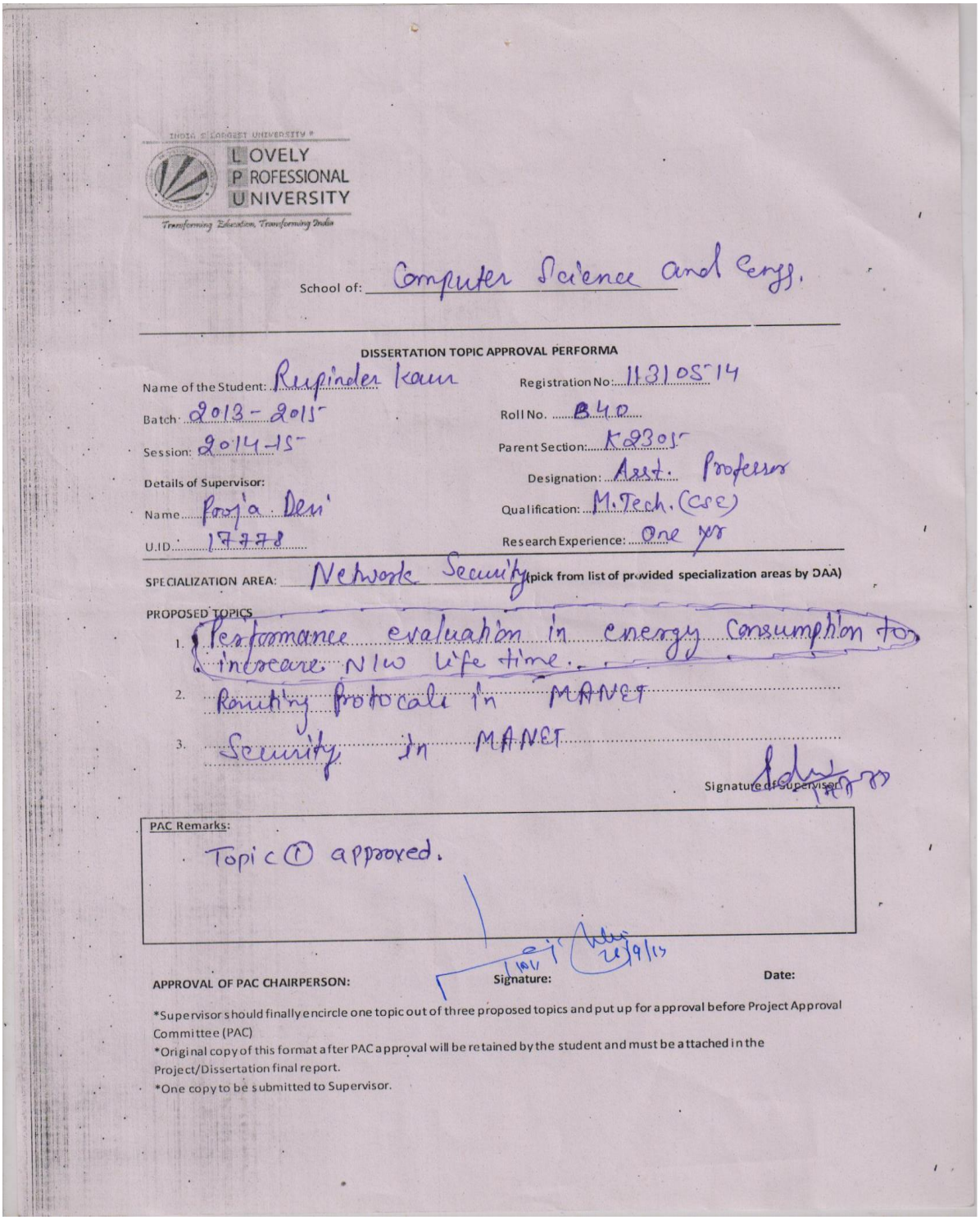
Master of Technology in Computer Science and Engineering

Under the guidance of

Ms. Pooja Devi

(December 2014)

POC FORM



LOVELY PROFESSIONAL UNIVERSITY
Transforming Education, Transforming India

School of: Computer Science and Engg.

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Rupinder kaur Registration No: 11305714

Batch: 2013-2015 Roll No. B40

Session: 2014-15 Parent Section: K2305

Details of Supervisor: Designation: Asst. Professor

Name: Pooja Devi Qualification: M.Tech. (CSE)

U.ID: 17778 Research Experience: One yr

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

PROPOSED TOPICS

1. Performance evaluation in energy consumption to increase N/w life time.
2. Routing protocals in MANET
3. Security in MANET

Signature of Supervisor:

PAC Remarks:

Topic (1) approved.

APPROVAL OF PAC CHAIRPERSON: Signature: Date: 25/9/14

*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

This work presents an overview of the Distributed mutual exclusion algorithm & various enhanced variations done on distributed mutual exclusion. In DME Permission-based algorithm is used for discovering clusters of the nodes. The initial point selection effects on the results of the algorithm, both in the number of clusters found and their cluster headers. Methods to enhance the Permission-based clustering algorithm are discussed. With the help of these methods increase the concurrency between the nodes, decrease the synchronization delay and decrease response time. Some enhanced variations improve the efficiency and accuracy of algorithm. Basically in all the methods the main aim is to increase the life of each node in the network or increase the battery power which will decrease the computational time. Various enhancements done on DME are collected, so by using these enhancements one can build a new hybrid algorithm which will be more efficient, accurate and less time consuming than the previous work.

ACKNOWLEGEMENT

First and foremost, I want to thank the Department of CSE of Lovely Professional University for giving me permission to begin Thesis in first instance, to do necessary research work and to use required data. I would like to acknowledge the assistance provided to me by the library staff of L.P.U. Inspiration to action is the most important ingredient required throughout the task. I am deeply indebted to my mentor Ms. Pooja Devi (Asst. Prof) whose help, stimulating suggestions and encouragement helped me in all the time of research. I express my gratitude to my parents for being a continuous source of encouragement and for their financial aids given to me. Finally, I would like to express my gratitude to all those who helped and supported me.

DECLARATION

In hereby declare that the pre dissertation proposal entitled, **"Performance Evaluation in Energy consumption to increase the Network Life time"** submitted for 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:

Reg. No. 11310514

CERTIFICATE

This is to certify that **Rupinder Kaur** Registration Number **11310514** has completed M. Tech dissertation proposal **"Performance Evaluation in Energy consumption to increase the Network Life time"** 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 and Engineering.

Date: Signature of Advisor

Pooja Devi

UID: **17778**

Table of Contents

List of figures

Title **Page no**

Chapter 1
Introduction

The network is a group of computers, called nodes, which are either connected through wired or wireless. A network can be a public or private network. These computer networks are used in our daily life, like in business organizations, colleges, government agencies and also to the individual life's. In a daily routine millions of transactions and communications are provided by these computer networks. As internet is open to public access so day by day the security of networks is faced by the attackers. Whether a business organization launches their private network to run the communication between the employees, but to increase access to the outside world they have to connect to the Internet because only the Internet can provide the global connectivity. So it means there is risk to one and all networks. Here the term network security comes into picture. It is type of replace of information to communicate with one another. The network is a group of computers, called nodes, which are either connected through wired or wireless. A network can be a public or private network. As internet is open to public access so day by day the security of networks is faced by the attackers. Currently each node in a network can act as a router at the same time, and these nodes are independent to move freely.

"Flooding" is used to forward the data from one node to other one. So because of this the topology changes frequently and quickly. MANET, the data should be routed via intermediate nodes, and these intermediate nodes will act as a router. Each node can be moved ON/OFF without detect other nodes. For communication single hoping and multi-hopping is used. MANET is a self-configuring setup. In MANET nodes are move freely in any direction. The nodes can communicate which are present in the range. Nodes act as router and host. The sources and destination nodes act as host nodes and intermediate nodes act as router because data is transfer through these intermediate nodes.

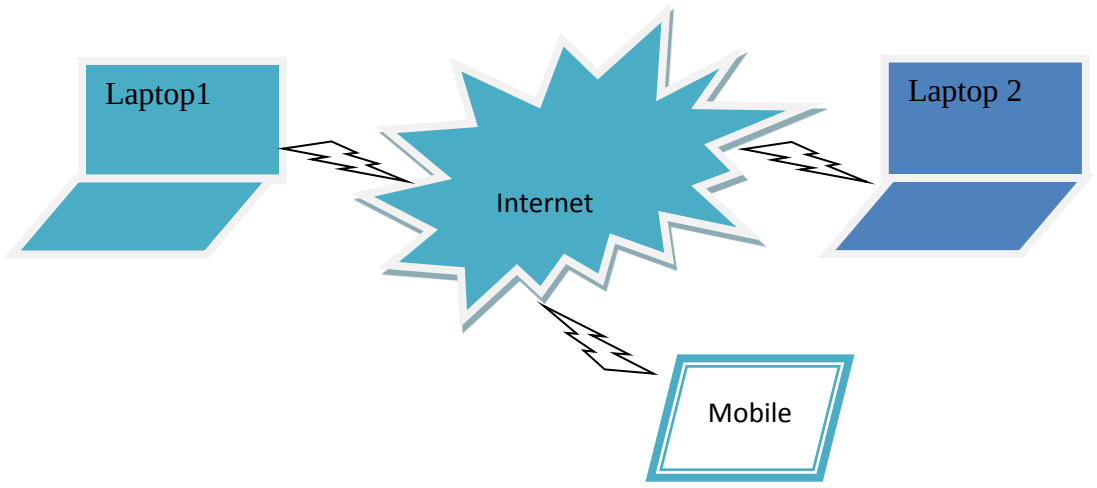


Figure1.1: Diagrammatically representation of computer networks [2]

Networking is used to allocate info like facts message. Sharing assets can be software type or hardware categories. It is central administration system or supports these types of system [6]. A network can be wired network besides network. In wireless network wires are not used for communication but in wired network communication can take place through the wires.

Following are the different category of network:

1. MAN, LAN and WAN.
2. Peer-to-peer and client/server
3. Bus, star, and ring topology.
4. Coaxial cables and fiber-optic cables.

1.1 Wireless Networks [6]

Wires are not used in wireless network because it is infrastructure less. Communication can take place through the radio waves at physical level. Data can be transmitting from one device to another device through the radio frequency. It is also called as Wi-Fi or WANL.802.11 is the IEEE standard of wireless network.

Types of wireless networks:

1. Infrastructure-based Approach

2. Ad hoc Approach

1. **Infrastructure based system**: Infrastructure based wireless networks, proceeds only among the wireless nodes present and the access points (AP). A number of wireless networks collectively can create a logical wireless network, so that organized the access points along with the in-between fixed network can connect with many other wireless networks to collectively create a bigger network that will be outside the range of the actual radio coverage. The AP controls the intermediate access; it works like a link to different networks, either wireless or wired.

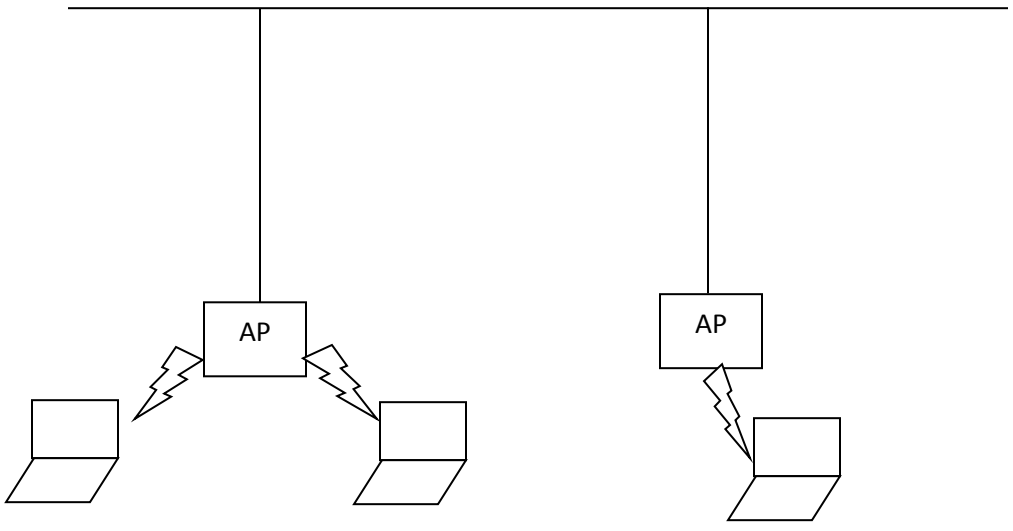


Fig.1.2 Infrastructure based Network [1]

Figure 1.2 shows the infrastructure-based wireless network. The design of these networks is simpler as much of the required network functionality lies within the AP. In Infrastructure-based networks some of the flexibility is lost that the wireless networks can further offer, e.g., they cannot be deployed in any disaster scenario in cases when, due to destruction, no infrastructure is left.

One example of infrastructure-based networks is Cellular Phone Network. The satellite-based cell phones also have an infrastructure, i.e. the satellites.

2. Ad hoc network

It is not the centralized network because it has no infrastructure and data is not being stored at one placed. That's way it is decentralized network. Like routers are used in wired network for communicating one wired network to other so it has pre-existing structure but in ad hoc network access points are used. Commonly ad hoc network is used in crucial conditions. Nodes that are present in the range of radio waves can communicate directly and no need any base station. There is no fixed infrastructure needed.

1.2.1 Categories of Ad-hoc Network [1]

Types of Ad-hoc network as following:

1. MANET
2. Wireless Sensor Network (WSN)
3. Wireless Mesh Network (WMN)

1. MANET

MANET is a mobile Ad-hoc network. Mobile nodes that are present in particular range can transmit data. While data direct from source to endpoint data is transmit over the in-between nodes and network chose shortest path for transmission of data. Nodes can act both routers and hosts. Node has capability to self-configure.

2. Wireless Sensor Network

Wireless sensor is a computer network which is collected of a large number of sensor nodes. A sensor node usually consists of memory, a processor, sensors, actuators and they do have communication ability. Over a wireless medium, the sensor nodes are allowable to communicate with each other's. It is the collection of sensing devices. These devices are wireless. It is centralized network. In wireless sensor network, cables are not required so that it is inexpensive to setup the network.

3. Wireless Mesh System

Wireless meshes networks prepared by gateways, mesh routers and mesh clients. The mesh consumers are could be laptops, cell phones and other wireless devices. The traffic is forwarded by mesh routers to and from the gateways but not connect to the internet.

1.3 MANET: MANET is a group of mobiles that are connected organized to form a network which is free of any infrastructure. It means there is no base station compulsory in MANET. So the nodes are presents in the range of network can communicate directly. MANET is a routable networking position on the highest of a link layer. Currently each node in a network can act as a router at the same time, and these nodes are independent to move freely. "Flooding" is used to forward the data from one node to other one. So because of this the topology changes frequently and quickly. MANET, the data should be routed via intermediate nodes, and these intermediate nodes will act as a router. Each node can be moved ON/OFF without detect other nodes. For

communication single hoping and multi-hopping is used. MANET is a self-configuring setup.

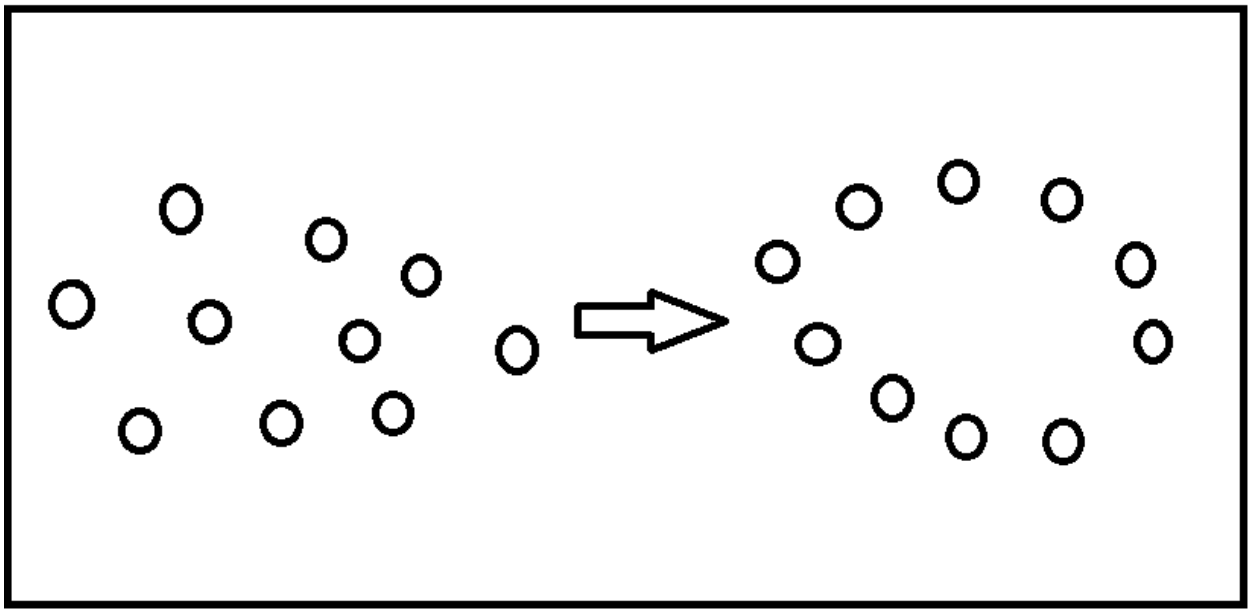


Fig.1.3 MANET Infrastructure

Every node need onward traffic dissimilar to its individual use, and then be a router. The main task is construction a MANET is equipping both devices to incessantly preserve the info essential to just path traffic. [1]

1.1 Characteristics of MANET:

1. Easy to deploy: MANET has no central controller. It is infrastructure less network. There is no access point needed by it. It has no fixed topology. Its topology changes frequently.

2. Do not need backbone infrastructure support: MANET requires no administrator i.e. no central controller. So it doesn't require any backbone to arrange network.

3. Suitable when infrastructure is absent, destroyed or unreasonable: It is very useful when infrastructure is absent. Because the node can easily joins or leaves the network any time.

4. Flexible: MANET is flexible to deploy. It doesn't have any fixed topology. So it can be transformed its topology regularly.

5. In MANET each node acts like a router and host: Any node can join and leave the network at any time. In this situation node can be act as router or host.

6. Nodes have less memory, power and light weight features: nodes has small in size so that it has less memory, power and light weight.

7. Distributed in nature: MANET has no central controller because it is infrastructure less network. It is in distributed in nature.

8. Dynamic network topology: MANET has no infrastructure. So that there is no fixed topology present in the network and topology changed frequently. MANET is based on dynamic network topology.

1.2 Applications

1) **Local Level**: MANET may be used at local level for example at home-based networks where devices can interconnect straight to exchange information between them.
2) **Military environments**: Military equipment consists of some sort of computer equipment's. Ad-hoc network can be used in military to maintain the information network between the soldiers, vehicles, and military information head-quarters.
3) **Commercial Sector:** In rescue or emergency operations mobile ad hoc network can be used, e.g. flood, earthquake or in fire.
4) **Wireless sensor Networks**: Mobile nodes contain small sized sensors that can be used to collect real time data i.e. pressure, temperature, etc.

1.3 Advantages of MANET:

- MANET required only wireless connection.
- In MANET each device and node can move independently in any direction but within range.
- This network can locate at any place and time.
- MANET required less time and cost.

- Does not require any cabling.
- MANET is temporary.

1.4 Routing Protocols:

The most significant and a problematic method to preserve in MANET is the routing mechanism. An ad hoc routing protocol is nothing but a concurrence between nodes as to how they control routing packets in the middle of themselves. The nodes in an ad hoc network discover routes as they do not have any previous knowledge about the topology. Routing protocols in MANETs are categorized into three different classes.

1. Reactive protocols: It is On Demand routing protocol. Route only create when it required. When a node wants to communicate a packet to additional node first check route through on demand and after that create the connection between the nodes. The source node initiates the route discovery segment. There are mainly two stages in reactive routing mechanism after the node needs to send data to the destination. The source node broadcasts Route Request messages and is extend across the complete network. Routes are added to the list one time the Route Reply packets derive from the destination reach the source using different forwarders. Example DSR, AODV, TORA.

A. AODV(Ad-hoc On-demand Distance Vector)

It is on-demand routing protocol. AODV has less memory overhead and creates the unicast routes from sources to destination. When the link is fail, message is send to effected nodes. AODV use three messages: Route Request, Route Error and Route reply. Data are used to control and keep the ways after source to endpoint in using UDP packets. At every time it is essential toward make the original route from source to endpoint, when the node demanding transmissions Route Requests. This message remains reached to next hop then route is determined or destination itself and Route Reply reaches to creator of the request. If the link failure occur the Route Error message is generated.

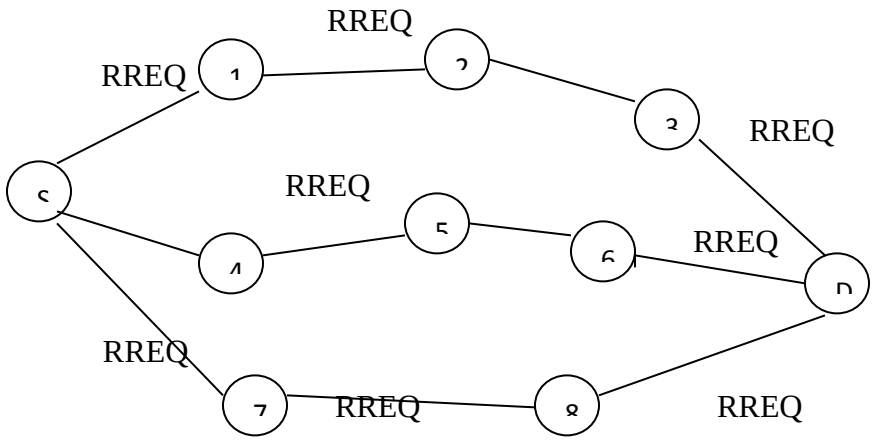


Fig. 1.4 AODV paths established through RREQ

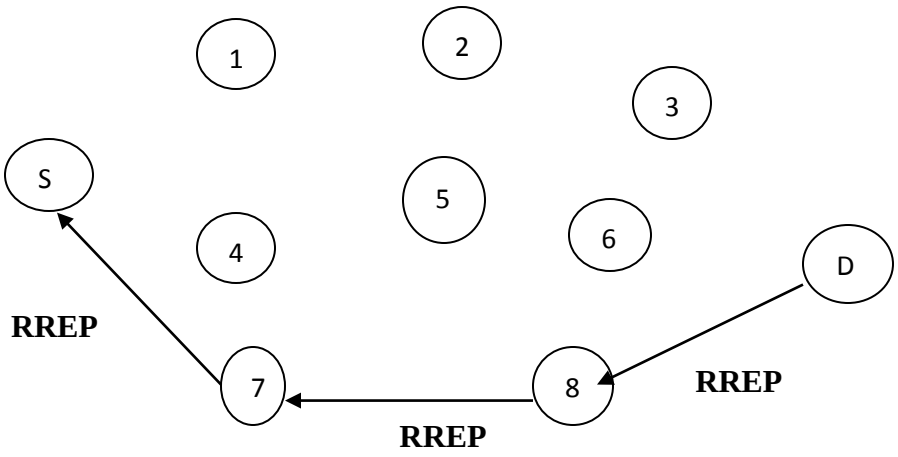


Fig.1.5 Final Path established

B. Dynamic Source Routing

It is reactive routing protocol. It also has on-demand feature like AODV. It is also based on source routing. DSR allows the net to be totally self-ordered and self-configuring. DSR procedure permits outcome a basis way through many network nodes. Each data transmit through in its header entirely, message pass dynamically from the list of nodes.

2. Proactive Protocols: - It preserves the route data when it is needed. It uses an already existing route. These protocols maintain routes to all possible destinations even while a few of the routes may not be required. Every node in the network maintains tables of routes and when the network topology changes, updates are sending across the network. For maintain the routes node send the control message. Route maintains is difficult because lot of bandwidth is used for route prevention. These protocols invite a lot of routing overhead. There are some really good advantages of proactive protocols. Types are DSDV, WRP and OLSR. [11]

A. Destination distance sequence vector (DSDV):

It is table driven routing procedure. It is established on the idea of the normal Bellman-Ford Routing Algorithm with definite improvements. The sequence number is used to separate stale paths from new ones and to avoid the loops creation. Each node has a routing table that essential list of all existing endpoints, the allotted sequence number by the destination node and the number of hops to spread the target. If a significant modification has occurred in its table from the preceding update a station also carries its routing table. If two routes have the same sequence number then the route with the shortest route is used he occasionally stations spread their routing tables to their instant neighbors. DSDV does not maintenance multi-path routing. It carries shortest path of good quality, trust worthy and supportive [9].

B. Wireless Routing Protocol (WRP)

It is a routing protocol created on distance vector routing protocol. Each node in the network saves a Routing table, Distance table, a Link-Cost table and a Message Retransmission list (MRL). MRL has in order to let a node recognize which of its neighbor has not recognized of update message and to retransmit update message to that neighbor. The node is mandatory to send an idle Hello message to guarantee connectivity If there is no modification in routing table since last update to receive an update message the node adjusts its distance table and looks for improved paths by new information [11].

C. Zone-Based Hierarchical Link State Routing Protocol (ZHLS)

Network is distributed into non-overlapping regions in this protocol. ZHLS defines two level of topologies Zone level & node level. A node level topology expresses how nodes are connected to each other actually of a zone. Zone level tells how zones are linked. A node LSP of a node contains its neighbor node information and is broadcast with the zone where as a zone LSP comprises the zone information and is broadcast globally. It comes under hybrid category. [17]

D. **Optimized Link State Routing (OLSR):-** OLSR is dynamic link state protocol which assembles link state data and dynamically computes the best routes inside the network.

3. Hybrid protocols: It is association of proactive and of reactive routing .ZRP sand TORA.

1.5 Energy consumption in MANET:-

In MANET, all node stakes batteries devoted toward it, which is inspired during the process of transmission i.e. during transmission, reception and overhearing and many other reasons. It is very problematic to swap batteries or to re-charge them. So to rise the long lifetime of the network; the existing battery power necessity be sensibly used. There is essential to reduce the energy consumption and handle the available energy for extended network connection. If power goes down, network connection will not be present, and will influence our transmission also. So there is requirement of different strategies to reduce the wastage of energy consumption at different levels.

1.5.1 Token Based Algorithm in MANET:

1. The group mutual exclusion (GME) problem is a simplification of the ME problem. **Group mutual exclusion**: procedures now the similar collection can go in a critical CS concurrently or no two procedures in dissimilar sets enter a CS at a time.
2. Critical section is a part of program that accesses shared resources.

3. In TBME processes, a single token is shared between the hosts and if a host possesses the token than it is allowed to enter the critical section.

   In PBME, the node that wants to arrive in critical section must first obtain approval from rest of the nodes by exchanging messages.

   In **quorum based mutual exclusion algorithms**, each node gets permission from a subset of nodes referred as quorum for executing critical section. Any two quorums contain a common host.

4. **Distributed Mutual Exclusion (DME) algorithms must satisfy following properties:**
   - **Safety:** No two processes, requesting for a different group can be in their critical sections simultaneously.
   - **Freedom from deadlocks:** Double or additional hosts must not unceasingly delay for communications that will not ever reach.
   - **Freedom from starvation:** Host necessity not delay endlessly to perform the critical section though additional hosts are frequently performing critical section.
   - **Fairness:** The requirements for entering critical section are performed in order of their arrival in system.

5. Look-ahead technique is used. All nodes including arbitrator will use this technique.

```
--Executed by the initiator: --
//Generate the Upper Triangular Matrix
M_u
for{ i = 0 to |S|-1}
        for{j= i+1 to |S|-1}
        m_ij = random(0,1);
        endfor
endfor
broadcast M_u to all other hosts;
```

```
--Executed by all the hosts: -----
//Step 1: Generate the Lower Triangular Matrix M_l
for{ i = 0 to |S|-1}
for{j= 0 to i-1} m_ij =1-m_ji;  endfor
endfor
//Step 2: Initialize the Info_set and Status_set
// for host S_i//
for  { j= 0 to |S|-1and j !=i}
     if {m_ij==0} put S_j into Info_Set_i;
     else  put S_j into Status_set_i;
endfor
```

Fig. 1.5Algorithm for Initialization[3]

Here, Info set of i means it holds all those nodes to which i node sends request message.

In our case, each node and arbitrator node has Info set e.g.: Info set of node 1 contains {node 2, node 3, and arbitrator}

Status set of i contains those sites from which i receives request message. E.g.: Status Set of 1 contains {node 4, node 5}

This whole process means node 1 sends request message only to node 2, node 3 and arbitrator. Node 1 receives request message only from nodes 4 and 5.

Node 2 contains in its status set {node 1} and not in its info set.

Chapter 2

Literature Review

Already the selection of "Network Security" as my wide zone of thesis, I have studied various research papers, base papers, books and manuals. Papers help out me to invention a specific problematic zone where I start my work for thesis. Papers related to problem field defined under purpose of learning &publication year.

In **March 2013**, "A Token based Distributed Group Mutual Exclusion Algorithm with Quorums for MANET", this research paper was written by **Talele P., Penurkar M**. This paper defines the GME problem. In this problem, same type of processes can request the CS and can execute CS concurrently. Basically, the different type of processes can request their CS and executes in equally exclusive method. The DME algorithm is used for collection of ME difficult. Token based algorithm is used, process that can found a token enter a CS. Message complexity is decrease. When a process request a message, it use coterie as communication structure. A coterie is an established by quorums. Any two quorums assign at minimum one process and process act as gateway between the two quorums. The proposed algorithm can reach high concurrency, measure the performance of processes that enter in CS. of performance for number of procedures that can be in critical [11].

In "A Merging Clustering Algorithm for Mobile Ad Hoc Network" written by **Dagdeviren O., ErciyesK**. They describe the cluster merging method. Clustering is generally used approach in various problems like routing and resource management in MANET. Clustering approach is ease to implement, that merging the clusters to form advanced level by rise their level. They show operation of algorithm and examine its time, message complexity. The algorithm planned is accessible. It has a lesser time and message complexity [6].

In **2013** "A Permission-based Clustering mutual Exclusion Algorithm for mobile ad-hoc network" proposed by **Gupta A**.". They described PBMUTEX in MANET. Author explained about the resource allocation in MANET. They proposed method for ME in MANET which is created on gathering and idea of weight flinging. Procedure is based on cluster hierarchal method which is help to decrease the message complexity [8].

In **2013,** "Arbitration based Reliable Distributed Exclusion for Mobile Ad-hoc Networks**"** described around DME permits critical re-sources share between dissimilar nodes in a MANET situation. Paper places all nodes in district regions. By properly operating performance of arbiter nodes, that procedure the link among two adjacent districts, guaranteed that approval is established to all causal node, regard less size of the system. They must use a solitary supplementary communication, HOLD message, to confirm that DME accuracy is reached for together inter-region and intra-region communications. Fault tolerance influences for the projected procedure similarly exist. To our knowledge, it is the main DME procedure that usages the concept of areas then fault tolerance in MANETs. [15]

In **2011**, "An Efficient Mobile Authentication Scheme for Wireless Networks" author is **Caimu Tang**. Author debated about future capable verification mechanisms for low-power devices. Proposed scheme the mobile place lone essential to reach one package for common verification .They used the elliptic-curve-crypto scheme created hope allocation Mechanism to generate group pass code for mobile station authentication. With make usage of this verification instrument various active & passive attacks resolve be barred with the DOS attack. Mobile device genuine with the staying base station only by the conversation of one packet. Purposed tool is compulsory fewer calculations and fewer data interchange as compared to other verification systems. [20]

In **2010** IEEE "A Novel Permission-based Reliable Distributed Mutual Exclusion Algorithm for MANETs" written by **Parameswaran M. And Hota C**. They discover novel PBMUTEX is used for solving their problem. DME is provided that to access the shared CS resources to different nodes. The paper use the new message called 'HOLD' message to make sure that which node is currently execute in CS [10].

In **2009**"Enhancing the Performance of MANET by Monitoring the Energy Consumption and Use of Mobile Relay" Research paper was written by **B.N. Yuvaraju**. This paper uses the mobile relay to increase the energy of particular node. Mobile Relay is used to balance the load on a node hence reduce the energy consumption. They deal the problem of jamming and energy depletion [3].

In 2009, "A Distributed Mutual Exclusion Algorithm for MANET", by **Erciyes K. and Dagdeviren O**. Planned a DUMEX for MANET. This algorithm requires a ring of cluster coordinators as underlying topology. In first step topology is built by providing the clusters of mobile nodes and as second step backbone of the cluster heads in a ring is formed. R-Algorithm is modified version used on the top of this topology. The experimental result of this algorithm is decrease in message complexity with respect to original algorithm [7].

In 2009, "Evaluating the Energy Consumption Reduction in a MANET by Dynamically Switching-off Network Interface" **Author is Carlos J**. They create based on the RTS/CTS which switch off NIC will dynamically when i.e. neither sending idle nor receiving any data. DSR, DSDV, AODV, TORA algorithms used in research paper. These Algorithm provide security, reduce the network overhead, rate of topology change is less or medium [3].

In 2008, "Prevention of Attacks in MANET" authors are **LathaTamilselvan, V. Sankaranarayana.** Author proposed solution created on an improvement of the unique AODV protocol. According to planned explanation, the demanding node without transfer the Data packages to the response node at once, it has to delay till additional replies by following hop facts from the supplementary adjacent nodes. Later getting the first request it sets timer in the 'Timer Expired Table', for assembly the additional requirements from dissimilar nodes. It stores the 'series number', and the period at which the pack spreads, in a 'Collect Route Reply Table' (CRRT). Time for which each node will delay is proportionate to its distance after the source. It subtracts the 'timeout' rate based on incoming time of the first route demand. Later the timeout

rate, it first checks in CRRT whether here is some frequent next hop node. If any repeated next hop node occurs in the reply paths it accepts the routes are right or the casual of cruel routes is partial. [19]

In **August 2007**, "A fault tolerant mutual exclusion algorithm for mobile ad hoc networks", author **Yang J., Cao J. and Wu W**. They planned a permission created message well-organized MUTEX algorithm for MANETs. Planned procedure used the "look-ahead" method to decrease the message difficulty. Planned mechanism to handle dozes and disconnections of mobile hosts and too accepts connection or host failures by timeout-based mechanisms. This is the first PBMUTEX procedure for MANET. Projected process displays the logical and simulation results, particularly when the movement is high or load close is small.

In **2006**, "Multiple Key Sharing and Distribution Scheme with Threshold for NEMO Group Communications", author **YixinJiangand.** Writer planned a different mutual verification and key exchange procedure. The two key features of procedure is uniqueness secrecy and session key regeneration. Protocol proposals protected roaming facilities to the appropriate user among the home and remaining negotiator or in small, procedure offers protected handoff to the reliable operator. The projected practice is created on the undisclosed intense opinion and self-certified arrangement. Procedure workings in two stages: First stage is the shared verification with secrecy which casings the use's actual individuality when an effective operator is roaming from the home-based negotiator to the waiting agent. This stage uses the time-based individuality (TID) in its place of the user's actual identity. Another stage is the session key renewal phase which renews the common key which is common among the honest user and the portion negotiator. [21]

In **2004,** "Routing Security in Wireless Ad Hoc Network" Authors are **Hongmei D., Wei Li, and Dharma P**. They planned process for sensing solitary black hole node. Planned technique, every node demands the RREP message after the source obtains response from in-between node and some malicious node enters it conveys the alarm message. .Single drawback of the planned

technique is that it works built on a statement that mischievous nodes do not work as a collection which is an incredible situation. [16]

In **2004**, "Key Management for Heterogeneous Ad Hoc Wireless Networks", authors are Seung Yi and Robin Kravets. They had discussed several mutual authentication schemes for MANET. They discoursed the symmetric key and asymmetric key delivery systems and PKI (public key distribution) arrangement which made on the symmetric key delivery order. A new verification scheme called as MOCA which mix class of pattern and use both PKI and asymmetric systems for joint verification. [17]

In 2001 "A Distributed Mutual exclusion algorithm for mobile ad hoc network" written by **Al.et R**. They describe the DMUTEX based on token exchange between the nodes. The algorithm is based on the logical ring. In TMUTEX two families of algorithm is used like token asking and circulating token [2].

In **2001**, "Distributed Mutual Exclusion algorithm in Mobile Ad hoc Networks: An overview*" written by **Benchaiba M., Bouabdallah A. and Badache N**. They planned the key for problematic of mutual exclusion in spread system. The projected explanation can be ordered in agreement based and token based procedures. Explanation also reflects physical topology of the net and offers best message and negligible synchronization stays. Logical assembly on net alike ring or a tree, these nets called interesting area. Writer defines the distributed mutual exclusion established for mobile situation and mainly for ad hoc network and other subjects associated to DME. [14]

Chapter 3

Present Work

3.1 Problem Formulation

Distributed mutual exclusion is basically used TBME algorithm and PBME algorithm. In proposed methodology token-based is used. In Token-based algorithm the concept of region is used. The proposed algorithm consists of dual sessions of tokens: - key token and deputize–token. The key token is accepted between two quorums through arbitrator. When a process request a message, it use coterie as communication structure. A coterie is an established by quorums. Any two quorums assign at minimum one process, and process act as gateway between the two quorums. But the main problem is that it has one arbiter that handles all node requests, so it increases the burden on arbitrator. If some failure occurs in the network and arbiter goes fail, whole network is destroyed. After that all nodes sends the requests to single arbiter and arbiter manage the FIFO to handle the all requests, it increases the network traffic. Some time network gets failed. The main problem of proposed methodology is that, the token is lost, it also increase the response time and decreases the synchronization stay.

Principle of projected process:

- **Requesting for Critical Section:**

Once node *i* want to move in Critical Section it first set timestamp request to existing period and send the request for Critical Section to the nodes which are present in info set including arbitrator and wait for reply message.

- **Receiving Request message from node *i*:**
    - ✓ The arbitrator receive message from node *i* then it directs the token to node *i* if it itself not in CS or has high priority otherwise it directs this wish to the nodes of its information set in another quorum.
    - ✓ If the node is ordinary node and receive appeal message form node *i* then it directs the response to node *i* if it itself not in CS or priority otherwise it stores this request in request queue.
    - ✓ When holder *j* the key token accepts a call by node *i* then furthered through arbitrator, after that request is placed into line of key token.

- ✓ Every request in line is decided permitting to the next directions:
    1. If there is not any node arrives in Critical Section, key token transmitted token message to demanded node.
    2. If node is in Critical Section and requested node is the equal as the existing node, negotiator directs a sub- token to requesting node. After route node *i* exit the Critical Section, if node *i* is owner of the key token it decrease the group size via one. Else node *i* grips a sub- token, it rearrange a sub-token by transfer an issue message.

3.2 Objectives of Study

Main objective of my research work are as following:

1. To decrease the number of messages per CS using "look-ahead" technique.

2. To optimize the parameters that decides the performance of the DMUTEX Algorithm like synchronization delay, response time.

3. To prove the accuracy of the algorithm like liveness, fairness, safety.

3.3 Research Methodology

The algorithm supposed toward complete in a scheme containing of M clusters and N nodes, every cluster have one cluster leader. Nodes be categorized as 0, 1……N-1, and cluster leaders are considered as 0, 1……..M-1. I will presume that there is a unique time stamp of node 'I'. In addition, the planned algorithm precedes the ensuing hypothesis taking place the nodes and clusters:

- Nodes need matchless identifications.
- No fresh cluster would be created while initialization.
- Global clock is maintained on each node for synchronization.
- Clustering of nodes and selection of cluster head is based on node unique ids.
- Size of cluster is fixed.
- Handshake protocol is used for reconfiguration of clusters.

- No node can move at the same time as the cluster configuration is in progress.
- No two clusters are related with each other.
- Status of nodes: IN CS ,Wait RP,IDLE

The performance of MUTEX algorithm is generally measured by four matrices:

- **Message Complexity: -** Number of message that is compulsory each critical execution by a site.
- **Synchronization delay: -**The required period when position leaves the critical section, & earlier the next location go in the Critical Section.
- **System Throughput: -** The frequency at which the spread network accomplishes desires for the Critical Section.
- **Response time: -** It is period wait a request from host delays for Critical Section.

The performance of proposed algorithm is shown in given below figure. Node 10 sends request for CS to cluster leader 20 by specify in its request message its id, cluster leader id and timestamp. As cluster leader 20 does not have CS therefore it enqueues node 10's request and promote forward it to cluster leader 19 which is present in its Info set. After receiving request from cluster leader 20, cluster leader 19 sends leader reply message, in case, its node does not want CS otherwise it enqueues request of cluster leader 20. Cluster leader 20 allowed its node 10 to enter the CS after getting leader reply message. The overall working of the proposed algorithm is presented in four scenarios.

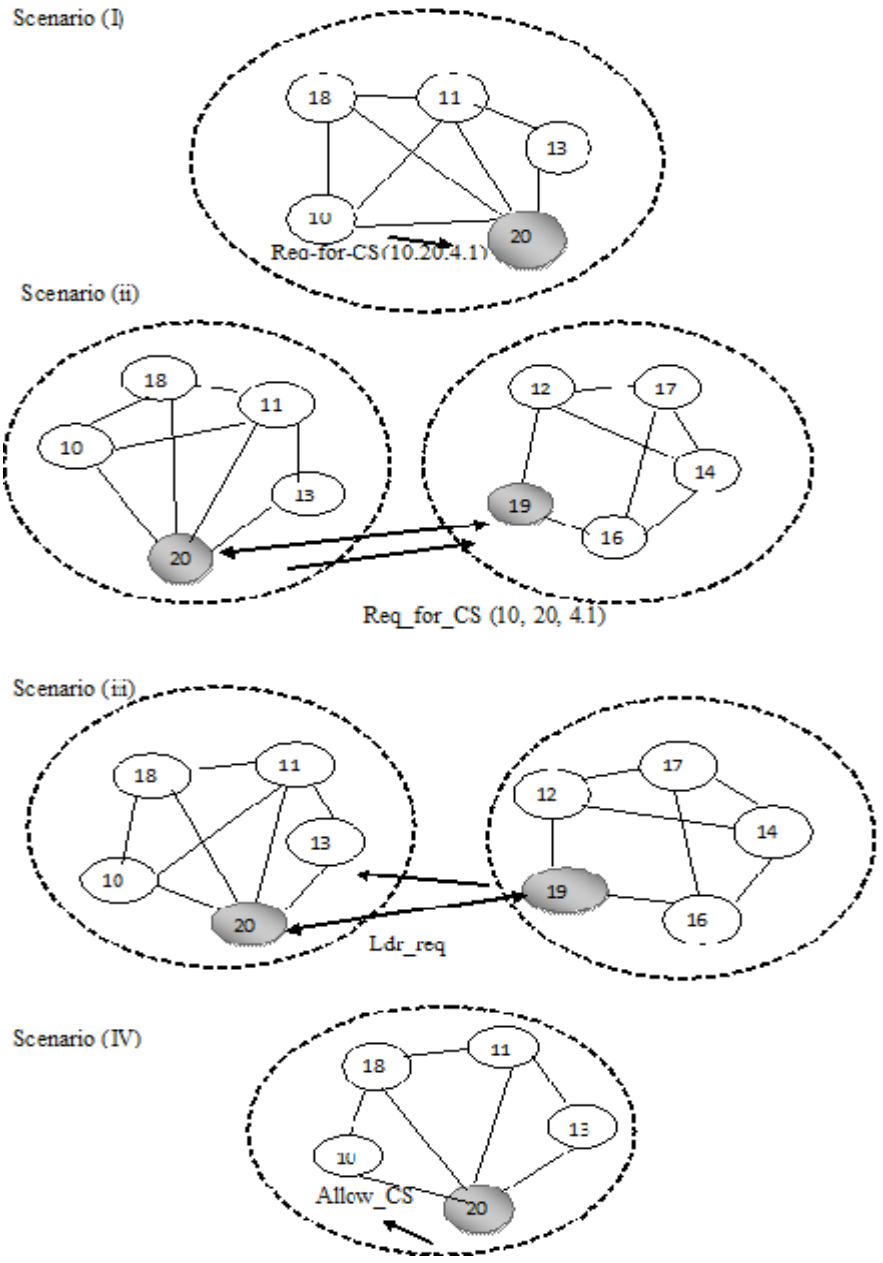


Figure 3.1 Execution of proposed work [7]

Flow chart:

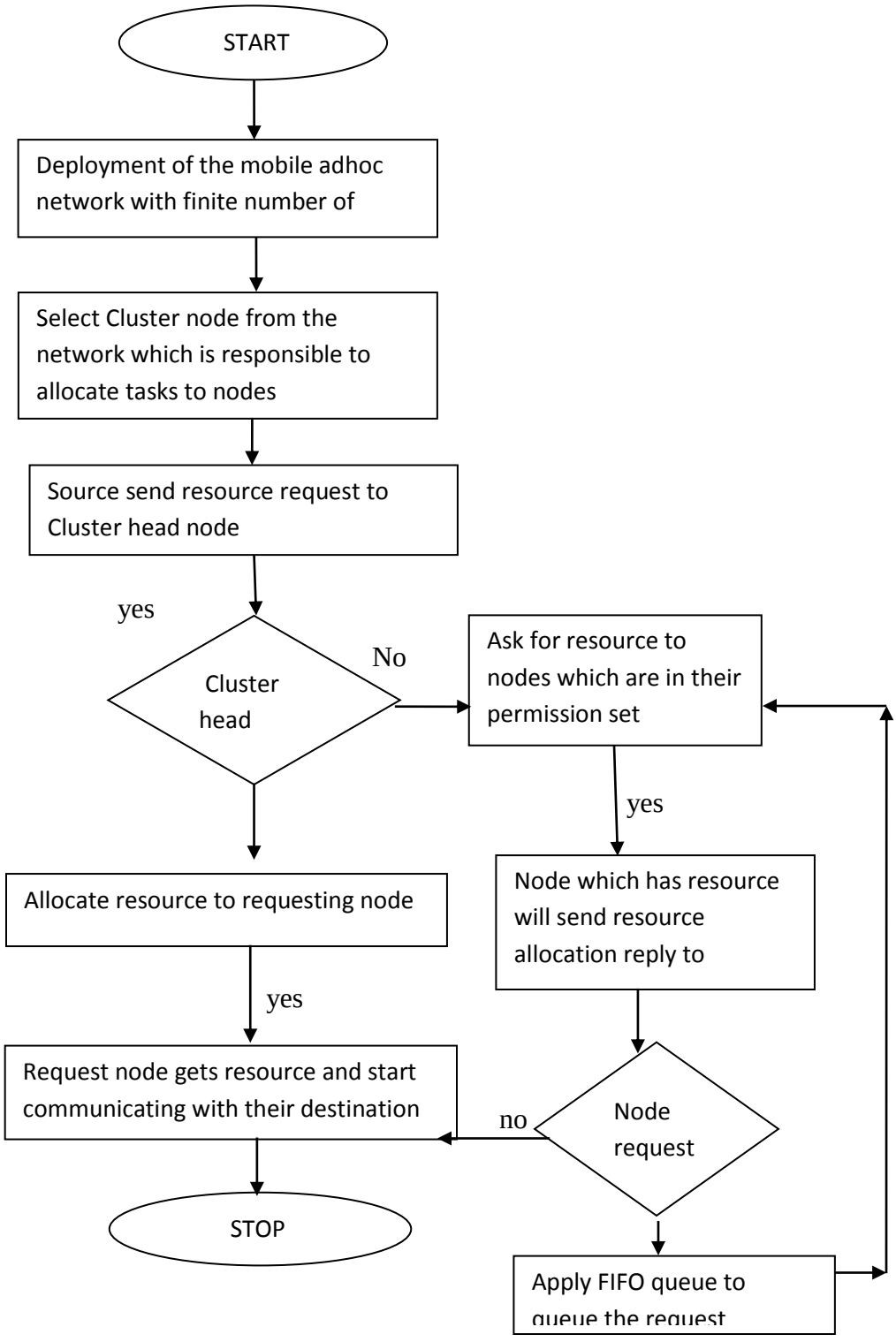


Figure3.2 Flow chart of future work

Chapter 4

Results and discussions

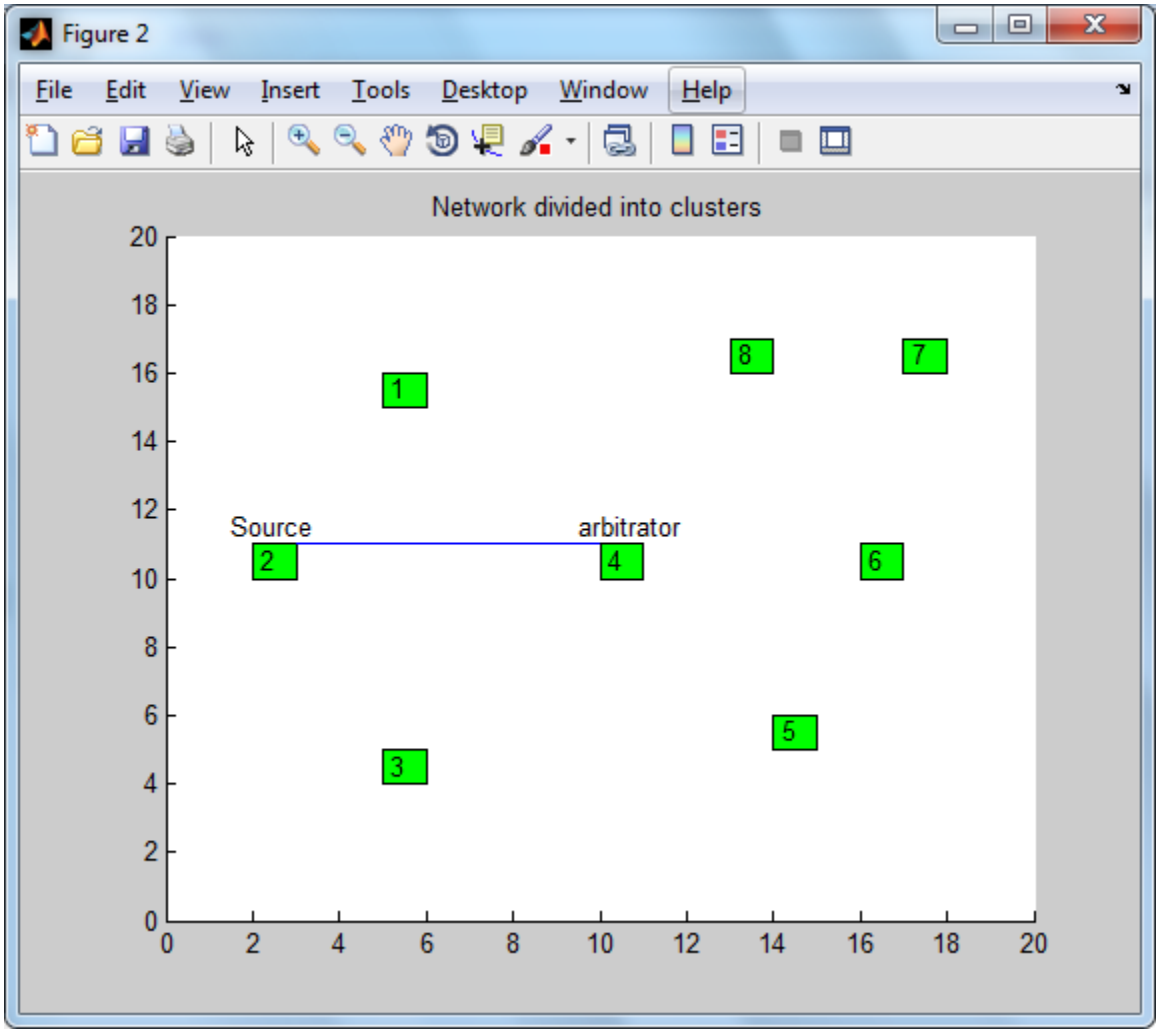


Fig 4.1: Network Deployment

The set-up is organized by the fixed number of movable nodes. In network source and arbitrator node is declared. The arbitrator node is to allocate tasks to the source node for which it requesting

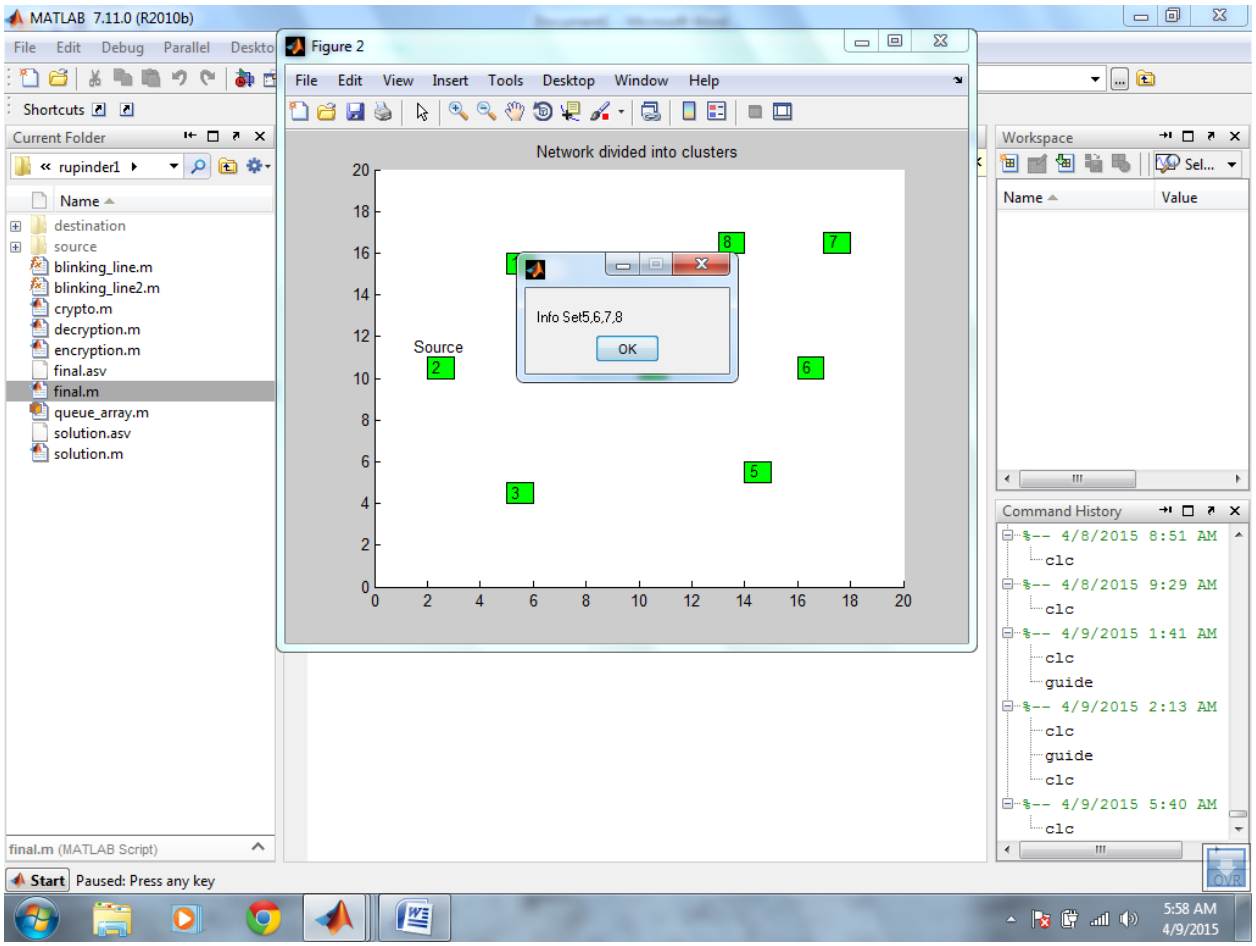


Fig 4.2: Checking Info set

This figure is checking info set of an arbitrator. The source node request to arbitrator node to the resources. The arbitrator node checks its info set which is 5, 6, 7 and 8.

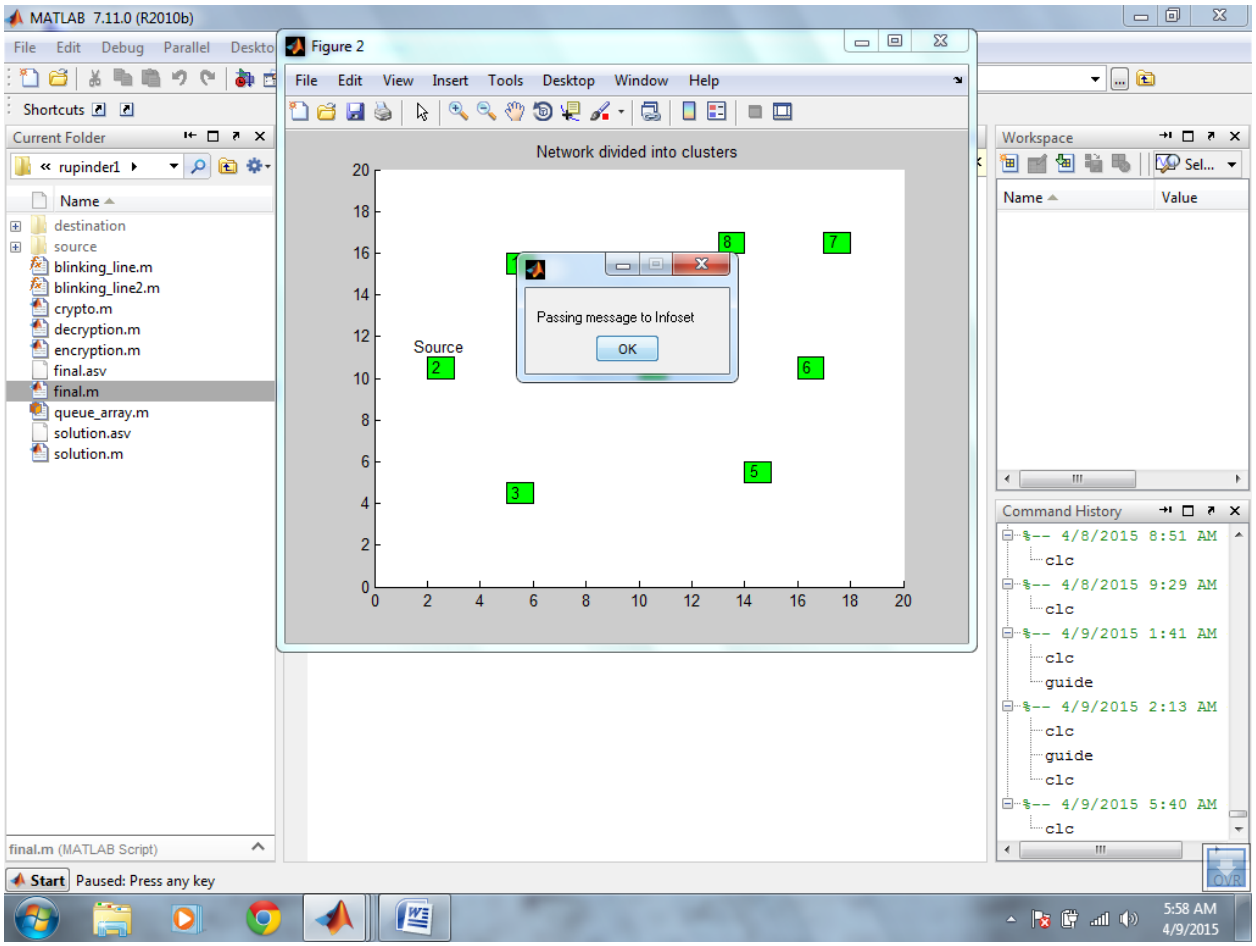


Fig 4.3: Passing message

The source node request to arbitrator node for the resources. The arbitrator node checks its info set which is 5, 6, 7 and 8. The arbitrator node passes the request to its info set node

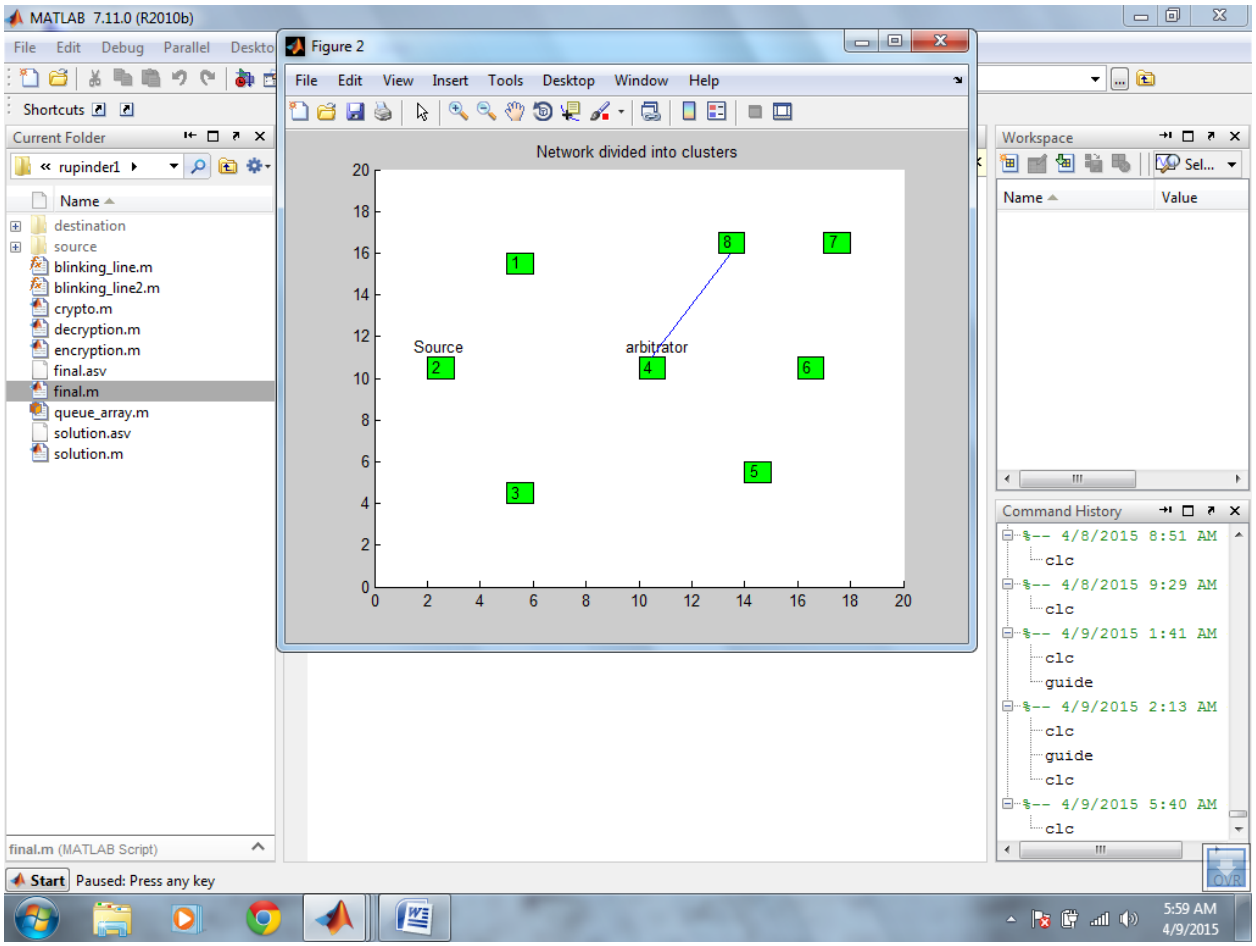


Fig4.4: Passing message

The source node request to arbitrator node for the resources. The arbitrator node checks its info set which is 5, 6, 7 and 8. The arbitrator node passes the request to its info set node. The arbitrator node pass request it 8 number node

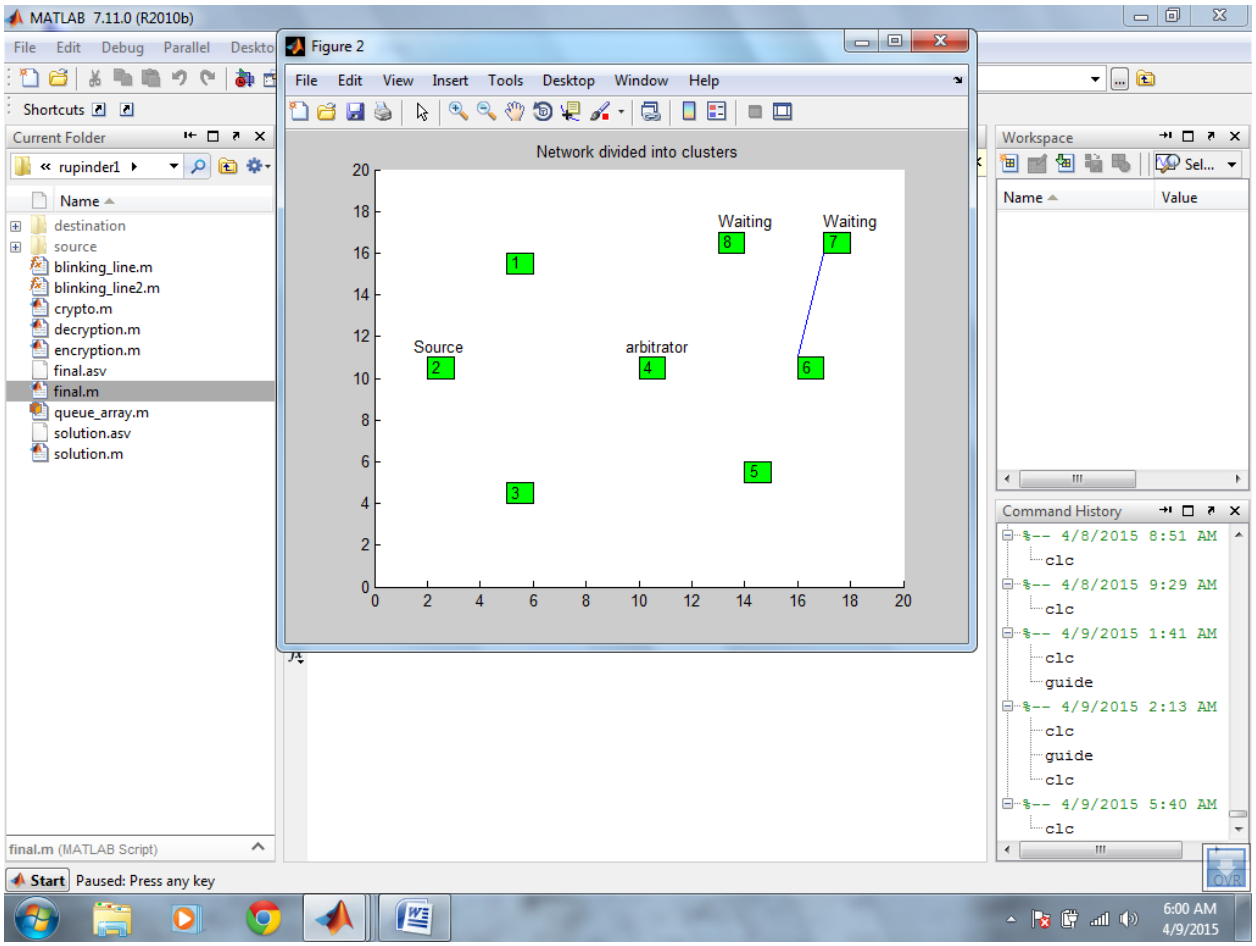


Fig 4.5: Passing message

The source node request to arbitrator node for the resources. The arbitrator node checks its info set which is 5, 6, 7 and 8. The arbitrator node passes the request to its info set node. The arbitrator node pass request it 8th node. The 8 number node haven't resources so it pass resources to 7 numbers node and change its state to waiting state

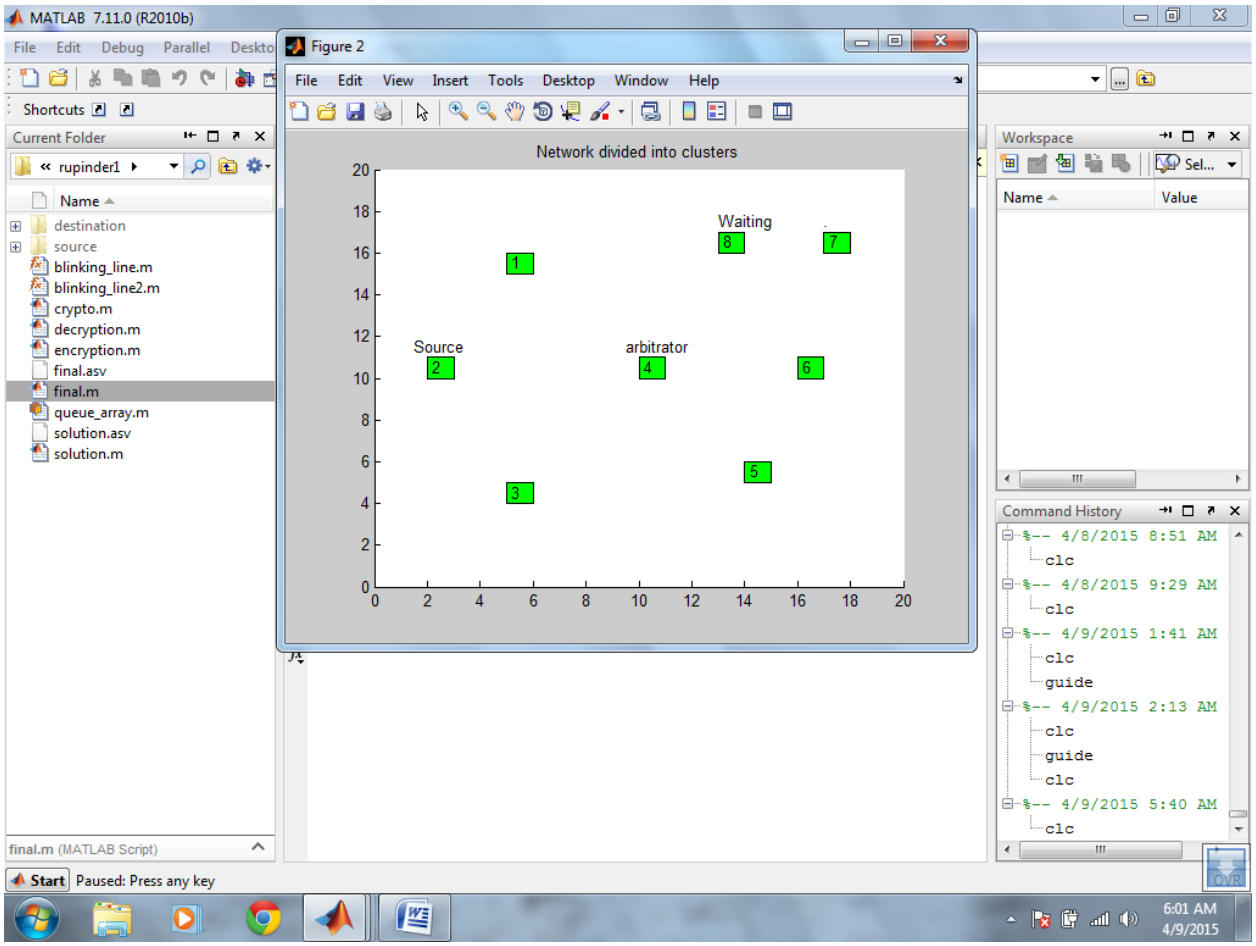


Fig 4.6: Getting Resources

The source node request to arbitrator node for the resources. The arbitrator node checks its info set which is 5, 6, 7 and 8. The arbitrator node passes the request to its info set node. The arbitrator node pass request it 8th node. The 8th node hasn't resources so it passes resources to 7 numbers node and changes its state to waiting state. The node assign resources and pass resources and requesting node

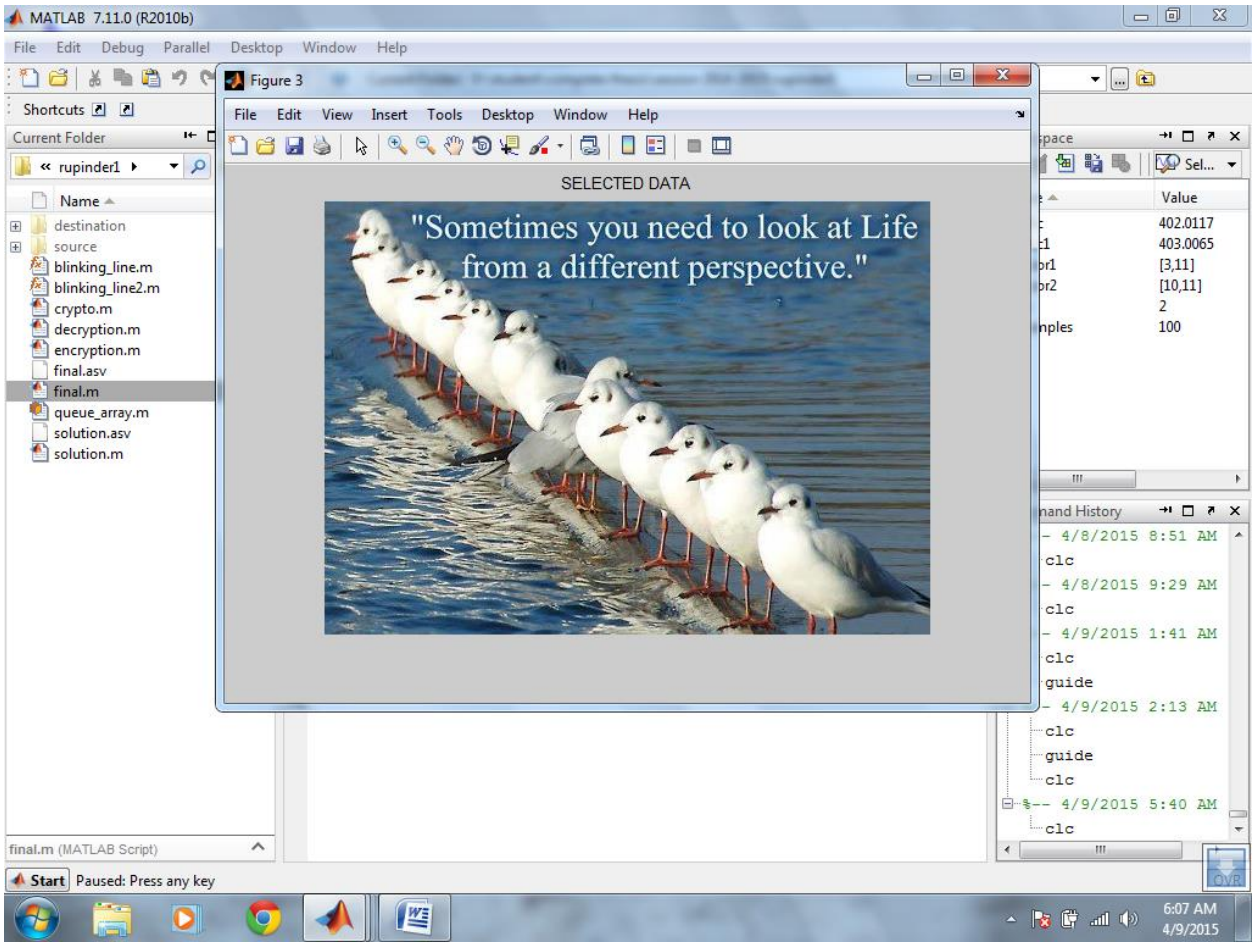


Figure 4.7 Getting Resources

Fig 4.7: Getting Resources arbitrator node checks its info set which is 5, 6, 7 and 8. The arbitrator node passes the request to its info set node. The arbitrator node pass request it 8th node. The 8th node hasn't resources so it passes resources to 7 numbers node and changes its state to waiting state. The node assign resources and pass resources and requesting node. The source node gets its resources and selects the data for transmission

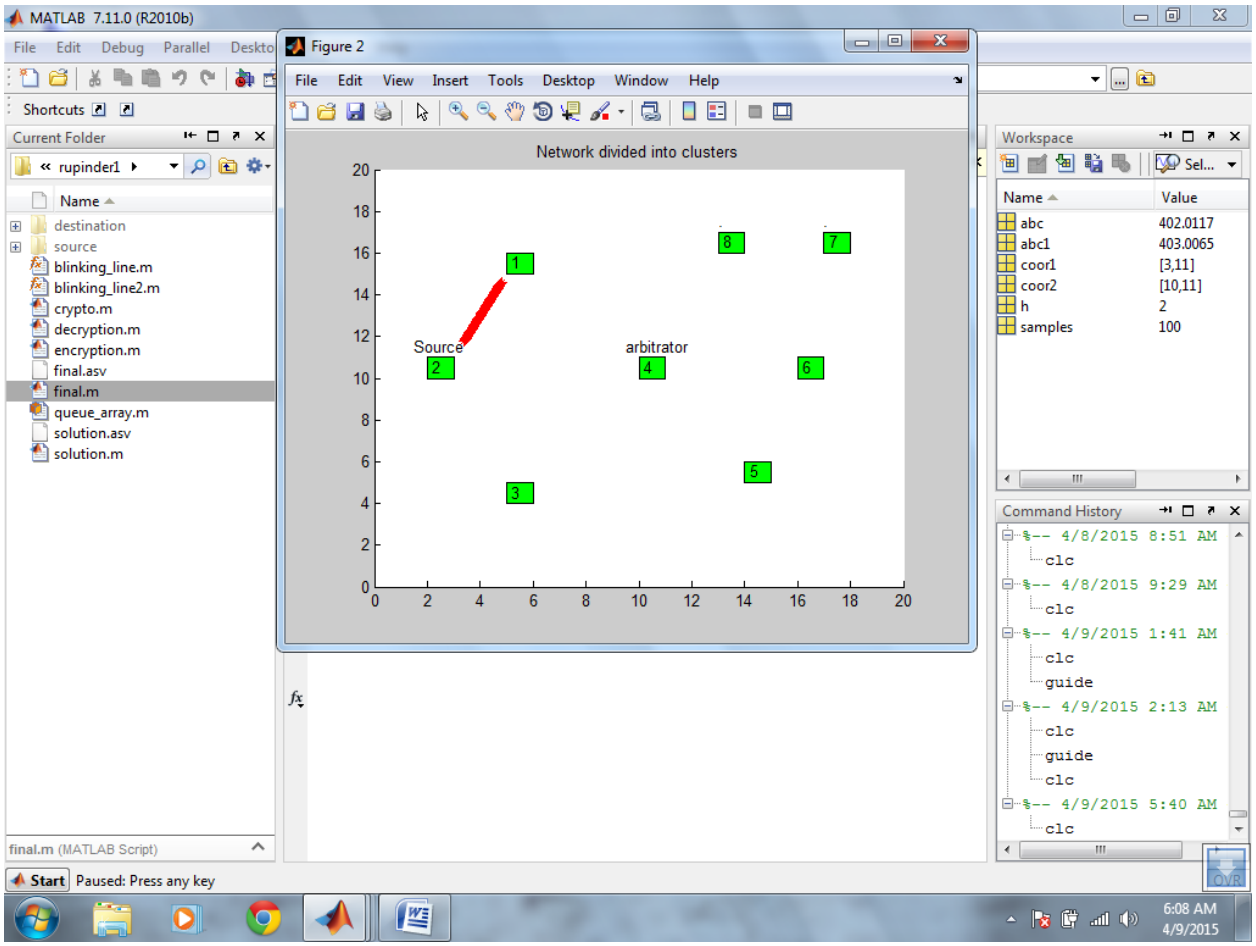


Fig4. 8: Transmission start

As shown in the figure 7, the source node request to arbitrator node for the resources. The arbitrator node checks its info set which is 5, 6, 7 and 8. The arbitrator node passes the request to its info set node. The arbitrator node pass request it 8^{th} node. The 8^{th} node hasn't resources so it passes resources to 7 numbers node and changes its state to waiting state. The node assign resources and pass resources and requesting node. The source node gets its resources and selects the data for transmission. The source node selects the data and transmits to destination

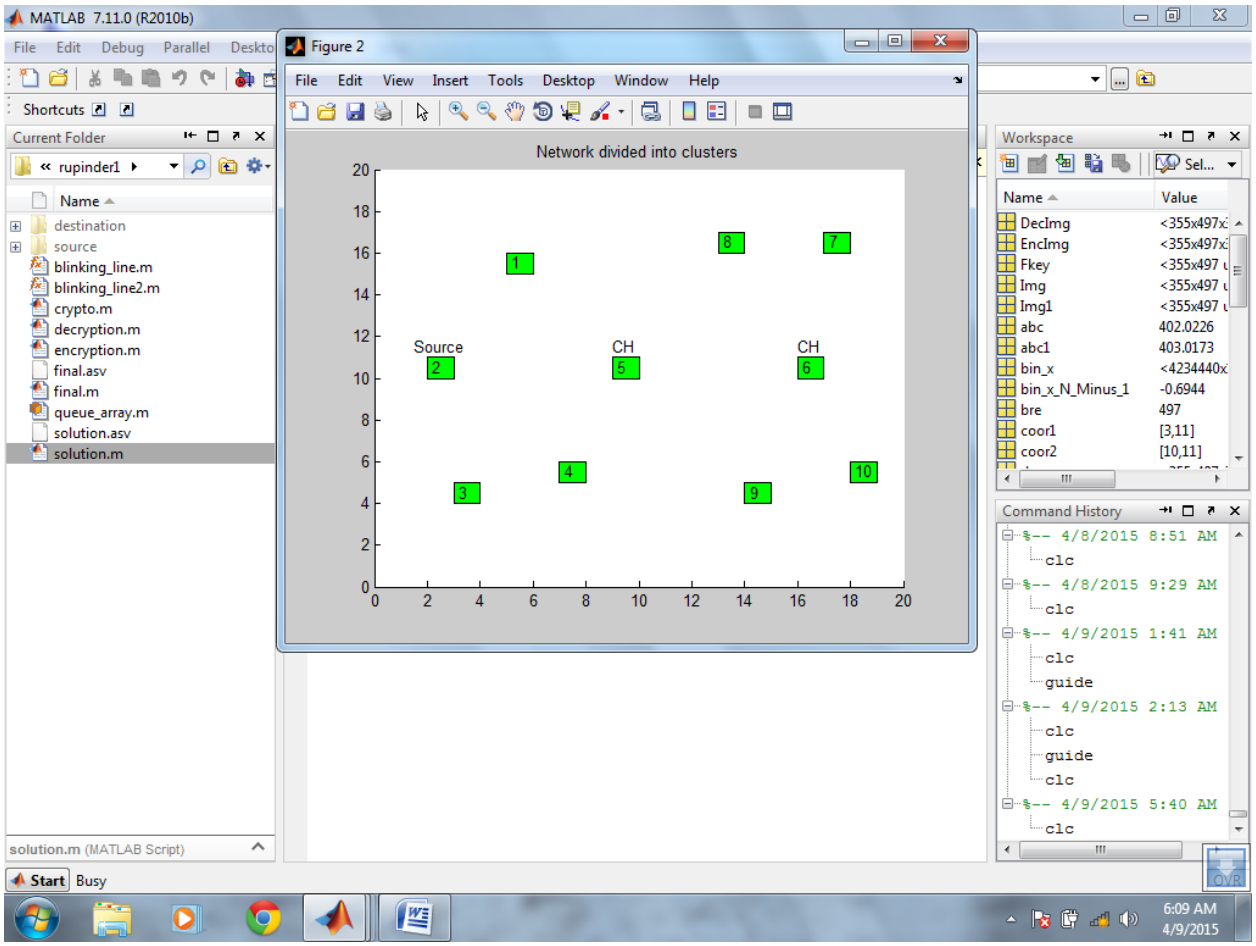


Fig4.9: Network Deployment

The set-up is arranged by the limited sum of movable nodes. In the network source and cluster node is declared. The cluster head node is to allocate tasks to the source node for which it requesting

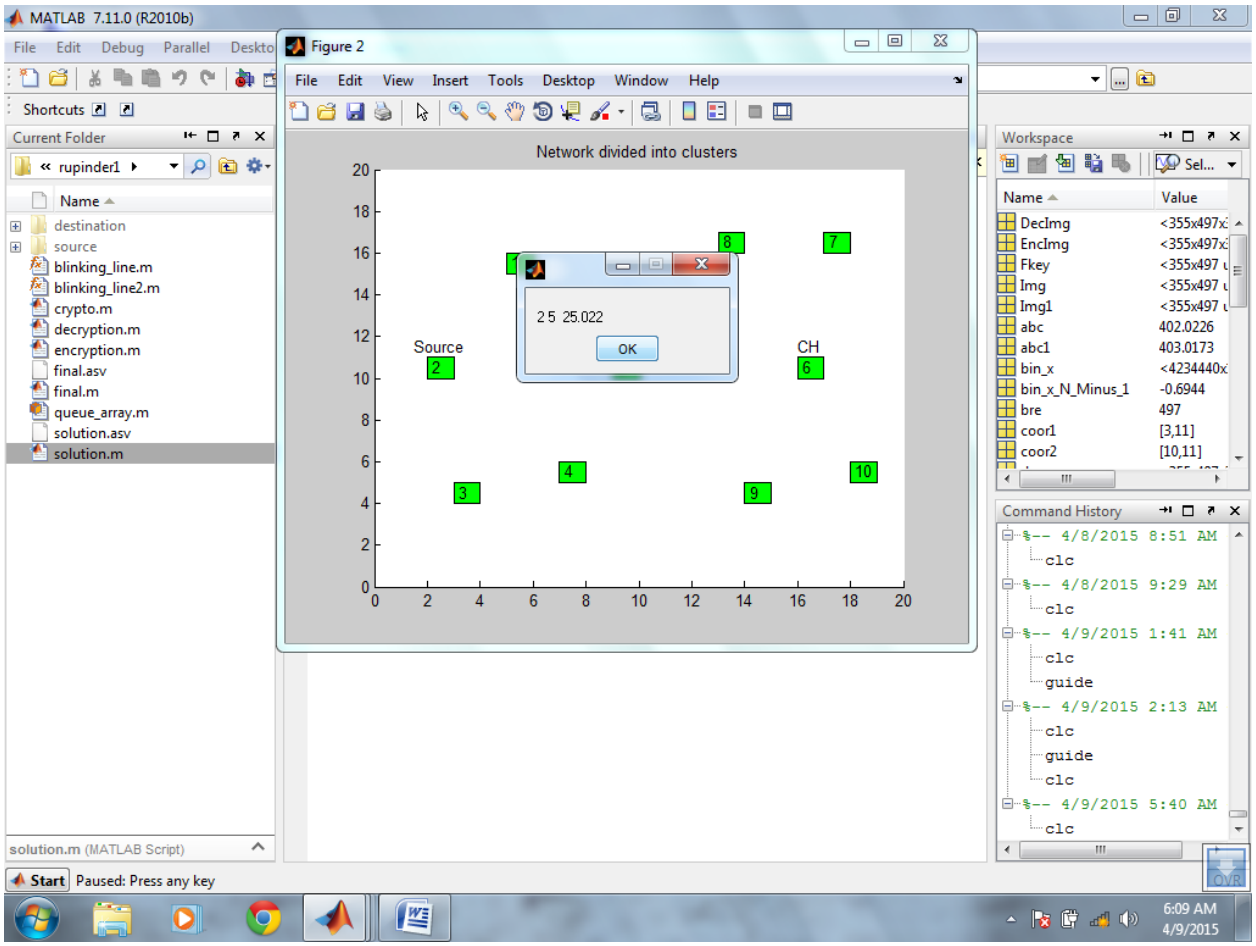


Fig4.10: Request for resources

The net is organized with the predetermined quantity of moveable nodes. In network source and cluster node is declared. The cluster head node is to allocate tasks to the source node for which it requesting. The cluster head 5 get request from node 2 at time 25.22

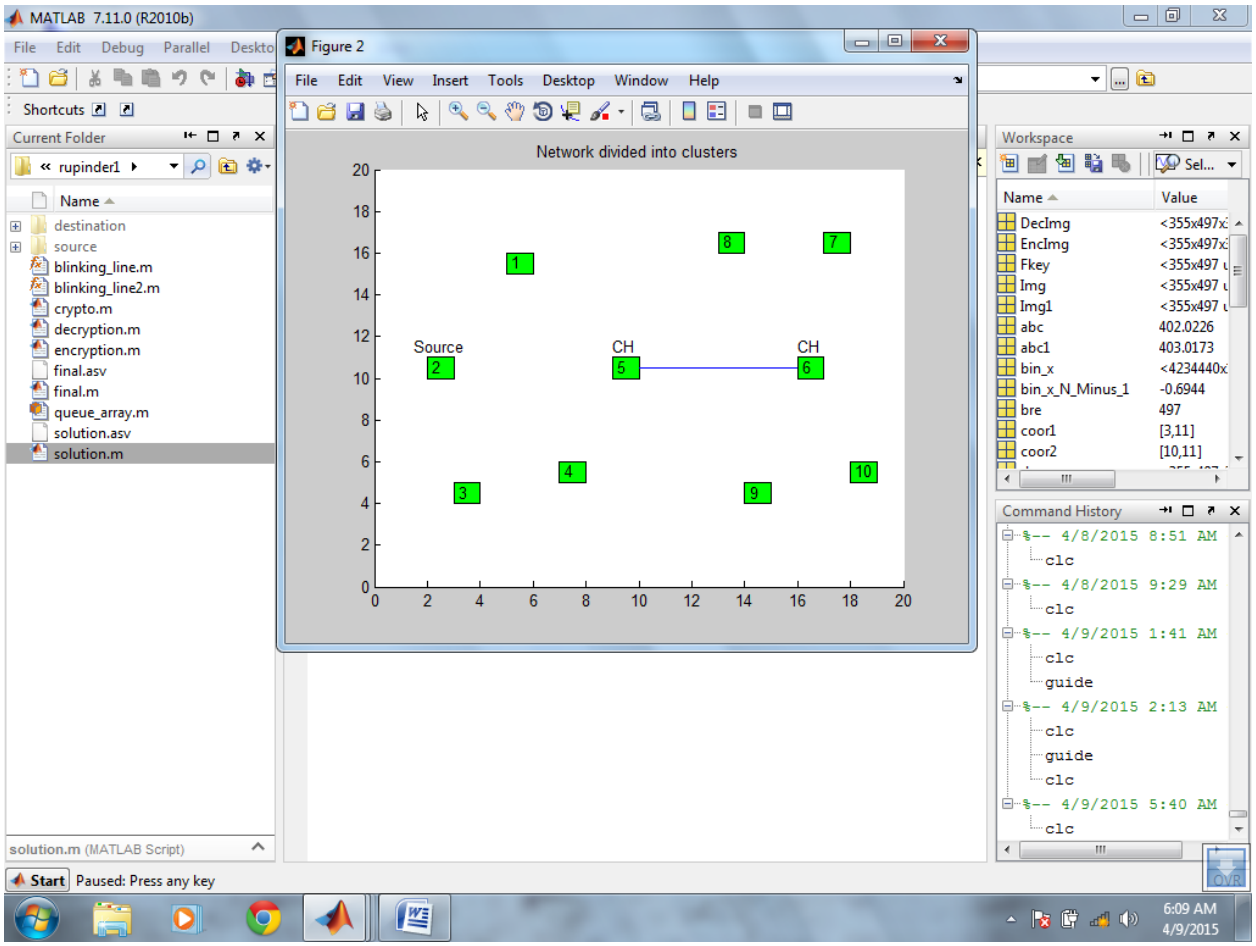


Fig4.11: Request for resources

The set-up is arranged with the limited amount of portable nodes. In network source and cluster node is declared. The cluster head node is to allocate tasks to the source node for which it requesting. The cluster head 5 get request from node 2 at time 25.22. The cluster head 5 pass the request to cluster head node 6.

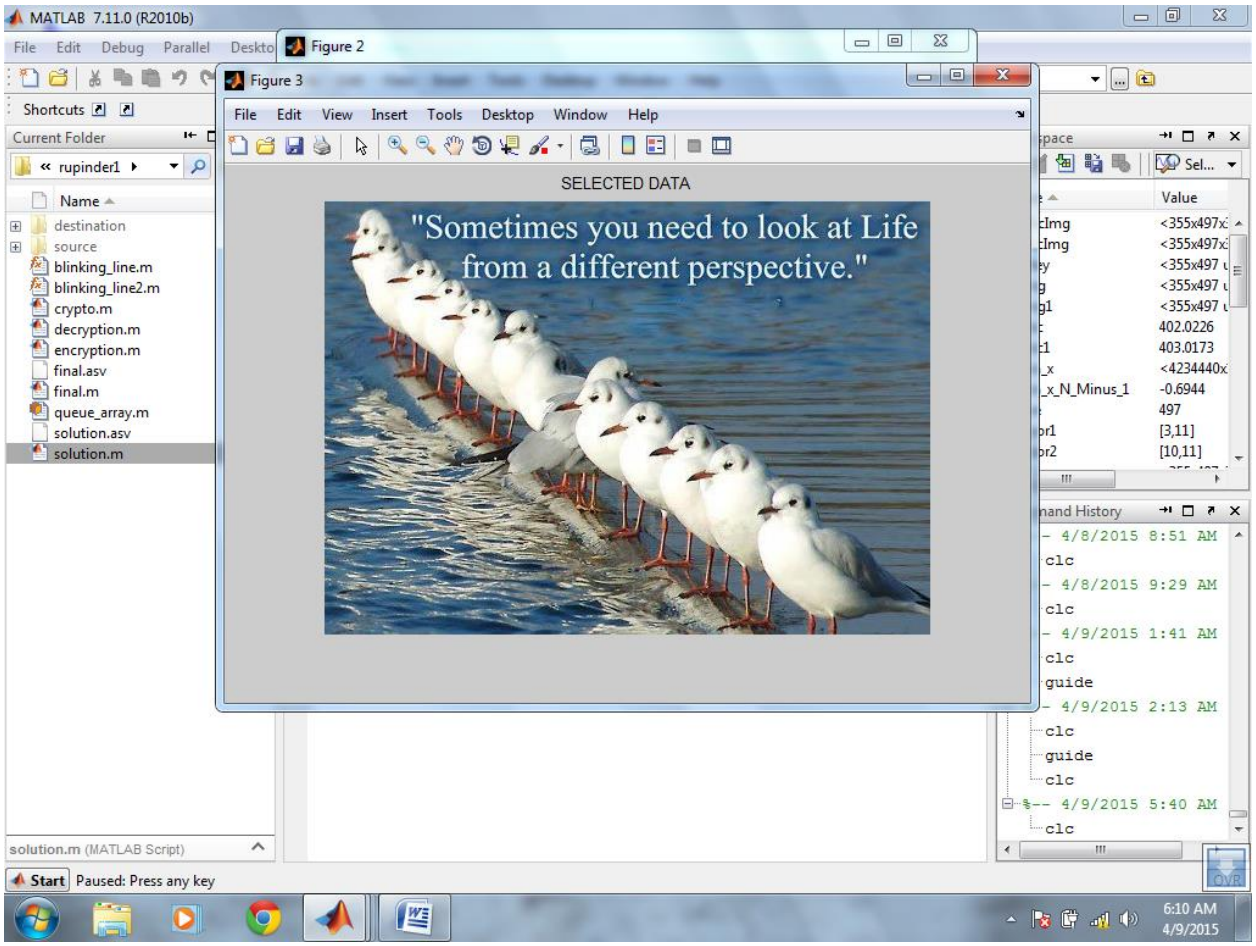


Fig4.12: Source select data for transmission

The set-up is installed with the limited figure of movable nodes. In network source and cluster node is declared. The cluster head node is to allocate tasks to the source node for which it requesting. The cluster head 5 get request from node 2 at time 25.22. The cluster head 5 pass the request to cluster head node 6. The cluster head gave resource to source node. The source node selects data for transmission

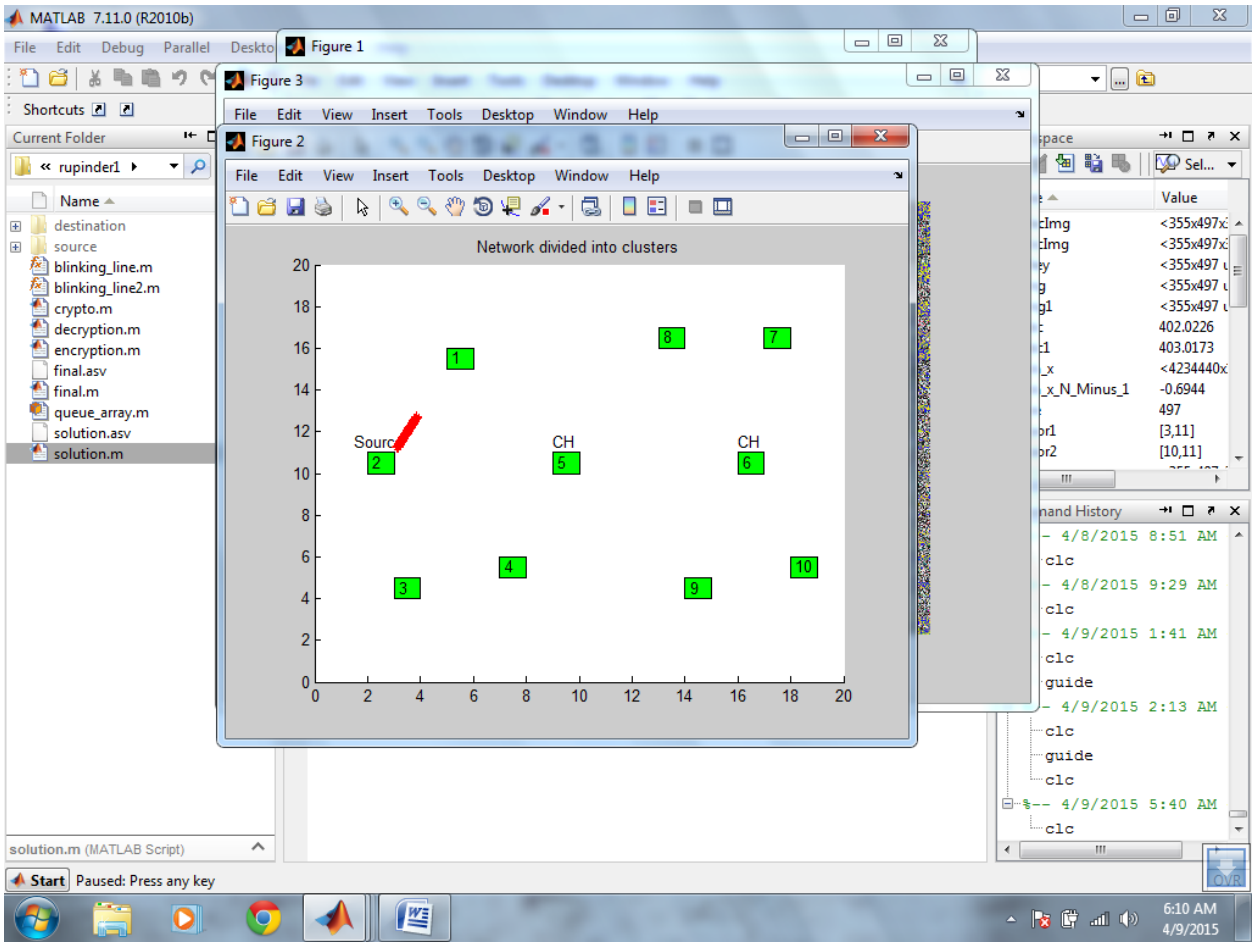


Fig4.13: Transmission start between source and destination

The set-up is installed per the fixed figure of portable nodes. In network source and cluster node is declared. The cluster head node is to allocate tasks to the source node for which it requesting. The cluster head 5 get request from node 2 at time 25.22. The cluster head 5 pass the request to cluster head node 6. The cluster head gave resource to source node. The source node select data for transmission and source node start sending data to destination node.

Fig.4.14 Delay graph

This graph shows the delay between old and new scenario. The delay of new is less then old. The given values show the delay occurs between the nodes. According to graphs values the delay in nodes is more in old technique but it is less in new scenario.

Fig.4.15 Message Complexity graph

This graph shows the message complexity of the new and old scenario. Message complexity is more in old scenario. When the no of nodes increase message also increase in old algorithm.

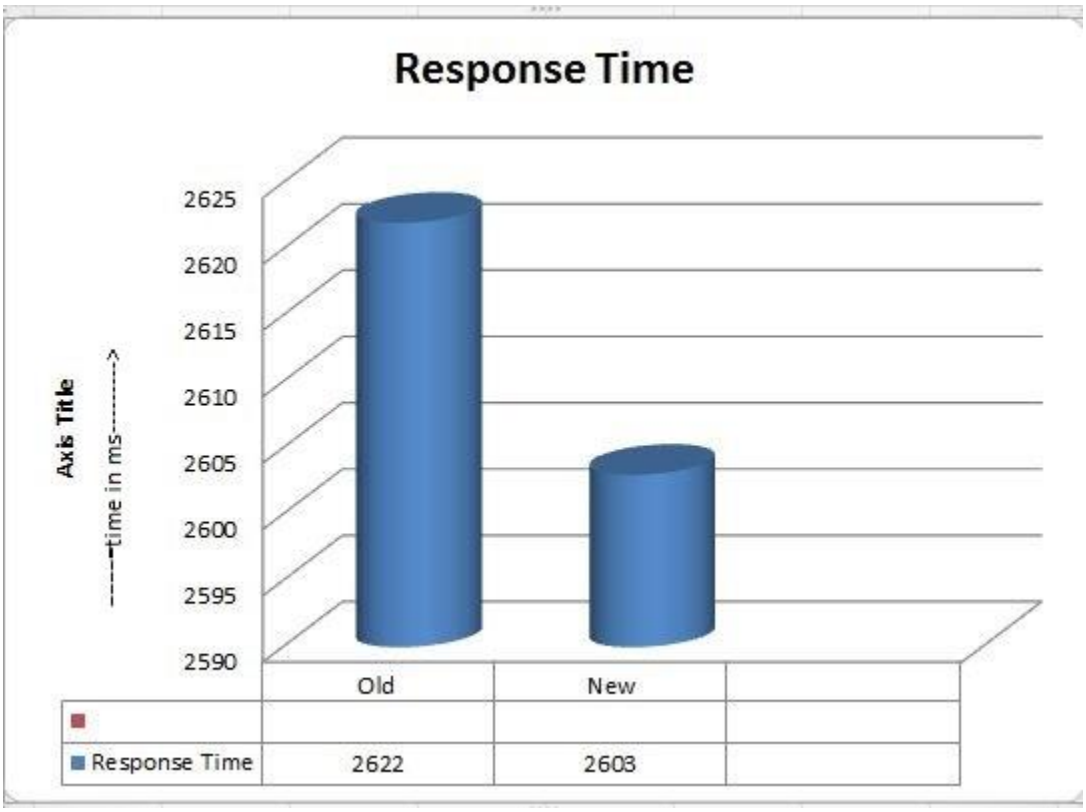


Fig.4.17 Response time graph

This describe the response time of old and new techniques. The response time of old scenario is more than new. Response time is that when a node sends the request message to cluster head, node wait for response.

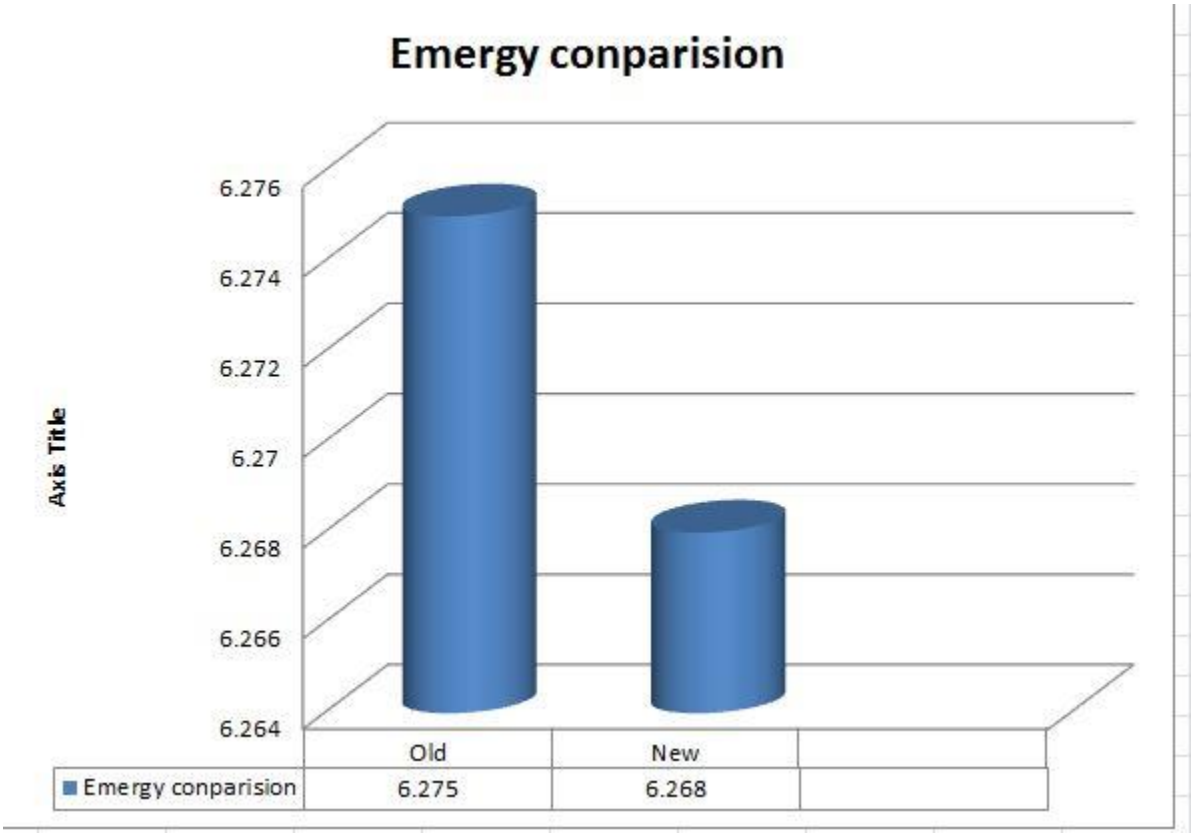


Fig.4.16 Energy Comparison graph

This graph shows the energy comparison between the old scenarios and new scenarios. When data transmit over the network the nodes consumes energy and it also reduces the life time of the nodes. It shows the energy consumed by the nodes in the old and new techniques.

Chapter 5

Conclusion and Future scope

The MANET is a collection of mobiles or devices that are associated together to form a network this is independent of any infrastructure. It means there is no BS required in MANET. So the nodes can interconnect by additional nodes which are in the variety of network only. In MANET, each node has batteries attached to it, which is consumed during the process of transmission i.e. during transmission, reception and overhearing and many other reasons. It is very difficult to replace batteries or to re-charge them. So to growth the longevity of the network; the available battery power must be judiciously used. To rise the long lifetime of the network or battery power of the node, through the proposed technique the problem is resolved using the mutual exclusion algorithm. The Permission-based MUTEX to grow the concurrency of the nodes, to decrease the response time and fall the synchronization time of the nodes. So that it will also support to raise the long life of the nodes. At last measure the performance of the exiting algorithm and the future algorithm.

Future Scope-: In MANET, each node has batteries attached to it, which is consumed during the process of transmission i.e. during transmission, reception and overhearing and many other reasons. It is very difficult to replace batteries or to re-charge them. So to growth the longevity of the network; the available battery power must be judiciously used. The proposed algorithm is permission-based mutual exclusion. Through this technique decrease the response time and fall the synchronization delay between nodes. So it supports to raise the life of the network or battery time of the nodes. For future here use the queue process because FIFO is not so effective. Critical section will not use because of when generate the queue, nodes that present in the queue will be automatically communicate with the other node according to its priority and there selective parameters according to requirement.

Chapter 6

References

Books

C.K. Toh. " Ad hoc Mobile wireless network protocal and system".

Research Paper

[1] Abhilasha, G. (2013). "A permission-based clustering mutual exclusion algorithm for mobile ad hoc network".

[2] Anju, S. (2012). "A Differential evalutaion algorithm for routing optimization in MANET".

[3] C., P. m. (2010). "A novel permission based reliable distributed mutual exclusion algorithm for MANET". *IEEE*.

[4] Chittarjan, M. a. (2013). Arbitration based Reliable Distributed Exclusion for Mobile Adhoc Networks".

[5] D., S. M. (1997). "A distributed mutual exclusion algorithm for mobile computing environment in information system".

[6] H., C. T. (2007). "A MANET Architecture Model".

[7] I., H. a. (n.d.). "An overview of MANET applications and challenges".

[8] J., C. (2009). "Evaluating the energy consumption reduction in MANET by dynamically switching-off network interface".

[9] Jailani, k. a. (2011). "Node selection based on energy consumption in MANET".

[10] Joshi, W. L. (2005). "Security Issues in Mobile Ad Hoc Networks- A Survey".

[11] K., S. Y. (2004). "Key Management for Heterogeneous Ad Hoc Wireless Networks". *IEEE*.

[12] Li, H. D. (2002). "Routing Security in Wireless Ad Hoc Network". *IEEE*.

[13] M., J. H. (2004). “An overview of Mobile Adhoc Networks: Applications and challenges”,.

[14] M., T. P. (2013). "A token-based distributed group mutual exclusion algotirthm with quorums for MANET".

[15] N., R. (2011).), “Study of Various Attacks in MANET and Elaborative Discussion of Rushing Attack on DSR with clustering scheme” Int. J. Advances Networking and Application Volume:3.

[16] O., D. (n.d.). "A merging clustering algorithm for mobile ad hoc network".

[17] O., E. K. (2009). "A distributed mutual exclusion algorithm for MANET".

[18] P., K. (2005). “Selfish MAC layer Misbehavior in wireless networks”. *IEEE*.

[19] Roberto, A. (2001). "Distributed Mutual Exclusion Algorithm for mobile ad hoc network".

[20] Tang, O. D. (2011). “An Efficient Mobile Authentication Scheme for Wireless Networks”. *IEEE*.

[21] Tsudik, G. (2010). “Anonymous Location-Aided Routing Protocols for Suspicious MANETs”.

[22] Tsudik, K. E. (2010). “ALARM: Anonymous Location-Aided". *IEEE*.

[23] V., L. T. (2008). “Prevention of Black Hole Attack in MANET”, Journal of Networks.

[24] Yuvaraju, B. (2009). "Enhancing the performance of MANET by monitoring the energy consumption and use of mobile relay".

III. Websites

[25] http://en.wikipedia.org/wiki/Mobile Ad Hoc Network.

[26] http://en.wikipedia.org/wiki/MANET.

[27] https://datatracker.ietf.org/wg/manet

Chapter 7

Appendix

AODV- Ad-Hoc on demand distance vector routing

CS- Critical Section

CTS- Clear to send

DME- Distributed Mutual Exclusion

DSDV- Destination sequenced distance vector

DSR- Dynamic source routing

MANET- Mobile Ad-hoc network

NIC- Network interface card

PBMUTEX- Permission-based mutual exclusion

RTS- Ready to send

TORA- Temporally ordered routing algorithm