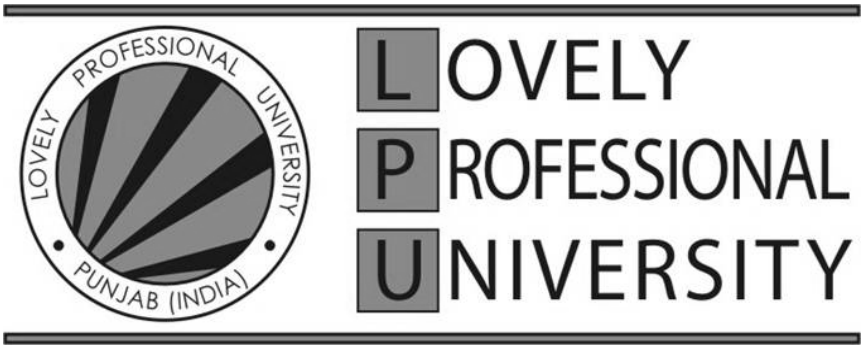

A Reliable Distributed Mutual Exclusion in MANET

A Dissertation proposal

Submitted

By

Mandeep Kaur

11308595

to

Department of Computer Science & 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

Shabnam Sharma

(Asst. Professor)

(May 2015)

PAC FORM

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: Mandeep Kaur — Registration No: 11308595

Batch: 2013-2015 — Roll No. B36

Session: 2014-15 — Parent Section: K2305

Details of Supervisor: — Designation: AP

Name: Shekhar Sharma — Qualification: M.Tech

U.ID: 14593 — Research Experience: 01

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

PROPOSED TOPICS

1. Energy consumption in MANET
2. Security aspects in MANET
3. Routing Protocol in MANET.

Signature of Supervisor: Shekhar 14/10/14

PAC Remarks:

Topic '1' is approved

APPROVAL OF PAC CHAIRPERSON: Signature: 11/10/14 Date:

*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

Mobile Adhoc Network is a decentralised type of infrastructure less network. This work presents an overview of the Distributed Mutual Exclusion algorithm &various enhancements done on distributed mutual exclusion. In DME, Permission-based algorithm and token based algorithm are used. The problem with Permission based Algorithm is of deadlock. The Proposed Methods are used to enhance the Permission based algorithm. With the help of these methods, we can increase the concurrency between the nodes, decrease the message complexity, synchronization delay and response time. By improving all these factors, the life time of the network will automatically increase.

ACKNOWLEDGEMENT

I feel great pleasure in submitting this report as the culmination of my guide's efforts. This required a very hard work, sincerity and devotion that I tried my best to put in my work and in turn gained a lot of knowledge and confidence from this analysis.

I am deeply grateful to my mentor respected **Miss. Shabnam Sharma, Assistant Professor, CSE, LPU** who has helped me in each and every step till the begin till now. She has been a constant guiding force and source of illumination for me. It entirely goes to her credit that this work has attained its final shape. I would like to thank her for her valuable advice and guidance. I would also like to thank all my friends who were always there to motivate me in every step. They helped me a lot, also thanks to all those persons who are directly or indirectly involved in completing my work.

Mandeep Kaur

CERTIFICATE

This is to certify that Mandeep **Kaur** has completed M.Tech dissertation Proposal Titled "**A Reliable Distributed Mutual Exclusion 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 in Computer Science.

Date: **Signature of Advisor**

Name

UID

DECLARATION

I hereby declare that the dissertation proposal entitled, "**A Reliable Distributed Mutual Exclusion 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: **Name MandeepKaur**

Reg No. 1130859

Table of Content

List of Figures

CHAPTER 1

INTRODUCTION

1.1 Ad hoc Network

Ad hoc network is a decentralized type of wireless network. There is no fixed infrastructure such as routers in wired networks or access points in wireless networks. There is no pre-existing infrastructure like base stations as mobile switching. All the nodes forward data to other nodes to participate in routing process. Basically it is a network which is used in emergency causes. Nodes which are within radio range of each other communicate directly via wireless links. Wireless network offers certain advantages over the wired networks that are explained as follows:

- Setting up such wireless system is fast and also the need for pulling out the cables through walls can also be reduced.
- They provide more flexibility and can adapt to changes in the Configuration of the network easily.
- Wireless networks can be used to the places that cannot be wired.

1.2 Classification of Ad-hoc networks

There are two types of classification existing in ad-hoc networks which are as following:

1. Single hop

2. Multi hop

Single-hop: Here nodes are in direct communication and both nodes are in range of each other. The probability of link failure is more in this hop.

Multi-hop: In this hop nodes are communicate with the help of internal nodes not directly. To reach from source to destination internal nodes participate.

1.2.1 Types of Ad-hoc Network

Wireless networks can be classified in two types. These are defined as follows:

1) Infrastructure Networks

2) Infrastructure less Networks

Infrastructure Networks:

Here in infrastructure network, communication takes place only between the nodes and the access points. The communication takes place between the nodes using access point which is used to control the medium access that acts as the bridge to the wireless and wired networks. Base stations are permanent here. If a node goes out of the range then it may enter into other base station's range. Cellular networks are one of the examples of infrastructure Network.

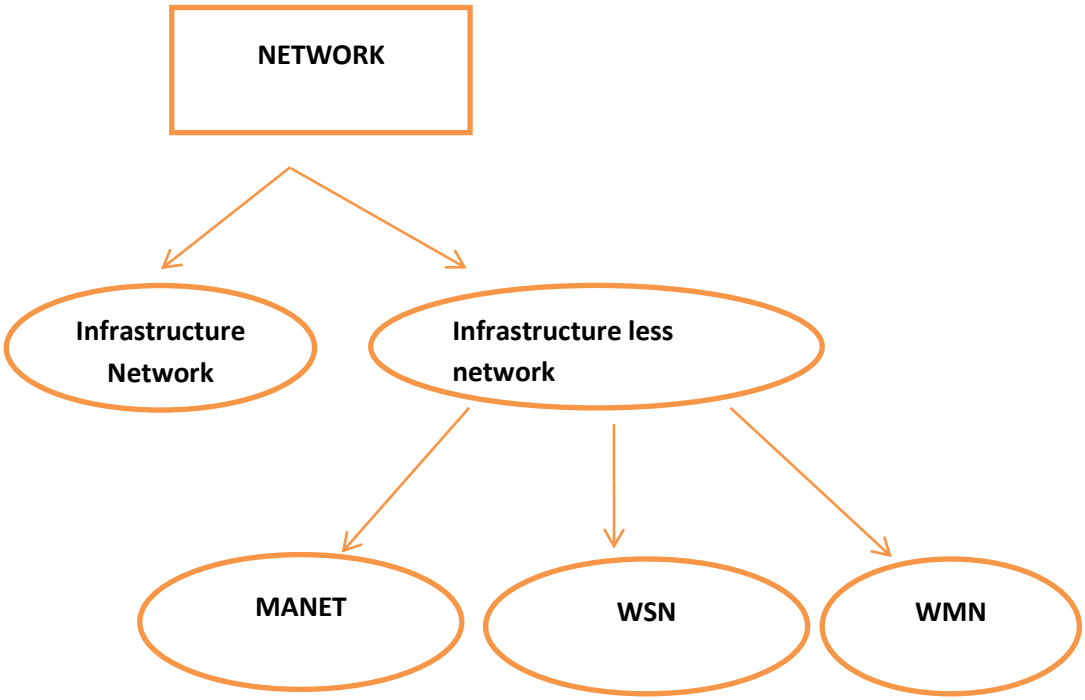

Fig 1.1: Classification of Network.

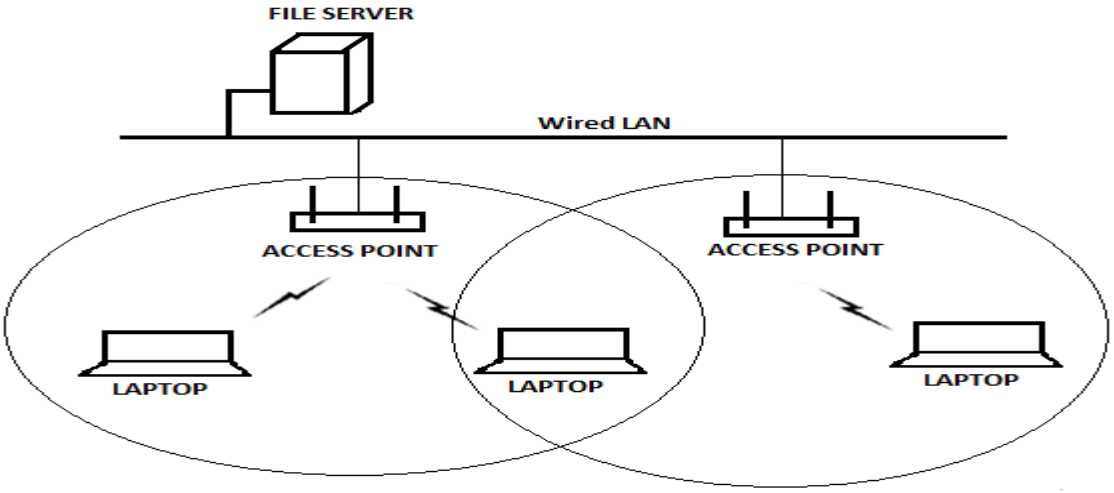

Fig 1.2 Cellular Networks

Infrastructure less Networks:

In this network, each node can communicate directly with other nodes as there is no need of access point for controlling medium access. Routers used here are not fixed. All the nodes are required to act as routers and all nodes are capable of movement and can be connected dynamically. All the devices here are wirelessly communicated to each other. In such types of network, file server contain BS of Wi-Max which controls all access points the range of 6kms. Here fig shows a simple peer to peer network with three nodes. The outermost nodes are not within the range of each other. However the middle node may be used to forward packets between the outer most nodes. The middle node will be acting as a router and the three nodes have formed an ad-hoc network.

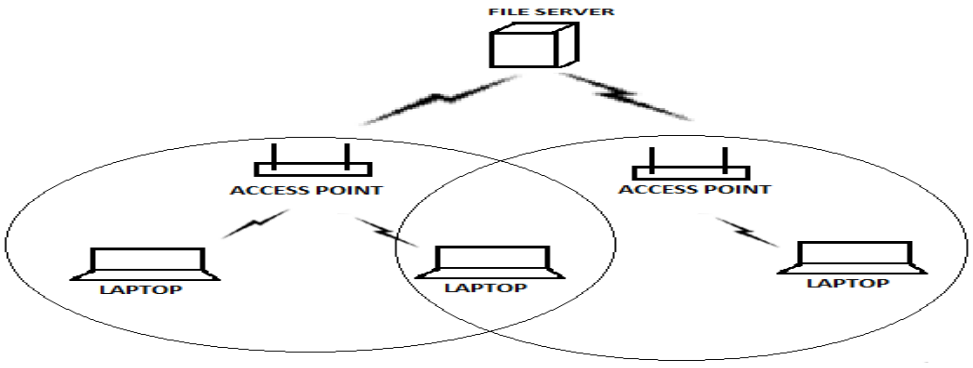

Fig 1.3 Infrastructure less network

MANET

MANET stands for Mobile ad-hoc Network is type of self-configuring infrastructure less network, where all the devices are connected by wireless links. It is a group of mobiles or other wireless devices that are connected together to form a network, which is independent of any infrastructure. It means there is no base station. So the nodes can communicate with other nodes which are in the range of network only. Here each node in a network can act as a router at the same time, and these nodes are independent to move freely. "Flooding" is a technique that is used to forward the data from one node to other one. So because of this this the topology changes frequently and unpredictably in MANET .The data should be routed via intermediate nodes, and these intermediate nodes will act as a router. For communication single hoping and multihopping is used.

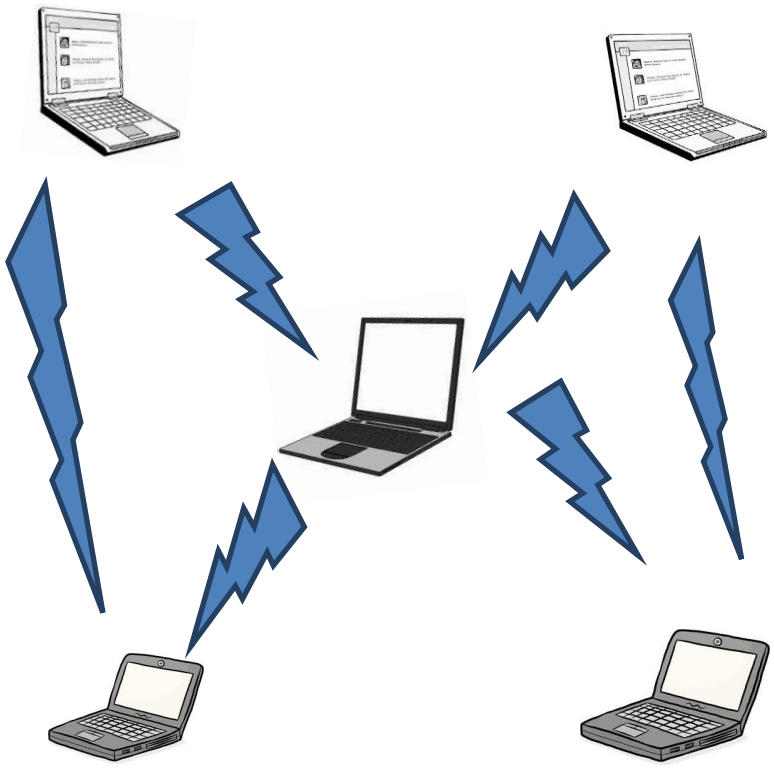

Fig 1.4 Mobile Adhoc Network

.

1.3 Characteristics of MANET

1. Easy to deploy: MANET has no central controller. It is inrastructureless 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.

1.4 Major challenges and issues in MANET

1. **Hidden terminal problem**: Here terminal A is hidden from C, but A and C can communicate with B. as A is communicating with B and B is also transmitting at the same time as it is not aware about A's transmission with B. So Collision will take place here. This leads to difficulties in media access control.

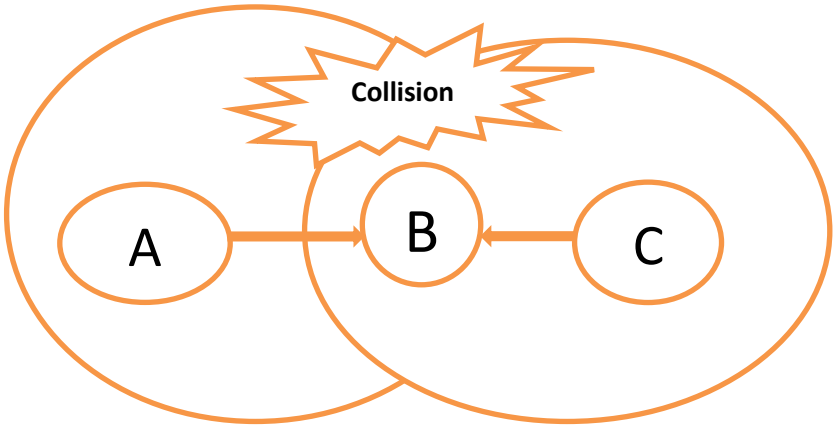

Fig 1.5 Hidden Terminal Problem

2. **Exposed Terminal Problem**: Due to a neighboring transmitter, when the node is prevented to send packets to other nodes, ETP arises. Here R1 and S1 are transmitting but in the same network node S2 wants to transmit the data to node R2, so transmission between R1 and S1 will prevent node S2 to send data to R2.

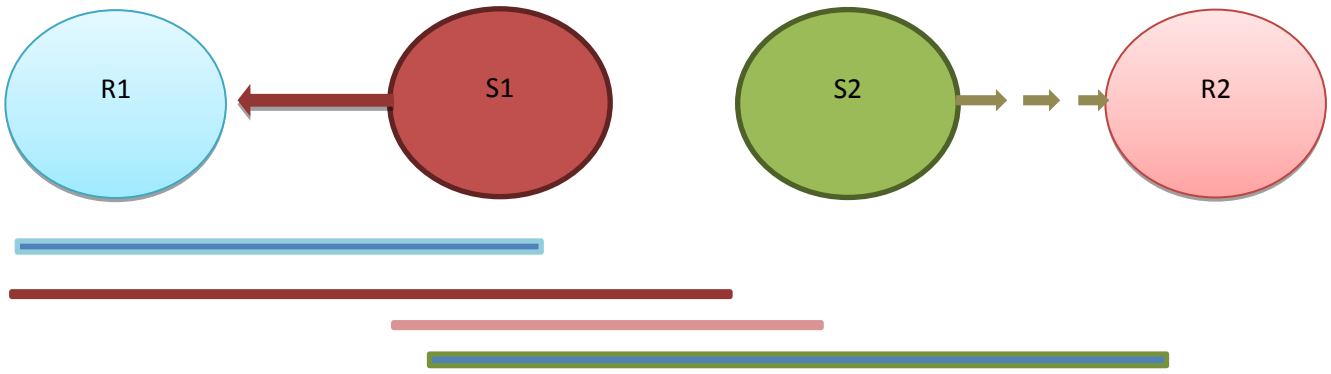

Fig 1.6 Exposed Terminal Problem

3. **Problems in Routing**: As the routers are in moving state. So the link changes quite often because of that the loss of packets will take place and cause the process of transmission. Because of link broken, the updates are sent often, so difficult to manage the routing tables. In some cases routing loops may exist.

4. **Problems in Access**: It arises because of distributed channel access; i.e. no fixed base station concept, it's hard to avoid the packet collision.
5. **Problem in Mobility**: It affects the signal transmission, communication, access of channel, routing, multicasting and other applications. Wireless consumes much power during the process of transmission, reception and overhearing, nodes have battery system attached to it that has low life time.
6. **Power consumption:** In MANET nodes have batteries attached to them. So the power is consumed while sending, reception, overhearing etc. recharging or replacing them is very difficult task. So to conserve energy is very challenging task.
7. **Power Problem**: Nodes in MANET are having batteries attached to them. So these batteries are consumed when they take part in the communication process. As the batteries in the nodes are limited so we have to use it very wisely. To reduce the wastage of energy in the nodes is one of the major challenges.
8. **Others:** Some other challenges includes Packet drop**,** Noise error, Contention and Security etc.

1.5 Applications:

1) **Local Level**: Manet may be used at local level for example at home networks, where wireless devices can communicate directly with each other to exchange information between them.
2) **Military environments**: Military equipment consists of some computer equipment's. Ad- hoc network can be used in military to maintain the information network between the soldiers, military information head-quarters and vehicles,.
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.

1.6 Advantages:

1. MANET required only wireless connection.
2. In MANET each device and node can move independently in any direction but within range.
3. This network can locate at any place and time.
4. MANET required less time and cost.
5. Does not require any cabling.
6. MANET is temporary.

1.7 Attacks on MANET :

There are two types of attacks in MANET :

1. Passive Attacks
2. Active Attacks

Passive Attacks:

In passive attack, without disturbing the communications operation data is exchanged in the network. The passive attacks are difficult to detect. Operations are not affected. The operations are supposed to be accomplished by a malicious node ignored and attempting to recover valuable data during listens to the channel . Examples of Passive Attacks are eavesdropping.

Active Attacks:

In active attack, it may harm the information and operation if any data or information is inserted into the network. It involves fabrication, disruption and modification, and also affects the operation of the network.

Example of active attacks is spoofing and impersonation.

CHAPTER 2

LITERATURE SURVEY

(G. Ricart, jan.1981) Discussed that for ME, nodes send requests message to all the nodes, other nodes either send a reply message or defer the response. The node receiving the request message can easily determine whether it should be allowed to enter critical section by sending reply message or not. Reply message is sent back to the requesting nodes according to their priorities which includes sequence numbers. If in case sequence number is same then we check the node number. The node having lowest sequence number will enter the CS first. If any node restarts(after failure), it should first notify other nodes that it failed, and wait for long to be sure that its old messages were delivered and the network processed its failure.

(Erciyes K. 2004) discusses architecture that consists of ring of clusters for DME algorithm. Proposed mechanism each node on the ring represents a cluster of nodes and implements various DME algorithms. Proposed architecture also implements Ricart-Agrawala and token-based algorithm. Message complexities for both algorithms reduce in architecture as well obtaining better response times parallel processing in clusters. Cluster head.

(Dagdeviren O, 2004) Described the cluster merging approach. Clustering is generally used approach in various problems like routing and resource management in MANET. Clustering approach is ease to implement. They proposed a fully distributed algorithm for clustering, that merge the clusters to form higher level by increase their level. They show operation of algorithm and analyze its time, message complexity. The algorithm proposed is scalable and has a low time and message complexity.

(Weigang Wu J. C., 2007) Suggested that infrastructure network, consists of two sets of entities i.e. MH and MSS, where MSS acts on behalf of other nodes to achieve mutual exclusion. In case of MANET, there is no MSS so it becomes difficult to solve the problems here. In case of TBMUTEX, a topology is maintained in ring or in tree in which the token

rotation takes place. Token is unique and the node having token can enter the CS. Every node has to maintain the information about its neighboring node only. There is a problem in token based algorithms i.e. token- and maintaining the topology is difficult here. On the other hand, in case of PBMUTEX we don't need to maintain the topology and because we are not passing any token to other nodes. Here priorities like lamport time-stamps are used to grant the permissions to the requester. Problem of large number of messages to be exchanged between the mobile hosts occurs here. So our major challenge is to reduce the number of messages in PBMUTEX. So Quorums are used to reduce the number of messages.

(LathaTamilselvan, V. Sankaranarayana, **2008)** proposed improvement of the unique AODV protocol. In this algorithm the requesting node will send the Data packets to the reply node at once, it will have to wait till extra replies with next hop details from the other neighboring nodes. After receiving the first request it sets timer, for gathering more requests from different nodes. It stores the sequence number, and the time at which the packet arrives, in a Collect Route Reply Table. Time for which each node will delay is proportional to its distance from the source. It computes the timeout rate based on arriving time of the first route request. After the timeout value, it first checks in CRRT whether there is any repeated next hop node. If any repeated next hop node exists in the reply paths it assumes the paths are correct or the chance of malicious paths is limited.

(N.Yuvaraju. B, 2009) Suggested that a node may die because of excessive utilization, results in energy depletion and also decreases performance. The rate at which energy is consumed depends on the application i.e. word, video or audio etc. based on the application we can estimate the available residual energy or remaining energy. Based on the rate of energy consumption and the remaining energy we can estimate the energy depletion early. Objective is to optimize the utility. Problem introduces are Congestion, energy depletion. Here we set multiple threshold value on a node i.e. low, high. High is for heavy applications and low is for light weight applications. On reaching high threshold, it will be taken as a critical so here mobile relay is required to balance the load on node. Algorithm used here are AODV, DSR and DSDV. He concluded that the energy level is measured based on the residual energy in a node, not depends on the rate at which energy is consumed. As a solution we can use the concept of Mobile Relays. Mobile Relay is used to balance the load on a node hence reduce the energy consumption.

(Ecriyes K, 2009) Proposed a DMUTEX algorithm 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_A algorithm 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.

(Kadir, Jailani, 2011) proposed a probability based node selection method to identify the intermediate nodes with stored energy that can withstand through the duration of Connection. DBEEP are used in this. The energy consumption level of node and the distance factor can be used to determine probability of intermediate node to be selected as a relay node to destination. This technique prevents the early failure of node.

(Bhatsangave, 2012) proposed the OADV which is the solution to the problems that arises in AODV. OADV modifies the mechanism of broadcasting of AODV In this routing protocol nodes does not send any RREQ to inter-mediate nodes unless there is sufficient battery lifetime. OADV avoids the unnecessary broadcasting of RREQ information. It is much better than AODV in terms of battery lifetime and throughput.

(Nema, 2012) Proposed the method to save the energy with AODV routing proto-col. Node in sleep mode consumes less power than idle mode. Energy based Ad-Hoc on-demand Routing algorithm balance the node's energy so that minimum energy level can be maintained within nodes and lifetimes can be increased. Here we set the minimum energy threshold value of node, when any nodes reaches to that limit it will go to sleep mode and hence save the energy.

(Juan-Carlos, 2012) Suggested that we can conserve power system, based on RTS/CTS dialogue of IEEE 802.11 standard, which will switch off the NIC dynamically when they are idle i.e. neither sending nor receiving any data. Algorithm used here are DSR (best), AODV, DSDV, TORA (worst). He concluded that approximately 25 to 60 percent energy can be saved by evaluating routing protocols.

(Sharma A, 2012) proposed a ROA to determine an optimal path from source to destination efficiently, using DE. Problem occurs here when no path is not determined from source to destination, serious problem like high transmission delay arises and then high energy consumption by this node will take place. They used Algorithm DE, GA, PSO, and SA. They concluded that DE shows better results than other algorithms by considering parameters like minimum routing cost and average execution time.

(Murali P, 2013) discussed about DMUTEX which helps mobile nodes to share the critical resources among them so they can reach from source to destination in the network. We place the nodes in a particular place by dividing them into different regions i.e. clusters. In cluster, cluster head will act as an arbitrator that will listen to the requests coming from mobile nodes to enter the critical section. Cluster head will decide whether or not to provide access to the nodes. Voting scheme is used here to grant the permission or allow the node to enter into critical section. If cluster want to allow the mobile node to enter the CS then it will send REPLY message to that willing node. At the same time only one node can enter the CS, so if there is any other node which is requesting to enter the CS then cluster head will send HOLD message to them so they will wait for their turn to enter the CS. Cluster head or arbitrator can have inter-communication or intra-communication within the network. Condition of deadlock arises here if at any time the arbitrator or cluster head fails to perform its function. Which results in extra consumption of resources i.e. energy, time etc. so the wastage of such resources can decreases the life time of the network.

(Talele P, 2013) Defines the GMUTEX. In this problem, same type of processes can request the CS and can execute their CS concurrently. Basically, the different type of processes can request their CS and executes in mutually exclusive manner. The distributed algorithm is used for GME problem in asynchronous message passing distributed systems. The algorithm is token based, process that can obtain a token can enter a CS. It reduces message complexity. When a process request a message, it use coterie as communication structure. Any two quorums allocate at least one process and process act as gateway between the two quorums. The proposed algorithm can reach high concurrency, which is a measurement of performance for number of processes that can be in critical**.**

(A, 2013). They described a PMUTEX and explained about the resource allocation in MANET. They proposed a new approach for mutual exclusion in MANET which is based on clustering and concept of weight throwing. Cluster based hierarchal approach uses in the algorithm which is help to reduce the message complexity and to reduce the number of message exchanged.

CHAPTER 3

PRESENT WORK

3.1 Group Mutual Exclusion Algorithms

GMUTEX allows those processes to enter a CS simultaneously which are in the same group. It means two processes that belongs to different groups cannot enter the CS at a time.

1. CS is a part of program that accesses shared resources.
2. In TBMUTEX, a unique token is shared among the nodes and the node having that token is allowed to enter the critical section.
3. In PBMUTEX, if the node wants to enter the critical section then it must obtain permission from rest of the other nodes first by exchanging messages.
4. In QBMUTEX, each node takes permission from a subset of nodes referred as quorum for executing critical section. Any two quorums contain a common host.

Token Based Algorithm in MANET:

The group mutual exclusion (GME) problem is a generalization of the mutual exclusion problem. **Group mutual exclusion**, only process which is in the same group can enter a critical section (CS) simultaneously. In other words, no two processes in different groups enter a CS at a time.

Critical section is a part of program that accesses shared resources.

In **token based mutual exclusion algorithms**, a unique token is shared among the hosts and if a host possesses the token than it is allowed to enter the critical section.

In **Permission based mutual exclusion algorithms**, the node that wants to enter in critical section (CS) must first obtain permission from rest of the nodes by exchanging messages.

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

Distributed Mutual Exclusion algorithms must satisfy following properties:

1 .**Safety**: No two processes, which are requesting for a different group can be in their critical sections concurrently.

2. **Freedom from deadlocks**: No Two or more hosts should continuously wait for messages that will never arrive.

3. **Freedom from starvation**: A host must not wait endlessly to execute the critical section while other hosts are frequently executing the critical section.

4. **Fairness:** The requests for entering critical section are executed in order of their arrival in the system.

3.2 Problem Formulation

The mobile ad hoc networks are self-configuring network in which mobile nodes can join or leave the network whenever they want. In such type of network it is very difficult for the resource reservation. In the previous times various resource reservation protocols had been proposed. Among all the proposed protocol clustering is the most efficient task allocation technique. Here in fig (3.1) S2 is common to both the region , so it will act as an Arbitrator. Site S0 from region 1 will send a request to arbitrator S2 to enter into the CS. Arbitrator contains a queue which stores the pending requests of sites for entering the CS. Here arbitrator receive request from S0 and it knows that there is no pending requests in its queue. In the meantime, site S1 also send a request to arbitrator, now arbitrator knows that they both are from the same region i.e. region 1.So the priority of S0 is more than S1. So S2 will remain in its queue. Arbitrator will send a token to S0 and it will enter into CS. When S3 will send a request to arbitrator for CS, Arbitrator will send a hold message to it, as there is pending request in its queue by S1.So it will not send reply. When the token reply message of S0 reaches to S1, it will into CS. When the REPLY message of S0 reaches S2, now it will check that there is still one more node in region 1 having higher priority than S3 and hence waits for the reply message from S1.

The main problem exists here in this technique is of deadlocks. When the problem of deadlock arises, the efficiency of the proposed techniques will reduce and energy

consumption in the network will increase. In this work, we will propose enhancement in the technique to remove condition of deadlock from the network.

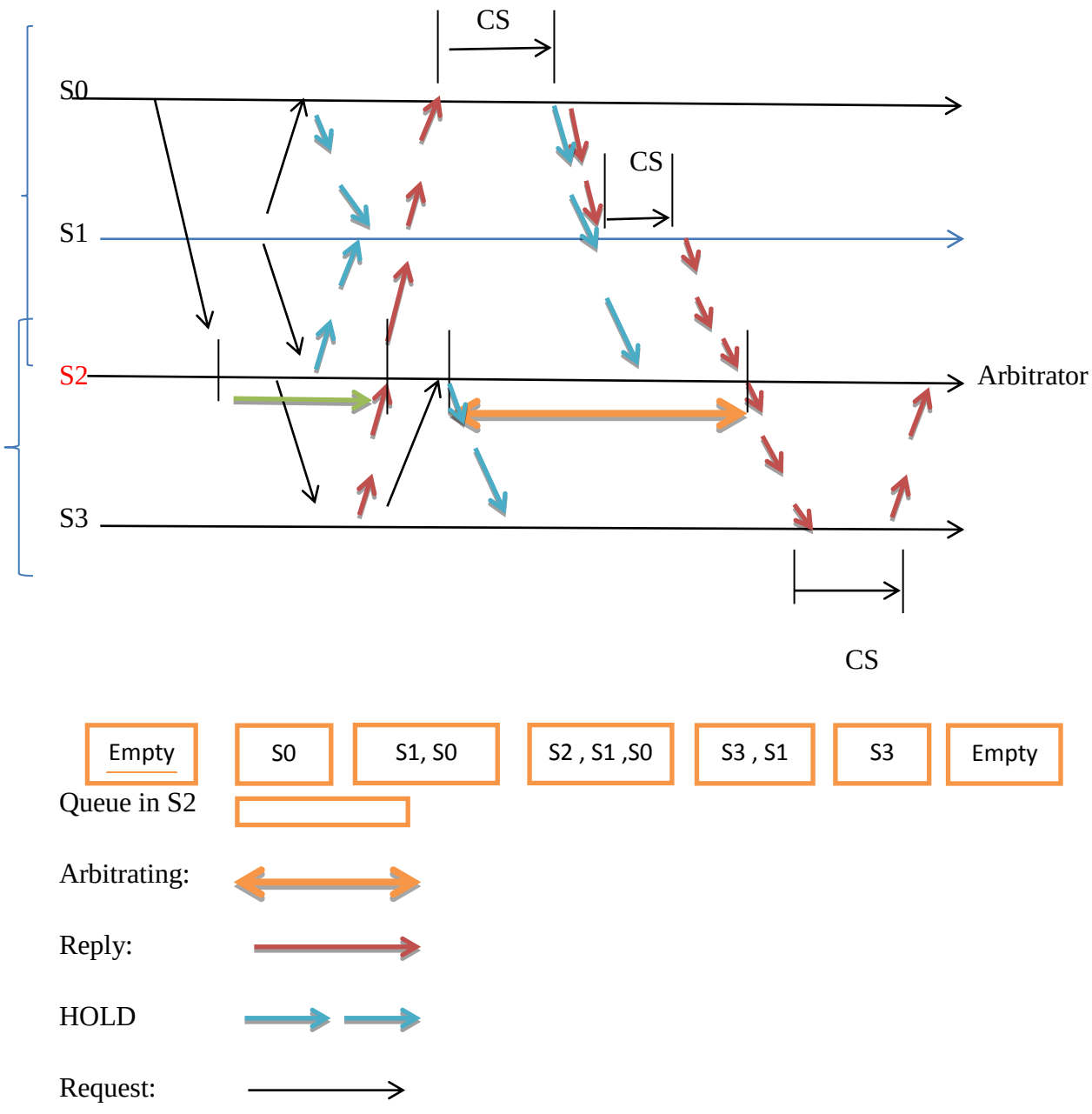

Fig3.1 Working of an Arbitrator.

3.3 Objective

The main of objective of our algorithm are:

1. To remove the problem of deadlock.
2. To optimize the performance parameters like synchronization delay and response time.
3. To reduce the message complexity.

3.4 Scope of study

In case of infrastructure less network, we do not require any infrastructure to work. Here each node can communicate directly with other nodes. So no access point is required for controlling medium access. As there are no fixed routers so all the nodes need to act as routers and all nodes are capable of moving and can be connected dynamically in an arbitrary manner. In MUTEX, only processes that belong to same group can enter a CS simultaneously i.e. no two processes in different groups enter a CS at a time part of program that accesses shared resources is called CS. In TBMUTEX a unique token is shared among the nodes. The node should have that token only then it can enter the CS. In case of PBMUTEX, the node that wants to enter in CS must first obtain permission from rest of the nodes in the network by exchanging messages. In QBMUTEX, each node takes permission from a subset of nodes referred as quorum for executing critical section. Any two quorums contain a common host. The main problem of deadlock condition arises in the architecture .So in this work, we will propose enhancement in the architecture to remove the problem of deadlock from the network. This will leads to increase the efficiency of the networks in terms of throughput, delay.

3.5 Flow Chart:

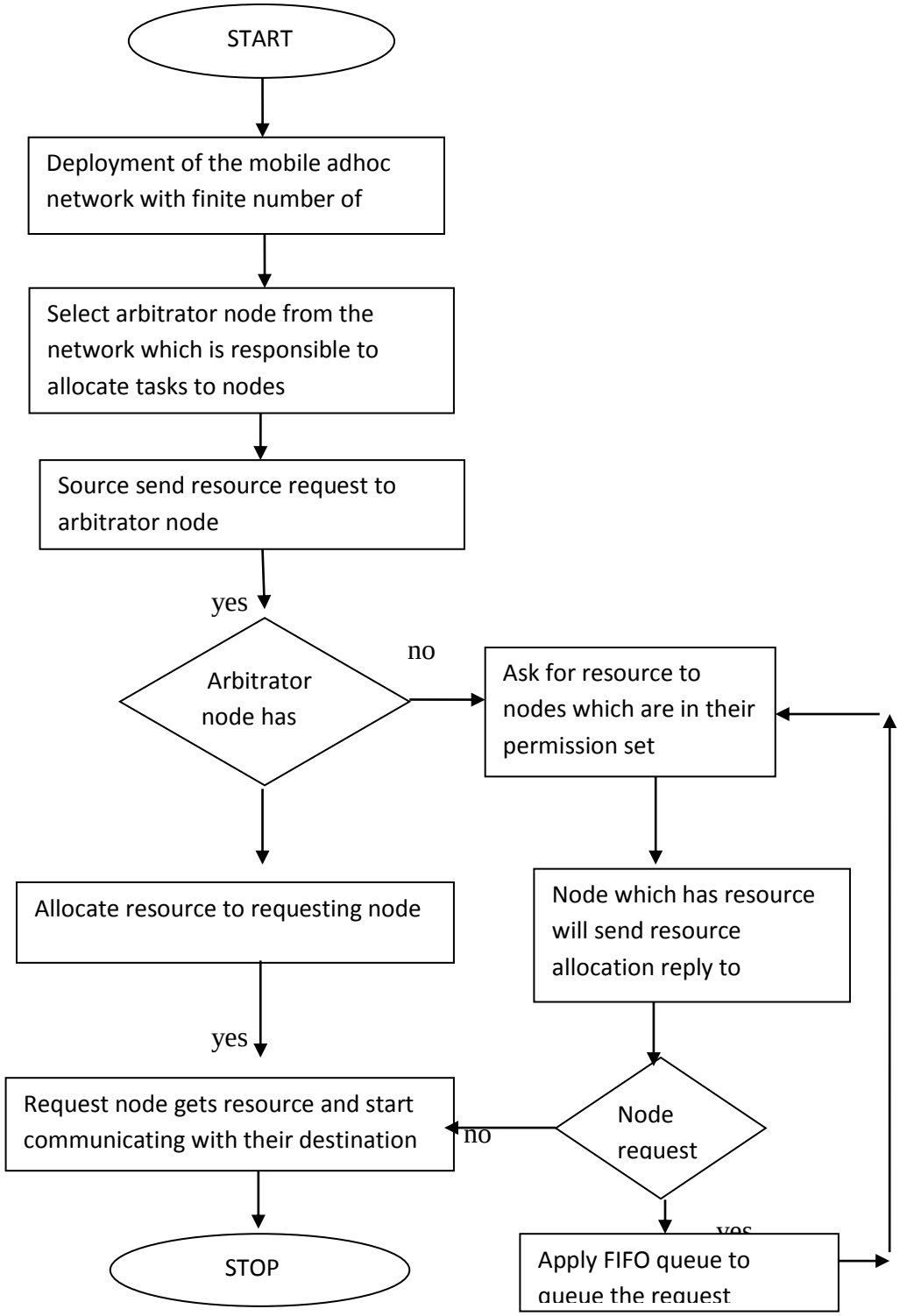

Fig. 3.2 Flow chart

3.6 Research Methodology

Computation Model Assumptions

- We consider a distributed System that consists of '*N'* nodes that are participating concurrently for resource.
- In order to synchronize the processes, a global clock is maintained on each node.
- Handshake protocol is used for region configuration.
- Total numbers of nodes are fixed in regions.
  Concept of Info set and Status set are introduced

The Proposed Algorithm

Our algorithm uses token based approach where the concept of region is used. The proposed algorithm consists of two types of tokens: - main token and sub-token. The main token is maintained as a unique identifier in the system. The main token is passed between two clusters through arbitrator.

A sub-token is generated by the holder of the main token and therefore, the number of sub-tokens may vary. A Sub token is passed between the nodes of single cluster. The primary motivation of the proposed algorithm is to achieve high concurrency, low response time with minimum synchronization delay

The Principle of Proposed Algorithm

First of all we will create the cluster by arranging the nodes at particular positions. In cluster, one node will be acting as a cluster head and other nodes will act cluster members.

Requesting for CS:

When node '*i'* wants to enter in CS, it first sets its timestamp request to the current time and then send the request to nodes for CS, which are present in *info_set* including arbitrator and wait for reply message.

Receiving Request message from node 'i'

- If this node is arbitrator itself and receives request message from node *'i',* then it will send the token to node '*i'* if it itself is not in CS or has high priority, otherwise it will send this request to the nodes of its info set in another region.
- If this node is ordinary node and receives request message from node *'i'* then it sends the reply to node '*i'* if it itself not in CS or has high priority otherwise it will store this request in request queue.
- When the holder '*k'* of the main token receives a request issued by node *i* and forwarded by arbitrator, then that arrived request is put into the queue of the main token

According to the following rules each request in the queue is granted:

- If there is no node which is executing the CS, then the main token will be transferred by a token message to the requesting node.
- If any process is already present in the CS and the requested group is the same as current one, then arbitrator will send a sub-token message to node 'I', as long as there is no request in another region with a higher priority. Otherwise, the request will be kept in the queue of the main token.
- When node 'I' exits the CS, if node 'I' is the holder of the main token then it will decrement the group size by one. Otherwise, i.e., node 'I' holds a sub-token, it returns a sub-token by sending a release message.

3.7 **Performance Metrics**

1. **Message complexity:** The number of messages that are required per execution by a site.
2. **Synchronization delay:** The required time when site leaves the critical section, and before the next site enters the CS.
3. **Response time:** It is the time interval that a request waits for its CS execution to be over after its request messages has been sent out.

3.8 Timeline

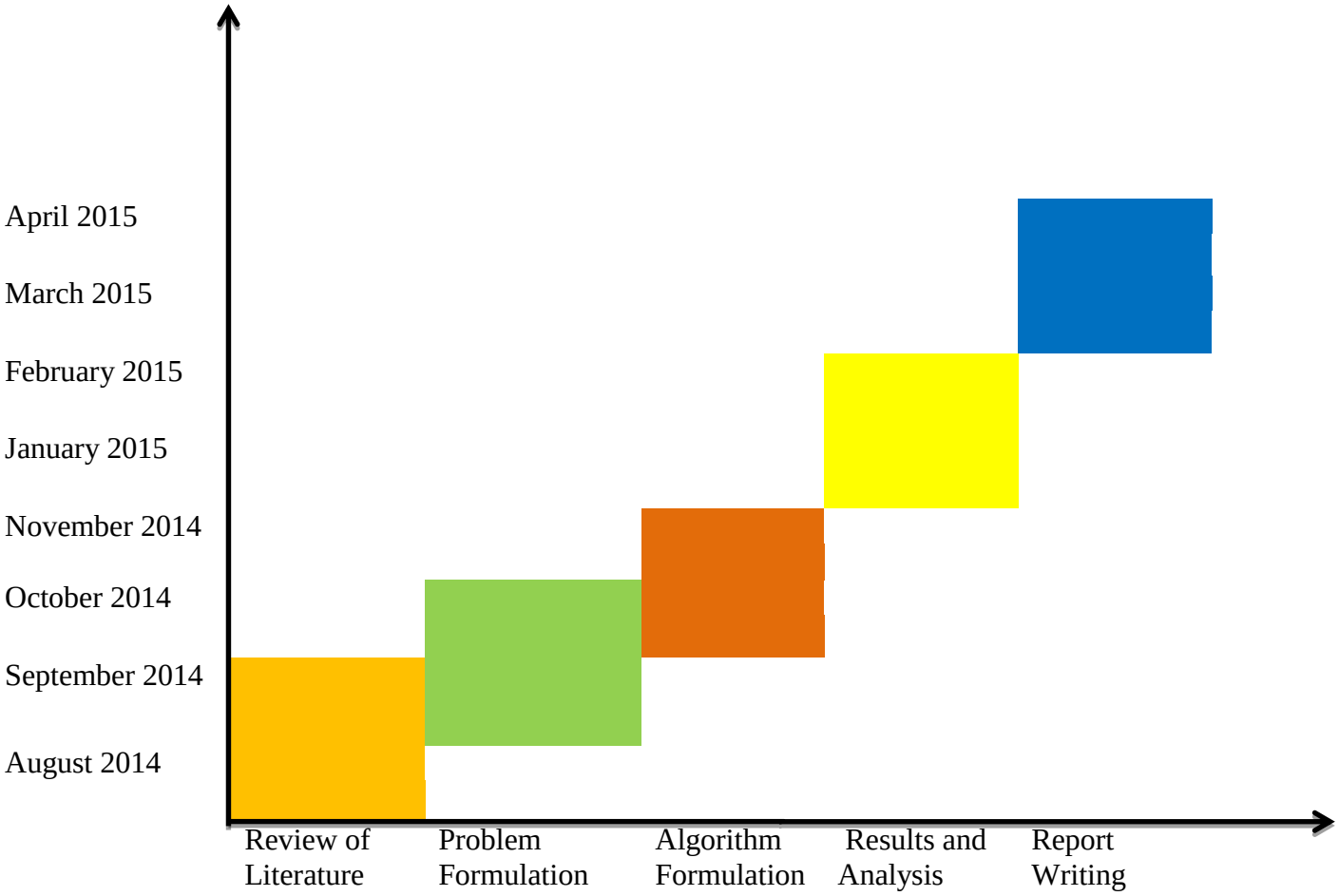

Fig 5.1 Timeline chart

CHAPTER 4

RESULTS AND DISCUSSIONS

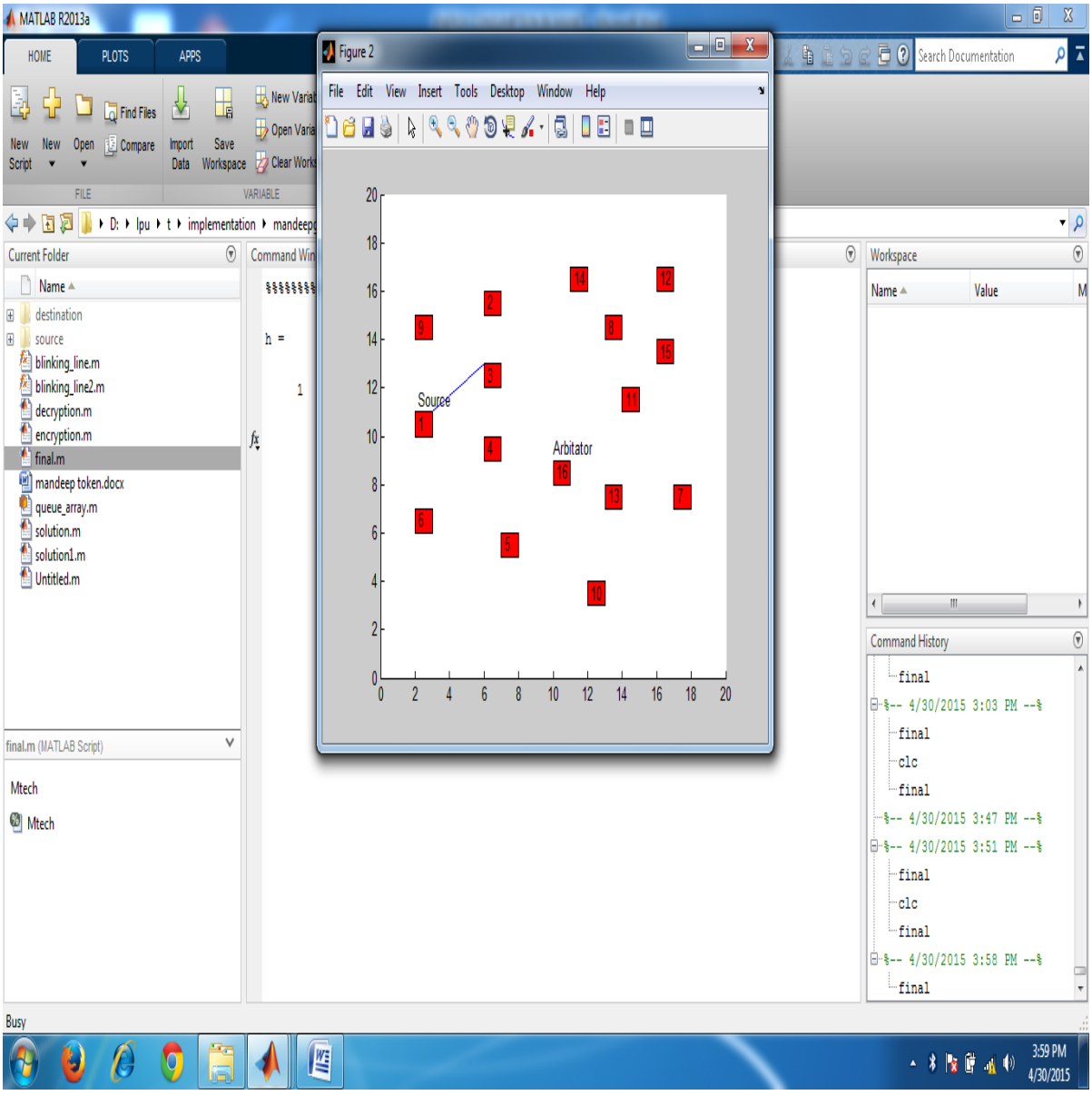

Fig 4.1. Network deployment

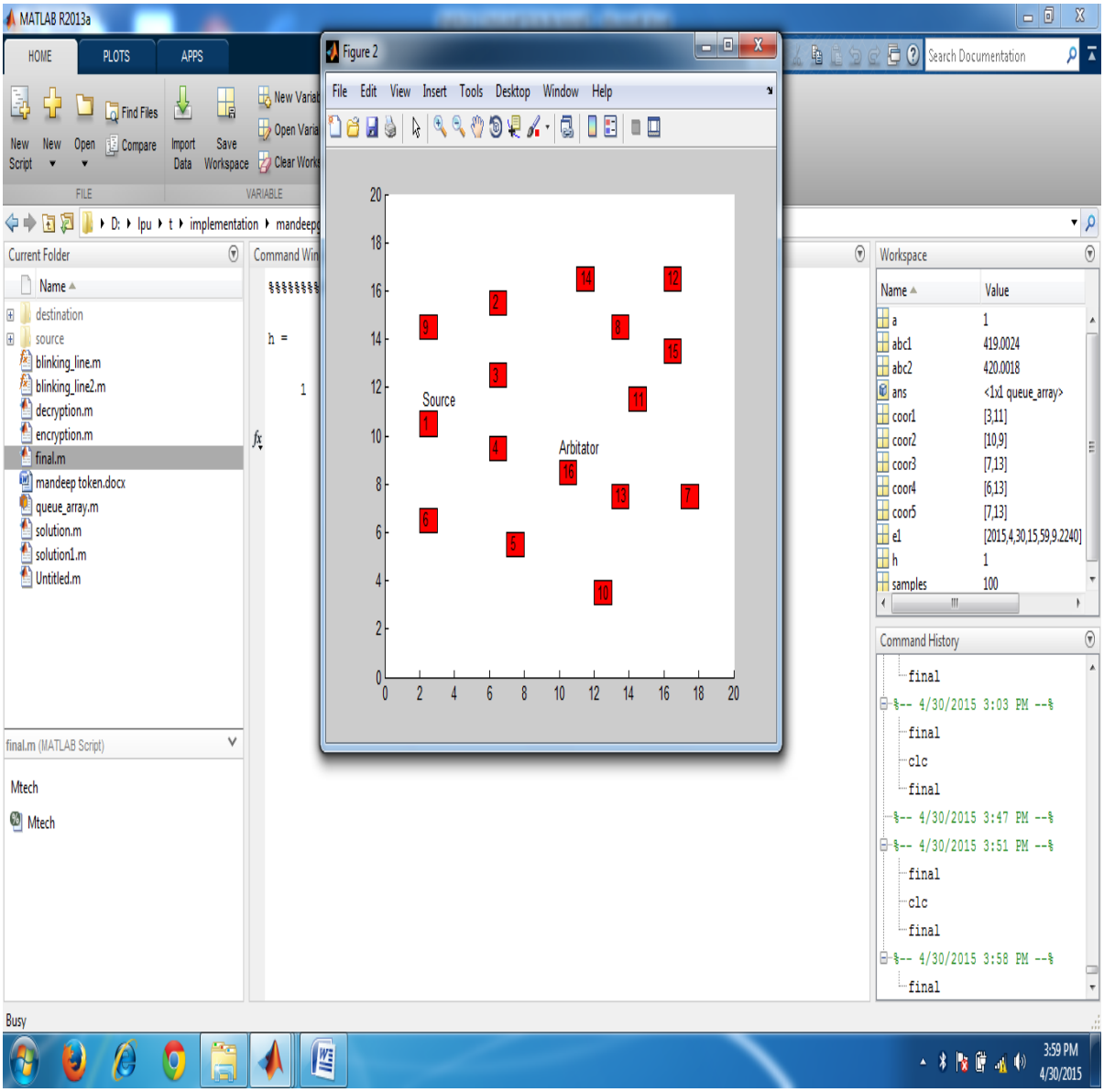

Fig 4.2 Arbitrator node

In figure 2, source node is node 1 and node 16 is common to both regions which will act as arbitrator.

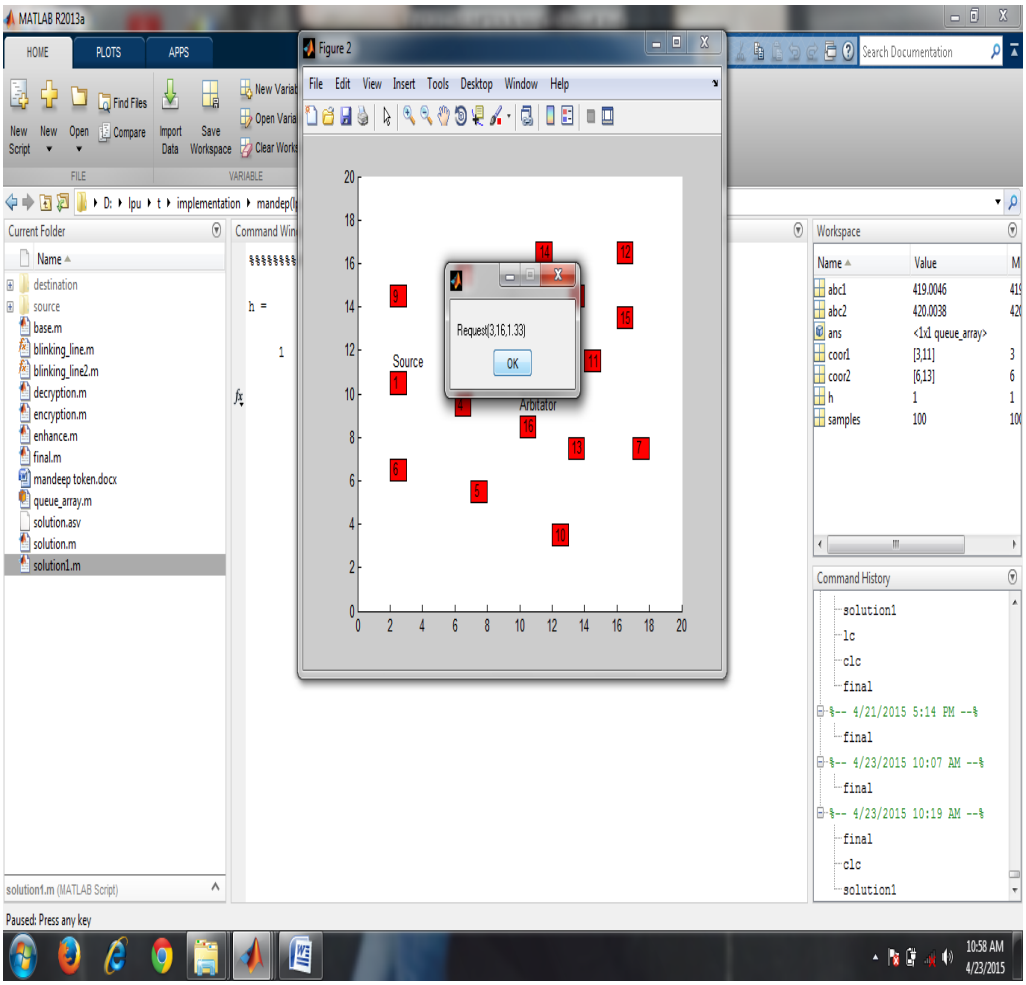

Fig 4.3 Network deployment with infoset

We have deployed 16, where node 1 is the source node in this figure , where permission based algorithm is used. Node number 3 will send a request to arbitrator node which is node number 16 at time stamp 1.33.

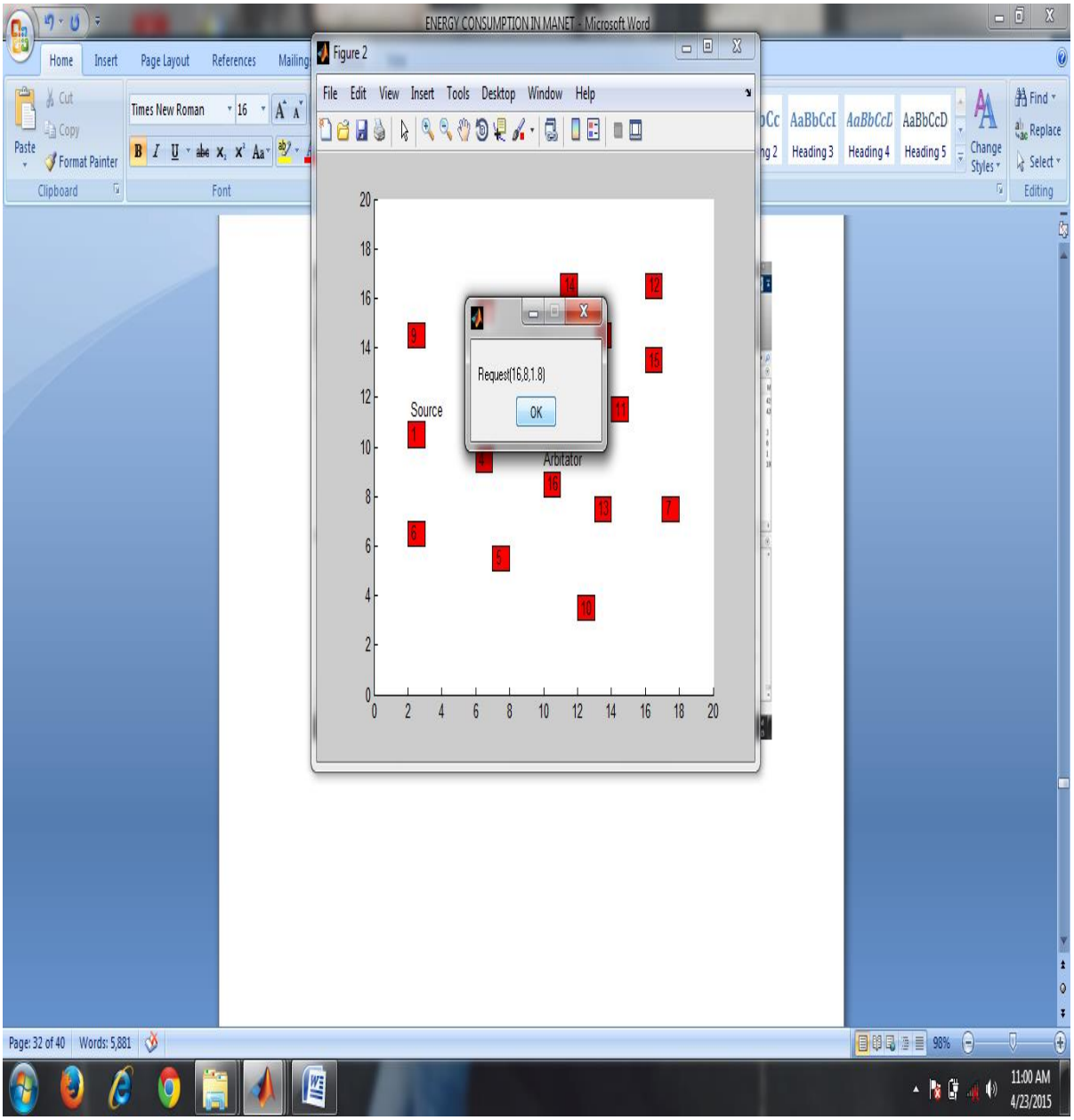

Fig 4.4 Arbitrator node sending request in infoset

Here arbitrator node 16 will send a request for resources to enter the critical section to its info set which includes node number 8, 11,13. At timestamp 1.8, node 16 will send request to node 8 as shown in figure.

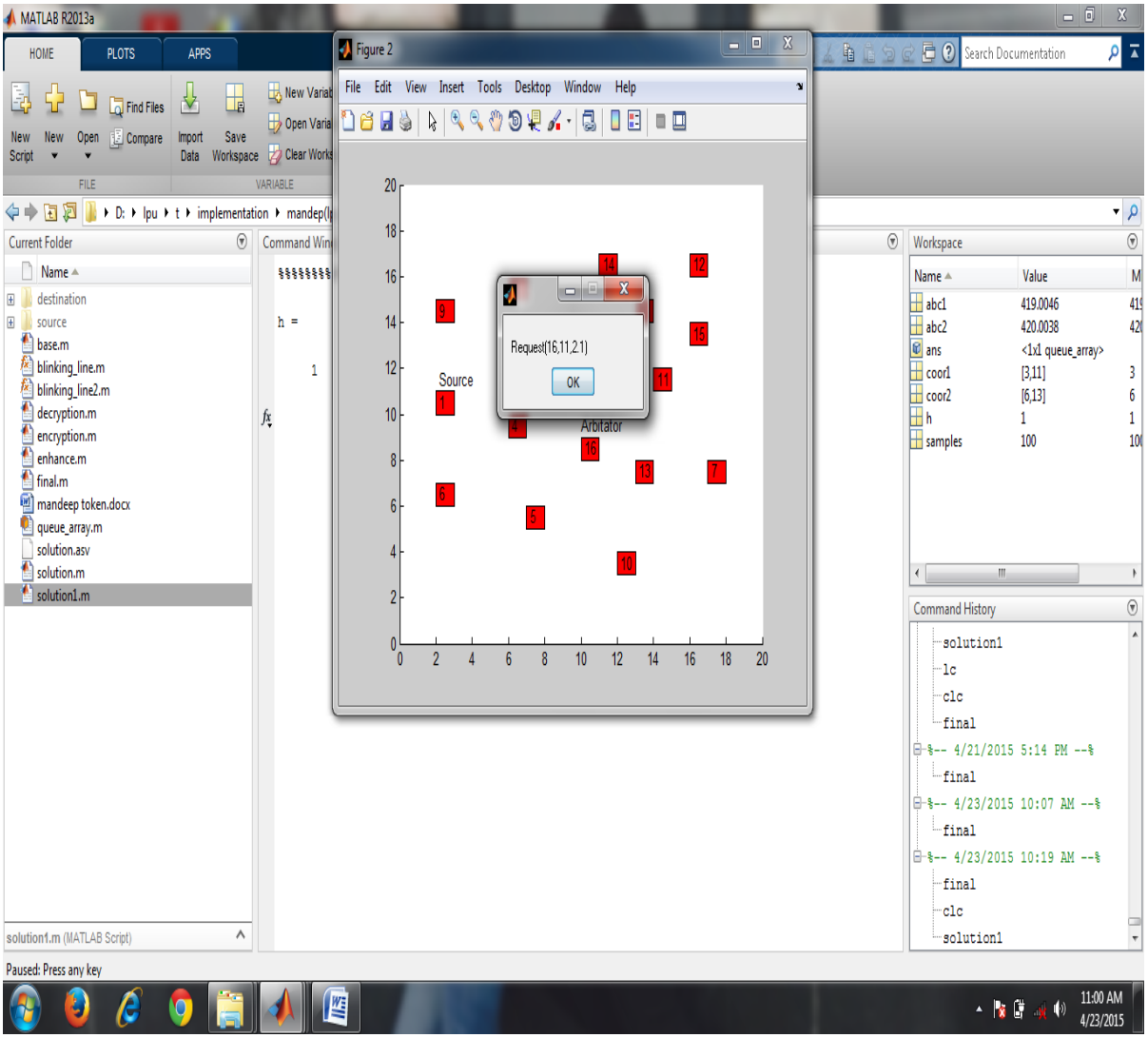

Fig 4.5 Arbitrator node Sending request in info set

Here arbitrator node 16 will send a request for resources to enter the critical section to its info set which includes node number 8, 11,13. At timestamp 1.8, node 16 will send request to node 11 as shown in figure**.**

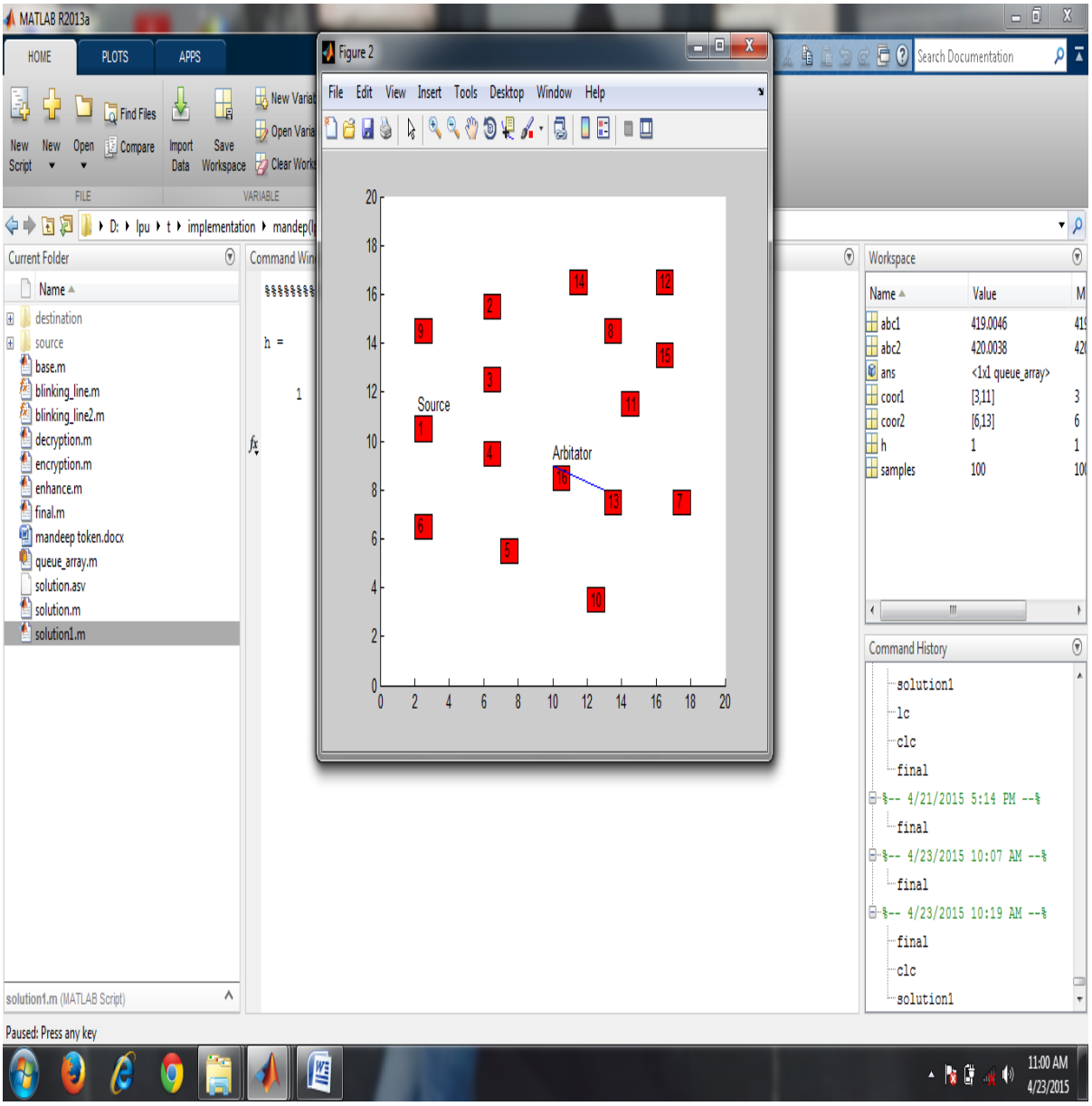

Fig 4.6 Arbitrator node requesting for resources

Here arbitrator node 16 will send a request for resources to enter the critical section to its info set which includes node number 8, 11, 13. At timestamp 1.8, node 16 will send request to node 13 as shown in figure.

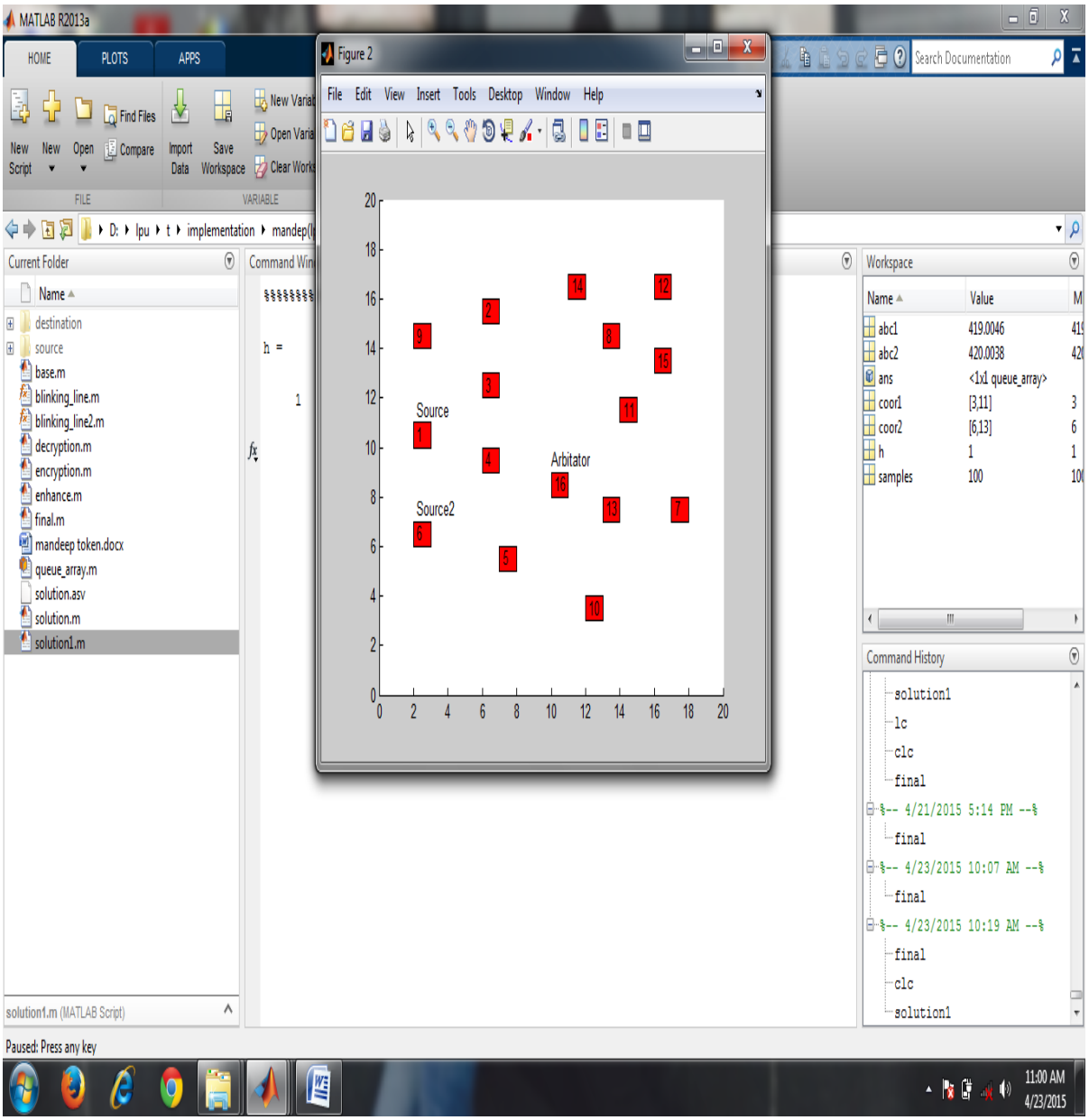

Fig 4.7 Requesting for resources

When source 1 has not received the reply message to enter the critical section,At the same time source 2 also sends request to arbitrator node to enter the critical section. So here the queue is maintained at arbitrator node which will grant the permission to nodes aa=ccording to the priority i.e according to timestamps.

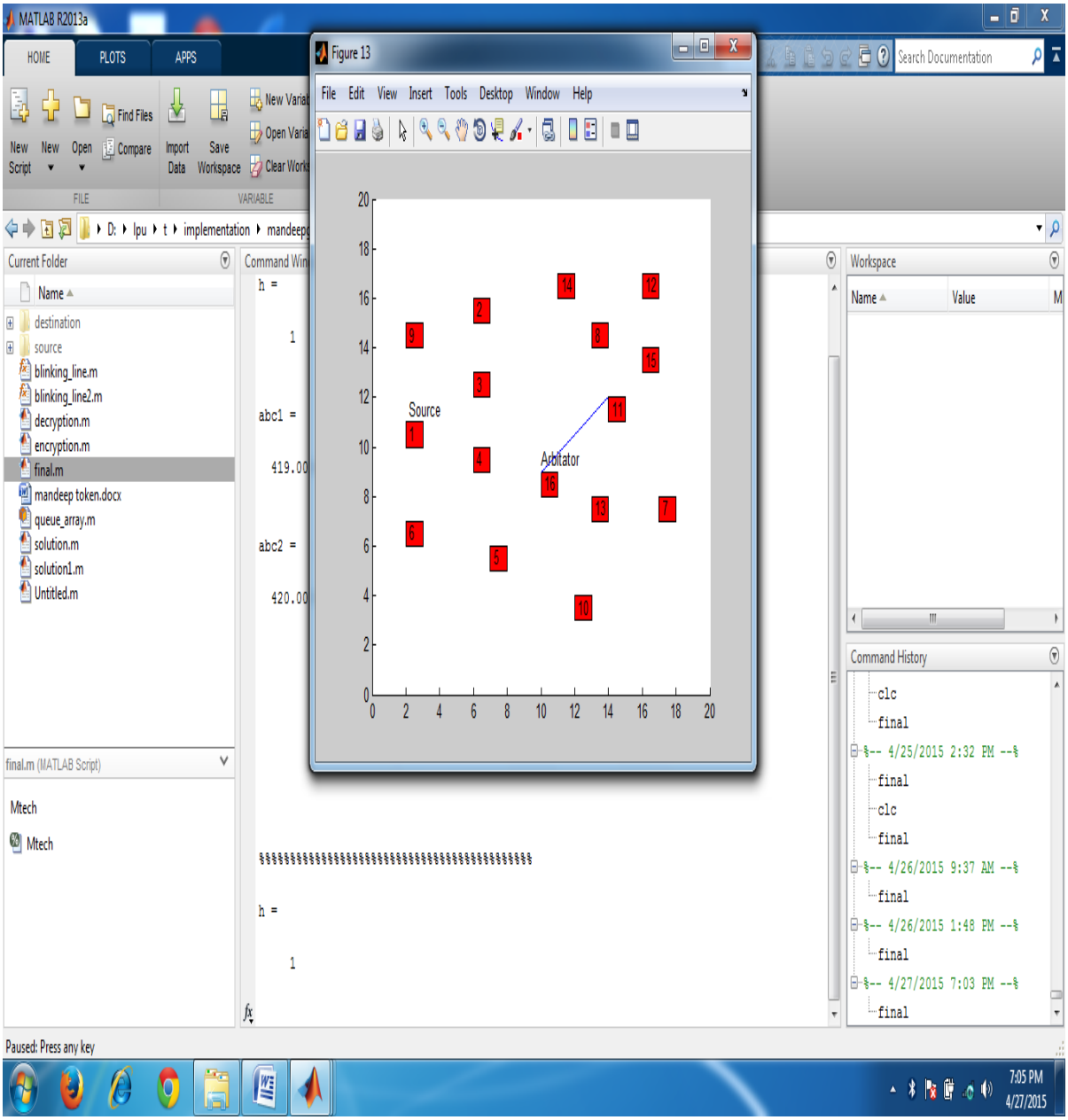

Fig 4.8 Requesting for resources

Here node 16 which is an arbitrator is sending request for resources to node 11 as shown in figure, so that node 1 can enter the critical section.

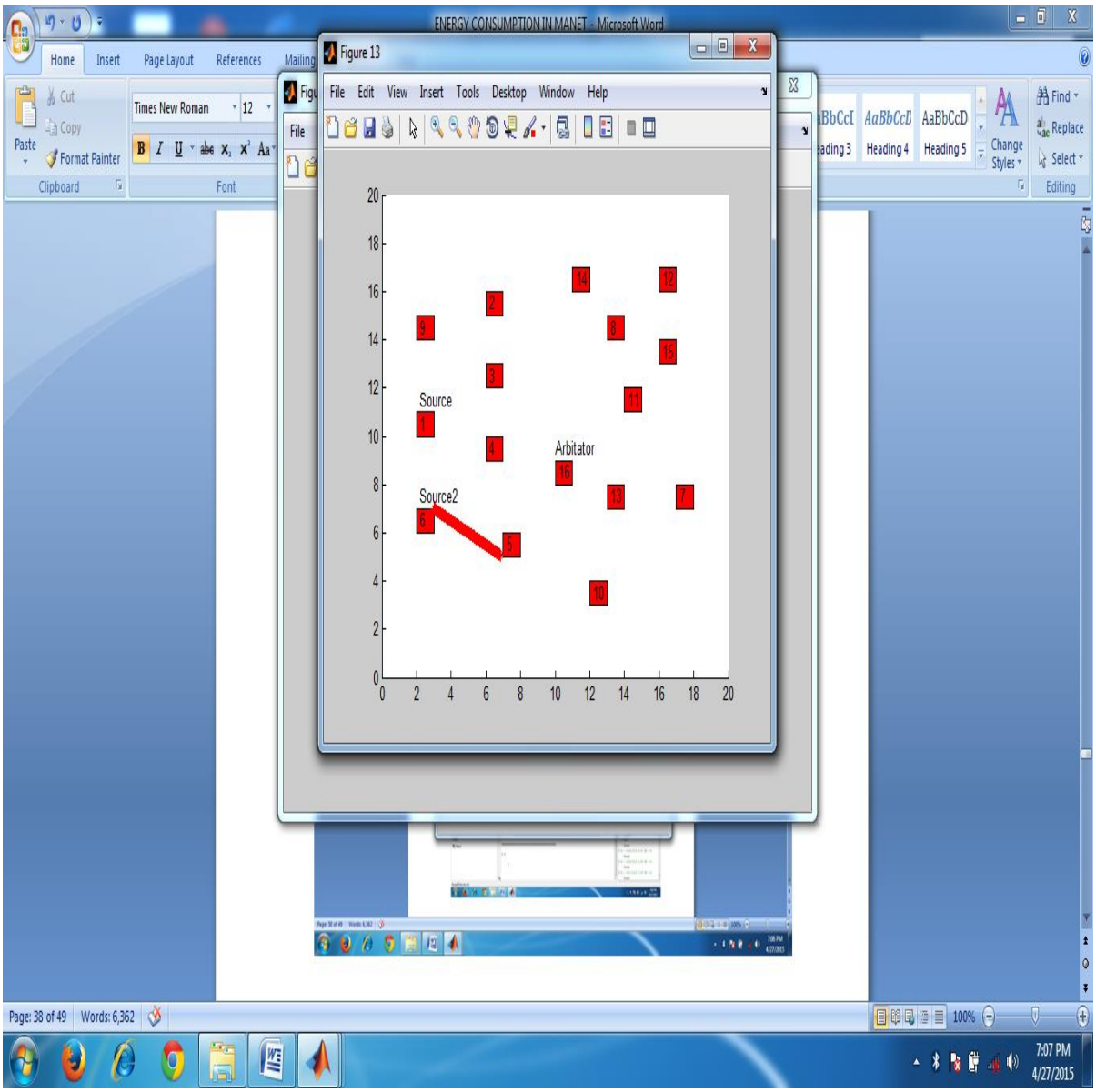

Fig 4.9 Transfer of data

After getting reply message from arbitrator node, source 2 node which is 6, will send data to node 5 as shown in figure.

Solution to problem:

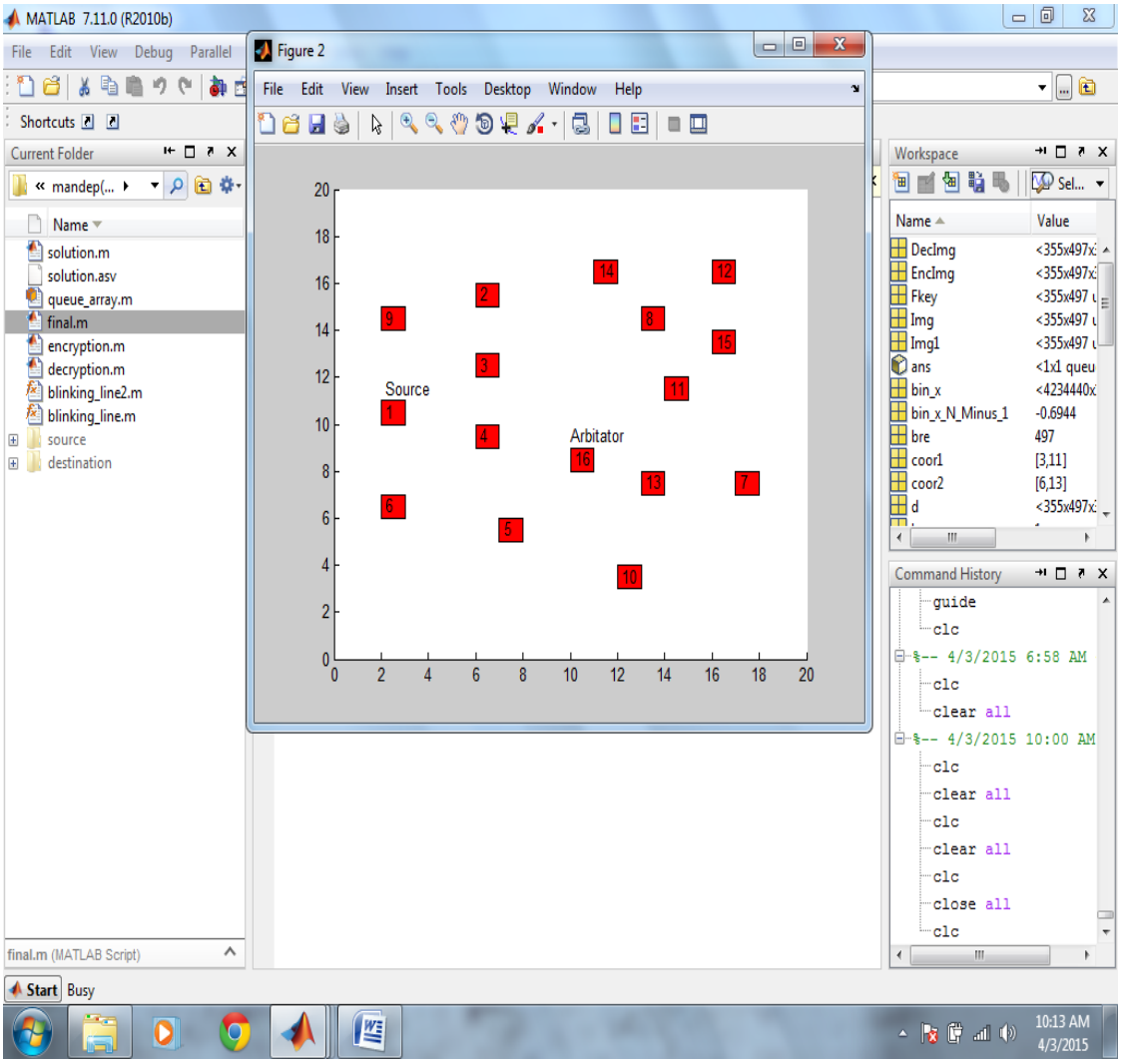

Fig 4.10: Network establishment

As shown in the figure 1, the network is deployed with the finite number of adhoc node. In the network source node and arbitrator node is defined. The arbitrator node will be responsible for resource allocation to the requesting node to enter into critical section.

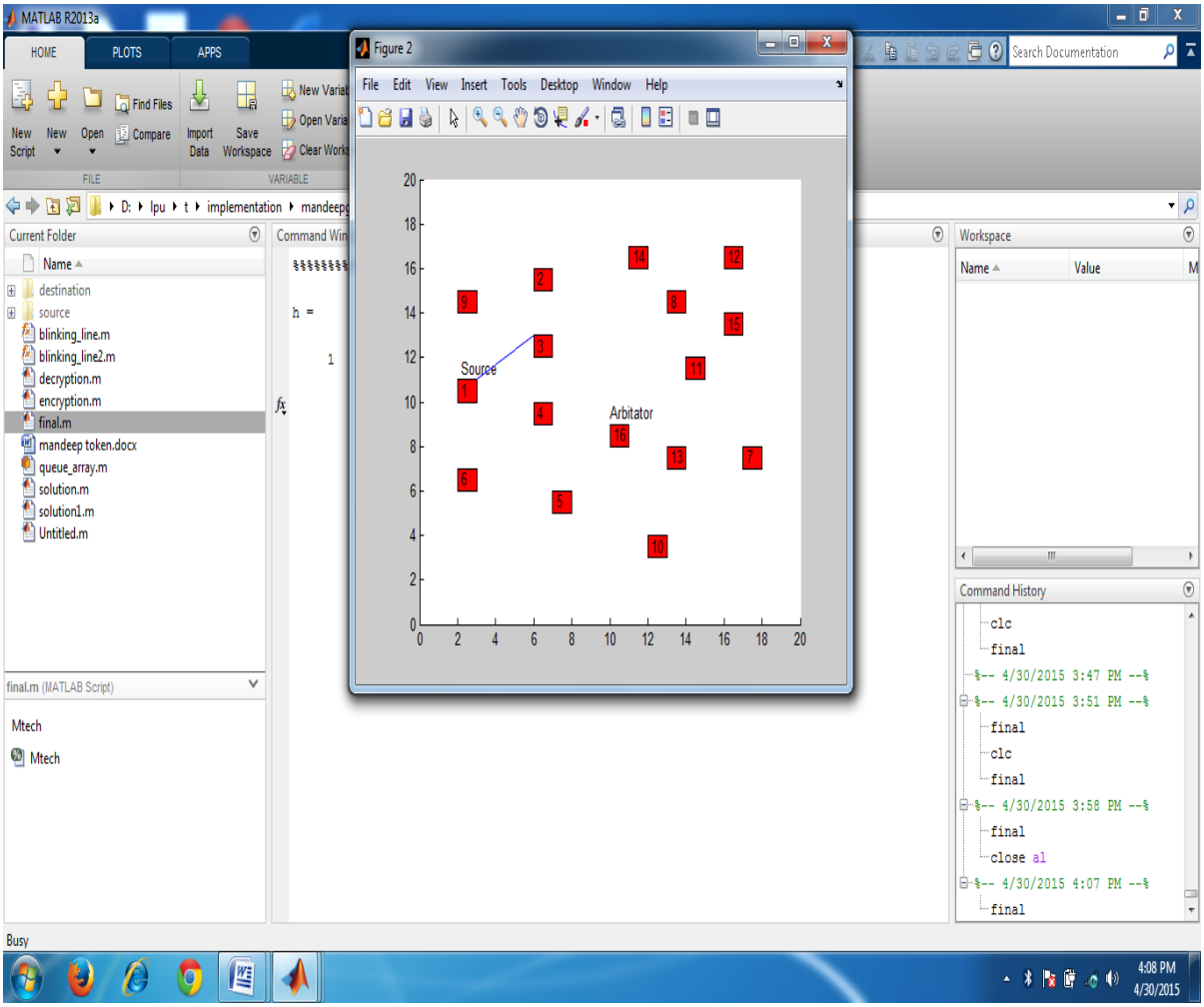

Fig 4.11 Requesting for resources

Node 1 is the source node which will send a request for resources to node 3 as shown in figure.

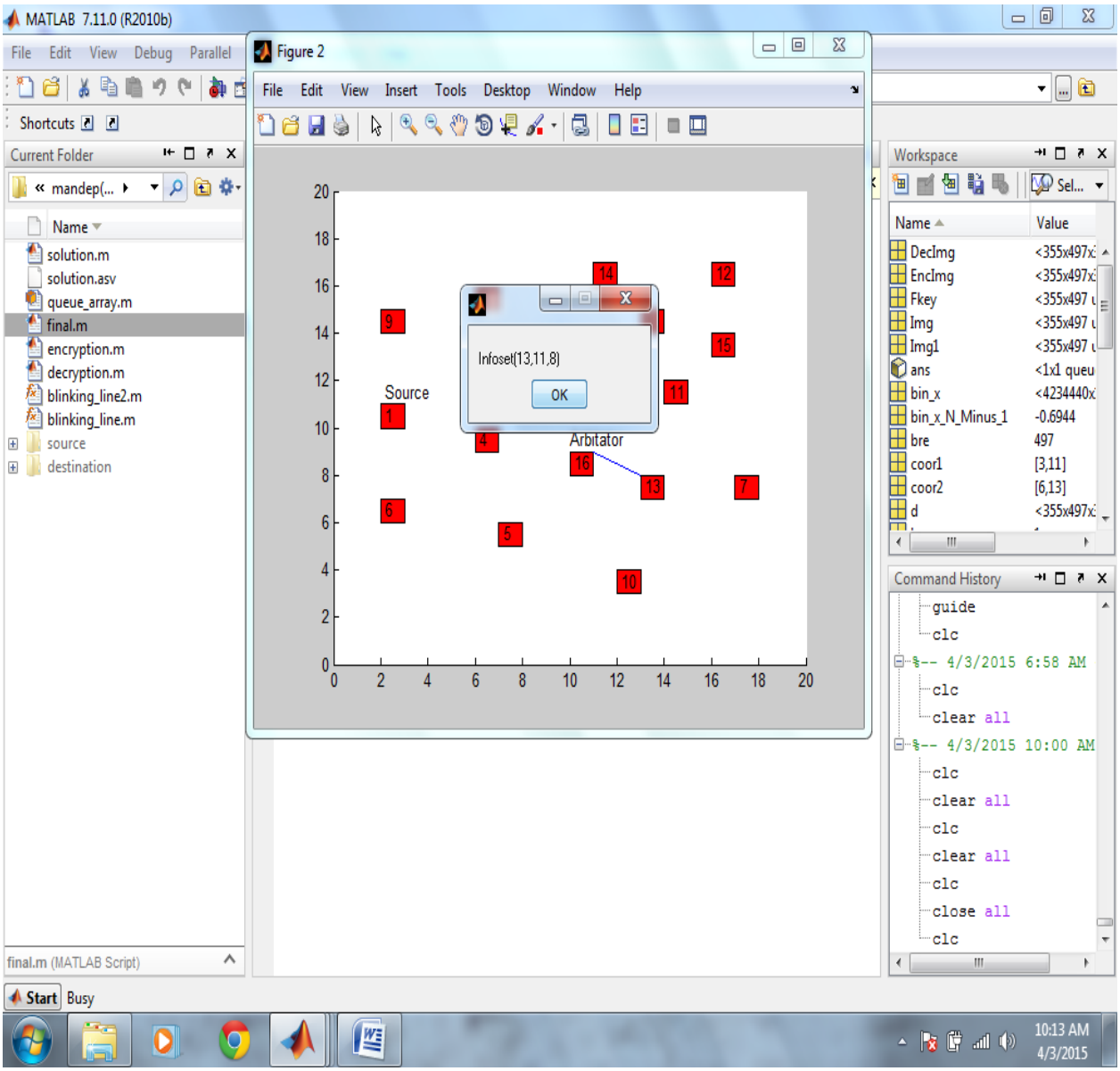

Fig 4.12 Checking for resources in infoset

As shown in the figure 2, the network is deployed with the finite number of adhoc node. In the network, source node and arbitrator node is defined. The arbitrator node will be responsible for resource allocation to the requesting node to enter into critical section. The source node sends request to arbitrator node to enter into critical section, arbitrator node check its info set and pass request to 13 number node .

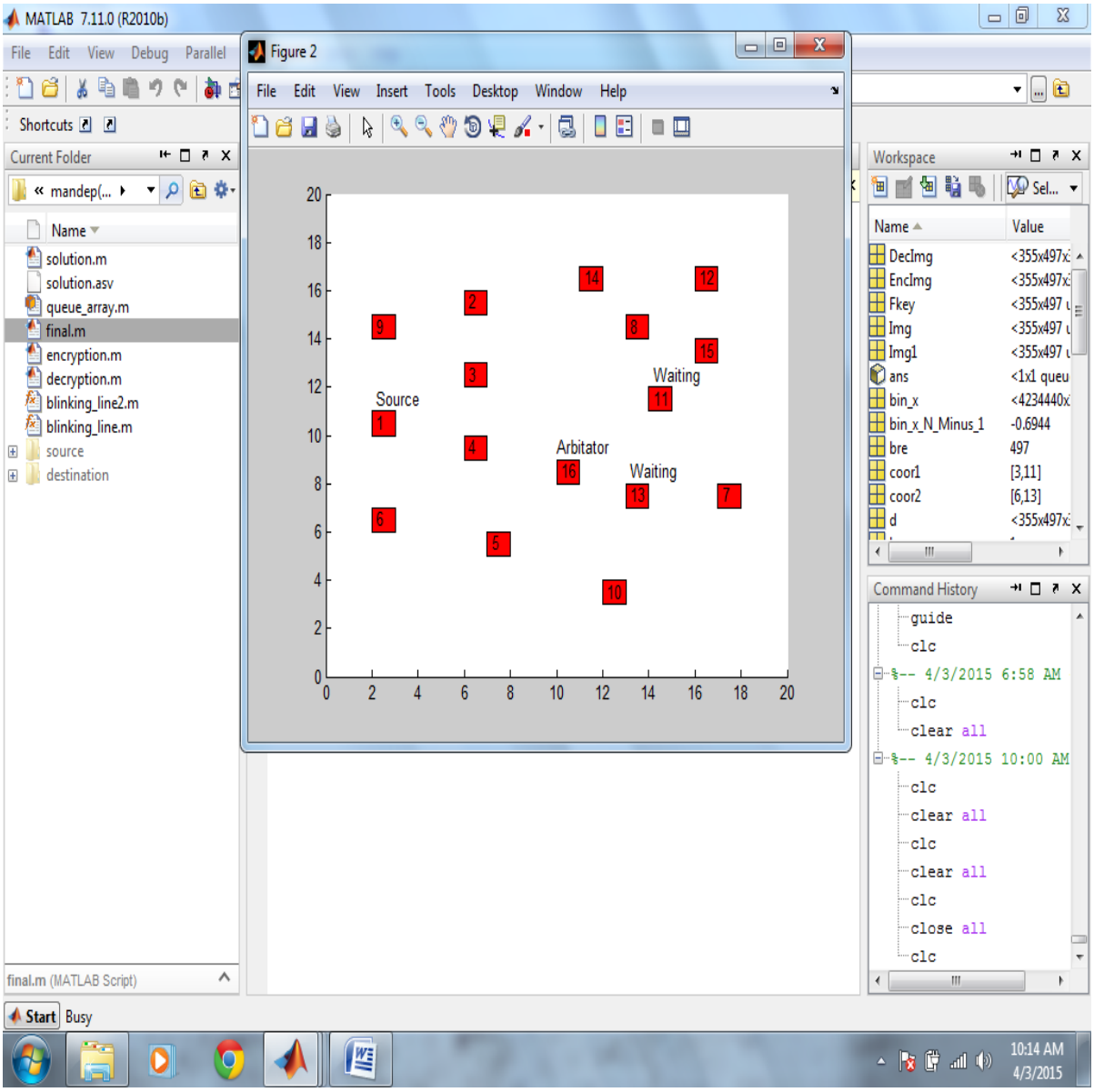

Fig 4.13 nodes waiting for resources

As shown in the figure 2, the 13 number node doesn't have resource and it will pass request to 11 number node, 11 number node will pass request to another node. The node 13 and 11 goes into waiting state and wait for the resources.

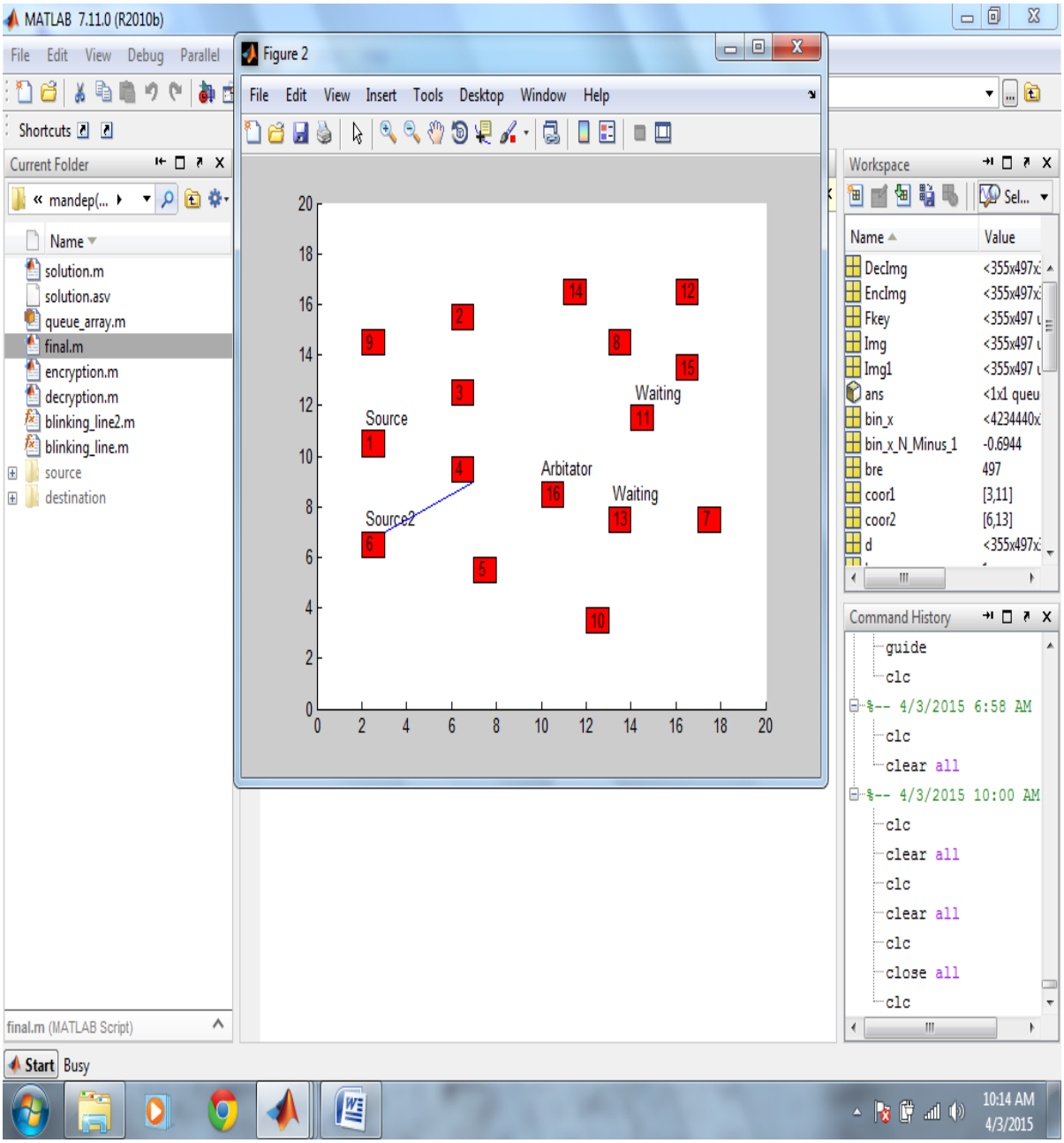

Fig 4.14 Source node Requesting for critical section

As shown in the figure 3, the network is deployed with the finite number of adhoc node. In the network source node and arbitrator node is defined. The arbitrator node will be responsible for resource allocation to the requesting node to enter into critical section. The source node request to arbitrator node to enter into critical section, arbitrator node check its info set and pass request to 13 number node . The 13 number node don't have resource and it

pass request to 11 number node, 11 number node pass request to another node. The node 13 and 11 goes into waiting state and wait for the resources . While nodes are in the waiting state, the source 2 request arbitrator to enter into critical section and its request will be put into queue.

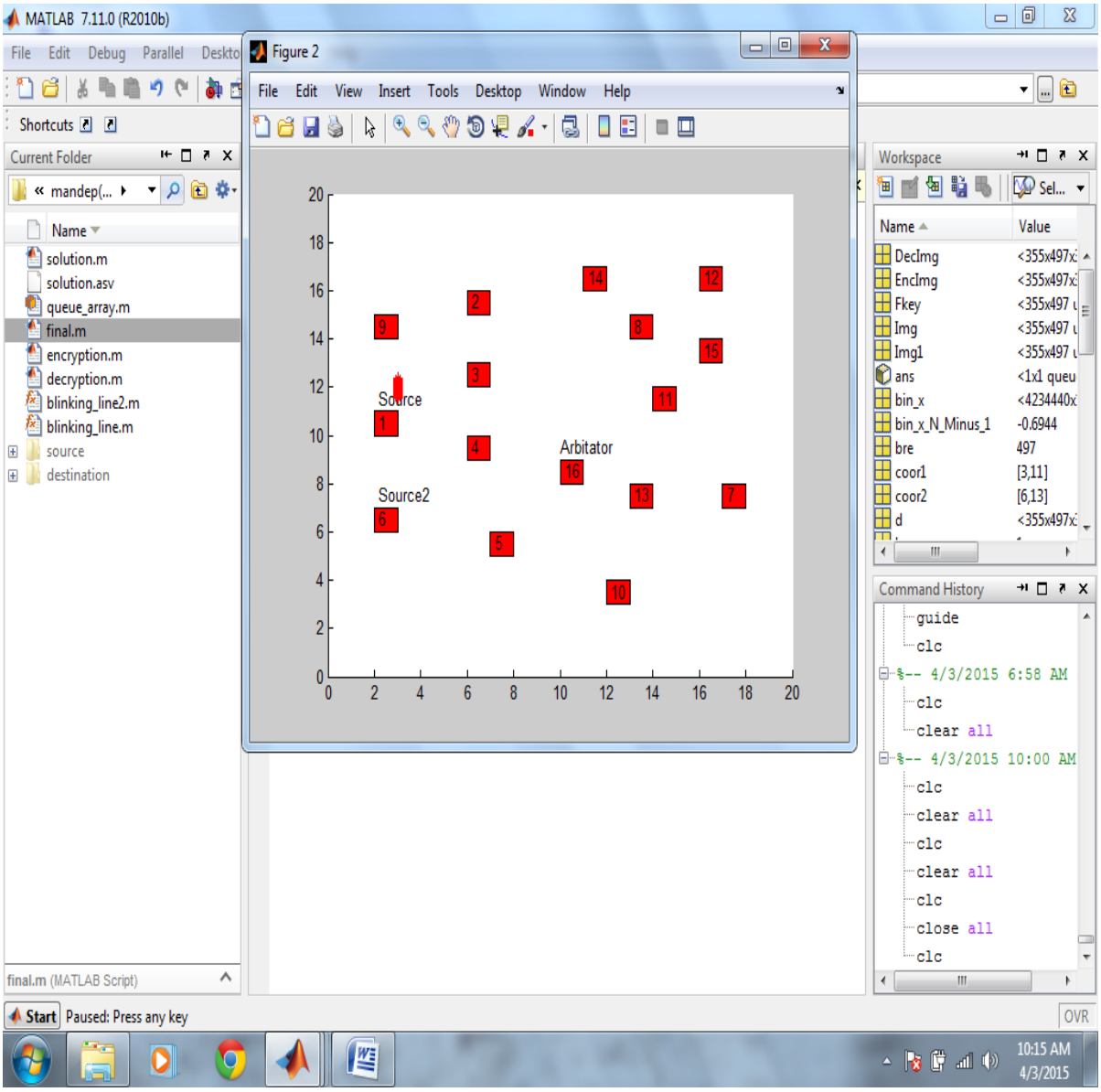

Fig 4. 15: Assigning critical section

As shown in the figure 4, the network is deployed with the finite number of adhoc node. In the network source node and arbitrator node is defined. The arbitrator node will be responsible for resource allocation to the requesting node to enter into critical section. The source node request to arbitrator node to enter into critical section, arbitrator node check its info set and pass request to 13 number node . The 13 number node don't have resource and it pass request to 11 number node, 11 number node pass request to another node. The node 13 and 11 goes into waiting state and wait for the resources. When node 13 and 11 gave the resource, it will provide resources to arbitrator and arbitrator will gave resource to source node. The source node after getting resource will send data to destination node.

Comparison:

We performed comparative evaluation of the proposed DME algorithm, i.e permission based and token based algorithms with the help of a simulator MATLAB. We have used the following three performance metrics for comparison. Response time, synchronization delay and message complexity.

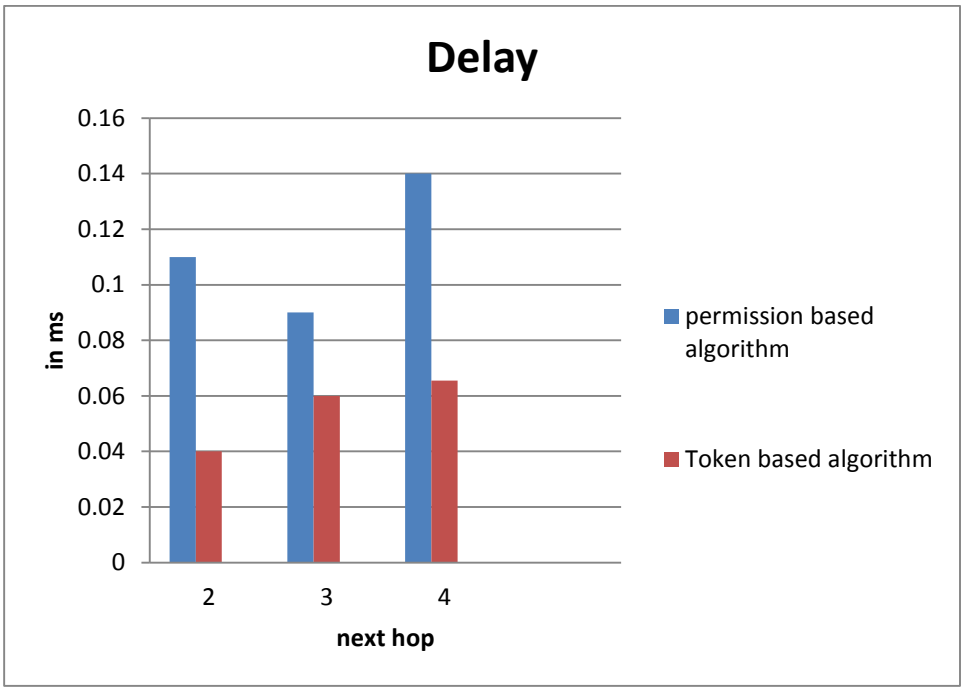

Fig 4.16 Delay vs. next hop

Fig shows the delay graph vs next hop taken by nodes in case of permission based and token based algorithm in mobile adhoc network.

So if we go through node 2 then there will be less delay i.e o.o4 ms in case of token based algorithm.

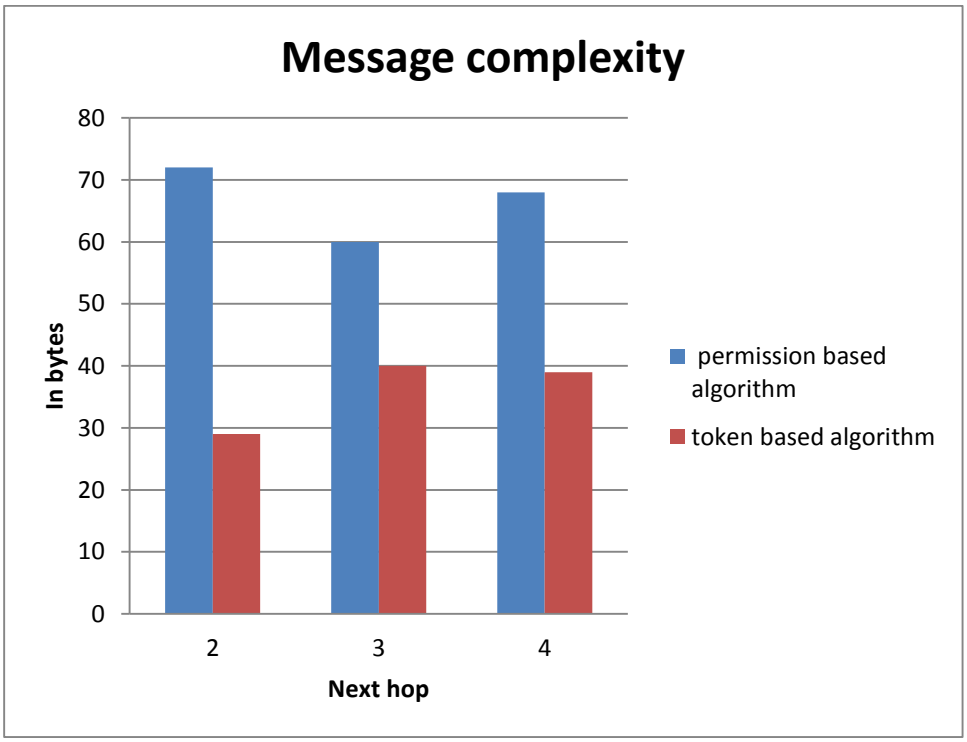

Fig 4.17 Message Complexity vs next hop

Here is the difference between outputs of both algorithms in case of message complexity. In token based algorithm message complexity is less as compared to permission based algorithm.

So if we choose path via node 2 then there will be less message complexity in case of token based algorithm as shown in figure.

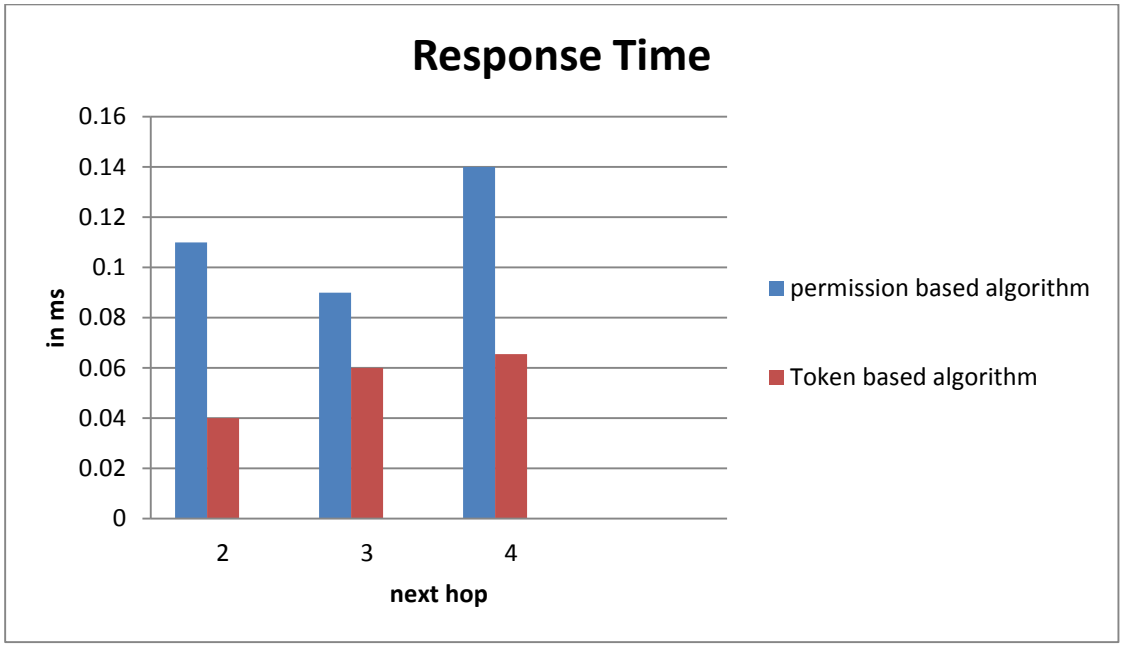

Fig. 4.18 Response Time vs next hop

Here is the difference between outputs of both algorithms in case of Response Time and next hop taken by nodes . In token based algorithm response time is less as compared to permission based algorithm.

So if we choose path via node 2 then there will be less Response time in case of token based algorithm as shown in figure

CHAPTER 5

CONCLUSION & FUTURE SCOPE

5.1 CONCLUSION

There are many distributed mutual exclusion algorithm for mobile adhoc network. even if the proposed algorithm is fully distributed, management of pending requests is centralized at the holder of the main tokens. The proposed algorithm achieves high concurrency, low response time and synchronization delay, reduce message complexity as compared to permission based algorithms**.**

5.2 FUTURE SCOPE

As we have worked on different methods i.e token based and permission base algorithms, for nodes to enter the critical section. In future we can work on queue that we used to store pending requests in our algorithm. In some cases FIFO is not that much efficient. So we will find different methods to assign priority to any node which is stored in a queue.

CHAPTER 6

REFERENCES

Anju Sharma, M. s. (2012). A Differential ealuation algorithm for routing optimization in manet. *International journal of computer science and network*.

Baisakh, N. k. (2012). " Energy Saving and Survival Routing Protocol For Mobile Ad-Hoc Network.

Bhatsangave. (2012). OADV routing algorithm for improving energy efficiency in manet. *International journal of computer applications*

DagdevirenOrhan "*A Merging Clustering Algorithm for Mobile Ad Hoc Network"*.

ErciyesKayyhan and DagdevirenOrhan(2009) "*A Distributed Mutual Exclusion Algorithm for MANET"*.

GuptaAbhilasha (2013)"*A Permission-based Clustering mutual exclusion algorithm for mobile ad hoc network".*

G.Ricart, A A. (jan.1981). An optimal algorithm for mutual exclusion in computer networks. *ACM*,9-1

Juan-carlos. (,). Evaluating the energy consumption reduction in manet by dynamically switching off the network interface.

Kadir, Jailani. (2011). Node Selection based on energy consumption in manet.

M. Singhal and D. Manivannan. (1997). A distributed mutual exclusion algorithm for mobile computing environments in information systems. 557-561.

M Benchaiba, A. B.-N. (n.d.). Distributed Mutual Exclusion Algorithm In Mobile Ad-Hoc Network:An Overview., (pp. 74-89).

Murali Parameswaran. (2013). Arbitration Based Reliable Distributed Mutual Exclusion for Mobile Adhoc Network. 380-387.

N, Y. B. (2009). enhancing the performance of manet by monitoring the energy consumption and use of mobile relay.

Nema. (2012). Energy Efficient Adaptive Routing Algorithm in manet with sleep mode. *International journal of advanced computer research*.

Shivshankar, s. g. (2013). Designing Energy Routing Protocol with Power Consumption Optimization in Manet". *IEEE*.

Talele Pratvina and Penurkar Milind (March 2013) . *A Token based Distributed Group Mutual Exclusion Algorithm with Quorums for MANE*T.

Weigang Wu, J. C. (2007). A Fault Tolerant Mutual Exclusion Algorithm For Mobile Adhoc Networks. *Science Direct*, 139-160.

Books

C.K.Toh "*Ad hoc Mobile Wireless Networks Protocols and Systems*".

My Publication

Paper published in "*Fourth International Conference On Wireless Networks And Embedded Systems WECON-2015*".

CHAPTER 7

APPENDIX

DSDV	*Destination-Sequenced Distance-Vector Routing*
OADV	Optimized Ad hoc On-Demand Distance Vector
AODV	Ad hoc On-Demand Distance Vector
DME	Distributed Mutual Exclusion
DSR	*Dynamic Source Routing*
MSS	Mobile Service Station
DE	Differential Evaluation
RA	Ricart-Agrawala
MUTEX	Mutual Exclusion
RTS	Request to Send
CTS	Clear to Send
MH	Mobile Host
CS	Critical Sections
BS	Base Stations