Medium Access Algorithm for Tactical Networks

by

Umar Ali
2010-NUST-MS PHD- ComE-27
MS-65 (CE)

Submitted to the Department of Computer Engineering in fulfillment of the requirements for the degree of

MASTER OF SCIENCE
in
COMPUTER ENGINEERING

Thesis Supervisor
Prof Dr Shoab Ahmad Khan

College of Electrical & Mechanical Engineering
National University of Sciences & Technology

2013

In the name of Allah, the most

Beneficent and the most Merciful

DECLARATION

I hereby declare that I have developed this thesis entirely on the basis of my personal efforts under the sincere guidance of my supervisor (Dr. Shoab Ahmad Khan). All the sources used in this thesis have been cited and the contents of this thesis have not been plagiarized. No portion of the work presented in this thesis has been submitted in support of any application for any other degree of qualification to this or any other university or institute of learning.

_____

Umar Ali

ACKNOWLEDGEMENTS

Innumerable words of praise and thanks to Allah, the Almighty, and the Creator of the universe for carving the path for me and always helping me out in the best possible way. Without His Will and Mercy, I would not have been able to accomplish this milestone. I am grateful to my parents for their immense love, moral support, encouragement and prayers throughout my academic career.

I am deeply beholden to my supervisor, Dr. Shoab Ahmad Khan, for his continuous guidance, inspiration, and patience. His ability of management and foresightedness taught me a lot of things which will be more helpful for me in my practical life.

I gratefully acknowledge the help and guidance provided by Guidance and Examination Committee members (Dr. Umer Munir, Dr. Saad Rehman and Dr. Asad Waqar Malik). Their valuable suggestions and comments were a great source to improve the research work presented in this thesis.

DEDICATION

To my parents and teachers

ABSTRACT

In this era the wireless networks are getting important everywhere as it doesn't require any physical medium or to lay down any medium like wires etc. it is more important in tactical/combat networks where it is impossible to lay down any other medium for the communication. The medium in the wireless network is air, which is a broadcast medium, means anyone can transmit a message in the form of signals at any time. This nature of the medium make it impossible to use without some management as if more than one node transmits at the same time the receiver of the signal will receive a garbage and no useful information. So this problem is to be handled by the system and the transmitting node must be capable of finding out when it should transmit and when it should not. This task is performed by the MAC (Medium Access Control) which is a sub-layer of the Data Link Layer. MAC layer basically deals with the access to the medium and based on the physical medium it uses different protocols to for the access of medium. For wireless networks especially of ad-hoc type collision is the main issue due to which the throughput decreases. Different protocols like 802.11, MACA and MACAW etc uses carrier sense to avoid collision but it also does not get rid of collisions. Other technique is time division multiple access (TDMA) in which every node has the information about when to transmit. This is made possible by dividing time into slots and a node is given access to the medium during the time slot which is assigned to it. This way the collision is avoided as every node has a pre-defined slot in which it can transmit. But this technique has a flaw of wastage of bandwidth when only few nodes are transmitting. Also there are special routing protocols on the network layer for the wireless ad-hoc networks so that the routes are easy to find and maintain. We have proposed a new algorithm to make maximum use of the bandwidth with avoiding the collision. We have proposed a new idea of merging two layers to avoid overheads of layers and merged network and data link layer into one and this new layer will now perform the task of two layers. We have made this design for the tactical networks that uses an AODV protocol for the routing and TDMA protocol for the medium access. Now instead of generating a message on the network layer and that message is then transmitted according to a new protocol on the MAC

layer now in a single layer a message is just mapped onto its respective time slot saving overhead. We have divided this task into two phases first is the finding of the route through the exchange of AODV control messages and then the actual communication. We have also made a node capable of sending more than one control messages at a time in a single time slot which saved a lot of time. Then we designed a slot allocation algorithm which made it possible to utilize the maximum bandwidth by finding out which slots are free and make used of them. The algorithm exploits the information exchanged in AODV control messages and in routing table and find out the free slots and allocates them to the active nodes. This way we have increased the throughput and also multiple slots are allocated to a node without any collision as the algorithm run on all the active nodes and every node has the information about which slot is allocated to it and which are to be left. The cross layer designs that exists are not exactly based on merging of layers rather they use the information of another layer to decide something and improve the communication but we have merged two layers into one and saved overhead. We have tested our algorithm on Matlab and it is very obvious from the results that sending multiple control messages in one slot saved a lot of frames and decreased call setup time and then the allocation algorithm proved to make maximum utilization of the bandwidth by allocating as much free slots to active nodes as possible.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.1. Motivation

Wireless networks share a broadcast medium (Air) and because of this when two nodes in the range transmit at the same time causes a collision. So in order to avoid the collision different techniques are used in MAC layer to inform the nodes about whether the space is free or currently occupied by some other transmitting node. There might be different techniques to ensure this e.g. 802.11 uses DCF (Distributed Coordination Function) [1].

It sounds good when we talk about mobile system but if the network is not systematically designed and is Ad-Hoc (like tactical/combat networks), and we have less bandwidth and no up-channel that we can setup slots using any control signals. So we are left with two choices, either we can allocate the slot statically to the nodes or we can fix the slot usage (like voice, data etc) and open them for contention. In both cases the network bandwidth is not fully utilized e.g. in the first case if only two nodes are active then the utilization of bandwidth is 2 slots out of n slots in one frame while in the second case slots are open for contention so every time a node has to use a slot it has to contend for it.

Now in order to overcome this problem in a rapidly changing Ad-Hoc networks like tactical networks we have worked on different protocols and studied them to see how if they can be modified to make the bandwidth utilization in tactical network better.

So first we worked on different aspects of routing protocols to be used in our technique and finally selected AODV and modified its messages to make it more utilizable.

Then we merged the two layers (the internet and link layer), that is instead of having two separate layers we have only one layer that is managing the task of both the layers. It might seem here that we are overloading the layer with the task of two layers but the basic theme behind doing this is that the type of packet in internet layer decides the slot and frame in which it will be mapped so instead of two layers we have merged them into one layer.

Then we divided the link layer MAC (Medium Access Control) TDMA frames into two categories:

1. Control Frames: for transmission of AODV control packets
2. Data Frames: for transmission of voice and other type of data

Based on modified AODV control packets the whole communication process is divided into two parts i.e. the nodes exchange the control packets first and based on these control packets all the active nodes in the topology have information about the communicating nodes. So based on this information we have designed an algorithm using which all the active nodes can find the slot(s) that it will use and when every node in the topology has the information about which slot is being used by which node then we get two advantages out of it

1. There will be no collision
2. Each communicating node will occupy more than one slot in a frame so there will be maximum slot utilization

1.2. Background

Currently no research has been conducted specifically related to the idea we have chosen rather people have worked on this using different aspect i.e. not exactly merging the layers but rather related it to the quality aspects.

We have chosen few papers to explain the work that other people have done.

According to [2] Mobile ad hoc networks (MANET) are becoming an integral part of the ubiquitous computing and they have provided infrastructure for the video applications and multimedia-on-demand, and Quality of Service (QoS) is to be considered to provide high success rate for multimedia data. The routes in the internet layers are maintained with a QoS factor to set the priority of data that is generated by application that require high success rate. The middleware layer between application and internet layer keep data priority information which is used by the internet layer providing cross layer design to increase success rate. Similarly middleware layer uses information to be updated about nodes location and its movement.

In [3] the authors claim to present a cross layer design which provides a routing algorithm that uses information from internet, link and physical layer. They have used the Ad hoc on-demand distance vector (AODV) and used information from physical layer signal strength and MAC layer information to keep up to date routes and designed a cross layer protocol.

In [4] the power of the node is used to make the design cross layer i.e. the low power nodes are able to receive from high power nodes but not vice versa so based on information from physical layer, the routing layer avoids the asymmetric links and discovers routes which are symmetric to forward data to the nodes which are low powered. So the basic theme is to avoid the asymmetric link and discover routes to such nodes which are symmetric and this is done using the information of power from the physical layer.

In [5] author presented a CLAODV (Cross Layer Ad-hoc on-demand Distance Vector), a reactive routing protocol. It is based on classic AODV routing protocol and utilized useful information of MAC sub-layer in routing and also improved timed Hello messages. It affords prompt and accurate local topology information and reduces protocol overhead.

1.3. Methodology

We have used different resources including IEEE, Springer.

Keywords: Cross-layer, Merged-Layers, Ad-Hoc, Slot Allocation, AODV, Tactical Networks

Using these keywords we have searched for a technique which has used a cross-layer or merged-layer design i.e. a design in which the internet and link layers are merged into a single layer but no such idea or research existed.

Then we searched different slot allocation algorithms to find out whether any of them is using the information in the routing table to allocate the slot but no such idea was found on any of the reputed journals.

Then we studied the RFC of the AODV (Ad-Hoc On-Demand Distance Vector) routing protocol [6] and studied its packet format and worked on modifying them to used in our merged-layer design.

1.4. Thesis Outlines

We have studied the techniques already being used in tactical networks [1] for slot allocation in a combat field network where the nodes are moving very fast and the topology of the network is changing rapidly and in [1] the technique that is being used is that two slots are fixed for the voice data and 2 slots out of the remaining 8 slots can be preempted if there are two simultaneous voice conversations going on and remaining slots can be used for contentions to be allocated.

So in this thesis we have merged the internet and link layer into one layer, then we modified the AODV control packets to get maximum utilization out of it keeping in view the bandwidth constraints and then designed a new algorithm to allocate slots to nodes based on the control information exchanged in AODV control packets

1.5. Summary

There are different techniques available on cross layer design but don't have a clear idea of merging layers and are based on previous techniques used in link layer design. AODV is a popular reactive routing protocol for ad-hoc networks with very light control packets and these packets can be modified to get maximum information to be exchanged in less number of control packets. There is no slot allocation algorithm that is based on information that is from internet layer to make the design truly cross layer. So a new technique with cross layer design using modified AODV control messages and a slot allocation algorithm based on these control packets can be proposed.

CHAPTER 2: BACKGROUND AND LITERATURE REVIEW

In this chapter we will describe in detail the concepts that are related to our work which include Ad hoc On-Demand Distance Vector (AODV) routing protocol, Time Division Multiple Access (TDMA) technique in Medium Access Layer, existing cross layer designs, existing slot allocation algorithms.

2.1. Medium Access Control

In reference to the OSI model of computer networking, medium access control (MAC) is a sub-layer of the data link layer, which is the second layer of the model. The basic aim of this layer is to provide a protocol which will provide several nodes an access channel mechanism that will enable them to communicate within a multiple access network with a shared medium. The hardware implementing the MAC is referred to medium access controller.

Data link layer actually has two sub-layers, medium access control (MAC) and logical link control (LLC). The point in dividing the link layer into two parts is because this is the point where the actual hardware comes into play in communication. The MAC sub-layer actually act as an interface between logical link layer (LLC) and physical layer. A MAC layer emulates a full-duplex logical communication channel in a multi-point network.

2.1.1 Functions of MAC

According to IEEE 802.3 standard the required functions of a MAC are

- Receive/transmit normal frames
- Half-duplex retransmission and back-off functions
- Append/check FCS (frame check sequence)
- Inter-frame gap enforcement
- Discard malformed frames

- Append(tx)/remove(rx) preamble, SFD, and padding
- Half-duplex compatibility: append(tx)/remove(rx) MAC address

2.1.2 Addressing Mechanism

In an IP-Ethernet network the local network address is called MAC address because it is part of the MAC layer in Ethernet implementations. The addressing mechanism that is followed in MAC layer is called physical address or MAC address.

A MAC address is number which is unique. A MAC assigned to a particular network interface (at the time of manufacture), that interface should be uniquely identified with that MAC address all around the world. In this way it is guaranteed that the network all the devices in a network will have a unique MAC address. In this way it is made possible to deliver packets to destination to devices in a sub-network i.e. hosts connected by repeaters, bridges, hubs and switches and not IP routers.

An example of network using MAC is perhaps an Ethernet network, extended by a wireless local area network (WLAN) access points and adapters, as they also have a same 48-bit MAC address as Ethernet.

2.1.3 Channel Access Control Mechanism

MAC provides channel access control mechanisms which are known as multiple access protocols. With this several stations can share same physical medium. Examples of a shared medium include bus networks, ring networks, wireless networks, hub networks and half-duplex point-to-point links. A multiple access protocol tend to detect or avoid data packet collisions if contention based channel access method is used, or reserve resources to establish a logical channel if a circuit switched channel access technique is used. Physical layer multiplex scheme affect the type of multiple access technique.

A commonly used multiple access protocol is CSMA/CD which is based on contention and is used in Ethernet Networks. The mechanism is utilized in a network collision domain e.g. in bus networks or hub based star topology network. An Ethernet network

can be divided into several collision domains, interconnected by hubs, repeaters, bridges and switches.

2.1.4 Common Multiple Access Schemes

Multiple access protocols which are commonly used can be divided into two categories, for wired Ethernet networks and for packet radio wireless networks

2.1.4.1 Multiple Access Protocols for Wired networks

The common multiple access protocols for wired networks are:

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
- Token bus (IEEE 802.4)
- Token ring (IEEE 802.5)
- Token passing

2.1.4.2 Multiple Access Protocols for Wireless networks

The common Multiple access schemes used in packet radio wireless networks are:

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- Slotted ALOHA
- Dynamic ALOHA
- Reservation ALOHA (R-ALOHA)
- Mobile Slotted ALOHA (MS-ALOHA)
- CDMA
- TDMA
- OFDMA

2.1.5 Design Issues for MAC in Ad hoc Wireless Networks

As we have already seen that MAC is used to provide a mechanism that will tell the node whether it can use the channel or not. Then we have listed down some mechanisms that are commonly used in wired and wireless networks.

Now as we are going to work on the ad hoc wireless network so first we will mention some of the issues that are to be considered when designing a MAC protocol for wireless ad hoc network. Firs we will list down the issues and then we will explain briefly each one of them.

Some of the issues that are to be considered are

- Bandwidth efficiency
- Real-time traffic support
- Synchronization
- Shared Broadcast medium
- Lack of central Coordination

Now we will briefly explain each of the issue.

2.1.5.1 Bandwidth efficiency

In a [7] wireless ad hoc network there is no centralized entity controlling the nodes; everyone is willing to forward packets to the destination and routes are find dynamically based on the connectivity of network. Ad hoc networks were originally designed for the military applications but due to advancement in transmission technologies and device portability, there was a growing interest in deploying wireless ad hoc networks in commercial applications like virtual classrooms, mobile data exchanges and home networking where each node is competing to acquire the shared wireless medium, so a mechanism is needed that should provide an effective and efficient bandwidth allocation to allow fair sharing of the system bandwidth.

The dynamic and decentralized nature of the ad hoc network means that the information must be passed from node to node about the network topology. In a dynamic network a distributed bandwidth allocation algorithm is usually considered over centralized one. The three criterions for the distributed allocation algorithm are the amount of data passed, convergence time and fair allocation of bandwidth.

Other than fair allocation of bandwidth the other issue is the wastage of bandwidth e.g. in mobile networks when the control packets are being exchanged the data channel is free and while the nodes are using data channel the control channel is being wasted.

Currently the most common and widely used MAC protocol in wireless ad hoc networks is IEEE 802.11 which is based on random access and lacks the ability of fair bandwidth allocation

2.1.5.2 Real-time Traffic Support

As it is already stated that ad hoc MAC protocol has an issue of bandwidth wastage so it is inherent that it is not suitable for the real time traffic as the real time traffic needs a reliable network and where the data is to be forward on top priority otherwise e.g. if there is a voice call going and the broadcast medium is being unfairly used among nodes then the node which has a real time data to pass might not be able to acquire the channel and thus communication will fail. So a MAC protocol should provide some mechanism to deal with the real time support.

2.1.5.3 Synchronization

Time synchronization should be taken into account when designing a MAC protocol for ad hoc wireless network. A time synchronization mechanism is mandatory for TDMA systems which are based on slots for reception and transmission. Synchronization involves using of scarce resources like bandwidth and battery power.

2.1.5.4 Shared Broadcast Medium

One of the major design issues in MAC protocol for the ad hoc network is the shared broadcast medium. A MAC protocol must provide a mechanism to avoid collisions as all the nodes in the network will try to acquire the channel so MAC protocol should define a policy about how and when a node will get access to the shared medium.

2.1.5.5 Exposed Node

Exposed node problem is when a node as shown in Figure 1 is in the range of the sender but is not in the range of receiver. This stops the node from sending data while it can send data without any collisions on the receiver node. To increase bandwidth efficiency a MAC protocol should enable an exposed terminal to send data in a controlled fashion without causing collisions in the on-going data transmission.

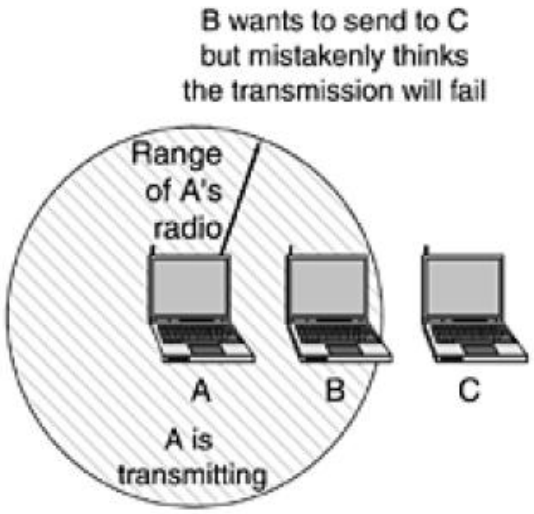

Figure 1: Exposed node problem

2.1.5.6 Hidden Node

A hidden node as shown in Figure 2 is the one which is in the range of receiver but not in the range of sender. So while the receiver is receiving data from the sender a hidden node can send data as it is unaware of the data transmission and can cause collision and can significantly reduce the throughput. So a MAC protocol should deal with the issue of the hidden nodes.

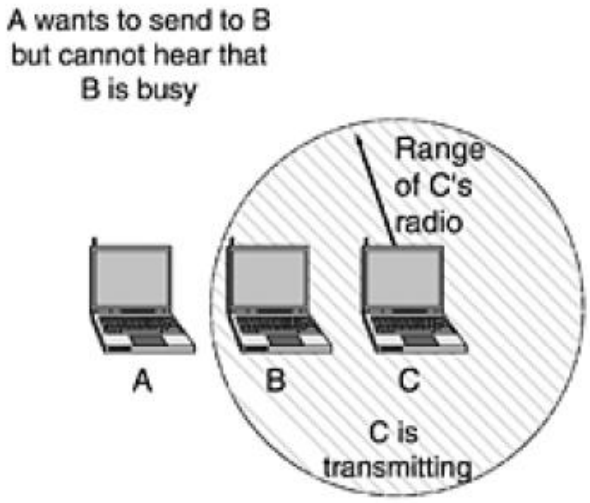

Figure 2: Hidden node problem

2.1.5.7 Lack of coordination

An ad hoc wireless network is distributed and lacks centralized entity so MAC protocol should provide a mechanism to make a node self sufficient to deal with issues in the absence of a centralized controlling entity.

2.1.6 Classification of MAC for ad hoc Networks

MAC protocol for ad hoc networks can be classified into the following categories:

- Contention-based protocols without reservation/scheduling
- Contention-based protocols with reservation mechanisms
- Contention-based protocols with scheduling mechanisms
- Protocols that do not fall to any of these categories

A flow chart for the [8] classification of MAC protocols for ad hoc networks is shown below:

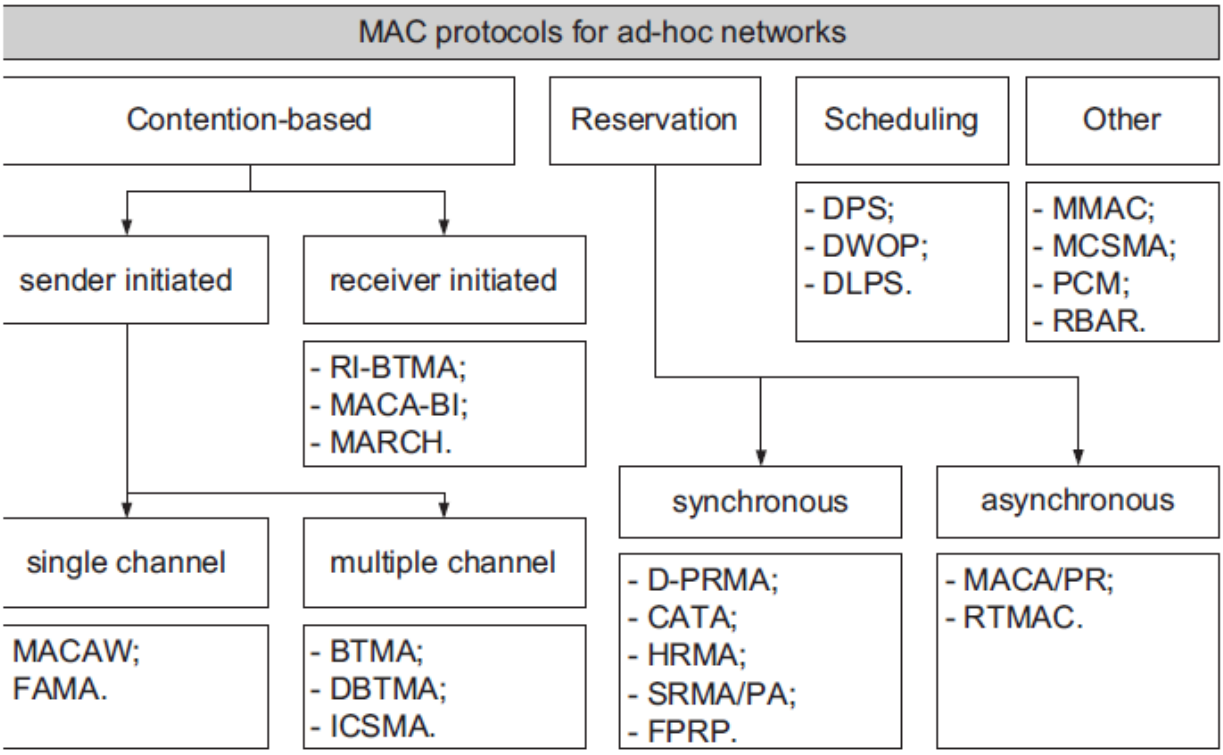

Figure 3: Flow chart of classification of MAC Protocols

Now we will discuss each category briefly

2.1.6.1 Contention-based Protocols without reservation/scheduling

The first category in MAC protocols for ad hoc networks is contention-based with no reservation or scheduling. The basic theme of protocols in this category is to content for the resource and winning node will acquire the channel.

The protocols which fall in this category are MACA, MACAW, BTMA, MACA-BI and MARCH. Now we will explain briefly some of these protocols.

Multiple Access with Collision Avoidance (MACA):

MACA is a slotted MAC protocol used in wireless LAN data transmissions; it is designed to avoid the collisions caused by hidden nodes and to simplify the exposed node problems.

In MACA a wireless node announces before it send a data frame so that other nodes can keep silence during that period. When a node want to transmit data it sends a Request-To-Send (RTS) presenting length of data frame to send. The receiver reply with Clear-To-Send (CTS) frame with the same length of data frame. While RTS is sent, the sending node keeps silent to avoid collision with CTS.

Wireless transmission may still occur in MACA and this limitation was removed in MACA for wireless (MACAW)

MACA for wireless (MACAW):

MACAW is a slotted MAC protocol widely used in ad hoc wireless networks and is also a foundation for many other MAC protocols for wireless sensor networks. The RTS/CTS mechanism in 802.11 is also adopted from this protocol. This protocol removed the flaws in traditional MACA protocol by introducing acknowledgements. The receiver acknowledges each data frame when it is received without error.

MACA for wireless (MACAW):

MACA-BI is an extension of MACA protocol and it eliminates the need of the CTS by using a ready-to-receive (RTR) packet from the receiver. The information about the traffic at neighboring nodes is sent in the data packets.

Medium access with reduced handshake (MARCH):

In MARCH the RTS packet is sent only for the first data packet of the stream instead of sending it separately for all data packets. A node knows about the packet arrival at the neighboring nodes by listening to the CTS signals.

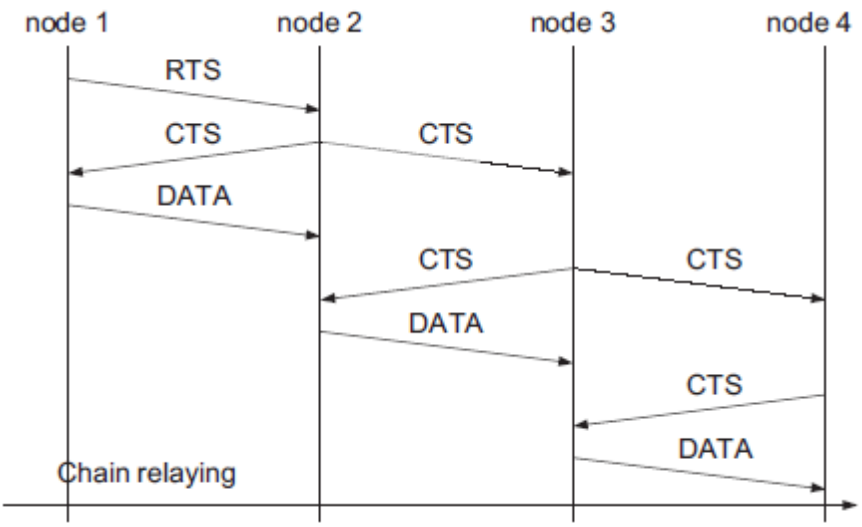

Figure 4: Relaying using MARCH

2.1.6.2 Contention-based Protocols with reservation

The second category of the MAC protocols is the contention-based protocols with reservation. The basic idea of contention with reservation is that the contention occurs only in the resource reservation phase. And once the resource (bandwidth) is reserved the node gets an exclusive access to the medium (channel).

Some of the protocols that fall under this category are D-PRMA, CATA, hop reservation multiple access protocol and SRMA/PA. Now we will explain each of these protocols briefly.

Distributed packet reservation multiple access protocol (D-PRMA):

D-PRMA is based [8] on TDMA scheme in which the channel is divided into frames as shown

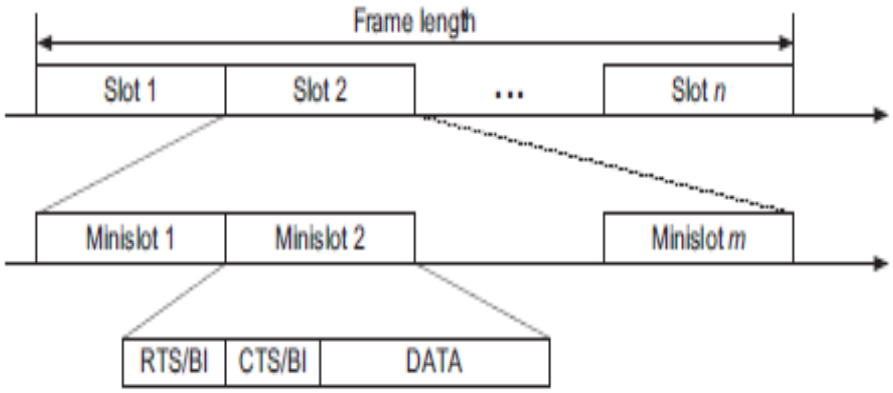

Figure 5: Slot structure of D-PRMA

The protocol operates as follows:

If a node has data to send then it has to contend in the first mini-slot of each slot. If the node wins the contention then it is granted all the remaining (m-1) mini-slots and the same slot in the subsequent frames is reserved for this node so that it can complete its transmission. The communication in the reserved slot the communication is done using TDD or FDD.

The whole slot reservation mechanism is that each mini-slot has a certain period of carrier sensing and if the node find that idle it will send RTS to the destination and the destination will reply with CTS in the CTS field of the same mini-slot and upon reception of the CTS the node is given access to all the remaining mini-slots.

The hidden node problem is solved by not allowing a node to transmit when it hears an RTS avoids the collision and a node hearing a CTS is not allowed to transmit for the remaining time slot period.

The exposed node problem is solved by making a node not to transmit when it hears an RTS but not CTS.

An advantage of D-PRMA is that it is best for voice applications and its major disadvantage is that it requires synchronization.

Collision avoidance time allocation protocol (CATA):

CATA is also a TDMA based scheme with a slot divided into CMS (control mini-slot) and DMS (Data mini-slot) as shown

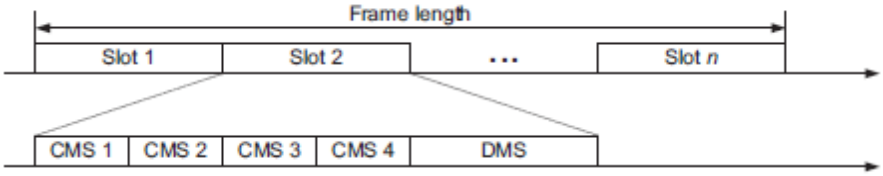

Figure 6: Slot structure of CATA

The operation of the protocol is as follows:

The receiver node of the data stream informs the source node of the stream about the reserved slot and the source then informs the destination about the interferences in the slot. Negative acknowledgements are used for reservation requests and control packets for the reservation slots information distribution.

The slot reservation in CATA is done as the sender senses the CMS 1 and if it turns out to be idle then the node send an RTS in CMS 2, the receiver upon reception of RTS reply with a CTS in CMS 3 and then sender acknowledge it by sending NTS (not to send) in CMS 4. The sender then sends data in DMS of the slot the process can be shown visually as:

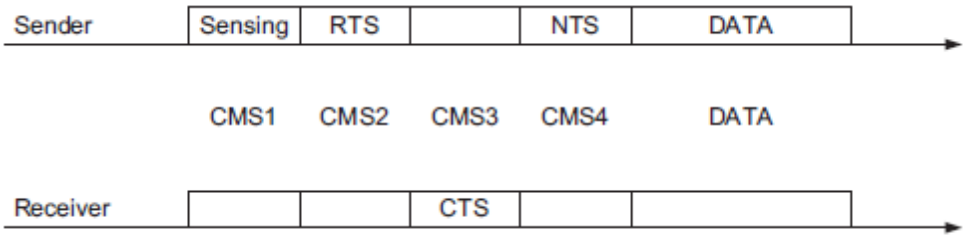

Figure 7: Slot reservation in CATA

Hop reservation multiple access protocol (HRMA):

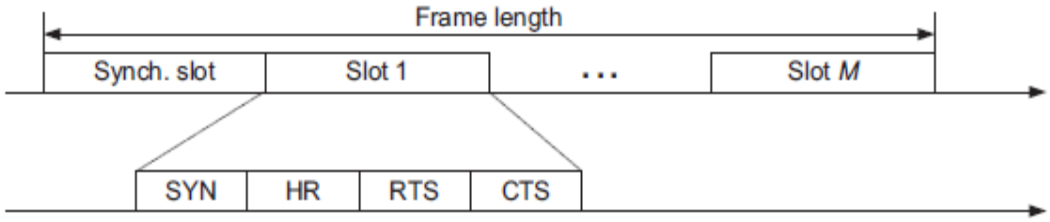

Figure 8: Frame Structure of HRMA

The working of the HRMA is as follows:

A node listen to the HR and if it is idle then it will send RTS and upon reception of RTS the destination node will reply with CTS and then it will wait for the data. If HR is not idle then the node will back-off for a random time and then sense the HR period again.

Soft reservation multiple access protocol with priority assignment (SRMA/PA):

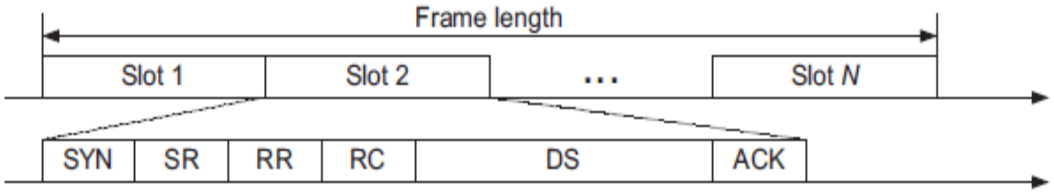

Figure 9: Frame Structure of SRMA/PA

2.1.6.3 Contention-based Protocols with scheduling mechanisms

In this category the basic aim of the MAC protocols is the transmission scheduling with considering metrics like delay targets of packets, traffic load at nodes and remaining battery power at nodes.

Protocols that fall in this category are DPS and DWOP. We will briefly explain each of these protocols.

Distributed priority scheduling (DPS):

This protocol is based on DCF mechanism of IEEE 802.11 using RTS-CTS-DATA-ACK.

The working of the protocol is that when a node has a data it sends RTS packet which carries priory index (delay etc), the receiver then responds with the CTS containing the priority tag. The neighbors retrieve this information from RTS and CTS and enter it in scheduling table and then the sender transmits data with the receiver responding with ACK and then the neighbors update their scheduling tables. The process can be visualized as

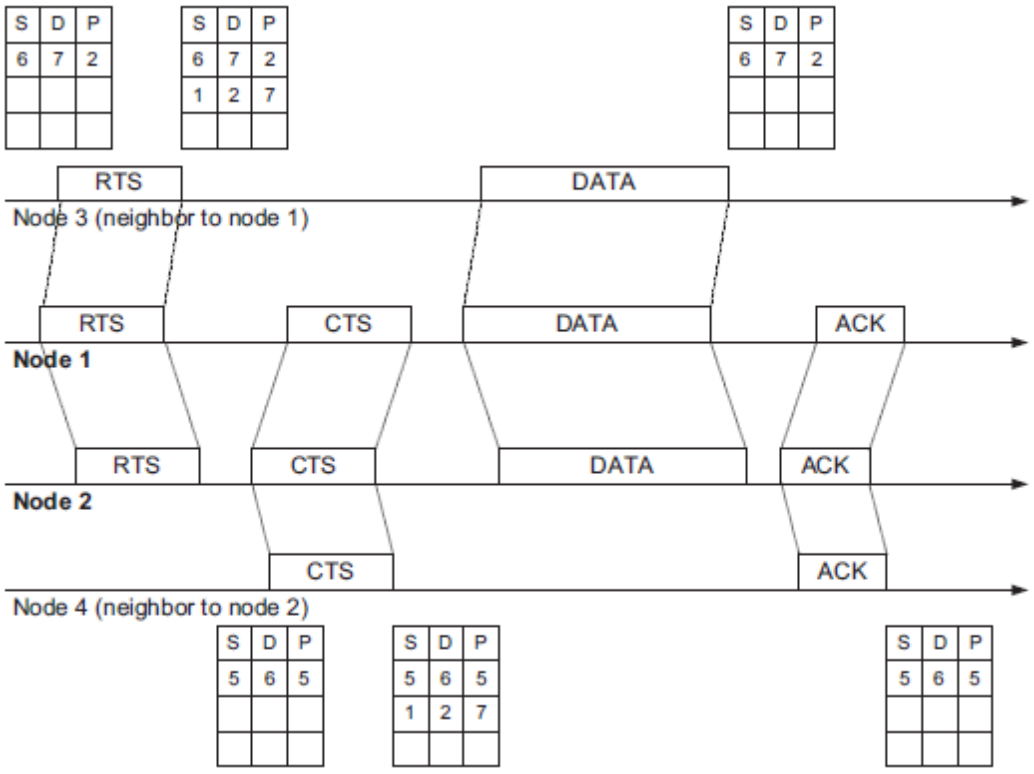

Figure 10: Frame Structure of SRMA/PA

The other categories of MAC protocols are

- MAC protocols for directional antennas
- Power Control MAC protocols

But as these protocols are not related to our work so we are not going to explain them in detail.

2.2. IEEE 802.11 contention based MAC protocol

802.11 protocol is widely used in MAC layer of wireless networks and is widely accepted standard that is designed by IEEE. It is a protocol that belongs to the contention based protocols of the MAC without any reservation or scheduling.

2.2.1 How WLAN systems are different?

First let us discuss how wireless LAN systems are different from those of wired. When we consider the design of the wired LAN system the physical location of the node is assume to be equivalent to an address while this is not always the case with 802.11 addressable stations. In 802.11 WLAN systems they are just the origins and destination of a message. The physical and operational characteristics are just defined by the terms used with the nodes like for location and mobility, the addressable units may b fixed, portable and mobile etc and node is just a destination of the message.

2.2.2 Impact of media on design

As the media used for the communication in 802.11 is different from wired media so the following things could impact the design of 802.11

- 802.11 has to use a medium that has no boundaries which are discoverable and stations with low power transceivers are unable to receive network frames
- The signals can be interfered by others which are sharing the medium
- The reliability of the medium is less as compared to the wired one
- Topologies are dynamic
- It lacks a full connectivity and it cannot be assumed that the every node can hear every other node, and a node might be hidden from other node(s)
- The propagation properties are time-varying and asymmetric
- Interference can also occur from logically disjoint 802.11 networks operating in overlapping areas

2.2.3 The impact of handling mobile nodes

The IEEE 802.11 protocol must handle the mobility of nodes a part from the portable nodes. Portable nodes are one that are moved from one location to other location but are always used when they are stationary, while mobile stations may access LAN while they are in motion.

For technical reasons it is not sufficient to handle only portable nodes as propagation effects causes nodes to appear mobile even when they are stationary.

Other issue is the power management as the mobile nodes will be mostly battery powered so power management is an important consideration in the design of 802.11.

2.2.4 MAC Architecture of 802.11

The MAC architecture of 802.11 as shown in Figure 11 is divided into different type of multiple access 802.11 is providing and based on this a node can used 802.11 in different modes based on the system available.

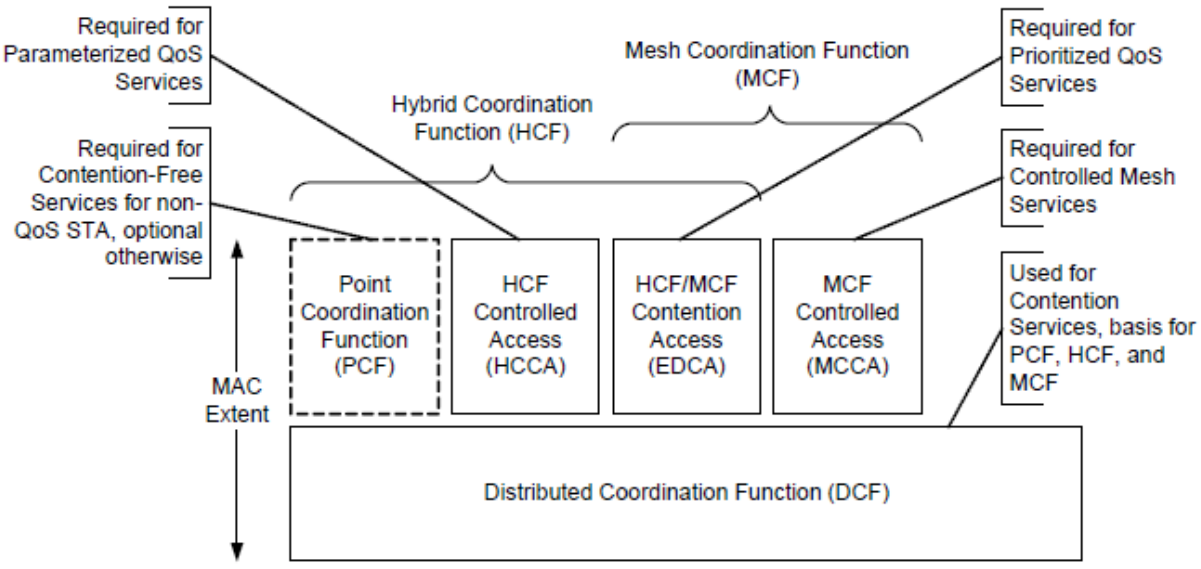

Figure 11: MAC architecture of IEEE 802.11

The modes of 802.11 can be

- Distributed Coordination Function (DCF)

- Point Coordination Function (PCF)
- Hybrid Coordination Function (HCF)
- Mesh Coordination Function (MCF)

Now we will discuss each one of the above briefly

2.2.5 Distributed Coordination Function (DCF)

This is the fundamental method used by IEEE 802.11 MAC and known as carrier sense multiple access with collision avoidance (CSMA/CA). DCF shall be implemented in all nodes. The operation of 802.11 in a node using DCF is as follows:

If a node want to transmit then it must sense the medium to determine if another node is transmitting. If the medium is free then the communication may proceed. The node should verify that the medium is idle for certain duration of time before attempting to transmit. If the node found the medium busy then it should defer till the end of the current transmission.

After a node has deferred or prior to attempting again to transmit a node should select a random back-off and should decrement this back-off interval counter if it keep finding the medium as idle. A transmission is considered successful if the ACK is received for the frame or if the frame with group address is transmitted completely. A refinement method may be used for further decreasing the collisions, that is after a node is deferred of transmission or prior to transmit again the nodes should exchange a short RTS and CTS messages.

2.2.6 Point Coordination Function (PCF)

The IEEE 802.11 MAC has also an option access method called PCF, which can only be used in the infrastructure network configurations. This access method uses a point coordination which operates on an access point which performs the operation of polling to determine which node has the right to transmit. PCF may also need to perform additional functions in cases where there is multiple coordinating BSS using same channel in overlapping physical space. PCF uses a virtual carrier sense mechanism with access priority mechanism. PCF should distribute information within beacon

management frames to gain medium access by setting NAV in nodes. The frame transmission under PCF may used the small inter frame space (IFS) than the IFS for frames transmitted via the DCF. The small inter frame space for PCF means that the PCF has a priority access to the medium in overlapping BSSs operating under DCF-access method. The point coordination controls the frame transmission of nodes to eliminate contention for small time intervals.

2.2.7 Hybrid Coordination Function (HCF)

This coordination function provides QoS facility and can only be used in QoS network configurations. This coordination function can be used in all QoS node except in mesh nodes which have to use MCF instead. HCF uses functions of both PCF and DCF with some enhanced mechanisms for the QoS specific requirements. The HCF uses both access methods enhanced distributed channel access (EDCA) and controlled channel access called HCF controlled channel access (HCCA).

2.2.8 Mesh Coordination Function (MCF)

This additional facility of coordination is meant for mesh networks where each node in a mesh must implement MCF only. It has both contention-based and contention-free access mechanism and is called MCF controlled channel access (MCCA).

2.2.9 Services

According to 802.11 standard, a wireless LAN must provide nine services. There are two categories of the services: distribution services and station services. The distribution services manage a cell membership and interaction with the nodes outside the cell while station services manage activity inside a cell. Now we will discuss each of these services separately.

2.2.9.1 Distribution Services

The distribution services are five and these services are provided by the base station to deal with the station mobility about when they enter or leave the cell

and how they attach and detach themselves from the base station. They are as follows:

1. **Association**

   This service deal with the nodes attaching themselves to the base stations. This happens when a node moves in to the radio range of the base station. When a node arrives in the radio range of the base station it announces its capabilities like data rates supported, need for PCF and power management requirements. A base station can accept or reject the node and upon acceptance a node must authenticate itself.

2. **Disassociation**

   One of the base station or node may disassociate and breaks the relationship. A node should use it before leaving or shutting down while a base station can also use it when it is going down for maintenance.

3. **Re-Association**

   This service is used for the changing of preferred base station. It might be useful for the nodes which are mobile and no data will be lost during handover if this service is used correctly.

4. **Distribution**

   The purpose of this service is to decide the route of the incoming local frames. If the frame's destination s local to the base station then it is sent straight over the air otherwise it is forwarded over the wired network.

5. **Integration**

   This service serves the purpose of translation from 802.11 frame's format to a different one that is used by the destination. This is required when the frame uses a different addressing scheme or frame format.

2.2.9.2 Station Services

The station services are intra-cell services and they are used after a node is associated with a base station and are as follows.

1. **Authentication**

   One of the problems with the wireless is the broadcast medium and anyone can send or receive the data, so a node must be authenticated before it can send or receive data. After a node associates itself with the base station, the base station sends a challenge frame to the node and asks for the secret key that is assigned to it. If the node passes the challenge and provide with the correct key the node is enrolled in the cell.

2. **Deauthentication**

   This service is used when a node leaves the network, so it deauthenticated and it may not use the network afterward.

3. **Privacy**

   As wireless is a broadcast medium and anything sent over it can be received by anyone who is in the range of the radio and is listening to the same frequency so the information over the wireless LAN is encrypted to keep its privacy. The encryption algorithm that is used is RC4, invented by Ronald Rivest of M.I.T.

4. **Data delivery**

   802.11 provides a node with the service of data sending and receiving as it is all about for which it was designed but the data transmission over 802.11 is modeled on Ethernet and is not guaranteed so higher layers must detect and correct errors in the data.

2.3. Ad hoc on-demand Distance Vector (AODV) Routing Protocol

The Ad hoc On-Demand Distance Vector (AODV) routing protocol is intended for use by mobile nodes in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times (even in the face of anomalous delivery of routing control messages), avoiding problems (such as "counting to infinity") associated with classical distance vector protocols.

The types of messages that are exchanged by nodes using AODV when finding route to destination are

2.3.1 Hello Messages

A node MAY offer connectivity information by broadcasting local Hello messages. A node will only use HELLO message for an active route. A node SHOULD only use hello messages if it is part of an active route. Every HELLO_INTERVAL milliseconds, the node checks it has sent a broadcast and if it did not then it will broadcast a RREP with TTL = 1 and this RREP message is called HELLO message. This message has the fields as described in Table 1

Table 1: HELLO message fields

Field Name	Field Value
Destination IP Address	The node's IP address
Destination Sequence Number	The node's latest sequence number
Hop Count	0
Lifetime	ALLOWED_HELLO_LOSS * HELLO_INTERVAL

The way a node can determine connectivity is by listening for packets from neighbors and if within the past DELETE_PERIOD it has received a Hello message and then not received any packets for more than ALLOWED_HELLO_LOSS*HELLO_INTERVAL milliseconds, then that node is assumed to be currently lost.

2.3.2 Route Request (RREQ) Message

A node generates a RREQ message when it does not find route to destination in its own routing table. This situation can arrive it the node has currently no knowledge of the destination node or the route to destination has expired or is already marked invalid. The Destination Sequence Number field in the RREQ message is copied and checked in the routing table. If sequence number is unknown then it's unknown sequence number flag must be set. The Originator Sequence Number in RREQ message is the node's own sequence number and must be incremented prior to insertion in a RREQ. The RREQ ID is also incremented by the current node. Each node uses only one RREQ ID. The Hop Count field is set to zero by the originating node and then is incremented by the intermediate nodes till it reaches the destination or the message is discarded if the TTL value hits zero.

Data packets waiting for a route (i.e., waiting for a RREP after a RREQ has been sent) should be buffered. This buffering SHOULD be "first-in, first-out" (FIFO). If a route discovery has been attempted RREQ_RETRIES times at the maximum TTL without receiving any RREP, all data packets destined for the corresponding destination should be dropped from the buffer and a Destination Unreachable message should be delivered to the application.

2.3.2.1 Controlling Dissemination of Route Request Messages

A binary exponential back-off for repeated attempts at route discovery must be used to reduce network congestion. At first source node should broadcasts a RREQ and wait for NET_TRAVERSAL_TIME milliseconds for the reception of RREP. If no RREP is received in that time the source sends a new RREQ and each time this request must be sent with an exponential backoff mean increasing the time of retry at each attempt to reduce the congestion on the network.

2.3.2.2 Processing and Forwarding Route Request Messages

A node receiving RREQ should first create or update a route to the previous hop without valid sequence number and check if it has already a RREQ with same

originator IP and RREQ ID in the last PATH_DISCOVERY_TIME. If its true, the node will discard the RREQ. If not then it will increment the hop count to account for the new hop through the intermediate node. Then as we already know the RREQ is also used to build a back path so that the destination and all the intermediate nodes has the knowledge of the originator of RREQ so the node will search for the reverse route to the Originator using longest-prefix matching. If the route does not exist then it is added to the table.

The format of the RREQ message is

Table 2: RREQ message fields

Type	|J|R|G|D|U|	Reserved	Hop Count
RREQ ID			
Destination IP Address			
Destination Sequence Number			
Originator IP Address			
Originator Sequence Number			

2.3.3 Route Reply (RREP) Message

Route Reply is generated when:

- The node itself is the destination, or
- The node has an active route to the destination, the destination sequence number in the routing table is valid and greater than or equal to the Destination Sequence Number of the RREQ and the "destination only" flag is not set

The Route Reply Packet generation is discussed in detail in Section 2.1.8.

The message format of the RREP message is

Table 3: RREP message fields

Type	|R|A|	Reserved	|Prefix Sz|	Hop Count
Destination IP address				
Destination Sequence Number				
Originator IP address				
Lifetime				

2.3.4 Maintaining Sequence Numbers

It is required to keep the latest entry in the routing table and this is done using sequence numbers in AODV protocol. This is the “destination sequence number”. This number is updated at the arrival of the new information about the sequence number from RREQ or RREP messages about that destination. This is made possible by each node in the network to guarantee loop-free routes towards the destination.

A destination node increments its sequence number in two conditions:

- When a node originates a route discovery, it increments its own sequence number. This prevents conflicts with previously established reverse routes towards the originator of the RREQ
- When a node originates a RREP in response to a RREQ, it update its own sequence number to the maximum of the current sequence number and the destination sequence number in the RREQ packet

In order to find out that the information about the destination is not stale, the node compare the current numerical value of the sequence number with the one obtained from AODV message. Comparison must be done using 32-bit arithmetic to accomplish sequence number rollover. If the difference between current and incoming sequence number is less than zero, the information about that destination in AODV message must be discarded since this information is stale.

One of the circumstances in which a node changes its destination sequence number is when an entry in the routing table expires or lost to the next hop towards that destination.

2.3.5 Routing Table Entries

After receiving AODV control packet from a neighbor or when a node creates or updates a route to a destination or subnet, it checks entry for that destination. If there is no entry corresponding to that destination then it is created. The sequence number is either taken from control packet or the valid sequence number field is set to false. A route is updated if the new sequence number is either:

i. Higher than the sequence number in the routing table
ii. Sequence numbers are equal, but hop count (of new information) plus one is smaller than the existing hop count, or
iii. Sequence number is unknown

2.3.6 Generating Route Requests

A node generates a RREQ when the route to a destination with which it wants to communicate is not available in its routing table, or the entry is expired or is marked invalid. The Destination Sequence Number field contains the last known sequence number or if it is unknown then the unknown sequence number flag must be set. The Originator Sequence Number is the node's own sequence number and is incremented prior to insertion in a RREQ. The RREQ ID field is incremented by one from the last RREQ ID used by the node generating the RREQ. The Hop Count field is set to zero.

The node originating the RREQ often wants a two way communication with the destination node. In such cases, the destination should also know the route back to the originating node. In order to accomplish this originating node selects this mode in the intermediate nodes by setting 'G' flag.

Buffering of data packets waiting for the route (i.e. waiting for RREP after RREQ is sent) should be used and in a "first-in first-out" fashion. If the TTL value for that RREQ is expired then all the data packets in the buffer must be dropped and a Destination Unreachable message should be delivered to the application.

2.3.7 Processing and Forwarding Route Requests

Upon receiving of RREQ, a node first creates or updates route to the previous hop without a valid sequence number then checks to determine whether it has received a RREQ with the same Originator IP Address and RREQ ID within at least the last PATH_DISCOVERY_TIME. If such RREQ has already been received, the node discards this RREQ.

If a node does not generate a RREP and the incoming packet IP header has a TTL greater than 1, the node then updates and broadcasts the RREQ to 255.255.255.255 on each of its

interfaces which are configured. RREQ packet is updated by decreasing TTL or hop limit field by one and increasing hop count field by one, to cater for the new hop through the intermediate node. Lastly the destination sequence number of the destination is set to the maximum of the corresponding value received in the RREQ message, but the forwarding node will not change the sequence number of destination even if the received value is larger.

Otherwise the node generates a RREP, and then discards the RREQ. Now if the intermediate node replies to every transmission of RREQs for a particular destination, it might happen that the destination will be unaware of the discovery messages and the destination might initiate a RREQ in case the originator attempts to establish a TCP session. So to make destination aware of the originator the originating node should set the "gratuitous RREP" (G') flag in the RREQ if the destination is likely to need a route to the originating node. So if an intermediate node respond to the RREQ with 'G' flag set, it must also unicast a gratuitous RREP to the destination node.

2.3.8 Generating Route Replies

Route Reply is generated when:

- The node itself is the destination, or
- The node has an active route to the destination, the destination sequence number in the routing table is valid and greater than or equal to the Destination Sequence Number of the RREQ and the "destination only" flag is not set

The node generating a RREP message copies the Destination IP Address and the Originator Sequence Number from the RREQ message to the corresponding fields in the RREP message.

After making a RREP, the node then unicast it to the next hop towards the originator of the RREQ, as the entry could be found in the routing table. As the RREP forward to the originator the Hop Count field is incremented be each hop. Thus, the RREP reaches the originator and the Hop Count represents the distance.

2.3.8.1 Route Reply Generation by the Destination

If the RREP generating node is the destination itself, it must increment own sequence number by one if it is equal to the RREQ packet value after incrementing it. Otherwise the sequence number is not changed. The destination node places its sequence number in the Destination Sequence Number field of the RREP and put zero in the Hop Count field.

2.3.8.2 Route Reply Generation by an Intermediate Node

If the node which is generating RREP is not the destination but instead it is an intermediate node and has an active route to the destination, it put its own sequence number for the destination into the Destination Sequence Number field in the RREP message.

The intermediate node updates the forward route entry by placing the destination IP Address. The intermediate node also update its routing table entry for the node originating the RREQ by place the next hop toward the destination in the precursor list for the reverse route entry.

2.3.9 Generating Gratuitous Route Replies

If a node receiving a RREQ responds with a RREP, it discards the RREQ. If the RREQ has the ‘G’ flag set and intermediate node returns a RREP to the originating node, it will also unicast a gratuitous RREP to the destination node.

Gratuitous RREP is sent to both the next hop and the destination node, just as if this RREP is generated by the destination and this intermediate node is forwarding it. The RREP that is sent to the originator of the RREQ is the same whether or not the 'G' bit is set.

2.3.10 Receiving and Forwarding Route Replies

A RREP receiving node searches (using longest-prefix matching) for a route to the previous hop, and is created if doesn’t exist, without a valid sequence number. Then the hop count value in the RREP is incremented by one to account for new hop through the

intermediate node. Then the node searches for the forward route to the destination and create if it doesn't exist, otherwise just Destination Sequence Number is updated.

2.4. Time Division Multiple Access (TDMA)

Time Division Multiple Access is a technique which is used in Link Layer to determine which node will occupy the channel. Briefly, in this technique each node occupies the channel and uses its full bandwidth for a small portion of time and then wait for its next turn. In ideal case we can say that if there are n nodes and each node can occupy the channel for t sec then a node can acquire channel after every (n * t) sec.

Time division multiple access (TDMA) is a channel access method for shared medium networks. It allows several users to share the same frequency channel by dividing the signal into different time slots. The users transmit in rapid succession, one after the other, each using its own time slot [9]. This allows multiple stations to share the same transmission medium (e.g. radio frequency channel) while using only a part of its channel capacity. TDMA is used in the digital 2G cellular systems such as Global System for Mobile Communications (GSM), IS-136, Personal Digital Cellular (PDC) and iDEN, and in the Digital Enhanced Cordless Telecommunications (DECT) standard for portable phones. It is also used extensively in satellite systems, combat-net radio systems, and PON networks for upstream traffic from premises to the operator. For usage of Dynamic TDMA packet mode communication, see below.

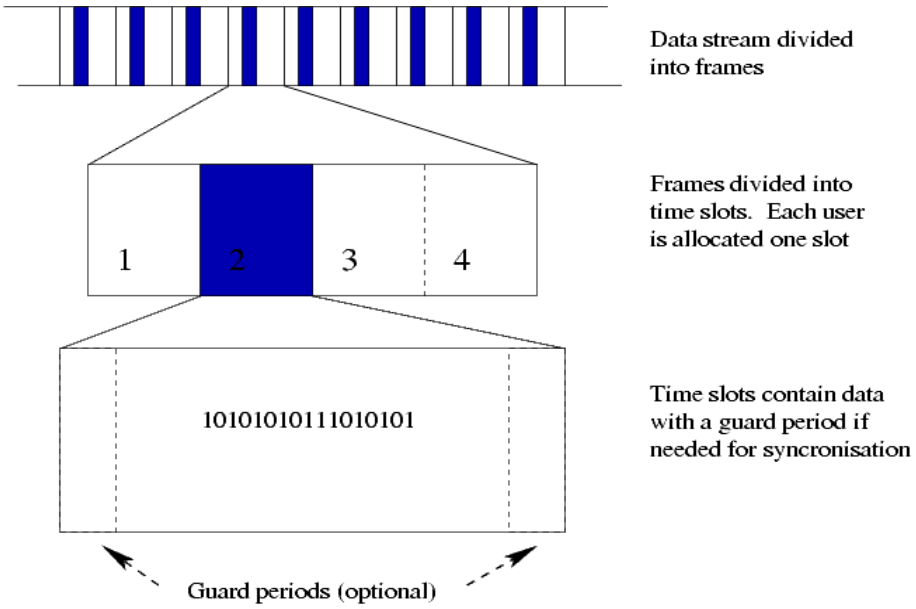

Figure 12: Figure showing the slotting in TDMA protocol of MAC Layer

In traditional mobile networks TDMA is used and slots are allocated to the end mobile node on its request using up-channel and using control signals on up-channel a slot is allocated on the down-channel.

2.5. Cross-Layer Design

There is no specific definition of the cross layer design and can be defined in several ways. It depends on how designers have thought of it when they proposed a design based on cross-layer. However in its simplest form most of the designer took it as the crossing of information among the layers in TCP/IP stack.

Different type of information has been made shared among the layers and based on this information quality is ensured and decisions on data forwarding are made. We have studied some of the examples and will discuss in detail about what they have done and how.

Mobile ad hoc networks (MANET) are becoming an integral [2] part of the ubiquitous computing and they have provided infrastructure for the video applications and multimedia-on-demand, and Quality of Service (QoS) is to be considered to provide high success rate for multimedia data. Providing QoS to applications is challenging in MANET where nodes are mobile, energy sources are scarce and bandwidth is limited. Because of these limitations

previous research has focused on physical layer problems like antennas [10][11], problems regarding MAC layer like collision avoidance in scheduling of frame [12][13], energy efficient transmission [14][15] and problems in network layer like routing packets in power-aware manner [16][17], with QoS Support [18][19], under different mobility models [20][21] and with the aid of location information [22][23]. In all these researches no one has considered distributed middleware and application services with assumption of underlying ad hoc network routing services. So in [2] the author proposed a design in which the routes in the internet layers are maintained with a QoS factor to set the priority of data that is generated by application that require high success rate.

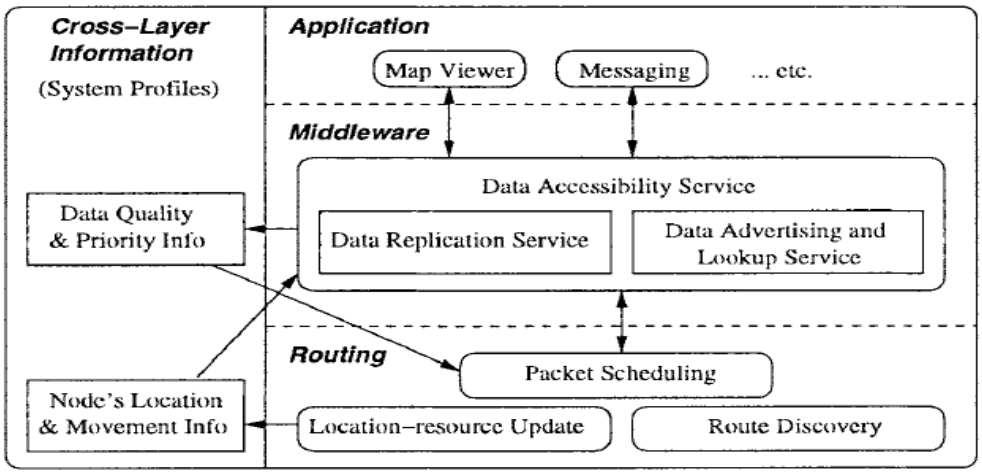

Figure 13: Cross layer design showing exchange of information between middleware layer and routing layer

The middleware layer between application and internet layer keep data priority information which is used by the internet layer providing cross layer design to increase success rate. Similarly middleware layer uses information to be updated about nodes location and its movement.

In [3] a new routing algorithm is proposed which is QoS routing algorithm and is a modified form of existing Ad hoc on-demand distance vector (AODV) protocol and works in conjunction with the MAC TDMA layer. The QoS algorithm take advantage of the multiple paths available to one destination but only one route is placed in the routing table and that route is selected on the basis of different QoS metrics based on the bandwidth requirements. The authors used the

path bandwidth calculation algorithm as proposed in [24] and solved the exposed and hidden nodes problem as proposed in [25] and used this bandwidth calculation on the destination node which expects to receive RREQ from different paths and based on the information of bandwidth it selects the best bandwidth path and send the RREP via that path to the originating node. The bandwidth requirement for a packet is calculated with the information from the application layer. The multimedia applications require more bandwidth so they are given more priority and high bandwidth paths.

In [4] the power of the node is used to make the design cross layer i.e. the low power nodes are able to receive from high power nodes but not vice versa, most commonly used MAC protocols like 802.11 Distributed Coordination Function (DCF) [26] checks the link bi-directionality only for unicast transmission, by performing the RTS-CTS two way handshake mechanism. So the RREQ sent by high power node will be received by low power node but its reply will not reach the high power node and communication will fail. So the signal strength information is shared with MAC and routing layer to decide the symmetry of the link

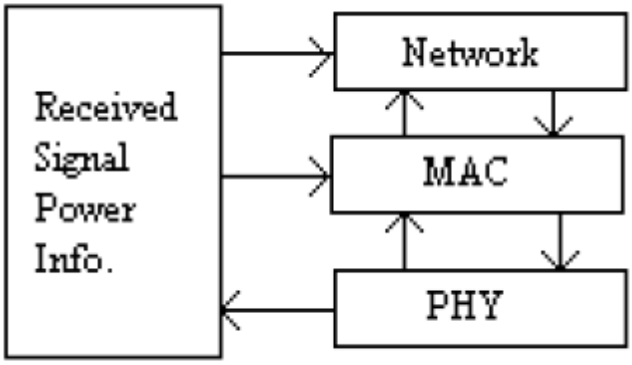

Figure 14: Figure showing that the Received Signal Power information from Physical layer is shared with Network and MAC layer

So based on information from physical layer, the routing layer avoids the asymmetric links and discovers routes which are symmetric to forward data to the nodes which are low powered. So the basic theme is to avoid the asymmetric link and discover routes to such nodes which are symmetric and this is done using the information of power from the physical layer.

In [5] author presented a CLAODV (Cross Layer Ad-hoc on-Demand Distance Vector), a reactive routing protocol. Cross-layer sharing [5] the status of network information is very helpful to optimize the operation of certain layers. It is based on classic AODV routing protocol and utilized useful information of MAC sub-layer in routing and also improved timed Hello messages. It affords prompt and accurate local topology information and reduces protocol overhead

2.6. Slot Allocation Algorithms in TDMA

As we did research on tactical networks and worked on finding existing cross-layer designs and the details of the 802.11 protocols. We did not find much on slot allocation algorithms for the tactical networks as the reason might be it is related to the military applications and they don't publish much of their work. Only thing that we find worth mentioning over here is the one from IEEE that is discussed next.

According to [27] slot allocation is crucial in tactical networks using TDMA as the efficiency and throughput of the network depends upon the efficient time slot resource management. The [27] paper presented a new dynamic time slot allocation for tactical networks of PRNET (Packet Radio Network).

The algorithm is divided into two parts: the cluster set-up phase and a steady-state phase. During the first part the mechanism similar to EC-TDMA and the BMA protocol is implemented and a cluster head is selected by election algorithm. The other members in the cluster become the slaves. In the steady state phase there are n frames which are equally divided into several slots. All the slots are data slots except for the first one which is control slot meant for sending control packets.

The control slot is further divided into 2s-2 parts where s is the number of sites in a cluster. Fir s-J time slots are allocated to the slave stations to send control packets to the head (master) station. And during the last s-J slots the master reply to the slave stations.

CHAPTER 3: METHODOLOGY

In this chapter we will describe in detail the work that we have done based on our background study and literature review. We will first describe the whole work briefly. Then will describe the whole work step by step in detail as the limitations in the current scheme and then our solution in the form of design and an algorithm.

3.1. Abstract of Work

We have worked on removing the limitations of the TDMA protocol particularly bandwidth utilization, hidden/exposed node problem and synchronization problem. First we have selected the routing protocol for our design which is Ad-hoc On Demand Distance Vector (AODV) and then modified its packet formats to fit for the best bandwidth utilization and then we used a merged layer design that is instead of having two layers Internet and Link Layer now we have a single layer performing the functions of both the layers so that we don't waste time in making packet then send to Link Layer then Link Layer do its own processing on it, instead now we have a single layer and the type of packet that a node want to send decides the type of TDMA slot in which it will be send so with this merged layer design we saved the work of one layer and put them together. Then the main problem was the wastage of the bandwidth in tactical networks where the communicating nodes are far less than the slots available so we solved this problem by designing a slot allocation algorithm which works on the findings of control messages exchanged by the AODV protocol and then that algorithm assign slots to each of the node so that in each frame the slots are reused to increase the bandwidth utilization and each node calculate its own slots which make all the active nodes synchronized.

3.2. Limitations in Existing Techniques

The complexity in MAC design for wireless ad hoc networks arises due to node mobility, radio link susceptibility and absence of central coordination. Research has been done to improve medium access performance in different aspects as identified by the different performance metrics. Tradeoffs among different performance metrics dictate the design of the MAC protocol such as throughput and fairness.

The traditional TDMA has a big flaw of bandwidth wastage, delay and low throughput when used in a tactical combat network where only few nodes are communicating. The probability that all the nodes are communicating is very small. So most of the time the bandwidth is being wasted as the slots remains empty and only a particular node to which it is assigned can use it e.g. if there are 30 slots and only 2 nodes (node 1 and node 3) are communicating with a hop distance of 1(node 2) then out of 30 slots only 3 slots are used which turn out to be 90% waste of bandwidth, high delay and low throughput. The scenario can be best explained with the use of a table showing usage of slots in a frame

Table 4: Slot usage in traditional MAC TDMA with 3 nodes active

Slot #	1	2	3	4	5	6	….	…..	30
Frame 1	Node 1 send its data	Node 2 forwards data	Node 3 send its data	Empty	Empty	Empty			Empty
Frame 2	Node 1 send its data	Node 2 forwards data	Node 3 send its data	Empty	Empty	Empty			Empty
Frame 3	Node 1 send its data	Node 2 forwards data	Node 3 send its data	Empty	Empty	Empty			Empty
Frame 4	Node 1 send its data	Node 2 forwards data	Node 3 send its data	Empty	Empty	Empty			Empty
. . .	. . .	. . .	. . .	. . .	. . .	. . .			. . .
. . .	. . .	. . .	. . .	. . .	. . .	. . .			. . .
Frame ‘n’	Node 1 send its data	Node 2 forwards data	Node 3 send its data	Empty	Empty	Empty			Empty

It can be easily seen in Table 4 that out of every 30 slots in one frame only three slots are used and there is a lot of wastage of bandwidth. A node sends it data in a slot get its turn after 30 slots and a delay of 30 times width of one slot. This can be reduced by using more slots in a frame if they are not being used by the other nodes.

Other interesting thing that we studied is the lightness of the AODV control messages. The messages are very small carrying a very little information. So looking at the scarceness of the slots and time constraints to set up a voice call, AODV messages can be modified to carry a little bit more significant information and more than one control messages can be accumulated and sent in one slot time if required.

3.3. Proposed Idea

The problem of bandwidth wastage is common in all MAC TDMA based techniques. The problem can be solved if we find some way to inform a node that which nodes are active and which are dead so that they have knowledge of the slots which are being wasted and active nodes can utilize those slots. So when all the nodes will have a knowledge about which slot it will use and which slot will be used by which other node there will be no collision at all and the bandwidth will be utilized at its maximum possible value.

3.4. Proposed Design

We are proposing a new technique of Time Division Multiple Access in which we have made a node capable to utilize the bandwidth as efficiently as possible e.g. if there are ‘n’ slots in a TDMA frame and only two nodes are communicating then the active nodes can use the slots of the other nodes which are either dead or are not communicating at that time. This can be done if a node has information about which nodes in the topology are communicating and their path and the hop distance between them. Once this information is available a node will be capable to use this information to find the slots that it can use and leave the other, and once all the slots in the topology are aware of which slot they will use then we will get two advantages out of it. One is that there will be no collision at all even if the nodes are using multiple slots in a frame and second is the wastage of bandwidth will be at its minimum.

3.5. Mechanism

We have devised a two phase scheme to achieve the above mentioned goals:

During the first part, nodes which have data to send or want to talk to other nodes just exchange control messages and build up their routing table and find paths to the destination and in the

second phase the nodes which have data to send use the slots of the other nodes as well to avoid the wastage of the bandwidth.

Dividing the task into two phases make it easier to utilize the slots which are being wasted in traditional TDMA techniques. In the first phase only control messages are exchanged and when the control messages are over all the active nodes have the knowledge of which node want to communicate with which other node and then before the second phase they run a slot allocation algorithm which utilizes the information that is available with the node about communicating node to find out which slot is being used by which node so by doing this there will be no collision in the second phase and one node will be utilizing more than one slots in a frame so the bandwidth is utilized efficiently.

We are using a merged layer design by combining the tasks of network layer and link layer, the type of data at network layer will decide the slot in which it is being sent. We are using AODV routing protocol for wireless networks and based on its control messages we have made some modifications in it to get maximum utilization out of it.

We have modified control messages of AODV and the way they are sent to decrease the route setup time as well as better utilization of the bandwidth.

We are also using multiple control messages in a single packet to get maximum utilization of the bandwidth.

3.6. Detailed Working of the proposed Scheme

We have used a 30 slot architecture to test our design mean we can have a maximum of 30 nodes at a time. We are assuming that the nodes which are communicating can be at a distance of 2 hops at maximum. Now let us assume a topology with 6 nodes with node id 1, 2, 3, 4, 5, 6 respectively and arranged as in Figure 15

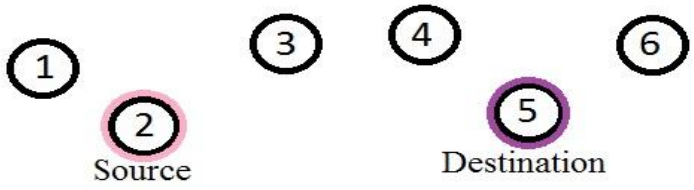

Figure 15: Arrangement of nodes

Now let us assume that node 2 want to talk to node 5. Using this example we will try to show that how all nodes are informed about the communication of node 2 and node 5 and using that information how they will decide to use the slots of inactive nodes.

First of all there will be silence and no one is sending any data. The node which wants to communicate will break the silence in the topology. In our example node 2 will break the silence and will send an AODV hello packet and based on these control messages a node also updates it routing table.

Now the silence period is over and all the active nodes will start exchanging the control messages. So after node 3 and node 1 receive hello packet of the node 2 both of them will update their routing tables and add an entry for a route to node 2 with a hop distance of 0. Then node3 will broadcast its hello packet and so on and at the end of the first frame node 2 through 6 have broadcast their hello packets and at the end of this frame the routing tables will be like node 2 will have entry of node 3 with hop distance of zero (note that node 2 has not received any hello from node 1 so its routing table will not contain entry to node 1), node 3 will have two entries one for node 2 and other for node 4 both at a hop distance of 0, node 4 will have entry of node 3 and node 5 both at zero hop distance, node 5 will have entry of node 4 and node 6 both at a hop distance of zero, node 6 will have entry of node 5 at zero hop, but node 1 has to wait for the second frame to do so as the silence was broken by node 2 so after that node 1 was not able to broadcast its hello before the second frame. The first frame will be like

Table 5: Control Frame 1

Slot #	1	2	3	4	5	6	….	…..	30
Frame 1		Node 2 will broadcast Hello	Node 3 will broadcast Hello	Node 4 will broadcast Hello	Node 5 will broadcast Hello	Node 6 will broadcast Hello			

Now in the second frame node 1 will broadcast it hello packet and upon receiving this hello packet node 2 will add a second entry to its routing table with a route to node 1 with a hop distance of zero, then node 2 will broadcast its RREQ packet to ask for the route to the node 5 from the neighbors. Now as we know that as the RREQ is received a node will setup back path also by adding an entry to it routing table with the node id of the originator and hop count in RREQ. Then node 3 will re-broadcast the RREQ message as it also don't have route to node 5 in its routing table, then node 4 will process this RREQ and first update its table with the entry of the originator and its hop count, that is it will add an entry of node 2 with a hop count of 1. As it has route to node 5 in its routing table so it will broadcast RREP message instead.

Now here is a modification in our scheme, in traditional AODV RREP messages are unicast but as RREP contain the information of the communicating nodes so we want this RREP to reach all the active nodes so in our scheme a node will broadcast RREP either in reply to a RREQ or will re-broadcast it.

So upon receiving RREP node 5 will re-broadcast this RREP and will also add an entry to the routing table as path to node 2 with a hop count of 2, and then node 6 will just rebroadcast the RREP.

Table 6: Control Frame 2

Slot #	1	2	3	4	5	6	….	…..	30
Frame 2	Node 1 will broadcast Hello	Node 2 will broadcast RREQ	Node 3 will re-broadcast RREQ	Node 4 will broadcast RREP	Node 5 will re-broadcast RREP	Node 6 will re-broadcast RREP			

In the next frame as node 1 has a RREQ from node 2 and it doesn't have a path to node 5 so it will re-broadcast this RREQ. Node 2 has nothing to do so it will wait for the response to its RREQ. Node 3 will re-broadcast the RREP and update its routing table with the entry of the destination in the RREP and its hop count, so it will add a route to node 5 with hop count of 1. Node 4.5.6 has nothing to do so they will just keep silent in this frame.

Table 7: Control Frame 3

Slot #	1	2	3	4	5	6	….	…..	30
Frame 3	Node 1 will re-broadcast RREQ		Node 3 will re-broadcast RREP						

Then node 2 will re-broadcast the RREP that it received from node 3 and also update its routing table with the route to node 5 with a hop count of 2. Node 3,4,5,6 will remain silent in this frame.

Table 8: Control Frame 4

Slot #	1	2	3	4	5	6	….	…..	30
Frame 4		Node 2 will re-broadcast RREP							

In this frame node 1 will re-broadcast RREP that it is received from node 2.

Table 9: Control Frame 5

Slot #	1	2	3	4	5	6	….	…..	30
Frame 5	Node 1 will re-broadcast RREP								

And frame 6 will be empty as there are no more control messages to be exchanged.

Table 10: Control Frame 6

Slot #	1	2	3	4	5	6	….	…..	30
Frame 6									

In our design in the worst case, it takes only six frames to exchange all the control messages necessary for the call setup so one super-frame structure contain first six control frames.

After the exchange of control packets every active node will have the RREP packet in their memory and it will run the below slot allocation algorithm and find a slot allocation vector which describes which node will occupy which slot.

Algorithm for slot allocation (for one node)

1. Declare array 'B'
2. $x = \{\left[\sum_{for\ all\ RREP}(hopCount + 1)\right] \times 2\} \div 30$
3. Sort RREPs in each node with respect to RREP IDs
4. For each RREP perform the following steps to find the slot numbers to occupy
    a. Declare array 'A' of size $[hopCount + 1] \times 2$ (hopCount from RREP)
    b. If this node is originator
        i. Allocate the first slot in 'A'
    c. Else if this node is receiver
        i. Allocate this slot in 'A' to the node
        $$[hopCount(*) + 1] + 1$$
        hopCount from RREP (*)
    d. Else if this node is relaying (two slots will be allocated, one for forward and one for backward communication)
        i. Allocate forward slot in 'A' by
        $$[hopCount(*) + 1] + 1$$
        hopCount from Routing Table to Originator (*)
        ii. Allocated backward slot in 'A' by
        $$[hopCount(*) + 1] + [hopCount(**) + 1] + 1$$
        hopCount to destination from Routing table (*)
        hopCount from RREP (**)
    e. Append array 'A' to array 'B' and clear array 'A'
5. Repeat array 'B' *x* number of times

The flow chart for the algorithm is shown in Figure 16

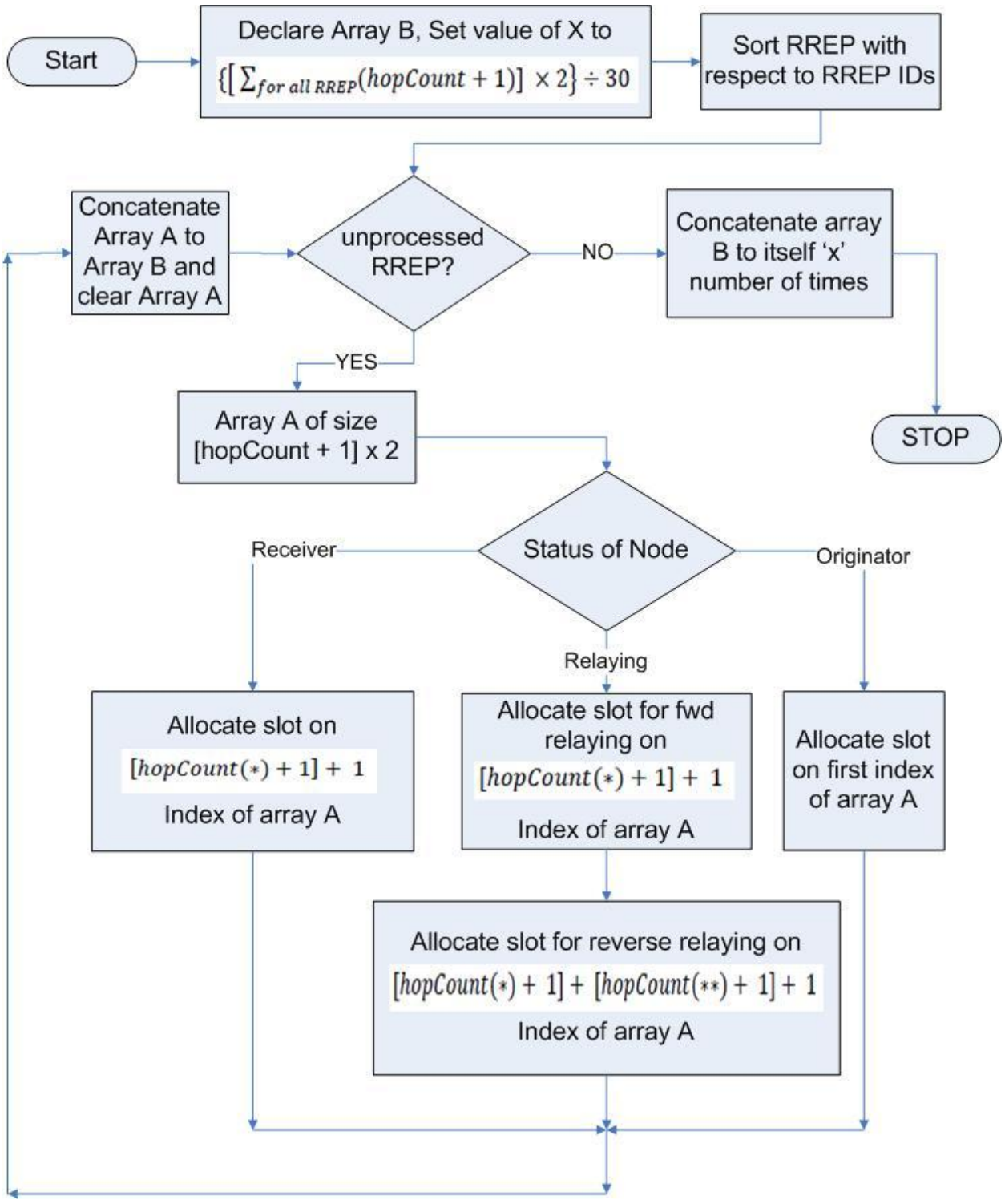

Figure 16: Flow chart diagram for slot allocation algorithm

After this every node will have a same allocation vector and every node will have knowledge of which slot is being occupied by which node. The allocation vector for above topology will be

Table 11: Slot Allocation Vector

2	3	4	5	4	3	2	3	4	5	4	3	2	3	4	5	4	3	2	3	4	5	4	3	2	3	4	5	4	3

As can be seen from the allocation vector it is very obvious that the bandwidth utilization is maximum in our case.

If we plot 30 frames of this allocation we get a graph like this

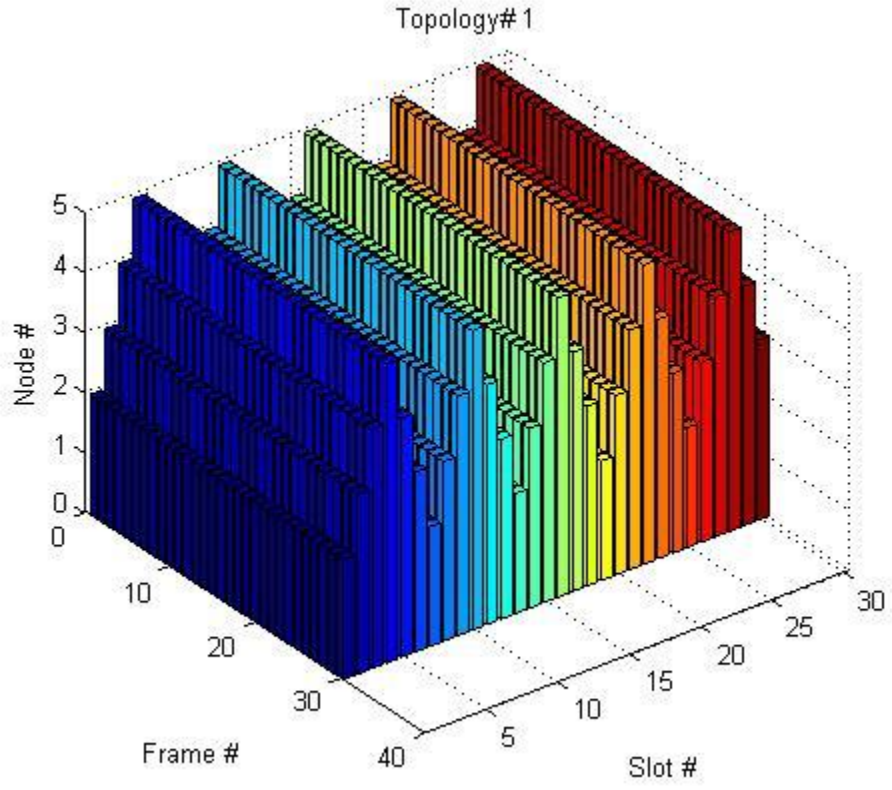

Figure 17: 30 data frames according to slots allocated by the algorithm

Node axis shows the node which occupied the slot. Slot axis shows 30 slots and Frame axis shows the number of frames (just first 30 frames out of a super frame are shown.

If it has been the traditional TDMA it would have been using just 4 slots in one frame but our design is using all 30 slots. It might not be the case always that our design make 30 slots out of all topologies and all kind of node communication but still it guarantee maximum utilization of the slots as we will see in the next chapter.

One of the other changes that we made to make our design work even better is to send multiple AODV control messages in one TDMA slot. As we see that in one frame a node get only one slot to send control messages but it might happen sometimes that a node has more than one control messages in a queue to transmit, so if a node has more than one control messages in its queue, it will need that number of frames to transmit all the messages. But we also know that the control messages are light and contain a very small piece of information while we also know that we can transmit much more amount of data in a slot than a single control message contain. So instead of waiting for the next frame to send the control messages waiting in the queue we have made a node to send all the queued messages in a single slot. This way we made the exchange of control information fast and decreased the number of control frames required which in turn reduced the call setup time.

CHAPTER 4: RESULTS AND DISCUSSION

In this chapter we are going to present the results that we obtained from our work. We are going to present the result that we obtained when we ran our algorithm for different topologies and show how our algorithm worked on different type of topologies and how it worked when the topologies were changing. We will also compare our design with the others as were presented in Chapter 2 to show how it is working better than that. We have divide this chapter to present the results in the form that first we will show that the algorithm that we have designed is working fine, then we will present the best case in which it give the maximum advantage to use. Then we will discuss the worst case during which the maximum slots are not used and then will discuss the constraints of our algorithm.

4.1. Results of the work

In this section we have just took a random topology just to test if the algorithm is working fine. We have just taken a random topology and tested our algorithm on it. The topology is shown in Figure 18

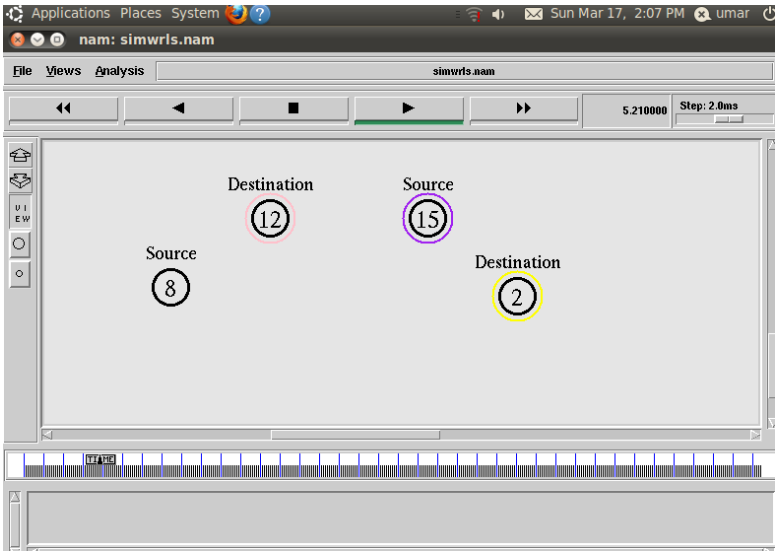

Figure 18: Topology with marked source and destination for testing algorithm

The design is such that first the node 8 wants to communicate with node 2 and node 15 wants to communicate with node 12. This is the average case topology in which the bandwidth utilization is such that only two slots in a frame are wasted in every data frame. The result that we obtained from the implementation of our algorithm on this topology is shown in Figure 19. The result shows the slot allocation that our algorithm did based on information that a node has in its routing table and from the RREP messages. We can see from the results that using our algorithm the bandwidth utilization is clearly much more than the traditional TDMA slot allocation and only two slots are being wasted per data frame. Has it been the traditional TDMA the 26 slots would have been unused which our algorithm assigned to the nodes as these slots are free due to inactivity of other nodes. So looking at this we can say in this case our algorithm increased the throughput 7 to 8 times than the traditional protocol.

These results shown in Figure 19 proves the working of our algorithm that our design is working well and the nodes are able to find the free slots and use them to increase the throughput.

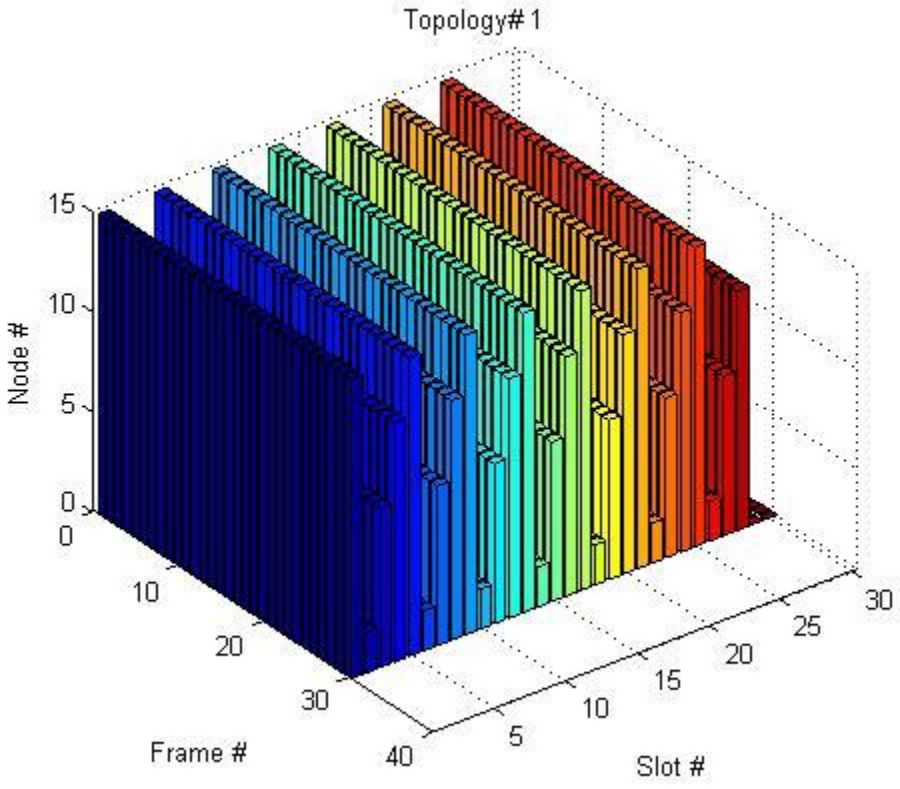

Figure 19: slot allocation for the topology of Figure 18

4.2. Best Case Results

In this section we will discuss our best case scenario. By the best case scenario we mean that all the 30 slots are being used and nothing is wasted. As our algorithm works on the repetition logic i.e. it calculates the slots and their sequence and then replicates them until it fills maximum slots. So the cases in which the number of slots that are to be replicated are divisors of 30 then those cases make best case and will use all the slots e.g. if the slots calculates are 2, 3, 5, 6, 10 and 15 then all the slots will be used.

The first scenario for the best case would be any if only two nodes are communicating with each other (while other nodes are inactive) and are at a hop distance of zero, mean they are directly in the radio range of each other. So at most two slots are needed for this communication. One for source to destination and other for the destination to the source. So our algorithm utilizes the other slots which are free and as the originally two slots were required so rest 28 slots are also used by our algorithm by replicating these two slots to other remaining slots.

We have presented two scenarios in Figure 20 and Figure 22 where only two nodes are communicating and will show the slot allocation that result from our algorithm.

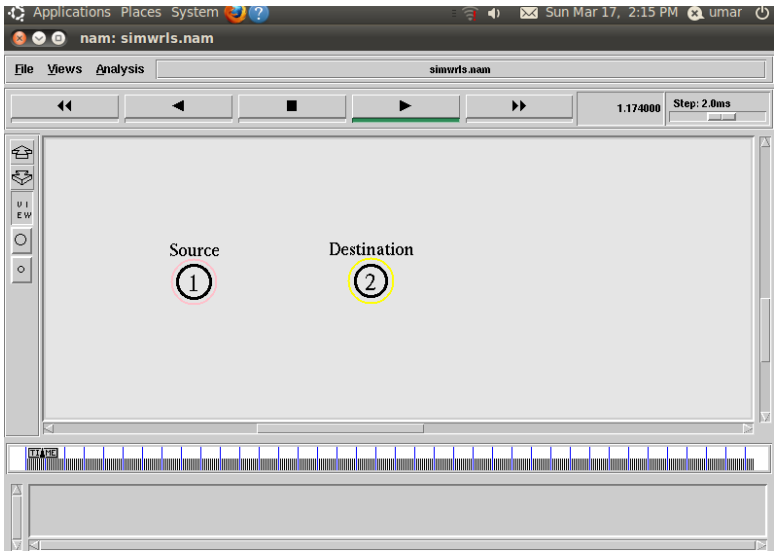

Figure 20: Best Case Scenario 1

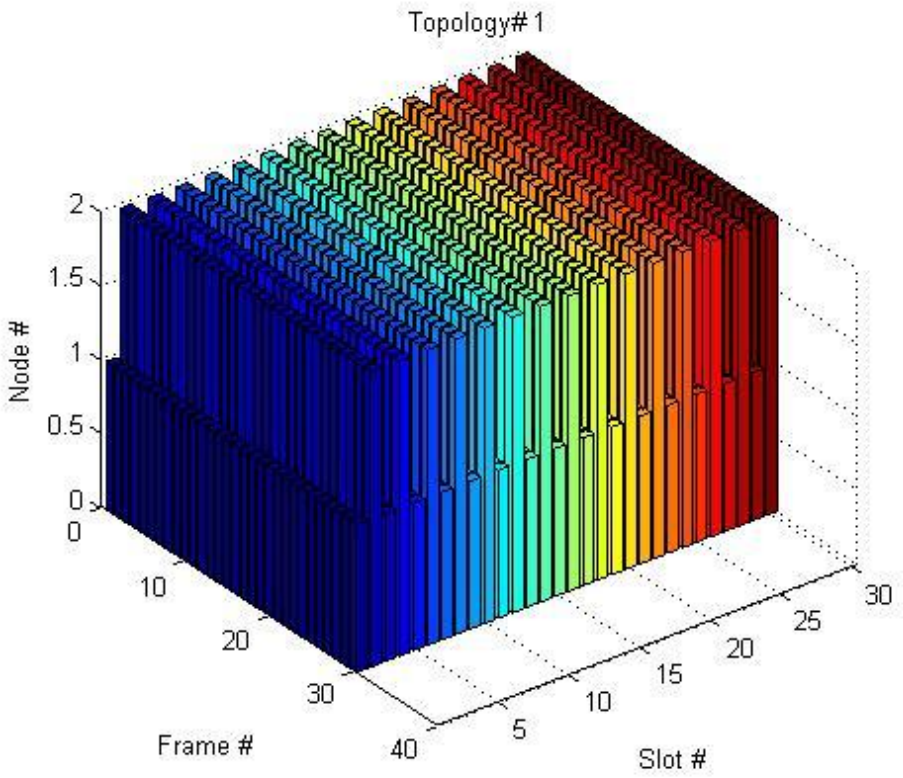

Figure 21: Result of slot allocation for best case scenario 1

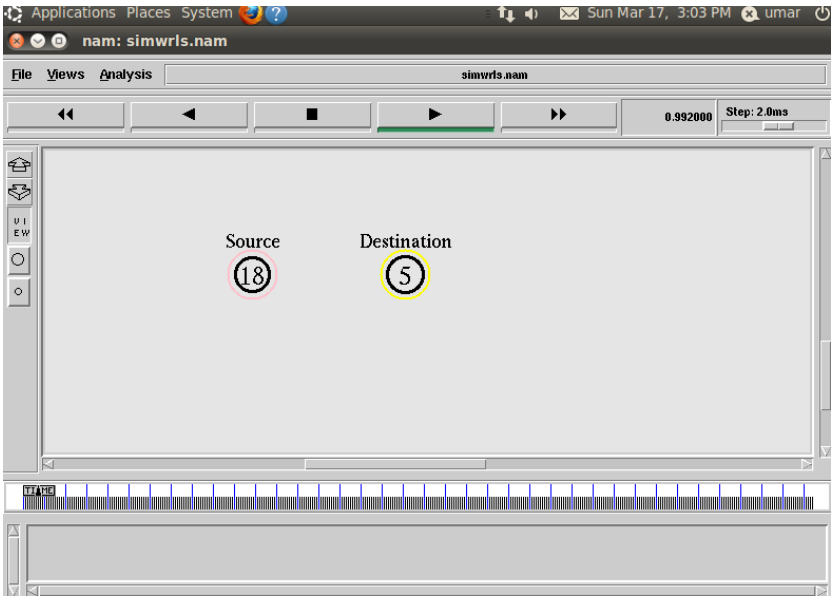

Figure 22: Best Case Scenario 2

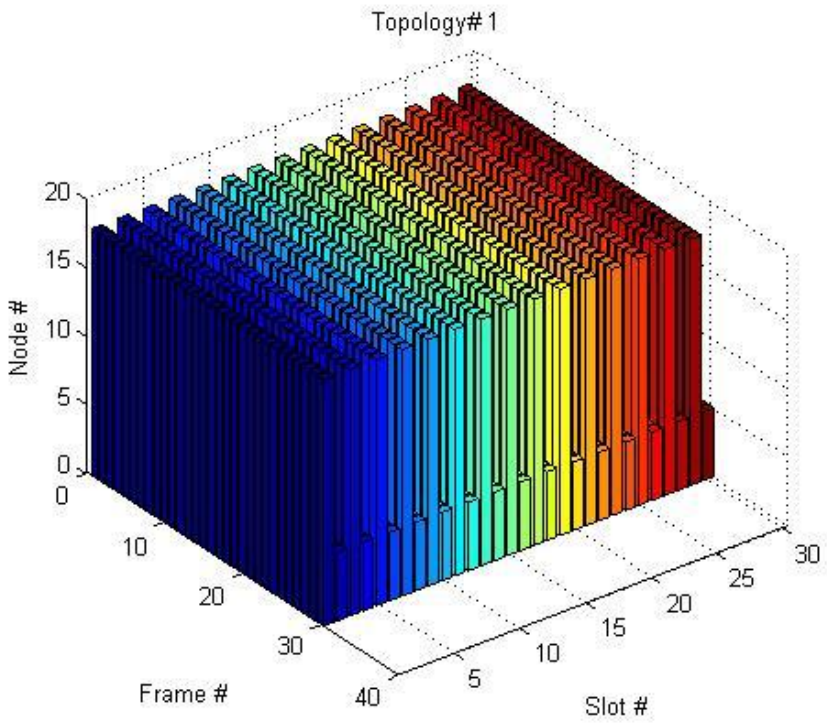

Figure 23: Result of slot allocation for best case scenario 2

One case is when there are two hops between sender and receiver then it require 6 slots to take the data to receiver and get back so our algorithm finds out the slots and replicate is 5 times to fill in all the 30 slots. One such scenario is shown below in Figure 24

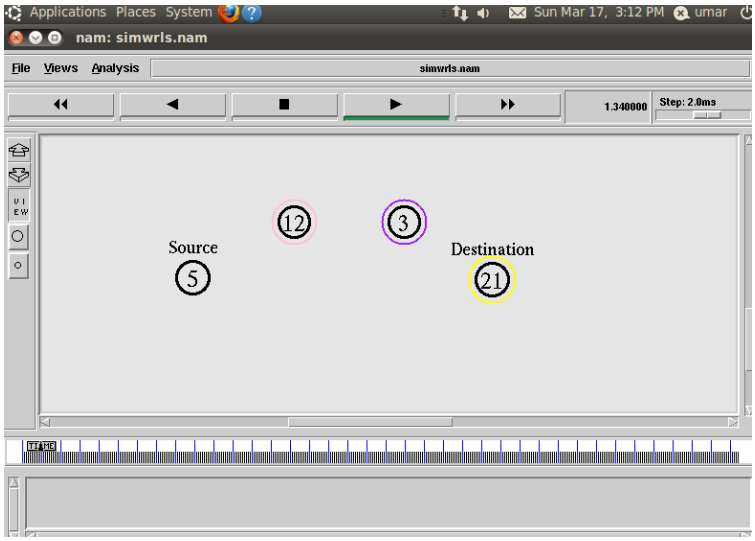

Figure 24: Best Case Scenario 3

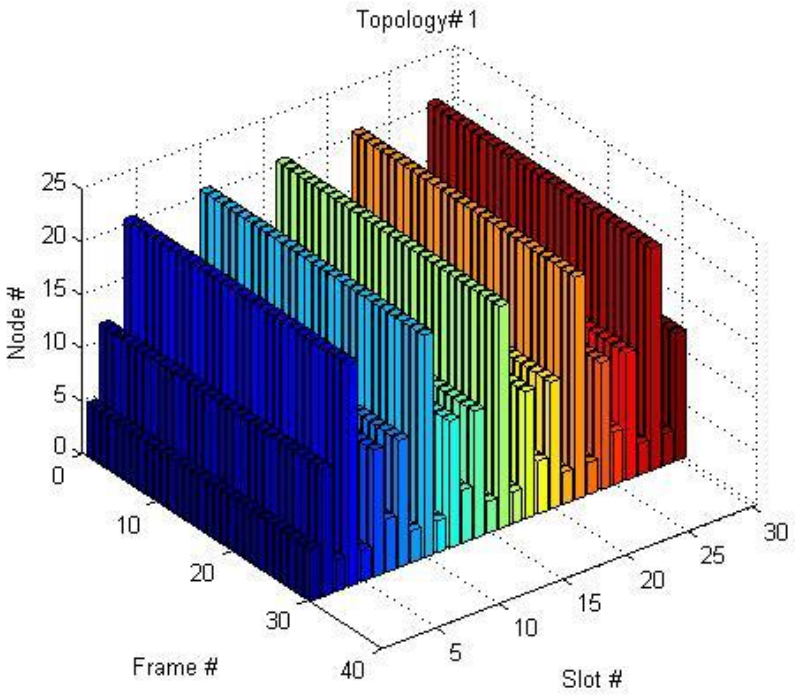

Figure 25: Result of slot allocation for best case scenario 3

Another best case can be when one communication is at a distance of one hop and other is zero hops as shown below in Figure 26. In this scenario node 9 wants to communicate with node 25 and node 18 wants to communicate with node 9.

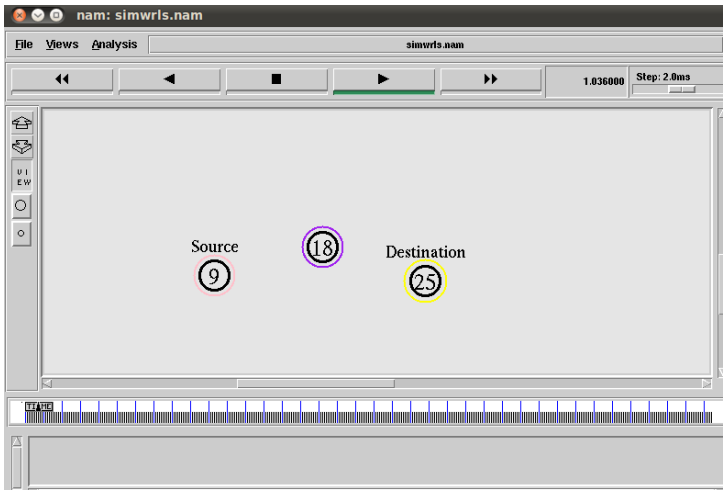

Figure 26: Best Case Scenario 4

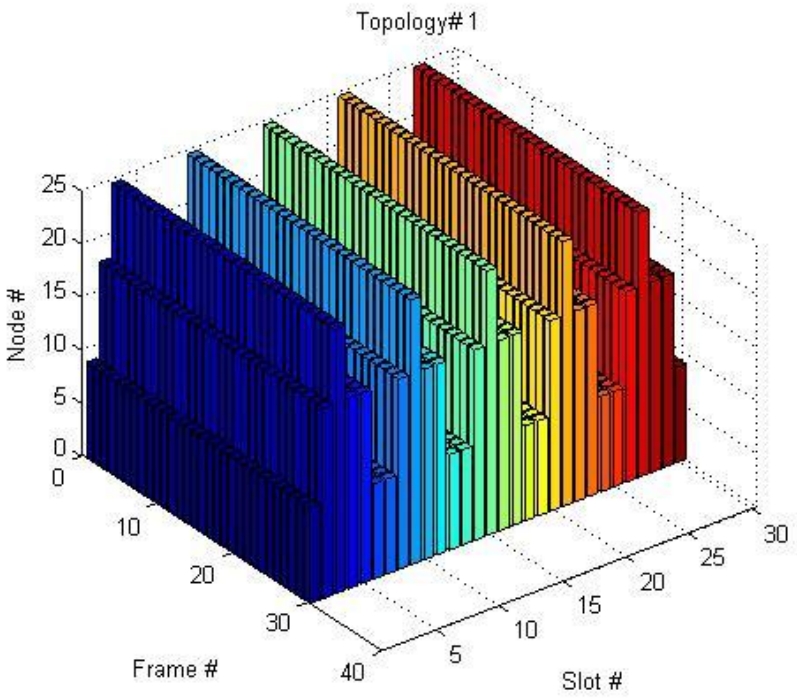

Figure 27: Result of slot allocation for best case scenario 4

4.3. Worst Case Results

In this section we will discuss the cases that in which our algorithm performance is less than the expected. We will present the cases when there is still some wastage of bandwidth due slots left unallocated. As we are assuming in our work that not more than two communications can occur at the same time so the worst case is one communication with two hop distance and another with zero hop requiring a total of 8 slots and replicating these will fill only 24 slots with a wastage of 6 slots.

Three worst case scenarios are presented in Figure 28, Figure 30 and Figure 32.

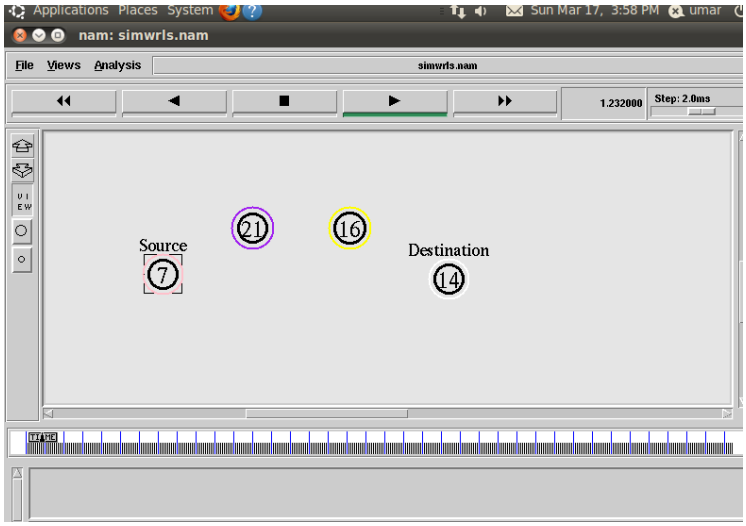

Figure 28: Worst Case Scenario 1

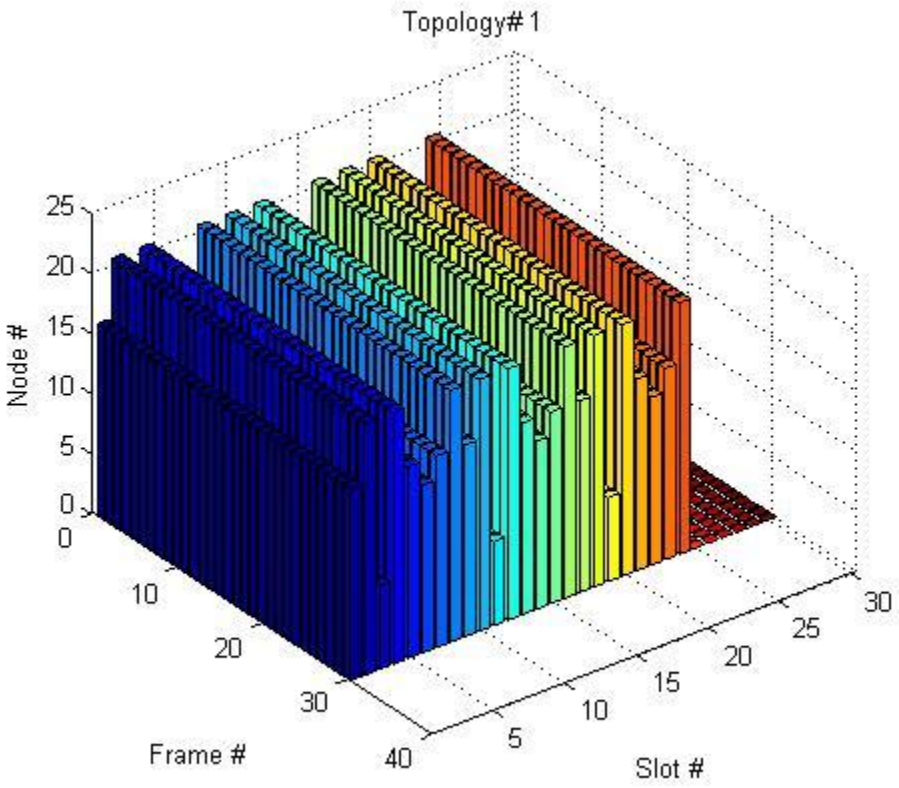

Figure 29: Result of slot allocation for worst case scenario 1

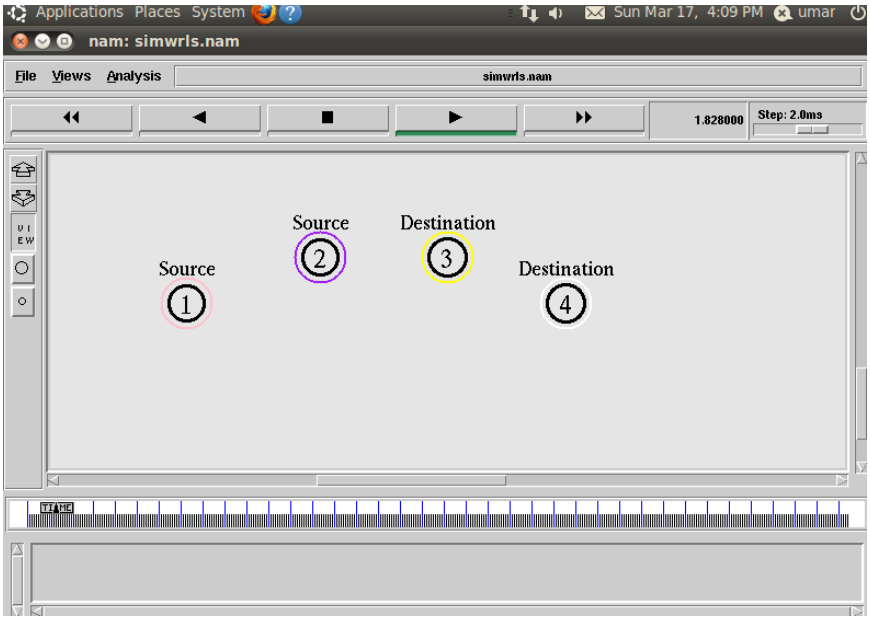

Figure 30: Worst Case Scenario 2

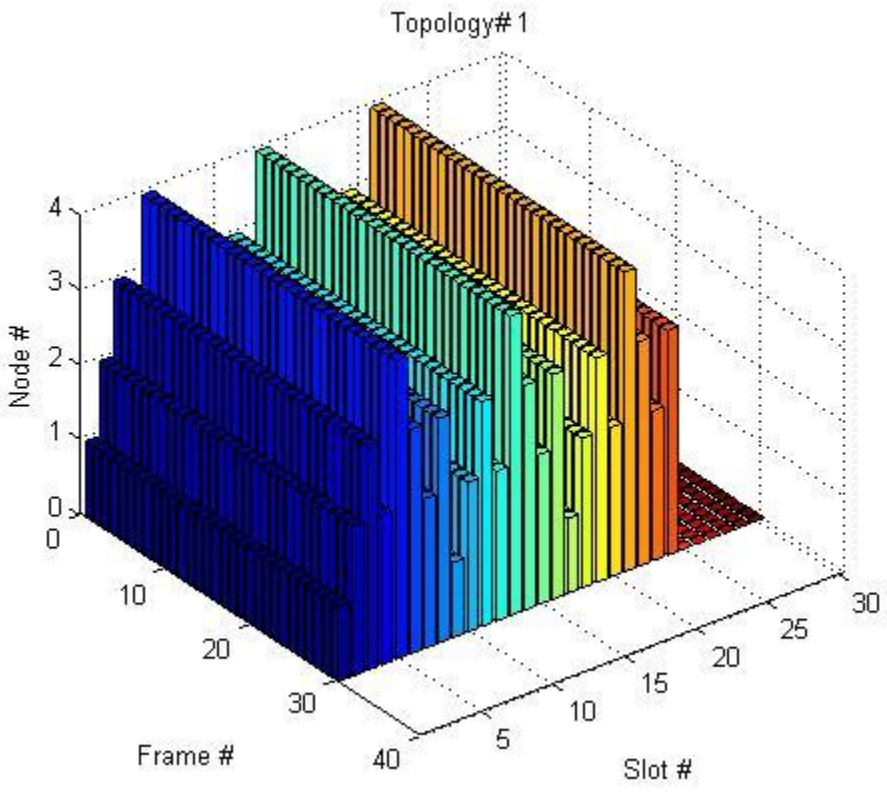

Figure 31: Result of slot allocation for worst case scenario 2

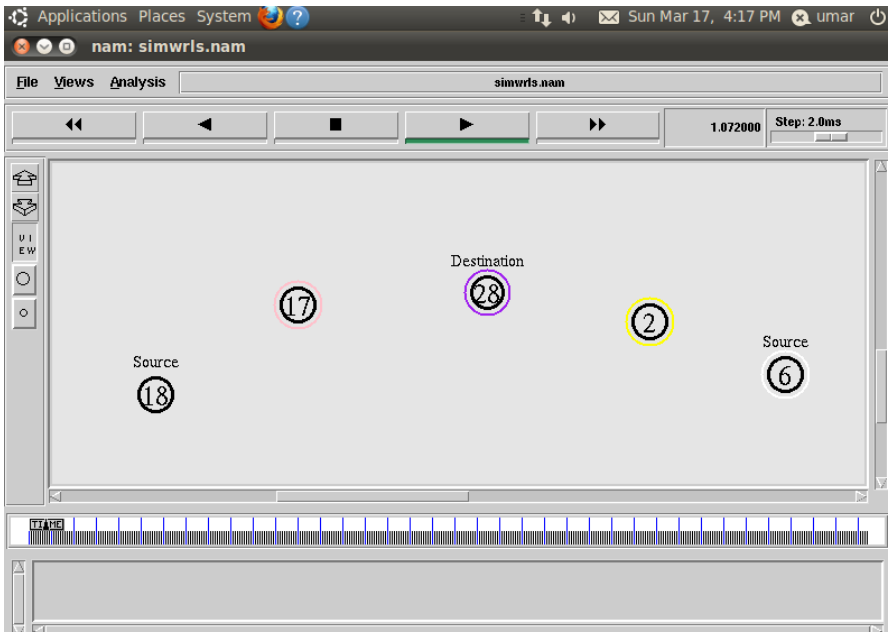

Figure 32: Worst Case Scenario 3

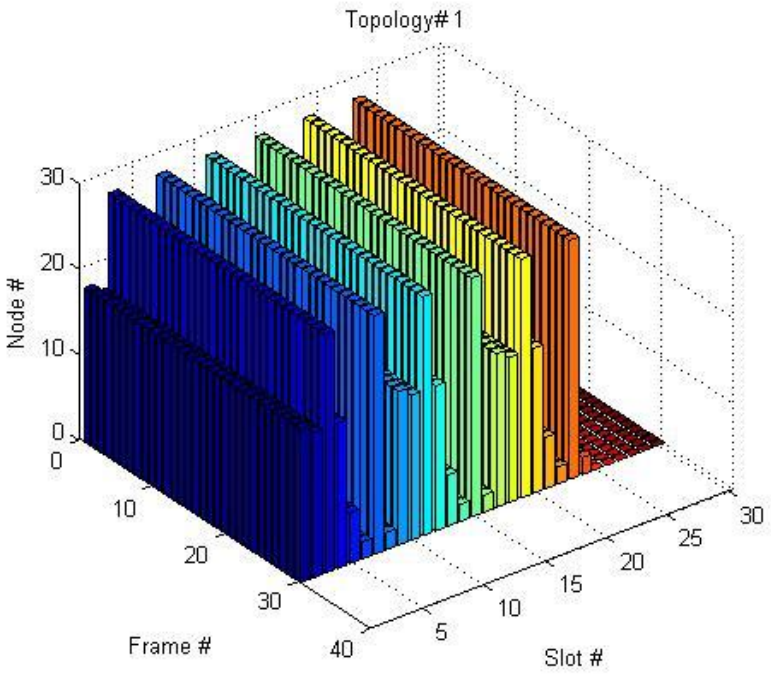

Figure 33: Result of slot allocation for worst case scenario 3

4.4. Comparison with Existing Techniques

After we have proposed a new algorithm and tested that it is working fine, we have compared it with some existing technique to see if have improved something or optimized something. Though there is no exact existing technique with which we can directly compare our results still we have compared it with existing TDMA technique and our results are much better than the existing TDMA with respect to bandwidth utilization and throughput.

To compare our results we have considered the same topology that we have used to explain the working of our algorithm. Now we will compare bandwidth, throughput and delay one by one

4.4.1 Bandwidth

We plotted the slot allocation used by the TDMA protocol (static allocation) and the results are shown below in the Figure

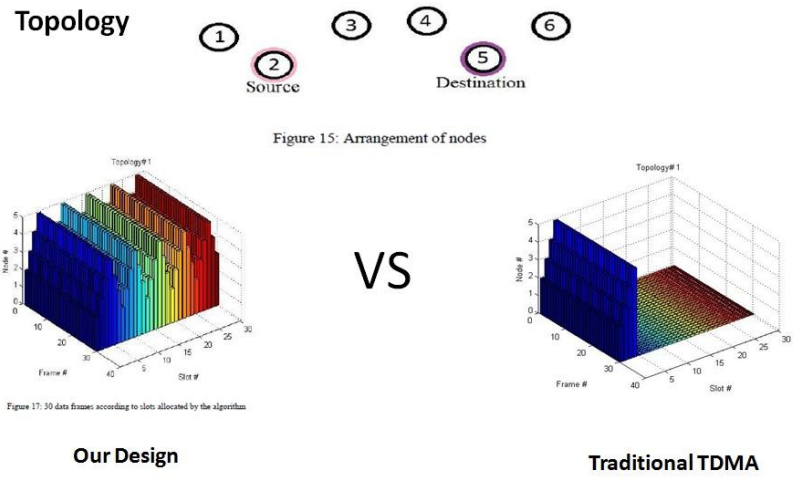

Figure 34: Comparison of Traditional TDMA with our Technique

Even if we don't explain, the results are pretty obvious. Now it depends upon the number of active nodes in the topology. In traditional TDMA the more the number of active nodes more will be the bandwidth utilization. While in our case bandwidth utilization will remain the same but the number of slots that are allocated to a node will decrease as the number of active nodes increase.

4.4.2 Throughput

Considering the other conditions as normal and finding the data than can be sent through the system.

To compare throughput we have calculated that the number of bits that can be transmitted in one slot are 490 excluding 150 bits of overhead for headers. So in case of traditional TDMA node 2 gets to send 490 bits of data in 30 slots (one frame) and if we have 36 frames (one super frame including 6 control frames and 30 data frames) and one frame is 330 ms long then node 2 can send (490 x 30) bits of data in (330 x 36) ms of time. So the throughput is 1.23 kbps.

Now in case of our algorithm for the topology that is discussed in Figure above node 2 gets 5 slots to send data in 30 slots (one frame) and if we have 36 frames (one super frame including 6 control frames and 30 data frames) and one frame is 330 ms long then node 2 can send (490 x 5 x 30) bits in (330 x 36) ms of time with a throughput of 6.18 kbps. Below is the figure showing comparison of the throughput of our technique with traditional TDMA showing the change in throughput in case of one source and destination if number of hops between them increases increase.

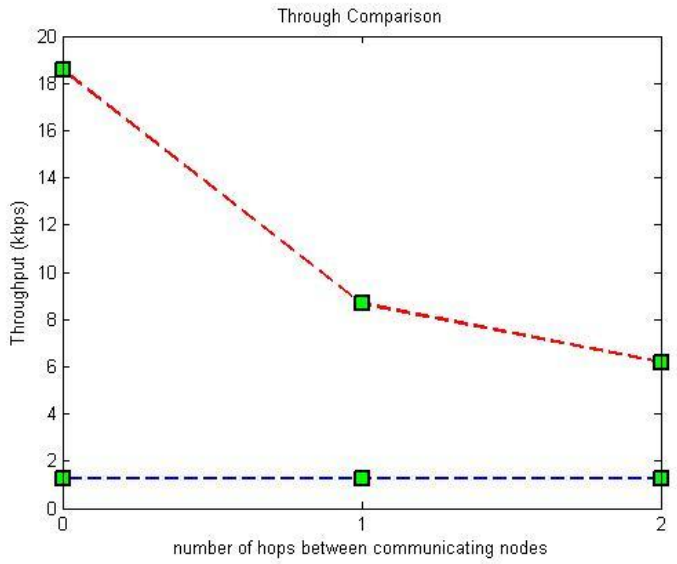

Figure 35: Throughput Comparison of our Technique with Traditional TDMA

4.5. Constraints

There are some constraints that we kept while designing the algorithm. One of the main constraints that we kept in our minds before designing was that there can be at most two simultaneous conversations. That is not more than two nodes can put a request to communicate at the same time. Second constraint that we kept in mind was that the destination node cannot be more than two hops away, means the destination node that is at a distance of more than two hops will be considered as unreachable.

CHAPTER 5: CONCLUSION AND FUTURE WORK

In this chapter we are going to briefly conclude our work. We will discuss it briefly from different aspects. Then we will identify some of the future work that can be done based on the work that we have done. As we have presented a very different and new idea so there are a lot of options for the future work and our current work is in a very early stage and it can lead to further design modifications and its implementation on the actual hardware. In the first section we will conclude our work and in the second section we will discuss about the future work.

5.1. Conclusion

In this thesis we have mainly developed an algorithm for the medium access that uses TDMA protocol. We have proposed a new design that uses layer merging of Network and MAC layer and use the information that is there in the AODV routing protocol control messages along with the information in the routing table and frame information and enables a node to decide which slot in the TDMA frames are to be used and which to be left for the other nodes. In our design a every node passes through two phases, in the first phase all of the nodes share control information in TDMA control frames using AODV control messages and after that, using the information that it has acquired during the exchange of control messages it run our algorithm and then decides itself that which of the slots it can acquire. Our design provides a collision free communication among nodes in a fast moving tactical network.

As it is already mentioned that the work in area of tactical networks has not been published as it is highly confidential. In our work we have first studied different routing protocols for ad-hoc networks and selected AODV to be used in our design as it is best for ad-hoc networks and is reactive and save memory, and then we studied the TDMA protocol and its working and its limitations. After thorough study of these two protocols on network and MAC layer we identified the simplicity of AODV protocol and modified its control messages to carry a little bit more information that can be very useful for some calculations and targeted the wastage of bandwidth in TDMA as slots remain unused since not all the nodes are active all the time.

Then we studied about cross-layer and merged-layer design and found out that work has been done to improve network performance by using information of one layer in another layer e.g. the signal strength information can be used by network layer to decide the route to the destination from hop whose signal strength is good. After the study of different cross-layer designs we decided to design something new i.e. instead of crossing the information among layers we decided to fully merge the network and MAC layers.

We have designed a new algorithm that decides about which slot a node can use by utilizing the information exchanged in control messages of AODV protocol. Now there is only one layer that is performing the duties of both network and MAC layer and the information that was being used by the network layer in the standard design is now directly being used on the MAC layer for the decisions. In our design we have divided a TDMA super frame into two types. One set of frames are called control frames and other data frames. During the control frames there is no slot reuse and every node can transmit only in its own slot. After the control frames every node runs our algorithm and find the slots that it will use. Then during the data frames every node uses the slots it calculated using the algorithm. This way our design make use of the simplicity of the AODV control messages and reuse the slots of the inactive nodes and provide a collision free communication using a merged layer design.

5.2. Future Work

The work that has been presented in this thesis is in its very initial stage. So there is a big scope for the future work from this thesis. We have just posed a new idea of merging of layers and developed an algorithm to allocate slots that efficiently utilizes the bandwidth. We have just simulated our work to test its working however a lot of work is still to be done to port this idea to the actual implementation. Some of the key future works that can be done out of this thesis are to solve the synchronization issue, to write a new layer which performs the functions of both network and MAC layer and make a simulation using some advanced tool like NS-3 or Opnet using the new merged layer.

REFERENCES

[1] Link Layer Design for a Military Narrowband Radio Network, Svein Haavik and Bjornar Libæk, Norwegian Defence Research Establishment (FFI), P.O. Box 25, NO-2027 Kjeller, Norway

[2] Cross-Layer Design for Data Accessibility in Mobile Ad Hoc Networks, KAI CHEN, SAMARTH H. SHAH and KLARA NAHRSTEDT, Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, IL 61801, U.S.A.

[3] Cross-Layer proposal for QoS Routing in Mobile Ad-Hoc Networks, María Canales, José Ramón Gállego, Ángela Hernández-Solana, Antonio Valdovinos, Communications Technology Group, University of Zaragoza. Zaragoza, SPAIN

[4] Performance Analysis of Cross Layer AODV for Heterogeneously Powered Ad-hoc Networks, B.Ramachandran Dept. of ECE S.R.M. Institute of Science and Technology Chennai- 603 203, S.Shanmugavel Dept. of ECE Anna University Chennai- 600 025

[5] A Cross-Layer AODV Routing Protocol Zhi Ren and Jing Su Wei Guo School of Communication and Information Engineering School of Communication and Information Engineering University of Electronic Science and Technology of China University of Electronic Science and Technology of China Chengdu, Sichuan Province, 610054, China Chengdu, Sichuan Province, 610054, China

[6] http://www.ietf.org/rfc/rfc3561.txt

[7] http://www.ee.cityu.edu.hk/~schan/allocation-mag.pdf

[8] www.cs.tut.fi/kurssit/TLT-2756/lect04.pdf

[9] http://en.wikipedia.org/wiki/Time_division_multiple_access

[10] S.A. Jafar and A.J. Goldsmith, "Beamforming Capacity and SNR Maximization for Multiple Antenna Systems with Covariance Feedback", in Proc. of IEEE Vehicular Technology Conference, May 2001.

[11] J.N. Laneman and G.W.Wornell, "Energy-Efficient Antenna Sharing and Relaying for Wireless Networks", in Proc. of IEEE Wireless Communications and Networking Conference, September 2000

[12] P.R. Kumar, “New Technological Vistas for Systems and Control: The Example of Wireless Networks”, IEEE Contro System Magazine, Vol. 21, No. 1, pp. 24–37, 2001

[13] Q. Zhao and L. Tong, “Semi-Blind Collision Resolution in Random Access Wireless Ad Hoc Networks”, IEEE Trans. on Signal Processing, Vol. 48, No. 9, 2000.

[14] S. Vishwanath and A.J. Goldsmith, “Optimum Power and Rate Allocation Strategies for Multiple Access Fading Channels”, in Proc. of IEEE Vehicular Technology Conference, 2001.

[15] J. Chen, K.M. Sivalingham, P. Agrawal and S. Kishore, “A Comparison of MAC Protocols for Wireless Local Networks Based on Battery Power Consumption”, in Proc. of IEEE INFOCOM’98, March 1998.

[16] J. Gomez, A.T. Campbell, M. Naghshineh and C. Bisdikian, “PARO: Power-Aware Routing Optimization for Wireless Ad Hoc Networks”, in Proc. of IEEE 9th International Conference on Network Protocols (ICNP2001), Riverside, California, November 2001.

[17] S. Singh, M. Woo and C.S. Raghavendra, “Power-Aware Routing in Mobile Ad Hoc Networks”, in Proc. Of ACM MobiComm ’98, October 1998.

[18] S. Chen and K. Nahrstedt, “Distributed Quality-of-Service Routing in Ad-Hoc Networks”, IEEE Journal of Selected Areas in Communication, Vol. 17, No. 8, 1999.

[19] S.-B. Lee, G.-S.Ahn, X. Zhang and A.T. Campbell, “INSIGNIA: An IP-Based Quality of Service Framework for Mobile Ad Hoc Networks”, Journal of Parallel and Distributed Computing, Vol. 60, pp. 374–406, 2000

[20] Y.-C. Hu and D.B. Johnson, “Catching Strategies in On-Demand Routing Protocols for Wireless Ad Hoc Networks”, in Proc. of ACM MobiComm 2000, August 2000.

[21] B. Liang and Z.J. Haas, “Predictive Distance-Based Mobility Management for PCS Networks”, in Proc. Of IEEE INFOCOM ’99, March 1999

[22] R. Castaneda and S.R. Das, “Query Localization Techniques for On-Demand Routing Protocols in Ad Hoc Networks”, in Proc. of ACM MobiComm ’99, August 1999.

[23] Y. Ko and N. Vaidya, “Location-Aided Routing (LAR) in Mobile Ad Hoc Networks”, in Proc. of ACM MobiComm ’98, October 1998.

[24] Zhu, C., Corson, M.S., “QoS Routing for Mobile Ad Hoc Networks” in Proc. IEEE INFOCOM’02, New York, USA, June, 2002.

[25] Haas, Z.J., and Jing Deng, “Dual busy tone multiple access (DBTMA) –a multiple access control scheme for ad hoc networks”, IEEE Transactions on Communications. Vol 50, issue 6, pp 975-985, 2002

[26] IEEE Standard 802.11 part 11, 1999: Wireless LAN MAC & PHY Layer Specifications

[27] Design and Simulation of Dynamic Slot Allocation Protocol for TDMA on Tactical, Internet, Shibai Yin, School of Information Engineering, Chang An University, Xi' An ,china, ruby1984xait@sina.com