IMPACTS AND MINIMIZATION OF INTERFERENCE IN ADHOC NETWORK

By

Christer Andrews
and
Jannatul Ferdous Kakon

Submitted to the

Department of Electrical and Electronic Engineering
Faculty of Sciences and Engineering
East West University

in partial fulfillment of the requirements for the degree of
Bachelor of Science in Electrical and Electronic Engineering
(B.Sc. in EEE)

[Summer, 2012]

Approved By

_____	_____
Thesis Advisor	Chairperson
Fakir Mashuque Alamgir	Mohammad Mojammel Al Hakim

Approval

The thesis titled ‘Impacts and Minimization of Interference in Adhoc Network’ submitted by Christer Andrews (2008-3-80-012) and Jannatul Ferdous Kakon (2008-3-80-003) in the semester of summer 2012 is approved as satisfactory in partial fulfillment of the requirements for the degree of Bachelor of Science in Electrical and Electronic Engineering.

Mohammad Mojammel Al Hakim
Chairperson, Dept. of Electrical and Electronics Engineering
East West University, Dhaka

Declaration

We, hereby declare our thesis work solely to be our own scholarly work. To the best of our knowledge, it has not been shared from any source without due acknowledgement and permission. It is being submitted in partial fulfillment of the requirements for the degree of Bachelor of Science in Electrical and Electronic Engineering. It has not been submitted before for any degree or examination in any other university.

_____

Christer Andrews

_____

Jannatul Ferdous Kakon

Summer Semester
August'2012

Abstract

A wireless adhoc network is a new archetype in wireless communication which doesn't require any fixed infrastructure such as base stations or mobile switching centre. Reducing interference is one of the main challenges in wireless ad hoc networks. The main aim of this thesis is to study various issues pertaining to wireless adhoc network and find ways to diminish the interference effect in this network. Starting with basic knowledge of adhoc networks, its applicability, security issues, and this thesis digs into details of existing research works in minimization of interference effect in adhoc network. Next the thesis work focuses on new ways to lessen the interference effect in adhoc network. A new solution is proposed to achieve our main goal which is both cost effective and simple. It is observed that the proposed minimization technique is a good one.

Keywords: Ad Hoc, Interference, Base Station.

Acknowledgements

We would like to express our heartiest and most sincere gratitude to our supervisor, Mr. Fakir Mashuque Alamgir, Lecturer, Department of Electrical and Electronics Engineering, East West University for his intelligent and well thought suggestions. He provided us with every bit of support he could manage. We were allowed to work on our own and whenever we lost our way, he guided us back to track with patience and interest.

We also wish to thank Mr. Avi for providing us unconditional support with his laptops for simulation purpose.

Authorization page

We hereby declare that we are the sole authors of this thesis. We authorize East West University to lend this thesis to other institutions or individuals for the purpose of scholarly research.

_____

Christer Andrews

_____

Jannatul Ferdous Kakon

We further authorize East West University to reproduce this thesis by photocopy or other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

_____

Christer Andrews

_____

Jannatul Ferdous Kakon

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

CHAPTER 1: Review of Networking

1.1. Network fundamentals:

1.1.1. Introduction

A network consists of two systems directly connected by a physical link such as a cable or wireless channel which allows them to communicate with each other. There are two types of networks:
LAN: Local Area Network
WAN: Wide Area Network.

Differences between LAN & WAN:

a) LANs typically cover shorter distances than WAN.
b) In a LAN each network host is connected to a common communication channel whereas WANs are characterized by point to point links between hosts.

Disadvantages of early Ethernet implement:

a) A single Ethernet cable had to connect all the stations.
b) Inserting a new host into the network involved breaking the cable connection resulting in a temporary loss of network connectivity.

However modern Ethernet implementations use a hub or switch as the common communication channel.

1.1.2. Some important terms

- **Wireless network**: Wireless network refers to any type of computer network that is not connected by cables of any kind. It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless communications networks are generally implemented and administered using a transmission system called radio waves. This implementation takes place at the physical layer of the OSI model network structure.

- **Topology**: The topology of a network describes the way in which devices are connected together.

- **Logical topology**: It is a network computing term used to describe the arrangement of devices on a network and how they communicate with one another.

- **Physical topology**: It defines how devices are connected to the network through the actual cables that transmit data, or the physical structure of the network.

- **Network protocol**: A common language and a set of rules governing the conversation are required for two or more to communicate across a network. The language and the rules collectively are known as a network protocol.

- **Protocol data units (PDU)**: The data exchanged between peer layers is divided into discrete units called PDU. The PDU is made of a section and the data payload.
  The header section contains important control information that will be used by the receiving peer layer. This information will include address fields which will tell the peer layer where to deliver the data.

- **Service Data Unit (SDU)**: It is a specific unit of data that has been passed down from an OSI layer to a lower layer and which the lower layer has not yet encapsulated into PDU. An SDU is a set of data that is sent by a user of the services of a given layer and is transmitted semantically unchanged to a peer service user.

- **Data flow**: Each receiving peer layer will strip off and read the header added by the sending peer. It will then deliver the data payload to the appropriate higher layer protocol or forward the data to another destination.

- **Multiple Protocol Stacks**: A lower layer may need to accept PDUs from multiple protocols at the layer above. This is known as multiplexing. It will also have to deliver

incoming data payloads to the appropriate higher layer protocol which is known as demultiplexing.

- **Protocol number**: The numeric identification of the upper layer protocol that an IP packet should be sent to.

- **Internet protocol**: The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

- **Routing Protocol**: A routing protocol is a protocol that specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network, the choice of the route being done by routing algorithms. Each router has a prior knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network.

- **Modal dispersion**: It is a process where a pulse is caused to disperse as it passes down the fibre in Multimode fibre.

- **The Internet**: It is a worldwide interconnection of networks using TCP/IP (Transmission Control Protocol/ Internet Protocol) – a set of networking protocols which allows communication between remote systems.

- **Bandwidth:** The size of the available range of frequencies.

- **Repeaters**: Repeaters are devices that operate at the physical layer. It acts at the Physical layer to restore the magnitude and quality of electromagnetic signals.

- **Attenuation**: The weakening of the signal as it propagates down the cable.

- **Interference**: Picking up stray electromagnetic radiation by the wire cables from neighboring communication cables

- **Thermal Noise**: Cables generate random electrical signals due to their thermal energy.

- **Distortion**: If the properties of the cable are not ideally matched to the signal, the shape of the signal can change as it propagates through the cable.

- **Hubs**: There are two types of hubs. They are:

- **Passive hubs**: The hubs which do not have an independent power supply are known as passive hubs. It will simply take a signal that arrives at one port and replicate it to the other ports.

- **Active hubs**: Hubs with their own power supplies are known as active hubs. It also functions as repeaters, boosting the signal before forwarding to other ports.

- **Bridges:** Bridges connect physically separate network segments together to form a single LAN. They do not forward all the frames from one network segment to another. They examine the header of each frame to determine the source and destination MAC addresses. In this way they build tables of which MAC addresses belong to each segment. They then use this information to determine whether to forward a frame or not.
  Bridges operate at the Data link layer, using frame header information.

- **Spanning Tree Protocol (STP)**: This allows bridges to stop forwarding frames on some of their interfaces to create a loop free network. If a bridge fails, the remaining bridges can reactivate some of their interfaces to ensure that all network segments are still connected.

- **Wireless Access Points (WAP):** Wireless Access Points forward frames between end stations in a WLAN. It also carries out some processing based on the data in the frame, such as MAC address filtering and authentication, which are used to implement security. They forward packets towards remote network destinations, based on the contents of their routing tables.

- **Brouters**: A Brouter is a device that performs the functions of both a bridge and a router. It can be used to forward frames or packets between two network segments. Routers never forward broadcast packets.

- **Gateways**: Gateways allow systems to communicate with each other when using programs that are similar in function, but which are based on different underlying protocols, and so cannot communicate directly. Gateways can operate at OSI layers 4 to 7.

Table 1: Devices used in OSI Layer [30]

OSI Layer	Device
Application	Gateway
Presentation	
Session	
Transport	
Network	Router, Brouter
Data Link	Bridge. Switch, Access Point
Physical	Repeater, Hub

- **Basic Ethernet operation:** When a station sends a frame to another station, it includes the destination MAC address in the frame header. Every station reads this address. Only the station with the destination address reads the rest of the frame. Each end of the cable is terminated by a 50 ohm resistor in order to prevent signals from being reflected back from the end of the cable and corrupting data.

- **Collision:** It can happen that two stations, detecting no traffic on the channel, both start transmitting. In this case the signals will overlap and the frames will be corrupted. This is known as collision.

- **Crosstalk:** One of the main source of interference in a twisted pair cable is neighboring wire pairs which can radiate away some of the energy from their signals. This form of interference is called crosstalk.

- **Fibre – Optic cabling:** It consists of a central glass core surrounded by a cladding also made of glass, which is surrounded by a protective plastic coating. The optical properties of the core and cladding are made to differ in such a way that light entering the core is totally internally reflected at the boundary between core and cladding. Signals are transmitted by modulating a light source at one end of the core and detecting it at the other end.

- **Multimode Fibre (MMF):** The fibre is typically 50 or 62.5 microns in diameter. A micron is one millionth of a meter.

- **Single mode Fibre (SMF):** This fibre is 9 microns in diameter. It is used with longer wavelength light from a laser. So pulses do not disperse as they pass along it.

1.1.3. OSI Model

The Open Systems Interconnection model (OSI model) is a prescription of characterizing and standardizing the functions of a communications system in terms of abstraction layers. Similar communication functions are grouped in to logical layers. It breaks down the network functions into seven layers.

Table 2: The OSI Model [30]

OSI Model			
	Data unit	**Layer**	**Function**
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data
		5. Session	Interhost communication, managing sessions between applications
	Segments	4. Transport	End-to-end connections, reliability and flow control
Media layers	Packet	3. Network	Path determination and logical addressing
	Frame	2. Data link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

1.1.4. Description of OSI layers

Layer 1. - Physical layer:

It defines the relationship between a device and a transmission medium. This includes the layout of pins, voltages, cable specifications, hubs, repeaters etc. It is responsible for converting each frame into a sequence of electromagnetic bits, which can be transmitted across the communications channel. It is not concerned with the structure or meaning of the data transmitted. Physical layer specifications are concerned with the following:

- The physical characteristics of the transmission medium such as its impedance.
- How bits are represented.
- Which frequencies are used to transmit signals?
- How to determine when transmission starts and ends by transmitting certain bit patterns.

The major functions performed by the physical layer:

- Establishment and termination of a connection to a communications medium.
- Participation in the process.
- Modulation.

Layer 2. - The data link layer:

The data link layer is responsible for the transmission of data from one system to another, directly connected to it. It accepts packets from the Network layer above and encapsulates them into frames.

A frame usually has three parts:

- Header: it contains control information such as the source and destination addresses for the frame as well as the identifier of the protocol of the encapsulated packet.
- Data Payload: it consists of the encapsulated packet.
- Trailer: it usually contains a checksum used to verify the integrity of the data.

Data Link Sub layers:

The data link layer is divided into two sub layers:

1. Logical Link Control (LLC): it accepts and delivers packets from the network layer above. It allows more than one network layer protocol to be used.

2. Media Access Control (MAC): it is responsible for generating frames appropriate to the particular network interface in use. It allows more than one network adapter to be supported.

MAC addresses: In LANs, where many hosts are directly connected to each other, it is necessary to have address that uniquely identifies the destination host. Each LAN network adapter has a unique built in address called the MAC address. LAN frames carry the source and destination

MAC addresses in their headers. MAC addresses by themselves cannot be used to route data to distant networks. There are two main reasons for this:

1. Only LAN interfaces have MAC addresses. This means that it would be impossible to send frames to a remote serial interface.
2. There is a general problem of how to forward data to a remote destination.

Layer 3. - The Network layer:

The network layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network while maintaining the quality of service requested by the transport layer. It performs network routing functions. The network layer is divided into three sub layers:

1. Sub-network access: it considers protocols that deal with the interface to networks such as X.25.
2. Sub-network – dependent convergence: it is necessary to bring the level of a transit network up to the level of networks on either side.
3. Sub-network –independent convergence: it handles transfer across multiple networks.

Routers only need to know the addresses of other networks rather than the addresses of each individual host, making the routing tables much smaller and easier to update. All hosts sharing the same network address should be connected to the same physical network.

Layer 4. - The Transport layer:

The transport layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. It controls the reliability of a given link through flow control, segmentation and error control. It can keep track of the segments and retransmit those that fail.
The PDU for TCP is known as a segment, and the PDU for UDP (User Datagram Protocol) is known as a datagram.

Layer 5. - The Session layer:

The session layer controls the connections between computers. It establishes, manages and terminates the connections between the local and remote application.

Layer 6. - The Presentation layer:

It is responsible for handing data represented in different formats on different systems, as well as for encrypting and decrypting data. This layer provides independence from data representation by translating between application and network formats. This layer formats and encrypts data to be sent across a network. It is sometimes called the syntax layer.

Layer 7. - The Application layer:

The application layer defines protocols for network applications. It also identifies communication partners, determining resource availability and synchronizing communication.

1.1.5. Wireless LANs

There are two main types of WLAN:

1. Unstructured AD-HOC WLAN: It can be formed when mobile computers equipped with wireless network adapters come into close proximity for example Bluetooth devices.
2. Infrastructure WLAN: It uses fixed wireless network access points. Wireless computers can use them as wireless hubs.

WLANs use specific radio frequencies, rather than copper or fibre optic cables to transmit data.

Features of WLANs:

Security: Any PC equipped with an appropriate wireless adapter can access the radio frequencies used by WLANs.

Duplex transmission: In modern LANs using switches, full duplex transmission is possible between the switch and any PC directly attached to it.

Range: The range of WLANs is limited to a few tens of metres.

Collision handling: WLANs use a collision avoidance mechanism (CSMA/CA), which introduces delays between transmissions to ensure that collisions do not occur.

How wireless data is encoded:

Radio transmission uses a radio wave with a base frequency; this wave is modulated to carry information. Modulation involves changing some characteristic of the wave in order to encode data.
One way of modulating the wave would be to modify its amplitude. This type of modulation is known as AM (Amplitude Modulation). Another method would be to vary the frequency. This method is known as FM (Frequency Modulation). A third option is to break the pattern of the wave, moving it forwards or backwards.

Wireless Interference: In order to reduce the chances of two different systems using the same frequency at the same time, there are a number of techniques used to achieve this – FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum), OFDM (Orthogonal Frequency Division Multiplexing) and MIMO (Multiple Input/ Multiple Output).

FHSS: The sending and receiving stations switch between frequencies according to an agreed sequence. If another WLAN is using the same frequency range, the chances of both WLANs using the same frequency within that range, at the same time, are minimized.

DSSS: It mixes the data signal with a large amount of redundant information and transmits it over a number of different frequencies simultaneously. The redundant information is subtracted by the receiver to recover the original signal. The redundant information, sometimes known as the chipping code, is designed to be like white noise.

OFDM: Like DSSS, this technique spreads the signal over several frequencies simultaneously. One of the problems with using different frequencies which are close together is crosstalk, where there is interference between signals on neighboring frequencies. It ensures that there is no interference between adjacent signals even when the signals overlap.

MIMO: It is a technique used to enhance OFDM transmissions by using multiple antennas to transmit and receive signals. This increases the overall speed of data transmission.

CSMA/CD:

When a WLAN station wishes to send a frame to another station, it goes through the following steps:

1. Listen to the channel to determine if it is idle. If the channel is busy, try again later.
2. Wait for a specified time. If the channel is still idle, send an RTS (Request to Send) frame to the receiver, indicating how long the data transmission will be, in order to reserve the channel for the transmission of the data frame.
3. Wait for the receiver to send a CTS (Clear to Send) frame, confirming the reservation. This frame tells others not to transmit during the reserved interval, also known as the Network Allocation Vector.
4. Send the data frame. Then wait a specified time for the receiver to send an ACK (acknowledgement) frame.

1.1.6. Factors affecting Transmission Speed

Interference: Common sources of interference include other WLANs operating in the same, or adjacent, channels, cordless phones and microwave ovens.

Range: The distance between end stations and the access point will also affect the speed.

Physical environment: The presence of walls between a station and the access point will reduce the range of the signal.

Using different protocols in the same WLAN: Allowing newer equipment to interoperate with the existing installations makes it easier to migrate to new standards.

Maximizing Transmission speed:
When positioning equipment, we should bear some points in mind:

1. Place the access point in such a way as to minimize the distance to the furthest station.
2. Where possible, we should ensure that there is a line of sight between the access point and each station.
3. We should avoid placing stations close to large metal objects.
4. When operating in a mixed protocol environment, upgrade all the equipment to use the same protocol as soon as practicable.

Most WLANs are infrastructure WLANs, where stations connect to an access point, which acts as a hub relaying frames between the stations. The set of services provided by this type of WLAN, where there is one access point is known as a Basic Service Set (BSS).
By using more than one access point, we can extend the range of a WLAN. The set of services provided by this type of WLAN, where there is more than one access point is known as an Extended Service Set (ESS).

1.1.7. Wireless Security

Any device equipped with a wireless network adapter has the potential to access a WLAN, even if the device is located outside the organization's premises, e.g. in another building or in the street. Security is even more pressing concern in WLANs .We need special security protocols to ensure an adequate level of protection. There are two main issues that WLAN security protocols need to address. They are:

1. Encryption: Ensuring the data transmitted on wireless channels cannot be read and deciphered by devices not belonging to the WLAN.
2. Authentication: Ensuring that only devices that are entitled to do so can access the WLAN.

1.1.8. WLAN Security Threats

Table 3: Security Threats in WLAN [30]

Threat	Solution
War driving and unauthorized Network access	Strong mutual authentication: This is done through the use of secret passwords. These passwords are not sent directly across the network.
Information stealing	Strong encryption: This involves the use of mathematical algorithms to scramble transmitted data so that it can only be decrypted using a secret key.
Rogue access points	Intruder detection system(IDS) and strong authentication: Strong authentication should prevent client stations from attaching to rogue APs.

1.1.9. Other LAN technologies

Token ring: In common with all broadcast technologies, Token ring faces the problem of how to handle stations that want to transmit at the same time as each other. This is known as contention. Token ring avoids collisions by using a form of CSMA/CA. A special frame, called, a token, travels round the ring passing through each station in turn. Any station, which needs to transmit, must first capture the token. As there is only one token on the ring, only one station can transmit at any given time. After the station has sent its frame onto the ring, it releases the token to continue its progress around the ring- making it available for capture by other stations.

Packet switched networks: In a packet-switched network, the infrastructure provider accepts data packets from a sender and routes those packets through a network or packet switches, before delivering them to the receiver. Packets from the same source to the same destination, may take different routes through the network. The packet switches function like routers.

At the local exchange or Central Office (CO), the voice traffic is split from the data traffic. This is done by a DSLAM (Digital Subscriber Line Access Multiplexer). The voice traffic is routed to the PSTN.

The term contention ratio refers to how many subscribers might, at any one time, be trying to use the link between the DSLAM and the router. A contention ratio of 50:1 means that there might be up to 50 users to access the router at any one time.

1.2. Networking with TCP/IP

1.2.1. TCP/IP Protocols

The TCP/IP protocols form part of four layer architecture.

Table 4: TCP/IP Model [30]

	OSI Model	TCP/IP Model	
7	Application	Application	4
6	Presentation		
5	Session		
4	Transport	Transport	3
3	Network	Internet	2
2	Data Link	Network Interface	1
1	Physical		

1.2.2. The Internet Layer

The internet layer is responsible for addressing and routing.

Table 5: The Internet Layer [30]

Internet protocol (IP)	It is the core internet layer protocol. It defines the structure of IP packets and is responsible for addressing and routing across a network.
Address resolution protocol (ARP)	Maps IP addresses to the MAC addresses needed in order to send frames across a LAN.
Internet control and messaging protocol (ICMP)	Helps to maintain IP networks and diagnose problems in them.
Internet group management protocol (IGMP)	Maintains IP multicasting, the ability to address packets to multiple addresses.
Routing protocols.	Optional protocols which handle the exchange of routing information between routers

Internet Protocol (IP)

Each network interface connected to a TCP/IP network should have a unique logical address which allows packets to be routed to it.

An IP address has two parts- a network portion, the prefix, and a host portion, the suffix. In a network consisting of multiple network segments connected together by routers, the routers need to know how to forward packets to remote destinations. They do this on the basis of information stored in their routing tables.

Protocol numbers identify internet layer and transport layer protocols.

Packet fragmentation and reassembly:

A router may receive a packet which it needs to forward across a network link whose maximum frame size is too small to contain the entire packet. In this case, the router divides the packet into a number of fragments which are sent separately across the link. The fragments can be identified as belonging to the original by their identification number. When the fragments arrive at the destination host they can be reassembled in the correct order using the identification number together with the information in the fragmentation field.

Address Resolution Protocol (ARP)

When a packet is sent across a LAN data link it needs to be encapsulated in a frame with the destination MAC address of the destination host. ARP is used to map the IP address of the destination host to its MAC address. These mappings are then stored in an ARP cache in memory. ARP determines the destination MAC address for each frame by first looking in the ARP cache for an entry matching the destination IP address of the outbound frame. If there is a matching entry, the MAC address is retrieved from the cache. If not, ARP broadcasts an ARP request onto the local subnet, requiring the host MAC address. The ARP cache will have to be updated manually.

Reverse Address Resolution Protocol (RARP)

This protocol was used for dynamic IP configuration of hosts. Through this a host to determine its own IP address by broadcasting a RARP request.

Internet Control Message Protocol (ICMP)

ICMP is a protocol whose function is to help maintain TCP/IP networks and diagnose faults in them. ICMP control messages are encapsulated within IP packets, and can be routed throughout a network. The functions of ICMP are:

1. Build and maintain route tables.
2. Diagnose problems: The ping utility is used to send ICMP echo requests to an IP address and wait for ICMP echo response. It is used to test whether a host is reachable. The trace route utility is used to determine the path taken by packets to reach the host.
3. Adjust flow control to prevent link or router saturation.
4. Internet Group Management Protocol (IGMP)

1.2.3. The Transport Layer

The transport layer is responsible for end to end communication between hosts on the network. There are two transport layer protocols: a.) Transmission Control Protocol (TCP) b.) User datagram Protocol (UDP)

The function of the transport layer is to accept data from, and deliver data to, the appropriate application layer protocol.

Transmission Control Protocol (TCP)

TCP provides a connection orientated, reliable, byte system service applications. TCP only provides one to one communications. It accepts a byte stream from application, which it breaks into segments.

Port numbers:

Port numbers are used to specify which applications receive the contents of TCP segments. Port numbers in the range 1-1023 are well known port numbers.

Vendors may also reserve port numbers as registered ports for vendor specific applications. These are in the range 1024-49151. Ports in the range 49152 to 65535 are known as private or dynamic ports for temporary use by individuals.

The port number is one of three pieces of information required to specify a unique end point on the network, which is known as a socket. A socket comprises of: IP address, Transport layer protocol, Port number.

TCP ensures reliable connections by requiring that each segment sent is acknowledged. If a segment is not acknowledged within a certain time out period, it will be re- transmitted. The acknowledgement might not be received for different reasons. These include loss of the sent segment or acknowledgement, due to network failure or congestion. Also the inability of the receiving host to process arriving packets play an important role in this case. Finally, if no acknowledgements are received, the connection will be terminated.

Flow control using sliding windows

Having to acknowledge each segment before the next can be sent can be an inefficient way of transferring data. It is handled by the TCP by allowing some segments to be sent without acknowledgement. The number of segments that can be sent without acknowledgement is determined by the window size.

A receiving host can request the sender to increase or decrease the size of its window, by setting the value of its Window field. This is useful when the host cannot process all the traffic that it is receiving.

Terminating a TCP connection:

A TCP connection is terminated by a four way process. The processes are:

1. When an application on host A is ready to terminate the connection, it sends a segment which contains any remaining data with the FIN (Final) flag set to 1.

2. Host B immediately acknowledges this segment.

3. It then sends one or more segments containing any outstanding data from its application.

4. After acknowledgement of host B's final segment by host A, the connection is terminated.

User Datagram Protocol (UDP):

UDP provides a connectionless, unreliable transport service. It neither guarantees delivery of UDP datagrams, nor informs applications if it fails to deliver datagrams. Own mechanism must be used by the applications to ensure reliable delivery.

UDP is used for one- to- many communications – ie. broadcasts and multicasts, where connections are not established. As UDP is a much simpler protocol than TCP, it usually requires few system resources.

1.2.4. The Application Layer

There are many Application layer protocols like:

1. Telnet: It is a network terminal emulation utility. It suffers from the disadvantage that all the data is sent unencrypted over the network.

2. Trivial File transfer protocol (TFTP): It is used to copy files from a TFTP server to a TFTP client. It does not support encryption or authentication. It is a quick, convenient but not very secure way of downloading files to a router.

3. Dynamic host configuration protocol (DHCP): A DHCP server maintains a range of IP addresses and corresponding subnet masks which it can offer to DHCP clients. It can provide other IP configuration information, such as default gateway and DNS server addresses.

4. Domain Name System (DNS): DNS servers resolve domain names to corresponding IP addresses.

1.3. Basic Router Configuration

Hardware components of router:

1. RAM (Random Access Memory)
2. ROM (Read- only memory)
3. Flash Memory
4. NVRAM (Non- volatile RAM)
5. Configuration Register
6. Physical Interfaces

Software components of router:

1. ROM microcode:
    a) Bootstrap code
    b) Power – On self test code
    c) ROM monitor
    d) RXBOOT

2. Internetworking operating system (IOS)

The Boot Sequence: when a router is on the following steps are executed:

1. Power – On self test: Hardware is detected and tested from microcode resident in ROM.
2. Load and Run Bootstrap Code: This is loaded from ROM and run.
3. Find IOS software: If the configuration file is being used, the location of the IOS software can be specified in the boot system entry.
4. Load IOS software: The IOS software is loaded from the location specified.
5. Load Configuration File: The rest of the start- up configuration file is loaded.
6. Run: Once the router is configured, it is set to operate.

The IOS Command Line Interface (CLI):

The CLI is the interface which allows a user to issue commands to the IOS from a channel called a line. There are three types of line:

1. The console line: It takes its input from a terminal attached to the console port.
2. The auxiliary line: It takes its input from a remote terminal via an asynchronous modem attached to the auxiliary port.
3. Virtual terminal lines: They take their input via a network interface from a network terminal.

Command modes: The command line interface is used to issue EXEC mode commands, such as **show** and **ping**, which have an immediate effect, as well as Configuration Mode commands, which modify the configuration file.

There are two EXEC Modes:

1. Privileged EXEC Mode – it has the ability to make modifications to the router's configuration by entering a Configuration Mode.
2. User EXEC Mode – it allows access to a limited set of CLI commands.

Table 6: Special Configuration Modes

Mode	Function
Interface	Used to configure physical interface
Subinterface	Used to configure logical interfaces on a physical interface
Controller	Used to configure controllers such as E1 and T1 serial controllers
Line	Used to configure terminal lines
Router	Used to configure IP routing protocols
IPX-router	Used to configure IPX protocols

CHAPTER 2: Introduction to Ad hoc Networks

2.1. Introduction

Wireless networks have received a considerable amount of required interest in the last decade due to the fact that users can connect easily to the network without any wires. Moreover the recent drop in wireless equipment attracted more users. Many wireless networks are available in the market such as PAN, Wi-Fi and many more. Wi-Fi is the most common of them as it is required to connect to internet and other users in the provided network. But the most versatile network available is adhoc network. It is said because it requires no pre-planning to setup any connection which means it can be applied very frequently in battlefields, in disaster relief, in rescue operations or in any kind of emergency situation. In this type of network, a mobile node behaves as a host and router concurrently. All these factors give an extra edge over other conventional networks with any type of infrastructure. It can also be very useful when there is no possibility of setting up fixed networks due to geographical restrictions or cost ineffectiveness. Now major concern in wireless network is interference which ruins the desired communication between two users if any new user appears operating in the same or nearly same frequency.

2.1.1. What is an Ad hoc network?

An adhoc network is a self-organizing multi-hop wireless network, which relies neither on fixed infrastructure nor on predetermined connectivity. Ad-hoc networks are commonly used whenever a number of electronic devices are spread across a geographical area and no central communication hub exists. [10, 11]. It is an autonomous system consisting of routers and hosts, which are able to support mobility and organize themselves arbitrarily.

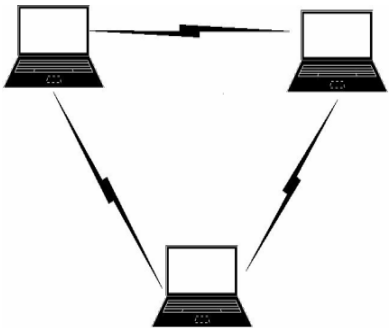

Figure 1: An Adhoc Network

An ad-hoc network is made up of multiple “nodes” connected by “links”. Links are influenced by the node's resources (e.g. transmitter power, computing power and memory) and by behavioral properties (e.g. reliability), as well as by link properties (e.g. length-of-link and signal loss, interference and noise). Since links can be connected or disconnected at any time, a functioning network must be able to cope with this dynamic restructuring, preferably in a way that is timely, efficient, reliable, robust and scalable. The network must allow any two nodes to communicate, by relaying the information via other nodes. A “path” is a series of links that connects two nodes. Various routing methods use one or two paths between any two nodes; flooding methods use all or most of the available paths. In most wireless ad hoc networks, the nodes compete for access to shared wireless medium, often resulting in interference. Using cooperative wireless communications improves immunity to interference by having the destination node combine self-interference and other-node interference to improve decoding of the desired signal. [1,17,18]

Figure 2: Features of an Adhoc Network

Adhoc networks can be formed quickly due to the presence of dynamic and adaptive routing protocols. It is reconfigurable. High node mobility and lack of centralized body gives it an extra edge over other networks.

Wireless ad hoc networks can be classified [1] by their application:

- mobile ad-hoc networks (MANET)
- wireless mesh networks (WMN)
- wireless sensor networks (WSN)

Mesh network is a generic name for multi hop ad hoc network.

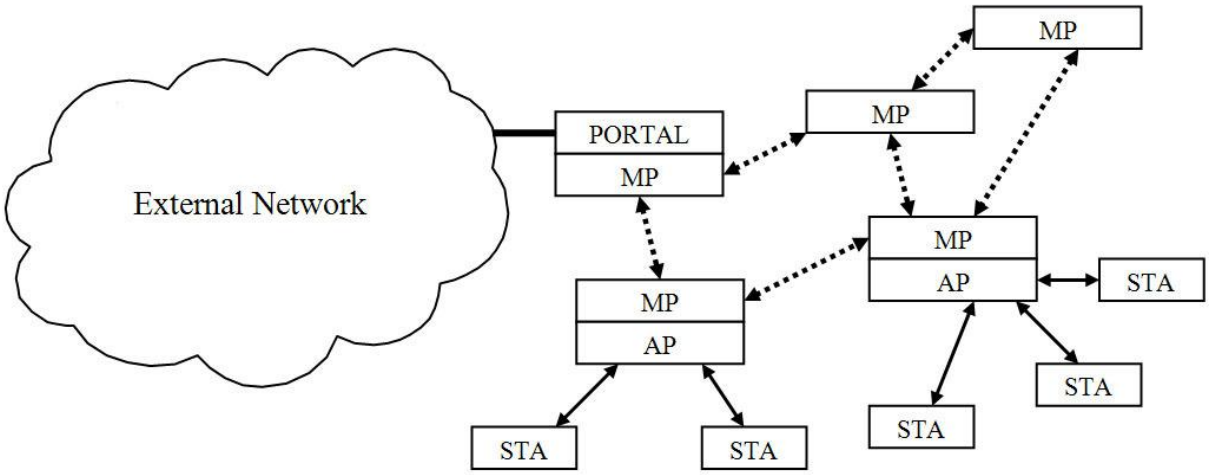

Figure 3: Mesh Network

2.1.2. Advantages of Ad hoc Network

- **Router Free**: The main advantage of using an adhoc network is that it doesn't require any wireless router in order to connect to files on other computers and / or the internet.
- **Mobility**: Adhoc network can be created in nearly any situation where there are multiple wireless devices.
- **Easy connectivity**: Adhoc network needs only a few changes in the settings of the computer and no additional hardware or software, which makes it the ultimate choice for groups working with wireless devices and accessing only a single internet connection.[16]

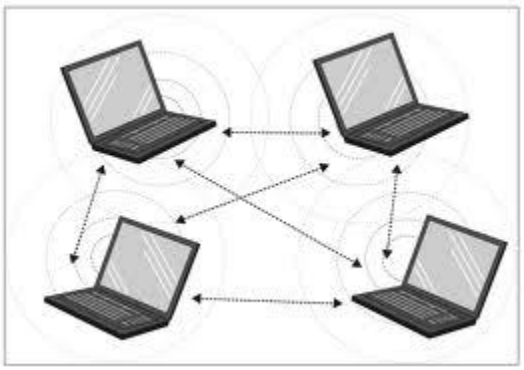

Figure 4: Router free Adhoc Network

2.1.3. Applications

Collaborative computing is the main application of ad hoc wireless network. The formation of ad hoc wireless network is needed where temporary communication infrastructure with network minimum configuration necessitates. For example, if a group of researchers want to share their documents in a meeting, ad hoc network formation is necessary to serve the purpose. Ad hoc wireless networks can be very useful in establishing communication among a group of soldiers for tactical operations. Setting up a fixed infrastructure for communication among a group of soldiers in enemy territories or in inhospitable terrains may not be possible. In such environments ad hoc wireless network provide the required communication mechanism quickly. Secure communication is of prime importance eavesdropping or other security threats can compromise the purpose of communication or the safety of personnel involved in this tactical operations. They also require the support of reliable and secure multimedia multicasting. As the

military applications require very secure communication at any cost, the vehicle mounted nodes can be assumed to be very sophisticated and powerful. They can have multiple high power transceivers, each with the ability to hop between different frequencies for security reasons. Such communication system can be assumed to be equipped with long life batteries that might not be economically viable for normal usage. [1,11]

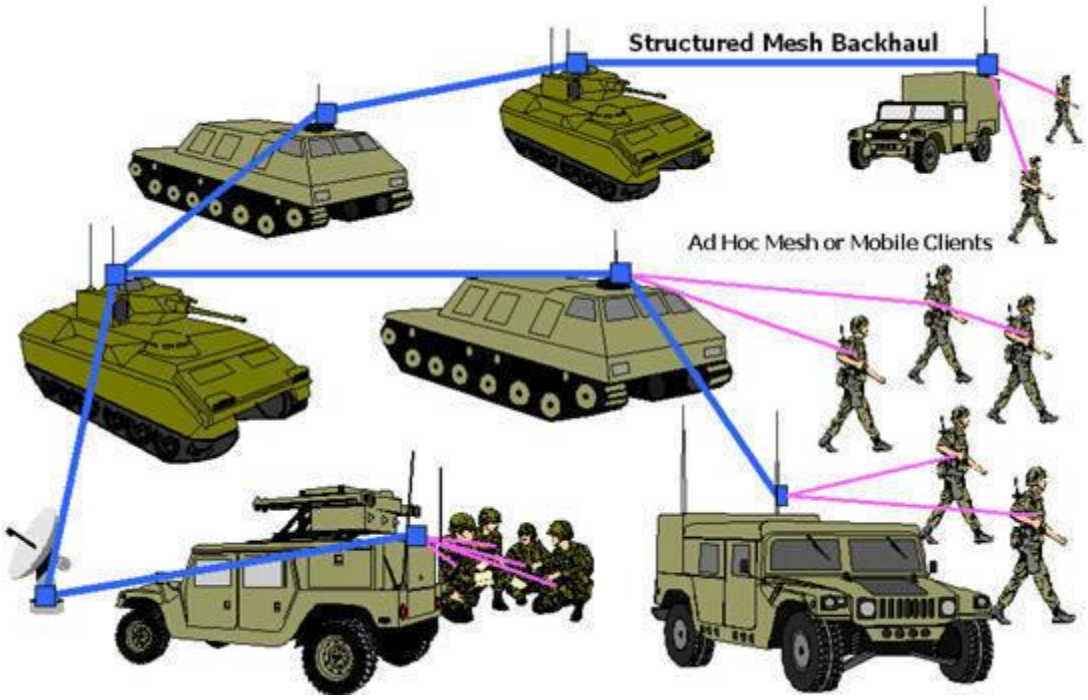

Figure 5: Military Applications

2.1.4. What is Adhoc mode in Wireless Networking?

On wireless computer networks, ad-hoc mode is a method for wireless devices to directly communicate with each other. Operating in ad-hoc mode allows all wireless devices within range of each other to discover and communicate in peer-to-peer fashion without involving central access points.

An ad-hoc network tends to feature a small group of devices all in very close proximity to each other. Performance suffers as the number of devices grows, and a large ad-hoc network quickly becomes difficult to manage. Ad-hoc networks cannot bridge to wired LANs or to the Internet without installing a special-purpose gateway.

Ad hoc networks make sense when needing to build a small, all-wireless LAN quickly and spend the minimum amount of money on equipment. Ad hoc networks also work well as a temporary fallback mechanism if normally-available infrastructure mode gear (access points or routers) stop functioning.

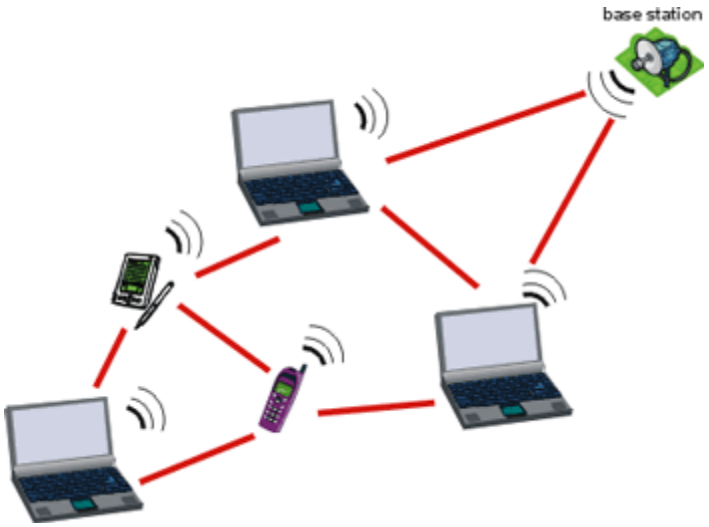

Figure 6: Ad Hoc mode

2.1.5. Interference in Adhoc Network

Packets of data are regularly sent in between neighboring nodes in adhoc network. These packets of data experience interference which is caused by simultaneous communications between other nodes in the network. 'The interference of a network is defined as the largest number of sensors that can directly communicate with a single plane in the plane.' One of the main challenges in models of wireless communication is interference. For instance, a node **A** may interfere with another node **B** if **A**'s interference range unintentionally covers **B**. Consequently, the amount of interference that **B** experiences is the number of such nodes **A**. [6]

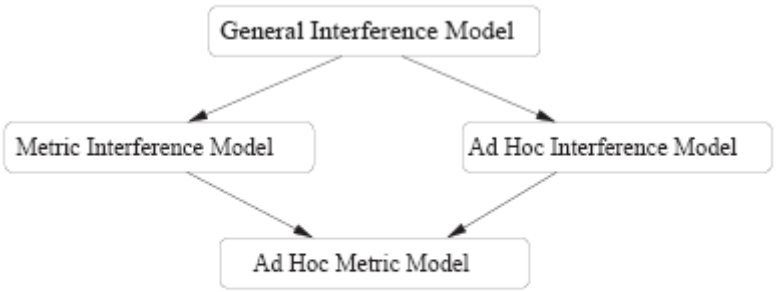

Figure 7: Relationship between Interference Models

The main aim of the interference reduction is to maximize the capacity and throughput of the system. Interference can be reduced by having nodes send with less transmission power. The area covered by the smaller transmission range will contain fewer nodes, yielding less interference. On the other hand, reducing the transmission range has the consequence of communication links being dropped. However, there is surely a limit to how much the transmission power can be decreased. In ad hoc networks, if the node's transmission ranges become too small and too many links are abandoned, the network may become disconnected. Hence, transmission ranges must be assigned to nodes in such a way that the desired global network properties are maintained. [6]

2.1.6. Essentials and vulnerabilities of Adhoc Network

The principle of ad hoc networks sounds like a great idea. A dynamic connection between devices that can be used from anywhere and offers limitless business, recreational and educational opportunities appears to be a promising technological advancement towards making our lives easier. However, as with conventional networks, security and safety considerations have to be taken into account.

Primarily adhoc networks can be secured by using passwords to prevent outside access but by nature they are very open to anyone. Their biggest advantage is also one of their biggest disadvantages: basically anyone with the proper hardware and knowledge of the network topology and protocols can connect to the network. This allows potential attackers to infiltrate the network and carry out attacks on its participants with the purpose of stealing or altering information.

Also, depending on the application, certain nodes or network components may be exposed to physical attacks which can disrupt the functionality. In contrary to conventional networks, ad hoc network hosts are more often than not part of an environment that is not maintained professionally. Wireless nodes might be scattered over a large (potentially unsecure) area, where it may pose difficult to supervise all of them.

Another specialty of ad hoc networks is their heavy reliance on inter-node communication. Due to the dynamic nature of the link between the single nodes, it may happen that a certain node B is not in range of node A. In these cases, the information can be routed through intermittent nodes. Even though this is of course not a new concept since it is heavily utilized in the infrastructure of the Internet, the fact that ad hoc network nodes are usually mobile and can disappear at any time (both from within the range of a particular node as well as from the entire network), the possibility that a certain data route becomes unavailable is significantly higher than in fixed-location networks. This makes it easier for attackers to disrupt the network than in conventional networks. To ensure proper operation, several attributes of these networks have to be protected against defects and more importantly against malicious intent. [31]

2.1.7. Comparison between Adhoc and Cellular network

Table 7: Comparison between Adhoc and Cellular network [1]

Cellular network	Ad Hoc network
Infrastructure is fixed	No infrastructure
Bandwidth is guaranteed	Radio channels are shared
Single hop	Multi hop
Uses circuit switch	Uses packet switch
Low call drop	More path breaks
Cost is high	Low cost
Employment of bandwidth reservation is easier	Bandwidth reservation is complex
Time synchronization is easier	Time synchronization is not so easy
By reusing geographical channel frequency spectrum can be reused	Dynamic frequency reuse
Used mainly in civilian and commercial sector	Mainly used in military and collaborate computing.
Maximizes call acceptance ratio and minimizes call drops	Find path with minimum overhead and quick reconfiguration
Widely deployed	Commercial deployment

2.1.8. Limitations of Ad hoc Network

Ad-hoc mode allows a Wi-Fi network to function without a central wireless router or access point. In a few situations, ad-hoc mode networking is preferable to the alternative infrastructure mode, but ad-hoc networks suffer from several key limitations. They are:

1. Wi-Fi devices in ad hoc mode offer minimal security against unwanted incoming connections. For example, ad-hoc Wi-Fi devices cannot disable SSID broadcast like infrastructure mode devices can. Attackers generally will have little difficulty connecting to your ad-hoc device if they get within signal range.

2. The Wi-Fi networking standards require only that ad-hoc mode communication supports 11 Mbps bandwidth. It should be expected that Wi-Fi devices supporting 54 Mbps or higher in infrastructure mode, will drop back to a maximum of 11 Mbps when changed to ad-hoc mode. Ad-hoc mode should generally be viewed as "slower" than infrastructure mode for this reason.

3. Signal strength indications accessible when connected in infrastructure mode will be unavailable in ad-hoc mode. Therefore, we will face some difficulty whenever re-positioning an ad-hoc device to achieve a better signal.

2.2. Issues in Adhoc wireless networks

When an ad-hoc wireless system is designed some major issues and challenges are considered. They are discussed in the following sub-chapters: [1]

2.2.1. Medium Access Scheme

The distributed arbitration for the shared Chanel for transmission of packets is the primary responsibility of a Medium Access control (MAC) protocol in adhoc wireless networks. To design a MAC protocol the major issues should be considered. They are:

- **Distributed Operation:** Where there is no centralized co-ordination is possible, in that environment, the adhoc wireless networks should be operated. Minimum control overhead is involved with the distribution of MAC design as well as partial co-ordination is also required.
- **Synchronization:** Time synchronization is required in the design of MAC protocol. For transmission and reception slots, where TDMA-based system exists, synchronization is mandatory. Usage of scarce resources live band width and battery power, synchronization is involved. For synchronization, the control packets are used which increases the network collisions.
- **Hidden terminals:** From the sender of a data transmission session, the hidden terminals are not reachable. Here, terminals are the nodes that are reachable to the

receiver of a session. The hidden terminals can reduce the through put of a MAC protocol and can cause collisions at the receiver node. MAC protocol should be able to alleviate the effects of hidden terminals.

- **Exposed terminals:** The nodes that are in the transmission range of the sender of an on-going session in the exposed terminals. They are prevented from making a transmission. In order to improve the sufficiency of the MAC protocol. The exposed nodes should be allowed to transmit in a controlled fashion without causing collision to the on-going data transfer.
- **Throughput:** The maximization of throughput of a system is the attempt of the MAC protocol which is employed in adhoc wireless networks. It minimizes the occurrence of collisions, minimize control overhead.
- **Access delay:** The average delay that any packet experiences to get transmitted is the Access delay. In MAC protocol, the delay is minimized.
- **Fairness:** The ability of the MAC to provide an equal share of the bandwidth to all competing nodes is the fairness. Fairness is either node based or flow based. The former proved an equal bandwidth share for competing nodes and the latter provides an equal share for competing data transfer sessions. The multi-hop relaying done by the nodes, so, fairness is important.
- **Real time traffic support:** Supporting time sensitive traffic such as voice, video and real time data requires explicit support from the MAC protocol. It is required ion a contention based channel access environment, without any central coordination, with limited bandwidth and with location dependent contention.
- **Resource reservation:** Bandwidth, delay, and jitter are the provisioning parameter of QOS which requires reservation of resource. These resources are like bandwidth, buffer space and processing power. This reservation becomes difficult for the mobility of the nodes of an ad hoc wireless network. To reserve the resource and provisioning of QOS is the requirement of a MAC protocol which should have the ability to do that.
- **Ability to measure resource availability:** The MAC protocol should be able to provide an estimation of resource availability at every node and used for congestion control decisions. To handle the resources such as bandwidth efficiently and perform call admission control based on their availability.

- **Capability for power control:** Reduction of energy consumption, decreases in interference and increases of frequency is happened by the transmission power control.
- **Adaptive rate control:** The variation of data bit rate achieved over a channel is referred by the adaptive rate control. If a MAC protocol has adaptive rate control and the sender and receiver are nearby then it can use a high data rate. When the sender and receiver move away from each other the data rate reduces adaptively.
- **Use of directional antenna:** The increase of spectrum reuse, interference reduction, and reduction of power consumption uses the directional antennas. Directional and omnidirectional antennas can't exist simultaneously.

2.2.2. Routing

A routing protocol faces some major challenges such as:

- **Mobility:** Mobility is one of the important properties of ad hoc wireless networks. It is associated with the nodes. The mobility of nodes results in frequent path breaks, packet collisions, transient loops, stale routing information and difficulty of resource reservation. The above issues can be efficiently solved by a good routing protocol.

- **Bandwidth constraint:** All nodes in the broadcast region share the channel. The bandwidth available per wireless link depends on the number of nodes and traffic they handle. The availability of every node is only a fraction of the total bandwidth.

- **Error prone and shared channel:** When the bit rate error of a wired counterpart is compared with a wireless channel, the bit rate error is very high in a wireless channel. This is taken into account in routing protocol design for ad hoc wireless network. The efficiency of the routing protocol can be improved by the consideration of the state of the wireless link, signal to noise ratio, and Path loss for routing in ad hoc wireless networks.
- **Location dependent contention:** The load on the wireless channel with varies with the number of nodes present in a given geographical region .When the number of nodes increases; it makes the contention for the channel high. A high number of collisions and a

subsequent wastage of bandwidth is the result of high contention for the channel. The formation of regions where channel contention is high can be avoided if a good routing protocol has built in mechanism for distributing the network load uniformly across the network.

- **Other resource constraints:** The capability of a routing protocol is limited by the constraints on resources such as computing power, battery power and buffer storage.

- **Minimum route acquisition delay:** The node that does not have a route to a particular destination node should be as minimal as possible is the route acquisition delay. The delay varies with the size of the network and network load.

- **Quick route reconfiguration:** In order to handle Path breaks and subsequent packet losses, the routing protocol should be able to quickly perform route reconfiguration. This is the requirement for the unpredictable changes of the network topology.

- **Loop free routing:** To avoid unnecessary wastage of network bandwidth, loop free routing is the fundamental requirement. In ad hoc networks transient loops form the route due to the random movement of nodes. This transient routs should be detected and corrected by routing protocol.

- **Distributed routing approach:** Ad hoc wireless network can be called fully distributed network where the centralized routing can consume a large amount of bandwidth.

- **Minimum control overhead:** To found a new route, the control packets exchanged and maintenance of existing routes should keep possibly minimal. The consumption of precious bandwidth is controlled by control packets. Data packet collisions are also caused by this and thus reduce network throughput.

- **Scalability:** The scaling ability of a routing protocol with a large number of nodes in a network is the scalability. Minimization of control overhead and routing protocol adaption to the network size is its requirement.

- **Provisioning of quality of service:** To provide a certain level of quality of service as demanded by the nodes or the calls category depends on the routing protocol. So, it should be able to fulfill the requirement.

- **Support for time sensitive traffic:** Support for time sensitive traffic is the requirement of tactical communications and similar applications. Routing protocol should have the ability to support both hard real time and soft real time traffic.

- **Security and privacy:** Routing protocol should be able to resilient to threats and vulnerabilities. To avoid resource consumption, denial of service, impersonation and possibly similar attacks, the routing protocol should have in built capability against an ad hoc wireless network.

2.2.3. Multicasting

In the typical applications of ad hoc wireless networks, multicasting is very important. It has special application on emergency search and rescue operations and military communication. To carry out certain tasks that require point to point, point to multipoint voice and data communication, nodes form groups. The multicasting becomes very challenging because of the mobility of the nodes, constraint of power source and bandwidth. A tree based multicast structure is highly unstable in ad hoc wireless network. To include broken links, frequent readjustment is needed. So traditional wired network multicast protocols do not perform well. Due to frequent tree breaks, a tree shaped topology provides high multicast efficiency with low packet delivery ratio. Provisioning of multiple links among the nodes in an ad hoc wireless network results in a mesh shaped structure. It performs well in a high mobility environment. The design of multicast routing protocols depends on some major issues which are as follows:

- **Robustness:** The multicast routing protocol should be able to recover and reconfigure quickly from potential mobility induced link breaks. It is suitable in highly dynamic environments.

- **Efficiency:** To deliver a data packet to all the group members, the multicast protocol should be able to make a minimum number of transmissions.

- **Control overhead:** Minimal control overhead for the multicast session is the demand of the scarce bandwidth availability in ad hoc wireless network.

- **Quality of service:** The data transferred in a multicast session is time sensitive. So, QOS support is essential in multicast routing.

- **Efficient group management:** The process of accepting multicast session members and maintaining the connectivity among them until the session expires is the group management minimal exchange of control is needed in the management performance.

- **Scalability:** Scaling with a large number of nodes is important. So multicast routing protocol should have the ability to scale.
- **Security:** In military communications, session number authentication and non members prevention from gaining unauthorized information is very important.

2.2.4. Pricing Scheme

An adhoc wireless networks functioning depends on the presence of relaying nodes and their willingness to relay on the nodes traffic. A relaying neighbor node may not be interested in relaying a call. In this case it may shut down. It may be happened at the presence of sufficient node density. As an example if an optimal route passes through an intermediate node to the other and the node is off, then the first node set up will be costlier and non optimal to another which consumes more resources. It also affects the throughput of the system. Here the intermediate nodes relay the data packets expend battery charge and computing power. So it should

compensate properly. Thus pricing schemes are required. Pricing scheme is required especially for the successful commercial deployment of adhoc wireless network.

2.2.5. Self Organization

Organization and maintenance of network is an important property of an ad hoc wireless network. Neighbor discovery, topology organization and reorganization are the activities which are required to perform in ad hoc wireless network. In neighbor discovery phase, the information about the neighbors gathered by every node maintains the information in appropriate data structure. Periodic transmission of short packets is required here which is called beacons or promiscuous snooping on the channel to detect the neighbors' activities. The variation of transmission power to improve upon spectrum reusability is permitted only by certain MAC protocols. In a topology organization phase, the information gathered by the node is about the entire network or a part of network. For a topology reorganization phase, by incorporating the topological changes the ad hoc wireless networks update the topology information. These changes occurred due to the mobility of nodes, failure of nodes or complete depletion of power sources of the nodes. Periodic or aperiodic topological information exchange and adaptability are the two major activities of reorganization. Major topological reorganization is required in network partitioning and merging two existing partitions. Perform quickly and efficiently of self organization is the requirement of an ad hoc wireless network which should be very transparent to the user and application.

2.2.6. Security

Communication security is very important in ads hoc wireless network. There are two types of attacks against ad hoc wireless network: active attacks and passive attacks. Passive attacks refer to the attempts made by malicious nodes for perceive the nature of activities and to obtain information transected in the network without disrupting the operation. Active attacks disrupt the operation of the network. External attacks are the active attacks where the network outside nodes executes and internal attacks are the active attacks where the nodes are from the same network. Some major security threats exist in ad hoc wireless network. They are:

- **Denial of service:** The attack effected by making the network resources unavailable for service to other nodes, either by consuming the bandwidth or by overloading the system, is known as denial of service. By keeping a target node busy making it process unnecessary packets, a DOS attacks interrupts the operation.

- **Resources consumption:** For an easy internal attack, the scarce availability of resource is the main reason.

- **Energy depletion:** Energy source constrain the nodes in an ad hoc wireless network and this type of attack deplete the battery power of critical nodes.

- **Buffer overflows:** By filling the routing table with unwanted routing entries or consuming the data packet buffer space with unwanted data, can carry out buffer overflow attack. Dropping of a large number of data packets, losses of critical information is lead by this type of attacks. Preventing a node from updating route information for important definitions and filling the routing table with routs for nonexistent destinations are the problems lead by the route table attacks.

- **Host impersonation:** A compromised internal node responds with appropriate control packets, to create wrong route entries. It can terminate the traffic meant for the intended destination node.

- **Information discloser:** By deliberate discloser of confidential information to unauthorized nodes, a compromised node can act as an informer. For military application, the amount and the periodicity of traffic between a selected pair of nodes and pattern of traffic changes is very important. In resource constrained ad hoc wireless network, using of filter traffic is not suitable.

- **Interference:** A common attack in defense applications is to jam the wireless communication by creating a wide spectrum noise. It is done by single wide band jammer

and sweeping across the spectrum. To protect against such external threats, the MAC and physical layer technologies should be able to handle.

2.2.7. Scalability

To lead a big ad hoc wireless network, traditional applications such as military, emergency operations and crowd control is not enough. Commercial deployment shows early trends for a widespread installation of ad hoc wireless network for mainstream wireless communication. The scalability may be improved by the hybrid architectures which combine the multi hop radio relaying in the presence of infrastructure.

2.2.8. Addressing and service discovery

Due to the absence of any centralized coordinator in ad hoc wireless network, addressing and service discovery assume significance. To participate in communication, a globally unique address in the connected part is required. To allocate non duplicate address to the nodes, auto configuration of address is required. To maintain unique addressing throughout the connected parts of the network, duplicate address detection mechanisms are required. It is especially required where the topology is highly dynamic, frequent partitioning and merging of wireless components. In this network the nodes should have the ability to locate service provided by other nodes. Topological changes force a change in the location of the service provider as well, hence fixed positioning of a server providing a particular service is ruled out. Rather identifying the current location of the service provider gather importance. The integration of service discovery with route acquisition mechanism violates the traditional design objects of the routing protocol. But it is viable alternative. Service discovery protocols should be separated from the network layer protocol.

CHAPTER 3: Literature Survey

Different research papers, books and journals were read during the literature survey relating to our thesis work. Some of the topics that we have gone through during this period are in the following subchapters.

3.1 Topology control to minimize interference

Due to the limited power and memory, a wireless node prefers to only maintain the information of a subset of neighbors it can communicate, which is called topology control.

Topology control is one of the ways to reduce the power consumption and improve network longevity. By using topology control algorithm, interference can be reduced. In order to extend network lifetime, reducing node power consumption is the main goal of topology control. Topology control algorithm basically replaces longer links by shorter links in the network. It forces the nodes to use several shorter hops so that it can use lower transmission path and save energy as the energy required to transmit a message increases with distance. This can be done by using multiple channels instead of a single channel. Topology control refers to selecting only a subset of available communication links for data transmission. If interference is lower, then collisions and packet transmissions are few and power consumption is also lower. So, to use a topology which gives low interference is also the main goal of topology control. [2,11,24,25]

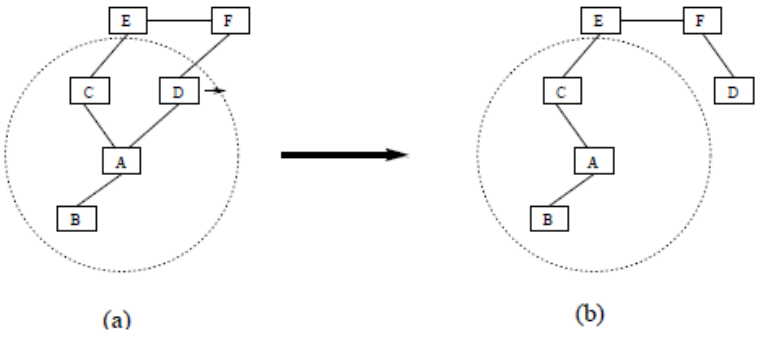

Figure 8: Topology change in ad hoc network [7]

Some researchers in research papers mentioned that general proposed topology control cannot constrain interference effectively. So, they proposed connectivity preserving and spanner constructions that minimize interference. Reducing of transmission power of nodes can cause interference. By sparseness or low node degree of the resulting topology graph, interference aspect is maintained. Here sometimes it is done by without providing rigorous motivation. To formulate the tradeoff between energy conservation and network connectivity, interference definition was employed. They stated some requirements which were to meet to the resulting topology. Connectivity and spanner property are the two requirements. Connectivity means the indirect connection between two nodes are in a given network which should be connected in the resulting topology. On the resulting topology, the shortest path between any pair of nodes should be longer at most by a constant factor than in a given network's shortest path which is connecting the same pair of node. An optimization problem also occurs by stating such requirements. They showed that the currently proposed topology control algorithm committed a substantial mistake. [24,25]

They proposed a centralized algorithm which can compute the interference minimal connectivity topology. They also presented a distributed local algorithm which computes interference optimal spanner topology. They also showed by simulation that average case graphs particularly Gabriel graph and Relative neighborhood graph can reduce interference.

Furthermore, 'Neighbor attachment' is another process to reduce interference between nodes by establishing links between nodes that on the physical layer are visible to each other. [26]

Another process to minimize the interference is to assign a suitable transmission radius to each of the given points in the plane, so as to minimize the maximum number of transmission ranges overlapping at any point. [27]

Interference can also be reduced by limiting the communication radius between the nodes. It can be done by using an algorithm that assigns a transmission radius to a given list of sensors in a way that the network is connected and has low interference.

3.2 Licensed and Unlicensed Frequencies

All wireless technologies use the airwaves to transmit and receive information. So that many different technologies can use the airwaves simultaneously, wireless spectrum is carved up into chunks called frequency bands. For example, broadcast VHF television is assigned one frequency band, while AM radio is assigned another frequency band. These are licensed bands, meaning that individual companies pay a licensing fee for the exclusive right to transmit on assigned channels within that band in a given geographic area.

Licensing is a way of ensuring that wireless operators do not interfere with each other's transmissions. Without licensing, interference would garble both transmitters' signals, preventing decent reception. With licensing, the only place where interference occurs is usually at the outer edge of the license-holder's assigned coverage area.

However, licensing would be very impractical for certain uses, like communication between cordless handset and base unit, or interaction between wireless keyboard and PC. Instead, these wireless technologies transmit in unlicensed frequency bands -- usually the 2.4 GHz ISM band allocated in most countries for use by anyone, without a license. Another commonly-used unlicensed band is the 5 GHz UNII band. Spectrum allocation varies by country.

Unlicensed wireless technologies don't require any permission, as long as products and users comply with the rules associated with that unlicensed band (for example, maximum transmission power). But unlicensed wireless technologies are, by nature, vulnerable to interference. This is why at home or business WLAN can experience signal corruption caused by a neighbor's WLAN operating on the same channel within the 2.4 or 5 GHz band. When using an unlicensed technology like Wi-Fi, one have to make adjustments to avoid interference, and the radio environment is likely to continue to change over time. On the other hand, technologies like EV-DO and UMTS are less prone to interference because wireless carrier purchased the right to use those licensed frequencies. Of course, we can't put up our own EV-DO network -- we have to pay the license holder for service. But we can create our own WLAN anywhere, anytime, using the unlicensed band for free. That's the trade-off between licensed and unlicensed wireless.

3G networks have licensed fixed frequency bands. These bands are 1885–2025 GHz and 2110–2200 GHz. Wi-Fi WLANs (11b) also have a fixed frequency band: 2410–2480 GHz. This latter

band is in the ISM (Industrial, Scientific and Medical), a free band also used by systems other than Wi-Fi.

Both types of frequency bands are part of WiMAX:

1. Licensed bands;
2. License-exempt bands.

It is often mentioned that unlicensed frequencies of WiMAX will be used for limited coverages, campuses (enterprise or academic), particular initiatives, etc. In other words, operator revenue should come only from licensed frequencies where the service can be more easily guaranteed. In some countries and regions, attributed licenses are known as agnostic licenses, i.e. no specific technology or other requirements are mandatory. Only frequency filter shapes and maximum transmitted power are indicated. For example, in these bands, an operator can have 3G or UMTS. However, not all attributed frequencies are agnostic. In some countries, a WiMAX licensed band may only be used for WiMAX operation. Additional constraints may also exist. For example, WiMAX cannot be used for mobile operations in some countries.

The standard indicates that the RF (Radio Frequency) centre frequency is the centre of the frequency band in which a BS or an SS may transmit. Uplink and downlink centre frequencies must be multiples of 250 kHz. The required precision is of the order of 10^{-5} (depending on the Physical Layer and whether it is the BS or the SS).

3.3 Omni-directional vs Directional Antennas

3.3.1 Basic Antenna Concepts

An antenna is a passive device which does not offer any added power to the signal. Instead, an antenna simply redirects the energy it receives from the transmitter. The redirection of this energy has the effect of providing more energy in one direction, and less energy in all other directions.

Antennas are rated in comparison to isotropic or dipole antennas. An isotropic antenna is a theoretical antenna with a uniform three-dimensional radiation pattern. In other words, a theoretical isotropic antenna has a perfect 360 degree vertical and horizontal beam width or a spherical radiation pattern. It is an ideal antenna which radiates in all directions and has a gain of

1 (0 dB), i.e. zero gain and zero loss. It is used to compare the power level of a given antenna to the theoretical isotropic antenna. Unlike isotropic antennas, dipole antennas are real antennas. The dipole radiation pattern is 360 degrees in the horizontal plane and approximately 75 degrees in the vertical plane and resembles a donut in shape. Because the beam is slightly concentrated, dipole antennas have a gain over isotropic antennas of 2.14 dB in the horizontal plane.

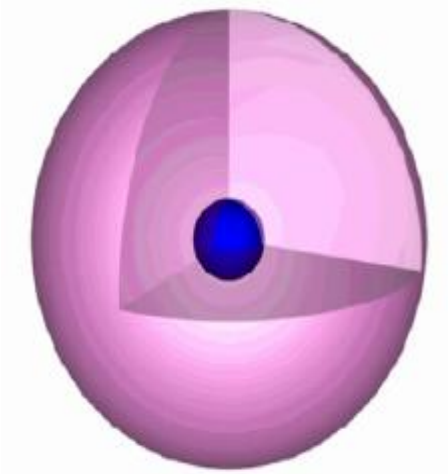

Figure 9: Radiation of isotropic antenna

An antenna gives the wireless system three fundamental properties: gain, direction and polarization.

Gain is a measure of increase in power. Gain is the amount of increase in energy that an antenna adds to a radio frequency (RF) signal.

Direction is the shape of the transmission pattern. As the gain of a directional antenna increases, the angle of radiation usually decreases. This provides a greater coverage distance, but with a reduced coverage angle. The coverage area or radiation pattern is measured in degrees. These angles are measured in degrees and are called beam widths. Beam widths are defined in both horizontal and vertical plains. Beam width is the angular separation between the half power points (3dB points) in the radiation pattern of the antenna in any plane. Therefore, for an antenna you have horizontal beam width and vertical beam width. The higher the gain of the antennas, the smaller the vertical beam width is.

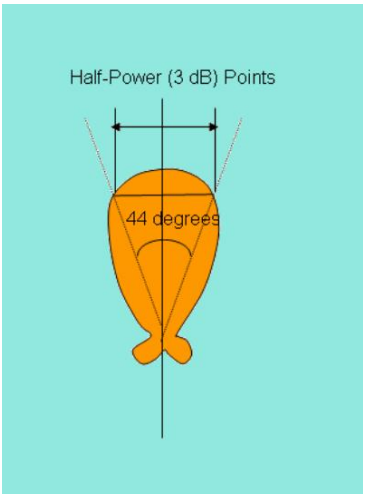

Figure 10: Beam width of antenna

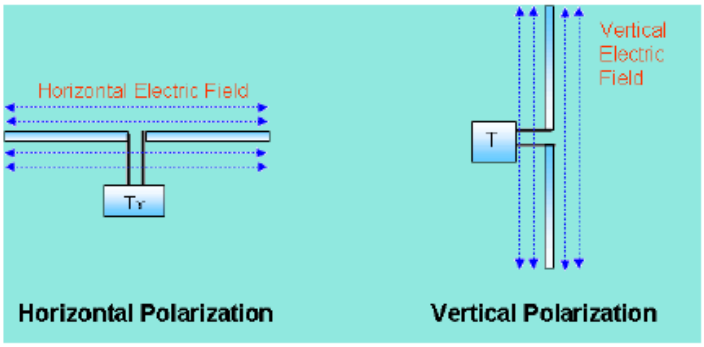

Figure 11: Antenna polarization

An antenna can have a gain of 21 dBi, a front-to-back ratio of 20 dB or a front-to-side ratio of 15 dB. This means the gain in the backward direction is 1 dBi, and gain off the side is 6 dBi. In order to optimize the overall performance of a wireless LAN, it is important to understand how to maximize radio coverage with the appropriate antenna selection and placement.[24,28,29]

Antennas can be broadly classified as omnidirectional and directional antennas, which depends on the directionality.

3.3.2 Omni-directional Antenna

Omnidirectional antennas have a similar radiation pattern. These antennas provide a 360 degree horizontal radiation pattern. These are used when coverage is required in all directions (horizontally) from the antenna with varying degrees of vertical coverage. Polarization is the physical orientation of the element on the antenna that actually emits the RF energy. The omni directional antenna radiates or receives equally well in all directions. It is also called the "non-directional" antenna because it does not favor any particular direction with the four cardinal signals. An omnidirectional antenna is usually a vertical polarized antenna.

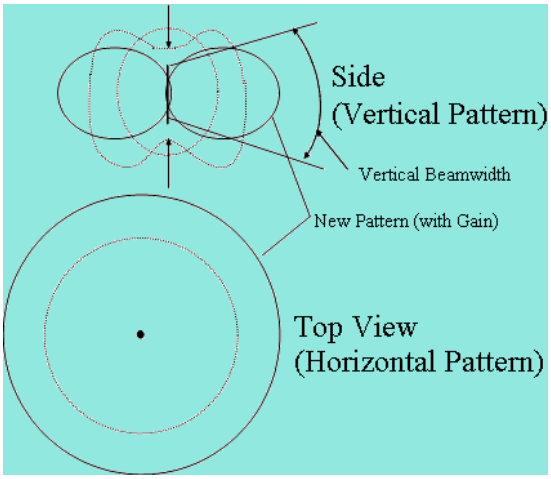

Figure 12: Radiation pattern of an omni antennae

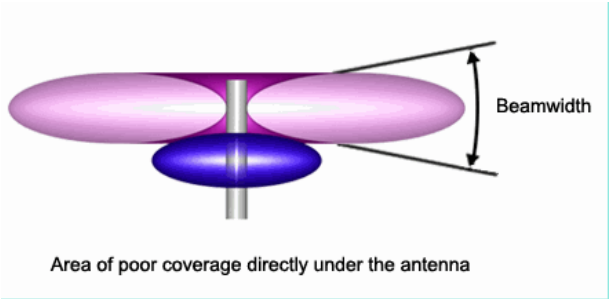

Figure 13: Omni Antenna with no coverage below the Antenna

Omni directional antennas are very easy to install. Due to the 360 degrees horizontal pattern, it can even be mounted upside down from a ceiling in the indoor environment. Also, because of its shape it is very convenient to attach these antennas to the product. For example, you might see

Rubber Duck antennas attached to the wireless APs. In order to obtain an omnidirectional gain from an isotropic antenna, energy lobes are pushed in from the top and the bottom, and forced out in a doughnut type pattern. If we continue to push in on the ends of the balloon (isotropic antenna pattern), a pancake effect with very narrow vertical beam width results, but with a large horizontal coverage. This type of antenna design can deliver very long communications distances, but has one drawback which is poor coverage below the antenna. If we try to cover an area from a high point, we see a big hole below the antenna with no coverage.

This problem can be partially solved with the design of something called down tilt. With down tilt, the beam widths are manipulated to provide more coverage below the antenna than above the antenna. This solution of downtilt is not possible in an omni antenna because of the nature of its radiation pattern.

The omni directional antenna is usually a vertically polarized antenna, so you cannot have advantages of using cross polarization here to fight interference.

A low gain omni antenna provides a perfect coverage for an indoor environment. It covers more area near the AP or a wireless device in order to increase the probability of receiving the signal in a multipath environment. [24, 28, 29]

3.3.3 Directional Antenna

A **directional antenna** or **beam antenna** is an antenna which radiates greater power in one or more directions allowing for increased performance on transmit and receive and reduced interference from unwanted sources. Directional antennas focus the RF energy in a particular direction. As the gain of a directional antenna increases, the coverage distance increases, but the effective coverage angle decreases. For directional antennas, the lobes are pushed in a certain direction and little energy is there on the back side of the antenna.

Another important aspect of the antenna is the front-to-back ratio. It measures the directivity of the antenna. It is a ratio of energy which antenna is directing in a particular direction, which depends on its radiation pattern to the energy which is left behind the antenna or wasted. The higher the gain of the antenna, the higher the front-to-back ratio is. A good antenna front-to-back ratio is normally 20 dB.

With the directional antennas, we can divert the RF energy in a particular direction to farther distances. Therefore, you can cover long ranges, but the effective beamwidth decreases. This type of antenna is helpful in near LOS coverage, such as covering hallways, long corridors, isle structures with spaces in between, etc. However, as the angular coverage is less, we cannot cover large areas. This is a disadvantage for general indoor coverage because we would like to cover a wider angular area around the AP. Antenna arrays should face in the direction where the coverage is desired, which can sometimes make mounting a challenge. [24,28,29]

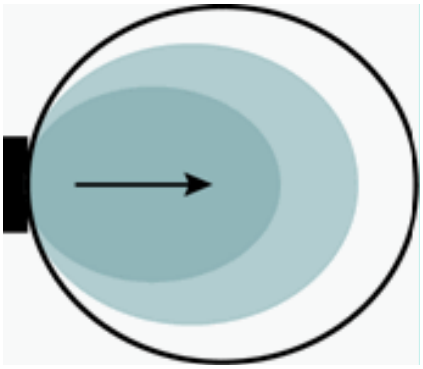

Figure 14: Radiation Pattern of Directional Antenna

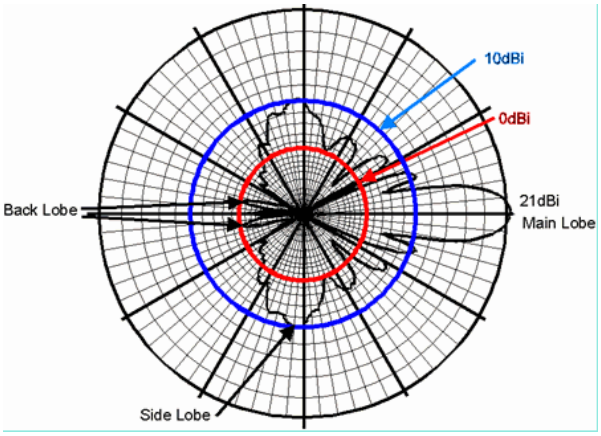

Figure 15: Radiation Pattern of Directional Antenna with central lobes

3.4 Hidden and Exposed node problem

Hidden node problem:

In wireless networking, the hidden node problem or hidden terminal problem occurs when a node is visible from a wireless access point (AP), but not from other nodes communicating with said AP. This leads to difficulties in media access control. Hidden nodes in a wireless network refer to nodes that are out of range of other nodes or a collection of nodes. Here each node is within communication range of the AP, but the nodes cannot communicate with each other, as they do not have a physical connection to each other.

Suppose node **B** is transmitting data to node **C** and that node **A** cannot listen do node **B**'s transmission. So, node **A** may start its transmission to node **C**, while node **C** is receiving data from **B**. A collision will occur in node **C**. This problem is known as the hidden node problem

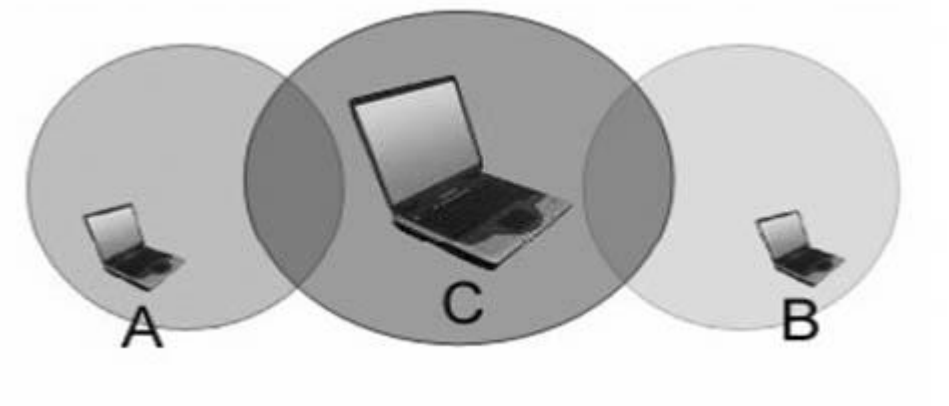

Figure 16: Hidden node problem

The problem is when nodes **A** and **B** start to send packets simultaneously to the access point. Since node **A** and **B** cannot sense the carrier, Carrier sense multiple access with collision avoidance (CSMA/CA) does not work, and collisions occur, scrambling data. To overcome this problem, handshaking is implemented in conjunction with the CSMA/CA scheme. [32]

The hidden node problem can be observed easily in widespread (>50m radius) WLAN setups with many nodes that use directional antennas and have high upload. Newer standards such as

WiMAX assign time slots to individual stations, thus preventing multiple nodes from sending simultaneously and ensuring fairness even in over-subscription scenarios.

The methods that can be employed to solve hidden node problem are:

1. Increase transmitting power from the nodes: Increasing the power of the nodes can solve the hidden node problem by allowing the cell around each node to increase in size, thus enabling the non- hidden nodes to detect the hidden node.

2. Use of omnidirectional antennas: Nodes using directional antennas are nearly invisible to nodes that are not positioned the direction of the antenna. So omnidirectional antennas can be used for widespread networks.

3. Remove obstacles: Obstacles also hinder the communication with other nodes. So any obstacles that may hinder may be removed.

4. Move the node: Another method of solving the hidden node problem is moving the nodes so that they can all hear each other. If it is found that the hidden node problem is the result of a user moving his computer to an area that is hidden from the other wireless nodes, it may be necessary to have that user move again. The alternative to forcing users to move is extending the wireless LAN to add proper coverage to the hidden area, by using additional access points.

5. Use of protocol enhancement software: There are several software implementations of additional protocols that essentially implement a polling or token passing strategy. Then, a master (typically the access point) dynamically polls clients for data. Clients are not allowed to send data without the master's invitation. This eliminates the hidden node problem at the cost of increased latency and less maximum throughput.

Exposed node problem:

In wireless networks, the exposed node problem occurs when a node is prevented from sending packets to other nodes due to a neighboring transmitter. Consider an example of 4 nodes labeled **R1**, **S1**, **S2**, and **R2**, where the two receivers are out of range of each other, yet the two transmitters in the middle are in range of each other. Here, if a transmission between **S1** and **R1** is taking place, node **S2** is prevented from transmitting to **R2** as it concludes after carrier sense that it will interfere with the transmission by its neighbor **S1**. However note that **R2** could still receive the transmission of **S2** without interference because it is out of range of **S1**.

IEEE 802.11 RTS/CTS mechanism helps to solve this problem only if the nodes are synchronized and packet sizes and data rates are the same for both the transmitting nodes. When a node hears an RTS from a neighboring node, but not the corresponding CTS, that node can deduce that it is an exposed node and is permitted to transmit to other neighboring nodes.

If the nodes are not synchronized (or if the packet sizes are different or the data rates are different) the problem may occur that the sender will not hear the CTS or the ACK during the transmission of data of the second sender.

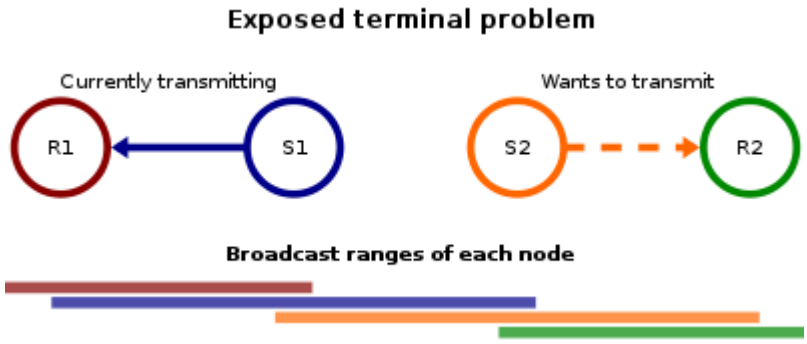

Figure 17: Exposed node problem

3.5 Solution to Hidden and Exposed Node problem

3.5.1 MAC Protocols to solve Hidden and Exposed Node problem

The **media access control** (**MAC**) data communication protocol sub-layer, also known as the medium access control, is a sublayer of the data link layer specified in the seven-layer OSI model (layer 2). It provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g. Ethernet. The hardware that implements the MAC is referred to as a medium access controller.

The MAC sub-layer acts as an interface between the logical link control (LLC) sublayer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-point network. This channel may provide unicast, multicast or broadcast communication service.

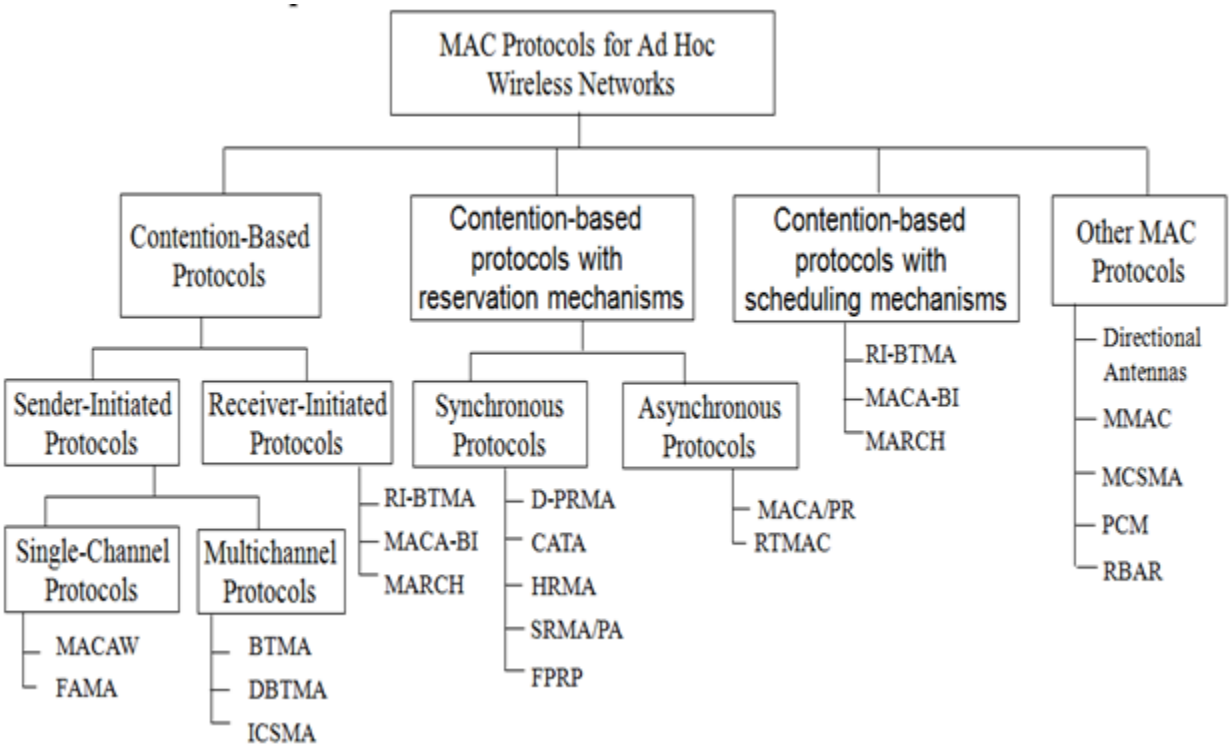

Figure 18: Types of MAC protocols [22]

Here our main aim is to identify different types of MAC protocol which can reduce or minimize the hidden and exposed terminal problem. Different types of MAC protocol to solve these problems are discussed below: [13,21,22,23]

- **Multiple Access collision Avoidance Protocol (MACA):**

This protocol is one of the earliest protocols proposed by KARN. It is an alternative to carrier sensing that does not use Carrier Sense Multiple Access (CSMA). Multiple access with collision avoidance (MACA) can be used avoid hidden terminal and exposed terminal problem.

The process is described below:

1. When a node wants to transmit a data packet, it first transmits a RTS (Request To Send) frame.
2. The receiver node, on receiving the RTS packet, if it is ready to receive the data packet, transmits a CTS (Clear to Send) packet.
3. Once the sender receives the CTS packet without any error, it starts transmitting the data packet.
4. If a packet transmitted by a node is lost, the node uses the binary exponential back-off (BEB) algorithm to back off a random interval of time before retrying.
5. In the BEB mechanism, a collision is detected each time and node doubles its maximum back off window.
6. Both the RTS and CTS packets carry the expected duration of the data packet transmission.
7. A node near the receiver (overcoming the hidden node problem) on hearing the CTS packet, defers its transmission till the receiver receives the data packet.
8. A node near the sender (overcoming the exposed node problem) hears the RTS is free to transmit simultaneously when the sender is transmitting data.

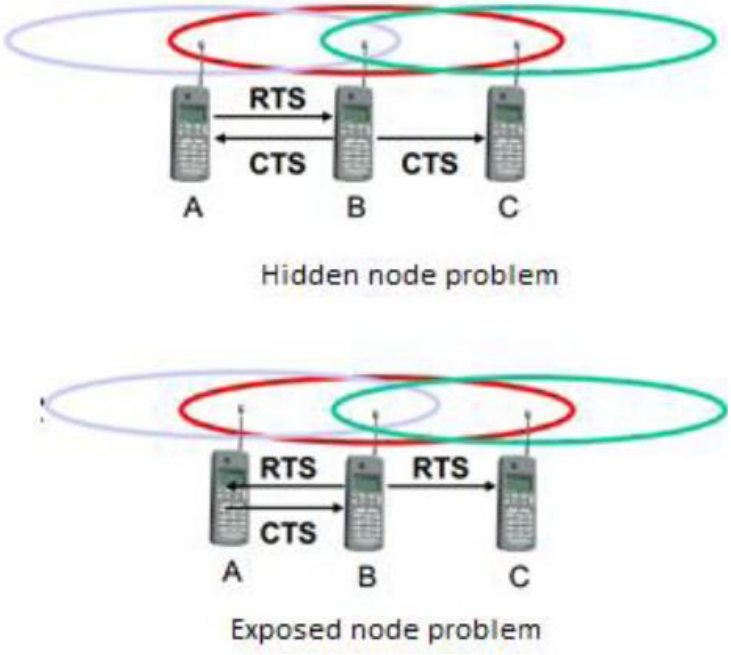

Figure 19: Process of MACA

- **<u>Multiple Access collision Avoidance for Wireless (MACAW) Protocol:</u>**

It uses a five step RTS–CTS–DS–DATA–ACK exchange. MACAW allows much faster error recovery at the data link layer by using the acknowledgment packet (ACK) that is returned from the receiving node to the sending node as soon as data reception is completed. MACAW achieves significantly higher throughput compared to MACA. It however does not fully solve the hidden and exposed terminal problems.

The whole process of MACAW:

1. The sender senses the carrier to see and transmits a RTS frame if no nearby station transmits a RTS.

2. The receiver replies with a CTS frame.

3. Neighbors

- See CTS, and then keep quiet.
- See RTS but not CTS, and then keep quiet until the CTS is back to the sender.

4. The receiver sends an ACK when receiving a frame while the neighbors keep silent until they see ACK.
5. There is no collision detection as the senders know collision when they don't receive CTS. So they each wait for the exponential backoff time.

- **Floor Acquisition Multiple Access (FAMA):**

The Floor Acquisition Multiple Access (FAMA) is another MACA based scheme that requires every transmitting station to acquire control of the floor (i.e., the wireless channel) before it actually sends any data packet. Unlike MACA or MACAW, FAMA requires that collision avoidance should be performed both at the sender as well as the receiver. In order to acquire the floor, the sending node sends out an RTS using either non-persistent packet sensing (NPS) or non-persistent carrier sensing (NCS). The receiver responds with a CTS packet, which contains the address of the sending node. Any station overhearing this CTS packet knows about the station that has acquired the floor. The CTS packets are repeated long enough for the benefit of any hidden sender that did not register another sending node's RTS. There are two variations of FAMA. They are:

- RTS-CTS exchange with no carrier-sensing uses the ALOHA protocol for transmitting RTS packets.
- RTS-CTS exchange with non- persistent carrier-sensing uses non-persistent CSMA for the same purpose.

- **Busy Tone Multiple Access (BTMA) Protocol:**

It is one of the earliest protocols proposed to overcome the hidden terminal problem.
The transmission channel is split into two parts:

- A data channel for data packet transmission.
- A control channel used to transmit the busy tone signal.

When a node is ready for transmission, it senses the channel to check whether the busy tone is active. If not, it turns on the busy tone signal and starts data transmission. Otherwise, it

reschedules the packet for transmission after some random rescheduling delay. When a node is transmitting, no other node in the two-hop neighborhood of the transmitting node is permitted to simultaneously transmit.

- **Multiple access collision avoidance-by invitation (MACA-BI) Protocols:**

In typical sender-initiated protocols, the sending node needs to switch to receive mode (to get CTS) immediately after transmitting the RTS. Each such exchange of control packets adds to turn around time, reducing the overall throughput. MACA-BI is a receiver-initiated protocol and it reduces the number of such control packet exchanges. Instead of a sender waiting to gain access to the channel, MACA-BI requires a receiver to request the sender to send the data, by using a Ready-To-Receive (RTR) packet instead of the RTS and the CTS packets. Therefore, it is a two-way exchange (RTR–DATA) as against the three-way exchange (RTS–CTS–DATA) of MACA. Since the transmitter cannot send any data before being asked by the receiver, there has to be a traffic prediction algorithm built into the receiver so it can know when to request data from the sender. The efficiency of this algorithm determines the communication throughput of the system. When the receiver receives this data, it is able to predict the backlog in the transmitter and send further RTR packets accordingly. There is a provision for a transmitter to send an RTS packet if its input buffer overflows. In such a case, the system reverts to MACA. The MACA-BI scheme works efficiently in networks with predictable traffic pattern. The hidden node problem is overcome by this protocol.

- **Use of directional antennas in MAC protocol:**

MAC protocols use directional antennas. The advantage of this method is that the signals are transmitted only in one direction. The nodes in other directions are therefore no longer prone to interference or collision effects, and spatial reuse is facilitated. The signal interference is reduced, system throughput is increased, channel reuse is improved, low probability of detection, robustness to jamming, and other beneficial features.

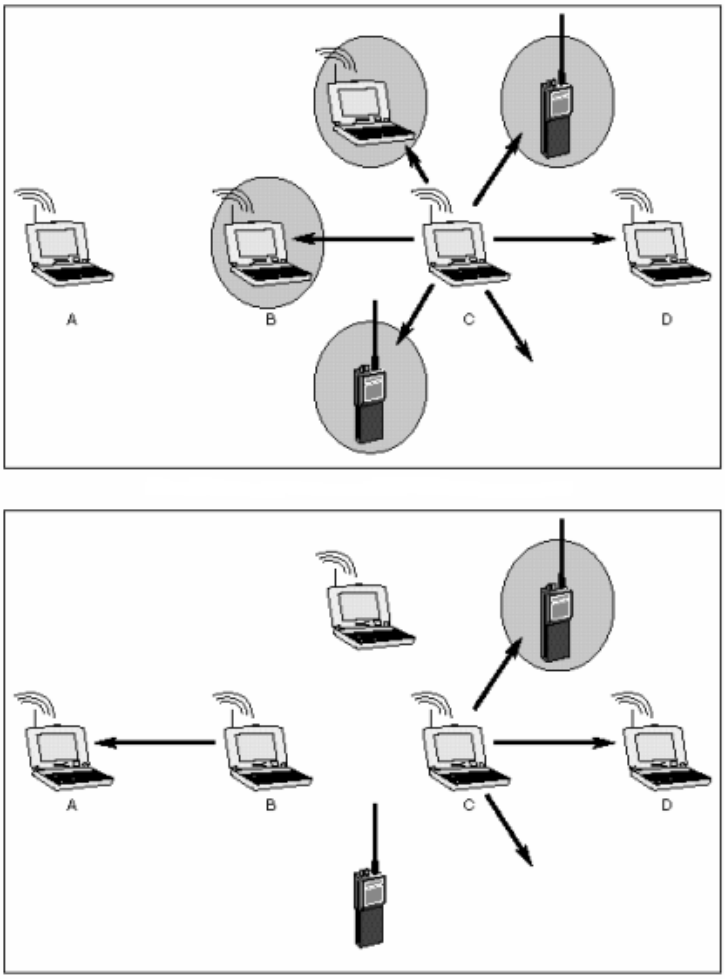

Figure 20: Directional Antennas in MAC protocol

3.6 Existing Research Works

Many researchers have worked in this field. We have studied their research papers and have gained important knowledge that helped us in our thesis work. Some of the important points that we have understood from studying their research papers are noted below:

1. **A Comparison Study of Omnidirectional and Directional MAC Protocols for Ad hoc Networks – by** Zhuochuan Huang and Chien-Chung Shen

Huang and Shen conducted a comparison study of existing directional and omnidirectional MAC protocols by contrasting their features and evaluating their performance under various network load and topology. Specifically, they presented justification for the better performance of some directional antenna based MAC protocols by using the metric of *effective spatial reuse*, which is also verified by their simulation study. [13]

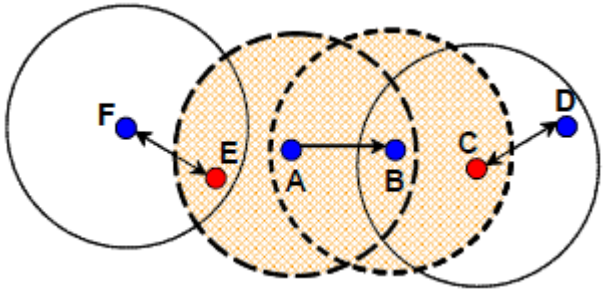

Figure 21: Example of spatial reuse

2. **Interference Minimization in Physical Model of Wireless Networks - by** Hakob Aslanyan

In order to minimize the interference in adhoc network Hakob proposed to assign a transmission power to each node of a network such that the network is connected and at the same time the maximum of accumulated signal straight on network nodes is minimum. He considers more general interference model, 'the physical interference model', where sender nodes' signal straight on a given node is a function of a sender/receiver node pair and sender nodes' transmission

power. For this model he gave a polynomial time approximation algorithm which finds a connected network with at most $O((\text{opt} \ln n)^2 / \beta)$ interference, where $\beta \geq 1$ is the minimum signal straight necessary on receiver node for successfully receiving a message. [14]

3. **Interference Minimization in Wireless Networks - by** Hakob Aslanyan and Jose Rolim

This is the second research that Hakob has done relating to interference minimization. Here he has teamed up with Jose. Both of them together proposed to assign a transmission radius to each node of a network, to make it connected and at the same time to minimize the maximum number of overlapping transmission ranges on each node of a network. Additional means of topology control besides the connectivity is blocking the long line connections at the receiver level. We propose a polynomial time approximation algorithm which finds a connected network with at most $O((\text{opt} \ln n)^2)$ interference where 'opt' is the minimal interference of the given network of n nodes. The lower bound for this problem, where a general distance function is considered, has been proven to be $O(\ln n)$. The algorithm is known which finds a network where the maximum interference is bounded by $O(\sqrt{n})$. [4]

4. **Minimizing Interference in Ad Hoc and Sensor Networks**- by Thomas Moscibroda and Roger Wattenhofer

According to Thomas and Roger the amount of interference experienced by a node *v* corresponds to the number of other nodes whose transmission range covers *v*. At the cost of communication links being dropped, interference can be reduced by decreasing the node's transmission power. In this paper, they have studied the problem of minimizing the average interference while still maintaining desired network properties, such as connectivity, point-to-point connections, or multicast trees. [6]

5. **Minimizing Interferences in Wireless Ad Hoc Networks through Topology Control –** by Guinian Feng, Soung Chang Liew and Pingyi Fan.

This paper investigates minimizing mutual interferences in wireless ad hoc networks by means of topology control. Prior work defines interference as a relationship between link and node. This paper attempts to capture the physical situation more realistically by defining interference as a relationship between link and link. They formulated the pair-wise interference condition between two links, and showed that the interference conditions for the minimum-transmit-power strategy and the equal-transmit-power strategy are equivalent. Based on the pair-wise definition, they further investigated the "typical" interference relationship between a link and all other links in its surrounding. To characterize the extent of the interference between a link and its surrounding links, they defined a new metric called the 'interference coefficient'. They investigated the property of 'interference coefficient' in detail by means of analysis and simulation. Based on the insight obtained, they proposed a topology control algorithm – 'minimum interference algorithm' (MIA) – to minimize the overall network interference. Simulation results indicate that the network topologies produced by MIA show good performance in terms of network interference and spanner property compared with known algorithms such as LIFE, disk graph, Gabriel Graph and *k*-NEIGH. They have considered MIA to minimize network interference while conserving energy and maintaining good spanner property. Since MIA minimizes network interference, it is optimal and has better performance than other algorithms in that respect. [24]

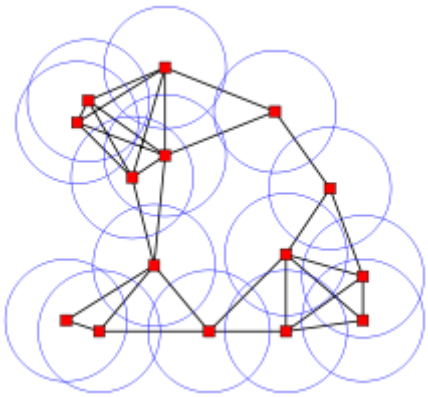

Figure 22: Disk Graph

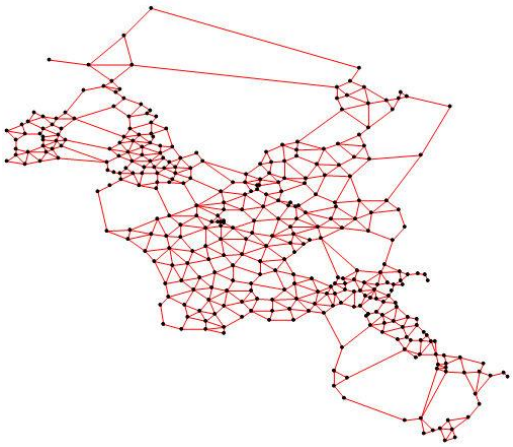

Figure 23: Gabriel Graph

6. **Minimizing Interference for the Highway Model in Wireless Ad-Hoc and Sensor Networks** – by Haisheng Tan, Tiancheng Lou, Francis C.M. Lau, Yuexuan Wang, and Shiteng Chen

Finding a low-interference connected topology is one of the fundamental problems in wireless ad-hoc and sensor networks. The receiver-centric interference on a node is the number of other nodes whose transmission ranges covers the node. The problem of reducing interference through adjusting the nodes' transmission ranges in a connected network can be formulated as that of connecting the nodes by a spanning tree while minimizing interference. In this paper, they have studied minimization of the average interference and the maximum interference for the high-way model, where all the nodes are arbitrarily distributed on a line. Two exact algorithms are proposed. One constructs the optimal topology that minimizes the average interference among all the nodes in polynomial time, $O(n^3 \Delta^3)$, where n is the number of nodes and Δ is the maximum node degree. The other algorithm constructs the optimal topology that minimizes the maximum interference in sub-exponential time, $O(n^3 \Delta O(k))$, where $k = O(\sqrt[4]{\Delta})$ is the minimum maximum interference. In this paper, they studied the problem to minimize the receiver-centric interference for the highway model. Based on the no-cross property and using dynamic programming, the first polynomial-time exact algorithm for constructing a connected topology with minimum

average interference is proposed. They gave also the first sub-exponential-time exact algorithm for constructing a connected topology while minimizing the maximum interference. [12]

7. **Low-Interference Topology Control for Wireless Ad Hoc Networks** – by Kousha Moaveni-Nejad and Xiang-Yang Li

Topology control has been well studied in wireless ad hoc networks. However, only a few topology control methods take into account the low interference as a goal of their methods. Some researchers tried to reduce the interference by lowering node energy consumption (i.e. by reducing the transmission power) or by devising low degree topology controls, but none of those protocols can guarantee low interference. In this paper, Nejad and Li projected algorithms to construct a network topology for wireless ad hoc networks such that the maximum (or average) link (or node) interference of the topology is either minimized or approximately minimized. They planned algorithms to construct a network topology for wireless ad hoc network such that the maximum link (or node), or the average interference of the topology is either minimized or approximately minimized. They also have studied how to construct topology locally with small interference while it is power efficient for unicast routing. [2]

8. **Future Directions in Ad hoc Networking Research** – by Anders Lindgren, Kaustubh S. Phanse, Tomas Johansson, Robert Brannstrom, and Christer Ahlund

Current research on ad hoc networks has mainly focused on connected networks where it is always possible to find a contiguous path between source and destination. There is however a number of scenarios where network partitioning is rather common, which renders regular ad hoc routing and transport protocols useless. There has been some research on routing in purely intermittently connected networks where all communication is local between peering nodes and the mobility of nodes is used to bring messages closer to their destination as shown in the figure no. 24. [3]

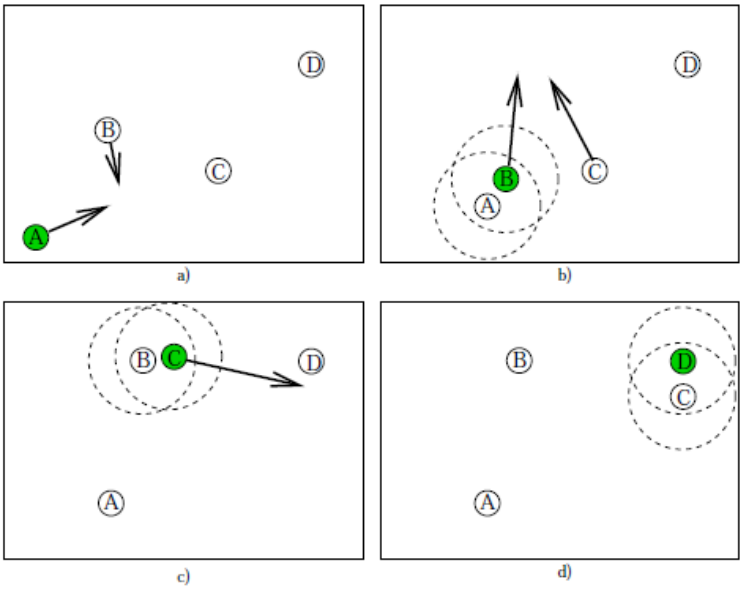

Figure 24: Transitive communication

9. **Interference Aware Multipath Selection for Video Streaming in Wireless Ad Hoc Networks** – by Wei Wei and Avideh Zakhor

In their paper, Wei and Zakhor proposed a novel multipath selection framework for video streaming over wireless ad hoc networks. They proposed a heuristic interference-aware multipath routing protocol based on the estimation of concurrent packet drop probability of two paths, taking into account interference between links. Through both simulations and actual experiments, they showed that the performance of the proposed protocol is close to that of the optimal solution, and is better than that of other heuristic protocols. With the increase in the bandwidth of wireless channels, and in the computing power of mobile devices, video applications are expected to become widespread in wireless ad hoc networks in a near future. [5]

10. **Securing Ad Hoc Networks** – by Lidong Zhou and Zygmunt J. Haas

Ad hoc networks are a new wireless networking paradigm for mobile hosts. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, Zhou and Haas studied the threats that an ad hoc network faces and the security goals to be achieved. They identified the new challenges and opportunities posed by this new networking environment and

explored new approaches to secure its communication. In particular, they took advantage of the inherent redundancy in ad hoc networks, multiple routes between nodes to defend routing against denial of service attacks. They also used replication and new cryptographic schemes, such as threshold cryptography, to build a highly secure and highly available key management service, which forms the core of our security framework. [7]

11. **A Review Paper On Ad Hoc Network Security –** by Karan Singh, Rama Shankar Yadav, and Ranvijay

In this article, they have presented an overview of the existing security scenario in the Ad-hoc network environment. They discussed key management and Ad-hoc routing of wireless Ad-hoc networks. They have briefly presented the most popular protocols that follow the table-driven and the source-initiated on-demand approaches. Their comparison between the proposed solutions and parameters of ad hoc network shows the performance according to secure protocols. They have also discussed about routing protocol and challenges and authentication in ad hoc network. [8]

3.7. Justification of this project

A primary issue in wireless communication is interference where communication between two parties is affected by transmissions from a third party. High interference increases the probability of packet collisions and therefore packet retransmission which can significantly affect the effectiveness of the system and the energy use. Therefore it is desirable to keep a low interference at every node. Reducing interference is one of the main challenges in wireless communication, and particularly in ad hoc networks. So the main aim of this thesis is to mitigate the effect of interference in adhoc networks. The starting process is to show the interference effect and then design an estimated filter from some mathematical expression and simulation using some definite value. Here interference is considered due to the other users or nodes operating in same channel and not by any other method. Filter estimation process is both cost effective and simple which makes the minimization of interference process easier.

CHAPTER 4: Project Framework

4.1 Methodology adopted and type of research

Minimization of interference in adhoc network is an explanatory research methodology. A design of filter is proposed to reduce the interference effect or it can be said an algorithm is developed which can be useful in the world of adhoc networks. This can in turn increase the capacity of network which can be useful in future development. The research focuses on the extending the current theory for the interference handling in adhoc networks. Before this research, many journals and research papers has been studied and then it was decided to go for designing an optimum filter. The other aim of the research is to show directional antenna could be a better choice to eliminate hidden and exposed terminal problems in adhoc networks.

The research can be classified as a quantitative research since the validation of proposed model of a filter solely depends on mathematical and simulation results. Moreover some mathematical model, theorems and hypothesis is also used for the result. Quantitative research always depends on the statistical model using some theoretical data and some simulation result. This resembles a bridge between a proposed theory and real application.

A detailed study of different journals was done for checking out the work done in the context of interference. So there was some interesting work done on to minimize the interference. There was actually several ways of minimizing the interference and most importantly how the interference is created. Actually there are several ways of creation of interference as the network discussed in this research works on 2.4 GHz frequency which comes under unlicensed spectrum so as an example a cordless phone can create interference. The research work is carried out using the interference created by other users i.e. other users act as interferer.

Two remedies are discussed here to lessen the interference created by other users working on same frequency and most probably on the same channel. The remedies are:

- A filter is designed to reduce the interference and it can possibly be matched to a real filter to make a real filter. The filter described here is an estimated filter made on some definite value, mathematical theorems and simulation of all the input using a code.

- Directional antenna can be preferred instead of Omni-directional antenna to remove the hidden and exposed terminal problem faced by Omni-directional antenna which gives rise to unexpected delay and packet loss due to interference created by other users.

4.2 Experimental setup

This chapter is going to discuss the setup process of the adhoc network.

4.2.1 Setup of Adhoc Network

1. At first we select our central computer. This computer must remain on at all times in order for other computers to connect to the ad hoc network.

2. Next we click "Start" and press "Connect To." We choose "Show All Connections." If we don't see "Connect To," then we go to "Control Panel" and select "Network Connections."

3. Now we click "Set up a connection or network". We choose "Set up an ad hoc network" and click "Next." We follow the steps in the network creation wizard to create our network.

4. Then we right-click our wireless connection under "Network Connections." We choose "Properties" and click the "Wireless Networks" tab.

5. Next we press "Add" to create a new network. Then we type a short name for our network in the "Network Name" box. We choose our security options from the selections of "No authentication (open)," "WEP" and "WPA-2 Personal." WEP and WPA-2 are the best choices for good security, with WPA-2 being the better selection, as it is more secure than WEP.

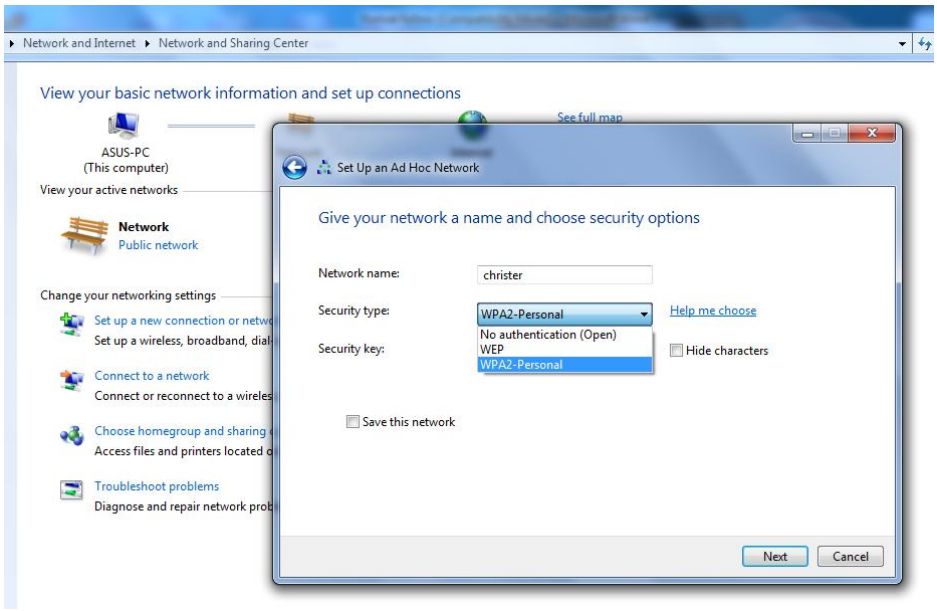

Figure 25: Security options in Adhoc network

6. Now we have to enter a security key or passphrase that is a string of eight to sixty-three letters and numbers. We must make a note of our passphrase, keeping in mind that the letters are case sensitive. If we use upper-case letters, we have to be sure to record them properly. Later we will enter the same passphrase when we set up other computers on our ad hoc network.

7. We check the "This is a computer to computer (ad hoc) network" checkbox at the bottom of the screen. We press "OK" to create the network and right-click our Internet connection and choose "Properties." Next we go to "Advanced" and check the "Allow other users to connect through this computer's Internet connection" box. Then we choose "Wireless" as our connection type and we press "OK" to share our Internet connection.

8. Then we click "Next" to create our ad hoc network. A panel should appear indicating our adhoc network is ready for use.

9. We then use another computer to scan for available wireless networks to find the ad hoc network we created. We select our network and click "Connect." The computers should

now be able to communicate over our ad hoc network.

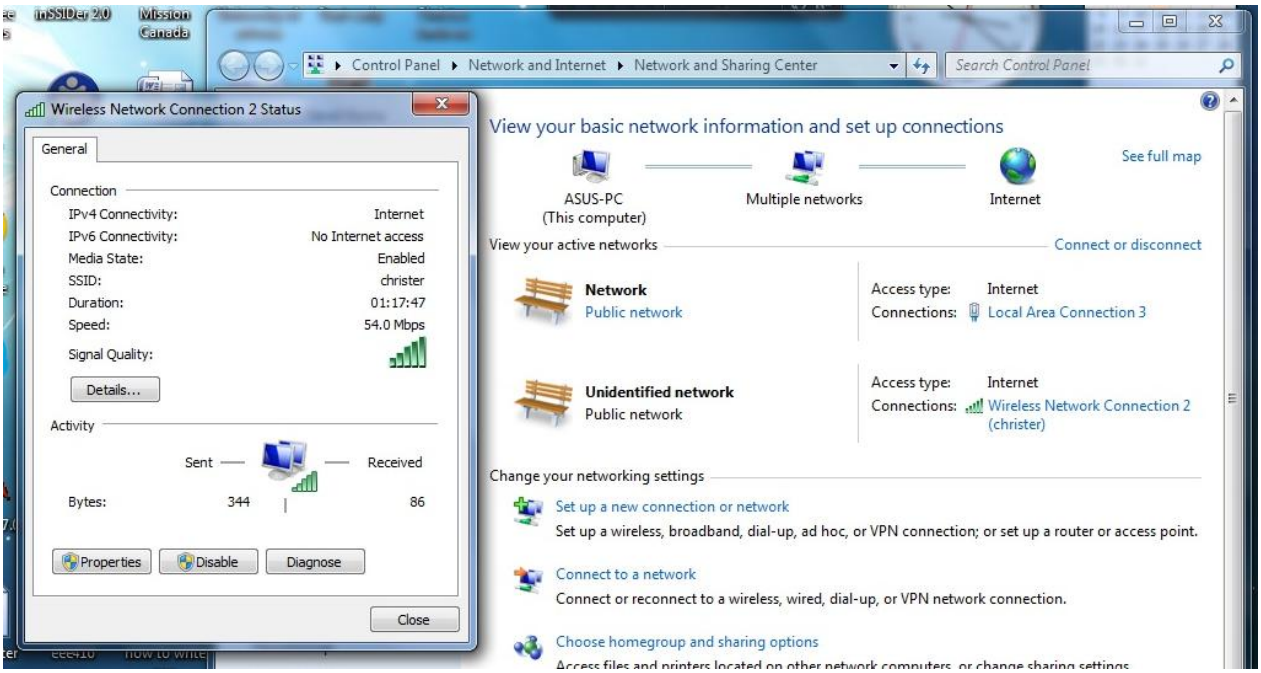

Figure 26: Connection status of Adhoc network

To set up an ad-hoc wireless network, each wireless adapter must be configured for ad-hoc mode versus the alternative infrastructure mode. In addition, all wireless adapters on the ad-hoc network must use the same SSID and the same channel number. [15]

4.2.2 Security options

There are three security options in the adhoc network. They are:

- No authentication (open): This type of connection is not secured as no password is required for connection and can be accessed by anyone inside the network. This can be possibly created when the session is very short. This type of connection is not preferred.

- WEP (Wired Equivalent Privacy): As the name suggests, this is wireless equivalent to wired LANs security by encrypting data transmissions which further avoids unwanted entry to the connected network.WEP is not often used in IEEE 802.11b as its power is not adequate to run WEP without any additional degradation. Though WEP is secured but still it has some defects like inadequate message authentication, 802.11 access control mechanism and much more. This deficiency can attract hackers to get into the network and cause damage by gathering only a sufficient amount of data collected from WEP protocol.

- WPA2- Personal (Wi-Fi Protected Access Version 2): Before discussing WPA2, WPA should be introduced. WPA is promoted by Wi-Fi alliance to overcome the drawback of WEP. It supports AES (Advanced Encryption Standard) which is a type of encryption algorithm highly rated by cryptographers eventually replaced DES (Data Encryption Standard) which is another type of encryption algorithm in VPN (Virtual Private Network) due to the resistance from all known cryptanalysis. For home users PSK (Pre-Shared Key) is granted which requires a password to connect with other users. WPA2 is a successor to WPA which also includes IEEE 802.11i standard and also backward compatible to AES providing stronger encryptions. It is more secured than WEP.

Any of these can be used to create an adhoc network. Both WEP and WPA2 requires password to make any connection with other users.

4.3 Proof of Interference

The simulation is done using softwares named MATLAB, VISTUMBLER and INSSIDER. Three laptops have been used in the simulation process. At the end of the simulation an external laptop joins the adhoc network created by us. Here L1 is the receiver laptop and L2 and L3 are transmitter laptop. L1 was kept in one room and L2 and L3 were moved nearly at a distance of 6

meters from L1. L1 was using the software INSSIDER for capturing the signals coming from other laptops. It is an effective software to check the interference in between the laptops.

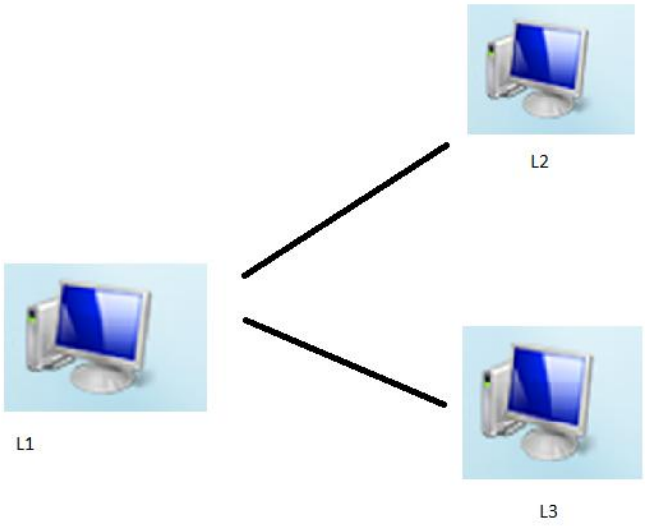

Figure 27: Arrangement of Simulation laptops

The software named VISTUMBLER is used here to analyze the adhoc connection between the laptops in the network. The X-axis of the graph shows the signal strength and the Y-axis shows the time. The simulations generated by the VISTUMBLER are as follows:

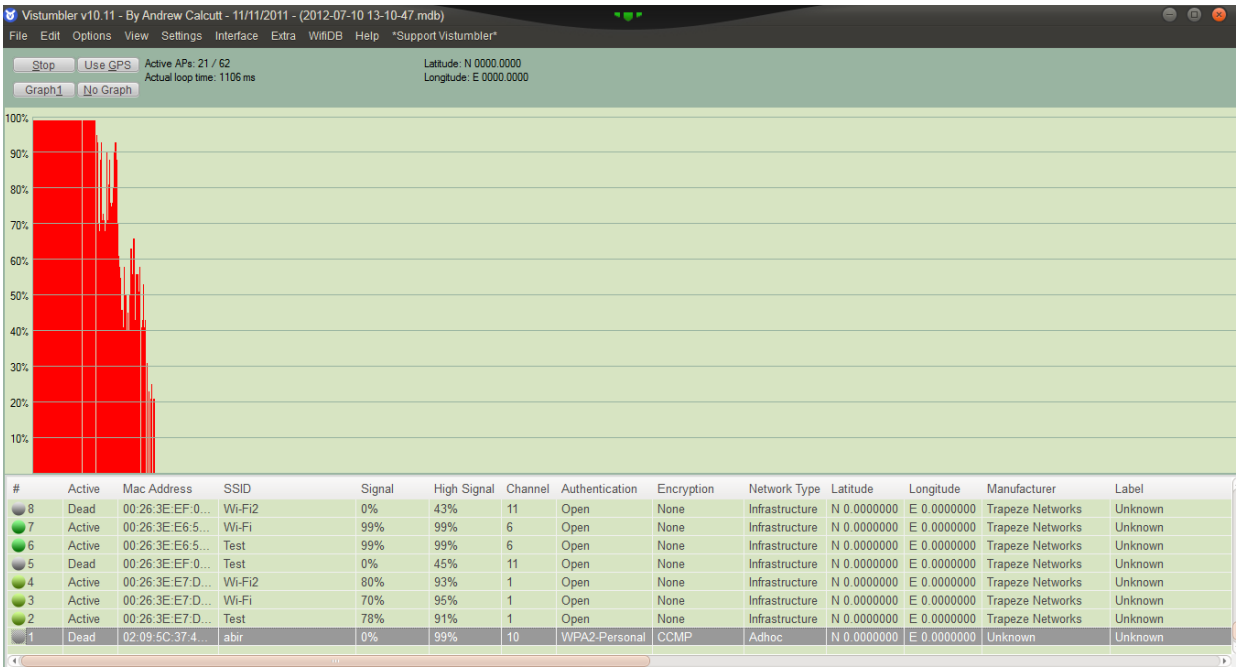

Figure 28: VISTUMBLER- SHOT 1

In shot 1 of VISTUMBLER simulation it can be observed that initially the signal strength is 100% but as time goes by the signal strength reduces. This degradation in the graph is due to the movement of other laptops in the network to a certain distance from the central laptop, L1 with respect to time. As the laptops move farther away the signal strength decreases gradually and the signal strength reaches to a minimum of 20%.

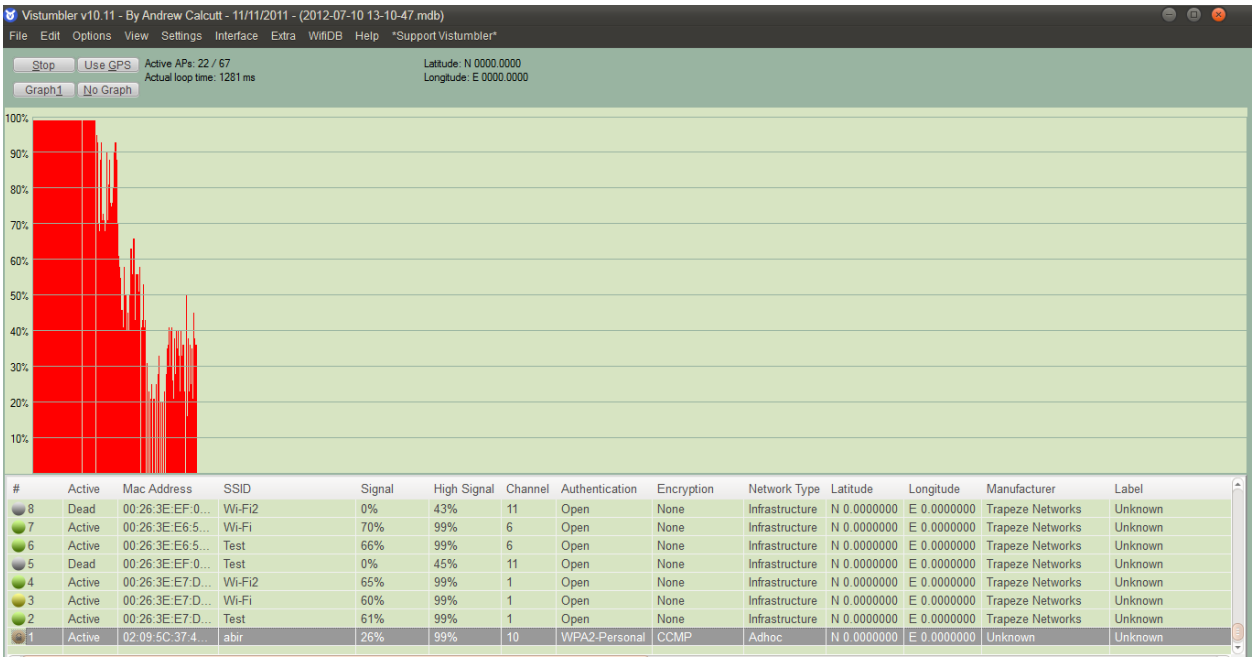

Figure 29: VISTUMBLER- SHOT 2

In shot 2 it can be observed that the signal strength increases gradually from 20% as the laptops come closer to the central laptop i.e. L1.

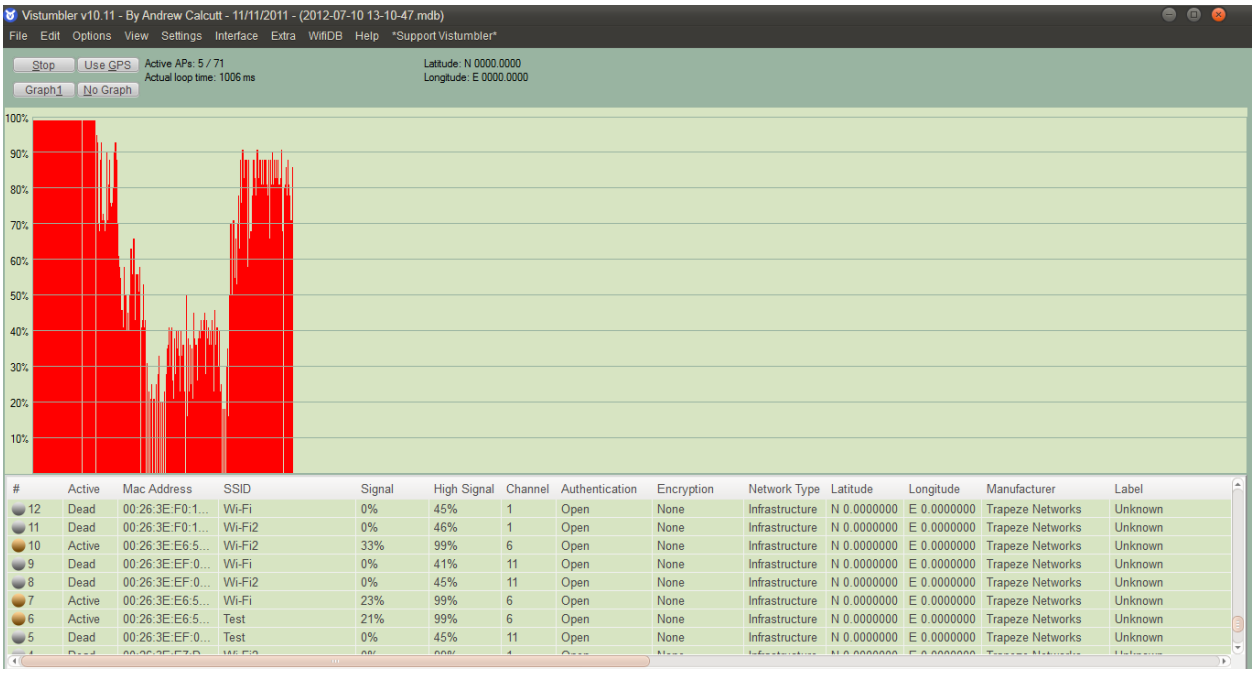

Figure 30: VISTUMBLER- SHOT 3

In shot 3 it is seen that the signal strength is gradually increasing as other laptops are coming closer. A point for lookout is that in the middle of the graph the signal strength suddenly decreased to 20% from 45% for a very short time which was due to the unexpected interference of an external laptop.

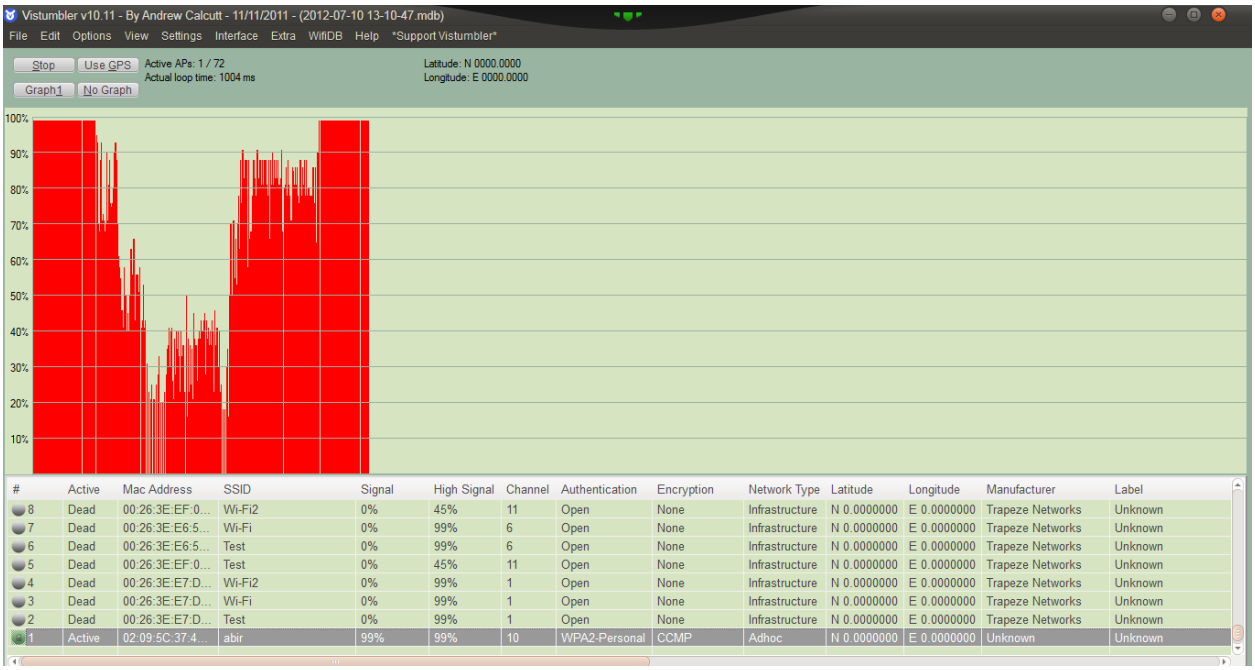

Figure 31: VISTUMBLER- SHOT 4

In shot 4 it is observed that the signal strength has reached 100% as all the laptops in the network are close to each other.

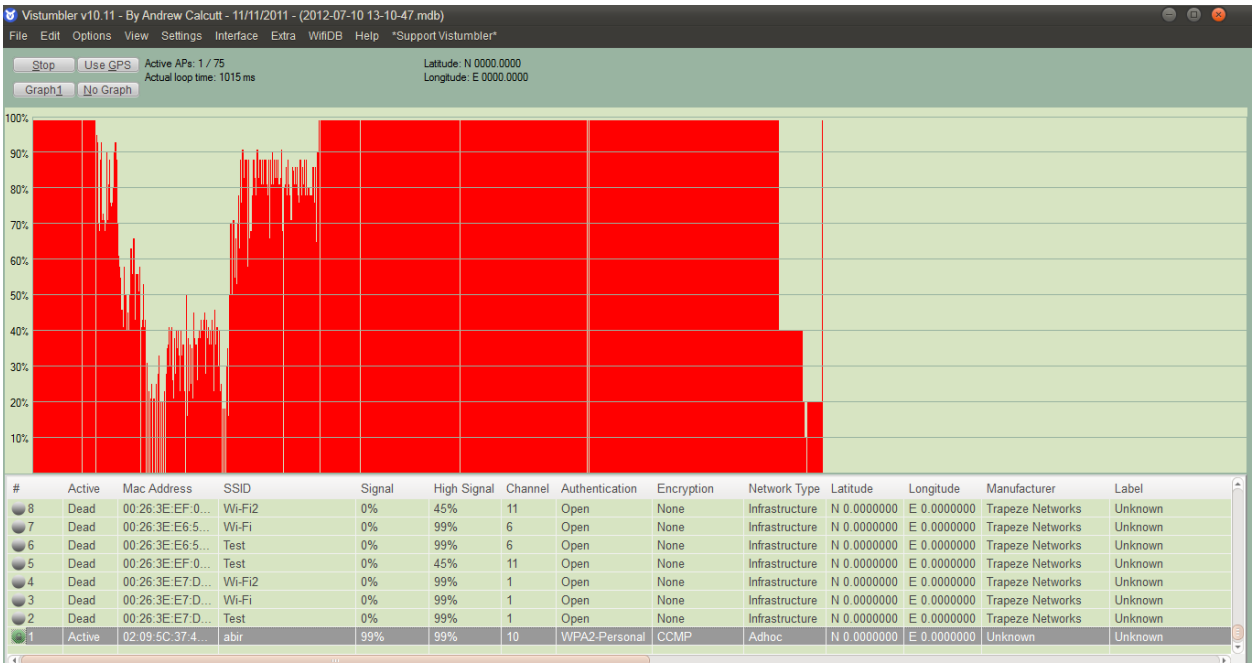

Figure 32: VISTUMBLER- SHOT 5

In shot 5 it is seen that as time passes by, the signal strength remains at 100% as the laptops are kept close to each other.

Simulation results generated by the software INSSIDER to check the interference between the laptops in the adhoc network are as follows:

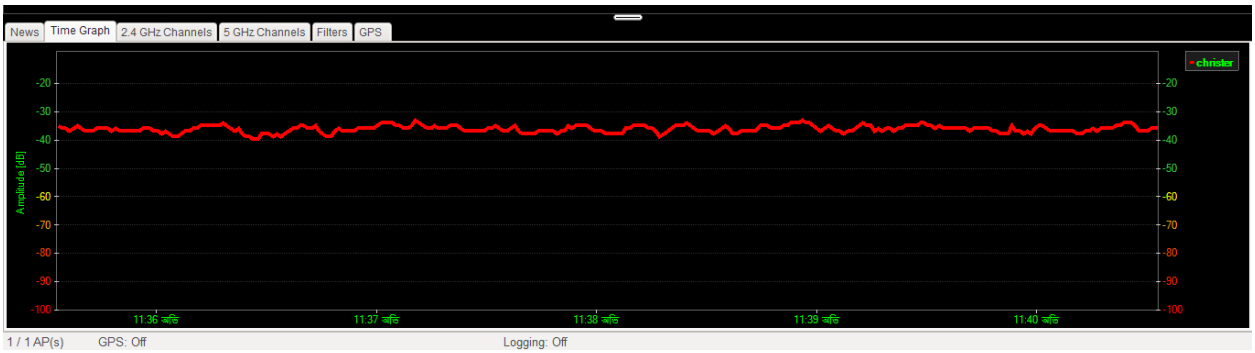

Figure 33: INSSIDER- SHOT 1

Here only L1 is in the adhoc network. So the signal amplitude is constant at -35 dB. There are no other interference.

Figure 34: INSSIDER- SHOT 2

Here L2 is added to the network. The signal amplitude decreases as there is interference in between L1 and L2.

Figure 35: INSSIDER- SHOT 3

Next, L3 was kept in front of L1 while the connection between L2 and L3 was established. Now a great change can be seen. The signal strength is more compared to the previous one. This shows the uncertainty of the wireless networks.

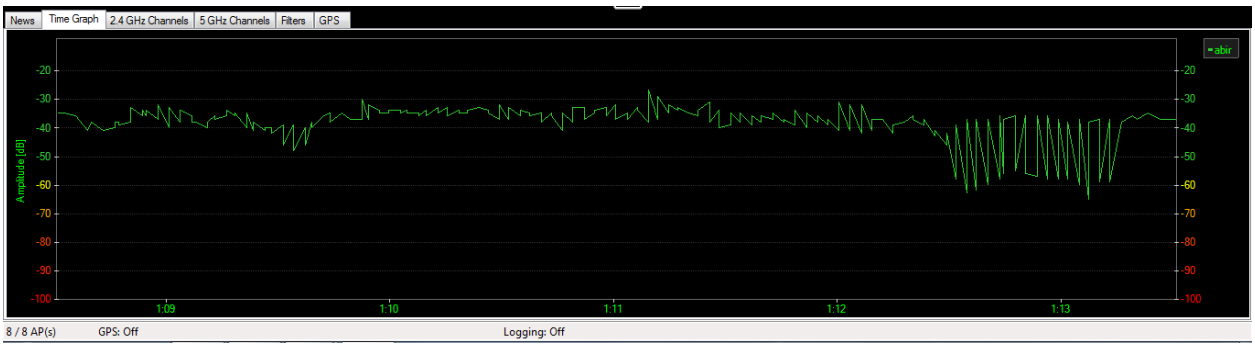

Figure 36: INSSIDER- SHOT 4

The interference increased as the laptops were moved away from L1.

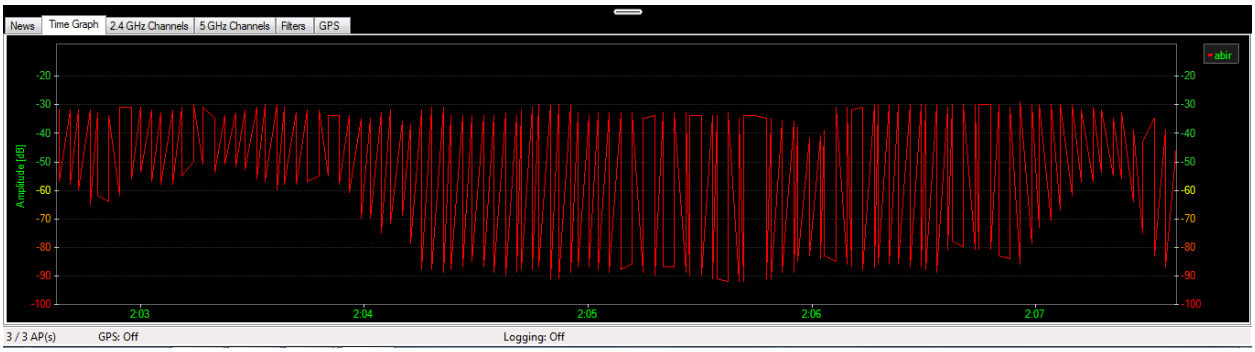

Figure 37: INSSIDER- SHOT 5

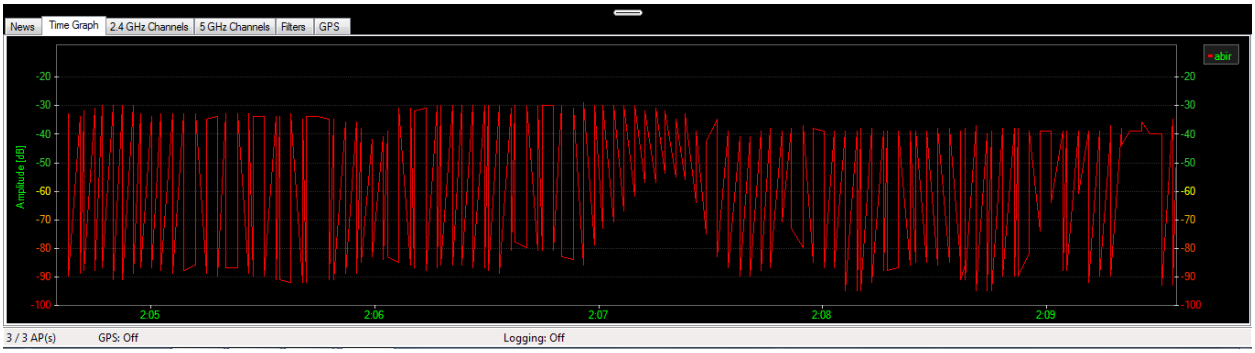

Figure 38: INSSIDER- SHOT 6

The two simulation graphs above show the increased interference as the laptops were moved farther apart from L1.

Figure 39: INSSIDER- SHOT 7

The interference reached its maximum when an external laptop entered into the network.

Figure 40: INSSIDER- SHOT 8

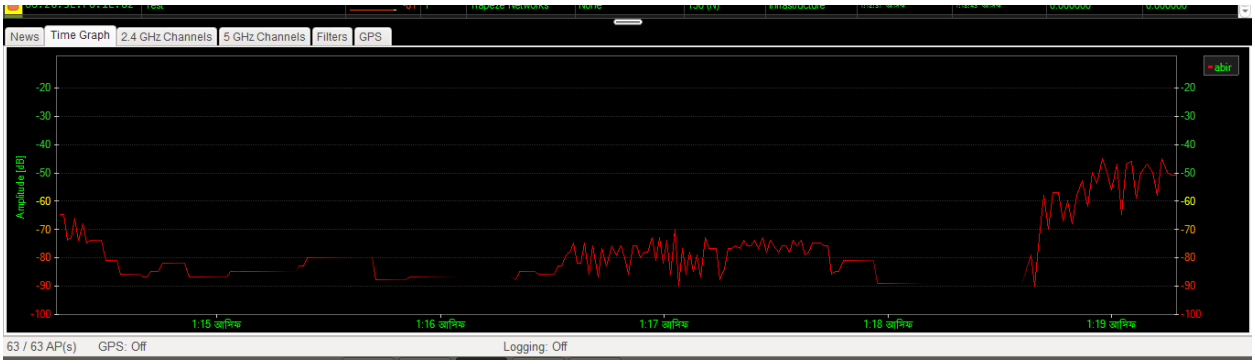

Figure 41: INSSIDER- SHOT 9

The above figures show that the signals almost faded away as the laptops were nearly out of range of L1.

Figure 42: INSSIDER- SHOT 10

Now both laptop L2 and L3 started their respective ad-hoc networks. For the first 6-7 minutes the both signal were nearly constant having a large interference while using different channels. In that time the position of both L1 and L2 were changed randomly but the signal strength never changed very strangely. After that L2 and L3 were disconnected so a straight line was in the graph.

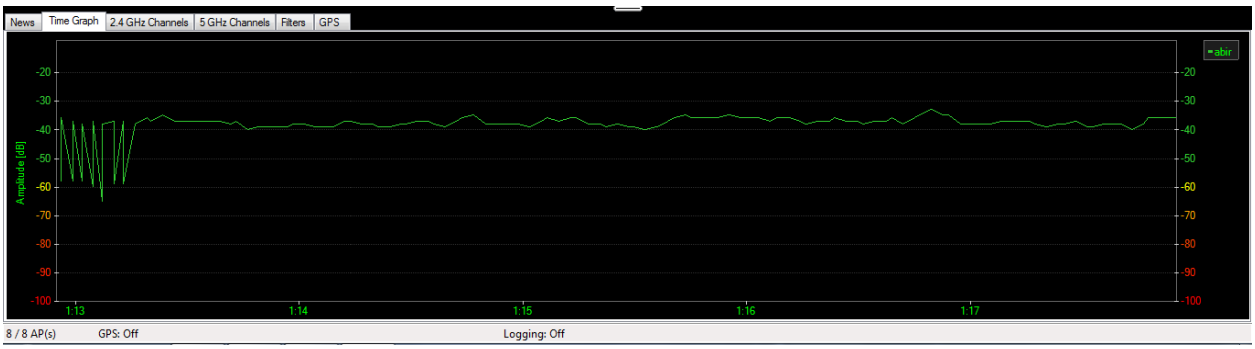

Figure 43: INSSIDER- SHOT 11

This is the final scenario when all the connections are disconnected in the network and the amplitude is constant at -35dB.

CHATER 5. Proposed solution to interference

Filter Estimation using MATLAB

The main aim of this project is to mitigate the effect of interference in a wireless adhoc network. For mitigation, some mathematical equations are used which can further be used for making a filter to tackle the interferers which are none other than users who are not supposed to be in that network. Here one estimated filter model is described to work with simulation results provided from some equations. The interferer can be related to Hidden and Exposed node problem.

A simple model is taken to describe a basic receiver. The equation used is as follows:

$$\boxed{Y = Hx + n} \quad \text{.....[33]}$$

- Here Y is the received signal. It is a (n*1) matrix.
- H is the (n*n) channel matrix. Here the values of the matrix depend on the channel.

$$H = \begin{vmatrix} h_{11} & h_{12} & \dots & h_{1K} \\ h_{21} & h_{22} & \dots & h_{2K} \\ h_{31} & h_{32} & \dots & h_{3K} \\ h_{41} & h_{42} & \dots & h_{4K} \end{vmatrix} \quad \text{.....[33]}$$

- X is the transmitted signal of (n*1) matrix sent by k number of users.
- N is the Gaussian noise of (n*1) matrix from the channel which cannot be tolerated. It has to be considered with the received signal whenever any assumption is taken.

- n is the length of the filter.

Now the general notion is when a signal is transmitted and received by the receiver, in general, it is not possible to get the actual signal when it is received. So error minimization technique is used. This can be described with an equation which is as follows:

$$\boxed{e_1 = x_1 - \tilde{x}_1} \quad \text{.....[33]}$$

- e_1 = error in estimation
- x_1 = transmitted signal
- $\tilde{x}_1$ = estimated signal

The above equation shows the error in estimation can be calculated and can also be minimized so that the receiver can get nearly same signal as the transmitted one. The estimated error should be as less as possible to retrieve the required signal. An LMS approach is used to train the filter coefficient so that after a number of trains, the desired signal can be achieved. It can be said an adaptive LMS algorithm is used to update the linear filter coefficients.

$\tilde{x}_1$ can also be written as

$$\boxed{\tilde{x}_i = \mathbf{g}_i^T \mathbf{y}} \quad \text{.....[33]}$$

Here g_1 is the actual received signal

This is the part of the method which is known as Linear MMSE- Wiener solution. Now the new formula used to determine the signal is:

$$\varepsilon_{\min} = \min\left(E\left\{ \left| x_i - \mathbf{g}_i^T \mathbf{y} \right|^2 \right\} \right) \quad \text{.....[33]}$$

$\varepsilon_{\min}$ = mean square error

Here the information bits used are BPSK (Binary Phase Shift Keying) as the information can only be +1 or -1 which makes the estimation little easy. These bits are passed through a pseudo-random spreading code. The following code taken from the Matlab code shows the BPSK bit passing through spreading code.

The mean square error (MSE) formula can also be written as:

$$\varepsilon_{\min} = \sum_{i=0}^{Ltrain} \left| x_i - \tilde{x}_i \right|^2$$

Here Ltrain is the training length which is taken as 6000 in this project for better understanding of MSE. The lower MSE will mean less error which means a better received signal. The load ratio is defined as the ratio of the number of users by the spreading gain. So load ratio changes for every number of users added and when the load ratio is <1, then the system is said to under saturated. When it comes to >1, then the system is said to be oversaturated.

A multiuser detector filter has been employed as a model filter so that it can be entertained to make the simulation more realistic. The coefficients for the forward and backward coefficients of filter area are taken as Successive DFD (S - DFD) and Parallel DFD (P- DFD) respectively.

The following figures are plots of MSE vs Training length or bits. The x-axis shows the number of training length used and Y-axis shows the MSE.

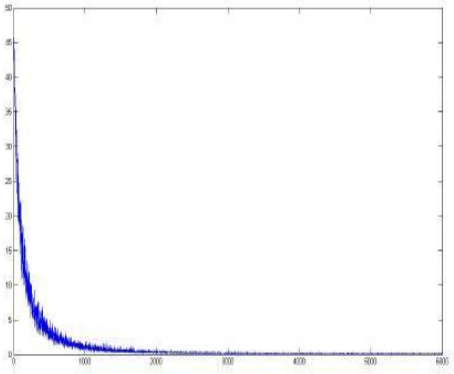

Figure 44: MSE vs Training length- user 3

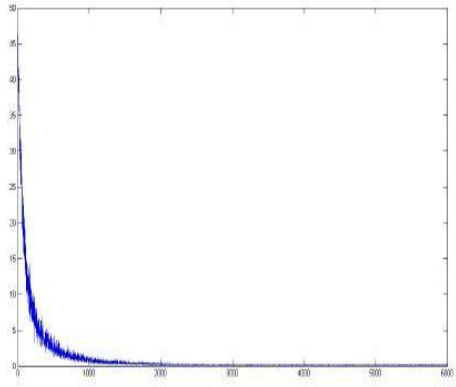

Figure 45: MSE vs Training length- user 7

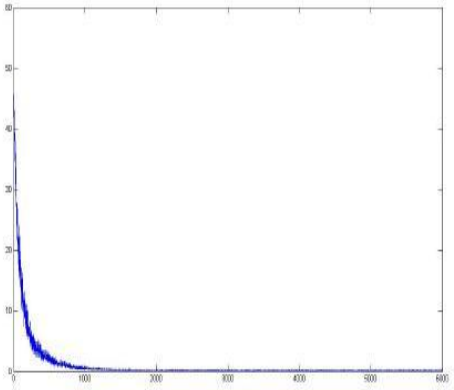

Figure 46: MSE vs Training length- user 10

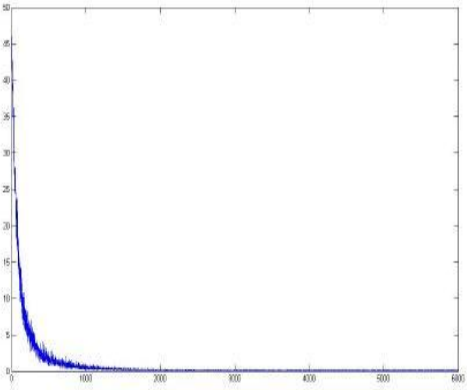

Figure 47: MSE vs Training length- user 12

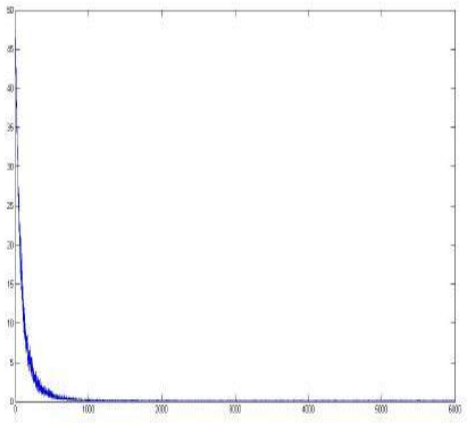

Figure 48: MSE vs Training length- user 15

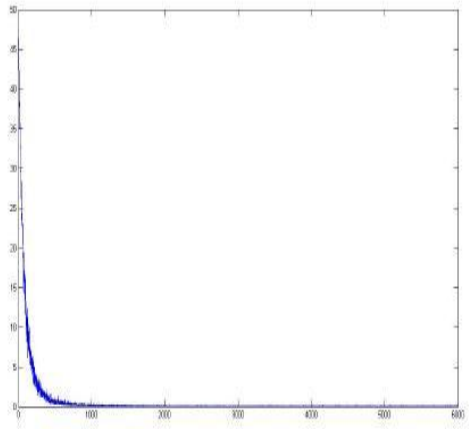

Figure 49: MSE vs Training length- user 17

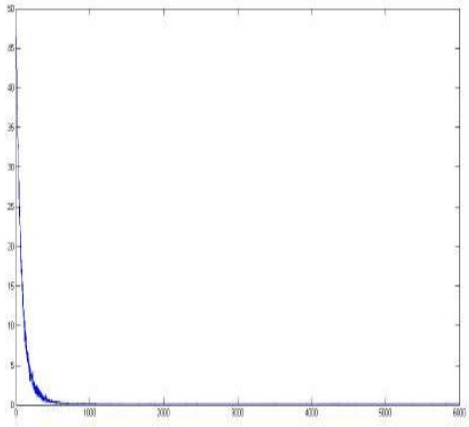

Figure 50: MSE vs Training length- user 18

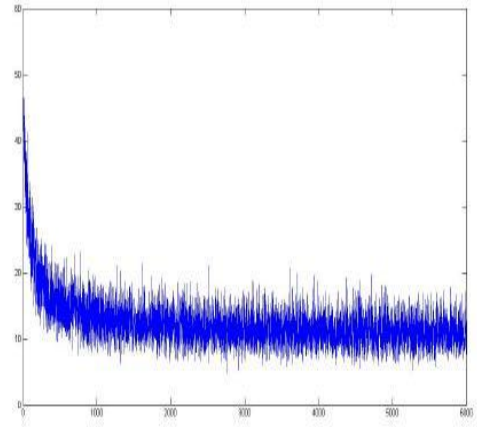

Figure 51: MSE vs Training length- user 19

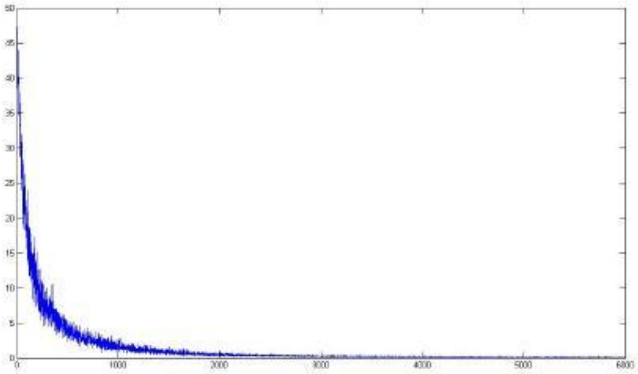

Figure 52: MSE vs Training length- user 20

As it can be seen from the above figures for different number of users, the greater the number of users the more is the fluctuation of MSE at different training length. However after a certain amount of training length, it is possible to get a steady MSE. From 0 to 1000 training length, the graph shows a steep downfall in the MSE which is actually good for the estimated filter. The above plots for different number of users show that fluctuation has decreased rather than increasing with increasing number of users which shows the effectiveness of our proposed estimated filter in minimizing the interference in ad-hoc network.

Now we shall see plots of EA vs packets. Here an average called Enfumble average (EA) is used to show the average MSE of last 200 packets received by the system. This is done to verify whether the estimated filter works reliably and transmits all the information to the receiver.

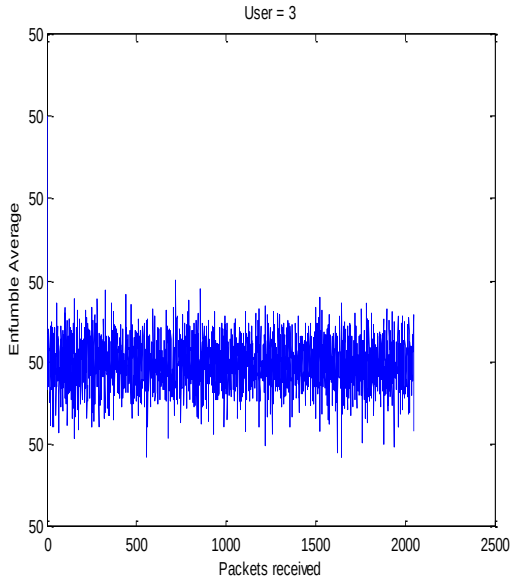

Figure 53: EA vs Packets - user 3

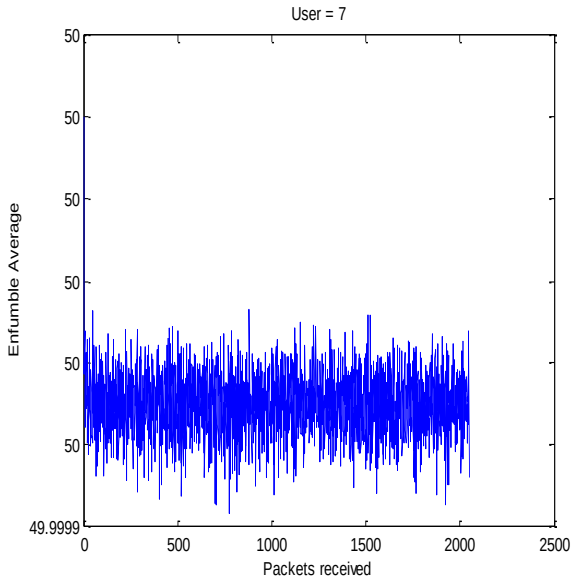

Figure 54: EA vs Packets - user 7

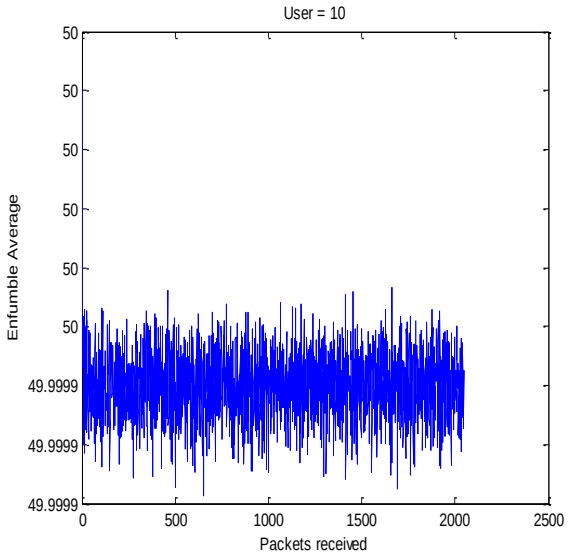

Figure 55: EA vs Packets - user 10

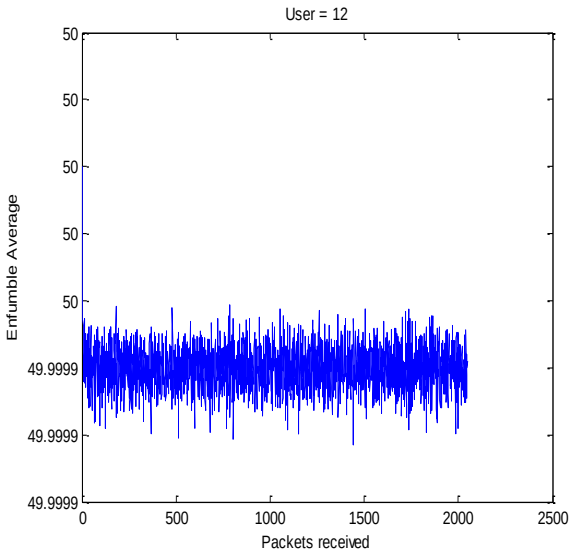

Figure 56: EA vs Packets - user 12

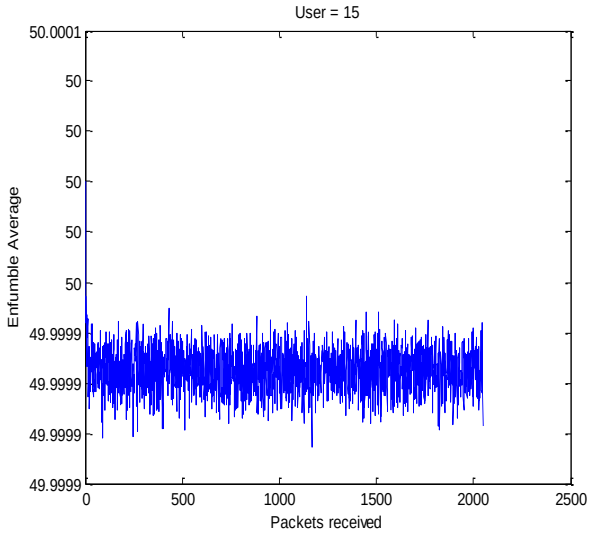

Figure 57: EA vs Packets - user 15

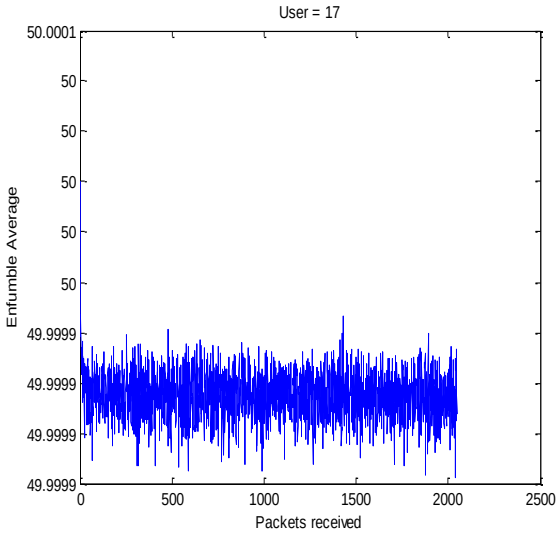

Figure 58: EA vs Packets - user 17

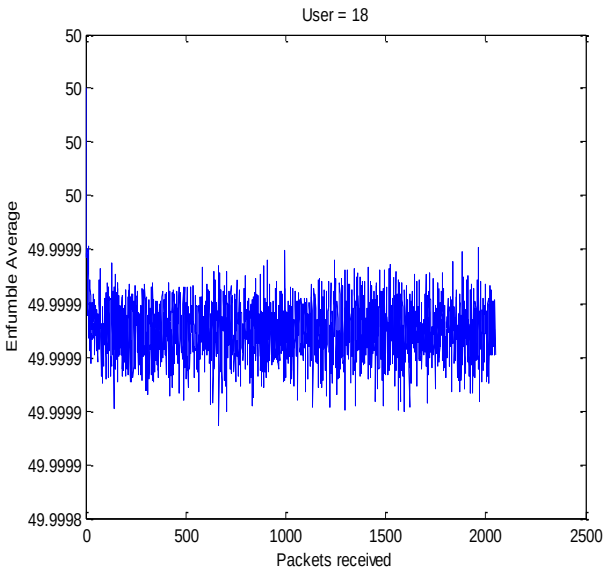

Figure 59: EA vs Packets - user 18

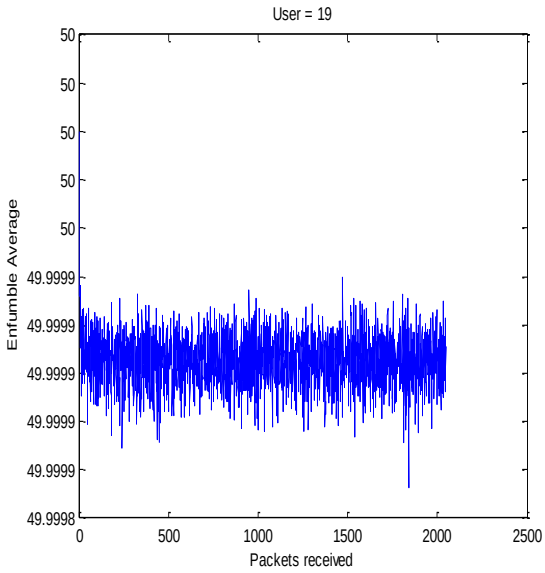

Figure 60: EA vs Packets - user 19

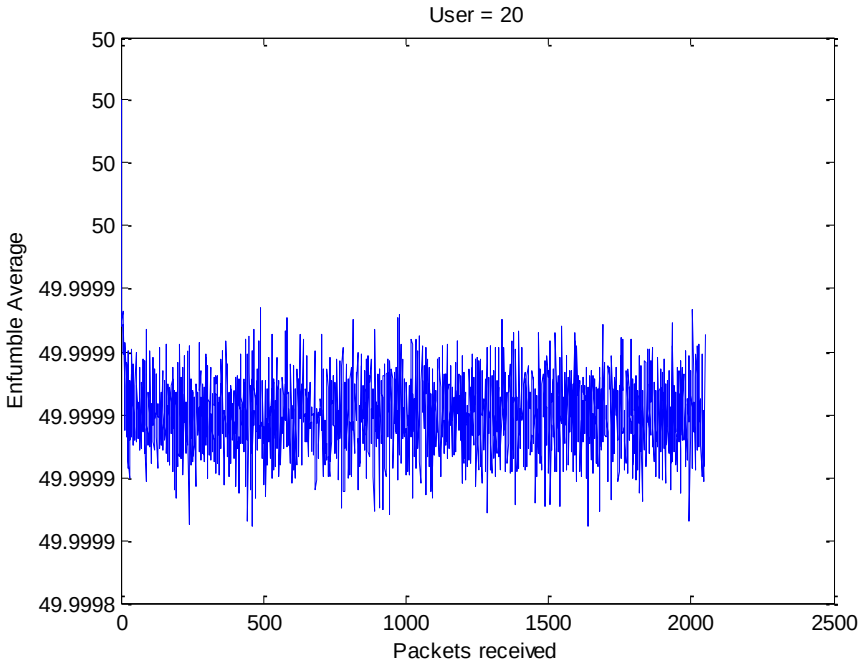

Figure 61: EA vs Packets - user 20

From the above plots it is clearly observed that the enfumble average remains constant around 50 and as number of users increases, the enfumble average decreases but the decrease is not significant which clearly shows the minimizing effect of our estimated filter. Moreover no information is lost in this process.

CHAPTER 6: Conclusion

6.1 Problems faced

- A simulator named Qualnet came from reading some papers which gave an idea of simulating the ad-hoc networks in respect of showing interference or the use of directional antenna. After a long time of research on this simulator, it was believed that it is difficult to handle this simulator so after a week the idea was dropped
- The issues which created problem in the experiment were the connection between three laptops. All the three laptop were of IEEE 802.11 b/g standards but still there was a big problem however it didn't create any big problem but still was debatable. Most of the laptops used in this project for experiment used IEEE 802.11 g as default. When a connection was made in between laptops one of them used 802.11b as default. The problem was due to the fact that the software used for detection of signal was only capable of detecting network cards which worked on IEEE 802.11 g. So to overcome this problem other laptop was used for the purpose.
- The other weird problem came in the picture when a laptop was detecting signals from two laptops but there were three detected signals in the graph of the software. The three sources of signal had three different MAC addresses also. So theoretically it is impossible to have two different MAC addresses from same laptop using a single wireless network card. This problem was overcome by just restarting the software.
- The theoretical ways of getting advantage of using directional antenna over omni-directional were tried using some path loss model but no success due to the fact that the model can be used for any of the antennas.
- We required constant equal internet speed in all the laptops which was difficult to ensure.

6.2 Future Work

This part consist the discussion of using the direction antenna instead of omni-directional and the estimated filter for reduction of interference created by other users.

First the antennas used in the laptops have to be discussed as it was used for showing the interference in the system and then appropriate research was done.

Challenges regarding antenna designs in Laptops are:

- Very compact
- Excessive use of conducting materials which creates problem for antennas
- Effect of other design limitation as mechanical and industrial design

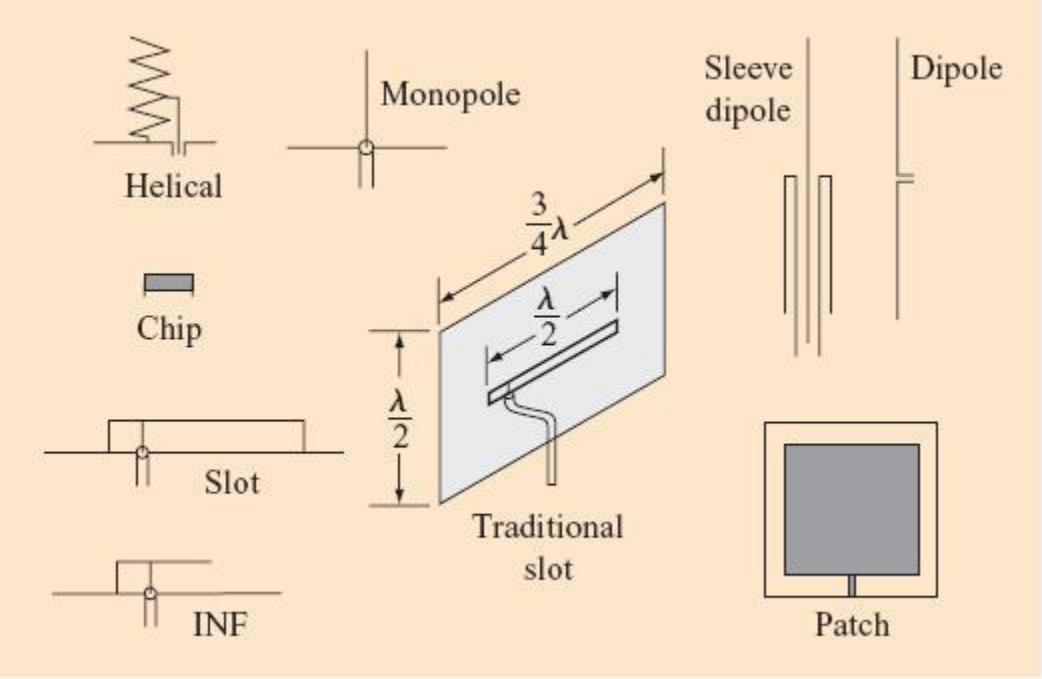

Figure 62: Possible Antennas for Laptops

Dipole and Sleeve dipole antennas work on same principle but the major difference is that one is centre fed and other one is end fed. Dipole antennas are more difficult to use but has wider bandwidth when compared to sleeve dipole antennas.

Helical antennas are small and have narrow bandwidth when compared with monopole antennas. The above antennas work excellent when mounted on top of the display.

Traditional slot and patch antennas are very large so they are placed on the surface of display.

Slot and INF antennas have broad bandwidth so they are an excellent contender to be considered for laptops. Both have similar impedance characteristics. To decrease impedance feed point is moved to slot centre and for increase feed point is moved to slot centre. The slot length is a quarter wavelength long for the INF antenna which makes it more eligible to be used in laptops as very less space is allocated for antenna for the laptops.

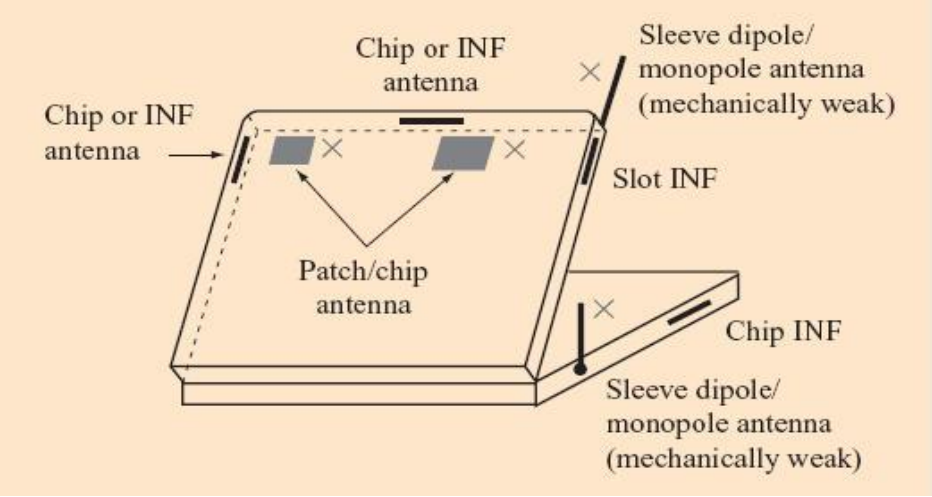

Figure 63: Possible location of different types of antennas in a laptop

Slot and INF have different radiations characteristics.

Advantages of INF over Slot antennas

- Quarter wavelength long as compared with half wavelength long for slot antennas
- Slot antennas has narrower bandwidth than INF
- Two polarization and omni directional radiation pattern

But slot antennas radiate more energy in horizontal direction and hence good for wireless LAN application. The actual problem in deploying antenna system is the lack of space. The only space is either beneath the keyboard surface or the screen. Most of the debate will be on the use of directional antenna in Wi-Fi/Ad-hoc networks due to the complex structure of the antenna. Still

the reach of directional antenna in any mobile device is restricted due to the cost involved but the ongoing work in wireless will someday make it possible in a reasonable cost.

The estimated filter which is showed in this paper is simulated with some values. So it can be changed at any respect of time. The values here taken are considered to an optimal values for ad-hoc network. Such as the value of SNR taken in the code that is also described before and the training length can be taken anything more than 2000 or less whichever gets the MSE optimal or constant at some time. It is not possible to get a constant value but the average will do.

The estimated filters coefficient can be matched to a filter and the real filter can be designed through this method.

The interference in adhoc network is shown and based on some theoretical analysis of omni-directional antenna; directional antenna is proposed in order to minimize the interference. The estimated filter can be designed in real life by using some matched filter to use it with the filter co-efficients to get the desired filter. The desired value of the factors used in the estimation can be treated as the real value as it can get the simulation to work.

The interference can be shown more accurately with some simulators like Qualnet. Although there are so many MAC protocols for directional antenna but a new protocol can be designed to tackle with the disadvantages of the directional antennas. Due to the cost factor, smart directional antennas are still not used but in future the advancement in the wireless system can decrease the cost factor. From the graphs, it can be understood that the estimated filter can be used for the users till load ratio is 1. After that it is very difficult to accommodate more number of users. A different type of estimation can also be taken to optimize while designing the filter.

6.3 Final Words

We believe that interference in wireless networks (and particularly in ad hoc and sensor networks) will be a major issue in the future that ought to be of interest to both practitioners and theoreticians alike. There are many paths for future research. The study of more complex network properties that need to be maintained is clearly one of them.

References

[1] C.Siva Ram Murthy and B.S. Manoj, " Ad hoc Wireless Networks- Architectures and Protocols", 2nd edition, Pearson Education, 2007

[2] Kousha Moaveni-Nejad and Xiang-Yang Li, "Low-Interference Topology Control for Wireless Ad Hoc Networks", USA, Old City Publishing, Inc., 2005.

[3] Anders Lindgren, Kaustubh S. Phanse,Tomas Johansson, Robert Brannstrom and Christer Ahlund, "Future Directions in Ad hoc Networking Research", Lulea University of Technology, Skellefte Campus, Sweden, April 18, 2005.

[4] Hakob Aslanyan, Jose Rolim, "Interference Minimization in Wireless Networks", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2010

[5] Wei Wei and Avideh Zakhor, "Interference Aware Multipath Selection for Video Streaming in Wireless Ad Hoc Networks", IEEE Transactions on Circuits And Systems For Video Technology, VOL. 19, NO. 2, pp: 165-178, February 2009

[6] Thomas Moscibroda and Roger Wattenhofer, "Minimizing Interference in Ad Hoc and Sensor Networks", DIALM-POMC'05, Cologne, Germany, September 2, 2005,

[7] Lidong Zhou and Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE network, special issue on network security, November/December, 1999

[8] Karan Singh, Rama Shankar Yadav, Ranvijay**, "**A Review Paper On Ad Hoc Network Security", International Journal of Computer Science and Security, Volume (1): Issue (1), pp: 52-69.

[9] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding- Royer, "A Secure Routing Protocol for Ad Hoc Networks", Washington DC 20007

[10] M. Benkert, J. Gudmundsson, H. Haverkort, and A. Wol, "Constructing minimum-interference networks", Computer Geometry Theory Applications, 40(3):179{194, 2008.

[11] P. Santi, "Topology control in wireless ad hoc and sensor networks", ACM Computer Survey, 37(2):164{194, 2005.

[12] Haisheng Tan, Tiancheng Lou, Francis C.M. Lau, Yuexuan Wang, and Shiteng Chen, "Minimizing Interference for the Highway Model in Wireless Ad-Hoc and Sensor Networks", SOFSEM 2011, LNCS 6543, pp. 520–532, Springer-Verlag Berlin Heidelberg, 2011

[13] Zhuochuan Huang and Chien-Chung Shen, "A Comparison Study of Omnidirectional and Directional MAC Protocols for Ad hoc Networks", University of Delaware, Newark, DE 19716

[14] Hakob Aslanyan, "Interference Minimization In Physical Model Of Wireless Networks", International Journal "Information Theories and Applications", Vol. 17, Number 3, pp: 235- 248, 2010,

[15] "How to set up an Ad hoc network"- http://www.ehow.com/how_6927360_setup-ad-hoc-network.html

[16] "The advantages of Ad hoc network" - http://www.ehow.com/list_6793071_advantages-ad-hoc-networks.html

[17] "Wireless networks" - http://en.wikipedia.org/wiki/Wireless_network

[18] "Mobile Ad hoc Network" - http://en.wikipedia.org/wiki/Mobile_ad_hoc_network

[19] "Security services" - http://en.wikipedia.org/wiki/Security_service_(telecommunication)

[20] "Routing Protocol" - http://en.wikipedia.org/wiki/Routing_protocol

[21] "MAC Protocols" - http://www.cs.binghamton.edu/~kang/teaching/cs580s/mac_survey.pdf

[22] "MAC Protocols" - http://www.cs.jhu.edu/~cs647/mac_lecture_3.pdf

[23] "MAC Protocols" - http://www.cse.iitb.ac.in/~sri/papers/expnode-ic3n03.pdf

[24] Guinian Feng, Soung Chang Liew, Pingyi Fan, "Minimizing Interferences in Wireless Ad Hoc Networks through Topology Control", ICC 2008, pp: 2332- 2336, IEEE Communication Society, 2008.

[25] "Does Topology Control Reduce Interference?" - www.dcg.ethz.ch/publications/p7125-burkhart.pdf

[26] " Neighbour Attachment Process" – http://dl.acm.org/citation.cfm?id=1333958

[27] " Transmission Radius" - http://dl.acm.org/citation.cfm?id=1387504

[28] "Different types of Antenna" - http://zuji.51.net/bcl/download/tnote01.pdf

[29] "Different types of Antenna" - http://people.scs.carleton.ca/~kranakis/Papers/opodis-04.pdf

[30] "CCNA – Delegate Manual", version 1.1, JUST IT, 2009

[31] Adam Burg, " Ad hoc network specific attacks", Technische Universitat Munchen, 2003

[32] Leonardo Hideki, Raphael Martins, Arthur Guerrante, Ricardo Carrano, Luiz Magalhães, "Evaluating The Impact Of Rts-Cts In Olpc's Xos' Mesh Networks", Universidade Federal Fluminense (UFF), Rio-de-Jenerio, Brazil

[33] Ronald E. Walpole, Raymond H. Myers, Sharon L. Myers, Keying Ye, 'Probability & Statistics for Engineers & Scientists (9th edition)" Prientice Hall | 2011 | ISBN: 0321629116

Appendix

The full and complete MATLAB code developed for our proposed estimated filter.

```
clear all;
clc

global Users
global SprGain
global lx
global trainl
global FFFsize
global FBFsize
global x_bpsk
global SprSeq

Users=15;
SprGain=16;
lx=2048
OPERATINGSNR=30%suitable for ad-hoc networks%
trainl=6000
FFFsize=SprGain;
FBFsize=Users;
num_sim=50
MAXRATIO=0
STEPCHANGE=1

global trainl lx

Pn=10^(-OPERATINGSNR/10);
Amp=sqrt(Pn);


Graph1=zeros(1,trainl);
Graph2=zeros(1,lx);
for sim=1:num_sim
   %The random spreading-sequence is generated for every simulation
   rand('state',sum(100*clock))
   SprSeq=randn(Users,SprGain);
   for k=1:Users
      SprSeq(k,:)=SprSeq(k,:)/sqrt(sum(SprSeq(k,:).^2));
   end

   %The packets change for every simulation. So, does the received
   %signal-symbol vector
```

```
    rand('state',sum(100*clock))
    x_bpsk=sign(rand(Users,lx)-0.5);
    r_ch=zeros(1,lx*SprGain);
    for n=1:lx
       tmp=0;
       for k=1:Users
          tmp=SprSeq(k,1:SprGain)*x_bpsk(k,n)+tmp;
       end
       r_ch((n-1)*SprGain+1:n*SprGain)=tmp;
    end
    r_ch(1:lx*SprGain)=r_ch(1:lx*SprGain)+Amp*randn(1,lx*SprGain);

    index=0;

    for fbratio=0:STEPCHANGE:MAXRATIO
       %indexing from 1 is accepted in MATLAB
       %(compared to the classical from 0)
       index=index+1;

       r_softout_uc=zeros(Users,lx);

       %It does not matter if the same packet is re-used for every
       %step-size constant ratio, because the forward (wf) and the
       %backward (wb) filters are re-trained for different step-size
       % ratio's by seeting them to zero-initial values
       wf=zeros(Users,FFFsize);
       wb=zeros(Users,FBFsize);

       m1=0.008; %nearly saturated system, 15/16

       m2=m1*fbratio;
       mmudf=0.0000001;
       mmudb=mmudf*fbratio;
       [wf,wb,mse_t]=trainF(Amp,m1,m2,wf,wb,SprSeq);

       [r_softout_uc, mse]=useF(r_ch,wf,mmudf,wb,mmudb);

       Graph1(1,:)=Graph1(1,:)+ mse_t(1,:);
       Graph2(1,:)=Graph2(1,:)+ mse(1,:);
       [fbratio sim]
    end % Step size ratio loop
end % End for simulations loop
figure;plot(Graph1(1,:))
figure;plot(Graph2(1,:))
```

Call function: Trainf

```
function   [wf,wb,mse_t]=trainF(Amp,m1,m2,wf,wb,SprSeq)
% Train a decision feedback mulStiuser estimator (DFME) with a known
% training sequence

global ltrain SprGain Users FFFsize FBFsize
 rand('state',sum(100*clock))
er1=0;
xtrain=sign(rand(Users,ltrain)-0.5);
r=zeros(1,ltrain*SprGain);
%r=(spreading sequence)*(individual binary symbol) FOR THE ENTIRE PACKET
for n=1:ltrain
   tmp=0;
   for k=1:Users
      tmp=SprSeq(k,1:SprGain)*xtrain(k,n)+tmp;
   end
   r((n-1)*SprGain+1:n*SprGain)=tmp;
end
r(1:ltrain*SprGain)=r(1:ltrain*SprGain)+Amp*randn(1,ltrain*SprGain);

wf=zeros(Users,FFFsize);
wb=zeros(Users,FBFsize);
mse_t=zeros(Users,ltrain);

for k=1:Users
   for n1=1:ltrain
      z1=0;
      for n2=1:FFFsize
         z1=z1+wf(k,n2)*r((n1-1)*SprGain+n2);
      end
      for n2=1:FBFsize %Parallel DFD type, all the users-interference is taken onboard
         z1=z1-wb(k,n2)*xtrain(n2,n1);
      end
      er1=xtrain(k,n1)-z1;
      mse_t(k,n1)=er1*er1;
      for n2=1:FFFsize
         wf(k,n2)=wf(k,n2)+m1*er1*r((n1-1)*SprGain+n2);
      end

      for n2=1:FBFsize
         wb(k,n2)=wb(k,n2)-m2*er1*xtrain(n2,n1);
      end
      wb(k,k)=0;
   end
end
```

Call function: Usef

```
function  [r_softout_uc, mse]=useF(r_ch,wf,m1,wb,m2)
% Decision directed mode
%
global lx Users SprGain FFFsize FBFsize

r_softout_uc=zeros(Users,lx);
for n1=1:lx
   xd=zeros(1,Users);
   for k=1:Users
      z1=0;
      for n2=1:FFFsize
         z1=z1+wf(k,n2)*r_ch((n1-1)*SprGain+n2);
      end
      for n2=1:FBFsize %Parallel DFD type, all the users-interference is taken onboard
         z1=z1-wb(k,n2)*xd(n2);
      end
      r_softout_uc(k,n1)=z1;
      xd(k)=sign(z1);
      if z1==0 z1=-1;
      end
      er1=z1-xd(k);
      mse(k,n1)=er1*er1;
      for n2=1:FFFsize
         wf(k,n2)=wf(k,n2)+m1*er1*r_ch((n1-1)*SprGain+n2);
      end

      for n2=1:FBFsize
         wb(k,n2)=wb(k,n2)-m2*er1*xd(n2);
      end
      wb(k,k)=0;
   end
end
```