NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

WIRELESS LAN PERFORMANCE & SIMULATION SOFTWARE COMPONENTS

Graduation Project
COM – 400

Student: **Muhammad Irfan Javed**

Supervisor: **Mr. Izzet Agoren**

Nicosia - 2004

In the name of ALLAH, who is the most merciful and most gracious.

ACKNOWLEDGEMENTS

First of all I would like to thank my ***ALLAH*** who helped me during this project and who helps me in every aspect of my life. Without the help of ***ALLAH*** I was not this caliber to complete my project.

I would like to express my deep appreciation to my advisor ***Mr.Izzet Agoren***, who helped me to approach the problems from different perspectives and to define the scope of what I needed to accomplish, his suggestions and observations were extremely helpful throughout this project. He always pointed out my mistakes and suggested solutions to the problems I encountered and without his guidance, suggestions and encouragement. It was not possible to find the right track in finishing this work in such a good manner.

A special note of appreciation goes to my ***parents*** and all the other ***family members*** for their unlimited encouragement, prayers, support and love during my life.

I would also like to thank my ***housemates*** who encouraged and helped me during my project.

ABSTRACT

The scope of IEEE 802.11 is to develop a Medium Access Control (MAC) sublayer and Physical Layer (PHY) specification for wireless connectivity for fixed, portable and moving stations within a local area.

A thorough understanding of the medium and data-link layers of WLAN is critical for developing and understanding simulation program for WLAN. So, therefore this project also provides you the architectures and techniques implemented in MAC layer of the IEEE 802.11 standard in detail.

This project also focuses on the basic concepts and techniques used in simulation design because the simulation provides highly detailed and accurate statistical information, and can serve as a robust platform for further simulation studies involving WLAN. Simulation involves using a set of equation and state information to measure the performance of a network.

This project also presents the analysis based on the results of simulation. I shall show you that simulation is good tool for examining the performance of the MAC layer.

End part of this project described the weaknesses, pitfalls and some existing problems in IEEE 802.11 standard which I observed during my research. I also describe some ideas to these problems which may help to solve these problems.

TABLE OF CONTENTS

Chapter 2 Background

CHAPTER 4 Simulation Results

Chapter 5 Conclusions

Chapter 6 Future Work

CHAPTER 1

WLAN OVERVIEW

1.0:- Introduction

This chapter defines the WLAN grammatically and technically. Advantages and Applications of WLAN are also given.

WLAN Overview helps you to understand the basic points, functionality of Wireless LAN (WLAN) and IEEE standards for WLAN. It focuses on the technologies implemented in WLAN and techniques used in WLAN.

It will also introduce you with OSI Model, Physical and MAC layers in WLAN technology aspects.

A basic knowledge of networking concepts and terminology used in wireless Communications and TCP/IP is assumed.

1.1:- What is a Wireless LAN (WLAN)?

"***Wireless***" as: - "Without wire or wires; specifically operating with electromagnetic waves and not with conducting wire."

"***LAN***" as: - "A short distance data communications network (typically within a building or campus) used to link computers and peripheral devices under some form of standard control."

1.1.1:-Technical Definition

A Wireless Local Area Network (WLAN) is a LAN which uses radio frequency (RF) and infrared (IR) technology to transmit and receive data over the air.

1.2:- What Is the Interest in Wireless LAN?

- No more cables…
- Mobility
- Increased productivity
- Competition
- Flexibility
- Easy to deploy and setup
- Temporary Networking
- Greater range

1.3:- Wireless LAN Considerations

- The topology of a wireless network is dynamic
- The topology is not always fully-connected
- Air as a medium has no absolute boundaries
- The medium is not well-protected from external signals

1.4:- IEEE Standard for Wireless LAN (WLAN)

The Institute of Electrical and Electronics Engineers (IEEE) has established the IEEE 802.11 standard, which is the predominant standard for wireless LANs. Any LAN application, network operating system, or protocol including TCP/IP, will run on 802.11-compliant WLANs as they would over Ethernet. LAN's. The existing standard and its amendments describe WLAN PHY (Physical layer): Spread spectrum, OFDM, Infrared and MAC layers.

802.11	The original WLAN Standard . Supports 1 Mbps to 2 Mbps.
802.11a	High speed WLAN standard for 5 Ghz band. Supports 54 Mbps.
I802.11b	WLAN standard for 2.4 Ghz band. Supports 11 Mbps.
802.11e	Address quality of service requirements for all IEEE WLAN radio interfaces.
802.11f	Defines inter-access point communications to facilitate multiple vendor-distributed WLAN networks.
802.11g	Establishes an additional modulation technique for 2.4 Ghz band. Intended to provide speeds up to 54 Mbps.
802.11h	Defines the spectrum management of the 5 Ghz band for use in Europe and in Asia Pacific.
802.11i	Address the current security weaknesses for both authentication and encryption protocols. The standard encompasses 802.1X, TKIP, and AES protocols.

Table 1.1:- *IEEE 802.11x with related features*

The aim of the 802.11 standard was to develop a MAC and PHY layer for wireless connectivity for fixed, portable and moving stations within a local area. The higher OSI-layers are the same as in any other 802.X standard; this means that at this level there is no difference perceptible between wired and wireless media

1.5:- WLAN Topologies

There are two operation modes defined in IEEE 802.11x: Infrastructure Mode and Ad Hoc Mode.

1.5.1:- Independent Basic Service Set (IBSS)

IBSS mode is a set of 802.11 wireless stations that communicate directly with each other without using an access point or any connection to a wired network. This basic topology is useful in order to quickly and easily set up a wireless network anywhere a wireless infrastructure does not exist such as a hotel room, a convention center, and our airport.

Independent Basic Service Set (IBSS) is also called *Peer-To-Peer* mode or an *Ad-Hoc*. In an IBSS, the mobile stations communicate directly with each other provided they are within the range of each other.

Important to notice when talking about ad-hoc networks is the capacity of this configuration. The capacity of wireless ad-hoc networks can be very low, due to the requirement that nodes forward each others' packets. Capacity is the limiting factor: a large mobility causes a high volume of routing queries and updates which brings along high congestion, which leads to packet losses.

1.5.2:- Basic Service Set (BSS)

The *Basic Service Set* (BSS) consists of a group of any number of communicating stations. It is a basic building block of an 802.11 wireless LAN.

1.5.3:- Infrastructure Basic Service Set

An Infrastructure Basic Service Set is a BSS with a component called an *Access Point* (AP). All stations in the BSS communicate with the access point and no

longer communicate directly. All frames are relayed between stations by the access point. The access point may also provide connection to a distribution system. There is no restriction on for the distribution system to be wired or wireless.

1.5.4:- Extended Service Set (ESS)

802.11 extends the range of mobility to an arbitrary range through the *Extended Service Set* (ESS). An extended service set is a set of infrastructure BSS's, where the access points communicate amongst themselves to forward traffic from one BSS to another to facilitate movement of stations between BSS's. The access point performs this communication through the distribution system. The distribution system is the backbone of the wireless LAN and may be constructed of either a wired LAN or wireless network.

Access points that act as routers can also assign an IP address to your PC's using DHCP services.

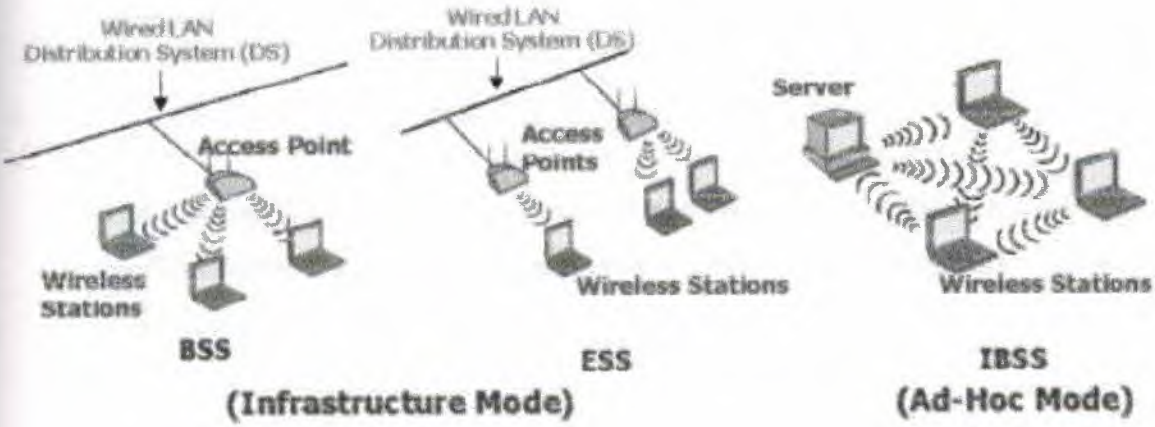


***Figure 1.1:-** 802.11 modes [3]*

1.6:- Access Points

Access point is another term that can be used very generally in reference to a point of access to a network. However, in the context of this book, access point most often refers

to a base station for the IEEE 802.11 wireless LAN protocol. Access points provide computers that are equipped with a mobile radio card to access a LAN, usually via an Ethernet connection.

1.7:- The 802.11x Physical Layer

The Physical layer (PHY) sits below the MAC and serves as an interface to the physical medium. 802.11 defines three different PHYs: direct sequence spread spectrum (DSSS), frequency hoping spread spectrum, and infrared.

1.7.1:- Physical Layer Convergence Procedure (PLCP) sub layer

PLCP adapts the capabilities of the physical medium dependent system to the Physical Layer service. It presents an interface for the MAC sub layer to write to and provides carrier sense and Clear Channel Assessment (CCA).

Upon reception of a frame from the MAC, the PLCP sublayer first adds preamble and header information then passes the entire frame down to the PMD. The preamble consists of a synchronization field (SYNC) and start frame delimiter field (SFD).

1.7.2:- Physical Media Dependent (PMD) sub layer

PMD defines the method of transmitting and receiving data through a wireless medium between two or more stations each using the same modulation system. It takes care of the wireless encoding.

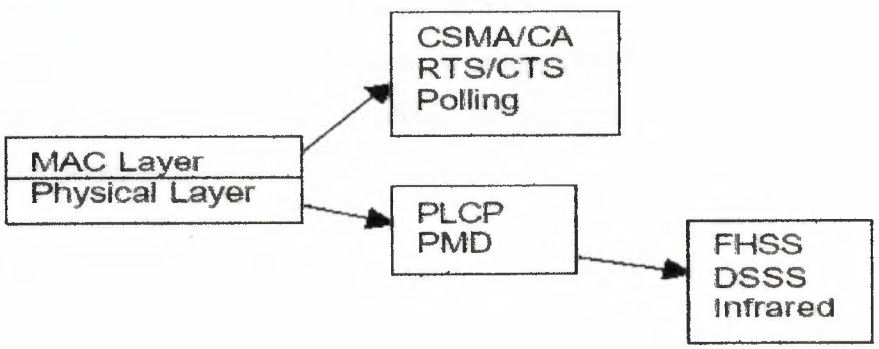


Figure 1.2:-Functions and sublayers of MAC and Physical layer

Two main technologies are used for wireless communications

1.7.3:- Infrared (IR)

IR is not a useful technology for use in a WLAN system since it is used for short distance communications. There is a standard for such products called IrDA.

1.7.4:- Radio Frequency (RF)

RF in this case is located in the 2.4GHz ISM-band. RF is capable of being used for 'not line of sight' and longer distances situations.

There are two methods of spread spectrum modulation used within the unlicensed 2.4-GHz frequency band: frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum(DSSS). Spread spectrum is ideal for data communications because it is less susceptible to radio noise and creates little interference, it is used to comply with the regulations for use in the ISM band.

Using frequency hopping, the 2.4GHz band is divided into 75 1-MHz-channels. FHSS allows for a less complex radio design than DSSS but FHSS is limited to a 2-Mbps data transfer rate, the reason for this are the FCC regulations that restrict subchannel bandwidth to 1 MHz, causing many hops which means a high amount of hopping overhead. For wireless LAN applications, DSSS is a better choice. DSSS divides the 2.4GHz band into 14 channels (in the US only 11 channels are available). Channels used at the same location should be separated 25 MHz from each other to avoid interference. This means that only 3 channels can exist at the same location (figure 2). FHSS and DSSS are fundamentally different signaling mechanisms and are not capable of interoperating with each other.

1.8:- The 802.11 data link layer

A 802.11 data link layer is divided in two sub layers.

1.8.1:- Logical Link Control (LLC)

The LLC sub layer is the same in 802.11 and other 802 LANs and can easily be plugged in into a wired LAN.

1.8.2:- Media Access Control (MAC)

802.11 defines a different MAC protocol. For Ethernet LANs, the CSMA/CD protocol regulates the access of the stations. In a WLAN collision, detection is not possible.

The 802.11 standard defines the protocol and compatible interconnection of data communication equipment via the air, radio or infrared.

1.9:- OSI and Wireless: Layer 3 and Up

The OSI system model applies to the configuration, management, and troubleshooting of WLANs far beyond Layers 1 and 2. Certainly, Layers 1 and 2 are key to WLANs, but the other layers play key roles as well. For example, all configurations of wireless APs and bridges are done through Telnet and HTTP, two Application-layer protocols. The Web interface on APs and bridges use HTTP in their graphical interfaces. This is a key topic to understand because if there is a problem accessing the Web interface, you need to be able to use your knowledge of the OSI system model to troubleshoot the problem. Could the problem be caused by an access list on a router between your system and the AP, is it a problem with general network connectivity, can you ping the AP's TCP/IP Address? These all come into play in determining the cause of the failure.

Bridges and APs also use other protocols in the OSI system model. Examples include the following:

- *Dynamic Host Configuration Protocol* (DHCP) at Layer 7 to automatically obtain a TCP/IP address on the network from a DHCP server.

- *Extensible Authentication Protocol* (EAP) at Layer 7 working with RADIUS.

- *Remote Authentication Dial In User Service* (RADIUS) at Layer 7 in conjunction with EAP to authenticate WLAN users.
- WEP at Layer 2 to encrypt/decrypt data on the WLAN.

1.10:- SUMMARY

1. Mobility is the most important advantage of WLAN.
2. The aim of the 802.11 standard was to develop a MAC and PHY layer for wireless connectivity for fixed, portable and moving stations within a local area.
3. Access points provide computers that are equipped with a mobile radio card to access a LAN, usually via an Ethernet connection.
4. There are two operation modes defined in IEEE 802.11x :
   - Infrastructure Mode
   - Ad Hoc Mode
5. Access points that act as routers can also assign an IP address to your PC's using DHCP services.
6. WLAN standards are defined at PHY layer and MAC layer of the OSI system model.
7. The Physical layer of the OSI system model is responsible for defining the electrical and mechanical aspects of networking
8. Infrared (IR) is not a useful technology for WLAN even for short distances.
9. There are two methods of Spread Spectrum modulation used within the unlicensed 2.4-GHz frequency band:
   - Frequency Hopping Spread Spectrum (FHSS)
   - Direct Sequence Spread Spectrum(DSSS)
10. Spread spectrum is ideal for Wireless LAN because it is less susceptible to radio noise and creates little interference, it is used to comply with the regulations for use in the ISM band.
11. The Data-link layer defines the protocol that control the Physical layer, determining such issues as how the medium is accessed and shared, how

devices or stations on the medium are addressed and how data is framed before transmission on the medium.

12. A 802.11 data link layer is divided in two sub layers:
    - Logical Link Control (LLC)
    - Media Access Control (MAC)
13. To control access to the network MAC layer uses a medium access scheme named collision sense multiple access with collision avoidance (CSMA/CA) and exponential back off. This scheme is similar to the collision sense multiple access with collision detection (CSMA/CD) that is used in Ethernet (IEEE 802.3). Collision avoidance, however, must be used instead of collision detection because wireless devices cannot generally transmit and receive at the same time.
14. Layer 1 and 2 play a key role in WLAN technology. But other layers also took part in WLAN networking.

CHAPTER 2

BACKGROUND

2.0:- Introduction

One of the most significant differences between wireless protocols and Ethernet is the way in which they handle flow control. Some existing challenges are also under discussion in this chapter.

This chapter begins our exploration of the Medium Access Control (MAC) layer of the 802.11 standard in detail because It is not possible, to design simulation program for WLAN without a thorough and detailed understanding of the WLAN MAC protocols. This chapter also discusses the data encapsulation in 802.11 frames.

The entire document on IEEE standards on wireless 802.11 MAC can be downloaded from the following site:

http://standards.ieee.org/reading/ieee/std/lanman/802.11-1999.pdf

The key to the 802.11 specification is the MAC. It rides on every physical layer and controls the transmission of user data into the air. It provides the core framing operations and the interaction with a wired network backbone. Different physical layers may provide different transmission speeds, all of which are supposed to interoperate.

802.11 does not depart from the previous IEEE 802 standards in any radical way. The standard successfully adapts Ethernet-style networking to radio links. Like Ethernet, 802.11 uses a *Carrier Sense Multiple Access (CSMA)* scheme to control access to the transmission medium. However, collisions waste valuable transmission capacity, so rather than the *CSMA/Collision Detection (CSMA/CD)* employed by Ethernet, 802.11 uses *CSMA/Collision Avoidance (CSMA/CA)*. Also like Ethernet, 802.11 uses a distributed access scheme with no centralized controller. Each 802.11 station uses the same method to gain access to the medium. The major differences between 802.11 and Ethernet stem from the differences in the underlying medium.

2.1:- Challenges for the MAC

Differences between the wireless network environment and the traditional wired environment create challenges for network protocol designers. This section examines a number of the hurdles that the 802.11 designers faced.

2.1.1:- RF Link Quality

On a wired Ethernet, it is reasonable to transmit a frame and assume that the destination receives it correctly. Radio links are different, especially when the frequencies used are unlicensed ISM bands. Even narrowband transmissions are subject to noise and interference, but unlicensed devices must assume that interference will exist and work around it. The designers of 802.11 considered ways to work around the radiation from microwave ovens and other RF sources. In addition to the noise, multipath fading may also lead to situations in which frames cannot be transmitted because a node moves into a dead spot.

Unlike many other link layer protocols, 802.11 incorporates positive acknowledgments. All transmitted frames must be acknowledged, as shown in *Figure 2.1*. If any part of the transfer fails, the frame is considered lost.

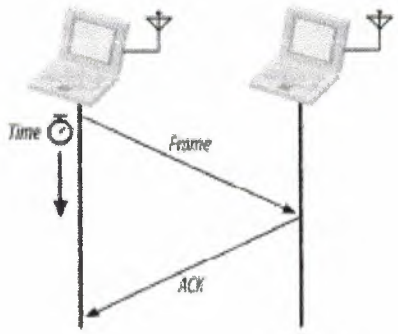


Figure2.1:- *Positive acknowledgment of data transmissions*

The sequence in *Figure 2.1* is an atomic operation. 802.11 allows stations to lock out contention (conflict) during atomic operations so that atomic sequences are not interrupted by other stations attempting to use the transmission medium.

2.1.2:- The Hidden Node Problem

In Ethernet networks, stations depend on the reception of transmissions to perform the carrier sensing functions of CSMA/CD. Wires in the physical medium contain the signals and distribute them to network nodes. Wireless networks have fuzzier boundaries, sometimes to the point where each node may not be able to communicate with every other node in the wireless network, as in *Figure 2.2*.

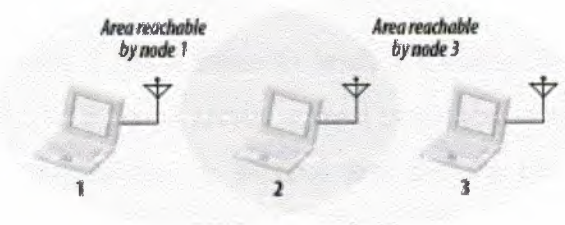


Figure 2.2:- *Nodes 1 and 3 are "Hidden"*

In the figure, node 2 can communicate with both nodes 1 and 3, but something prevents nodes 1 and 3 from communicating directly. (The obstacle itself is not relevant; it could be as simple as nodes 1 and 3 being as far away from 2 as possible, so the radio waves cannot reach the full distance from 1 to 3.) From the perspective of node 1, node 3 is a "hidden" node. If a simple transmit-and-pray protocol was used, it would be easy for node 1 and node 3 to transmit

Simultaneously, thus rendering node 2 unable to make sense of anything. Furthermore, nodes 1 and 3 would not have any indication of the error because the collision was local to node 2.

Collisions resulting from hidden nodes may be hard to detect in wireless networks because wireless transceivers are generally half-duplex; they don't transmit and receive at the same time. To prevent collisions, 802.11 allows stations to use Request to Send (RTS) and Clear to Send (CTS) signals to clear out an area. *Figure 2.3* illustrates the procedure.

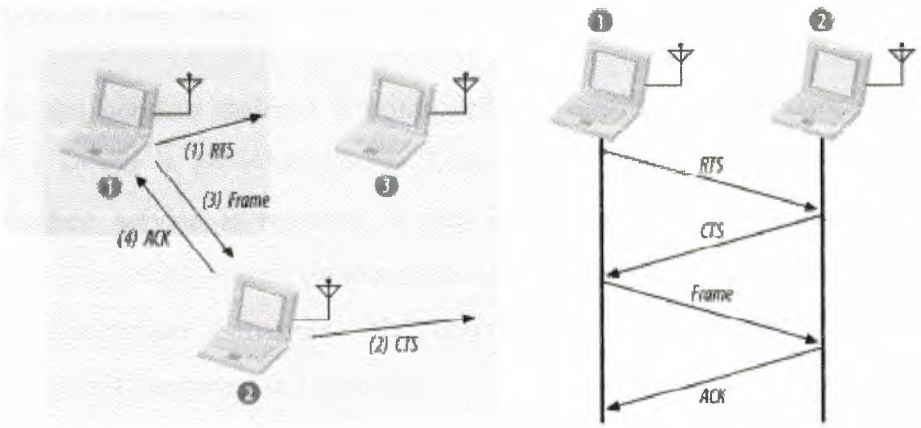


Figure 2.3:- *RTS/CTS clearing*

In *Figure 2.3*, node 1 has a frame to send; it initiates the process by sending an RTS frame. The RTS frame serves several purposes: in addition to reserving the radio link for transmission, it silences any stations that hear it. If the target station receives an RTS, it responds with a CTS. Like the RTS frame, the CTS frame silences stations in the immediate vicinity. Once the RTS/CTS exchange is complete, node 1 can transmit its frames without worry of interference from

any hidden nodes. Hidden nodes beyond the range of the sending station are silenced by the CTS from the receiver.

When the RTS/CTS clearing procedure is used, any frames must be positively acknowledged. The multiframe RTS/CTS transmission procedure consumes a fair amount of capacity, especially because of the additional latency incurred before transmission can commence. As a result, it is used only in high-capacity environments and environments with significant contention on transmission. For lower-capacity environments, it is not necessary.

You can control the RTS/CTS procedure by setting the RTS threshold if the device driver for your 802.11 card allows you to adjust it. The RTS/CTS exchange is performed for frames larger than the threshold. Frames shorter than the threshold are simply sent.

2.2:- MAC Access Modes and Timing

Access to the wireless medium is controlled by coordination functions. Ethernet-like CSMA/CA access is provided by the *Distributed Coordination Function* (DCF). If contention-free service is required, it can be provided by the *Point Coordination Function* (PCF), which is built on top of the DCF. Contention-free services are provided only in infrastructure networks. The coordination functions are described in the following list and illustrated in *Figure2.4.*

2.2.1:- Distributed Coordination Function (DCF)

The DCF is the basis of the standard CSMA/CA access mechanism. Like Ethernet, it first checks to see that the radio link is clear before transmitting. To avoid collisions, stations use a random backoff after each frame, with the first transmitter seizing the channel. In some circumstances, the DCF may use the CTS/RTS clearing technique to further reduce the possibility of collisions.

2.2.2:- Point Coordination Function (PCF)

Point coordination provides contention-free services. Special stations called point coordinators are used to ensure that the medium is provided without contention. Point coordinators reside in access points, so the PCF is restricted to infrastructure networks. To gain priority over standard contention-based services, the PCF allows stations to transmit frames after a shorter interval.

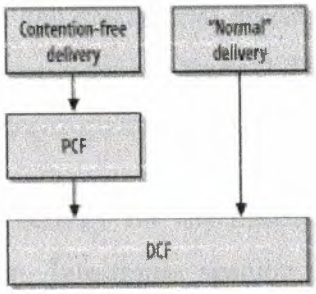


Figure 2.4:- *MAC coordination functions*

2.3:- Carrier-Sensing Functions and the Network Allocation Vector

Carrier sensing is used to determine if the medium is available. Two types of carrier-sensing functions in 802.11 manage this process: the physical carrier-sensing and virtual carrier-sensing functions. If either carrier-sensing function indicates that the medium is busy, the MAC reports this to higher layers.

2.3.1:- Physical Carrier-sensing

Physical carrier-Sensing functions are provided by the physical layer in question and depend on the medium and modulation used.

2.3.2:- Virtual Carrier-sensing

Virtual Carrier-sensing is provided by the *Network Allocation Vector* (NAV). Most 802.11 frames carry a duration field, which can be used to reserve the medium for a fixed time period.

2.3.3:-Network Allocation Vector (NAV)

The NAV is a timer that indicates the amount of time the medium will be reserved. Stations set the NAV to the time for which they expect to use the medium, including any frames necessary to complete the current operation. Other stations count down from the NAV to 0. When the NAV is nonzero, the virtual carrier-sensing function indicates that the medium is busy; when the NAV reaches 0, the virtual carrier-sensing function indicates that the medium is idle.

By using the NAV, stations can ensure that atomic operations are not interrupted. For example, the RTS/CTS sequence in *Figure 2.3* is atomic. *Figure 2.5* shows how the NAV protects the sequence from interruption.

The shaded bars represent activity on the medium by stations, and each bar is labeled with the frame type. Interframe spacing is depicted by the lack of any activity. Finally, the NAV timer is represented by the bars on the NAV line at the bottom of the figure. The NAV is carried in the frame headers on the RTS and CTS frames; it is depicted on its own line to show how the NAV relates to actual transmissions in the air. When a NAV bar is present on the NAV line, stations should defer access to the medium because the virtual carrier-sensing mechanism will indicate a busy medium.

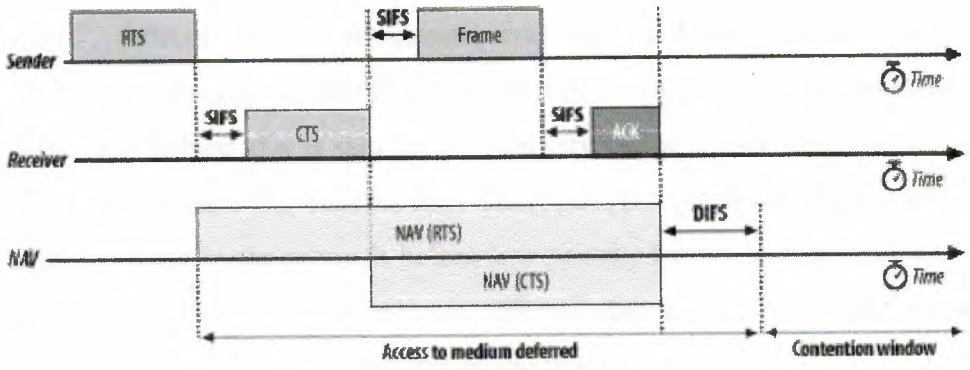


Figure 2.5:- *Using the NAV for virtual carrier sensing*

To ensure that the sequence is not interrupted, node 1 sets the NAV in its RTS to block access to the medium while the RTS is being transmitted. All stations that hear the RTS defer access to the medium until the NAV elapses.

RTS frames are not necessarily heard by every station in the network. Therefore, the recipient of the intended transmission responds with a CTS that includes a shorter NAV. This NAV prevents other stations from accessing the medium until the transmission completes. After the sequence completes, the medium can be used by any station after Distributed InterFrame Space (DIFS), which is depicted by the contention window beginning at the right side of the figure.

2.3.4:- Interframe Spacing

As with traditional Ethernet, the interframe spacing plays a large role in coordinating access to the transmission medium. 802.11 uses four different interframe spaces. Three are used to determine medium access; the relationship between them is shown in *Figure 2.6.*

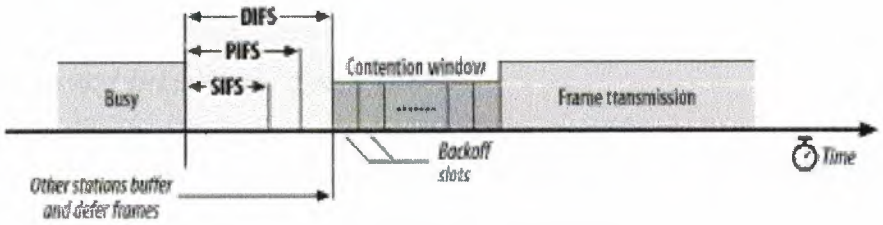


***Figure 2.6**:- Interframe spacing relationships*

We've already seen that as part of the collision avoidance built into the 802.11 MAC, stations delay transmission until the medium becomes idle. Varying interframe spacings create different priority levels for different types of traffic. The logic behind this is simple: high-priority traffic doesn't have to wait as long after the medium has become idle. Therefore, if there is any high-priority traffic waiting, it grabs the network before low-priority frames have a chance to try. To assist with interoperability between different data rates, the interframe space is a fixed amount of time, independent of the transmission speed.

2.3.4.1:- Short InterFrame Space (SIFS)

The SIFS is used for the highest-priority transmissions, such as RTS/CTS frames and positive acknowledgments. High-priority transmissions can begin once the SIFS has elapsed. Once these high-priority transmissions begin, the medium

becomes busy, so frames transmitted after the SIFS has elapsed have priority over frames that can be transmitted only after longer intervals.

2.3.4.2:- PCF InterFrame Space (PIFS)

The PIFS, sometimes erroneously called the priority interframe space, is used by the PCF during contention-free operation. Stations with data to transmit in the contention-free period can transmit after the PIFS has elapsed and preempt any contention-based traffic.

2.3.4.3:- DCF InterFrame Space (DIFS)

The DIFS is the minimum medium idle time for contention-based services. Stations may have immediate access to the medium if it has been free for a period longer than the DIFS.

2.3.4.4:- Extended InterFrame Space (EIFS)

The EIFS is not illustrated in *Figure 2.6* because it is not a fixed interval. It is used only when there is an error in frame transmission.

2.3.5:- Interframe spacing and priority

Atomic operations start like regular transmissions: they must wait for the DIFS before they can begin. However, the second and any subsequent steps in an atomic operation take place using the SIFS, rather than during the DIFS. This means that the second (and subsequent) parts of an atomic operation will grab the medium before another type of frame can be transmitted. By using the SIFS and the NAV, stations can seize (capture) the medium for as long as necessary. In *Figure 2.5*, for example, the short interframe space is used between the different units of the atomic exchange. After the sender gains access to the medium, the receiver replies with a CTS after the SIFS. Any stations that might attempt to access the medium at the conclusion of the RTS would wait for one DIFS interval. Partway through the DIFS interval, though, the SIFS interval elapses, and the CTS is transmitted.

2.3.6:- Contention-Based Access Using the DCF

Most traffic uses the DCF, which provides a standard Ethernet-like contention-based service. The DCF allows multiple independent stations to interact without central control, and thus may be used either in IBSS networks or in infrastructure networks.

Before attempting to transmit, each station checks whether the medium is idle. If the medium is not idle, stations defer to each other and employ an orderly exponential backoff algorithm to avoid collisions.
In distilling the 802.11 MAC rules, there is a basic set of rules that are always used, and additional rules may be applied depending on the circumstances. Two basic rules apply to all transmissions using the DCF:

1. If the medium has been idle for longer than the DIFS, transmission can begin immediately. Carrier sensing is performed using both a physical medium-dependent method and the virtual Network Allocation Vector (NAV) method.
    a. If the previous frame was received without errors, the medium must be free for at least the DIFS.
    b. If the previous transmission contained errors, the medium must be free for the amount of the EIFS.
2. If the medium is busy, the station must wait for the channel to become idle. 802.11 refers to the wait as access delay. If access is delayed, the station waits for the medium to become idle for the DIFS and prepares for the exponential backoff procedure.

Additional rules may apply in certain situations. Many of these rules depend on the particular situation "on the wire" and are specific to the results of previous transmissions.

1. Error recovery is the responsibility of the station sending a frame. Senders expect acknowledgments for each transmitted frame and are responsible for retrying the transmission until it is successful.

a. Positive acknowledgments are the only indication of success. Atomic exchanges must complete in their entirety to be successful. If an acknowledgment is expected and does not arrive, the sender considers the transmission lost and must retry.
b. All unicast data must be acknowledged.
c. Any failure increments a retry counter, and the transmission is retried. A failure can be due to a failure to gain access to the medium or a lack of an acknowledgment. However, there is a longer congestion window when transmissions are retried.

2. Multiframe sequences may update the NAV with each step in the transmission procedure. When a station receives a medium reservation that is longer than the current NAV, it updates the NAV. Setting the NAV is done on a frame-by-frame basis.
3. The following types of frames can be transmitted after the SIFS and thus receive maximum priority: acknowledgments, the CTS in an RTS/CTS exchange sequence, and fragments in fragment sequences.
    a. Once a station has transmitted the first frame in a sequence, it has gained control of the channel. Any additional frames and their acknowledgments can be sent using the short interframe space, which locks out any other stations.
    b. Additional frames in the sequence update the NAV for the expected additional time the medium will be used.
    c. Packets larger than the fragmentation threshold must be fragmented.

2.3.7:- Error Recovery with the DCF

Error detection and correction is up to the station that begins an atomic frame exchange. When an error is detected, the station with data must resend the frame. Errors must be detected by the sending station. In some cases, the sender can suppose frame loss by the lack of a positive acknowledgment from the receiver. Retry counters are incremented when frames are retransmitted.

Each frame or fragment has a single retry counter associated with it. Stations have two retry counters: the short retry count and the long retry count. Frames

that are shorter than the RTS threshold are considered to be short; frames longer than the threshold are long. Depending on the length of the frame, it is associated with either a short or long retry counter. Frame retry counts begin at 0 and are incremented when a frame transmission fails.

The short retry count is reset to 0 when:

- A CTS frame is received in response to a transmitted RTS
- A MAC-layer acknowledgment is received after a non fragmented transmission
- A broadcast or multicast frame is received

The long retry count is reset to 0 when:

- A MAC-layer acknowledgment is received for a frame longer than the RTS threshold
- A broadcast or multicast frame is received

In addition to the associated retry count, fragments are given a maximum "lifetime" by the MAC. When the first fragment is transmitted, the lifetime counter is started. When the lifetime limit is reached, the frame is discarded and no attempt is made to transmit any remaining fragments.

2.3.8:- Backoff with the DCF

After frame transmission has completed and the DIFS has elapsed, stations may attempt to transmit congestion-based data. A period called the *contention window* or *backoff window* follows the DIFS. This window is divided into slots. Slot length is medium-dependent; higher-speed physical layers use shorter slot times.

Stations pick a random slot and wait for that slot before attempting to access the medium; all slots are equally likely selections. When several stations are attempting to transmit, the station that picks the first slot (the station with the lowest random number) wins.

2.4:- Fragmentation and Reassembly

Higher-level packets and some large management frames may need to be broken into smaller pieces to fit through the wireless channel

Wireless LAN stations may attempt to fragment transmissions so that interference affects only on small fragments, not large frames. By immediately reducing the

amount of data that can be corrupted by interference, fragmentation may result in a higher effective throughput.

Fragmentation takes place when a higher-level packet's length exceeds the fragmentation threshold configured by the network administrator. Fragments all have the same frame sequence number but have ascending fragment numbers to aid in reassembly. Frame control information also indicates whether more fragments are coming. All of the fragments that comprise a frame are normally sent in a fragmentation burst, which is shown in *Figure 2.7.* This figure also incorporates an RTS/CTS exchange, because it is common for the fragmentation and RTS/CTS thresholds to be set to the same value. The figure also shows how the NAV and SIFS are used in combination to control access to the medium.

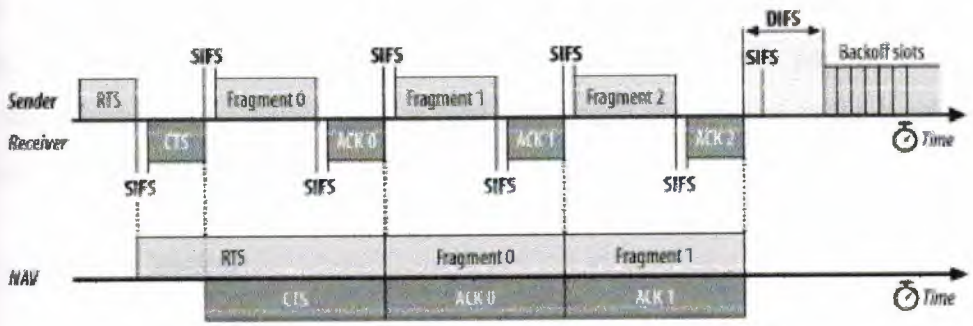


Figure 2.7:- *Fragmentation burst*

Fragments and their acknowledgments are separated by the SIFS, so a station retains control of the channel during a fragmentation burst. The NAV is also used to ensure that other stations don't use the channel during the fragmentation burst. As with any RTS/CTS exchange, the RTS and CTS both set the NAV from the expected time to the end of the first fragments in the air. Subsequent fragments then form a chain. Each fragment sets the NAV to hold the medium until the end of the acknowledgment for the

next frame. Fragment 0 sets the NAV to hold the medium until ACK 1, fragment 1 sets the NAV to hold the medium until ACK 2, and so on. After the last fragment and its acknowledgment have been sent, the NAV is set to 0, indicating that the medium will be released after the fragmentation burst completes.

2.5:- Frame Format

To meet the challenges posed by a wireless data link, the MAC was forced to adopt several unique features, not the least of which was the use of four address fields. Not all frames use all the address fields, and the values assigned to the address fields may change depending on the type of MAC frame being transmitted

Figure 2.8 shows the generic 802.11 MAC frame. All diagrams in this section follow the IEEE conventions in 802.11. Fields are transmitted from left to right, and the most significant bits appear last.

Figure2.8:- *Generic 802.11 MAC frame*

802.11 MAC frames do not include some of the classic Ethernet frame features, most notably the type/length field and the preamble. The preamble is part of the physical layer, and encapsulation details such as type and length are present in the header on the data carried in the 802.11 frame.

2.5.1:- Frame Control

Each frame starts with a ***two-byte or 16 bits*** Frame Control subfield, shown in *Figure 2.9.* The components of the Frame Control subfield are:

2.5.1.1:-Protocol version

Two bits indicate which version of the 802.11 MAC is contained in the rest of the frame. At present, only one version of the 802.11 MAC has been developed; it is assigned the protocol number 0. Other values will appear when the IEEE

standardizes changes to the MAC that render it incompatible with the initial specification.

2.5.1.2:- Type and subtype fields

Two bits long Type and subtype fields identify the type of frame used. To handle with noise and unreliability, a number of management functions are incorporated into the 802.11 MAC. Some, such as the RTS/CTS operations and the acknowledgments, have already been discussed. *Table 2.1* shows how the type and subtype identifiers are used to create the different classes of frames.

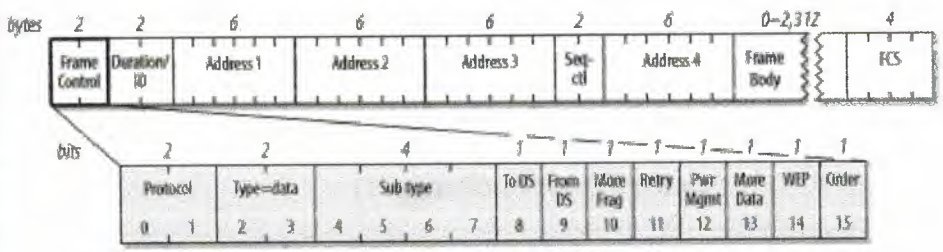


***Figure 2.9:-** Frame control field*

***Table 2.1:-** Type and subtype identifiers*

Subtype value	**Subtype name**
Management frames (type=00)[a]	
0000	Association request
0001	Association response
0010	Re-association request
0011	Re-association response
0100	Probe request
0101	Probe response
1000	Beacon

Table 2.1:- Type and subtype identifiers

Subtype value	**Subtype name**
1001	Announcement traffic indication message (ATIM)
1010	Disassociation
1011	Authentication
1100	Deauthentication
Control frames (type=01)[b]	
1010	Power Save (PS)-Poll
1011	RTS
1100	CTS
1101	Acknowledgment (ACK)
1110	Contention-Free (CF)-End
1111	CF-End+CF-Ack
Data frames (type=10)[c]	
0000	Data
0001	Data+CF-Ack
0010	Data+CF-Poll
0011	Data+CF-Ack+CF-Poll
0100	Null data (no data transmitted)
0101	CF-Ack (no data transmitted)
0110	CF-Poll (no data transmitted)
0111	Data+CF-Ack+CF-Poll
(Frame type 11 is reserved)	

[a] Management subtypes 0110-0111 and 1101-1111 are reserved and not currently used.

[b] Control subtypes 0000-1001 are reserved and not currently used.

[c] Data subtypes 1000-1111 are reserved and not currently used.

In *Table 2.1*, bit strings are written most-significant bit first, which is the reverse of the order used in *Figure 2.9*. Therefore, the frame type is the third bit in the frame control field followed by the second bit (b3 b2), and the subtype is the seventh bit, followed by the sixth, fifth, and fourth bits (b7 b6 b5 b4).

2.5.1.3:- ToDS and FromDS bits

These bits indicate whether a frame is designed for the distribution system. All frames on infrastructure networks will have one of the distribution system's bits set. *Table 2.2* shows how these bits are interpreted.

Table 2.2:- Interpreting the ToDS and FromDS bits

	To DS=0	**To DS=1**
From DS=0	All management and control frames Data frames within an IBSS (never infrastructure data frames)	Data frames transmitted from a wireless station in an infrastructure network
From DS=1	Data frames received for a wireless station in an infrastructure network	Data frames on a "wireless bridge"

2.5.1.4:- More fragments bit

This bit functions much like the "more fragments" bit in IP. When a higher-level packet has been fragmented by the MAC, the initial fragment and any following nonfinal fragments set this bit to 1. Some management frames may be large enough to require fragmentation; all other frames set this bit to 0.

2.5.1.5:- Retry bit

From time to time, frames may be retransmitted. Any retransmitted frames set this bit to 1 to aid the receiving station in eliminating duplicate frames.

2.5.1.6:- Power management bit

Network adapters built on 802.11 are often built to the PC Card form factor and used in battery-powered laptop or handheld computers. To conserve battery life, many small devices have the ability to power down parts of the network interface. This bit indicates whether the sender will be in a power-saving mode after the completion of the current atomic frame exchange. One indicates that the station will be in power-save mode, and 0 indicates that the station will be active. Access

points perform a number of important management functions and are not allowed to save power, so this bit is always 0 in frames transmitted by an access point.

2.5.1.7:- More data bit

To accommodate stations in a power-saving mode, access points may buffer frames received from the distribution system. An access point sets this bit to indicate that at least one frame is available and is addressed to a dozing station.

2.5.1.8:- WEP bit

Wireless transmissions are inherently easier to intercept than transmissions on a fixed network. 802.11 defines a set of encryption routines called Wired Equivalent Privacy (WEP) to protect and authenticate data. When a frame has been processed by WEP, this bit is set to 1, and the frame changes slightly.

2.5.1.9:- Order bit

Frames and fragments can be transmitted in order at the cost of additional processing by both the sending and receiving MACs. When the "strict ordering" delivery is employed, this bit is set to 1.

2.5.2 Duration/ID Field

The Duration/ID field follows the frame control field. This field has several uses and takes one of the three forms shown in *Figure 3.10.*.

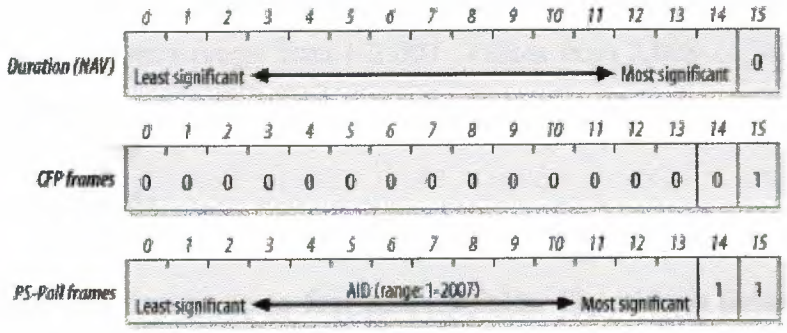


Fig 2.10:-*Duration/ID Field*

2.5.2.1:- Duration: setting the NAV

When *bit 15* is 0, the duration/ID field is used to set the NAV. The value represents the number of microseconds that the medium is expected to remain busy for the transmission currently in progress.

2.5.2.2:- Frames transmitted during contention-free periods

During the contention-free periods, bit 14 is 0 and bit 15 is 1. All other bits are 0, so the duration/ID field takes a value of 32,768. This value is interpreted as a NAV. It allows any stations that did not receive the Beacon[3] announcing the contention-free period to update the NAV with a suitably large value to avoid interfering with contention-free transmissions.

[3] Beacon frames are a subtype of management frames, which is why "Beacon" is capitalized.

2.5.2.3:- PS-Poll frames

Bits 14 and 15 are both set to 0 in PS-Poll frames. Mobile stations may elect to save battery power by turning off antennas. Dozing stations must wake up periodically. To ensure that no frames are lost, stations awaking from their slumber transmit a PS-Poll frame to retrieve any buffered frames from the access point. Along with this request, waking stations incorporate the Association ID (AID) that indicates which BSS they belong to. The AID is included in the PS-Poll frame and may range from 1-2,007. Values from 2,008-16,383 are reserved and not used.

2.5.3:- Address Fields

An 802.11 frame may contain up to four address fields. The address fields are numbered because different fields are used for different purposes depending on the frame type. The general rule of thumb is that Address 1 is used for the receiver, Address 2 for the transmitter, with the Address 3 field used for filtering by the receiver. Addressing in 802.11 follows the conventions used for the other IEEE 802 networks, including Ethernet. Addresses are 48 bits long. If the first bit sent to the physical medium is a 0, the address represents a single station (unicast). When the first bit is a 1, the address represents a group of physical stations and is called a multicast address. If all bit are 1s, then the frame is a broadcast and is delivered to all stations connected to the wireless medium.

48-bit addresses are used for a variety of purposes:

2.5.3.1:- Destination address

As in Ethernet, the destination address is the 48-bit IEEE MAC identifier that corresponds to the final recipient: the station that will hand the frame to higher protocol layers for processing.

2.5.3.2:- Source address

This is the 48-bit IEEE MAC identifier that identifies the source of the transmission. Only one station can be the source of a frame, so the Individual/Group bit is always 0 to indicate an individual station.

2.5.3.3:- Receiver address

This is a 48-bit IEEE MAC identifier that indicates which wireless station should process the frame. If it is a wireless station, the receiver address is the destination address. For frames destined to a node on an Ethernet connected to an access point, the receiver is the wireless interface in the access point, and the destination address may be a router attached to the Ethernet.

2.5.3.4:-Transmitter address

This is a 48-bit IEEE MAC address to identify the wireless interface that transmitted the frame onto the wireless medium. The transmitter address is used only in wireless bridging.

2.5.3.5:- Basic Service Set ID (BSSID)

To identify different wireless LANs in the same area, stations may be assigned to a BSS. In infrastructure networks, the BSSID is the MAC address used by the wireless interface in the access point. Ad hoc networks generate a random BSSID with the Universal/Local bit set to 1 to prevent conflicts with officially assigned MAC addresses.

The number of address fields used depends on the type of frame. Most data frames use three fields for source, destination, and BSSID. The number and arrangement of address fields in a data frame depends on how the frame is traveling relative to the distribution system. Most transmissions use three addresses, which is why only three of the four addresses are contiguous in the frame format.

2.5.4:- Sequence Control Field

This 16-bit field is used for both defragmentation and discarding duplicate frames. It is composed of a 4-bit fragment number field and a 12-bit sequence number field, as shown in *Figure 2.11.*

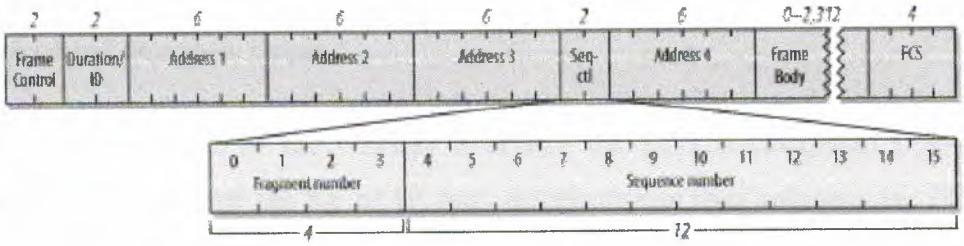


Figure 2.11:- *Sequence Control field*

Higher-level frames are each given a sequence number as they are passed to the MAC for transmission. The sequence number subfield operates as a modulo-4096 counter of the frames transmitted. It begins at 0 and increments by 1 for each higher-level packet handled by the MAC. If higher-level packets are fragmented, all fragments will have the same sequence number. When frames are retransmitted, the sequence number is not changed.

What differs between fragments is the fragment number. The first fragment is given a fragment number of 0. Each successive fragment increments the fragment number by one. Retransmitted fragments keep their original sequence numbers to assist in reassembly.

2.5.5:- Frame Body

The frame body, also called the Data field, moves the higher-layer payload from station to station. 802.11 can transmit frames with a maximum payload of 2,304 bytes of higher-level data. (Implementations must support frame bodies of 2,312 bytes to accommodate WEP overhead.) 802.2 LLC headers use 8 bytes for a maximum network protocol payload of 2,296 bytes. Preventing fragmentation must be done at the protocol layer. On IP networks, Path MTU Discovery (RFC 1191) will prevent the transmission of frames with Data fields larger than 1,500 bytes.

2.5.6:- Frame Check Sequence

As with Ethernet, the 802.11 frame closes with a Frame Check Sequence (FCS). The FCS is often referred to as the Cyclic Redundancy Check (CRC) because of the underlying mathematical operations. The FCS allows stations to check the integrity of received frames. All fields in the MAC header and the body of the frame are included in the FCS. Although 802.3 and 802.11 use the same method to calculate the FCS, the MAC header used in 802.11 is different from the header used in 802.3, so the FCS must be recalculated by access points.

When frames are sent to the wireless interface, the FCS is calculated before those frames are sent out over the RF or IR link. Receivers can then calculate the FCS from the received frame and compare it to the received FCS. If the two match, there is a high probability that the frame was not damaged in transit.

On Ethernets, frames with a bad FCS are simply discarded, and frames with a good FCS are passed up the protocol stack. On 802.11 networks, frames that pass the integrity check may also require the receiver to send an acknowledgment. For example, data frames that are received correctly must be positively acknowledged, or they are retransmitted. 802.11 does not have a negative acknowledgment for frames that fail the FCS; stations must wait for the acknowledgment timeout before retransmitting.

2.6:- Encapsulation of Higher-Layer Protocols Within 802.11

Like all other 802 link layers, 802.11 can transport any network-layer protocol. Unlike Ethernet, 802.11 relies on 802.2 Logical-Link Control (LLC) encapsulation to carry higher-level protocols. *Figure 2.12* shows how 802.2 LLC encapsulation is used to carry an IP packet. In the figure, the "MAC headers" for 802.1h and RFC 1042 might be the 12 bytes of source and destination MAC address information on Ethernet or the long 802.11 MAC header from the previous section.

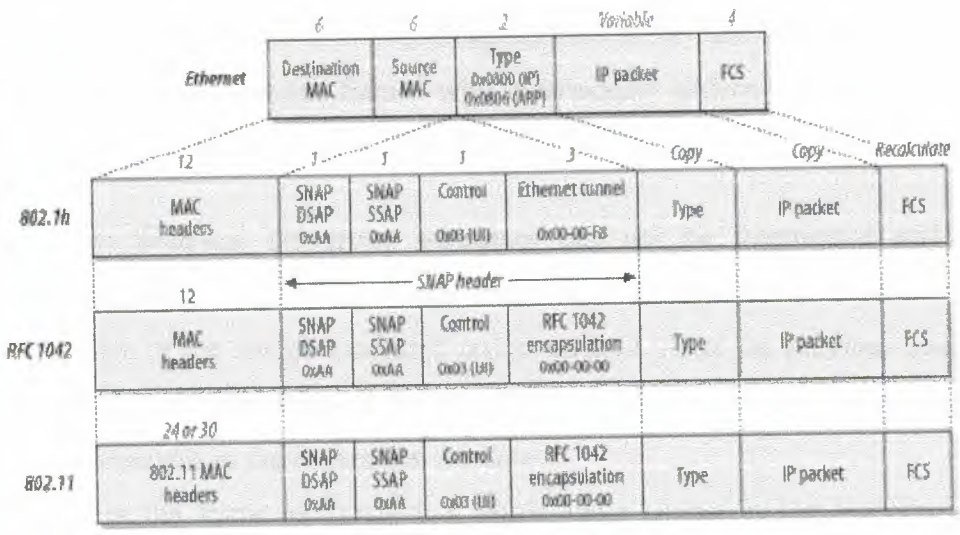


Figure 2.12:- *IP encapsulation in 802.11*

Two different methods can be used to encapsulate LLC data for transmission. One is described in RFC 1042, and the other in 802.1h. As you can see in *Figure 2.12*, though, the two methods are quite similar. An Ethernet frame is shown in the top line of *Figure 2.12.* It has a MAC header composed of source and destination MAC addresses, a type code, the embedded packet, and a frame check field. In the IP world, the Type code is either 0x0800 (2048 decimal) for IP itself, or 0x0806 (2054 decimal) for the Address Resolution Protocol (ARP).

2.7:- Contention-Based Data Service

The additional features incorporated into 802.11 to add reliability lead to a confusing tangle of rules about which types of frames are permitted at any point. They also make it more difficult for network administrators to know which frame exchanges they can expect to see on networks.

2.7.1:- Broadcast and Multicast Data or Management Frames

Broadcast and multicast frames have the simplest frame exchanges because there is no acknowledgment. Framing and addressing are somewhat more complex in 802.11, so the types of frames that match this rule are the following:

- Broadcast data frames with a broadcast address in the Address1 field
- Multicast data frames with a multicast address in the Address1 field
- Broadcast management frames with a broadcast address in the Address1 field (Beacon, Probe Request, and IBSS ATIM frames)

Frames designed for group addresses can not be fragmented and are not acknowledged. The entire atomic sequence is a single frame, sent according to the rules of the contention-based access control. After the previous transmission concludes, all stations wait for the DIFS and begin counting down the random delay intervals in the contention window.

Because the frame exchange is a single-frame sequence, the NAV is set to 0. With no further frames to follow, there is no need to use the virtual carrier-sense mechanism to lock other stations out of using the medium. After the frame is transmitted, all stations wait through the DIFS and begin counting down through the contention window for any delayed frames. See *Figure 2.13.*

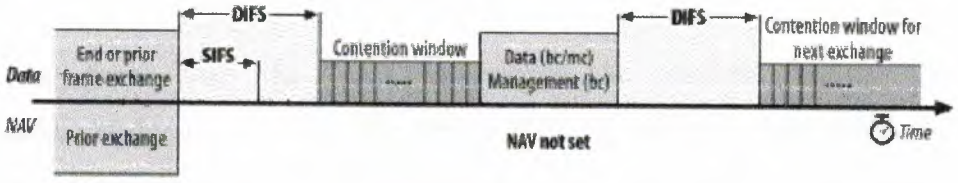


Figure2.13:- Broadcast/multicast data and broadcast management atomic frame exchange

Depending on the environment, frames sent to group addresses may have lower service quality because the frames are not acknowledged. Some stations may therefore miss broadcast or multicast traffic, but there is no facility built into the MAC for retransmitting broadcast or multicast frames.

2.7.2:- Unicast Frames

Frames that are destined for a single station are called directed data by the 802.11 standard. This book uses the more common term unicast. Unicast frames must be acknowledged to ensure reliability, which means that a variety of mechanisms can be used to improve efficiency. All the sequences in this section

apply to any unicast frame and thus can apply to management frames and data frames. In practice, these operations are usually observed only with data frames.

2.7.2.1:- Basic positive acknowledgment (final fragment)

Reliable transmission between two stations is based on simple positive acknowledgments. Unicast data frames must be acknowledged, or the frame is assumed to be lost. The most basic case is a single frame and its accompanying acknowledgment, as shown in *Figure 3.14*

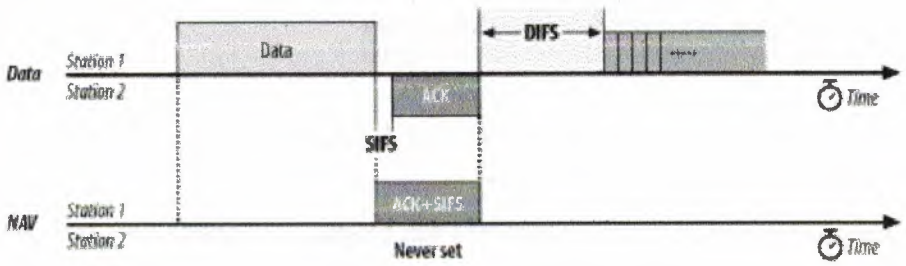


***Figure 3.14**:- Basic positive acknowledgment of data*

The frame uses the NAV to reserve the medium for the frame, its acknowledgment, and the intervening SIFS. By setting a long NAV, the sender locks the virtual carrier for the entire sequence, guaranteeing that the recipient of the frame can send the acknowledgment. Because the sequence concludes with the ACK, no further virtual carrier locking is necessary, and the NAV in the ACK is set to 0.

3.7.2.2:- Fragmentation

Many higher-layer network protocols, including IP, incorporate fragmentation. The disadvantage of network-layer fragmentation is that reassembly is performed by the final destination; if any of the fragments are lost, the entire packet must be retransmitted. Link layers may incorporate fragmentation to boost speed over a single hop with a small MTU (This is the approach used by Multi-link PPP (RFC 1990)).802.11 can also use fragmentation to help avoid interference. Radio interference is often in the form of short, high-energy bursts and is frequently synchronized with the AC power line. Breaking a large frame into small

frames allows a larger percentage of the frames to arrive undamaged. The basic fragmentation scheme is shown in *Figure 2.15.*

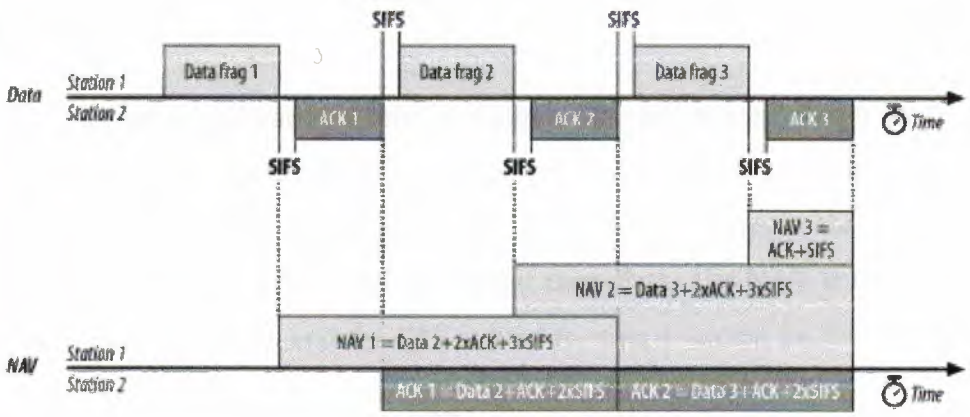


Figure 2.15:- *Fragmentation*

The last two frames exchanged are the same as in the previous sequence, and the NAV is set identically. However, all previous frames use the NAV to lock the medium for the next frame. The first data frame sets the NAV for a long enough period to accommodate its ACK, the next fragment, and the acknowledgment following the next fragment. To indicate that it is a fragment, the MAC sets the More Fragments bit in the frame control field to 1. All nonfinal ACKs continue to extend the lock for the next data fragment and its ACK. Subsequent data frames then continue to lengthen the NAV to include successive acknowledgments until the final data frame, which sets the More Fragments bit to 0, and the final ACK, which sets the NAV to 0. No limit is placed on the number of fragments, but the total frame length must be shorter than any constraint placed on the exchange by the PHY.

Fragmentation is controlled by the fragmentation threshold parameter in the MAC. Most network card drivers allow you to configure this parameter. Any frames larger than the fragmentation threshold are fragmented in an implementation-dependent way. Network administrators can change the fragmentation threshold to tune network behavior. Higher fragmentation thresholds mean that frames are delivered with less overhead, but the cost to a lost or damaged frame is much higher because more data must be discarded and

Retransmitted. Low fragmentation thresholds have much higher overhead, but they offer increased robustness in the face of hostile conditions.

2.7.2.3:- RTS/CTS

To guarantee reservation of the medium and uninterrupted data transmission, a station can use the RTS/CTS exchange. *Figure 2.16* shows this process. The RTS/CTS exchange acts exactly like the initial exchange in the fragmentation case, except that the RTS frame does not carry data. The NAV in the RTS allows the CTS to complete, and the CTS is used to reserve access for the data frame.

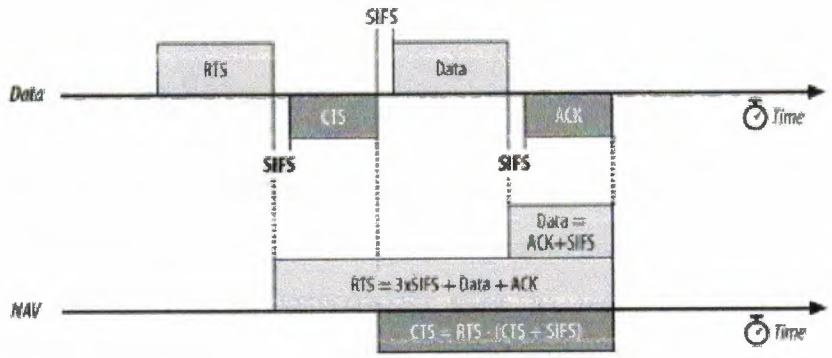


***Figure 2.16:-** RTS/CTS lockout*

RTS/CTS can be used for all frame exchanges, none of them, or something in between. Like fragmentation, RTS/CTS behavior is controlled by a threshold set in the driver software. Frames larger than the threshold are preceded by an RTS/CTS exchange to clear the medium, while smaller frames are simply transmitted.

2.7.2.4:- RTS/CTS with fragmentation

In practice, the RTS/CTS exchange is often combined with fragmentation (*Figure 2.17*). Fragmented frames are usually quite long and thus benefit from the use of the RTS/CTS procedure to ensure exclusive access to the medium, free from contention from hidden nodes. Some vendors set the default fragmentation threshold to be identical to the default RTS/CTS threshold.

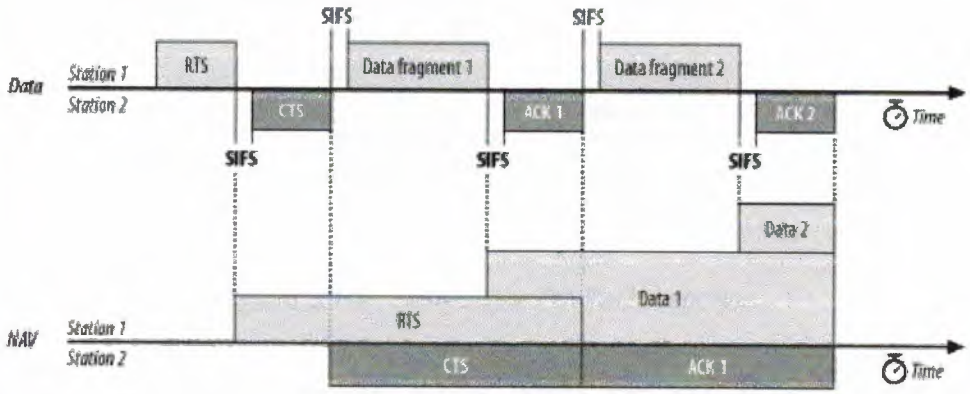


***Figure 2.17:-** RTS/CTS with fragmentation*

2.7.3:- Power-Saving Sequences

The most power-hungry components in RF systems are the amplifiers used to boost a signal immediately prior to transmission and to boost the received signal to an intelligible level immediately after its reception. 802.11 stations can maximize battery life by shutting down the radio transceiver and sleeping periodically. During sleeping periods, access points buffer any unicast frames for sleeping stations. These frames are announced by subsequent Beacon frames. To retrieve buffered frames, newly awakened stations use PS-Poll frames.

Access points can respond immediately to the PS-Poll. After a short interframe space, an access point may transmit the frame. *Figure 2.18* shows an implied NAV as a result of the PS-Poll frame. The PS-Poll frame contains an Association ID in the Duration/ID field so that the access point can determine which frames were buffered for the mobile station. However, the MAC specification requires all stations receiving a PS-Poll to update the NAV with an implied value equal to a SIFS and one ACK. Although the NAV is too short for the data frame, the access point acquires that the medium and all stations defer access for the entire data frame. At the conclusion of the data frame, the NAV is updated to reflect the value in the header of the data frame.

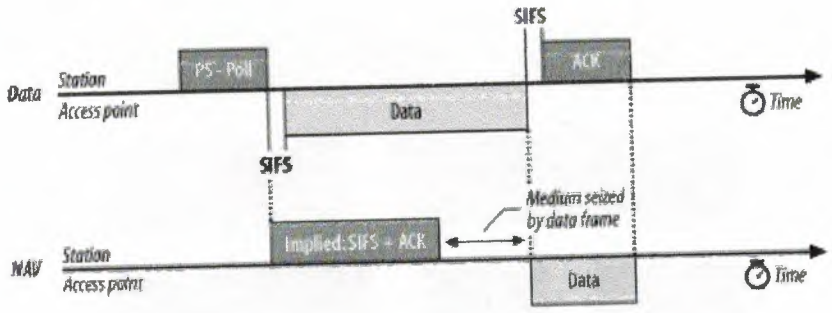


Figure 2.18:- *Immediate PS-Poll response*

Instead of an immediate response, access points can also respond with a simple acknowledgment. This is called a delayed response because the access point acknowledges the request for the buffered frame but does not act on it immediately. A station requesting a frame with a PS-Poll must stay awake until it is delivered. Under contention-based service, however, the access point can deliver a frame at any point. A station cannot return to a low-power mode until it receives a Beacon frame in which its bit in the traffic indication map (TIM) is clear.

2.8:- Functional Structure of IEEE 802.11 MAC layer

Both RFC 1042 and 802.1h are derivatives of 802.2's *Sub-Network Access Protocol* (SNAP). The MAC addresses are copied into the beginning of the encapsulation frame, and then a SNAP header is inserted. SNAP headers begin with a Destination Service Access Point (DSAP) and a Source Service Access Point (SSAP). After the addresses, SNAP includes a Control header. Like High-Level Data Link Control (HDLC) and its progeny, the Control field is set to 0x03 to denote Unnumbered Information (UI), a category that maps well to the best-effort delivery of IP datagrams. The last field inserted by SNAP is an Organizationally Unique Identifier (OUI).

The architecture of the IEEE 802.11 MAC layer is given in *Figure 2.19.*

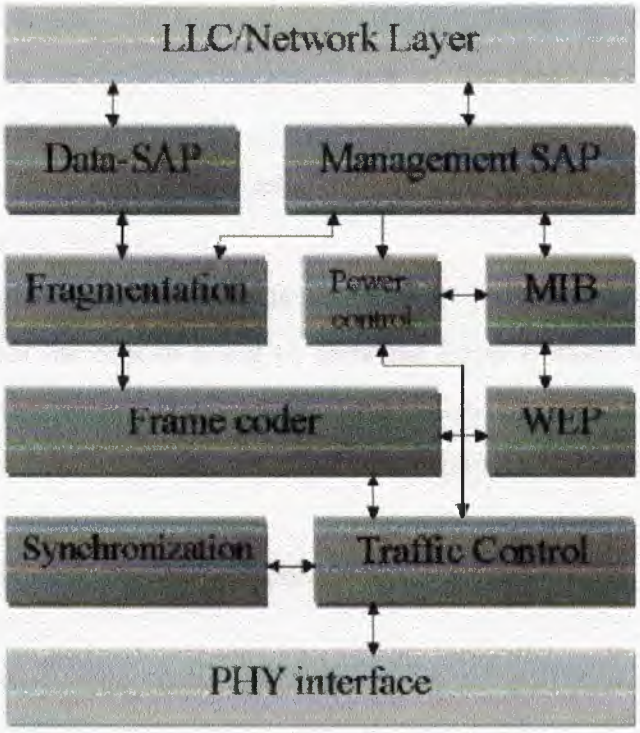


***Figure2.19**:- IEEE 802.11 MAC architecture*

Initially, the IEEE hoped that the 1-byte service access points would be adequate to handle the number of network protocols, but this proved to be an overly optimistic assessment of the state of the world. As a result, SNAP copies the type code from the original Ethernet frame.

2.9:- SUMMARY

- The main mode for accessing the network medium is a traditional contention-based access method, though it employs collision avoidance (CSMA/CA) rather than collision detection (CSMA/CD).
- Unicast frames must be acknowledged to ensure reliability.
- Frames designed for group addresses cannot be fragmented and are not acknowledged.
- Frames sent to group addresses may have lower service quality because the frames are not acknowledged.

- The disadvantage of network-layer fragmentation is that reassembly is performed by the final destination; if any of the fragments are lost, the entire packet must be retransmitted
- Breaking a large frame into small frames allows a larger percentage of the frames to arrive undamaged.
- Higher fragmentation thresholds mean that frames are delivered with less overhead, but the cost to a lost or damaged frame is much higher because more data must be discarded and retransmitted. Low fragmentation thresholds have much higher overhead, but they offer increased robustness in the face of hostile conditions.
- Support for both ad-hoc and infrastructure wireless LAN (Access Points and Station QSTA).
- On the fly Encryption/decryption WEP (48 bit RCA PRNG algorithm).
- MAC-level fragmentation and de-fragmentation.
- Allows support of QoS (802.11e), Security (802.11i) and DFS/TPC standard extensions (802.11h)
- DCF/EDCF and PCF/HCF support: bandwidth reservation, contention free medium access, traffic category management (priority and queue based).
- Support of advanced QoS oriented schemes such as Burst Acknowledge mode.

CHAPTER 3

SIMULATION & SOFTWARE COMPONENTS

3.0:- Introduction

The goal of ***Simulation and Software Components*** is to give basic ideas of simulation, modeling, simulation languages, validation, and output data analysis.

This is a chapter about techniques for using computers to imitate, or simulate, the operations of various kinds of real-world facilities and processes.

We shall also discuss systems and models in considerably more detail and then show how to write computer programs to simulate systems of varying degrees of complexity.

At the end of this chapter I shall give you a simulation program written in MATLAB which will simulate the MAC layer 802.11 network and shall also give you a sample output in order to understand the behavior of this simulation program.

3.1:- Simulation

Simulation means to estimate, imitate by using some mathematical formulas, methods and algorithms.

Technically Simulation can be defined as:

Simulation involves using a set of equation and state information to measure the performance of a network.

3.2:- The Nature of Simulation

If the relationships that compose the model are simple enough, it may be possible to use mathematical methods (such as algebra, calculus, or probability theory) to obtain exact information on questions of interest; this is called an analytic solution. However, most real-world systems are too complex to allow realistic models to be evaluated analytically, and these models must he studied by means of simulation.

In a simulation, we use a computer to evaluate a model numerically, and data are gathered in order to estimate the desired true characteristics of the model.

3.3:- Applications

Application areas for simulation are numerous and diverse. Below is a list of some particular kinds of problems for which simulation has been found to be a useful and powerful tool.

- Designing and analyzing manufacturing systems
- Evaluating hardware and software requirements for a computer system
- Evaluating a new military weapons system or tactic
- Determining ordering policies for an inventory system
- Designing communications systems and message protocols for them
- Designing and operating transportation facilities such as freeways, airports, Subways or ports.

• Evaluating designs for service organizations such as hospitals, post offices, or fast-food restaurants

• Analyzing financial or economic systems

As a technique, simulation is one of the most widely used in operations research and management science.

3.4:- Systems, Models, and Simulation

3.4.1:- System

In practice, what is meant by "the system" depends on the objectives of a particular study. The collection of entities that compose a system for one study might be only a subset of the overall system for another.

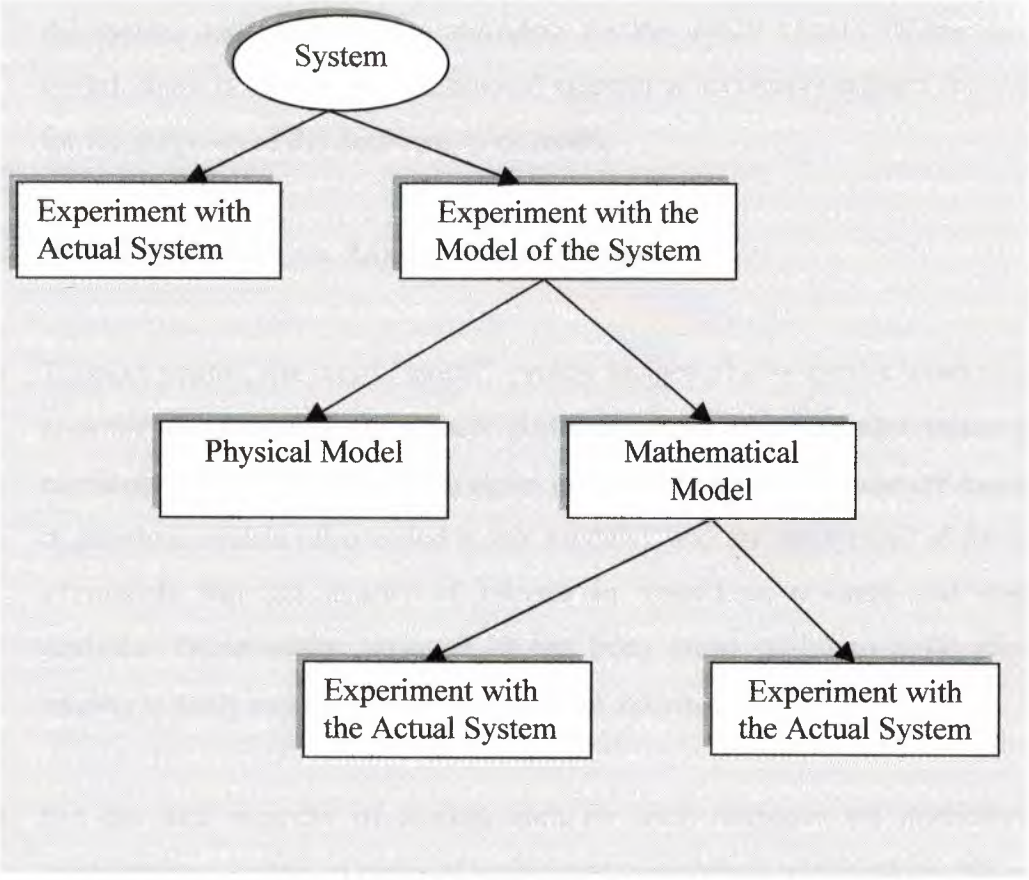


Fig3.1:- Ways to study a SYSTEM

3.4.2:- State

We define the state of a system to be that collection of variables necessary to describe a system at a particular time, relative to the objective of a study.

3.4.3:- Experiment with the Actual System vs. Experiment with a Model of the System

- If it is possible (and cost-effective) to alter the system physically and then let it operate under the new conditions, it is probably desirable to do so, for in this case there is no question about whether what we study is relevant. However, it is rarely feasible to do this, because such an experiment would often be too costly or too disruptive to the system.

- For some reasons, it is usually necessary to build a model as a representation of the system and study it as a surrogate for the actual system. When using a model, there is always the question of whether it accurately reflects the system for the purposes of the decisions to be made.

3.4.4:- Physical Model vs. Mathematical Model

- To most people, the word "model" evokes images of clay cars in wind tunnels, cockpits disconnected from their airplanes to be used in pilot training, or miniature supertankers scurrying about in a swimming pool. These are examples of physical models (also called iconic models), and arc not typical of the kinds of models that are usually of interest in operations research and systems analysis. Occasionally, however, it has been found useful to build physical models to study engineering or management systems.

- But the vast majority of models built for such purposes are mathematical, representing a system in terms of logical and quantitative relationships that are then manipulated and changed to see how the model reacts, and thus how the system would react—if the mathematical model is a valid one.

3.4.5:- Analytical Solution vs. Simulation

- Once we have built a mathematical model, it must then be examined to see how it can be used to answer the questions of interest about the system it is supposed to represent. If the model is simple enough, it may be possible to work with its relationships and quantities to get an exact, *analytical* solution.

- Many systems are highly complex, so that valid mathematical models of them are themselves complex, precluding an possibility of an analytical solution. In this case, the model must be studied by means of simulation, i.e., numerically

  exercising the model for the input in question to see how they affect the output measures of performance.

3.4.6:- Static vs. Dynamic Simulation Models

- A static simulation model is representation of a system at a particular time, or one that may be used represent a system in which time simply plays no role.

- On the other hand. a dynamic simulation model represents a system as it evolves over time, such as a conveyor system in a factory.

3.4.7:- Deterministic vs. Stochastic Simulation Models

- If a simulation model does not contain any probabilistic (i.e., random) components, it is called ***Deterministic***; a complicated (and analytically intractable) system of different equations describing a chemical reaction might be such a model. In deterministic models, the output is "determined" once the set of input quantities and relationships in the model have been specified, even though might take a lot of computer time to evaluate what it is.
- Many systems however, must be modeled as having at least some random input components, and these give rise to ***stochastic simulation*** models.

3.4.8:- Continuous vs. Discrete Simulation Models

- ***Continuous simulation*** concerns the modeling over time of a system by a representation in which the state variables change continuously with respect to time. An airplane moving through the air is an example of a continuous system.

- ***Discrete simulation*** concerns the modeling of a system as it evolves over time by a representation in which the state variables change instantaneously at separate points in time. A bank is an example of discrete simulation.

- Some systems are neither discrete nor completely continuous; the need may arise to construct a model with aspects of both discrete and continuous simulation, resulting in a ***Combined Discrete-Continuous Simulation.***

3.5:- Components and Organization of a Simulation Model

Although simulation has been applied to a great diversity of real-world systems, all simulation models share a number of common components and there is a logical organization for these components that promotes the coding, debugging, and future changing of a simulation model's computer program. In particular, the following components will be found in most simulation models.

3.5.1:- System state

The collection of state variables necessary to describe the system at a particular time.

3.5.2:- Simulation clock

A variable giving the current value of simulated time.

3.5.3:- Event list

A list containing the next time when each type of event will occur.

3.5.4:- Statistical counters

Variables used for storing statistical information about system performance.

3.5.5:- Initialization routine

A subprogram to initialize the simulation model at time zero.

3.5.6:- Timing routine

A subprogram that determines the next event from the event list and then advances the simulation clock to the time when that event is to occur.

3.5.7:- Event routine

A subprogram that updates the system state when a particular type of event occurs (there is one event routine for each event type).

3.5.8:- Library routines

A set of subprograms used to generate random observations from probability distributions that were determined as a part of simulation model.

3.5.9:- Report Generator

A subprogram that computes estimate (from the statistical counter) of the desired measures of performance and produces a report when the simulation ends.

3.5.10:- Main Program

A subprogram that invokes the timing routine to determine the next event routine to update the system state appropriately. The main program may also check for termination and invoke the report generator when the simulation is over.

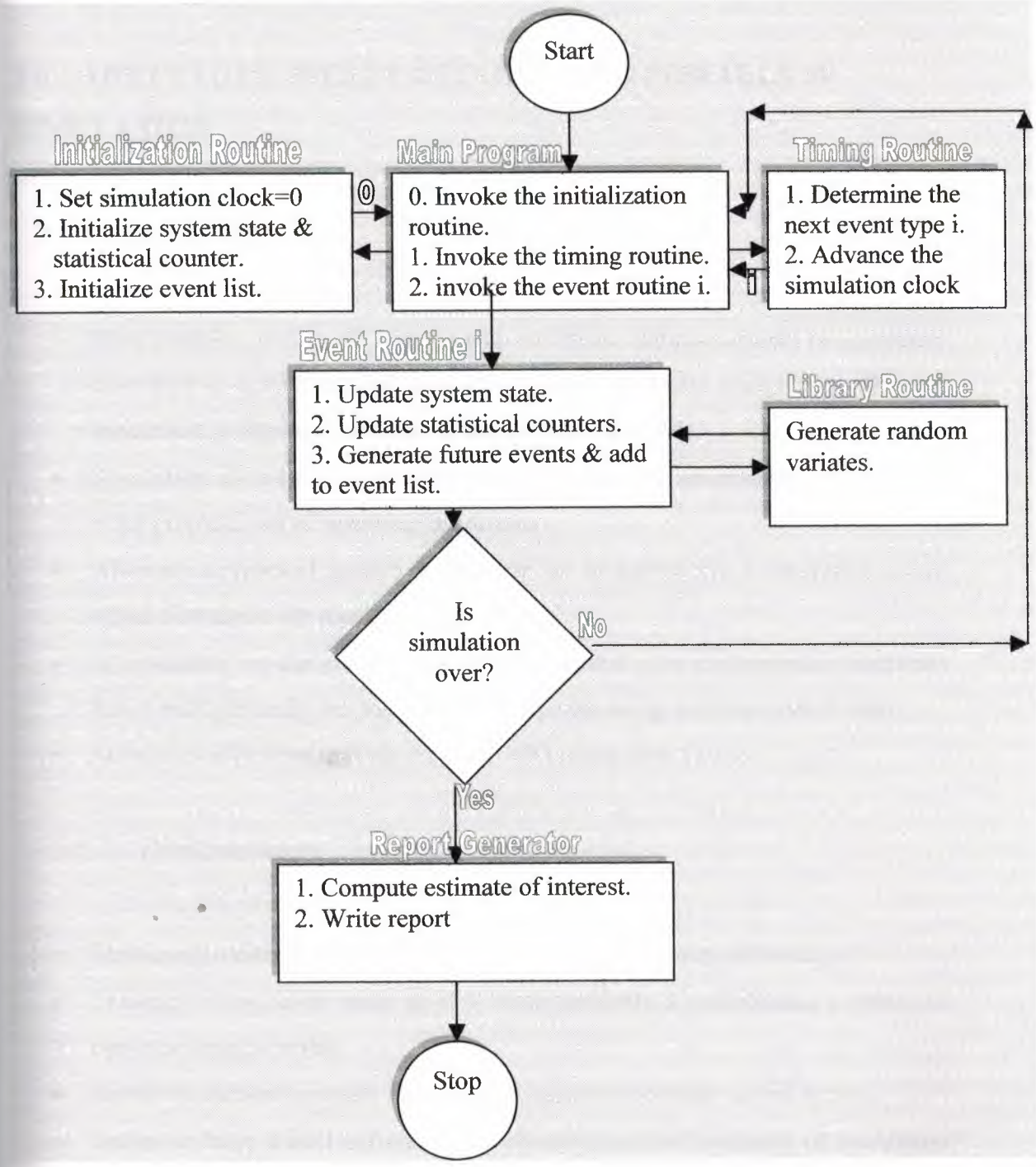


Figure 3.2:- *General Algorithm for Simulation*

3.6:- ADVATAGES, DISADVANTAGES, AND PITFALLS 0F SIMULATION

3.6.1:-Advantages

- Most complex, real world systems with stochastic elements cannot be accurately described by a mathematical model that can be evaluated analytically .Thus, a simulation is often the only type of investigation possible.
- Simulation allows one to estimate the performance of an existing system under some projected set of operating conditions
- Alternative proposed system designs can be compared via a simulation to see which best meets are specified requirement.
- In simulation we can maintain much better control over experimental conditions than would generally we possible when experimenting with the system itself.
- Simulation allows us to study a system with along time frame.

3.6.2:- Disadvantages

- Simulation models are often expensive and time consuming to develop.
- Treating a simulation study as if it were primarily a complicated exercise in computer programming.
- Failure to account correctly for source of random ness in the actual system
- Failure to have a well defined set of objectives at the beginning of simulation study.
- Making a single replication of a particular system design and treating the output statistics as the "true answer".
- Each run of stochastic simulation model produces only estimates of the model true characteristics for a particular set of input parameters
- Using wrong measures of performance
- Inappropriate level of model detail.

3.7:- Classification of Simulation Seawares

In this section I shall discuss various aspects of simulation software, including two different ways in which it can be classified.

3.7.1:- Simulation Languages vs. Simulators

- A ***simulation language*** is a computer package that is general in nature and may have special features for certain types of applications. For example, SIMAN and MATLAB have manufacturing modules for conveyors and a automated guided vehicle. A model is developed in a simulation language by writing a program using the language's modeling constructs. The major strength of most languages is their ability to model almost any kind of system, regardless of the system's operating procedures or control logic. Possible drawbacks of simulation languages are the need for programming expertise and the possibly long coding and debugging time associated with modeling complex systems.(relative to simulators, if applicable.

- A ***Simulator*** is a computer package that allows one to simulate a system contained in a specific class of systems with little or no programming. For example, NS (Network Simulator).
  The major advantage of a simulator is that "program" development time may be considerably less than that for a simulation language.

  Another advantage is that most simulators have modeling constructs related specifically to the components of the target class of systems, which is particularly desirable for operational personnel.

  The major drawback of many simulators is that they are limited to modeling only those system configurations allowed by their standard features.

3.8:- Modeling Approaches

- In the ***Event-Scheduling Approach***, a system is modeled by identifying its characteristic events and then writing a set of event routines that give a detailed description of the state changes taking place at the time of each event. The simulation evolves over time by executing the events in increasing order of their time of occurrence. Here a basic property of an event routine is that no simulated time passes during its execution.

- A ***Process*** is a time-ordered sequence of interrelated events separated by passages of time, which describes the entire experience of an "entity" as it flows through a "system." The process corresponding to an entity arriving to and being served at a single server. A system or simulation model may have several different types of processes. Corresponding to each process in the model, there is a process "routine" that describes the entire history of its "process entity" as it moves through the corresponding process. A process "routine" explicitly contains the passage of simulated time and generally has multiple entry points.

3.9:- DESIRABLE SOFTWARE FEATURES

I now give number of additional features that should be available in a contemporary simulation package.

3.9.1:- General Features

- Perhaps the most important feature for a simulation package to have is ***modeling flexibility***, because no two systems are exactly same. If the simulation package does not have the necessary capabilities for a particular application then the system must be -approximated, resulting in a model with unknown validity. Entities should have general attributes (e.g., due date, message length, etc.), which

  can be appropriately changed; this capability is generally available in simulation languages but is less common in simulators.

- Ease of ***model development*** is another very important feature, due to the short time frame for many projects. The accuracy and speed of the modeling process will be increased if the package has good debugging aids, such as an interactive debugger, on-line input error checking, and on-line help.

- Fast ***model execution speed*** is particularly important for very large models (e.g., certain military applications) and when the simulation model is to be run on a microcomputer.

- The ***maximum model size*** allowed by the simulation package may be an important factor when the model is to be executed on a microcomputer. For some packages, the maximum model size is currently less than 100 K bytes,

- It is also desirable for a simulation package to be available for a number of different computer classes (i.e., microcomputer, work station, and mini-computer/mainframe), and for the software to be ***compatible across these classes***.
  Thus, for example, a model could be developed on a microcomputer and then uploaded to a minicomputer or mainframe for execution of the production runs.

3.9.2:- Animation

- Most contemporary animation packages operate in a ***concurrent mode***, where the animation is displayed while the simulation is actually running (perhaps slowed down to allow for visual comprehension).

- On the other hand, some animation packages function in a ***playback mode***, where the animation is displayed after the simulation is completed from state changes recorded in a disk file. Several examples of animation and graphics are given in color Plate 1.

3.9.3:- Statistical Capabilities

- Since most real-world systems exhibit some sort of random behavior, a simulation package must contain good statistical capabilities that should actually be used. In general, each source of system randomness (inter-arrival times, service times, machine operating times, etc.) needs to be modeled by a ***probability distribution***.

- A simulation package should contain a wide variety of ***standard distributions*** (e.g., exponential, gamma, and triangular), should be able to use distributions based on observed system data and should contain a multiple-stream random-number generator to facilitate comparing alternative system designs.

3.10:- 802.11 MAC Layer Simulation Design

Wireless 802.11 MAC protocol is simulated with following simplifications:

1. Only Distributed Control Function (DCF) is in use. I did not make use of the Point Control Function (PCF).
2. No RTS (Ready To Send) or CTS (Clear To Send) messages are exchanged.
3. Since in the typical scenario of wireless 802.11 MAC, distance between communicating stations are very close, propagation delays are assumed to be zero.

In the simulation, the effect of following parameters regarding the operating environment can be studied:

1. Number of mobile communication stations.
2. Transmission range of each station. (Normalized by the length scale of station spacing.)
3. Mobility of stations.
4. Packet Size

Now I shall give you MATLAB codes for WLAN 802.11 MAC layer simulation. These codes simulate the IBSS (Ad-Hock mode) only. WLAN_MAC_802.11.m will simulate the MAC layer and SHOW1.m will show you graphics.

Note:-

Please note that both [WLAN_MAC_802.11.m] & [show1.m] files are required to run the simulator. Make sure they are in the same directory.

3.10.1:- wireless_demo.m

MATLAB code for wireless_demo.m is given in Appendix-1.

3.10.2:- Show1.m

MATLAB code for show1.m is given in Appendix-2

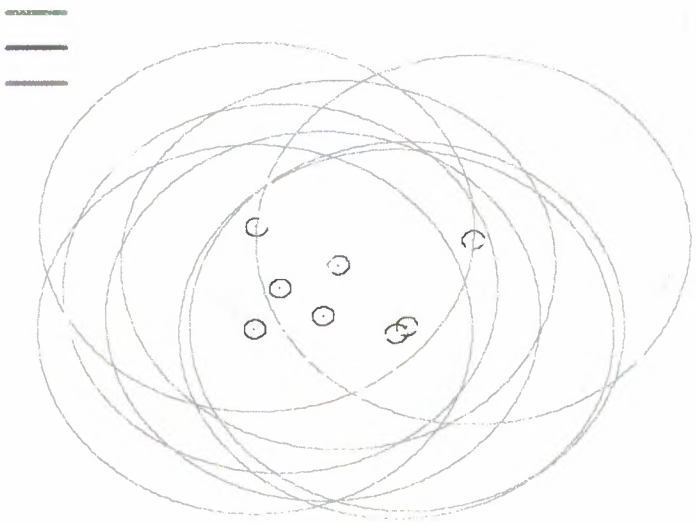
3.10.3:- Sample Screen Layout

When you will run the WLAN_MAC_802.11.m code in MATLAB it will ask you following parameters to enter:

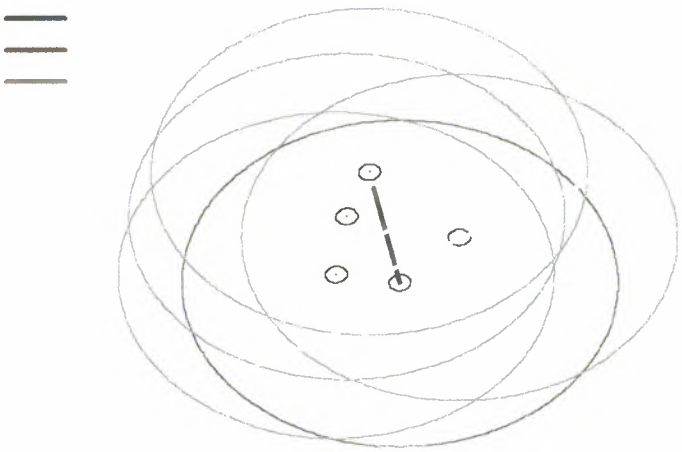
```
Length scale of Station spacing is 1
ans=
©IRFAN JAVED 992074 COM 400@NEAR EAST UNIVERSITY
ans=
Simulation parameters _____ [default value]
Please, Enter the Number of Stations?_____[5]
Please, Enter the Range of Radio Frequency?_____[3]
Time Scale of random motion? (SlotTime=2)_____[200]
Average Transmission Time (packet size)?_____[16]
Simulation Time In (ms)? (SlotTime=2)_____[600]
Show graphic?_____[y]
```

3.10.4:- Graphical Illustration

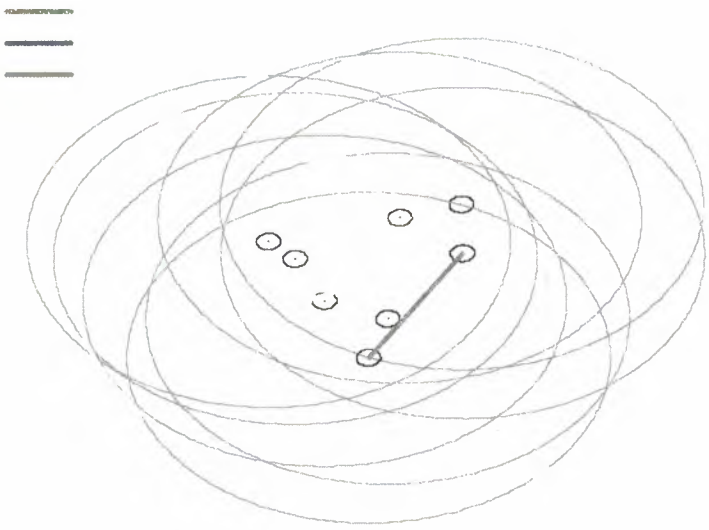
3.10.4.1:- Idle Network



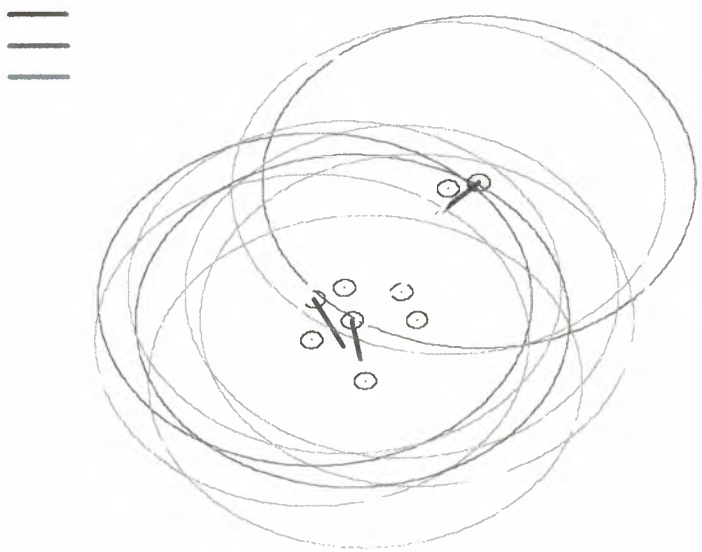
3.10.4.2:- Successful Packet Transmission



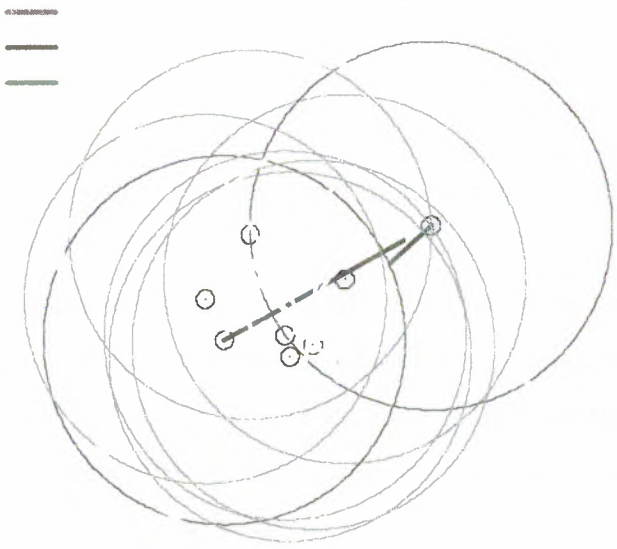
3.10.4.3:- Successful Ack Packet Transmission



3.10.4.5:- Collision in Packet Transmission



3.10.4.6:- Unreachable Packet



3.10.5:- Simulation Output Screen Layout

At the end of simulation output will like this:

```
transmission
14

collision
7

unreachable
2

ACK_collision
0
ACK_unreachable
0
```

3.11:- SUMMARY

From above study we summarize the following:

- A simulation is a valuable tool for understanding and studying the performance and behavior of the wireless networks.
- The facility or process of interest is usually called a system, and in order to study it scientifically we often have to make a set of assumptions about how it works.
- These assumptions, which usually take the form of mathematical or logical relationships, constitute a model that is used to try to gain some understanding of how the corresponding system behaves.
- All simulation models share a number of common components and there is a logical organization for these components that promotes the coding, debugging, and future changing of a simulation model's computer program.
- A simulation language is a computer package that is general in nature and may have special features for certain types of applications.
- A Simulator is a computer package that allows one to simulate a system contained in a specific class of systems with little or no programming.

CHAPTER 4

SIMULAITON RESULTS

4.0:- Introduction

In this chapter I shall explain the results with graphs which I got after simulation. These results help you to understand the behavior of WLAN in real world.

This chapter also provides you best and worst scenarios for WLAN according to their parameters.

It also helps you to understand how simulation is used to measure and analyze the performance of Wireless LAN

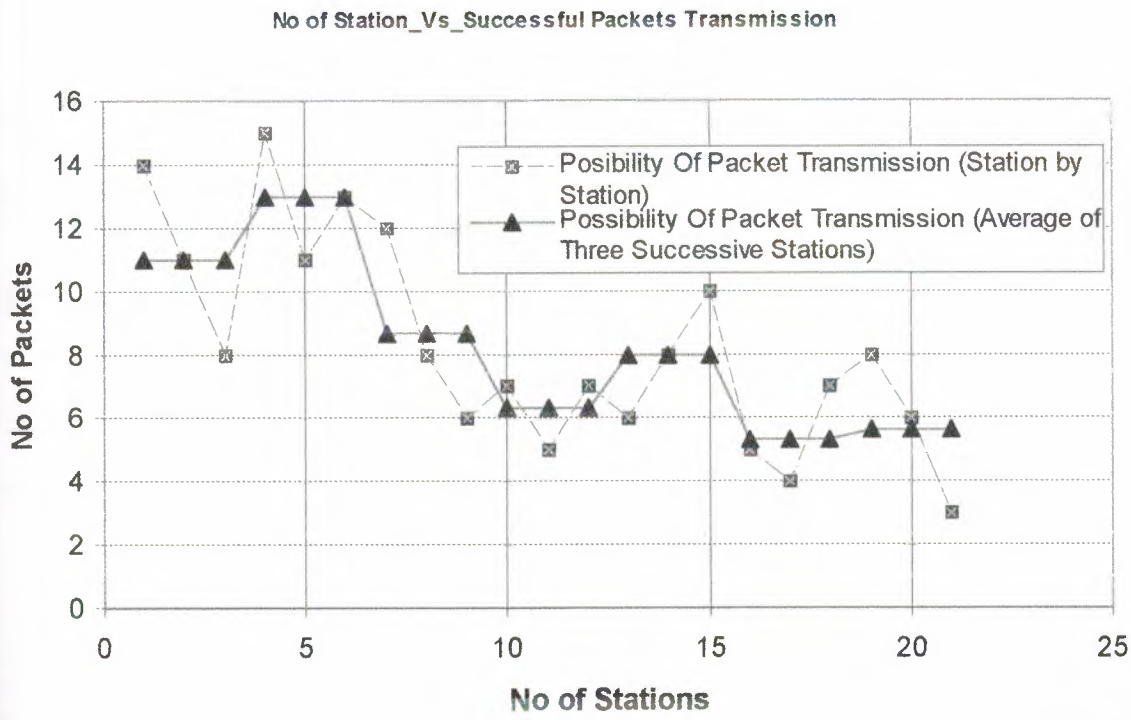
It is difficult and expensive to test wireless protocols in the real world. Therefore most tests are carried out using simulation. Most simulations are of static wireless nodes. These static simulations are appropriate for testing actual configurations.

In the simulation, the effect of following parameters regarding the operating environment can be studied:

1. Number of mobile communication stations.
2. Average packet size
3. Transmission range of each station. (Normalized by the length scale of station spacing.
4. Mobility of stations.

4.1:- Number of mobile communication stations

4.1.1:- No of Stations Vs Successful Packet Transmission



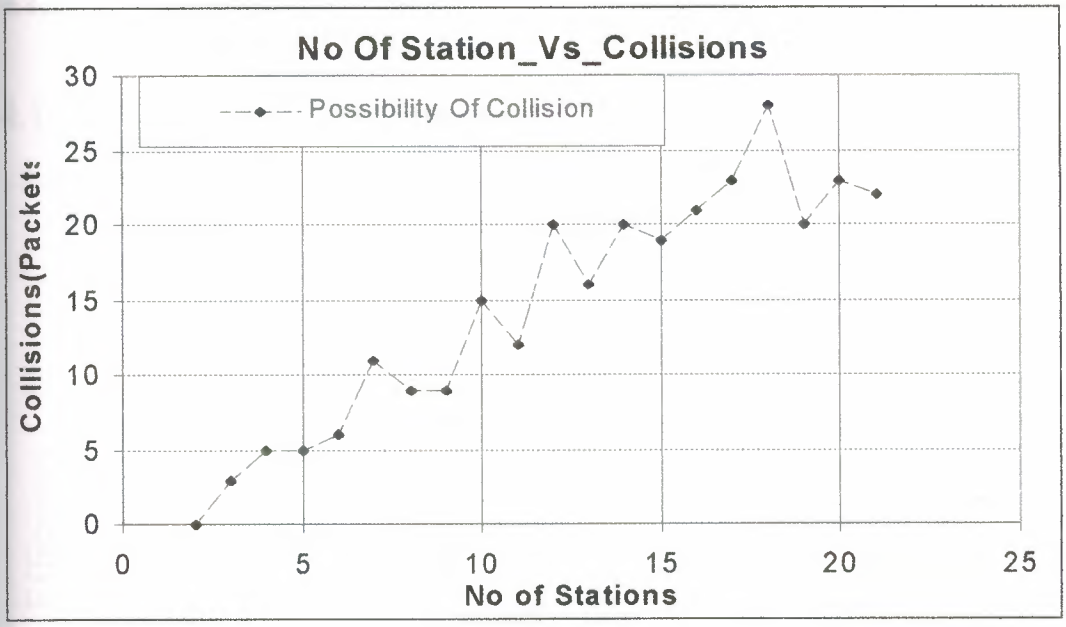
4.1.1.1:-Best Scenario

No of station = 4

4.1.1.2:- Worst Scenario

No of Stations= 21

4.1.2:- NO Of Stations Vs Collisions



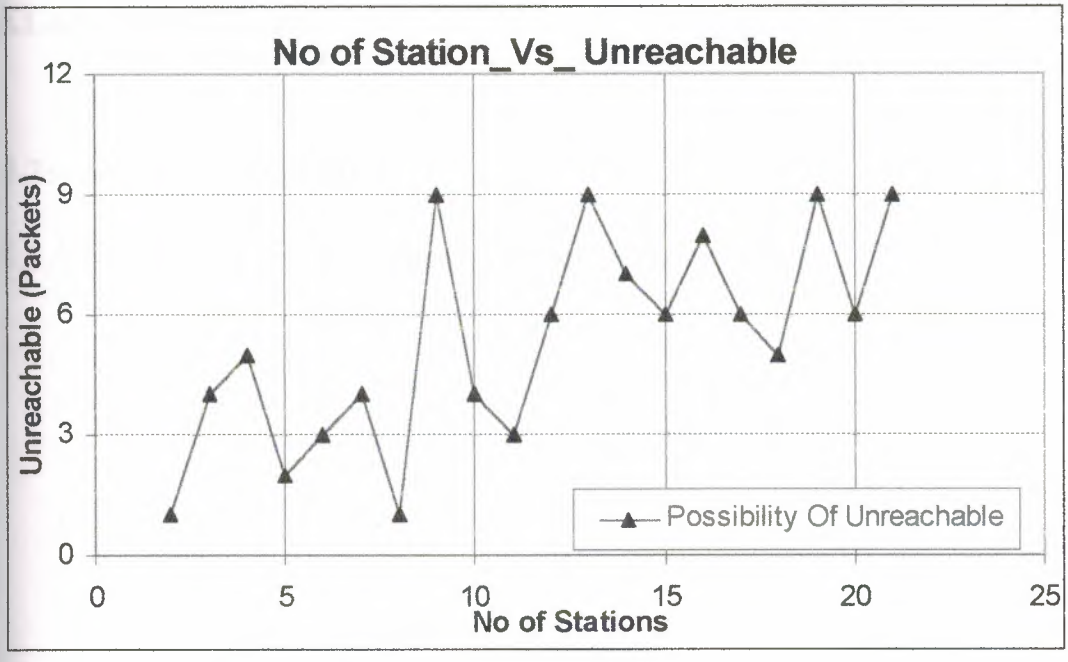
4.1.2.1:- Best Scenario

No Of Station=2

4.1.2.2:- Worst Scenario

No Of Stations=18

4.1.3:- No Of Stations Vs Unreachable



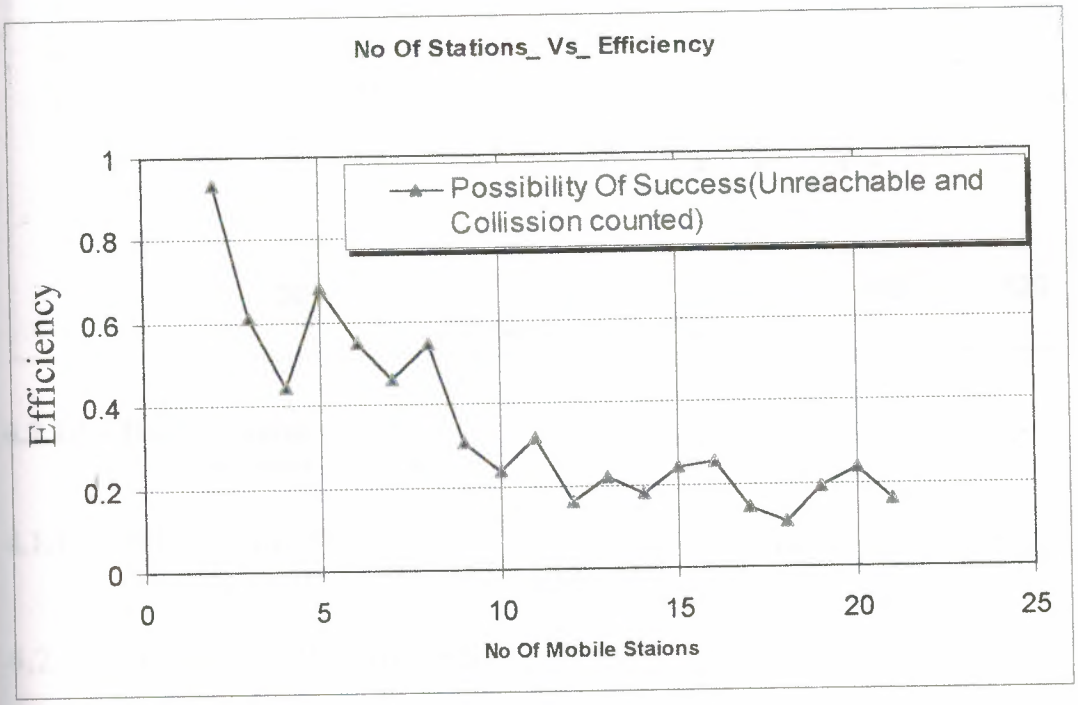
4.1.3.1:- Best Scenario

No of Stations=2,8

4.1.3.2:- Worst Scenario

No of Station=9,13,19,21

4.1.4:- No Of Stations Vs Efficiency



4.1.4.1:- Best Scenario

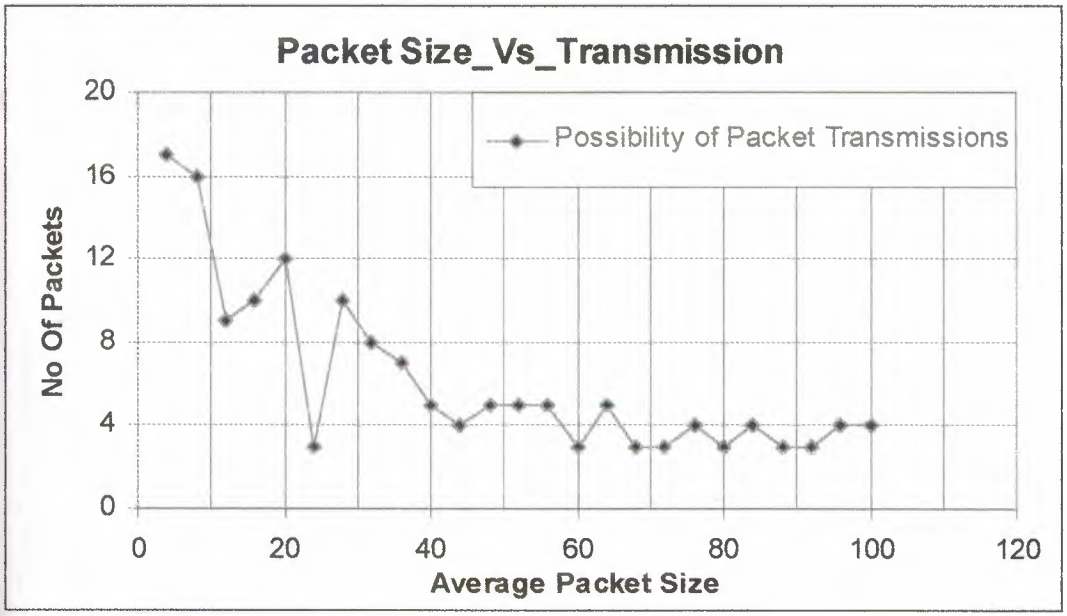
No of Stations=2

4.1.4.2:- Worst Scenario

No of Stations=18

4.2:- Average packet size

4.2.1:- Packet Size Vs Successful Packets Transmission



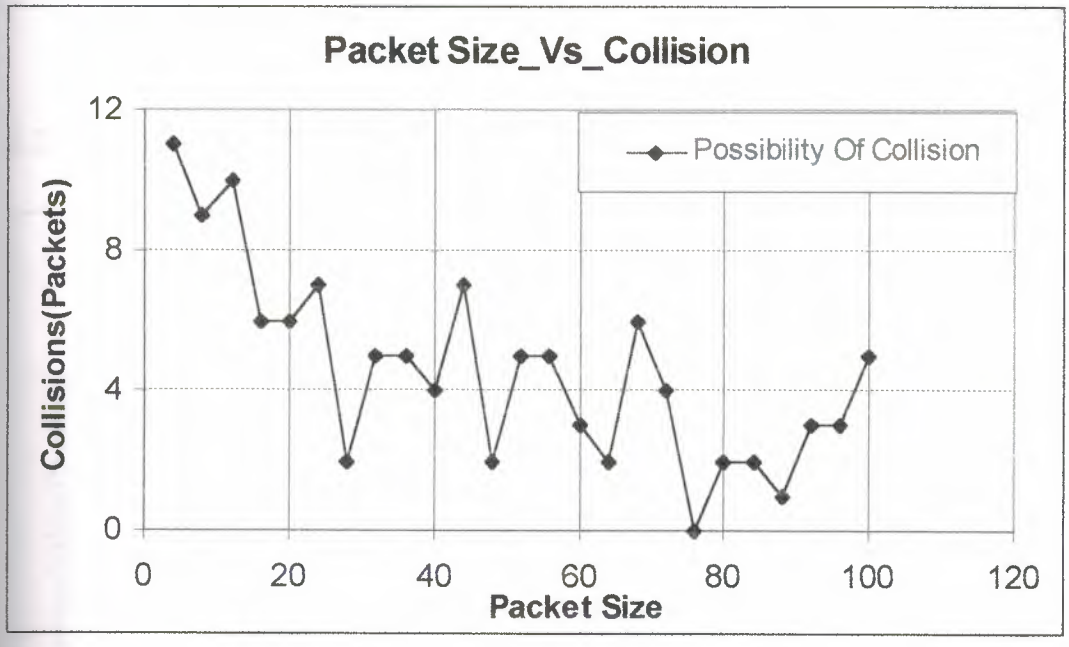
4.2.1.1:- Best Scenario

Average Packet Size=4

4.1.1.2:- Worst Scenario

Average Packet Size=60,68,72,80,88,92

4.2.2:- Packet Size Vs Collisions



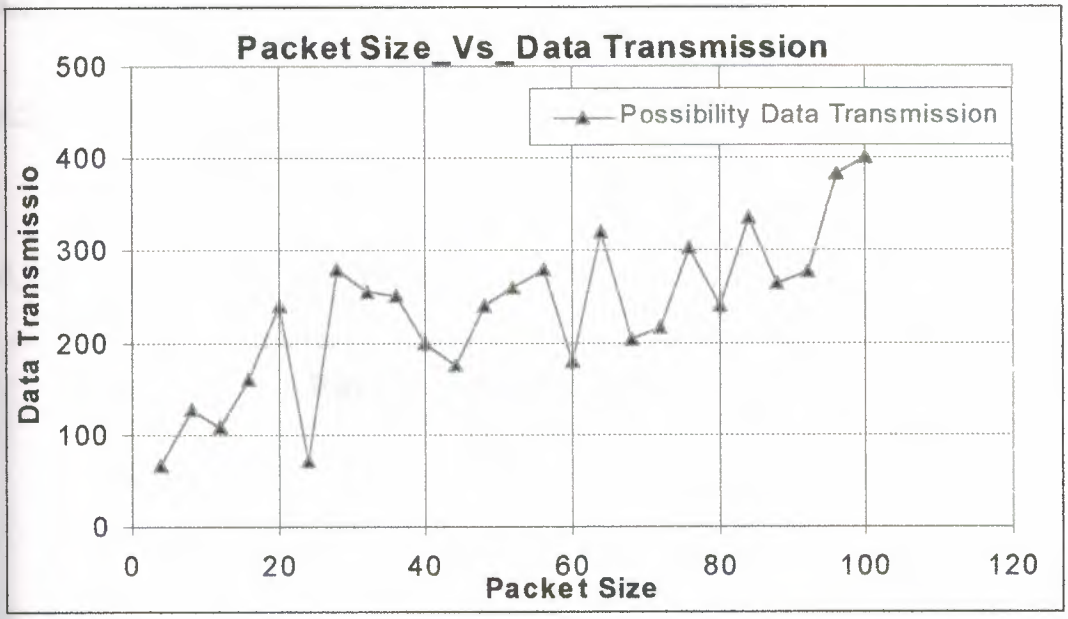
2.2.2.1:- Best Scenario

Average Packet Size=76

4.2.2.2:- Worst Scenario

Average Packet Size=4

4.2.3:- Packet Size Vs Data Transmission



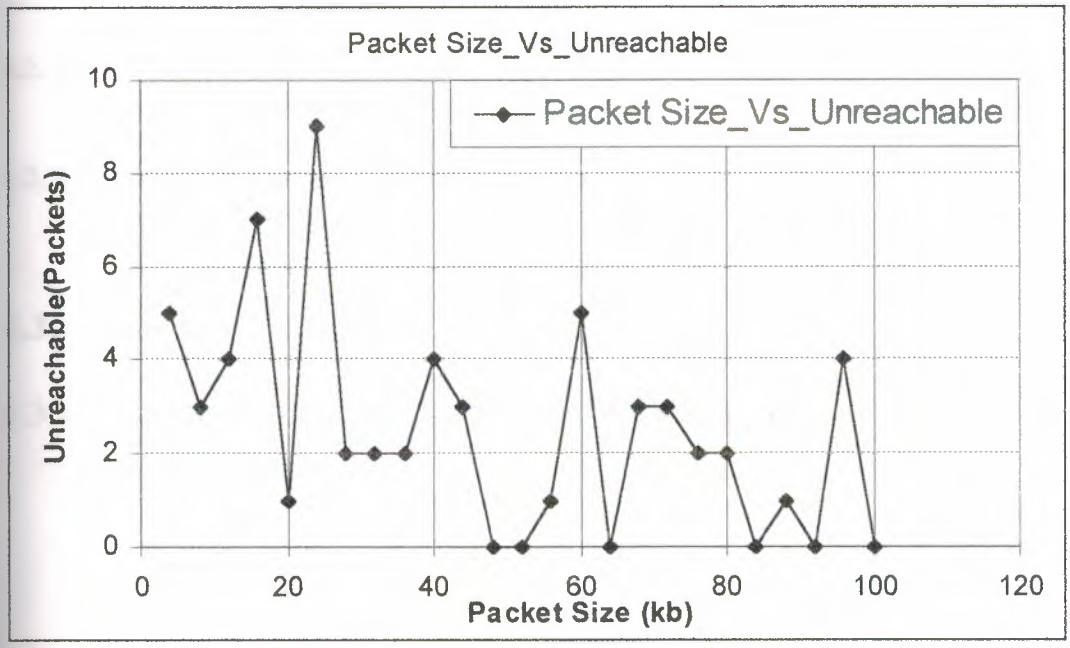
4.2.3.1:- Best Scenario

Average Packet Size=100

4.2.3.2:- Worst Scenario

Average Packet Size=4

4.2.4:- Packet Size Vs Unreachable



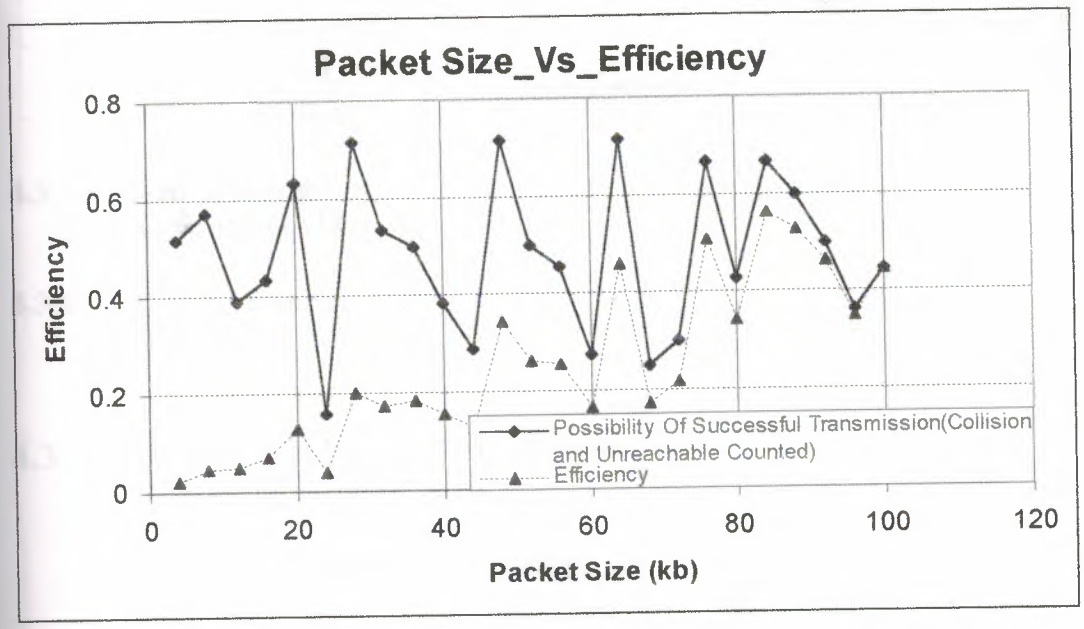
4.2.4.1:- Best Scenario:-

Average Packet Size=48,52,64,84,92,100

4.2.4.2:- Worst Scenario:-

Average Packet Size=24

4.2.5:- Packet Size Vs Efficiency



4.2.5.1:- Best Scenario

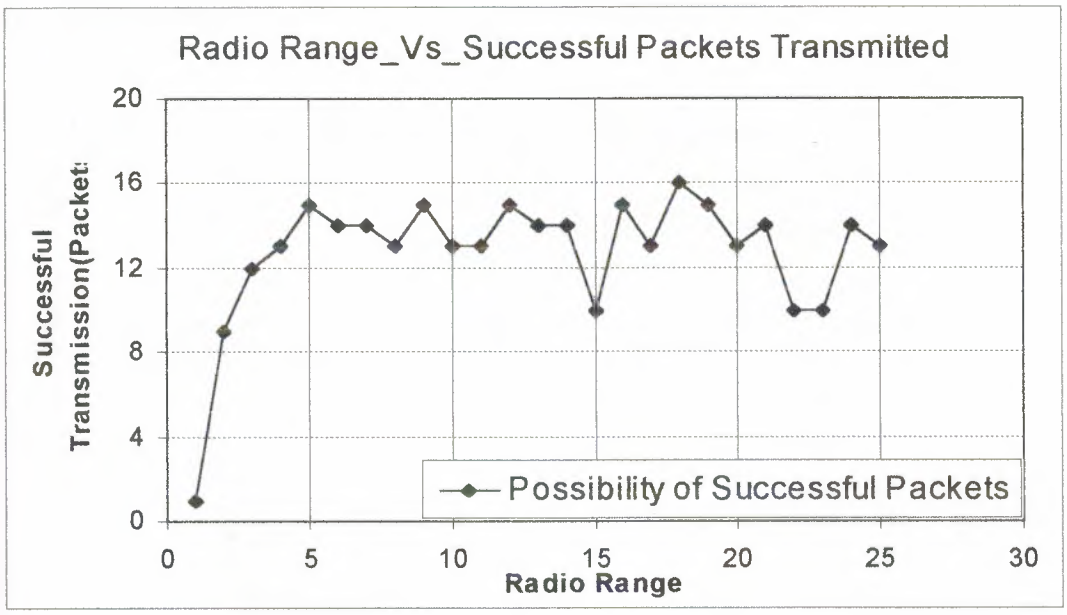
Average Packet Size=84

4.2.5.2:- Worst Scenario

Average Packet Size=4

4.3:- Transmission Range

4.3.1:- Transmission Range Vs Successful Packet Transmission



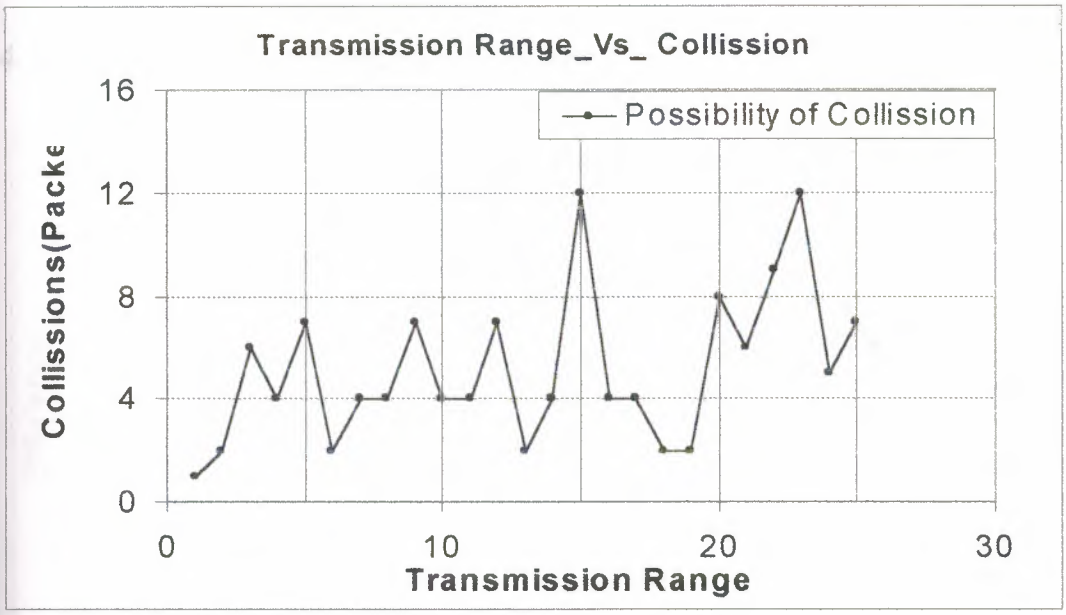
4.3.1.1:- Best Scenario

Radio Range=18

4.3.1.2:- Worst Scenario

Radio Range=1

4.3.2:- Transmission Range Vs Collisions



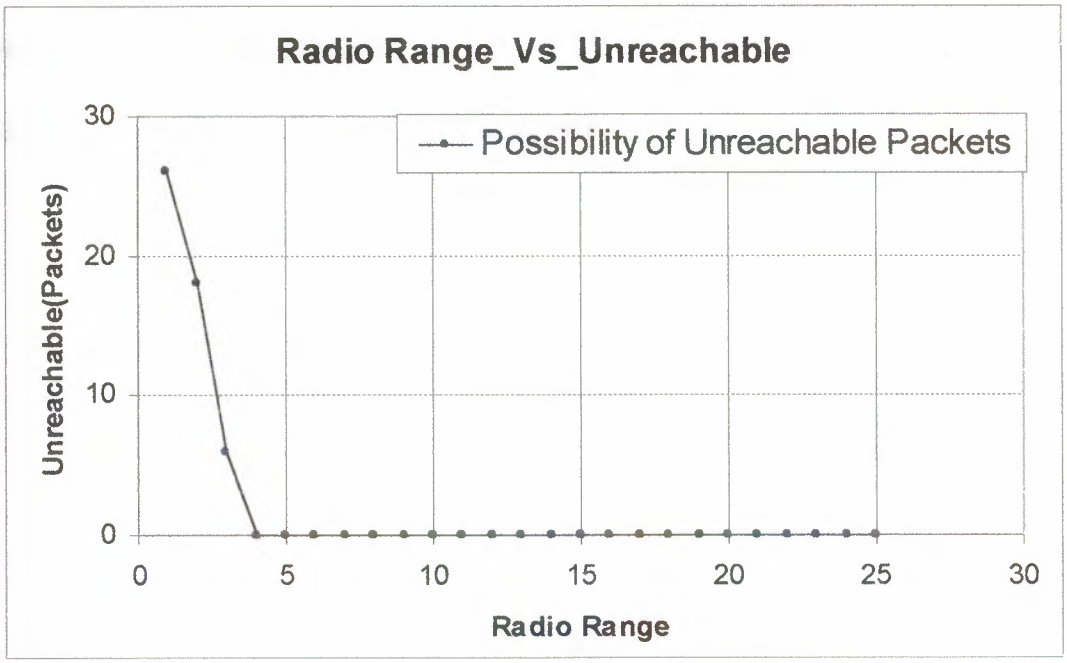
4.3.2.1:- Best Scenario

Radio Range=1

4.3.2.2:- Worst Scenario

Radio Range=15,23

4.3.3:- Transmission Range Vs Unreachable



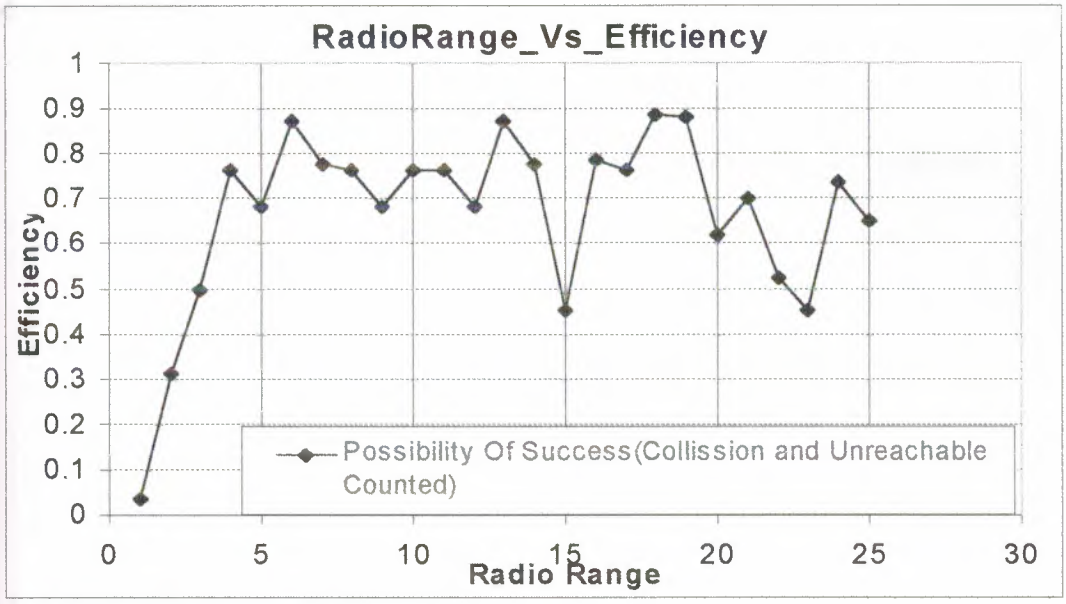
4.3.3.1:- Best Scenario

Radio Range=4,5,6,...,25

4.3.3.2:- Worst Scenario

Radio Range=1

4.3.4:- Transmission Range Vs Efficiency



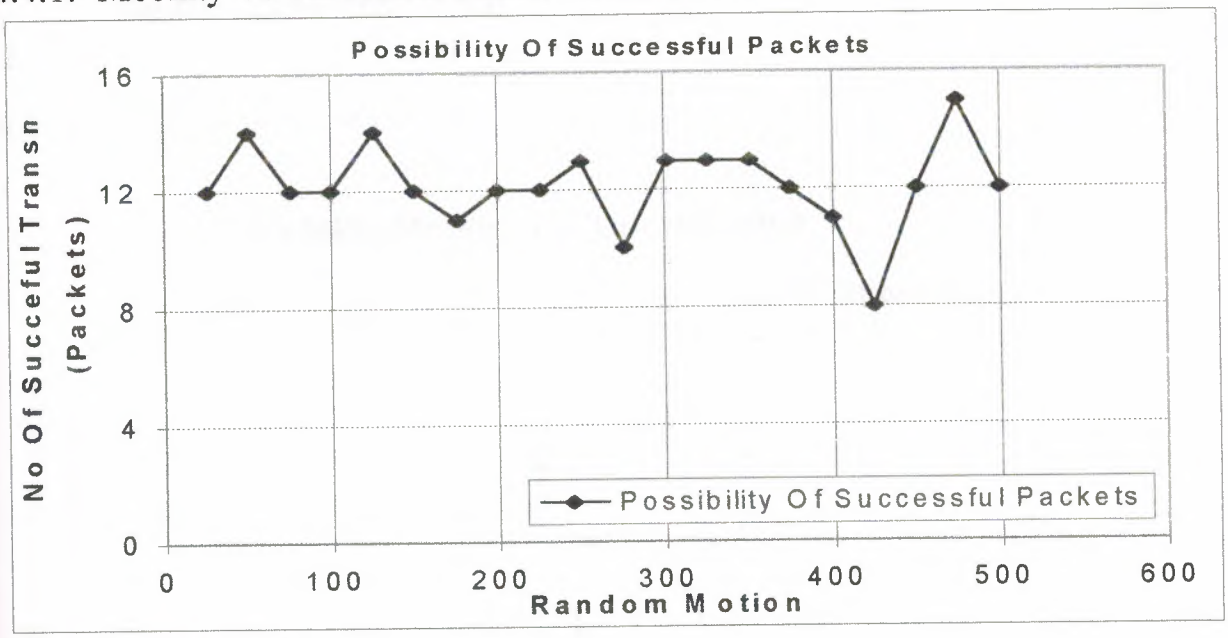
4.3.4.1:- Best Scenario

Radio Range=18

4.3.4.2:- Worst Scenario
Radio Range=1

4.4:- Mobility Of Stations

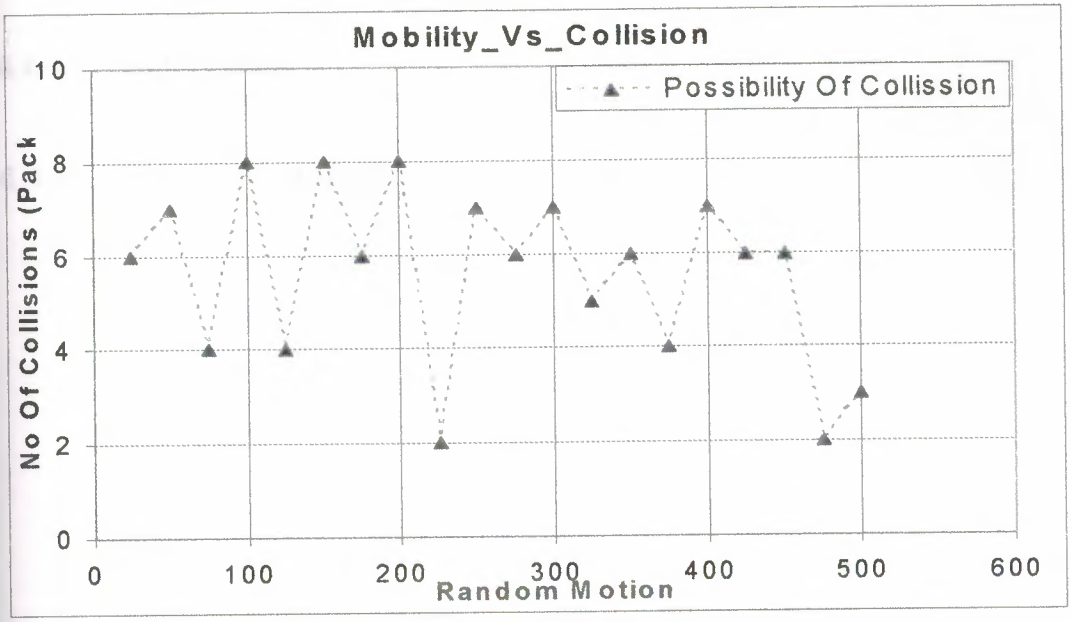
4.4.1:- Mobility Vs Successful Packet transmission



4.4.1.1:- Best Scenario
Random Motion=475

4.4.1.2:- Worst Scenario
Random Motion=425

4.4.2:- Mobility Vs Collisions



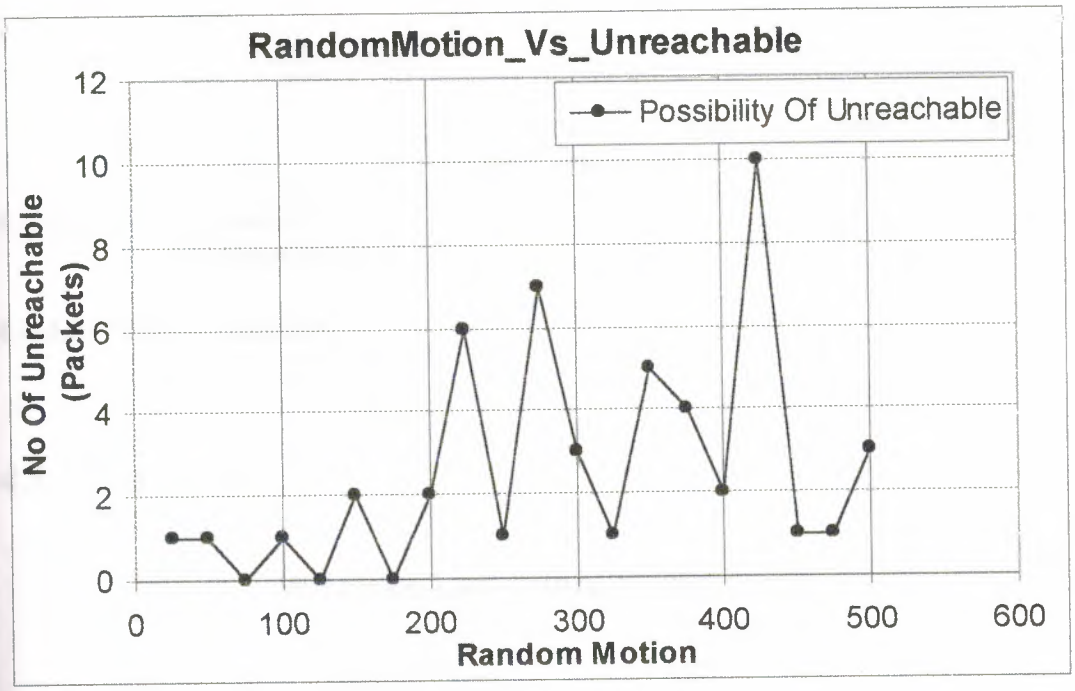
4.4.2.1:- Best Scenario

Random Motion=225,475

4.4.2.2:- Worst Scenario

Random Motion=100,150,200

4.4.3:- Mobility Vs Unreachable



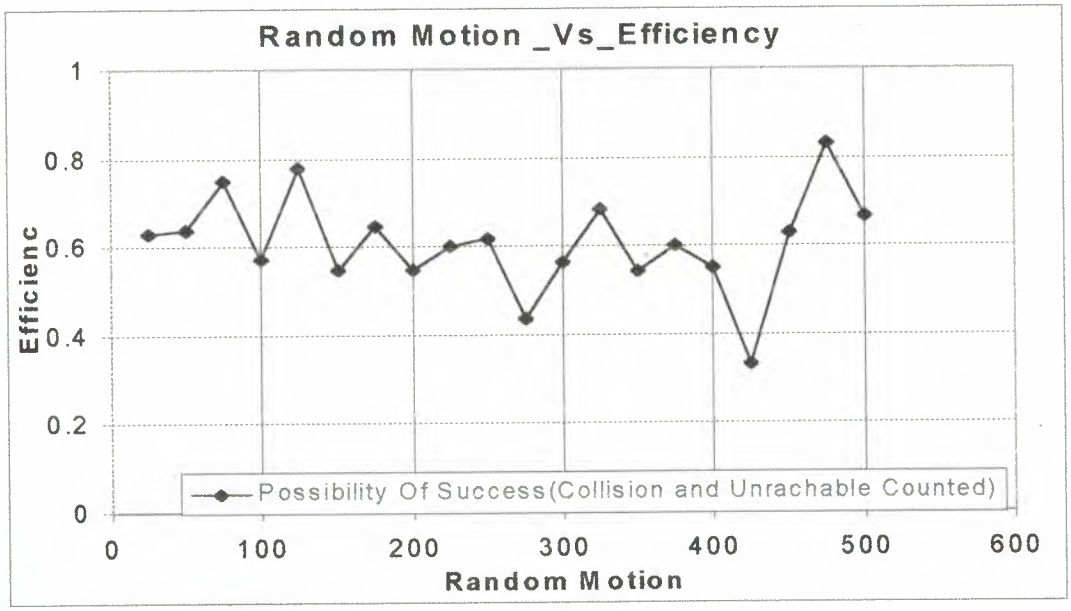
4.4.3.1:- Best Scenario

Random Motion=75,125,175

4.4.3.2:- Worst Scenario

Random Motion=425

4.4.4:- Mobility Vs Efficiency



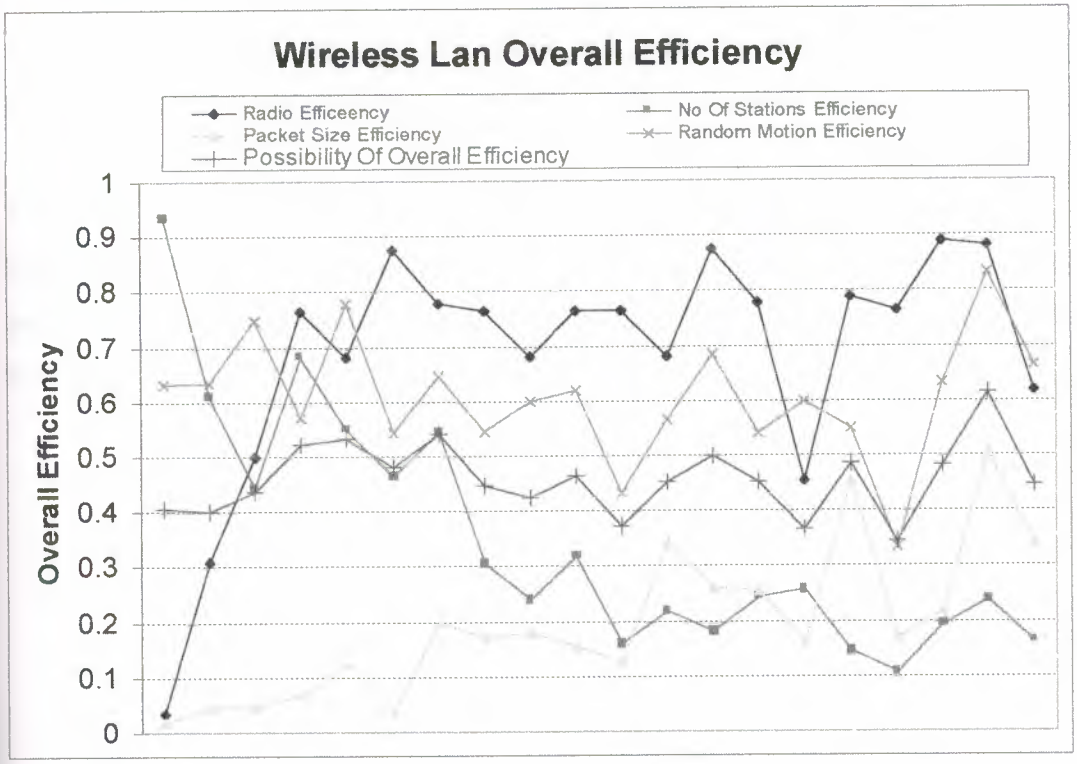
4.4.4.1:- Best Scenario

Random Motion=475

4.4.4.2:- Worst Scenario

Random Motion=425

4.5:- SUMMARY



CHAPTER 5

CONCLUSIONS

5.0:- Introduction

This chapter will provide you conclusions based on results which I discussed in previous chapter ***Simulation Results***.

In this chapter, I present an overall view on this subject in a detailed analysis of the major factors involved. Specially, I shall show how TCP can be affected by mobility.

Additionally, I shall highlight the main features and weaknesses of the existing proposed schemes, and point out the main open issues in this area.

The main aim of this whole project is to model a Wireless LAN network where it shows best performance according to their given parameters. So, at the end of this chapter I presents some WLAN models in different scenarios these models are based on results of simulation which we did in previous chapter.

5.1:- Conclusions

- Radio Frequency (RF) or Infrared (IR) is used as a transmission medium for data transfer in WLAN and It has fuzzy boundaries.
- The key to the WLAN specification is the MAC. It rides on every physical layer and controls the transmission of user data into the air. 802.11 uses a *Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)* scheme to control access to the transmission medium.
- Analysis and simulation are good tool for examine the performance of the physical or MAC layer. These two tools are very flexible but more time is spent in the research and setup simulation than experimentation.
- The capacity of wireless ad-hoc networks can be very low, due to the requirement that nodes forward each other's packets. Capacity is the limiting factor: a large mobility causes a high volume of routing queries and updates which brings along high congestion, which leads to packet losses.
- From simulation results, I concluded that packet size should be greater then 1000kb for better performance and transmission rate.
- Now I shall design a WLAN network where user are within office and mobility is very low. Figure 5.1(a) shows that how we can design transmission range. Arrows in *Figure 5.1(b)* representing the path of data transmission.

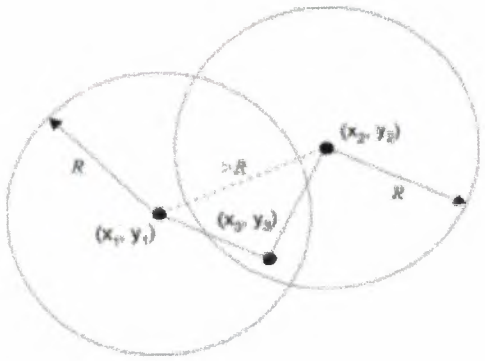


Figure 5.1(a):-*Adjustment of Transmission Range*

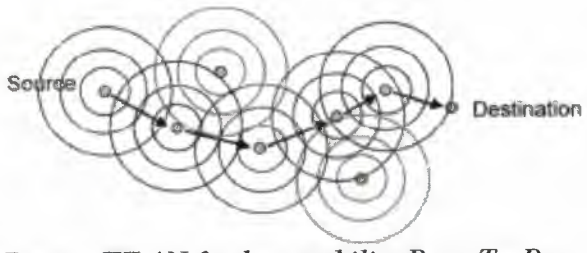
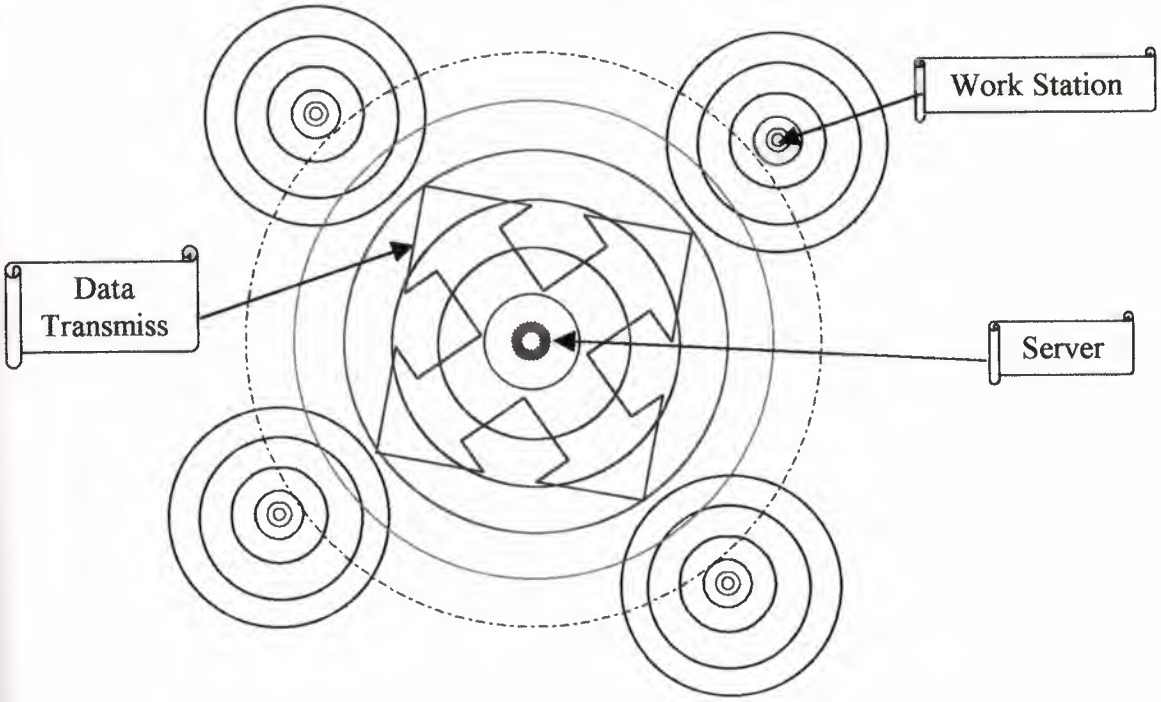


Figure 5.1(b):-Design WLAN for low mobility Peer-To-Peer Communication

- Now I shows you how we can design WLAN where network is Client/Server If you see in *Figure 5.2* server can communicate with each work station but work stations are hidden for each other. In this scenario I assume that work stations are always communicate with server only. Work stations can communicate with each other via server only.



- High probability of both network partition and route failures due to mobility.
- TCP has been shown to perform poorly over wireless links.
- The investigation shows that the amount of data being transmitted in the medium can be controlled through the manipulation of TCP window sizes.

- From my whole project I concluded that the MAC layer has a three-fold duty:

1. Firstly, it ensures that data is received reliably, so that when errors occur they are noted and the corrupted data is not passed up the protocol stack.
2. Secondly, it controls access to the wireless medium in a way that both minimizes data collisions and fairly distributes available bandwidth among all the stations.
3. Thirdly, it should protect data from decoding by unwanted listeners. Each of these tasks is made more difficult than in the case of wired networks because of the peculiarities of the wireless medium.

CHAPTER 6

FUTURE WORK

6.0:- Introduction

This chapter focuses on Future of the WLAN and I shall mention some existing problems in 802.11 protocols.

This chapter describes challenges underlying WLAN, which I observed during my research. These problems should solve in order to have a better transmission rate, better use of transmission medium, flexibility, reliable communication and security.

This chapter also provides you some ideas, which can solve these problems. These ideas can be implemented in given simulation program to analyze the performance of network.

Although WLANs have been available commercially for several years, there was no international standard available until the recent approval of IEEE 802.11. Due to the fact that a large number of manufacturers announced the introduction of IEEE 802.11 conforming products recently, we expect most of the WLANs to be IEEE 802.11 compatible in the near future. Thus, a thorough understanding of IEEE 802.11 will benefit the future development of user applications for the standard.

Ideally, users of wireless networks want the same services and capabilities that they have commonly experienced with wired networks. However, the wireless community faces certain challenges and constraints such as interference and reliability. In order to adapt user applications to WLANs, an intensive understanding of the medium and the data-link layer of WLANs is critical.

As WLANs become popular and given the poor performance of TCP over wireless links becomes more relevant, more detailed studies are necessary.
Yet, research in the area of WLAN is receiving much attention from academia, industry, and government. Since these networks pose many complex issues, there are many open problems for research and opportunities for making significant contributions

6.1:- Challenges for WLAN

WLAN pose some tough challenges to TCP because it was not designed to operate in such a highly dynamic scenario in terms of topology. In reality, even though TCP has evolved significantly over the years toward a robust and reliable service protocol, the focus has been primarily on wired networks.
In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency and rescue operations,

disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of WLANs.

6.1.1:- Protocol Design

The Transmission Control Protocol (TCP) raises a number of issues when required to work in a wireless environment. In particular, within an ad hoc network, where changes can happen somewhat quickly and unpredictably, it has to deal with new tough challenges.

The design of network protocols for these networks is a complex issue. Regardless of the application, WLANs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to WLANs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues.

6.1.2:- Mobility

Wireless networks are fundamentally about mobility. 802.11 deployments have successfully demonstrated that users are interested in mobility and that mobile connectivity is a long-felt need in the networking world. After all, users move, but network jacks do not.

However, 802.11 offers only link-layer mobility, and that is possible only when the access points can all communicate with each other to keep track of mobile stations. Standardization of the IEEE 802.11 Task Group should make it easier to merge multiple distinct wireless networks into each other.

6.1.3:- Hidden Node Problem

Each node in a wireless ad hoc network functions as both a host and a router, and the control of the network is distributed among the nodes. The network topology is in general dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of

having mobile nodes. Hence, there is a need for efficient routing protocols to allow the nodes to communicate over multihop paths consisting of possibly several links in a way that does not use any more of the network "resources" than necessary.

6.1.4:- Routing

The network should be able to adaptively alter the routing paths to alleviate any of these effects.

6.1.5:- IP Allocation

It's easy to overlook the problems that mobility causes at the IP level. It's easy to say that a wireless node should receive a new IP address when it moves from one part of a larger network to another, but in practice, it isn't simple. How do you get the node to notice that it should abandon its current address and ask for a new one? What happens to network connections that are open when the node's IP address changes?

5.1.6:- Planning the location of Access Point (AP)

It's difficult and sometimes impossible to predict radio wave Propagation due to its fuzzy boundaries. Therefore, it is not easy to locate the location of access points. So, there is a need to find a proper solution for this problem.

6.1.7:- Security

Wireless networks have all been tarred with the brush of poor security. Weaknesses in the Wired Equivalent Privacy (WEP) standard made the news with a great deal of regularity in 2001, culminating with a total break partway through the year. Even against this backdrop, though, the market for 802.11 network equipment has exploded. Better security mechanisms are needed to usher in centrally coordinated rollouts at large, security-conscious institutions, but the apparent security weaknesses in current equipment have not prevented the market from forming and growing rapidly.

6.1.8:- Radio Resources

So far, wireless networks have had a free ride. They are fairly exotic, and wireless cards still aren't common so wireless networks tend to have relatively few users and the networks themselves are physically relatively far apart. What happens when they're stressed? What would a wireless network be like if it had, say, 1,000 users (which can easily be supported by a well-designed wired network)? What would it be like in a large office building, where you might have half a dozen companies, each with its own network, in the space of two or three floors?

We don't really have the answers to these questions yet. As wireless becomes more common, we'll be forced to answer them. It is clear, though, that there are resource constraints. Current technologies will suffer from overcrowding within the unlicensed 2.4-GHz band. 802.11a and other technologies will move to the 5-GHz band, but crowding will eventually become an issue there, too. Meanwhile, commercial users are fighting for additional frequency space, and it's not likely that governments will allocate more spectrum to unlicensed users.

Bibliography

1. Simulation Modeling & Analysis[Second Edition] by Averill M.law , W.David Kelton.

2. COTTON, I. [1979], Technologies for local area computer networks.

3. FRANTA, W. R and I. CHLAMTAC [1981], Local networks, Lexington books, Lexington Massachusetts.

4. GREEN, P.E (ED) [1982], Computer network Architectures and protocols, Plenum Press, New York.

5. Tanedaum Andrew S. Computer Network,1996

WORLD WIDE WEB

1. http://www.cisco.com

2. www.IEEE.net

3. www.mit.edu

4. www.wirelessvalley.com

5. www.wireless-nets.com

APPENDIX-1

```
% COMENT LINE
% START OF WLAN_MAC_802.11.m SIMULATION CODE
'Length scale of Station spacing is 1'
'IRFAN JAVED 992074 COM 400@NEAR EAST UNIVERSITY'

'Simulation parameters _____ [default value]'

n=input('Please, Enter the Number of Stations?_____[5] ');

if length(n)==0

  n=5;

end

r=input('Please, Enter the Range of Radio Frequency?_____[3] ');

if length(r)= =0

  r=3;

end

motion_scale=input('Time Scale of random motion? (SlotTime=2)_____[200] ');

if length(motion_scale)= =0

  motion_scale=200;


end

frame_size=input('Average Transmission Time (packet size)?_____[16] ');

if length(frame_size)= =0

  frame_size=16;

end

max_simutime=input('Simulation Time In ms? (SlotTime=2)_____[600] ');  %ms

if length(max_simutime)= =0

  max_simutime=600;

end

sss=input('Show graphic?_____[y] ');

if length(sss)==0
```

```
  sss='y';
end
ph=0:0.02:2*pi;
if sss=='y'
figure
hold on

j=sqrt(-1);
for i=1:n
  h1(i)=plot(exp(j*ph)*(1+r),'EraseMode','xor','color','r','Marker','o','Markersize',5);
  h2(i)=plot(exp(j*ph)*(1+r),'EraseMode','xor');
%h3(i)=plot(exp(j*ph)*(1+r),'EraseMode','xor');
h4(i)=plot(exp(j*ph)*(1+r),'EraseMode','xor');
h5(i)=plot(exp(j*ph)*(1+r),'EraseMode','xor','LineWidth',3,'color','r');
h6(i)=plot(exp(j*ph)*(1+r),'EraseMode','xor','LineWidth',3,'color','g');
%h7(i)=plot(exp(j*ph)*(1+r),'EraseMode','xor','LineWidth',3,'color','m');
end
tempx=-(1+r)*1.2;
tempy=(1+r)*1.2;
offsetx=(1+r)/5;
offsety=(1+r)/7;
plot([tempx,tempx+offsetx],[tempy,tempy],'color','r','LineWidth',3);
text(tempx+offsetx*1.2,tempy,'Data packet within transmission range');
plot([tempx,tempx+offsetx],[tempy-offsety,tempy-offsety],'color','m','LineWidth',3);
text(tempx+offsetx*1.2,tempy-offsety,'Data packet outside transmission range');
plot([tempx,tempx+offsetx],[tempy-offsety*2,tempy-offsety*2],'color','g','LineWidth',3);
text(tempx+offsetx*1.2,tempy-offsety*2,'ACK packet');
```

```
end
traffic=1.0;
ACK_length=4;
Sifs=2;
SlotTime=2;
alpha=0.5^(1/motion_scale);
Eb2=0.001;
beta=(1-alpha^2-Eb2)/(2*Eb2-Eb2*alpha+(1-alpha^2)*alpha);
ER2=(1-beta^2)*Eb2;
Difs=Sifs+2*SlotTime;
state=zeros(1,n);
Timer=zeros(1,n);
pos_x=randn(1,n);
pos_y=randn(1,n);
pos_x_change=sqrt(Eb2)*randn(1,n);
pos_y_change=sqrt(Eb2)*rand(1,n);
PCWmin=3;
PCWmax=8;
PCW=PCWmin*ones(1,n);
RC=zeros(1,n);%retry counter
BC=zeros(1,n);%back-off counter
range=r*ones(1,n);
within=ones(n,n);
for i=1:n
  for k=1:n
    if ((pos_x(i)-pos_x(k))^2+(pos_y(i)-pos_y(k))^2>range(i)^2)
      within(i,k)=0;
```

```
    end
  end
end
current_frame_length=zeros(1,n);%Sifs+Difs+rand(1,n)*frame_size;
current_frame_dest=zeros(1,n);%ceil(rand(1,n)*n);
initial_cfl=zeros(1,n);
ACK_dest=zeros(1,n);
collision=0;
transmission=0;
unreachable=0;
ACK_collision=0;
ACK_unreachable=0;
for counter=1:max_simutime
  t0=clock;
  pos_x_change=beta*pos_x_change+randn(1,n)*sqrt(ER2);
  pos_y_change=beta*pos_y_change+randn(1,n)*sqrt(ER2);
  pos_x=pos_x*alpha+pos_x_change;
  pos_y=pos_y*alpha+pos_y_change;
within=ones(n,n);
        for i=1:n
        for k=1:n
        if ((pos_x(i)-pos_x(k))^2+(pos_y(i)-pos_y(k))^2>range(i)^2)
        within(i,k)=0;
        end
        end
  end
  sending=zeros(1,n);
```

```
sending(state>=5 | state<=-1)=1;
B_media=sending*within;
%Waiting for media
transit2=zeros(1,n);
transit2(state==1 & B_media<1)=1;
%  state(transit2>0)=2;
Timer(transit2>0)=Difs;
%Difs
transit1=zeros(1,n);
transit1(state==2 & B_media>0)=1;
%  state(transit1>0)=1;
Timer(state==2)=Timer(state==2)-1;
transit3=zeros(1,n);
transit3(state==2 & Timer<0)=1;
state(transit1>0)=1;
%Backing off
transit1(B_media>0 & state==3)=1;
% state(transit1>0)=1;
BC(state==3 & B_media<1)=BC(state==3 & B_media<1)-1;
transit5=zeros(1,n);
transit5(state==3 & BC<0)=1;
%  transitn=zeros(1,n);
% for i=1:n
%   if (transit5(i)>0 & B_media(current_frame_dest(i))<1 &
within(i,current_frame_dest(i))>0)
%     transitn(current_frame_dest(i))=1;
% end
% end
```

```
%sending
for i=1:n
  if (state(i)==5 & B_media(current_frame_dest(i))>1)
    state(i)=6;
  end
if (state(i)==5 & within(i,current_frame_dest(i))<1)
    state(i)=7;
  end
end
current_frame_length(state>=5)=current_frame_length(state>=5)-1;
transit0=zeros(1,n);
transit0(state>=5 & current_frame_length<=0)=1;
PCW(transit0>0 & state>5)=PCW(transit0>0 & state>5)+1;
PCW(PCW>PCWmax)=PCWmax;
PCW(transit0>0 & state==5)=PCWmin;
%current_frame_length
%state
%transit0
transmission=transmission+length(state(transit0>0 & state==5));
collision=collision+length(state(transit0>0 & state==6));
unreachable=unreachable+length(state(transit0>0 & state==7));
%state(transit0>0)=0;
transit4=zeros(1,n);
for i=1:n
  if (state(i)==5 & transit0(i)>0)
    ii=current_frame_dest(i);
    Timer(ii)=Sifs;
```

```
      transit4(ii)=1;
      ACK_dest(ii)=i;
    end
  end
  %ACK
  Timer(state==4 & B_media>0)=Sifs;
  Timer(state==4 & B_media<1)=Timer(state==4 & B_media<1)-1;
  transit_1=zeros(1,n);
  transit_1(state==4 & Timer<0)=1;
  Timer(transit_1>0)=ACK_length;
  for i=1:n
    if (state(i)==-1)
      ii=ACK_dest(i);
      if (B_media(ii)>1)
  state(i)=-2;
  end
      if (within(i,ii)<1)
        state(i)=-3;
      end
    end
  end
  Timer(state<=-1)=Timer(state<=-1)-1;
  transit0(state<=-1 & Timer<0)=1;
  ACK_collision=ACK_collision+length(state(state==-2 & transit0>0));
  ACK_unreachable=ACK_unreachable+length(state(state==-3 & transit0>0));
  %Idle
  state(transit0>0)=0;
```

```
temp=rand(1,n);
transit1(state==0 & temp<traffic)=1;
temp=Sifs+rand(1,n)*frame_size*2;
current_frame_length(transit1>0 & state==0)=temp(transit1>0 & state==0);
initial_cfl(transit1>0 & state==0)=current_frame_length(transit1>0 & state==0);
temp=ceil(rand(1,n)*n);
current_frame_dest(transit1>0 & state==0)=temp(transit1>0 & state==0);
for i=1:n
  while (current_frame_dest(i)==i | current_frame_dest(i)==0)
    current_frame_dest(i)=ceil(rand(1,1)*n);
  end
end
temp=floor(rand(1,n).*(2.^PCW));
BC(transit1>0 & state==0)=temp(transit1>0 & state==0)*SlotTime;
state(transit1>0)=1;
state(transit2>0)=2;
state(transit3>0)=3;
%state(transitn>0)=state(transitn>0)-9;
state(transit5>0)=5;
state(transit4>0)=4;
state(transit_1>0)=-1;
state(transit0>0)=0;
if sss=='y'
show1
drawnow
while etime(clock,t0)<0.1
   i=1;
```

```
 end
end
 % input('?');
end
transmission
collision
unreachable
ACK_collision
ACK_unreachable
```

%END OF ***WLAN_MAC_802.11.m*** SIMULATION CODE

Appendix- 2

% START OF ***show1.m*** CODE

```
 for i=1:n
   set(h1(i),'XData',pos_x(i),'YData',pos_y(i));
        set(h2(i),'XData',pos_x(i)+(range(i)/20)*cos(ph),'YData',pos_y(i)+sin(ph)*(rang
e(i)/20));
 %
set(h3(i),'XData',pos_x(i)+range(i)/3*2*cos(ph),'YData',pos_y(i)+sin(ph)*range(i)/3*2);

set(h4(i),'XData',pos_x(i)+range(i)*cos(ph),'YData',pos_y(i)+sin(ph)*range(i),'color','c')
;
   if (state(i)>=5)
      temp=1-current_frame_length(i)/initial_cfl(i);
      %temp=0.5;

set(h4(i),'XData',pos_x(i)+range(i)*cos(ph),'YData',pos_y(i)+sin(ph)*range(i),'color','m'
);
      if within(i,current_frame_dest(i))>0
```

```
set(h5(i),'XData',[pos_x(i),pos_x(i)+min(temp,range(i))*(pos_x(current_frame_dest(i))-
pos_x(i))],'YData',[pos_y(i),pos_y(i)+min(temp,range(i))*(pos_y(current_frame_dest(i)
)-pos_y(i))],'color','r');
    else
set(h5(i),'XData',[pos_x(i),pos_x(i)+min(temp,range(i))*(pos_x(current_frame_dest(i))-
pos_x(i))],'YData',[pos_y(i),pos_y(i)+min(temp,range(i))*(pos_y(current_frame_dest(i)
)-pos_y(i))],'color','m');
    end
%set(h7(i),'XData',[pos_x(i)+min(temp,range(i))*(pos_x(current_frame_dest(i))-
pos_x(i)),pos_x(i)+(min(temp,range(i))+temp-range(i))*(pos_x(current_frame_dest(i))-
pos_x(i))],'YData',[pos_y(i)+min(temp,range(i))*(pos_y(current_frame_dest(i))-
pos_y(i)),pos_y(i)+(min(temp,range(i))+temp-
range(i))*(pos_y(current_frame_dest(i))-pos_y(i))],'color','m');
  else
    set(h5(i),'color','w');
    %set(h7(i),'color','w');
  end
  if (state(i)<=-1)
    set(h6(i),'XData',[pos_x(i),pos_x(ACK_dest(i))],'YData',[pos_y(i),pos_y
(ACK_dest(i))],'color','g');
  else
    set(h6(i),'color','w');
  end
end
```

% END OF ***show1.m*** CODE