Faculty of Engineering,
Electronics and Communications Engineering,
Communications Systems,
Lab3, Section 5.
JUN 2021

Ghaidaa Samir Mohamed	**180**
Omar Mohamed Mounir	**163**
Omar Nabil Fathy	**165**
Omar Nasr Mohamed Younis	**166**

Communication Systems

Lab 3

Part 1: WIFI Report:

1. Introduction and History:

Wireless Local Area Network (WLAN)
First WLAN devices appeared on the market in mid 1990s and after 10 years WLAN became the main technology for connecting computers, smart phones, and tablets to the internet.
It's primary based on existing LAN standards created by IEEE for wired interconnection of computer (Ethernet Standards) [802.3]

2. Applications:

2.1. Wireless Internet.
2.2. Hotspot Internet (Wireless Internet Access Point).
2.3. Point to Point connections.
2.4. VOIP (Voice Over The Internet).
2.5. IoT applications and automation.

3. WLAN Protocol Stack:

The main application is to transport IP packets over layers of ISO protocol

- A number of management operations defined in layer 2 to address the wireless nature of the network.
- Layer 1 (physical layer) is a new development as WLAN uses airwaves instead of cables.

4. WLAN System Architecture:

4.1. Configuration1:

AD-Hoc mode:

- Two or more wireless devices communicate with each other directly.

- all devices are equal and Packets exchanged directly between two devices.

- All devices share the same medium, the Packets are received by all stations observe the channel However all stations except the intended recipient discard the incoming Packet.

  To configure Ad-hoc N-W

  The network must have a name [service set identity SSID].

  all users select the same Frequency Channel number.

  all users use the same Ciphering key.

  individuals IP address has to be configured in every device.

4.2. Configuration2:

Infrastructure Mode:

- Suitable to access to Local N.W and Internet.
- Access Points (AP)s used as a gateway between all wifeless and wireline Networks for all devices of the Basic Service set [BSS].
- If device A wants to send data Packet to device B packet is first sent to AP and it resends Packet to the destination address of device B.

5. Infrastructure Mode:

5.1. Advantages:

Two wireless devices can communicate with each other over a larger distance with AP in the middle.

5.2. Disadvantages:

A packet that is transmitted between two wireless devices has to be transmitted twice over the air.

6. Ad-Hoc NW Configuration:

To configure Ad-hoc N-W

The network must have the name [service set identity SSID].
All users select the same Frequency Channel number.
All users use the same ciphering key.
Individuals IP address has to be configured in every device.

7. WLAN Standards:

IEEE 802.11a 54 Mbps, 5 GHz PHY layer standard,1999
IEEE 802.11b Enhancements to 802.11 to support 5.5 and 11 Mbps,1999
IEEE 802.11c Bridge operation procedures [now included in the IEEE 802.1D],2001
IEEE 802.11d Country-to-country roaming extensions ,2001
IEEE 802.11e Enhancements: QoS, including packet bursting,2005
IEEE 802.11f Inter-Access Point Protocol [Stands Cancelled] 2003
IEEE 802.11g 54 Mbps, 2.4 GHz standard (backward compatible with b),2003
IEEE 802.11h Spectrum Managed 802.11a (5 GHz) for European compatibility,2004
IEEE 802.11i Enhanced security,2004
IEEE 802.11j Extensions for Japan,2004
IEEE 802.11k Radio resource measurement enhancements,2007
IEEE 802.11m Maintenance of the standard
IEEE 802.11n Higher throughput improvements using MIMO, 2009
IEEE 802.11w Protected Management Frames,2009

Standard	Frequency band	Theoretical max data rate
802.11b	2.4GH	1-11Mbps 6-54 Mbps
802.11g	2.4 GH	6-54 Mbps
802.11a	5 GH	6-600 Mbps
802.11n	2.4 GH/5 GH	Up to 6.93Gbps
802.11ac	S GH	Up to 6.76Gbps
802.11ad	60 GH	802.11b

<u>IEEE 802.11n</u>

Finally published in 2009, the aim of the IEEE 802.11n is to increase the MAC layer throughput from the previous standards. First conceived in the year 2002, the IEEE 802.11n task group has been studying various enhancements to the physical and MAC layers to improve throughput.
These enhancements include such items as changes to signal encoding schemes, multiple antennas, smart antennas, and changes to MAC protocols.
IEEE 802.11n introduced new MAC layer mechanisms to increase throughput. The standard uses MIMO and various new modulation and coding mechanisms to increase the data rates. The standard uses a fixed channel bandwidth of 20MHz, which is useful for backward compatibility with older standards. IEEE 802.11n also possesses an optional 40MHz channel.
Data rates up to 600 Mbps are achieved only with the maximum of four spatial streams using one 40 MHz-wide channel.
In order to increase the MAC layer efficiency, two new mechanisms were introduced in IEEE 802.11n.
These were:

1. Frame Aggregation
2. Block Acknowledgement

In the previous MAC layer, an STA waits for some time after sending a MAC frame. There is severe underutilization when the MAC frames are small.

The frame aggregation technique enabled STAs to aggregate small frames into larger ones.
To maximize efficiency, the maximum frame size is increased thereby allowing longer frames.
The Block Acknowledgement method discussed earlier is similar to the machine with the same name as in IEEE 802.11e

IEEE 802.11ad

The IEEE 802.11ad also known as WiGig is a relatively new standard published in December 2012. Its specification adds a "fast session transfer" feature, enabling the wireless devices to seamlessly transition between the legacy 2.4 GHz and 5 GHz bands and the 60 GHz frequency band.
To operate with optimal performance and range criteria, the IEEE 802.11ad provides the ability to move between the bands ensuring that computing devices are always "best connected," Through the vast improvements in spectral reuse at 60 GHz and efficient beamforming technology, IEEE 802.11ad enables great improvements in capacity.
Many users in a dense deployment can all maintain top-speed performance, without interfering with each other or having to share bandwidth as with the legacy
frequency bands.
The likely enhancements to 802.11 beyond a new 60 GHz PHY include MAC modifications for directional antennas,
personal basic service set, beamforming, fast session transfer between PHYs, and spatial reuse.

IEEE 802.11ac

One of the important standards currently under development is IEEE 802.11ac.
This standard is expected to be published by the end of 2014.
It is expected to provide a multi-station WLAN throughput of at least 1 Gbps and a single link throughput of at least 500 Mbps. This is achieved by extending the air interface concepts which are embraced by 802.11n like wider RF bandwidth (up to 160 MHz), more MIMO spatial streams (up to 8), multi-user MIMO, and high-density modulation.

8. WLAN Standards Cont.:

IEEE 802.11e

IEEE 802.11e was deployed in 2005 and is an important amendment to the IEEE 802.11 standard that provided a set of Quality of Service enhancements for wireless LAN applications through modifications to the Media Access Control (MAC) layer.

As discussed earlier, IEEE 802.11e accommodated time-scheduled and polled communication during null periods when no other data is moving through the system.

In addition, IEEE 802.11e improves polling efficiency and channel robustness. These enhancements should provide the quality which is necessary for services such as IP telephony and video streaming.

In a QSTA, a hybrid coordination function (HCF) replaces modules for a distributed coordination function (DCF) and point coordination function (PCF).

The HCF consists of enhanced distributed-channel access (EDCA) and HCF-controlled channel access (HCCA). EDCA extends the existing DCF mechanism to include priorities.

As with the PCF, HCCA centrally manages medium access.

IEEE 802.11f

To provide for wireless access point communications among multivendor systems, the IEEE 802.11f or Inter-Access Point Protocol was a recommendation that described an optional extension to IEEE 802.11. In addition to providing communication among WLAN stations in its area, an AP can also function as a bridge that connects any two 802.11 LANs across another type of network, such as an Ethernet, LAN, or a WMAN.

Thus, IEEE 802.11f facilitated the roaming of a device from one AP to another while ensuring transmission continuity. IEEE 802.11f standard was a Trial Use Recommended Practice and so the standard was later withdrawn by the IEEE 802 executive committee in 2006.

IEEE 802.11h

The European Union Military uses part of the 5 GHz frequency band for satellite and radar communication in addition to the IEEE 802.11a signals. So to handle such situations, IEEE 802.11h introduced two mechanisms. These were

1. Dynamic Frequency Selection (DFS)

2. Transmit Power Control (TPC)In the DFS scheme, the AP detects other networks operating in the same frequency band and changes the operating frequency of the WLAN to prevent a collision. On the other hand, TPC is used to keep the signal level below a certain preset level if there is a satellite signal in the nearby channels. Moreover, TPC can also be used to improve the link condition by switching over the working frequency to a more suitable channel that is clearer and also reduce power consumption [19].

The aim of the IEEE 802.11i standard was to address security issues. The security and authentication mechanisms at the MAC layer were defined in this standard. It addressed the security deficiencies in the Wired Equivalent Privacy (WEP) algorithm originally designed for the MAC layer of 802.11 [22-23]. Wired Equivalent Privacy (WEP) was shown to have security vulnerabilities.

IEEE 802.11w

The IEEE 802.11w was published in 2009 as an add-on to 802.11i covering management frame security. It introduces protected management frames with the help of mechanisms that enable data origin authenticity, data integrity, and replay protection

9. Limiting Interference between AP and ESS:

All APs of Ess is located in the same IP subnet.
All APs use the Same - SSID
All APs have to Send oN different frequencies.
The coverage of areas of different APs should overlap so the Client doesn't lose a message in border areas.

10. MAC Frame:

WLAN MAC frame format contains CSMA / CA and RTS / CTs; the CSMA / CA protocol is a carrier sensor that can have multiple access with collision avoidance, it functions as sending the signal only when the medium is free, but doesn’t send when the medium is busy. RTS and CTs avoid terminal problems.

11. GPS satellite blocks:

A beacon frame contains network information needed by a station before it can transmit a frame. They are used for announcing the presence of devices in a WLAN as well as synchronization of the devices and services.

Beacon frames are used as a part of BSS (basic service set). In infrastructure BSS, there are access points (APs) that are wireless routers forming the base stations for access. All the devices communicate with each other through APs. The APs transmit beacon frames periodically so that the devices know the status of the network channel. An independent BSS, devices communicate on a peer-to-peer basis and so beacon generation is distributed among the devices.

Frame body: Frame, a destination address, source address, capability information, DSPS, CFPS, TIM, FCS, DS

The body frame parts functionality:

- Timestamp − It is the time associated with the beacon frame. It helps in the synchronization of the devices in the WLAN. The devices update their local clocks according to the timestamp of the beacon frame.
- Beacon interval − The time gap between two consecutive transmissions of a beacon frame.
- Capability information − It contains information about the capability of the network. Sometimes referred to as the type field, it determines whether the network is infrastructure-based or ad hoc.
- SSID − Service Set Identifiers that serve as network names.
- Supported rates − It defines the transmission rates permitted by the channel.
- Frequency-hopping (FH) Parameter Set
- Direct-Sequence (DS) Parameter Set
- Contention-Free (CF) Parameter Set
- Traffic indication map (TIM) − It is a bitmap used in IEEE 802.11. The AP sends TIM periodically since a station needs to listen to at least one beacon during the beacon interval.

12. Ack Frame:

All APs of Ess is located in the same IP subnet.
All APs use the Same - SSID
All APs have to Send on different frequencies.

The coverage of areas of different APs should overlap so the Client doesn't lose a message in border areas.

13. CSMA/CA Protocol:

Carrier Sense Multiple Access with Collision Avoidance can listen, detect Standard medium Before node transmits data it checks or listens to the medium when the medium is free it sends its signal and when the medium is busy it waits for a random time and then tries again.

14. RTS And CTS Frame Formats:

If the terminal senses idle Medium, it sends an RTS Signal.
If APs see that no other terminal is transmitting APs send CTS Signal to the terminal.
If AP Was Busy, then the terminal waits a random time then sends another PTs signal to the AP.

The RTS frame contains five fields, which are:

- Frame Control
- Duration
- RA (Receiver Address)
- TA (Transmitter Address)
- FCS

The CTS frame contains four fields, which are:

- Frame Control
- Duration
- RA (Receiver Address)
- FCS

15. DSSS:

DSSS is sending the complementary of the sequence instead of the sequence.

It’s useful for avoiding the problem of multipath fading.

16. DSSS Cont.:

For 1 Mbps transmission in WLAN 11b, information bits are first grouped into blocks of 4 bits each. The first 2 bits are mapped and the rest of the two bits are mapped as per the CCK sequence. CCK uses code words to carry information signals. In other words, it spreads the data signal. Several phase angles are typically used to generate complex codewords of 8 bits.

For 11Mbps transmission in WLAN 11b, information bits are first grouped into blocks of 8 bits each. Then out of these 8 bits, 2 bits are encoded by a phase shift of the transmitted symbol relative to the previous symbol. The rest of the 6 bits are encoded using CCK.

17. OFDM:

orthogonal frequency division multiplexing is used to solve the problem of multipath fading

To solve the problem we

- Break up the signals into multiple low rate streams
- Each stream suffers from an almost flat narrow bandwidth channel
- Each is modulated over orthogonal frequency then simple equalization.

18. MIMO:

MIMO stands for multiple input multiple outputs

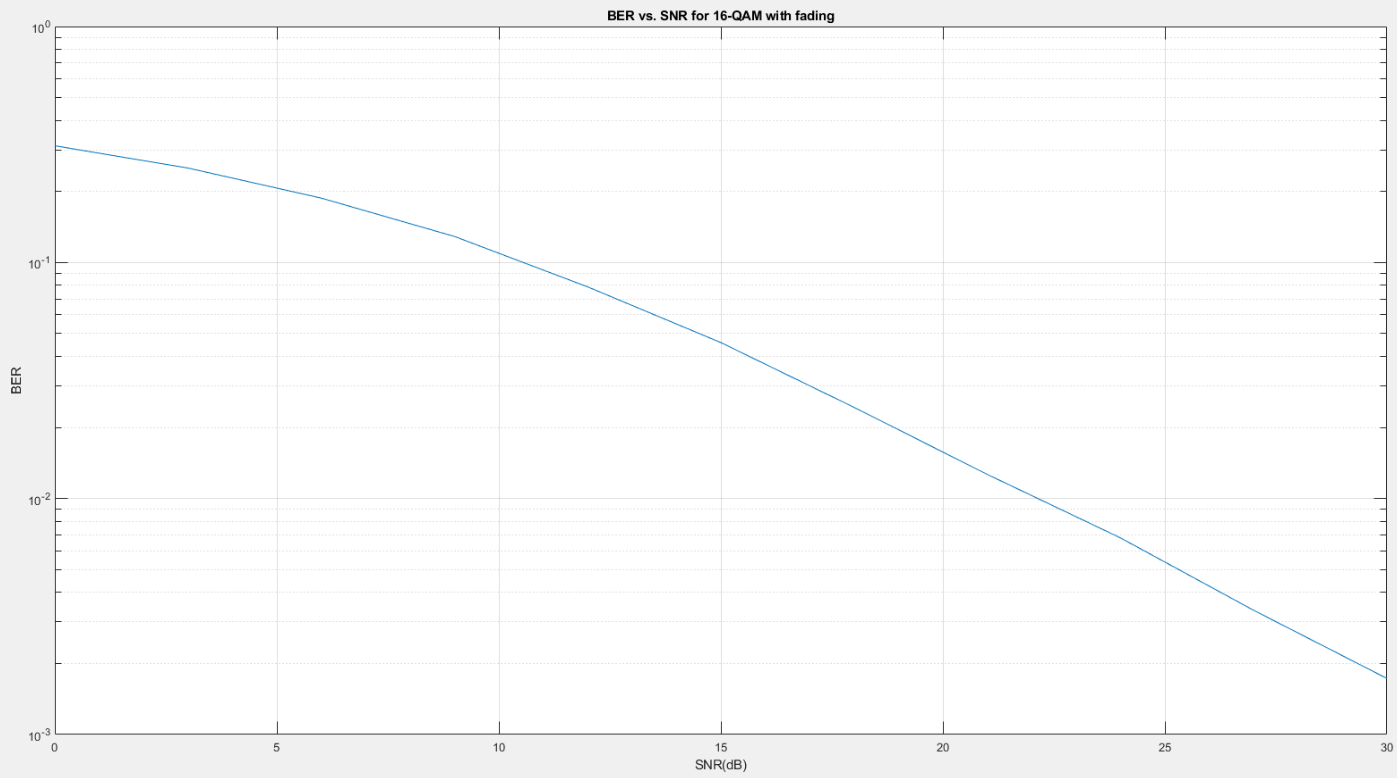
Use of multiple antennas in tx and RX

- Spatial multiplexing: split data across antennas (increase data rate)
- Diversity: send multiple copies of the same data to ensure correct reception (lower Ber)

Part 2: Experiment Related Questions

1. The type of antenna in it is MRF24WB0MA
2. In the code we will find SSID variable so I can change it to the name I want.
3. In the code we will find channels variable with values from 1 to 11 so i change all of them to the number of the channel I want
4. To change the mode of WLAN from Infrastructure to Ad-hoc We open the cmd and write this command: netsh wlan set profileparameter <ssid> connectiontype=ibss
   And we replace <ssid> with the SSID of out network.

Part 3: Mini-Simulations



```
clc; clear all; close all;
%% Initialization
Frames = 1000; %Number of Frames
fft_size = 128; %FFT Size (Number of subcarriers)
M = 16; K = log2(M); %16-QAM Modulation
delta = 312.5*10^(3); %Carrier Separation
delay_spread = 0.2*10^(-6); %Delay Spread
SNRdb = 0:3:30; %SNR Range in dB
delay_spread_max = delay_spread*fft_size*delta; %Number of paths
msg_size_bits = K*fft_size;
msg_size_symbols = msg_size_bits/K;
BER = zeros(length(SNRdb),Frames);
BER_avg = zeros(length(SNRdb),1);
%%
for i = 1:length(SNRdb)
for k = 1:Frames
%% Message Generation
msg_bits=randi([0,1],msg_size_symbols,K);
msg = bi2de(msg_bits,'left-msb')';
%% QAM Modulation
msg_mod = qammod(msg, M, "UnitAveragePower", true);
%% IFFT
msg_ofdm = sqrt(fft_size) * ifft(msg_mod);
```

```
%% ADD Cyclic Prefix
CP = msg_ofdm(end-31:end);
msg_CP = [CP msg_ofdm];
%% Channel (fading + noise)
[fadedSamples, gain] =ApplyFading(msg_CP,1,delay_spread_max);
msg_rx=awgn(fadedSamples,SNRdb(i),'measured');
%% Cyclic prefix removal
msg_rx_CP = msg_rx(33:end-7);
%% Freq domain equalization
msg_rx_fft = fft(msg_rx_CP)/sqrt(fft_size);
msg_eq = msg_rx_fft ./ fft(gain,128);
%% QAM Demodulation
msg_demod = qamdemod(msg_eq, M,"UnitAveragePower", true);
msg_demod_bits = de2bi(msg_demod,'left-msb');
%% BER calculation
[~,BER(i,k)] = biterr(msg_demod_bits,msg_bits);
BER_avg(i) = sum(BER(i,:))./Frames;
end
end
%% Plotting BER vs. SNR
figure
semilogy(SNRdb,BER_avg)
title('BER vs. SNR for 16-QAM with fading');
xlabel('SNR(dB)')
ylabel('BER')
grid on
```