**WiFi Training Program - Module 3 Assignment Answers**

**Q1.**

DIFFERENT IEEE 802.11 PHY STANDARDS :

1) IEEE 802.11 - 1997 (Wifi - 1)

a. It is the first ever wifi standard

b. It uses 2.4 GHz wifi frequency

c. Modulation techniques like DSSS (with 11 bit barker code and barker inversion for 0 bit), FHSS (2.5 times per second frequency change) were used.

d. Maximum speed of 2 Mbps was supported with no security features and with no advancements.

2) IEEE 802.11a - 1999

a. Here, entirely different specifications was used.

b. It used 5 GHz wifi frequency for avoiding interference (technology congestion)

c. It used OFDM modulation combined with other modulation schemes for subcarriers to improvise data rate. (here, the signal is divided into multiple subcarriers where each are frequency flat and orthogonal to each other avoiding ISI. Each subcarrier may have different modulation schemes improvising data rate. It also uses guard band to safeguard information in one subcarrier from another. It uses cyclic prefix technique that copies the last portion of OFDM symbol in front to protect it from the effect of multipath propogation)

d. Therefore, maximum theoretical data rate was 54 Mbps.

e. However, it supported very short range only due to maximum attenuation or power loss.

3) IEEE 802.11b - 1999 (Wifi - 2)

a. It was the first mass adopted wifi standard.

b. It used DSSS modulation (Original data is multiplied with PN sequence called chip sequence and therefore widening the spectrum of data transmission effectively reducing the PSD thus enabling signal robustness against jamming identification. Moreover, signal can be decoded iff the exact PN sequence used is known in receiver side. It also makes the signal less affected by narrow band interference) with CCK (Complementary Code Keying - 8 bit Chip CC)

c. Theoretical maximum data rate was 11 Mbps.

d. It used 2.4 GHz wifi frequency.

e. However, it was more susceptible to interference due to technological congestion that is technologies like microwave oven, Bluetooth has same centre frequency.

4) IEEE 802.11g - 2003 (Wifi - 3)

a. It was speed boosted version of both a and b substandards.

b. It used 2.4 GHz wifi frequency as like in 802.11b

c. It used OFDM modulation as like in 802.11a (52 carriers among which 4 for pilot sequences with 64 point FFT)

d. Theoretical maximum data rate was 54 Mbps.

5) IEEE 802.11n - 2009 (Wifi - 4)

a. It was entirely different standard since it introduced the idea of using dual wifi frequencies that is both 2.4 and 5 GHz frequencies in action.

b. It used MIMO in the architecture for establishing multiple frequency fading parallel streams to serve many users without hassle. (4\*4 MIMO) with frame aggregation and short guard interval (400 or 800 ns)

c. It widens the channel bandwidth from 20 to 40 MHz therefore improvising data rate.

d. It uses OFDM modulation scheme.

e. Theoretical maximum data rate was around 600 Mbps

6) IEEE 802.11ac - 2013 (Wifi - 5)

a. It was termed as "Gigabit Wifi Standard"

b. It uses only 5 GHz wifi frequency

c. It uses OFDM modulation but with 256 QAM for subcarriers to improvise data rate and stabilise SNR

d. It introduced MU-MIMO in the architecture. (It uses multiple antenna array and creates that many independent spatial parallel streams and serves by beamforming)

e. It introduced beamforming to focus Wifi signals towards intended clients.

f. Theoretical maximum data rate was around 6.9 Gbps

g. Channel got widened upto 80 / 160 MHz.

7) IEEE 802.11ax - 2019 (Wifi - 6 and Wifi - 6E)

a. It used triple frequencies that is 2.4, 5, 6 GHz (in wifi-6E substandard) wifi frequencies.

b. It introduced OFDMA - with 1024 QAM for serving more users simultaneously without affecting the quality of connectivity

c. It introduced BSS coloring - that is to avoid unnecessary deferring of transmissions therefore enhancing the channel utilization. (Generally, if APs uses same frequency channels nearby, it interferes with each other. Therefore, devices wait before transmission if they detect a signal from different network too. Each AP will be assigned a color - identifier. Now, devices check BSS color field in HE signal field in PHY header and if same color detected as of its BSS, it defers the transmission thereby showing regular behaviour if not, it treats it as external interference and if RSSI < CCA threshold, it may continue the transmission)

d. It introduces TWT (Target Wake Time) to improvise the battery life of devices

e. Theoretical maximum data rate was around 9.6 Gbps

8) IEEE 802.11be - Upcoming standard (Wifi - 7)

a. It also uses triple frequencies as like in wifi-6 and 6E

b. It uses OFDMA - 4096 QAM combination to maximise data rate. (it is the extension of OFDM which issues subcarriers (in the name of Resource Units) to users based on the data that need to be transmitted) providing QoS and best channel utilization.)

c. It improvises MIMO for more spatial streams

d. It uses MLO (Multi Link Operation) to use multiple channel with multiple frequencies for serving more clients with QoS (Wifi traditionally operates on single channel at a time. It uses Load balancing (packet scheduling) and aggregation to utilize the air media in the best manner. It is of two types - Simultaneous or active MLO - uses multiple bands at same time and alternating or switching MLO - that switches between links dynamically but one at a time).

Types:

1. Link Aggregation - combining multiple channels for enhanced throughput

2. Load balancing - shifts traffic across links dynamically but one at a time.

3. Redundancy - if one link fails, it shifts traffic to other links.

e. Theoretical maximum data rate was around 40 Gbps

f. Channel got widened upto 320 MHz.

**Q2.**

FHSS

1. Frequency Hopping Spread Spectrum.

2. the carrier frequency of the transmitted signal hops (changes) over a wide range of frequencies with respect to time.

3. It differs from FDM in the way that FDM doesn't change the frequency with respect to time.

4. It works based on PN sequence.

5. It offers resistance towards narrowband interference.

6. It offers security by making it hard to intercept without knowing hop pattern.

7. It uses primarily FSK as baseband modulator and then followed by Synthesizer which takes up the carrier frequency based on the current PN sequence and mapping among hop set.

8. Slow Frequency Hopping is the type where symbol rate is greater than hop rate that is carrier frequency hop spans multiple bits.

9. Whereas, fast frequency hopping is the type where symbol rate is lesser than hop rate that is multiple hops happen per symbol.

10. It requires very tight synchronization between sender and receiver.

11. It has some parameters like :

1. Number of hop frequencies or hop set length

2. Hop rate - Hops per second

3. Symbol rate - symbols per seconds.

4. Chip duration - duration of one hop (duration of jump that depends on PN seq length)

5. Dwell time - time the signal stays on one frequency

6. Hop bandwidth - freq space occupied at any hop - 2 \* del(f) + baseband bw

7. It trades spectral efficiency for security since it may occupy more bandwidth

12. Three solutions for synchronization between sender and receiver in FHSS.

1. With separate control channel, transmitter may send information like seed, hop rate, starting timestamp etc.

2. Blind sync - here, receiver detects energy in the possible spectrum and correlate with known symbol to get hop pattern.

3. For every hop, barker code like known pattern will be placed for recovering time and frequency misalignments if any.

DSSS:

1. Direct Sequence Spread Spectrum Modulation techniques is one of the very popular modulation schemes that was in use in wifi technology.

2. It basically extends or widens the bandwidth of the data being transmitted to larger bandwidth

3. Thereby reducing Power Spectral Density so as to avoid Narrow Band Interference

4. This also lets the signal get hidden under environmental noise to avoid information tapping.

5. It also enables the security to avoid eavesdropping by using unique PN sequence per session/user to extend the bandwidth by multiplying each bit of information with this chip sequence and transmits with 2.4 GHz carrier signal (spreading )thus making it harder to decode without using proper PN sequence in receiver side.

6. It also enables continuous transmission instead of FHSS which switches Frequency in realtime and expects frequency synchronization in receiver side for proper decoding.

7. It also offers spreading gain while dispreading the information in receiver side. (10 log (chip rate / baseband data rate))

8. It helps in achieving higher data rates like 11 Mbps in 802.11b wifi standard.

9. However it offers limited scalability due to unique PN sequence requirement.

10.It can’t avoid Wide Band Interference and inefficient spectrum usage

**Q3.**

USE OF MODULATION SCHEMES IN PHY LAYER IN WIFI

1. Modulation is the process of mapping input bits into symbols and eventually to waveforms for transmission.

2. It defines how carrier waveform (final form in air) is manipulated (amplitude, phase, frequency)

3. It defines the spectral efficiency by packing as many bits per Hz.

4. Generally, any bit stream will be broken per K bits and will be mapped as symbol and corresponding I and Q phases are used (as per constellation diagram) and accordingly waveform will be chosen (I corresponds to cosine part and Q corresponds to sine part of the wave - s(t) = I cos(2 pi f t) - Q sin(2 pi f t)) - QAM (16,64,256,1024,4096 bits/symbol)

5. In recent standards, this modulation techniques are combined with OFDM to increase bit rate in proportion to the number of sub carriers.

6. In constellation map, if more points are included, more bits/symbol will be created thereby increasing data rate but at the cost of reduced distance between points in map therefore leading to less resistance to noise or SNR degradation. (therefore, higher modulation requires high SNR and higher coding rate)

7. In prior to modulation, input bits will be undergoing source coding which is the process to reduce the redundant bits thereby compressing effective payload. Followed by, channel coding which is the process of adding redundant bits to the effective payload to detect and correct errors due to channel in receiver side. (channel coding - scrambling, interleaving, FEC)

8. In modern network, Rate Adaptation algorithm is employed which chooses the modulation scheme dynamically based on channel condition (RSSI, SNR, PER)

VARIOUS MODULATION SCHEMES USED ACROSS WIFI GENERATIONS

1. Wifi - 1 and 3 uses primarily the DSSS and CCK (Complementary Code Keying - it works well with DSSS which takes the modulated symbol bits and groups it again to form more complex yet orthogonal series of symbols to be processed for reducing cross talks between symbols and proved to be offering more resistance)

DSSS with 11 bit chip sequence and CCK for 5.5 and 11 Mbps

2. Wifi - 2,3 (with DSSS, CCK),4 (with MIMO),5 (with MU-MIMO) uses OFDM primarily with varying subcarriers and sub modulations of subcarriers improvising data rate.

OFDM with varying FFT sizes (64,128,512,1024,2048,4096) and varying submodulation schemes.

More bits/symbols require very clear channel but offers higher spectral efficiency and data rate.

OFDM is used to combat multipath fading, narrowband interference, frequency selectiveness.

For input bitstream, it should be grouped into K bits and to be applied the appropriate modulation scheme to map to symbols and map each symbol to each subcarrier and leave spaces for Null and Pilot sequences in OFDM symbol (1 OFDM symbol = complex symbols based on modulation tech and nulls and pilot values), followed by IFFT for these freq domain data to convert to time domain data (each IFFT result data is the N number of sinusoid orthogonal subcarriers whose amplitude and phase are decided by the symbols from modulation scheme).

Cyclic prefix is attached for making sure that delayed copies due to frequency selectiveness or multipath propagation effects and finally, the samples are converted to analog and RF front end takes over and transmits with I and Q values splitted from these final samples in the air.

3. Wifi - 6 (with MU-MIMO),7 (with MLO) uses OFDMA

Here, DCM (Dual Carrier Modulation) is introduced where same symbol is modulated across two subcarriers with conjugation for transmissions in lower SNR environments.

**Q4.**

OFDM FOR WLAN

1. Since the channel as LTI filter smearing the symbols across time , ISI will be created thereby copies of the same signal with different delay may reach receiver.

2. OFDM combats this by splitting the channel to multiple subcarriers reducing the frequency selective nature.

3. Offers much longer symbol duration (though expensive at receiver end) than that of delay spread.

4. Attaching cyclic prefix with OFDM symbol converts works against ISI (linear to circular convolution)

5. Even if some subcarrier data is lost, majority of the data reaches receiver. Moreover, Pilot sequences in the front of OFDM symbol helps in assessing the channel for receiver.

6. Tight spectral packing of subcarriers when compared to conventional FDM by ensuring orthogonality between subcarriers.

7. Adaptive bit loading uses higher modulation for good subcarriers dynamically.

8. Receiver setup becomes single tap equalizer for each subcarrier.

9. OFDM paves the way for advancements such as MU-MIMO enabling multiple streams per subcarrier, Beamforming for phase control per subcarrier, allocating different subcarriers to different users serving multiple users simultaneously, TWT scheduling of OFDM symbols for power saving.

**Q5.**

WIFI FREQUENCY BANDS

1. Basic 2.4 GHz band which is only 83.5 MHz wide supporting primarily 20 MHz channels (sometimes 40 MHz in 802.11n)

However, there are only 3 non-overlapping 20 MHz channels available in 2.4 GHz spectrum

Offers higher range but lesser data rate , preferred in congested scenario.

There are 14 channels in total within which 1, 6, 11 with 2414, 2437 and 2462 Hz being central frequencies are non overlapping.

2. 5 GHz band - around 700 MHz wide spectrum with 20 (25+ non overlapping channels), 40 (2 Nos), 80 (4 Nos), 160 (8 Nos)MHz channels available by bonding.

However, DFS is strictly required since radar intervention may occur in 5 GHz or surrounding frequencies. AP must vacate the channel withiin 10 seconds if so.

Unlicensed National Information Infrastructure primarily focusses on this band and releases many channels for both indoor and outdoor purposes with and without DFS.

3. 6 GHz band - around 1200 MHz wide spectrum with 50+ 20 MHz (233+) , 29 40 MHz , 14 80 MHz, 7 160 MHz and 3 320 MHz non overlapping channels.

Without DFS requirement and any other interference.

But severely affected by Range and attenuation.

Makes it ideal for OFDMA , low latency AR/VR and high data rate applications.

4. 60 GHz band - around 14 GHz wider band with each channel being gigabit wide for ultra high speed data applications

But suitable only for very short range communications as it easily gets absorbed even by oxygen in atmosphere.

3 20,40 MHz , 25 80,160 MHz, 59 320 MHz, 4 2.16 GHz non overlapping channels

**Q6.**

GUARD INTERVAL :

1. It is the time duration inserted between consecutive OFDM symbols to let receiver absorb any delayed versions of previous symbols due to multipath propagation.

2. Guard intervals will not be left empty or null rather in that duration, portion of OFDM (last) will be occupied in front for tackling the effect of tail overlapping.

3. Guard interval = cyclic prefix duration which simplifies the FFT equalization in receiver.

4. It will be effective iff duration of guard interval is greater than maximum delay spread.

5. However, more guard interval may reduce throughput as it is occupied with redundant data.

6. Thus choosing guard interval depends on the environment (Office - 200 to 300 nS since RMS delay spread is around 100 nS , Residential - 500 nS since RMS delay spread is around 200 nS, Stadium - 1 uS since RMS delay spread is around 500 nS)

7. Short GI (0.4 uS) is acceptable in low multipath areas like small homes offering higher throughput.

8. Standard GI (0.8 uS) in most indoor environments

9. Long GI (1.6-3.2 uS) in stadiums

**Q7,Q10,Q11,Q12.**

PHYSICAL LAYER IN WIFI

1. PHY layer is responsible for encoding and transmitting data over the wireless medium. It consists of three primary sublayers:

PMD (Physical Medium Dependent) Sublayer – Handles modulation and RF signal transmission.

PLCP (Physical Layer Convergence Procedure) Sublayer – Prepares data for transmission and manages synchronization.

PHY Management – Deals with state control, channel sensing, and power control

PMD sublayer:

1. It is the underlaying PHY layer to transmit the information in air thereby deciding the crucial RF, modulation and coding parameters , FEC , Antenna processing, Power control, Carrier sensing and interacts directly with RF front end.

PLCP sublayer:

1. It is responsible for framing, synchronization, error detection.

2. It comes before PMD defining all the required parameters and letting PMD complete the transmission by defining Modulation, RF parameters as discussed earlier.

3. It accepts MAC layer payload (MSDU) and adds PHY layer header PPDU by adding headers, preamble.

PHY management sublayer:

1. It controls the overall operation of PHY layer by channel scanning, dynamic power, gain control, Interference avoidance, channel assessment etc.

2. PPDU varies with respect to Wifi generations. General format of PPDU is Preamble - Header - PSDU (MAC layer payload)

3. In 802.11b :

\* Preamble is split into Synchronization (helps receiver lock in the signal) and Start Frame Delimiter (to let receiver know the start of the frame)

\* Header is split into Signal (Indicating the data rate), Service (Reserved for future use), Length (Entire frame length or duration), CRC (for PPDU)

4. In 802.11g :

\* Preamble is split into STF (Short Training Field - for Time synchronization (important in OFDM since without which symbol cannot be retrieved.) using autocorrelation between STF and received symbol to find start of OFDM symbol probably the STF) and LTF (Long Training Field - for Channel estimation)

\* Header is noted here as Signal field with Rate (indicating modulation scheme with data rate), Length (duration of packet), Parity (for error detection) and Tail (For signal integrity)

5. In 802.11n (High Throughput PPDU) :

\* L-SIG (Legacy field) for Rate, length, modulation scheme

\* L-STF (For AGC and timing sync)

\* L-LTF (For channel estimation)

\* HT Preamble - contains HT SIG1 (containing MCS, bandwidth, other transmission parameters) , HT STF (for MIMO channel estimation), HT LTF (for Equalization)

\* HT Header - contains HT SIG2 (for guard interval, STBC, coding), Service (for scrambler initialization and future use), Length (PSDU length), Tail (Convolutional decoding), CRC (for PPDU)

6. In 802.11ac (Very High Throughput PPDU)

\* L-SIG (Legacy field) for Rate, length, modulation scheme

\* L-STF (For AGC and timing sync)

\* L-LTF (For channel estimation)

\* VHT-SIGA1 and SIGA2 (for MCS, bandwidth, coding)

\* VHT-STF (for channel estimation

\* VHT-LTF (for equalization)

\* VHT-SIGB (for MU-MIMO related information)

\* VHT-Service (scrambler initialization and future use)

\* VHT-Length (frame length in bytes)

\* VHT-Tail (for convolutional decoding)

\* VHT-CRC (for error detection)

7. In 802.11ax (High Efficiency PPDU)

\* L-SIG (Legacy field) for Rate, length, modulation scheme

\* L-STF (For AGC and timing sync)

\* L-LTF (For channel estimation)

\* VHT-SIG-A and SIG-B (for MCS, bandwidth, coding and OFDMA , MU-MIMO related information in SIG-B)

\* VHT-STF (for AGC)

\* VHT-LTF (for channel estimation)

\* VHT-Service (scrambler initialization and future use)

\* VHT-Length (frame length in bytes)

\* VHT-Tail (for convolutional decoding)

\* VHT-CRC (for error detection)

MCS

1. It stands for Modulation, Coding Scheme, Spatial streams that ultimately defines the data rate (approximately throughput) of wifi transmission.

2. Tradeoff between data rate and SNR requirement with respect to MCS Index.

3. Formula for finding throughput is as follows:

throughput = ((number of data subcarriers) \* (number of spatial streams) \* (coding) \* (number of coded bits per subcarrier per stream)) / (OFDM symbol duration + guard interval)

**Q8.**

**OFDM AND OFDMA**

OFDM :

1. Splits a high-rate stream into many low-rate parallel streams over orthogonal subcarriers.

2. Single-user can only access the channel at a time.

3. Introduced in 802.11a/g/n/ac

4. Inefficient for small packets or multiple users.

5. Works with smaller FFT sizes when compared to OFDMA

6. Medium access is controlled by CSMA/CA (contention-based).

7. Offers moderate spectral efficiency

8. Latency increases in dense networks.

9. Easier receiver sync when compared to that of OFDMA

10. Ideal for high throughput single user devices

OFDMA :

1. It allows multiple users to transmit/receive on different sets of subcarriers simultaneously

2. Thereby Multi-user can access the channel at any time.

3. Introduced in 802.11ax (Wi-Fi 6) and 802.11be (Wi-Fi 7)

4. Scheduler divides subcarriers into Resource Units (RUs)

5. Efficient for IoT, mixed traffic and dense network applications

6. Parallel data transmission is enabled via RU which is split to users based on priority and data traffic.

7. It uses higher FFT size when compared with that of OFDM for finer RU granularity

8. Trigger Frames (from AP) allocate RUs for uplink and Multi-user Downlink is broadcast with specific RU mapping thereby controlled via centralized scheduling.

9. Subcarrier Water filling (power control) algorithm per RU is possible

10. But all users should be in perfect sync during reception which is complex to achieve.

11. OFDMA is more scalable than OFDM.

**Q9.**

**MIMO and MU-MIMO:**

MIMO

1. Introduced in 802.11n (Wi-Fi 4)

2. Offers spatial multiplexing for one user mainly if receiver understands channel (CSR) if not, then multiplexing efficiency can be compromised by using Alamouti-STBC

3. Uses multiple transmit and receive antennas.

4. Each spatial stream carries independent data.

5. Streams are separated using spatial diversity and channel estimation at the receiver.

6. Applied in both uplink and downlink streams.

7. Receiver should estimate the channel and cancel the effect of interference to get data

MU-MIMO

1. Introduced in 802.11ac (downlink), 802.11ax (DL/UL)

2. Offers Spatial multiplexing for multiple users

3. Multiple users per transmission interval

4. Efficient in dense networks

5. Access Point (AP) uses spatial beamforming to steer data to different users.

6. Requires advanced scheduling and Channel State Information (CSI).

7. Precoding will be required to get data with minimal cross talk.

8. Scheduler is required which groups users based on channel orthogonality, QoS etc.